UNIVERSIDADE DO PORTO
FACULDADE DE ENGENHARIA

Segurança em Redes de Computadores
–
Estudo de um Caso

Dissertação submetida para satisfação parcial dos
requisitos do grau de mestre em
Engenharia Electrotécnica e de Computadores
(Área de especialização de Telecomunicações)

José Manuel Moreira Estrela

Porto, Setembro de 98



FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Departamento de Engenharia Electrotécnica e de Computadores

Segurança em Redes de Computadores

—

Estudo de um Caso

José Manuel Moreira Estrela

Mestrado em Engenharia Electrotécnica e de Computadores
pela Faculdade de Engenharia da Universidade do Porto

Dissertação submetida para satisfação parcial dos
requisitos do grau de mestre
em
Engenharia Electrotécnica e de Computadores
(Área de especialização de Telecomunicações)

681.3(043)EST/SEG
UNIVERSIDADE DO PORTO
Faculdade de Engenharia
BIBLIOTECA H
N.º 43798
CDU
Data ___/___/ 19___

Dissertação realizada sob supervisão de
Professor Doutor José Ruela Fernandes,
do Departamento de Engenharia Electrotécnica e de Computadores
da Faculdade de Engenharia da Universidade do Porto

Porto, Setembro de 98

Índice

Resumo xiii

Summary xv

Prefácio xvii

I. Segurança em Redes de Computadores *1*

1. Introdução 3

1.1 Âmbito do Estudo 3

2. Caracterização do Problema da Segurança em Redes 5

2.1 Objectivos da Segurança 6

2.2 Tipos de Ataques à Segurança 7

2.2.1 Ataques Passivos 8

2.2.2 Ataques Activos 9

2.3 Caracterização dos Ataques 9

2.3.1 O Roubo de *Passwords* 10

2.3.2 Relacionamento "Social" 10

2.3.3 Os *Bugs* e as *Backdoors* 11

2.3.4 Falhas de Autenticação 11

2.3.5 Falhas Protocolares 12

2.3.6 Fuga de Informação 13

2.3.7 Negação do Serviço 14

2.4 Modelos de Segurança 14

2.4.1 Ausência de Segurança 14

2.4.2 Segurança Através da Obscuridade 15

2.4.3 Segurança do *host* 15

2.4.4 Segurança de Rede 16

2.4.5 Nenhum Modelo de Segurança Resolve Todos os Problemas 17

2.5 Estratégias de Segurança 17

2.5.1 Menor Privilégio 17

2.5.2 Defesa Reforçada 18

2.5.3 Ponto de Obstrução 18

2.5.4 Ligação Mais Fraca 18

2.5.5 Postura da *Falha Segura* 19

2.5.5.1 Atitude de Negação por Omissão 20

2.5.5.2 Atitude de Permissão por Omissão 20

2.5.6 Participação Universal 21

2.5.7 Diversidade da Defesa 21
2.5.8 Simplicidade 22
2.6 A Política de Segurança 22
2.6.1 Propósito da Política de Segurança 22
2.6.2 Atributos de uma Política de Segurança 23

3. Análise de Soluções 25
3.1 Autenticação 25
3.1.1 Autenticação de Utilizador 25
3.1.1.1 Passwords 26
3.1.1.2 Passwords de Utilização Única 26
3.1.1.3 Smart Cards 28
3.1.1.4 As Biométricas 28
3.1.2 Autenticação Máquina a Máquina 29
3.1.2.1 Técnicas Criptográficas 29
3.1.3 Controlo de Acesso 30
3.2 A Criptografia 30
3.2.1 Cifragem Convencional 31
3.2.1.1 Cifradores de Bloco e Modos de Operação 32
3.2.1.2 O DES 33
3.2.1.3 O Triple DES 33
3.2.1.4 IDEA 34
3.2.1.5 SKIPJACK 35
3.2.2 Cifragem de Chave Pública 35
3.2.2.1 Mal Entendidos 35
3.2.2.2 Características 36
3.2.2.3 Assinatura Digital 37
3.2.2.4 RSA 38
3.2.2.5 Digital Signature Standard (DSS) 40
3.2.3 Funções de *Hash* Seguras 41
3.2.3.1 MD5 43
3.2.3.2 Secure Hash Algorithm (SHA) 43
3.2.4 Aspectos Legais na Criptografia 44
3.2.4.1 A Situação Actual 44
3.2.4.2 As Restrições nos Diferentes Países 46
3.3 Comunicações Seguras sobre Redes Inseguras 46
3.3.1 O Sistema de Autenticação Kerberos 47
3.3.1.1 Limitações 50
3.3.2 Cifragem ao Nível da Ligação 50
3.3.3 Cifragem ao Nível de Rede e de Transporte 51
3.3.4 A Cifragem ao Nível da Aplicação 53
3.3.4.1 O Protocolo *Telnet* 53
3.3.4.2 Autenticar o SNMP 53
3.3.4.3 Correio Electrónico Seguro 54

3.3.4.4 Um API de Serviço de Segurança 55
3.3.5 Desafios e Soluções para a Segurança 56
3.3.5.1 O Tunnelling Cifrado 56
3.3.5.2 O Secure Sockets Layer (SSL) 59
3.3.5.3 A Identificação e Autenticação Fortezza 61
3.3.5.4 O Secure Electronic Transactions (SET) 62
3.3.5.5 O Secure Multipart Internet Mail Encoding (S/MIME) 63
3.4 Firewalls 64
3.4.1 Vantagens e Desvantagens dos *Firewalls* 64

4. Arquitecturas de *Firewall* 67
4.1 Sistemas de Filtragem de Pacotes 68
4.1.1 Vantagens da Filtragem de Pacotes 70
4.1.2 Desvantagens da Filtragem de Pacotes 70
4.1.3 O Processo de Filtragem de Pacotes 71
4.1.3.1 Protocolos Abaixo do IP 71
4.1.3.2 O Protocolo IP 72
4.1.3.3 O Protocolo TCP 73
4.1.3.4 O Protocolo UDP 74
4.1.3.5 O Protocolo ICMP 75
4.1.3.6 Protocolos da Camada da Aplicação 75
4.1.3.7 Protocolos não IP 76
4.2 Sistemas *Proxy* 76
4.2.1 A Necessidade dos *Proxies* 77
4.2.2 Vantagens dos *Proxies* 78
4.2.3 Desvantagens dos *Proxies* 78
4.2.4 O Funcionamento do *Proxy* 79
4.2.5 *Proxies* de Nível de Aplicação *Versus* de Nível de Circuito 80
4.2.6 *Proxies* Genéricos *Versus* Dedicados 81
4.2.7 Servidores *Proxy* Inteligentes 81
4.2.8 Segurança de Protocolos 82
4.3 O Stateful Inspection 82
4.3.1 Os Requisitos do Stateful Inspection 83
4.3.2 A Tecnologia Stateful Inspection 84
4.3.2.1 O Exemplo FTP 84
4.3.2.2 A Segurança dos Protocolos *Connectionless* tal como o UDP 85
4.4 Arquitecturas de *Firewalls* 85
4.4.1 Arquitectura de *Dual-Homed Host* 85
4.4.2 Arquitectura de *Screened Host* 87
4.4.3 Arquitectura de Subrede *Screened* 88
4.4.3.1 A Rede de Perímetro 89
4.4.3.2 O *Host* Bastião 90
4.4.3.3 O *Router* Interior 90
4.4.3.4 O *Router* Exterior 91

4.4.4 Variações das Arquitecturas de *Firewalls* 91
4.4.4.1 Subrede *Screened* com Múltiplos *Hosts* 92
4.4.4.2 Subrede Screened com *Dual-Homed Host* 93
4.4.4.3 Subrede *Screened* com *Routers* Interior/Exterior Combinados 93
4.4.4.4 Subrede *Screened* com *Host* Bastião *e Router* Exterior Combinados 94
4.4.4.5 Subrede *Screened* com *Host* Bastião e *Router* Interior Combinados 95
4.4.4.6 Subrede *Screened* com Várias Redes Internas 96
4.4.4.7 Subrede *Screened* com Vários *Routers* Exteriores 97
4.4.4.8 Subrede *Screened* com Várias Redes de Perímetro 98
4.5 Firewalls Internos 99
4.5.1 Redes Laboratório 99
4.5.2 Redes Inseguras 100
4.5.3 Redes de Alta Segurança 100
4.5.4 Joint Venture Firewalls 101
4.6 O Futuro dos *Firewalls* 102

5. As Redes Privadas Virtuais (VPNs) 103
5.1 As Tecnologias VPN 105
5.1.1 O Protocolo de Cifragem da Ligação SwIPe 105
5.1.2 O IPSec 105
5.1.2.1 Caracterização da Tecnologia IPSec 106
5.1.2.2 A Gestão de Chaves – Os *Standards* 107
5.1.3 O PPTP 108
5.2 As Tecnologias das Várias Áreas VPN 109
5.3 Perspectivas com as VPNs 109

6. Ferramentas de Monitorização e Diagnóstico 111
6.1 As Alternativas de Segurança 111
6.1.1 A Tecnologia de Segurança Estática 111
6.1.2 A Tecnologia de Segurança Activa 112
6.2 A Monitorização e Controlo Tradicionais 112
6.2.1 Ferramentas de Protecção, Monitorização e Auditoria 113
6.3 Sistemas de Auditoria de Vulnerabilidades e de Detecção de Intrusões 114
6.3.1 1ª Geração: Detecção de Intrusões pelo Reconhecimento de Regularidades 114
6.3.2 2ª Geração: *Scanners* Inteligentes de Detecção de Vulnerabilidades e Riscos 114
6.3.3 3ª Geração: Gestão de Segurança Adaptativa 115
6.3.4 O Futuro: Segurança de Rede de Auto-Resolução 116
6.4 As Ferramentas e Serviços de Segurança Activos 116
6.4.1 Ferramentas de Auditoria de Vulnerabilidades 116
6.4.2 Serviços de Monitorização 116
6.4.3 Detecção de Vírus 117
6.4.4 Detecção de Intrusões 117
6.4.5 Os Componentes Chave 118
6.4.5.1 Componente de Tempo real 118
6.4.5.2 Bloqueamento de Eventos 119

6.4.5.3 Alarmes Inteligentes 119
6.4.5.4 Ficheiros de *Log* e de *Tracing* 119
6.4.5.5 Transmissão Segura e Transparente 120
6.5 Opiniões Críticas e Perspectivas de Evolução 120

II. Estudo de um Caso *123*

7. Caracterização do Caso **125**
7.1 Caracterização Geral da Rede 126
7.2 Um Problema de Segurança 128
7.3 Perspectivas para uma Solução do Problema 128
7.3.1 A Opção de Separação Física das Duas Subredes 129
7.3.2 A Opção de Implementação de um Sistema de Segurança de Rede 130

8. Proposta de uma Solução **131**
8.1 Arquitectura da Solução a Implementar 131
8.1.1 As Alternativas do Sistema de Segurança 133
8.1.2 Configurações Particulares 133
8.2 Selecção das Ferramentas do Sistema de Segurança de Rede 135
8.2.1 Teste de Laboratório de *Firewalls* 135
8.2.1.1 A Escolha do Teste 136
8.2.2 As Opções de *Firewall* Seleccionadas 137
8.2.3 Teste de Laboratório de VPNs 137
8.2.3.1 A Escolha do Teste 138
8.2.4 As Opções VPN Seleccionadas 139
8.2.5 Teste de Laboratório de Sistemas de Detecção de Intrusão 140
8.2.5.1 A Escolha do Teste 140
8.2.6 As Opções de Sistema de Detecção de Intrusões Seleccionadas 141
8.2.7 Constrangimentos e Requisitos Técnicos 142
8.2.8 As Ferramentas Seleccionadas 143
8.3 A Auditoria do Sistema de Segurança de Rede 143
8.3.1 A Selecção da Ferramenta de Auditoria de Segurança 144
8.3.1.1 A Escolha do Teste 144
8.3.2 A Ferramenta de Auditoria de Segurança Seleccionada 144
8.4 A Plataforma/Sistema Operativo do Sistema 145
8.5 Pontos de Vulnerabilidade na Segurança de *Host* e Física 145
8.6 O Teste da Solução Proposta 146
8.6.1 A Plataforma de Teste 147
8.6.2 A Metodologia de Teste 147

9. Conclusões **149**

III. Apêndices *151*

A. Técnicas de Cifragem **153**
1. O DES 153
1.1 Cifragem 154

1.2 Decifração 155
1.3 O Poder do DES 155
2. IDEA 156
2.1 Iterações 157
3. MD5 159
4. Regulações da Cifragem em Alguns Países 162

B. Principais Elementos Activos de Rede 163

C. Testes de Laboratório 165
1. Testes de Laboratório de *Firewalls* 165
1.1 A Metodologia de Teste 165
1.2 Os Resultados do Teste 167
1.3 As Conclusões dos Outros Testes de Laboratório 169
1.4 Tabelas dos Testes de Laboratório de *Firewalls* 170
2. Testes de VPNs 175
2.1 A Metodologia de Teste 175
2.2 Os Resultados do Teste 177
2.3 As Conclusões dos Outros Testes de Laboratório 179
2.4 Tabelas dos Testes de Laboratório de VPNs 180
3. Testes de Sistemas de Detecção de Intrusões 186
3.1 A Metodologia de Teste 186
3.2 Os Resultados do Teste 187
3.3 As Conclusões dos Outros Testes de Laboratório 189
3.4 Tabelas dos Testes de Laboratório de IDSs 189
4. Constrangimentos e Requisitos Técnicos 193
5. Testes de Ferramentas de Auditoria de Segurança 195
5.1 A Metodologia de Teste 195
5.2 Os Resultados do Teste 196
5.3 As Conclusões dos Outros Testes de Laboratório 197
5.4 Tabelas dos Testes de Laboratório de Auditoria de Segurança 197

Bibliografia 200

Índice das Ilustrações

Figura 2.1 – Ameaças à Segurança [Stall95] 8
Figura 3.1 – Modelo do Sistema de Criptografia Convencional [Stall95] 32
Figura 3.2 – Triple DES [Stall95] 34
Figura 3.3 – Sistema Criptográfico de Chave Pública [Stall95] 37
Figura 3.4 – Duas Abordagens para a Assinatura Digital [Stall95] 41
Figura 3.5 – O Fluxo de Dados no Kerberos 49
Figura 3.6 – O Cabeçalho de Autenticação 51
Figura 3.7 – O Cabeçalho ESP para os Modos de Transporte e de Túnel 52
Figura 3.8 – Arquitectura Protocolar para Serviços de Transacções Seguras [Hunt98] 56
Figura 3.9 – Arquitectura de Intranet com Túneis Cifrados [Hunt98] 58
Figura 3.10 – Interacções do Sistema de Pagamento SET [Hunt98] 63
Figura 4.1 – A Arquitectura do Firewall e a sua Relação com o Modelo OSI [Hunt98] 67
Figura 4.2 – Esquema de um Firewall 68
Figura 4.3 – A Utilização de um Screening Router na Filtragem de Pacotes [ChapZw95] 68
Figura 4.4 – A Utilização de Serviços Proxy com um Dual-homed Host [ChapZw95] 77
Figura 4.5 – A Arquitectura do Stateful Inspection [CheckP98] 84
Figura 4.6 – Arquitectura de Dual-Homed Host [ChapZw95] 86
Figura 4.7 – Arquitectura de Screened Host [ChapZw95] 87
Figura 4.8 – Arquitectura de Subrede Screened (utilizando dois routers) [ChapZw95] 89
Figura 4.9 – Subrede Screened com Host Bastião e Servidor de Internet [ChapZw95] 92
Figura 4.10 – Subrede Screened com Dual-Homed Host (adaptada de [ChapZw95]) 93
Figura 4.11 – Subrede Screened com Routers Interior/Exterior Combinados [ChapZw95] 94
Figura 4.12 – Subrede Screened com Host Bastião e Router Exterior Combinados [ChapZw95] 94
Figura 4.13 – Subrede Screened com Host Bastião e Router Interior Combinados [ChapZw95] 95
Figura 4.14 – Múltiplas Redes Internas Ligadas a Interfaces Diferentes do Mesmo Router [ChapZw95] 96
Figura 4.15 – Arquitectura que Utiliza Vários Routers Exteriores [ChapZw95] 97
Figura 4.16 – Arquitectura que Utiliza Várias Redes de Perímetro [ChapZw95] 98
Figura 5.1 – Componentes de uma Arquitectura VPN 104
Figura 6.1 – Ferramentas de Auditoria de Vulnerabilidades 115
Figura 7.1 – Rede de Computadores do IPP 125
Figura 7.2 – Esquema Detalhado da Rede de Computadores do IPP 127
Figura 7.3 – A Solução da Separação Física das Duas Subredes 129
Figura 8.1 – Alternativas da Arquitectura do Sistema de Segurança 132
Figura 8.2 – Esquema Geral da Solução a Implementar 134
Figura 8.3 – A Plataforma de Teste 147
Figura 10.1 – Descrição Geral do Algoritmo DES [Stall95] 153

Figura 10.2 – Iteração do Algoritmo DES [Stall95] ____ *154*
Figura 10.3 – Esquema Geral do IDEA [Stall95] ____ *157*
Figura 10.4 – Iteração do IDEA (primeira iteração) [Stall95] ____ *158*
Figura 10.5 – Geração da Message Digest Utilizando o MD5 [Stall95] ____ *160*
Figura 10.6 – MD5: Processamento de um Único Bloco de 512 bits (HD_{MD5}) [Stall95] ____ *161*
Figura 10.7 – Combinação de 2 Routers para Obtenção de 2 Portas LAN ____ *164*
Figura 10.8 – Configuração da Plataforma de Teste [NewDC98f] ____ *166*
Figura 10.9 – Teste de Desempenho dos Firewalls [NewDC98f] ____ *169*
Figura 10.10 – Avaliação do Desempenho VPN [ShaDC98v] ____ *179*

Índice das Tabelas

Tabela 3.1 – Algoritmos de Cifragem Convencional Mais Importantes [Stall94a] 33
Tabela 3.2 – Algoritmos Criptográficos de Chave Pública mais Notáveis 38
Tabela 3.3 – O Algoritmo RSA 39
Tabela 3.4 – Algoritmos de Hash Seguro Mais Notáveis 43
Tabela 3.5 – Comparação entre o MD5 e o SHA 44
Tabela 3.6 – Notação do Kerberos 48
Tabela 3.7 – Serviços de Segurança do SSL [Hunt98] 60
Tabela 4.1 – Comparação das Arquitecturas de Firewall [CheckP98] 84
Tabela 5.1 – Os Standards das VPNs 109
Tabela 10.1 – Resultados do Estudo de [Wiener93] 156
Tabela 10.2 – Regulações da Cifragem em Alguns Paises 162
Tabela 10.3 – Os Firewalls em Teste [NewDC98f] 171
Tabela 10.4 – Cenários de Gestão do Firewall [NewDC98f] 172
Tabela 10.5 – Os Firewalls do Teste de Laboratório de Março de 97 [NewDC97f] 174
Tabela 10.6 – Os Firewalls do Teste de Laboratório de Maio de 97 [SeacBt97] 174
Tabela 10.7 – VPNs do Teste de Laboratório de Setembro de 97 [ShaDC98v] 182
Tabela 10.8 – Cenários de Gestão da VPN [ShaDC98v] 183
Tabela 10.9 – VPNs do Teste de Laboratório de Julho de 98 [NewDC98v] 184
Tabela 10.10 – As VPNs do Teste de Laboratório de Novembro de 97 [SterBt97] 185
Tabela 10.11 – Sistemas de Detecção de Intrusões do Teste de Laboratório de Agosto de 98 [NewDC98i] 190
Tabela 10.12 – Ataques Detectados em Redes com Tráfego [NewDC98i] 191
Tabela 10.13 – Teste de Stress do IDS [NewDC98i] 191
Tabela 10.14 – Gestão IDS do Teste de Laboratório de Agosto de 98 [NewDC98i] 192
Tabela 10.15 – Resultados do Teste de Laboratório de Maio de 98 [BroIW98i] 192
Tabela 10.16 – Resultados dos Testes Individuais 193
Tabela 10.17 – Restrições da Cifragem 194
Tabela 10.18 – As Ferramentas de Auditoria de Segurança da Network Computing [ShiNC98] 198
Tabela 10.19 – Caracteristicas de Scanning de Segurança [ShiNC98] 198
Tabela 10.20 – As Ferramentas de Auditoria de Segurança do Teste de Outubro de 97 [KatNW97] 198

Resumo

Esta dissertação abrange o estudo da segurança em redes de computadores de uma forma geral, e a sua aplicação a um caso concreto de uma subrede de computadores com fortes requisitos de segurança.

Caracteriza-se o problema da segurança em redes, definindo-se os requisitos de segurança e as abordagens para satisfazer esses requisitos, as categorias de ataques à segurança e a forma como estes são concretizados. Discutem-se mecanismos de protecção contra os ataques e as estratégias básicas no reforço da segurança dos *sites* e justifica-se a definição de uma política de segurança.

Expõem-se algumas soluções de segurança de rede: autenticação, criptografia e *firewalls*, e alguns dos protocolos de segurança mais representativos. Dedica-se particular atenção à arquitectura e tipos de *firewalls* e às várias opções arquitectónicas dos *firewalls*. São caracterizadas ainda as redes privadas virtuais (VPNs) e as novas ferramentas de monitorização e diagnóstico de tecnologia activa.

Numa segunda parte identificam-se os requisitos do caso concreto da rede em estudo e define-se a arquitectura da solução a adoptar (*firewall*, VPN e sistema de detecção de intrusões) com indicação das ferramentas comerciais a adoptar. É proposta uma metodologia de validação e auditoria da solução e a respectiva ferramenta de auditoria. São definidos também, no caso concreto, os pontos de vulnerabilidade na segurança de *host* e física. Finalmente é definido o plano e metodologia de teste da solução proposta.

Summary

The present thesis addresses the problem of computer network security and describes a case study of a computer subnet with strong security requirements.

Firstly the network security problem is characterised; the requirements and the means to satisfy these requirements are defined and the main types of security attacks are described. The mechanisms to protect against attacks and the basic strategies in the reinforcement of site security are discussed, and the need for a security policy is justified.

Some security solutions are presented: authentication, cryptography and firewalls, as well as some of the well-known security protocols. Firewall architectures, including types and options, are then described and evaluated. Virtual private networks (VPNs) and the new monitoring and diagnosis tools active technology are discussed next.

In the second part a case study is presented and a solution is proposed (firewall, VPN and an intrusion detection system) and the tools to adopt. A validation methodology and auditing is proposed, as well, including the required tools. The vulnerability points in host and physic security are also evaluated. Finally the plan and test methodology of the proposed solution is defined.

Prefácio

Este trabalho enquadra-se por um lado na satisfação dos requisitos exigidos para a dissertação de mestrado e, por outro lado, no âmbito da realização do trabalho de gestão da Rede Administrativa do Instituto Politécnico do Porto, uma subrede de computadores com fortes requisitos de segurança, e que suscitou o tema a esta dissertação.

O problema da segurança de redes de computadores não se pode considerar de forma alguma um assunto resolvido e já com soluções cabais para os diferentes problemas de segurança que se colocam e que sejam adaptáveis de forma simples a qualquer rede particular. Colocou-se assim como objectivo a estudar o problema de segurança em rede e as tecnologias associadas, bem como as arquitecturas das soluções de segurança desenvolvidas. Apresenta-se depois, com base na articulação e combinação dessas soluções, uma proposta de solução de segurança tendo por referência o caso em estudo.

As dificuldades inerentes a uma solução deste género centram-se na constante evolução das tecnologias de rede e nas potenciais falhas de segurança que poderão ser exploradas e, por outro lado, a abertura à Internet das redes de computadores tornam-nas vulneráveis à enorme quantidade de utilizadores mal intencionados. Face a estas dificuldades, a garantia da preservação da confidencialidade e integridade da informação nas redes de computadores torna-se problemática e a consequente aderência, por parte dos gestores das organizações, à interligação das redes restritas com a implementação de soluções de segurança não é, muitas das vezes, conseguida.

Agradecimentos

Agradeço ao Professor Luís Soares, presidente do Instituto Politécnico do Porto, pelas facilidades concedidas à frequência do mestrado e pela disponibilização dos meios necessários à realização desta dissertação de mestrado.

Agradeço também ao Professor José Ruela Fernandes, orientador deste projecto, pela enorme disponibilidade e pelas orientações dadas na realização desta dissertação.

Quero agradecer ainda a todos os meus familiares, amigos e colegas de trabalho que de alguma forma contribuíram para a realização deste "projecto".

I

I. Segurança em Redes de Computadores

1. Introdução

Esta dissertação visa o estudo e aprofundamento dos conhecimentos das tecnologias de segurança de redes, um problema que já não é novo mas que continua a restringir as capacidades da comunicação em rede. O reconhecimento da existência do problema e das limitações de ferramentas apropriadas, levou à necessidade de equacionar o problema do ponto de vista da articulação e perspectiva global entre as diferentes ferramentas, que respondem necessariamente a problemas parciais.

Este trabalho resultou da necessidade de integrar os problemas de segurança no contexto da actividade profissional na área da gestão de sistemas e redes de computadores mas que enfrentava um desafio nos problemas de segurança de diferentes segmentos de rede que se distribuíam por uma WAN. A complexidade do problema e a relativa superficialidade dos conhecimentos de segurança adquiridos até então, e a necessidade de dar resposta a um problema concreto levaram ao interesse na investigação dos conhecimentos nessa área e à necessidade de propor uma arquitectura de segurança de rede.

1.1 Âmbito do Estudo

Este estudo abrange de uma forma geral as tecnologias relacionadas com o tema da segurança em redes de computadores (parte I), e a sua aplicação a um caso concreto de uma subrede de computadores com fortes requisitos de segurança, concretizando-se na proposta de uma solução (parte II).

No 2º capítulo começa-se por fazer a caracterização do problema da segurança em redes. Definem-se os requisitos de segurança e caracterizam-se as abordagens para satisfazer esses requisitos. Enumeram-se as categorias de ataques à segurança de um sistema computacional ou rede de computadores e a forma como são concretizados os ataques. Discutem-se as abordagens que poderão ser seguidas na protecção contra ataques e algumas das estratégias básicas utilizadas na construção de *firewalls* e no reforço da segurança dos *sites*. Caracteriza-se ainda um elemento chave do planeamento de segurança de uma organização que é uma política de segurança.

No capítulo seguinte expõem-se algumas das soluções mais importantes na concretização da segurança de rede: a autenticação, a criptografia e os *firewalls*, e caracterizam-se alguns dos protocolos de segurança mais representativos.

Devido à sua importância o capítulo quarto aborda com detalhe a arquitectura de *firewalls*, e com relativo pormenor os tipos de *firewalls*: de filtragem de pacotes, sistemas *proxy* e sistemas Stateful Inspection. São caracterizadas as arquitecturas de *firewalls* mais importantes que podem reunir várias técnicas seleccionadas para resolver diferentes problemas e também algumas arquitecturas particulares.

No capítulo seguinte são estudadas as redes privadas virtuais (VPNs) e tecnologias associadas que utilizam técnicas de criptografia para cifrar as comunicações de rede restringindo as comunicações somente às autorizadas.

No capítulo 6 são descritas as novas ferramentas de monitorização e diagnóstico de tecnologia activa que reconhecem ataques e más utilizações e respondem com reconfigurações apropriadas e contramedidas.

Na parte II começa-se por caracterizar o caso da rede em estudo (capítulo 7), definindo-se o problema de segurança envolvido e as perspectivas e opções para a sua resolução.

No capítulo 8 define-se a arquitectura da solução proposta e seleccionam-se as ferramentas comerciais para a concretização da arquitectura definida: *firewall*, VPN e sistema de detecção de intrusões. É definida também uma forma de validação e auditoria da solução e proposta uma ferramenta de auditoria de segurança. São ainda definidos os pontos de vulnerabilidade na segurança de *host* e física que podem comprometer a solução de segurança de rede e apontadas algumas soluções. Finalmente é definido o plano e metodologia de teste da solução proposta, obrigando os constrangimentos de tempo a reportar os resultados para um suplemento da tese.

No capítulo das conclusões analisou-se o estudo efectuado das soluções de segurança e a eficácia da solução proposta, bem como na necessidade de se efectuar um teste exaustivo à solução.

2. Caracterização do Problema da Segurança em Redes

A **segurança da informação** teve sempre uma enorme relevância para as pessoas e organizações. A obtenção de determinada informação relevante permite obter vantagem competitiva, sem que o detentor dessa informação possa sequer ter conhecimento disso. O acesso e a alteração de dados de forma ilícita pode levar uma organização a tomar acções que de outro modo não tomaria, e pode acarretar enormes prejuízos para organizações ou pessoas, em benefício próprio do atacante.

Os requisitos da segurança da informação numa organização sofreram duas grandes alterações nas últimas décadas. Antes da utilização generalizada de equipamentos computacionais, a segurança da informação era providenciada primariamente por meios físicos e administrativos [Stall95].

Com a introdução do computador, a necessidade de ferramentas para a protecção de ficheiros ou outra informação armazenada no computador tornou-se evidente; este é especialmente o caso de sistemas partilhados, tal como sistemas de *time-sharing*. A necessidade é ainda mais crítica para sistemas que possam ser acedidos através de uma rede telefónica pública ou duma rede de dados. A **segurança de computadores** é a designação genérica para o conjunto de ferramentas para proteger os dados e prevenir o ataque dos *hackers*[1].

A segunda maior alteração que afectou a segurança foi a introdução de sistemas distribuídos e a utilização de redes e facilidades de comunicação para o transporte de dados entre computadores. São necessárias medidas de **segurança de rede** para proteger os dados durante a sua transmissão. De facto, o termo segurança de rede é algo enganoso, porque virtualmente

---

[1] Na literatura anglo-saxónica são usadas as denominações *Hacker* e *Cracker* com significados semelhantes. É o indivíduo que tenta aceder a redes e facilidades computacionais para as quais não foi autorizado. No entanto, os *Hackers* tendem a fazer uma distinção relativamente às intenções e idoneidade de cada um. [Anoni97] define:

Hacker – Pessoa intensamente interessada no funcionamento recôndito de qualquer sistema operativo. A maioria das vezes têm um conhecimento avançado de sistemas operativos e linguagens de programação. Os *hackers* procuram intensamente novos conhecimentos, partilham livremente as suas descobertas e nunca danificam os dados intencionalmente.

Cracker – Pessoa que quebra o mecanismo de entrada ou de alguma forma viola a integridade do sistema de máquinas remotas, com intenções maliciosas. Os *crackers*, tendo ganho acesso não autorizado, destroem dados vitais, negam o serviço legítimo de utilizadores, ou basicamente causam problemas aos seus alvos.

todas as organizações empresariais, governamentais e académicas ligam os seus equipamentos computacionais através de um conjunto de subredes interligadas, referidas muitas vezes por *internetwork*. A **segurança de *internetworks*** consiste nas medidas para deter, prevenir, detectar e corrigir violações de segurança que envolvam a transmissão de informação.

No entanto não existem limites claros entre estas três formas de segurança. Por exemplo, um dos mais publicitados tipos de ataque em sistemas de informação é o vírus de computador. Um vírus pode ser introduzido fisicamente num sistema através de uma disquete ou pode também chegar através da *internetwork*. Em ambos os casos, uma vez o vírus residente no computador, são necessárias ferramentas internas de segurança para detectar e recuperar do vírus.

2.1 Objectivos da Segurança

Para definir as necessidades de segurança de uma organização de forma efectiva e para avaliar e escolher vários produtos e estratégias de segurança, o gestor responsável pela segurança necessita de um processo sistemático para definir os requisitos de segurança e caracterizar as abordagens para satisfazer esses requisitos. Uma abordagem possível consiste em considerar três aspectos da segurança da informação [Stall95]:

- *Ataque à segurança*: Qualquer acção que compromete a segurança da informação de uma organização.
- *Mecanismo de segurança*: Mecanismo que é concebido para detectar, prevenir ou recuperar de um ataque de segurança. Os mecanismos de segurança serão estudados no segundo capítulo.
- *Serviço de segurança*: Serviço que melhora a segurança do sistema de processamento de dados e da transferência de informação de uma organização. O serviço opõe-se aos ataques à segurança e utiliza um ou mais mecanismos de segurança para providenciar o serviço.

A pesquisa e desenvolvimento da segurança de computadores e redes concentraram-se em alguns serviços de segurança gerais que incluem as várias funções requeridas por uma facilidade de segurança de informação.

Os objectivos de segurança de computadores e redes podem assim ser obtidos pelos seguintes serviços de segurança[2]:

[2] Não existe uniformidade na classificação dos serviços de segurança na literatura sobre segurança. Por exemplo, o termo autenticidade refere-se à verificação da identidade mas pode ser utilizado para referir as várias funções da integridade.

- *Confidencialidade*: Requer que a informação num sistema computacional e a informação transmitida sejam acessíveis somente para as partes autorizadas. Os tipos de acesso são: ler, visualizar, imprimir, ou mesmo a revelação da existência do objecto.
- *Autenticação*: Requer que a origem de uma mensagem seja correctamente identificada, assegurando-se que a identidade não é falsa.
- *Integridade*: Requer que os recursos computacionais e a informação transmitida sejam possíveis de modificação somente pelas partes autorizadas. A modificação inclui escrever, alterar, alterar o estado, apagar, criar, e atrasar ou repetir mensagens transmitidas.
- *Não repúdio*: Requer que nem o emissor nem o receptor de uma mensagem possam negar a sua transmissão.
- *Controlo de acesso*: Requer que o acesso a recursos de informação seja controlado por ou para o sistema em foco.
- *Disponibilidade*: Requer que os recursos computacionais estejam disponíveis para as partes autorizadas quando necessário.

2.2 Tipos de Ataques à Segurança

Os tipos de ataque à segurança de um sistema computacional ou rede de computadores são melhor caracterizados vendo-se a função do computador como providenciando informação. Em geral, existe um fluxo de informação de uma fonte, tal como um ficheiro ou conteúdo de uma região de memória, para um destino, tal como outro ficheiro ou utilizador. Este fluxo normal é representado na Figura 2.1(a) [Stall95].

Existem quatro categorias de ataques à segurança de um sistema computacional ou rede de computadores: interrupção, intercepção, modificação e forjar. Estas ameaças exploram as vulnerabilidades dos recursos computacionais [Pfleeg97].

- *Interrupção*: Um recurso do sistema é destruído, perde-se, ou torna-se indisponível ou inútil. É um ataque à *disponibilidade*. Exemplos de interrupção incluem a destruição de um componente de hardware, o corte de uma linha de comunicações ou a desactivação do sistema de gestão de ficheiros.
- *Intercepção*: Uma parte não autorizada ganha acesso a um recurso. Consiste num ataque à *confidencialidade*. A parte não autorizada pode ser uma pessoa, um programa ou um computador. Exemplos incluem o *wiretapping*[3] para a captura de dados numa rede e a cópia de ficheiros ou programas.

[3] O termo geral *wiretap* significa a intercepção de comunicações. Apesar de o termo ter conotações físicas, não é necessário contacto real. Pode ser efectuado de forma disfarçada, sem que nem o emissor nem o receptor da comunicação saibam que o conteúdo tenha sido interceptado [Pfleeg97]. O *wiretapping* passivo é a escuta, ou intercepção da comunicação. O *wiretapping* activo significa a injecção de algo na comunicação.

- *Modificação*: Uma parte não autorizada não só ganha acesso mas também interfere com um recurso. É um ataque à *integridade*. Exemplos incluem a alteração de valores num ficheiro de dados, a alteração de um programa de forma a este executar de forma diferente e a modificação do conteúdo de mensagens transmitidas numa rede. Existindo mesmo a possibilidade de modificação de hardware.
- *Forjar*: Uma parte não autorizada insere objectos forjados no sistema. Consiste num ataque à *autenticidade*. Exemplos incluem a inserção de mensagens ou transacções espúrias numa rede de comunicações ou a adição de registos numa base de dados.

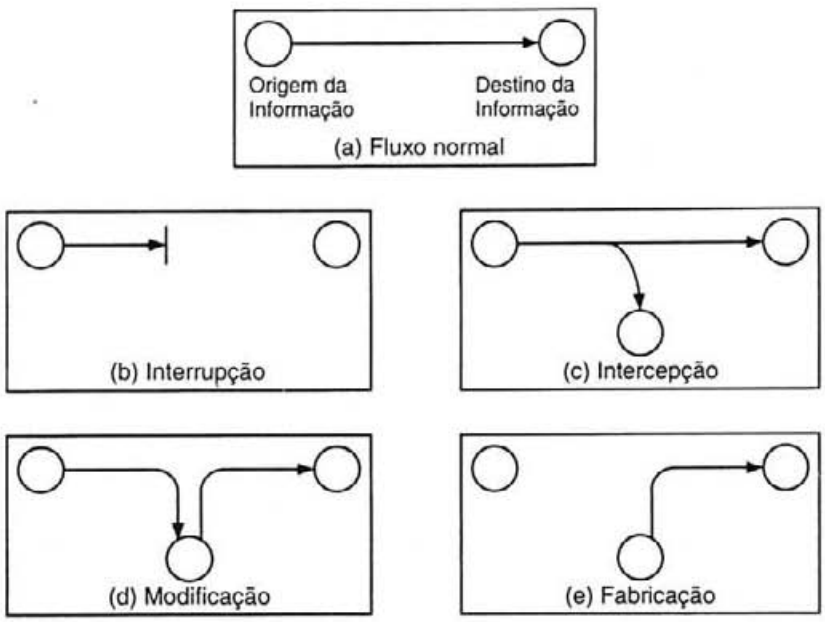


Figura 2.1 – Ameaças à Segurança [Stall95]

2.2.1 Ataques Passivos

Os ataques passivos são de natureza de escuta ou monitorização de transmissões. O objectivo do oponente é obter informação que esteja a ser transmitida. Os ataques passivos são da categoria *intercepção* e envolvem dois tipos de ataques: obtenção do conteúdo de mensagens e análise de tráfego.

A *obtenção do conteúdo de mensagens* poderá ser utilizada numa mensagem de correio electrónico ou transferência de um ficheiro e se os seus conteúdos forem sensíveis ou confidenciais, dever-se-á prevenir que o oponente possa entender o respectivo conteúdo.

A *análise de tráfego* é um ataque mais subtil. Mesmo utilizando-se uma técnica para mascarar o conteúdo de mensagens ou outro tráfego de informação, tal como a cifragem, o oponente poderá determinar a localização e identidade dos comunicadores e poderá observar a frequência e tamanho das mensagens trocadas. Esta informação poderá ser útil na determinação da natureza da comunicação que está a decorrer.

Os ataques passivos são muito difíceis de detectar já que não envolvem qualquer alteração dos dados; no entanto, é possível prevenir o sucesso desses ataques.

2.2.2 Ataques Activos

Os ataques activos envolvem alguma modificação do fluxo de dados ou a criação de dados falsos e podem ser subdivididos em quatro tipos: mascaramento, repetição, modificação de mensagens e negação do serviço.

O *mascaramento* tem lugar quando uma entidade finge ser outra entidade. Normalmente inclui uma das outras formas de ataque activo. Por exemplo, podem ser capturadas e repetidas sequências de autenticação após ser transmitida uma sequência de autenticação válida, permitindo que uma entidade autorizada com poucos privilégios possa obter privilégios extra ao fingir ser uma entidade que tem esses privilégios.

A *repetição* envolve a captura passiva de unidades de dados e a sua subsequente retransmissão para produzir um efeito não autorizado.

A *modificação de mensagens* significa que alguma parte de uma mensagem legítima é alterada, ou que mensagens são atrasadas ou reordenadas para produzir um efeito não autorizado.

A *negação do serviço* evita ou inibe a utilização normal ou a gestão das facilidades de comunicação. Este ataque pode ter um alvo específico, por exemplo, uma entidade pode suprimir todas as mensagens direccionadas para um destino particular. Outra forma de negação de serviço é o bloqueamento de uma rede inteira, quer pela desactivação da rede ou saturando-a com mensagens de forma a degradar o desempenho da rede.

É bastante difícil prevenir de forma absoluta os ataques activos já que seria necessária a protecção física de todas as facilidades e linhas de comunicação em cada momento. Outra abordagem seria detectar os ataques e recuperar o bloqueamento ou atrasos causados. A detecção como tem um efeito dissuasor pode também contribuir para a prevenção.

2.3 Caracterização dos Ataques

Como vimos anteriormente os tipos de ataque à segurança de um sistema computacional ou rede de computadores são: interrupção, intercepção, modificação e fabricação. Estes tipos de ataque são concretizados de maneiras diversas que serão descritas nas secções seguintes, bem como as suas contramedidas.

2.3.1 O Roubo de *Passwords*

O acesso mais fácil a um computador é normalmente a porta da frente, o que é o mesmo que dizer o comando *login*. Na maioria dos sistemas um *login* com sucesso baseia-se no fornecimento da *password* correcta dentro de um número razoável de tentativas [ChesBe94].

No sistema UNIX o ficheiro de *passwords* é cifrado, mas de um universo legível, o que origina ataques *off-line* com apoio de dicionários. Gasta mais tempo de CPU mas o *cracking* pode ser feito longe da máquina em risco. O *ficheiro de passwords sombra*[4] permite evitar este ataque mas muitos sistemas não o implementam e alguns que o implementam fazem-no de forma deficiente.

Novos serviços como o FTP requerem a mesma autenticação mas, curiosamente usam uma rotina diferente. Todo o código do *login* é pobremente replicado no FTP, originando mais *buracos*. Com código de *wiretapping* simples ou sofisticado é possível apanhar *passwords* dos primeiros pacotes de uma sessão *telnet*.

O objectivo imediato de muitos ataques de rede não é o *quebrar* directamente mas apanhar o ficheiro de *passwords*. Alguns serviços que foram utilizados para apanhar ficheiros de *passwords* são o FTP, TFTP, o sistema de mail, NIS, rsh, finger, uucp, X11 e outros. São muitas facilidades para o atacante, se o administrador do sistema é descuidado ou não acerta na escolha do sistema. As medidas defensivas a tomar incluem um grande cuidado e uma atitude conservadora face ao *software*, pois o *cracker* só precisa de vencer uma vez.

2.3.2 Relacionamento "Social"

As *passwords* podem ser muitas vezes encontradas afixadas perto de um terminal ou escritas em documentação perto do teclado. Esta situação implica o acesso físico que sai fora do âmbito deste estudo.

A abordagem ao relacionamento "social" normalmente envolve um contacto telefónico e alguma conversação de forma a dissimular a identidade e assim obter-se o acesso ao sistema.

Existem ainda outras abordagens, tal como o *mail-spoofing*[5]. O aviso do CERT[6], CA-

---

[4] Alguns sistemas permitem esconder as *passwords* de *hash*, mesmo dos utilizadores legítimos, no *ficheiro de passwords sombra*.

[5] *Spoofing* é o acto de usar uma máquina para se fazer passar por outra, forjando a identidade ou o endereço da outra [Anoni97].

[6] CERT – Computer Emergency Response Team, é provavelmente a mais conhecida organização de segurança da Internet. A CERT cria avisos de segurança e distribui-os através da comunidade da Internet. Estes avisos

91:04 (18 de Abril de 1991), alerta contra mensagens supostamente de um administrador de sistema pedindo aos utilizadores que executem um "programa teste", o qual pede a introdução da *password*.

Certas acções não devem ser tomadas sem uma forte autenticação, já que é necessário ter a certeza sobre quem é que efectua determinados pedidos. Na maioria das circunstâncias um *handshake* de três passos – uma mensagem e resposta, seguida pelo pedido em causa – é suficiente. Isto não é completamente seguro, mesmo uma *account* de utilizador privilegiado pode ser penetrada. Para uma autenticação mais forte é recomendada a utilização de um sistema criptográfico de *mail*.

2.3.3 Os *Bugs* e as *Backdoors*

Uma das formas que levou a que o Internet Worm se espalhasse foi pelo envio de código diferente ao *finger daemon*[7]. Como o protocolo não especifica o tamanho máximo do *buffer* na chamada *gets*, o Worm excede o tamanho do *buffer* com o seu próprio código sobrepondo o endereço de retorno na pilha do comando *gets*. Quando a subrotina finalmente retorna, salta para o *buffer* originando a replicação do programa e a consequente procura e infecção de máquinas vulneráveis. Esta situação particular descreve as consequências de um problema geral: a escrita de *software* correcto parece ser um problema que não está ao alcance da ciência da computação pois os *bugs* abundam.

O Internet Worm permite tirar as seguintes ilações: o efeito de um *bug* não está limitado aos efeitos ou abusos de um serviço particular envolvido. Ao contrário, o sistema inteiro pode ser atacado devido à falha de um componente.

Não existe uma defesa perfeita, mas poderão ser tomadas medidas para corrigir estes problemas. A primeira medida para obviar esta situação será a verificação exaustiva da correcção dos programas. Outra medida é a atribuição de menos privilégios. Não atribuir aos *daemons* de rede qualquer privilégio que eles não necessitem, especialmente nas máquinas *firewall*.

2.3.4 Falhas de Autenticação

Muitas das situações descritas derivam de falhas de mecanismos de autenticação. Por exemplo, a validação por endereço de origem pode funcionar em determinadas circunstâncias, mas o *hackers* podem utilizar o *portmapper* para retransmitir determinados pedidos. Neste

---

dizem respeito às últimas vulnerabilidades de segurança conhecidas, na maioria dos sistemas operativos.

[7] Um *Daemon* é um programa que permanece sempre activo e escuta continuamente a ocorrência de um determinado evento; quando esse evento ocorre o *daemon* executa determinada acção.
O serviço *finger* é um utilitário que providencia informação sobre os utilizadores de um dado sistema.

caso, o servidor final é enganado, a mensagem tal como parece ao servidor é de facto de origem local mas a sua proveniência final é algures.

A autenticação baseada em endereços também falha se a máquina origem não for confiável. Os PCs são o exemplo óbvio. O mecanismo existente por altura dos computadores de tempo partilhado já não funciona já que os utilizadores podem controlar as suas próprias máquinas. Claro que a alternativa das *passwords* vulgares também não é solução numa rede cheia de computadores pessoais, o *sniffing*[8] de *passwords* seria muito fácil.

Por vezes a autenticação falha porque o protocolo não transporta a informação correcta. Nem o TCP nem o IP identificam o utilizador emissor, e em algumas máquinas este conceito nem sequer existe.

Mesmo a autenticação criptográfica da máquina ou utilizador emissores pode não ser suficiente; uma máquina insegura não pode efectuar cifragem segura.

2.3.5 Falhas Protocolares

Certos ataques ocorrem em situações em que os protocolos têm *bugs* ou são inadequados, inibindo dessa forma a aplicação de executar correctamente. Um caso importante é o ataque do número de sequência do TCP.

A ordem nos pacotes IP é mantida pelo número de sequência; cada *byte* enviado, tal como os pedidos de *open* e *close*, são numerados individualmente. Cada mensagem TCP é marcada como proveniente de um determinado *host* e número de porta, e para um *host* e porta de destino. O tuplo quádruplo (*localhost, localport, remotehost, remoteport*) identifica de forma única uma determinada conexão TCP.

Os números de sequência têm uma outra função. Como o número de sequência inicial para cada nova conexão muda constantemente, é possível para o TCP detectar pacotes antigos de prévias encarnações do mesmo circuito (i.e. prévias utilizações do mesmo tuplo quádruplo).

No entanto existe aqui uma ameaça. Se um atacante conseguir prever a escolha do número de sequência inicial do alvo do ataque, e [MORR85] mostra que isto é de facto possível em determinadas circunstâncias, então é possível ao atacante enganar a outra máquina fazendo-lhe crer que está a comunicar com uma máquina confiável. Nesse caso, os protocolos que dependem do endereço IP fonte para autenticação (ex.: os comandos "r" do UNIX) podem ser explorados para penetrar o sistema alvo. Isto é conhecido como o *ataque do número de se-*

[8] Um *sniffer* é um dispositivo, de hardware ou software, que pode ler cada pacote enviado ao longo da rede [Anoni97].

quência.

Devido à insuficiente aleatoriedade na geração do número de sequência inicial de uma conexão, é possível para o atacante tentar efectuar o *spoofing* do endereço fonte. Considerando-se a importância da autenticação baseada em endereço, a definição do protocolo é inadequada. Outros protocolos que se baseiam em números de sequência podem ser vulneráveis ao mesmo tipo de ataque; é o caso do DNS[9] e qualquer dos protocolos baseados em RPC[10].

Os protocolos seguros devem ser suportados em bases seguras. Se considerarmos, por exemplo, o protocolo RPC Seguro apesar de bem intencionado e bem melhor que a simples alternativa baseada em endereços, tem vários problemas sérios.

O primeiro é a distribuição de chaves. Os *hosts* que pretendam comunicar de forma segura devem conhecer as chaves públicas dos outros (a criptografia de chave pública é caracterizada no capítulo 2). Mas esta informação é transmitida via NIS (*Network Information Service*), um serviço inseguro com base no RPC. Se esta troca de informação for comprometida, então os restantes passos de autenticação não resultam de igual forma.

Para além disso os *hosts* devem obter as suas próprias chaves privadas. Novamente são utilizados o NIS e o RPC, apesar de com maior segurança já que as chaves privadas são cifradas, mas são protegidas somente por uma *password*, com todos os perigos daí advindos. Ironicamente, a existência do ficheiro contendo as chaves pública e privada criou uma vulnerabilidade de segurança adicional: uma nova possibilidade para a descoberta de *passwords*.

Finalmente, é negociada uma chave de sessão temporária, mas o algoritmo criptográfico utilizado para a negociação foi já criptanalisado como demonstram [LAMA91].

2.3.6 Fuga de Informação

A maioria dos protocolos deixam escapar alguma informação. Muitas das vezes é essa a intenção da pessoa que utiliza esses serviços: obter essa informação. Esta informação poderá ser o alvo de espionagem ou pode ser desejada para uma tentativa de entrada no sistema. O protocolo *finger* é um exemplo óbvio, para além do seu interesse para obter *passwords*, a informação pode ser obtida para o relacionamento "social".

Uma fonte de informação é o DNS, desde detalhes das organizações até listas de alvos. Mas o controlo da fuga de informação é difícil, muitas vezes a única solução é limitar o DNS visível externamente somente a máquinas *gateway*.

---

[9] Domain Name System – sistema de base de dados distribuída utilizada para mapear nomes de *hosts* em endereços IP e vice-versa.

[10] RPC – *Remote Procedure Call*, protocolo da Sun Microsystems.

Os *hackers* mais sofisticados sabem isso, com certeza, e não se deixam enganar sobre as máquinas existentes. Eles efectuam a pesquisa de espaço de endereços e números de portas, na procura de *hosts* escondidos e serviços de interesse. A melhor defesa para isto é um *firewall*, pois se eles não conseguirem enviar pacotes para uma máquina então será mais improvável conseguirem atingi-la.

2.3.7 Negação do Serviço

Algumas pessoas gostam de bloquear os sistemas computacionais dos outros. Este comportamento toma muitas formas. A forma mais rude e fácil é tentar encher o disco de alguém enviando *mail* ou utilizando o FTP para enviar algumas centenas de *megabytes*. É difícil definir um limite no consumo de recursos, pois para além das necessidades dos utilizadores privilegiados, será muito fácil enviar, em vez disso, 1 MB algumas centenas de vezes, criando uma grande quantidade de processos de recepção na máquina, bloqueando-a ainda mais. As medidas de prevenção será aumentar os recursos para melhor fazer frente a estas situações, separar áreas para o *mail*, o FTP e especialmente os dados de *logging*, e efectuar a preparação para uma falha sem consequências.

Outras formas de vandalismo aos computadores são mais subtis. Algumas pessoas gostam de enviar pacotes ICMP falsos para um *site* para causar a desordem nas suas comunicações. Por vezes essas mensagens são de destino inatingível, outras vezes são as mais confusas e "mortais" mensagens que apagam a máscara de subrede do *host*. Os *hosts* "escutam" estas mensagens quando não enviaram tal pedido. Outros *hackers* atacam os protocolos de *routing*, não para penetrar numa máquina, mas para lhe negar a possibilidade de comunicar.

Uma filtragem agressiva pode ser uma óptima medida de protecção, mas não existem garantias absolutas. Poderá ser muito difícil de detectar a diferença entre mensagens genuínas, falhas vulgares e ataques.

2.4 Modelos de Segurança

Que abordagens poderão ser seguidas de forma a proteger contra o género de ataques que foram salientados na secção anterior? É possível escolher entre uma variedade de modelos de segurança, ou abordagens, que vão desde a ausência de segurança até à designada *segurança através da obscuridade*, e segurança do *host* até à segurança de rede [ChapZw95].

2.4.1 Ausência de Segurança

A abordagem mais simples possível é não apostar nada na segurança, e utilizar somente os recursos de segurança mínimos fornecidos por omissão com os *hosts* e com a rede. Este modelo, por ser passivo face aos ataques e por não oferecer mecanismos de segurança é o menos desejável.

2.4.2 Segurança Através da Obscuridade

Com este modelo, presume-se que um sistema é seguro simplesmente porque, supostamente, ninguém sabe da sua existência, conteúdo, medidas de segurança, ou qualquer outro aspecto. Esta abordagem raramente funciona durante muito tempo, pois existem demasiadas maneiras de encontrar um alvo atractivo.

Muitas abordagens pressupõem que, mesmo que sejam descobertos pelos atacantes, uma pequena companhia ou uma máquina pessoal não serão do interesse dos intrusos. Pelo contrário, para os atacantes pequenas companhias ou máquinas pessoais constituem alvos fáceis. Tentarão forçar o acesso e poderão fazer consideráveis estragos se permanecerem no sistema enquanto tentam cobrir as *suas pistas*.

Qualquer rede que necessite de acesso à Internet, tem de ter um *site* para efectuar pelo menos um registo mínimo, e muita desta informação de registo deve estar disponível na Internet. De cada vez que um utilizador utilizar serviços na Internet, a sua presença estará assinalada pelo menos pelo fornecedor do serviço. Os intrusos detectam novas ligações, na esperança que esses *sites* não tenham ainda medidas de segurança implementadas.

Existem variadíssimas formas para alguém determinar informação de segurança sensível sobre um *site*. Por exemplo, saber que hardware ou software estão instalados e qual o sistema operativo e versão, fornece aos intrusos pistas importantes sobre que *buracos* de segurança poderão tentar explorar. Podem obter esta informação a partir do registo do *host* ou tentando ligar à máquina.

Os *hackers* têm bastante tempo disponível, e podem evitar ter de pesquisar factos obscuros, simplesmente tentando todas as possibilidades. Em última análise, a *segurança através da obscuridade* não é uma boa alternativa de segurança.

2.4.3 Segurança do *host*

A segurança do *host* é provavelmente o modelo de segurança de computador mais comum. Com este modelo reforça-se a segurança de cada máquina separadamente. No entanto, o problema deste modelo é que, apesar de funcionar em máquinas isoladas, não funciona com um número grande de máquinas.

O maior impedimento a uma efectiva segurança dos *hosts* é a complexidade e diversidade dos ambientes computacionais modernos, com máquinas de múltiplos tipos e diferentes fornecedores, com diversos sistemas operativos e cada um com o seus problemas de segurança. Mesmo em diferentes versões de um sistema operativo encontram-se problemas de segurança significativamente diferentes. Mesmo em versões idênticas de um mesmo sistema operativo, configurações diferentes (serviços activos, etc.) podem originar diferentes problemas de segurança.

Mesmo com máquinas absolutamente idênticas, a implementação e manutenção da segurança dos *hosts* é complexa e trabalhosa. Mesmo com todo o trabalho executado correctamente, a segurança falha por vezes devido a *bugs* de software ou devido à inexistência de software de segurança adequado para determinadas funções requeridas.

A segurança do *host* baseia-se também em boas intenções e na perícia daqueles que têm acesso privilegiado a qualquer máquina. À medida que o número de máquinas aumenta, o número de utilizadores privilegiados geralmente aumenta também. Como a segurança de uma máquina é mais complexa do que a simples ligação à rede, poderão surgir máquinas inseguras na rede. O mero facto de, supostamente, não ser possível ligar máquinas sem o conhecimento do gestor da rede é irrelevante, já que as pessoas idealizam esquemas inovadores de ligação à rede se tiverem necessidade disso.

O modelo de segurança do *host* pode ser bastante apropriado para pequenos *sites* ou *sites* com requisitos extremos de segurança. De facto, todos os *sites* devem incluir algum nível de segurança do *host* nos seus planos de segurança globais. Mesmo se adoptado o modelo de segurança de rede, descrito na secção seguinte, alguns sistemas beneficiarão da mais forte segurança do *host*. Por exemplo, mesmo se for implementado um *firewall* para a defesa da rede interna, existirão alguns sistemas expostos ao exterior que precisem de segurança de *host*.

O modelo de segurança do *host*, sozinho, não compensa ser utilizado a não ser nos pequenos *sites* ou *hosts* isolados, pois a sua implementação requer demasiadas restrições e demasiadas pessoas.

2.4.4 Segurança de Rede

À medida que os *sites* aumentam e se diversificam, e a sua segurança numa base *host* a *host* se torna mais complexa, o modelo de segurança de rede é o mais indicado. Com o modelo de segurança de rede é dada maior importância ao controlo de acesso à rede pelos vários *hosts* e aos serviços que eles oferecem, em vez da segurança um a um.

As abordagens de segurança de rede incluem a construção de *firewalls* de forma a proteger os sistemas e as redes internas, utilizando fortes esquemas de autenticação e utilizando a cifragem para proteger dados particularmente sensíveis quando estes transitam na rede.

Um *site* pode obter uma vantagem tremenda das medidas de segurança pela utilização do modelo de segurança de rede. Por exemplo, um simples *firewall* de rede pode proteger centenas, milhares ou mesmo dezenas de milhar de máquinas contra ataques provenientes de redes situadas para lá do *firewall*, independentemente do nível de segurança do *host* das máquinas individuais.

2.4.5 Nenhum Modelo de Segurança Resolve Todos os Problemas

Nenhum modelo de segurança pode prevenir uma pessoa hostil mas com acesso legítimo de propositadamente causar danos num *site* ou obter informação confidencial. É possível proteger o *site* de acidentes e ignorância internamente, e de actos externos maliciosos, mas não é possível proteger o *site* dos seus legítimos utilizadores sem inibir seriamente as suas capacidades de utilização dos computadores.

Nenhum modelo de segurança fornece protecção perfeita. É possível minimizar os ataques ou reduzir as suas consequências, mas é extremamente difícil evitá-los totalmente. Mesmo os *sites* mais seguros e dedicados têm um incidente de segurança de tantos em tantos anos. A segurança pode não prever todos os incidentes, mas pode evitar que um incidente danifique seriamente ou mesmo deite abaixo a própria organização.

2.5 Estratégias de Segurança

É importante entender algumas das estratégias básicas utilizadas na construção de *firewalls* e no reforço da segurança dos *sites*. As estratégias de segurança não constituem revelações surpreendentes, antes são abordagens claras e simples.

2.5.1 Menor Privilégio

O princípio mais fundamental da segurança (qualquer tipo de segurança, não só segurança de computadores e redes) é o do menor privilégio [ChapZw95]. Basicamente, este princípio significa que qualquer objecto (utilizador, programa, sistema ou outro) deve ter somente os privilégios que o objecto necessita para efectuar as tarefas atribuídas. O menor privilégio é um principio importante para a limitação das exposições aos ataques e para limitar os danos causados por ataques particulares.

Cada utilizador provavelmente não necessita de aceder a todos os serviços da Internet. Cada utilizador provavelmente não necessita de modificar (ou mesmo ler) cada ficheiro do sistema. Cada sistema provavelmente não necessita de aceder a todos os ficheiros dos outros sistemas.

Muitos dos problemas de segurança comuns na Internet podem ser vistos como falhas ao seguimento do princípio do menor privilégio. Por exemplo, existem alguns problemas de segurança descobertos no Sendmail, que é um programa complexo. O problema é que o Sendmail executa (pelo menos algum tempo) o *setuid* para o utilizador *root*, e muitos dos ataques contra o Sendmail tiram vantagem disto. Como executa como *root*, o Sendmail é um alvo valioso que chama a atenção dos atacantes; o facto de ser um programa complexo só lhes facilita a tarefa. Isto implica que os programas privilegiados devem ser o mais simples possível e, se um programa complexo requerer privilégios, será necessário separar e isolar os com-

ponentes que necessitam de privilégios dos componentes complexos.

Existem dois problemas na tentativa de reforçar o princípio do menor privilégio. Em primeiro lugar, pode ser complexo de implementar quando não existir já um projecto dos programas e protocolos utilizados. Em segundo lugar, é possível acabar por implementar algo menos que o menor privilégio ao atribuir menos privilégios do que os minimamente necessários.

2.5.2 Defesa Reforçada

Outro princípio da segurança (novamente qualquer tipo de segurança) é a defesa reforçada. Não depender somente de um mecanismo de segurança, mesmo que pareça forte; pelo contrário, instalar múltiplos mecanismos que se reforcem mutuamente.

Os *firewalls* não são uma solução completa para toda a gama de problemas de segurança da Internet. Qualquer segurança, mesmo o *firewall* que pareça mais impenetrável, pode ser quebrado por atacantes que estão prontos a arriscar-se o suficiente para terem a possibilidade de obter resultados. O objectivo deverá ser tornar a tentativa demasiado arriscada ou demasiado dispendiosa para os ataques que se espera enfrentar. Podendo adoptar-se múltiplos mecanismos que providenciam redundância uns aos outros: segurança de rede (um *firewall*), segurança de *host* e segurança humana (educação dos utilizadores, administração do sistema cuidada, etc.).

2.5.3 Ponto de Obstrução

Um ponto de obstrução força os atacantes a utilizar um canal estreito, o qual pode ser monitorado e controlado. Na segurança de rede, o *firewall* entre um *site* e a Internet (assumindo que existe só uma ligação) é esse ponto de obstrução. Quem quer que ataque o *site* a partir da Internet terá que o fazer através desse canal, o qual deverá ser defendido desses ataques.

O ponto de obstrução é inútil se existir uma forma efectiva de um atacante o tornear. Porquê atacar o *firewall* se existem linhas de *dial-up* inseguras que poderão ser atacadas mais facilmente e provavelmente com mais sucesso? Uma segunda ligação à Internet, mesmo de forma indirecta, como uma ligação a outra organização que tem a sua própria ligação à Internet, é uma brecha ainda mais ameaçadora. Os atacantes encontrarão certamente ligações, mesmo utilizando caminhos mais longos, para o *site*.

2.5.4 Ligação Mais Fraca

Um princípio fundamental da segurança é que uma cadeia é tão forte quanto a sua ligação mais fraca e uma parede é tão forte quanto o seu ponto mais fraco. Os atacantes mais inteligentes tentam localizar esse ponto fraco e concentram aí as suas atenções. É por isso

necessário ter atenção aos pontos fracos da defesa de forma a tomarem-se medidas para eliminá-los e monitorar atentamente aqueles que não seja possível eliminar.

Existe sempre uma ligação mais fraca; no entanto, a solução é tornar essa ligação suficientemente forte de forma proporcional ao risco. Por exemplo, normalmente é razoável dirigir mais a atenção para os ataques de rede do que para os ataques físicos ao *site*; consequentemente é aceitável considerar a segurança de rede a ligação mais fraca. No entanto, não é razoável negligenciar a segurança física pois permanecem aí algumas ameaças.

Os modelos de segurança do *host* sofrem de uma interacção particularmente séria entre "pontos de obstrução" e "ligações mais fracas". Não existe ponto de obstrução, o que significa que existem bastantes ligações, e muitas delas podem ser de facto fracas.

2.5.5 Postura da *Falha Segura*

Outro princípio fundamental da segurança é de que os sistemas, se falharem, devem falhar de forma segura, quer dizer, devem falhar de forma que neguem o acesso a um atacante. A falha pode resultar também na negação do acesso aos utilizadores legítimos até o problema estar resolvido, mas este é um comportamento aceitável.

A maioria dos sistemas de segurança executam a *falha segura*. Por exemplo, se um *router* de filtragem de pacotes falhar, não deixa passar nenhum pacote, e se uma aplicação *proxy* deixar de funcionar deixa de providenciar qualquer serviço. Por outro lado, alguns sistemas de filtragem de pacotes baseados em *hosts* executam também outras aplicações que providenciam serviços; se a aplicação de filtragem de pacotes falhar, os pacotes serão enviados para as outras aplicações, o que não é um cenário de *falha segura* e deve ser evitado.

A maior aplicação deste princípio na segurança de rede é a escolha da postura do *site* no que respeita à segurança. Uma maior tendência em ser restritiva ou permissiva, uma maior inclinação em direcção da segurança ou da liberdade.

Existem duas atitudes fundamentais que podem ser tomadas no que respeita às decisões e políticas de segurança:

- Atitude da negação por omissão: especifica somente o que é permitido e proíbe tudo o resto.
- Atitude de permissão por omissão: especifica somente o que é proibido e permite tudo o resto.

Do ponto de vista da segurança, é óbvio que a atitude de negação por omissão é a abordagem indicada. No entanto, é importante tornar esta atitude clara para os utilizadores e para a administração e explicar as razões que estão por trás desta atitude, de forma a que o ponto de vista da segurança seja entendido.

2.5.5.1 Atitude de Negação por Omissão

O que não é expressamente permitido é proibido. Esta atitude faz sentido do ponto de vista da segurança porque é uma postura de *falha segura* .

Com a atitude de negação por omissão é proibido tudo por omissão, depois, para determinar o que será permitido deve-se:

- Verificar os serviços que os utilizadores necessitam.
- Considerar as implicações de segurança desses serviços e a forma de os providenciar de forma segura.
- Só devem ser permitidos os serviços que possam ser providenciados de forma segura e que tenham uma necessidade legítima.

Os serviços são permitidos numa análise caso a caso. Para um serviço, pode determinar-se que se pode providenciar o serviço para todos os utilizadores e ser efectuado de forma segura com sistemas disponíveis de filtragem de pacotes ou *proxys*. Para outro serviço, somente um pequeno número de utilizadores ou sistemas o podem requerer ou poderá determinar-se que o serviço não poderá ser adequadamente seguro por nenhum dos meios disponíveis. O objectivo é encontrar um compromisso que seja adequado para cada situação particular.

2.5.5.2 Atitude de Permissão por Omissão

Aquilo que não é expressamente proibido é permitido. Assume-se que tudo é, por omissão, permitido e que acções e serviços específicos mais sensíveis serão depois proibidas à medida que for necessário. Esta atitude não é definitivamente uma atitude de *falha segura*.

Assume-se que se sabem precisamente quais são os perigos específicos, como explicá-los aos utilizadores e como se pode defender contra eles. Tentar adivinhar que perigos podem estar num sistema ou fora do sistema na Internet é essencialmente uma tarefa impossível. Existem demasiados problemas possíveis e demasiada informação (ex.: novas falhas de segurança, novas explorações de falhas de segurança antigas, etc.) para que se possam manter actualizados.

A atitude de permissão por omissão tende a degenerar numa luta entre a manutenção do *firewall* e os utilizadores. O gestor da rede prepara defesas contra as acções dos utilizadores, mas estes idealizam novas formas, normalmente inseguras, de efectuar as acções, e o processo repete-se vezes sem conta. Inevitavelmente, existirão sempre períodos de vulnerabilidade entre a altura em que o sistema é activado, a altura em que o problema de segurança é descoberto, e a altura em que o gestor é capaz de responder ao problema.

As únicas pessoas que beneficiam da atitude de permissão por omissão são os potenci-

ais atacantes, porque o gestor do *firewall* não conseguirá possivelmente resolver todos os problemas de segurança, estará constantemente ocupado com a *luta* de manutenção da segurança do *firewall*, e estará demasiado ocupado para notar as actividades dos atacantes.

2.5.6 Participação Universal

Para serem perfeitamente efectivos, a maioria dos sistemas de segurança requerem a participação universal dos utilizadores do *site*, ou pelo menos a ausência de oposição activa. Se alguém se opuser aos mecanismos de segurança implementados, então um atacante poderá atacar em primeiro lugar o sistema desse utilizador, atacando depois todo o *site* a partir do seu interior. Por exemplo, o melhor sistema *firewall* não protegerá a rede se alguém, que o encara como um mecanismo sem utilidade, activar uma conexão *backdoor* entre o *site* e a Internet de forma a circunscrever o *firewall*.

Mas existem muitas outras formas mais mundanas de oposição que poderão afectar a segurança. É necessária a participação de todos para relatar acontecimentos estranhos que poderão estar relacionados com a segurança, pois o gestor não pode ver tudo. Obviamente, a participação voluntária é bastante preferível à participação involuntária (ordenada), pois o objectivo é obter a ajuda dos utilizadores, e não que eles procurem formas de não cooperar. Isto significa que é necessário informar os utilizadores dos benefícios da segurança e convencê-los que os benefícios ultrapassam os custos.

2.5.7 Diversidade da Defesa

Tal como se pode obter segurança adicional pela utilização de um número diverso de sistemas para providenciar a defesa reforçada, é possível também obter segurança adicional pela utilização de diferentes tipos de sistemas. Se todos os sistemas forem iguais, alguém que saiba como forçar a entrada num deles saberá provavelmente como forçar a entrada em todos eles.

A ideia que está por trás da diversidade da defesa é que utilizando sistemas de segurança de diferentes fornecedores se pode reduzir as hipóteses de *bugs* comuns ou configurações erradas que comprometam o sistema. No entanto, existe um compromisso em termos de complexidade e custo, a instalação de múltiplos sistemas diferentes será mais difícil, demorará mais tempo e será mais cara do que a instalação de um simples sistema ou mesmo vários sistemas idênticos.

É necessário ter cuidado com a diversidade ilusória. A simples utilização de, por exemplo, sistemas UNIX de diferentes fornecedores não fornecerá a diversidade, porque a maioria dos sistemas UNIX são baseados no código fonte BSD ou System V e existem muitos *bugs* ou problemas de segurança nas suas versões originais que foram propagadas na maioria das versões específicas dos fornecedores desses sistemas operativos.

É também necessário ter em atenção que diversos sistemas configurados pela mesma pessoa ou grupo de pessoas podem partilhar problemas comuns se estes tiverem origem em raízes conceptuais em vez de tecnológicas. Se o problema for um mal entendido relativamente a como um determinado protocolo trabalha, por exemplo, os vários sistemas podem ser todos configurados incorrectamente da igual forma.

Apesar de muitos *sites* concordarem que a utilização de múltiplos tipos de sistemas pode potencialmente aumentar a segurança, alguns concluem no entanto que a diversidade da defesa é mais prejudicial que benéfica, e que os ganhos potenciais e melhorias de segurança não compensam os custos. Em cada *site* deve ser feita a sua própria avaliação e decisão no que respeita a esta estratégia.

2.5.8 Simplicidade

A simplicidade é uma estratégia de segurança porque mantendo as coisas simples torna-se mais fácil perceber se são ou não seguras. A complexidade fornece muitos sítios onde se ocultam pormenores de segurança.

Os programas complexos têm mais *bugs*, os quais podem ser problemas de segurança. Mesmo se os *bugs* não forem eles próprios problemas de segurança, logo que os utilizadores comecem a esperar que o sistema se comporte de forma errática, aceitarão qualquer comportamento do sistema o que comprometerá o reconhecimento e relato de problemas de segurança.

2.6 A Política de Segurança

Um elemento chave do planeamento de segurança de uma organização é uma política de segurança efectiva. As questões que uma política de segurança deve responder são *quem* pode aceder a *que recursos* e de que *forma* [Pfleeg97].

Uma expressão de política de segurança deve especificar:

- Os objectivos de segurança da organização (por exemplo, proteger os dados da fuga de informação, proteger a integridade dos dados, etc.),
- Onde recai a responsabilidade pela segurança (por exemplo, num pequeno grupo de computadores de segurança),
- O compromisso de segurança da organização (por exemplo, a posição da segurança na estrutura da organização).

2.6.1 Propósito da Política de Segurança

Uma política de segurança é escrita para diferentes grupos; cada grupo tem uma razão

diferente para usar a política de segurança e, por isso, uma expectativa diferente.

Todas as organizações têm "clientes" ou **beneficiários** de algum género. Um negócio tem clientes pagantes, mas o público em geral também pode beneficiar pela existência do serviço, e os beneficiários de uma escola ou universidade são os seus estudantes, professores, e as pessoas em geral.

Todos estes beneficiários, em vários graus, dependem na existência ou acesso aos computadores, os seus dados e programas, e poder computacional. Para estas pessoas, a continuidade e integridade desses meios computacionais são muito importantes. Nalguns casos, a confidencialidade e integridade dos dados é muito importante. As necessidades dos beneficiários deve ser considerada e reafirmada numa política de segurança.

Os **utilizadores** legitimamente esperam um certo grau de confidencialidade, integridade e constante disponibilidade dos recursos computacionais ao seu dispor. Precisam também de saber e apreciar qual é o uso aceitável dos computadores, dados, e programas. Para os utilizadores, uma política de segurança deve reafirmar o compromisso entre esses requisitos.

Finalmente, cada componente de equipamento computacional tem um **dono**, que pode não ser o utilizador. O dono, tal como um negócio ou uma universidade, fornece o equipamento aos utilizadores para um dado propósito, tal como uma educação mais avançada, suporte ao comércio, ou uma produtividade melhorada. Uma política de segurança deve também reflectir as expectativas dos donos.

A política de segurança deve assim relacionar as necessidades dos beneficiários, utilizadores e donos, e efectuar o compromisso das prioridades de todas as comunidades afectadas.

2.6.2 Atributos de uma Política de Segurança

A política de segurança deve expressar o **propósito** (ou propósitos) da computação, reflectindo os requisitos dos beneficiários, utilizadores, e donos. Exemplos de propósitos são "preservar a confidencialidade dos clientes" ou "assegurar uma disponibilidade contínua". Uma expressão clara e sucinta do propósito da computação ajudará a justificar os requisitos de protecção que serão expressos mais tarde.

A política de segurança deve também expressar a quê que se aplica. Somente aos computadores de rede? Aos dados dos clientes? A todos os programas? As respostas a estas questões ajudam a identificar as classes de **recursos protegidos** e o grau de protecção.

Deve ser definido agora como é que o acesso será assegurado (e como será negado o acesso a pessoas não autorizadas). A política de segurança deve expressar, em termos gerais, que grau de **protecção** deve ser fornecido a que tipos de recursos.

A política de segurança deve ser completa, a sua **cobertura** deve aplicar-se a ou excluir explicitamente todas as possíveis situações. Para além disso, deve ser suficientemente geral para se aplicar naturalmente a novas situações.

Uma política de segurança deve evoluir e adaptar-se bem. Como já foi referido, não deve ser alterada sempre que surjam novas situações, mas deve também ser actualizável sempre que for necessário. Uma característica importante da **durabilidade** é que a política de segurança não deve ficar condicionada a dados específicos que possam mudar ou a mecanismos de protecção específicos que quase de certeza mudarão.

A política de segurança deve ser **realista**. Os requisitos de protecção expressos devem ser realizáveis com os mecanismos existentes. Não é razoável requerer protecção absoluta da confidencialidade se não existirem controlos que possam fornecer protecção absoluta.

De forma a ter **utilidade**, a política de segurança deve ser lida, entendida, e seguida por todos. Uma política breve, escrita de forma clara e directa, terá mais possibilidades de ser efectiva.

3. Análise de Soluções

Neste capítulo analisam-se as soluções mais importantes na concretização da segurança de rede e caracterizam-se alguns dos mecanismos, técnicas e protocolos mais representativos.

3.1 Autenticação

A autenticação é o processo de verificação da identidade. Isto é distinto da asserção de identidade (conhecimento suficiente da identificação) e da decisão de quais os privilégios atribuídos a essa identidade (autorização). Apesar da importância dos três aspectos, a autenticação é o mais complicado na perspectiva de segurança de rede. Podem caracterizar-se duas formas de autenticação, a de um utilizador por uma máquina durante uma sequência de *login*, e a autenticação máquina a máquina durante a operação [ChesBe94].

As soluções para o primeiro problema são tipicamente categorizadas como "algo que tu sabes", "algo que tu tens" e "algo que tu és". A autenticação máquina à máquina é geralmente dividida em dois tipos: criptográfica e outros.

3.1.1 Autenticação de Utilizador

Apesar das *passwords* serem utilizadas frequentemente para autenticação, existe uma variedade de mecanismos de autenticação. Esses mecanismos podem ser classificados como verificando uma ou mais das seguintes propriedades [ChapZw95]:

- "Algo que tu sabes" – consiste no sistema tradicional de *passwords*.
- "Algo que tu tens" – mecanismos tais como listas de desafio/resposta, *passwords* de utilização única, *smart cards*, etc.
- "Algo que tu és" – é o campo das biométricas, incluindo as técnicas de leitura de impressões digitais, leitura da retina, análise da voz, etc.

Alguns sistemas combinam estas abordagens, por exemplo, um *smart card* que requer que o utilizador introduza um número de identificação pessoal é uma combinação de "algo que tu tens" e "algo que tu sabes". Em teoria, considera-se uma boa opção combinar pelo menos dois mecanismos, porque a "coisa que tu tens" é susceptível de roubo, e a "coisa que tu sabes" é comprometida pelo *sniffing* se transitar na rede, mas é difícil para alguém conseguir obter ambos ao mesmo tempo. No entanto, as máquinas ATM demonstram a fraqueza da

teoria, já que quando se efectua a autenticação revelam-se os dois mecanismos simultaneamente tornando a pessoa vulnerável.

3.1.1.1 *Passwords*

Como um meio de autenticação pessoal, as *passwords* são do tipo "algo que tu sabes". Isto é uma vantagem porque não é requerido nenhum equipamento especial, e é também uma desvantagem porque "o que tu sabes" pode ser dito a alguém, adivinhado ou capturado [Ches-Be94].

As *passwords* não podem ser vistas como mecanismos fortes de autenticação, no entanto são um mecanismo que não desaparecerá tão cedo, porque é simples, barato, conveniente e eficiente.

3.1.1.2 *Passwords* de Utilização Única

É possível obter um aumento significativo na segurança usando *passwords* de utilização única. Uma *password* de utilização única comporta-se exactamente como o seu nome indica: é usada somente uma vez, depois do que deixa de ser válida. Isto providencia uma defesa bastante forte contra escutas (ataque de *snooping*[1]) e comandos de acesso pouco seguros.

Existem várias formas possíveis de implementar um esquema de *password* de utilização única, a mais conhecida envolve a utilização de uma espécie de autenticador portátil, também conhecido como *dongle* ou *token*.

Um sistema de *password* de utilização única utiliza um desafio (não repetível) proveniente do *host*. O utilizador tem um dispositivo que é programado com uma chave secreta. O "desafio" é introduzido no dispositivo, que calcula uma função do "desafio" e da chave secreta, e este valor serve de *password*. Este algoritmo é facilmente implementado num computador pessoal.

Este esquema envolve "algo que tu tens", que é susceptível de ser roubado. A defesa usual é adicionar "algo que tu sabes" na forma de um número de identificação pessoal (PIN). A combinação destes dois factores é bastante eficaz.

Lamport propôs um esquema de *password* de utilização única [Lampor81], que pode ser implementado sem *hardware* especial. Assume-se que existe uma função F que é razoavelmente fácil de computar na direcção descendente mas efectivamente impossível de inverter

[1] Ataque de Snooping – escuta passiva do tráfego de rede de forma a capturar dados valiosos ou confidenciais, tais como *passwords*.

(as funções de *hash*, descritas na secção 3.2.3, são boas candidatas). Assume-se também que o utilizador tem uma *password* – x.

Para permitir que o utilizar efectue o *login* um determinado número de vezes (n), o *host* calcula $F^n(x)$ esse número de vezes. Assim, para permitir 1000 *logins* antes que a *password* altere, o *host* calcula $F^{1000}(x)$, e guarda somente este valor.

A primeira vez que o utilizador efectuar o *login*, fornecerá $F^{999}(x)$. O sistema validá-lo-á calculando $F(F^{999}(x)) = F^{1000}(x)$. Se o *login* estiver correcto, a *password* fornecida – $F^{999}(x)$ – torna-se o novo valor a guardar, que será usado para validar $F^{998}(x)$, a próxima *password* fornecida pelo utilizador. O cálculo do utilizador $F^n(x)$ pode ser efectuado por um autenticador portátil ou por um posto de trabalho confiável ou computador portátil.

A implementação da Bellcore para este esquema [Haller94], designada por S/Key, permite ao sistema autenticar efectivamente um utilizador, e nada no sistema comprometerá a *password* do utilizador se o próprio sistema ficar comprometido. O sistema tem a possibilidade de validar a resposta actual do utilizador, mas não consegue prever qual será a sua próxima resposta [ChapZw95].

O S/Key funciona pela aplicação interactiva de um mecanismo criptográfico, uma função de *hash* segura (secção 3.2.3), começando por um dado valor inicial. O algoritmo utilizado é o MD4[2].

O esquema S/Key pode ser utilizado de duas maneiras: as chaves podem ser geradas à medida que forem sendo necessárias ("a pedido") ou pode ser utilizada uma lista impressa de chaves.

Para a geração das chaves "a pedido", o utilizador precisa de um computador e de um programa para as gerar. O utilizador providencia o valor inicial e o número de chaves desejadas, que serão geradas pelo programa. O valor inicial terá de ser introduzido pelo utilizador ou lido de um ficheiro do computador. Ambas as situações poderão ter inconvenientes, na primeira situação a escolha da "*password*" poder ser fraca e sujeitar o sistema a ataques de dicionário. Se o valor inicial for lido de um ficheiro, pode ser mais aleatório mas existe o risco, provavelmente baixo, de o ficheiro ser roubado.

Na alternativa de utilizar uma lista impressa de chaves, o sistema gera aleatoriamente o valor inicial e a listagem deve ser simplesmente uma lista de chaves, sem qualquer identificação ou explicação. A lista poderá ser roubada, mas é necessário equacionar qual das situações será mais provável: que a lista seja roubada e que a pessoa saiba o seu significado e o

[2] MD4 – Message Digest function 4, foi desenvolvido por Ron Rivest que desenvolveu posteriormente o MD5 (secção 3.2.3.1) e cooperou no desenvolvimento do algoritmo RSA (secção 3.2.2.4).

que fazer com ela, ou que, não utilizando este esquema, a sessão de trabalho seja escutada.

3.1.1.3 *Smart Cards*

O *smart card* é um dispositivo portátil que dispõe de um CPU, portas de entrada/saída, e alguns *Kbytes* de memória não volátil acessível somente através do CPU. Se o leitor do cartão estiver integrado convenientemente com o posto de trabalho, o *smart card* pode efectuar qualquer das técnicas de validação descritas anteriormente, mas sem os seus pontos fracos. Os *smart cards* são "algo que tu tens" e são normalmente associados a "algo que tu sabes", um número de identificação pessoal [ChesBe94].

Alguns *smart cards* têm leitores portáteis e alguns estão já disponíveis no formato PCMCIA.

Se considerarmos o esquema de desafio/resposta, como normalmente implementado, o *host* precisará de ter uma cópia da chave secreta do utilizador. Isto constitui um perigo, a base de dados de chaves é extremamente sensível, e não deve ser guardada em computadores vulgares. É possível evitar este problema utilizando técnicas criptográficas de chave pública (secção 3.2.2), mas existe um problema: o *output* de todos os algoritmos de chave pública conhecidos é demasiado longo para ser digitado convenientemente, ou mesmo para ser mostrado num pequeno ecrã. Um *smart card* pode não só efectuar os cálculos mas também pode transmiti-los directamente para o *host* através das suas portas de entrada/saída.

3.1.1.4 As Biométricas

No terceiro método de autenticação um *host* efectua a medição de algo intrínseco ao utilizador, que poderá ser algo como uma impressão digital, um registo da voz, ou uma assinatura. Obviamente, é necessário *hardware* especial, o que limita a aplicabilidade das técnicas biométricas a comparativamente poucos ambientes. O aspecto mais relevante é que um identificador biométrico não pode ser nem dado nem roubado.

Na prática existem algumas limitações. O bom senso na segurança convencional indica que os dados de autenticação devem ser alterados regularmente, o que se torna impraticável no caso de uma impressão digital. Pela sua natureza as biométricas não dão respostas exactas, duas assinaturas não são absolutamente iguais, mesmo se do mesmo indivíduo, e descontando efeitos como a exaustão, disposição ou doença. Desta forma, deve ser introduzida alguma tolerância no algoritmo, o que introduz também alguma insegurança.

Alguns sistemas utilizam *smart cards* para guardar os dados biométricos de cada utilizador. Isto evita a necessidade das bases de dados nos *hosts*, dependendo em vez disso da segurança do cartão para evitar interferências. É também possível incorporar um desafio aleatório do *host* no protocolo entre o *smart card* e o utilizador, evitando assim ataques de repetição.

Não são conhecidas utilizações regulares de dados biométricos na Internet. Mas as potencialidades deste método, e o desenvolvimento de tecnologias associadas à autenticação de dados biométricos possibilitarão uma utilização mais alargada especialmente em redes privadas com fortes requisitos de segurança.

3.1.2 Autenticação Máquina a Máquina

A forma dominante de autenticação máquina a máquina na Internet depende da rede. A rede transmite não só a identidade do utilizador remoto, mas presume-se também que seja suficientemente precisa para que possa ser utilizada como uma identidade autenticada, o que é perigoso. Temos dois tipos de autenticação de rede, baseada em endereços e baseada em nomes. Para o primeiro, o endereço IP da origem é aceite. Os ataques nesta forma consistem no envio de algo a partir de um endereço fraudulento. A precisão da autenticação depende da dificuldade da detecção dessas falsificações, e essa detecção pode ser bastante difícil.

A autenticação baseada em nomes é ainda mais fraca. Requer que não só o endereço esteja correcto, mas também o nome associado com esse endereço. Isto abre uma nova possibilidade de ataque para os intrusos, que podem corromper qualquer mecanismo utilizado para mapear os endereços IP nos nomes dos *hosts*. Os ataques ao serviço DNS tentam explorar este caminho.

3.1.2.1 Técnicas Criptográficas

As técnicas criptográficas providenciam uma base muito mais forte para autenticação. Estas técnicas dependem da posse de algum "segredo" ou chave criptográfica. A posse desse segredo é equivalente à prova da autenticidade do utilizador envolvido. Um exemplo são os autenticadores portáteis referidos anteriormente.

Se alguém partilhar uma chave somente com uma outra parte, e receber uma mensagem cifrada com essa chave, então sabe-se quem enviou a mensagem, pois mais ninguém a pode ter gerado. Na verdade, um atacante pode gravar uma mensagem antiga e retransmiti-la mais tarde. Isto é conhecido por ataque de repetição.

Normalmente não se partilha uma chave com todas as partes com as quais se pretende comunicar. A solução mais comum é um centro de distribuição de chaves (KDC – Key Distribution Center) [NeeSch78; DenSac81]. Cada parte partilha uma chave, e por isso alguma confiança, com o KDC. O KDC actua como um intermediário quando são estabelecidas comunicações. A parte que inicia a comunicação contacta o KDC enviando uma mensagem autenticada que nomeia a outra parte. O KDC pode então preparar uma mensagem para a outra parte, e autentica-a com a chave que ambos partilham. Em nenhuma altura o emissor sabe da chave secreta do receptor. O Kerberos é uma implementação de um KDC bastante conhecida.

Apesar de a autenticação criptográfica ter muitas vantagens, um número de problemas

impediram a sua larga divulgação. Os dois problemas mais críticos são a necessidade de um KDC seguro, e a dificuldade de manutenção das chaves dos *hosts* secretas. Para o primeiro, é necessário utilizar uma máquina dedicada, numa instalação fisicamente segura, ou utilizar um protocolo de troca de chaves baseado em criptografia de chave pública.

Quem conseguir comprometer o KDC pode personalizar qualquer dos seus clientes. De igual forma, quem quer que saiba a chave de um *host* pode fazer-se passar por esse *host* e, em geral, qualquer dos seus utilizadores. Isto constitui um problema sério, já que os computadores não são muito bons na manutenção de segredos durante muito tempo. A melhor solução é *hardware* criptográfico especializado, talvez manter a chave num *smart card*, mas mesmo isso não é uma solução garantida porque alguém que tenha penetrado a máquina pode programar o hardware criptográfico.

3.1.3 Controlo de Acesso

Uma vez verificada a identidade da pessoa, o acesso será garantido somente aos serviços, aplicações e recursos para os quais tenha sido autorizado.

O controlo de acesso é uma séria preocupação na segurança de rede. Quando um sistema computacional faz parte de uma rede, os utilizadores e mesmo os gestores de rede podem não saber que outros utilizadores podem estar ligados à mesma rede. Desta forma, num ambiente de rede, o controlo de acesso deve proteger um sistema de rede e também evitar que utilizadores não autorizados passem por um sistema de rede para aceder a outros sistemas da rede [Pfleeg97].

3.2 A Criptografia

A criptografia é a solução usual para a necessidade de comunicar sobre ligações inseguras sem a exposição do sistema. A utilização mais comum da criptografia é, obviamente, a manutenção da comunicação secreta. A autenticação está também relacionada com a criptografia, quer dizer, um pacote que não seja cifrado com uma chave correcta não será decifrado em algo que faça sentido, o que limita consideravelmente a possibilidade de injecção de falsas mensagens [ChesBe94].

Um número crescente de aplicações e protocolos usados sobre a Internet têm facilidades significativas relacionadas com a segurança ou têm como finalidade primária a provisão de alguma facilidade de segurança. Ao nível da aplicação temos os exemplos da segurança de *e-mail* (Privacy Enhanced Mail – PEM, Pretty Good Privacy – PGP), gestão de rede (Simple Network Management Protocol version 2 – SNMPv2), e autenticação remota (Kerberos). Uma facilidade comum em todas estas aplicações e protocolos é a utilização de algoritmos criptográficos para implementar serviços de segurança particulares. A maioria destes algoritmos cabem em três categorias: algoritmos de cifragem convencional, algoritmos criptográfi-

cos de chave pública, e funções de *hash* seguras [Stall94a].

3.2.1 Cifragem Convencional

A cifragem convencional, também designada por cifragem simétrica ou cifragem de chave única, foi o único tipo de cifragem utilizada antes do desenvolvimento da cifragem de chave pública. Mantém-se há bastante tempo como o mais largamente utilizado dos dois tipos de cifragem.

Na cifragem convencional, a mensagem inteligível original, referida como texto corrente, é convertida em texto aparentemente sem sentido, designado por texto cifrado. O processo de cifragem consiste num algoritmo e numa chave. A chave é um valor independente do texto corrente que controla o algoritmo. O algoritmo produz uma saída diferente dependendo da chave específica utilizada na altura.

A alteração da chave altera o *output* do algoritmo. Logo que o texto cifrado é produzido, é logo transmitido. Na recepção, o texto cifrado é reconvertido no texto original utilizando-se um algoritmo de decifração e a mesma chave que foi utilizada para a cifragem.

A segurança da cifragem convencional depende de vários factores. Em primeiro lugar, o algoritmo de cifragem deve ser suficientemente poderoso para que seja impraticável decifrar uma mensagem com base somente do texto cifrado. Para além disso, a segurança da cifragem convencional depende do secretismo da chave, não no secretismo do algoritmo. Assume-se que é impraticável decifrar uma mensagem com base do texto cifrado mais o conhecimento do algoritmo de cifragem/decifração.

Esta característica da cifragem convencional é o que a torna praticável para uma larga utilização. O facto de o algoritmo não necessitar de ser mantido secreto significa que os fabricantes poderam desenvolver implementações de *chips* de baixo custo de algoritmos de cifragem de dados. Esses *chips* estão largamente disponíveis e incorporados em muitos produtos. Com a utilização da cifragem convencional, o principal problema de segurança é a manutenção do secretismo da chave.

A Figura 3.1 apresenta os elementos essenciais de um esquema de cifragem convencional. Existe uma fonte da mensagem, que produz uma mensagem em *plaintext*, $X = [X_1, X_2, ..., X_M]$. Os M elementos de X são caracteres de algum alfabeto finito. Actualmente, o alfabeto binário {0, 1} é utilizado tipicamente. Para a cifragem, é gerada uma chave da forma $K = [K_1, K_2, ..., K_J]$.

Se a chave for gerada na fonte da mensagem, então deve ser também providenciada ao destino através de algum canal seguro. Alternativamente, uma terceira parte pode gerar a chave e enviá-la de forma segura para a fonte e o destino.

Com a mensagem X e a chave K como *input*, o algoritmo de cifragem gera o texto cifrado $Y = [Y_1, Y_2, \ldots, Y_N]$. Podemos expressar isto como: $Y = E_K(X)$. Esta notação indica que Y é produzido utilizando o algoritmo de cifragem E como função do texto corrente X, com a função específica determinada pelo valor da chave K.

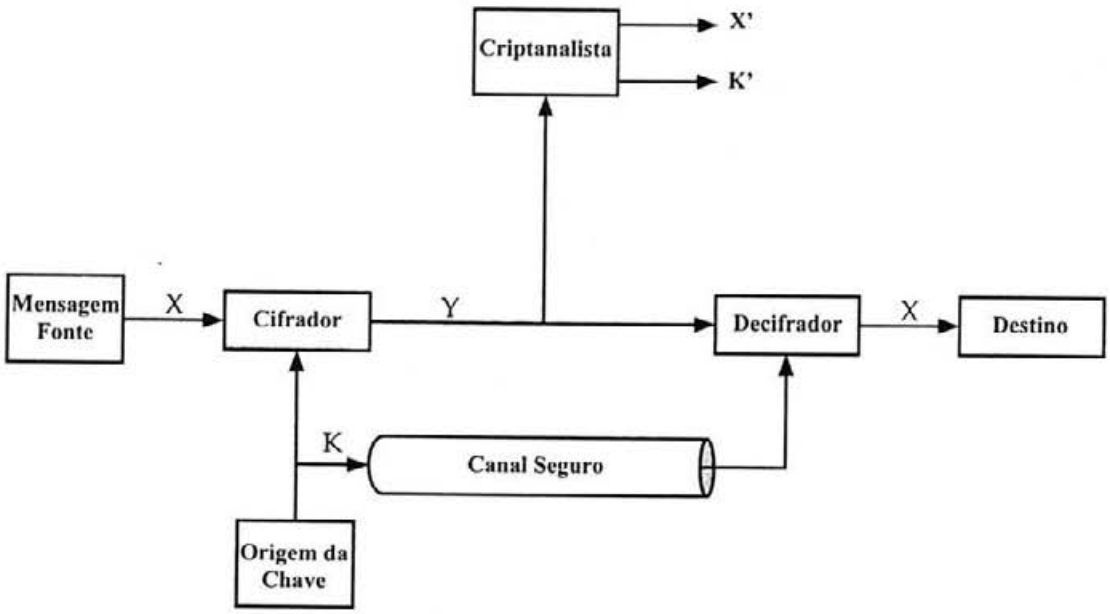


Figura 3.1 – Modelo do Sistema de Criptografia Convencional [Stall95]

O receptor, na posse da chave, é capaz de inverter a transformação: $X = D_K(Y)$. Um oponente que observa Y mas que não tenha acesso a K ou X, tentará obter X ou K ou ambos. Assume-se que o oponente não tem conhecimento dos algoritmos de cifragem (E) e decifração (D). Se o oponente estiver interessado somente nesta mensagem particular, então a focalização do esforço será recuperar X pela geração de um texto corrente estimado X'. Muitas vezes, no entanto, o oponente está interessado em ser capaz de ler mensagens futuras, nesse caso é feita uma tentativa de recuperar K gerando uma chave K' estimada.

3.2.1.1 Cifradores de Bloco e Modos de Operação

Os algoritmos de cifragem convencional mais utilizados são os "cifradores de bloco". Um cifrador de bloco processa o texto corrente de entrada em blocos de tamanho fixo, e produz um bloco de texto cifrado de tamanho igual para cada bloco de texto corrente. Alguns dos mais importantes cifradores de bloco estão listados na Tabela 3.1.

Os cifradores de bloco são utilizados geralmente como operações primitivas para implementar "modos de operação" mais complexos. O CBC (Cipher Block Chaining) é o mais importante modo de operação; a cada bloco de texto corrente é feito o OU-exclusivo com o bloco prévio antes da cifragem [ChesBe94].

Como os cifradores de bloco tratam cada bloco de texto independentemente, ficam

propícios a tipos de ataque como o *block replay*, nos quais blocos cifrados de uma transmissão são enviados numa segunda transmissão. A solução para este problema é o *block chaining*. Com o *block chaining*, cada bloco é combinado com o próximo bloco da mensagem, de forma que é impossível substituir um bloco cifrado por outro sem ser descoberto [Pfleeg97].

Algoritmo	Tamanho Chave (*bits*)	Tamanho Bloco (*bits*)	Exemplo de aplicações
DES	56	64	Kerberos, PEM, SNMPv2
Triple DES	112	64	PEM
IDEA	128	64	PGP
SKIPJACK	80	64	Clipper
DES = Data Encryption Standard			
IDEA = International Data Encryption Algorithm			
PEM = Privacy Enhanced Mail			
SNMPv2 = Simple Network Management Protocol, version 2			
PGP = Pretty Good Privacy			

Tabela 3.1 – Algoritmos de Cifragem Convencional Mais Importantes [Stall94a]

3.2.1.2 O DES

O esquema de cifragem mais largamente utilizado é definido no Data Encryption Standard (DES) adoptado desde 1977 pelo NIST (National Institute of Standards and Technology). O NIST recomenda o uso do DES para aplicações que não visem a protecção de informação classificada [Stall94a].

O DES é um cifrador de bloco que mapeia blocos de 64 *bits* de texto corrente em blocos de 64 *bits* de texto cifrado e vice versa. Utiliza uma chave de 56 *bits*.

A cifragem no DES é efectuada através de séries complexas de permutações e substituições. Com o resultado dessas operações é efectuado o OU exclusivo com o texto de *input*. Esta sequência é repetida 16 vezes, utilizando de cada vez uma ordenação diferente dos *bits* da chave. A tentativa de completar um *bit* da chave ou do texto corrente provocará uma mudança de aproximadamente 50% dos *bits* de *output*. Desta forma, quase nenhuma informação de *input* é revelada; pequenas alterações no texto corrente provocará variações massivas no texto cifrado [ChesBe94].

O esquema de cifragem do DES é caracterizado em pormenor no Apêndice A.1.

3.2.1.3 O Triple DES

Dadas as potenciais vulnerabilidades do DES a um ataque de força bruta, tem havido um interesse considerável numa alternativa. Uma abordagem será desenhar um algoritmo completamente novo, tal como o IDEA. Alternativamente, preservando os investimentos existentes, será de utilizar cifragem múltipla com o DES e múltiplas chaves.

A forma mais popular de DES múltiplo, referido por Triple DES, foi primeiramente proposto por [Wiener93] e normalizado em 1985 pelo American National Standards Institute (ANS X9.17). O Triple DES utiliza duas chaves e três execuções do algoritmo DES (Figura 3.2). A função segue uma sequência cifra-decifra-cifra (EDE):

$$C = E_{K1} [D_{K2} [E_{K1} [P]]]$$

Não existe significado criptográfico na utilização da decifração na segunda etapa. A única vantagem é que permite aos utilizadores do Triple DES decifrar dados cifrados por utilizadores do DES simples.

$$C = E_{K1} [D_{K1} [E_{K1} [P]]] = E_{K1} [P]$$

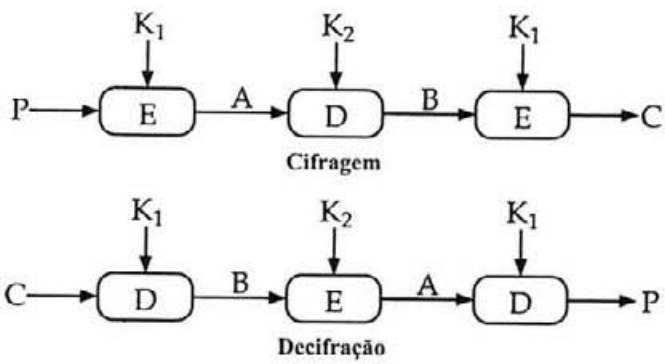


Figura 3.2 – Triple DES [Stall95]

Apesar de só serem utilizadas duas chaves, são necessárias três instâncias do algoritmo DES. Existe uma técnica simples, conhecida como ataque *meet-in-the-middle*, que reduz um sistema duplo DES com duas chaves à força relativa do DES simples. Com três iterações da função DES, o tamanho efectivo da chave é de 112 *bits*.

3.2.1.4 IDEA

O IDEA (International Data Encryption Algorithm) é um algoritmo de cifragem convencional orientado ao bloco, desenvolvido em 1990 por [LaiMas90]. Foi apresentada uma versão revista do algoritmo [LaiMas91], desenhada para fazer frente aos recentes avanços nos ataques criptanalíticos [Stall94a].

O IDEA é um cifrador de bloco que utiliza uma chave de 128 *bits* para cifrar dados em blocos de 64 *bits*.

O IDEA na sua estrutura geral é semelhante ao DES. A suâ força baseia-se na utilização de três operações diferentes – o OU exclusivo, a adição modular, e a multiplicação modular – em cada iteração. Adicionalmente, utiliza uma chave de 128 *bits* para protecção contra ataques de pesquisa exaustivos [ChesBe94].

O esquema global da cifragem IDEA está ilustrado no Apêndice A.2.

3.2.1.5 SKIPJACK

Em Abril de 1993, a administração Clinton anunciou uma proposta de tecnologia de cifragem que visava melhorar a segurança e privacidade das comunicações telefónicas. Em Julho, foi feito um anúncio mais formal com base num RFC (*request for comments*) proposto pela Federal Information Processing Standard.

Esta iniciativa, de acordo com o governo americano, tinha dois objectivos: (1) encorajar a larga utilização de uma tecnologia de cifragem que permita às agências governamentais, quando legalmente autorizadas, monitorar e efectuar o *wiretap* das comunicações privadas, e (2) providenciar ao público o acesso a uma tecnologia de cifragem sofisticada e poderosa de forma a corresponder às necessidades privadas, especialmente das empresas, para a manutenção da confidencialidade.

O algoritmo, referido por SKIPJACK, é um algoritmo de cifragem convencional. O SKIPJACK é um cifrador de bloco que utiliza uma chave de 80 *bits* para cifrar dados em blocos de 64 *bits*. O algoritmo envolve 32 etapas de processamento para uma única cifragem ou decifração, utilizando uma função não linear complexa para cada etapa. Isto é essencialmente o que é publicamente conhecido sobre o algoritmo.

3.2.2 Cifragem de Chave Pública

A cifragem de chave pública, primeiramente proposta por Diffie e Helman em 1976 [DifHel76], é o primeiro avanço verdadeiramente revolucionário na cifragem em milhares de anos. Os algoritmos de chave pública são baseados em funções matemáticas em vez de substituições ou permutações. Mas mais importante ainda, a criptografia de chave pública é assimétrica, envolvendo a utilização de duas chaves separadas, em contraste com a cifragem convencional simétrica, que utiliza só uma chave. A utilização de duas chaves tem profundas consequências nas áreas da confidencialidade, distribuição de chaves e autenticação [Stall94b].

3.2.2.1 Mal Entendidos

Existem vários mal entendidos respeitantes à cifragem de chave pública. Um desses mal entendidos é que a cifragem de chave pública é mais segura em relação à criptanálise que a cifragem convencional. De facto, a segurança de qualquer esquema de cifragem depende do tamanho da chave e do trabalho computacional envolvido na quebra da cifra. Não existe nada em princípio sobre a cifragem convencional e de chave pública que torne uma superior à outra do ponto de vista da resistência à criptanálise.

Um segundo mal entendido é que a cifragem de chave pública é uma técnica de utilização geral que tornou a cifragem convencional obsoleta. Pelo contrário, devido à sobrecarga

computacional dos esquemas actuais de cifragem de chave pública, não parece viável que a cifragem convencional seja abandonada.

Finalmente, existe o sentimento que a distribuição de chaves é trivial quando se utiliza a cifragem de chave pública, comparado com o pesado *handshaking* envolvido com os centros de distribuição de chaves da cifragem convencional. De facto, é necessário alguma forma de protocolo, muitas das vezes envolvendo um agente central, e os procedimentos envolvidos não são mais simples nem mais eficientes que os requeridos para a cifragem convencional.

3.2.2.2 Características

Um algoritmo criptográfico de chave pública baseia-se numa chave para cifragem e uma chave diferente mas relacionada para decifração. Esses algoritmos têm as seguintes características importantes:

- É computacionalmente impossível determinar a chave de decifração sabendo-se somente o algoritmo criptográfico e a chave de cifragem.

Adicionalmente, alguns algoritmos, tal como o RSA, também têm a seguinte característica:

- Qualquer das chaves relacionadas pode ser usada para a cifragem, com a outra usada para a decifração.

Os passos essenciais são os seguintes:

1. Cada *end system* numa rede gera um par de chaves para ser usado para cifragem e decifração das mensagens.
2. Cada sistema publica a sua chave de cifragem colocando-a num registo público ou ficheiro. Esta é a chave pública, a outra chave é mantida privada.
3. Se A quiser enviar uma mensagem para B, cifra a mensagem utilizando a chave pública de B.
4. Quando B receber a mensagem, decifra-a utilizando a sua chave privada. Mais nenhum receptor pode decifrar a mensagem porque só B conhece a sua chave privada.

Com esta abordagem, todos os participantes têm acesso às chaves públicas, e as chaves privadas são geradas localmente por cada participante, não precisando desta forma de serem distribuídas. Enquanto um sistema controlar as suas chaves privadas, as comunicações recebidas são seguras. Em qualquer altura, um sistema pode alterar a sua chave privada e publicar a respectiva chave pública do par, que substituirá a chave pública antiga.

A Figura 3.3 ilustra o processo; existe uma fonte A de uma mensagem, que produz uma mensagem de texto corrente, $X = [X_1, X_2, \ldots, X_M]$. Os M elementos de X são letras de

um alfabeto finito. A mensagem é destinada a B. B gerou um par de chaves relacionadas: uma chave pública KU_b, e uma chave privada KR_b. KR_b é secreta, conhecida só por B, enquanto KU_b está disponível publicamente, e portanto acessível a A.

Com a mensagem X e a chave de cifragem KU_b, A forma o texto cifrado $Y = [Y_1, Y_2, ..., Y_N]$:

$$Y = E_{KUb}(X)$$

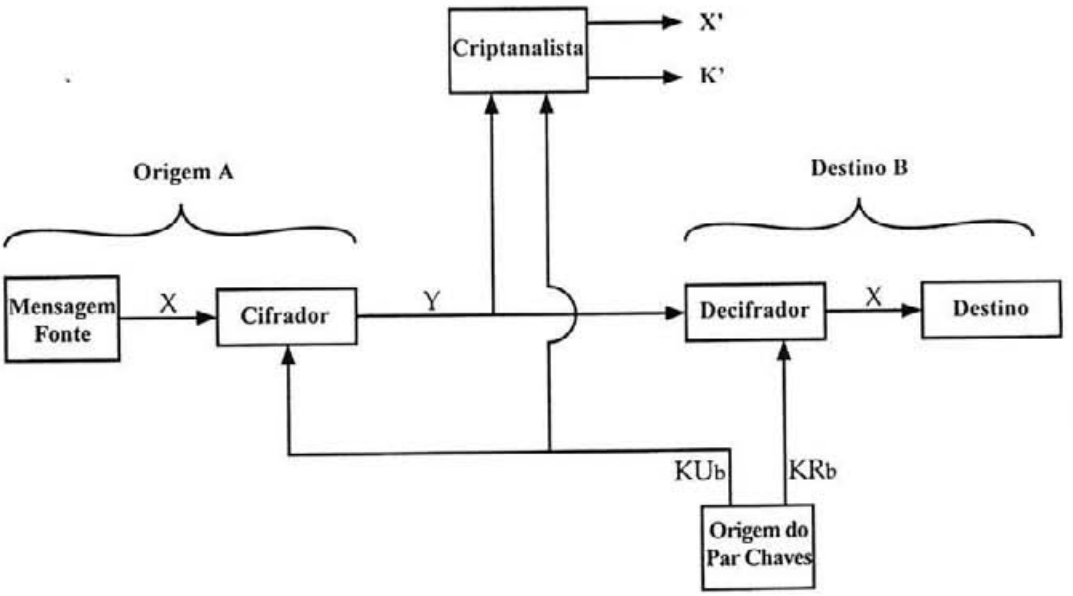


Figura 3.3 – Sistema Criptográfico de Chave Pública [Stall95]

O receptor, em posse da correspondente chave privada, pode inverter a transformação:

$$X = D_{KRb}(Y)$$

Um oponente, observando Y e tendo acesso a KU_b, mas não tendo acesso a KR_b ou X, tem de tentar recuperar X e/ou KR_b. Assume-se que o oponente tem conhecimento dos algoritmos de cifragem (E) e decifração (D).

3.2.2.3 Assinatura Digital

Como foi referido anteriormente, ambas as chaves relacionadas podem ser usadas para cifragem, com a outra utilizada para decifração. Isto permite implementar um esquema criptográfico bastante diferente:

$$Y = E_{KRa}(X)$$

$$X = D_{KUa}(Y)$$

Neste caso, A cifra uma mensagem para B utilizando a sua chave privada antes de a transmitir. B pode decifrar a mensagem utilizando a chave pública de A. Como a mensagem foi cifrada utilizando-se a chave privada de A, somente A pode ter preparado a mensagem. Desta forma, a mensagem cifrada serve de *assinatura digital*. Para além disso, é impossível alterar a mensagem sem aceder à chave privada de A, portanto a mensagem é autenticada quer em termos da fonte quer em termos de integridade de dados.

No esquema descrito, a mensagem completa é cifrada, o que apesar de validar o autor e o conteúdo, requer uma grande capacidade de armazenamento. Cada documento deve ser mantido em texto corrente para ser utilizado para fins práticos, e deve ser mantida também uma cópia em texto cifrado de forma que a origem e o conteúdo possam ser verificados em caso de disputa:

Uma forma mais eficiente de obter o mesmo resultado será cifrar um pequeno bloco de *bits* que é função do documento. Um tal bloco, designado um *autenticador*, deve ter a propriedade de ser impraticável alterar o documento sem alterar o autenticador. Se o autenticador for cifrado com a chave privada do emissor, serve como assinatura que verifica a origem, conteúdo e sequenciamento. Um código de *hash* seguro, descrito na secção 3.2.3 (Funções de *Hash* Seguras), pode servir para esta função.

É importante enfatizar que o processo de cifragem descrito não providencia confidencialidade; a mensagem a ser enviada está segura de alteração mas não está segura de escuta de comunicações. Isto é obvio no caso de uma assinatura baseada numa porção da mensagem, já que o resto da mensagem é transmitida sem cifragem. Mas mesmo no caso de cifragem completa, não existe protecção da confidencialidade pois qualquer observador pode decifrar a mensagem utilizando a chave pública do emissor.

Algoritmo	Funcionalidade	Exemplo de aplicações
RSA	Assinatura Digital; Cifragem	PEM, PGP
DSA	Assinatura Digital	DSS
RSA = Rivest, Shamir, Adleman		
DSA = Digital Signature Algorithm		
PEM = Privacy Enhanced Mail		
PGP = Pretty Good Privacy		
DSS = Digital Signature Standard		

Tabela 3.2 – Algoritmos Criptográficos de Chave Pública mais Notáveis

3.2.2.4 RSA

Um dos primeiros esquemas de cifragem de chave pública foi desenvolvido em 1997 por Ron Rivest, Adi Shamir, e Len Adleman, no MIT (Massachusetts Institute of Technology) e publicado em 1978 [RiShAd78]. O esquema *Rivest-Shamir-Adleman* (RSA) é desde essa altura a única abordagem de cifragem de chave pública largamente aceite e implementada. O RSA é

um cifrador de bloco no qual o texto corrente e o texto cifrado são inteiros entre 0 e n - 1 para qualquer n. Para um texto corrente M e um texto cifrado C, a cifragem e a decifração têm a seguinte forma:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Quer o emissor quer o receptor têm de saber o valor de n. O emissor sabe o valor de e, e somente o receptor sabe o valor de d. Portanto, é um algoritmo de cifragem de chave pública com a chave pública KU = $\{e, n\}$ e uma chave privada KR = $\{d, n\}$. Para este algoritmo ser satisfatório para cifragem de chave pública, os seguintes requisitos devem ser cumpridos:

1. É possível encontrar valores de e, d, n tal que $M^{ed} = M \bmod n$ para todos os $M < n$.
2. É relativamente fácil de calcular M^e e C^d para todos os valores de $M < n$.
3. É impraticável determinar d dados e e n (para valores grandes de e e n).

A Tabela 3.3 sumaria o algoritmo. Começa-se por seleccionar dois números primos, p e q e calcula-se os seu produto n, que é o módulo para a cifragem e decifração. A seguir, calcula-se *phi(n)*, que é o número de inteiros positivos menores que n e relativamente primos com n. Depois selecciona-se um inteiro d que é relativamente primo com *phi(n)* (i. e. o máximo divisor comum de d e *phi(n)* é 1). Finalmente, calcula-se e como o multiplicativo inverso de d, módulo *phi(n)*. Demonstra-se que d e e têm as propriedades desejadas.

Geração das Chaves	
Seleccionar p, q	p e q ambos primos
Calcular $n = p \times q$	
Calcular $phi(n) = (p - 1)(q - 1)$	
Seleccionar o inteiro d	$mdc(phi(n), d) = 1;\ 1 < d < phi(n)$
Calcular e	$e = d^{-1} \bmod phi(n)$
Chave Pública	KU = $\{e, n\}$
Chave Privada	KR = $\{d, n\}$
Cifragem	
Texto Corrente: $M < n$	
Texto Cifrado: $C = M^e \pmod n$	
Decifração	
Texto Cifrado: C	
Texto Corrente: $M = C^d \pmod n$	

Tabela 3.3 – O Algoritmo RSA

Supondo que o utilizar A publicou a sua chave pública e que o utilizar B deseja enviar a mensagem M a A, então B calcula $C = M^e \pmod n$ e transmite C. Na recepção deste texto cifrado, o utilizar A decifra-o calculando $M = C^d \pmod n$.

Existem duas abordagens possíveis para vencer o algoritmo RSA. O primeiro é a força bruta: tentar todas as chaves privadas possíveis. Desta forma quanto maior for o número de *bits* de *e* e *d*, mais seguro será o algoritmo. No entanto, devido aos cálculos envolvidos, na geração das chaves e na cifragem e decifração, quanto maior for o tamanho da chave mais lento o sistema será.

O Poder do RSA

A maioria das discussões sobre a criptanálise do RSA focam a tarefa de factorizar *p* nos seus dois factores primos. Até recentemente, pensa-se ser impraticável para números na ordem de cem dígitos decimais, que consiste em cerca de 300 *bits* ou mais.

Para demonstrar a força do RSA, os seus autores lançaram um desafio de decifrar uma mensagem cifrada utilizando um número de 129 dígitos decimais como módulo da chave pública. Os autores predisseram que levaria 40 quatriliões de anos, com a tecnologia actual, para descobrir o código.

O código foi descoberto por uma equipa mundial que colaborou através da Internet e utilizou mais de 1600 computadores depois de somente oito meses de trabalho [Leutw94]. Este resultado não invalida a utilização do RSA, significa simplesmente que devem ser utilizadas chaves maiores. Actualmente, uma chave de 1024 *bits* (cerca de 300 dígitos decimais), é considerada suficientemente forte para virtualmente todas as aplicações.

3.2.2.5 Digital Signature Standard (DSS)

O NIST (National Institute of Standards and Technology.) publicou o FIPS[3] PUB 186 designado Digital Signature Standard (DSS). O DSS utiliza o SHA (Secure Hash Algorithm) descrito na secção 3.2.3.2, e apresenta uma nova técnica de assinatura digital, o DAS (Digital Signature Algorithm). O DSS foi originalmente proposto em 1991 e revisto em 1993 em resposta a problemas levantados respeitantes à segurança do esquema [Stall95].

A abordagem DSS

O DSS usa um algoritmo que foi desenhado para providenciar somente a função de assinatura digital. Ao contrário do RSA, não pode ser usado para cifragem. Apesar disso, é uma técnica de chave pública [Stall94b]. O DSA é baseado na dificuldade de cálculo de logaritmos discretos [Stall95]. O algoritmo em si é bastante complexo e não será descrito aqui.

A Figura 3.4 contrasta a abordagem DSS para a geração de assinaturas digitais com algoritmos como o RSA. Na abordagem RSA, a mensagem a ser assinada é *input* de uma

[3] FIPS – Federal Information Processing Standard.

função de *hash* que produz um código de *hash* seguro de tamanho fixo. O código de *hash* é depois cifrado utilizando a chave privada do emissor para formar a assinatura. A mensagem e a assinatura são depois transmitidas. O receptor utiliza a mensagem para produzir o código de *hash*, e decifra a assinatura utilizando a chave pública do emissor. Se o código de *hash* calculado coincidir com a assinatura decifrada, a assinatura é aceite como válida. Como só o emissor conhece a chave privada, só o emissor poderia ter produzido a assinatura válida.

A abordagem DSS também utiliza uma função de *hash*. O código de *hash* é fornecido como *input* para a função de assinatura juntamente com um número aleatório k gerado para esta assinatura particular. A função de assinatura também depende da chave privada (KR_a) do emissor e de um conjunto de parâmetros que constitui uma chave pública global (KU_G). O resultado é uma assinatura constituída por dois componentes, s e r.

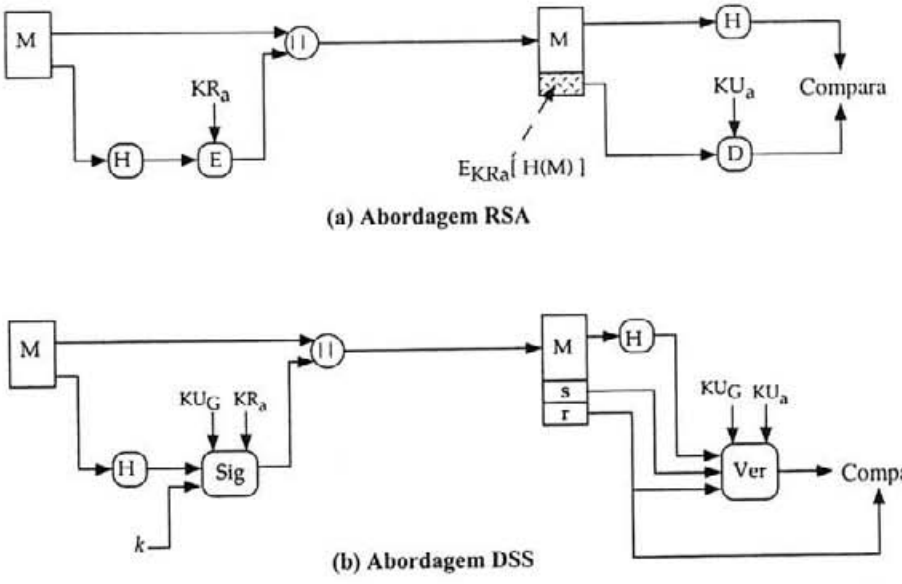


Figura 3.4 – Duas Abordagens para a Assinatura Digital [Stall95]

Na recepção, é gerado o código de *hash* da mensagem recebida, que juntamente com a assinatura é o *input* para uma função de verificação que depende também da chave pública global e da chave pública do emissor (KU_a), a qual é emparelhada com a chave privada do emissor. O *output* da função de verificação é um valor que é igual ao componente r da assinatura se a assinatura for válida. A função de assinatura é tal que só o emissor, com conhecimento da chave privada, pode ter produzido a assinatura válida.

3.2.3 Funções de *Hash* Seguras

Um valor de *hash* é gerado por uma função H da forma:

$$h = H(M)$$

Onde M é uma mensagem de tamanho variável, e H(M) é o valor de *hash* de tamanho

fixo. O valor de *hash* é adicionada à mensagem na fonte, numa altura em que se assume que a mensagem está correcta. O receptor autentica a mensagem recalculando o valor de *hash*. Como a função de *hash* não é secreta, é necessário alguma forma de proteger o valor de *hash* [Stall94b].

O propósito da função de *hash* é de produzir uma "impressão digital" de um ficheiro, mensagem, ou outro bloco de dados. Existem duas aplicações para as funções de *hash*: autenticação de mensagens e assinatura digital. Uma forma de usar uma função de *hash* para autenticação é adicionar um valor secreto, partilhado pelo emissor e receptor, à mensagem, e obter a função de *hash* da mensagem mais o valor secreto. A mensagem e a função de *hash* são transmitidas. Na recepção, o valor secreto é novamente adicionado à mensagem e a função de *hash* recalculada. Se os dois valores de *hash* coincidirem, assume-se que a mensagem não foi alterada.

Para aplicações de assinatura digital, o emissor calcula a função de *hash* de uma mensagem e cifra a função de *hash* com a sua chave privada. A mensagem e a função de *hash* cifrada é depois transmitida. O receptor calcula a função de *hash* e pode recuperar a função de *hash* transmitida decifrando-a com a chave pública do emissor. Novamente, a coincidência de valores assume que a mensagem não foi alterada. Para além disso, a função de *hash* cifrada funciona como uma assinatura já que só o referido emissor sabe a chave privada requerida.

Para ser eficaz na autenticação de mensagens e na assinatura digital, uma função de *hash* H deve ter as seguintes propriedades:

1. Pode ser aplicada a H um bloco de dados de qualquer tamanho.
2. H produz um *output* de tamanho fixo.
3. $H(x)$ é relativamente fácil de calcular para qualquer x, tornando praticáveis as implementações quer em *hardware* quer em *software*.
4. Para qualquer código m, é computacionalmente impraticável encontrar um x tal que $H(x) = m$.
5. Para um dado bloco x, é computacionalmente impraticável encontrar um y não igual a x com $H(y) = H(x)$.
6. É computacionalmente impraticável encontrar um par (x, y) tal que $H(x) = H(y)$.

A três primeiras propriedades são requisitos para a aplicação prática da função de *hash* à autenticação de mensagens.

A quarta propriedade é a propriedade "um sentido": É fácil gerar um código dada uma mensagem mas virtualmente impossível gerar uma mensagem dado um código. Esta propriedade é importante se a técnica de autenticação envolver a utilização de um valor secreto.

O valor secreto em si não é enviado, no entanto, se a função de *hash* não for "um sentido", um atacante pode facilmente descobrir o valor secreto: Se o atacante puder observar ou

interceptar uma transmissão, obtém a mensagem M e código de *hash* $C = H(S_{AB} \| M)$. O atacante pode então inverter a função de *hash* para obter $S_{AB} \| M = H^{-1}(C)$. Como o atacante tem agora M e $S_{AB} \| M$, será trivial recuperar S_{AB}.

A quinta propriedade garante que não pode ser encontrada uma mensagem alternativa com o mesmo valor de *hash* que uma dada mensagem. Isto impede que o código de *hash* possa ser forjado. Se esta propriedade não fosse verdadeira, um atacante poderia efectuar a seguinte sequência: observar ou interceptar uma mensagem e o seu código de *hash* cifrado; gerar um código de *hash* não cifrado a partir da mensagem; e gerar uma mensagem alternativa com o mesmo código de *hash*.

Uma função de *hash* que satisfaça as cinco primeiras propriedades da lista precedente é designada por função de *hash* fraca. Se a sexta propriedade for também verificada, é designada por função de *hash* forte. A sexta propriedade protege contra uma classe de ataques sofisticada conhecida por "Birthday Attack". Duas das mais seguras funções de *hash* estão listadas na Tabela 3.4.

Algoritmo	**Tamanho Código Hash (*bits*)**	**Exemplo Aplicações**
MD5	128	PEM, PGP, SNMPv2
SHA	160	DSS
MD5 = Message Digest, version 5		
SHA = Secure Hash Algorithm		
SNMPv2 = Simple Network Management Protocol, version 2		
PGP = Pretty Good Privacy		
PEM = Privacy Enhanced Mail		
DSS = Digital Signature Standard		

Tabela 3.4 – Algoritmos de *Hash* Seguro Mais Notáveis

3.2.3.1 MD5

O MD5 (Message-Digest Algorithm) foi desenvolvido por Ron Rivest [Rivest92]. O algoritmo tem como *input* uma mensagem de tamanho arbitrário e produz como *output* uma mensagem resumida (*digest*) de 128 *bits*. O *input* é processado em blocos de 512 *bits*.

- O apêndice A.3 descreve o processamento geral de uma mensagem para produzir o "resumo".

3.2.3.2 Secure Hash Algorithm (SHA)

O SHA (*Secure Hash Algorithm*) foi desenvolvido pelo NIST e publicado no FIPS PUB 180 em 1993. O SHA é baseado no algoritmo MD4, o percursor do MD5. É utilizado como parte da Digital Signature Standard, mas pode ser utilizado em qualquer aplicação que requeira um código de *hash*.

	MD5	SHA
Tamanho do "resumo"	128 *bits*	160 *bits*
Unidade básica de processamento	512 *bits*	512 *bits*
Número de passos	64 (quatro etapas de 16)	80
Tamanho máximo da mensagem	(infinito)	2^{64} *bits*
Funções lógicas primitivas	4	3
Constantes aditivas utilizadas	64	4

Tabela 3.5 – Comparação entre o MD5 e o SHA

A Tabela 3.5 sumaria as principais diferenças entre os dois algoritmos. Em termos comparativos, podemos analisar os seguintes objectivos de desenho:

Segurança: A diferença mais importante e mais óbvia, é que o resumo SHA é 32 *bits* maior que o resumo MD5. Se nenhum dos algoritmos contiver alguma falha estrutural vulnerável a um ataque criptanalítico, o que é até agora uma assunção razoável, então o SHA é o algoritmo mais forte. Utilizando uma técnica de força bruta, a dificuldade de produzir qualquer mensagem que tenha um dado "resumo" de mensagem é da ordem de 2^{128} operações para o MD5 e 2^{160} para o SHA, e a dificuldade de produzir duas mensagens tendo o mesmo "resumo" é da ordem de 2^{64} operações para MD5 e 2^{80} para o SHA.

Velocidade: Como ambos os algoritmos se baseiam bastante na adição módulo 2^{32}, ambos respondem bem em arquitecturas de 32 *bits*. O SHA envolve mais passos (80 *versus* 64) e tem de processar um *buffer* de 160 *bits* em comparação com o *buffer* de 128 *bits* do MD5. Desta forma, o SHA deve ser cerca de 25% mais lento que o MD5 no mesmo hardware.

Simplicidade e compactação: Ambos os algoritmos são simples de implementar, sem requisitos de grandes programas ou tabelas de substituição. No entanto, o SHA usa uma estrutura de passo simples, comparado com as quatro estruturas utilizadas no MD5. Para além disso, a manipulação das *words* do *buffer* é a mesma para todos os passos SHA, enquanto no MD5, o arranjo das *words* é especificada individualmente para cada passo. Portanto, nesta categoria o SHA é melhor.

3.2.4 Aspectos Legais na Criptografia

A criptografia está sujeita às políticas dos vários governos que detêm o direito de controlar a exportação, importação, e uso da cifragem no interesse da segurança nacional. Alguns países permitem-na, muitos restringem-na, e outros proíbem-na completamente, não deixando outra alternativa aos gestores de rede senão utilizar a cifragem mais forte disponível [DomDC98].

3.2.4.1 A Situação Actual

Dos esquemas de cifragem, o mais utilizado é o DES que é utilizado já há cerca de

vinte anos, o que o torna antigo e ineficiente para as necessidades actuais. Os especialistas dizem que o DES com uma chave de 40 *bits* pode ser quebrado numa questão de minutos, e que o DES com chaves de 56 *bits*, provavelmente suficientemente forte para a maioria das aplicações actuais, pode tornar-se vulnerável dentro de alguns anos[4]. Isso pode explicar a crescente popularidade do Triple DES pois cifra os dados três vezes utilizando diferentes chaves, o que equivale a um tamanho de chave de 112 *bits*.

Outras tecnologias oferecem diferentes tamanhos de chave, por exemplo o RC5 até 2.048 bits e o RSA não tem limite de tamanho de chave. Muitos produtos combinam tecnologias, utilizam um algoritmo rápido tal como o DES para a cifragem mas enviam a chave DES através de um método mais seguro como o RSA.

Desta forma a cifragem de dados coloca os governos num dilema; precisam de ponderar as necessidades de utilizadores que necessitam da maior segurança e fabricantes que competem internacionalmente com a possibilidade da tecnologia cair nas mãos de criminosos ou potenciais inimigos.

Os Estados Unidos da América, que detêm a maioria da produção de produtos de rede, têm estabelecido vários controlos de exportação ao longo do tempo. Antes de 1997, os EUA baseavam a sua política de exportações no tamanho da chave, mas desde então o ênfase foi direccionado para a "recuperação de chaves" – a possibilidade de agentes da lei retirarem chaves de uma base de dados central se necessário. Os fabricantes que utilizarem o mecanismo da recuperação de chaves nos seus produtos podem exportar cifragem com chaves de qualquer tamanho; aqueles que se comprometerem a fazê-lo no espaço de dois anos podem exportar cifragem de 56 bits até essa altura. Os fabricantes que não efectuarem o compromisso ficam limitados à exportação de produtos com um tamanho máximo de chave de 40 bits apenas (o DES é 56 bits), a não ser que esses produtos sejam para utilização em instituições bancárias.

Não só muitos fabricantes se recusaram a implementar a recuperação de chaves, mas outros países optaram por não seguir os EUA. Pior ainda, muitos fabricantes classificaram a recuperação de chaves como impraticável para a Internet. O grande problema está em quem deve ficar responsável pela base de dados central. Originalmente, os próprios governos ficariam com essa responsabilidade, mas a França é o único país ainda a apoiar essa proposta. Os EUA favorecem a utilização de organizações terceiras confiáveis, mas o problema é encontrar

---

[4] A RSA Data Security (www.rsa.com) anunciou em 17 de Julho de 98 que a Electronic Frontier Foundation (EFF) tinha quebrado o DES II Challenge em menos de 3 dias. Este desafio lançado em Janeiro de 97 pela RSA, tinha por objectivo demonstrar que a segurança das chaves DES de 56 bits oferece somente uma segurança marginal contra um adversário empenhado.
Os pesquisadores da EFF construíram um supercomputador de $250,000 que quebrou a chave DES, batendo o anterior recorde de 39 dias efectuado por uma rede de dezenas de milhares de computadores.

organizações em quem quer os fabricantes quer os governos possam confiar.

3.2.4.2 As Restrições nos Diferentes Países

A situação das restrições na criptografia leva a questionar como é que vários tipos de produtos de segurança – como *software* ou *hardware* VPN (ver capítulo 5), *firewalls*, e *software* de mensagens e *browsers* – podem ser utilizados. Nos EUA e no Canadá (onde os controlos de exportação dos EUA não se aplicam), os gestores de rede têm uma grande gama de escolha de equipamento

Nos outros países a situação é bem diferente. As exportações dos EUA são limitadas aos tamanhos de chave referidos, mas vendedores noutros países como a Netguard (Israel), a Radguard (Israel), e a Timestep (Canadá), podem oferecer o mesmo poder de chaves de cifragem como nos EUA desde que cumpram as normas de exportação menos restritivas dos seus próprios países.

Os diferentes países estão também sujeitos a regulamentos que restringem não só a exportação da cifragem, mas também a importação e a sua utilização (ver Tabela 10.2 no anexo A.4). No caso de Portugal, a importação e utilização da cifragem é permitida sem restrições.

Existem dois tratados internacionais que regulam a cifragem. Um, o tratado de Wassenaar que bane a exportação de equipamento de alta tecnologia (incluindo a cifragem) a países sob sanções das Nações Unidas. O outro, da União Europeia, obriga à livre circulação de produtos criptográficos na União Europeia e obriga os governos a evitarem as suas restrições normais no caso das assinaturas digitais que utilizam cifragem RSA de 128 bits ou mais.

3.3 Comunicações Seguras sobre Redes Inseguras

A cifragem permite criar comunicações seguras sobre canais inseguros. Cifrar o tráfego de rede providencia a privacidade e a autenticação. A privacidade é óbvia, se os dados são cifrados pelo emissor, enviados sobre uma rede insegura, e depois decifrados pelo receptor, os dados são mantidos privados de alguém que escute a rede insegura. A autenticação é menos óbvia, mas bastante útil. Basicamente, se o receptor conseguir decifrar os dados com sucesso, sabe que os dados devem ter vindo realmente do emissor (não de alguém que finge ser o emissor), porque os dados estão correctamente cifrados, e somente o emissor o pode ter efectuado. Assume-se, obviamente, que as chaves necessárias para ser mantido segredo foram mantidas secretas. Alguém que saiba as chaves pode violar quer a privacidade quer a autenticação [ChapZw95].

Após a caracterização da criptografia feita na secção anterior, serão caracterizados nesta secção sistemas de segurança de rede que fazendo uso da criptografia providenciam

mecanismos de obtenção de comunicações seguras.

Será caracterizado o Sistema de Autenticação Kerberos que para além da sua utilidade promissora – está bastante divulgado e está a ser considerado para adopção como *standard* na Internet – é um excelente *case study*, já que é uma implementação concreta, e tem sido sujeito a muitos estudos e a uma experiência considerável [ChesBe94]. As secções seguintes apresentam alguns sistemas de segurança em utilização actual e discutem os seus compromissos.

3.3.1 O Sistema de Autenticação Kerberos

O Sistema de Autenticação Kerberos [Bryant88; KohlNe93; MilOut87; SteOut88] foi projectado no MIT como parte do projecto Athena. Serve dois propósitos: autenticação e distribuição de chaves, providencia aos *hosts* – ou mais precisamente a vários serviços dos *hosts* – credenciais não forjáveis para identificar os utilizadores individuais [ChesBe94].

Cada utilizador e cada serviço partilha uma chave secreta com o centro de distribuição de chaves Kerberos; essas chaves actuam como chaves mestras para a distribuição de chaves de sessão. O protocolo básico é derivado de um originalmente proposto por Needham e Schroeder [NeeSch78; NeeSch87; DenSac81].

O Kerberos define a evidência de uma identidade principal. Um principal é geralmente um utilizador ou um serviço particular de uma máquina, que consiste do tuplo triplo: (*nome primário*, *instância*, *domínio*). Se o principal for um utilizador, o nome primário é o identificador de *login*, e a instância ou é nula ou representa atributos particulares do utilizador (ex.: *root*). Para um serviço, o nome do serviço é usado como o nome primário e o nome da máquina é utilizado como a instância (ex.: rlogin.myhost). O domínio é utilizado para distinguir entre diferentes domínios de autenticação; não havendo assim necessidade de uma base de dados Kerberos gigante e universalmente confiável, que sirva uma organização inteira.

Todas as mensagens Kerberos contêm um *checksum*, o qual é examinado após a decifração; se o *checksum* for válido, o receptor pode assumir que foi utilizada a chave correcta para a cifragem.

Os principais Kerberos podem obter "senhas" para serviços de um servidor especial conhecido como Servidor de Senhas de Garantia (TGS – Ticket-Granting Server). Uma senha contém informação vária identificando o principal, cifrada na chave privada do serviço (notação da Tabela 3.6):

$$K_s[T_{c,s}] = K_s[s, c, addr, timestamp, lifetime, K_{c,s}]. \quad (1)$$

C	Principal cliente
S	Principal servidor
Tgs	Servidor de senhas de garantia
K_x	Chave privada de "x"
$K_{c,s}$	Chave de sessão para "c" e "s"
$K_x[info]$	"*info*" cifrado na chave K_x
$K_s[T_{c,s}]$	Certificado cifrado para "c" usar "s"
$K_{c,s}[A_c]$	Autenticador cifrado para "c" usar "s"
Addr	Endereço IP do Cliente

Tabela 3.6 – Notação do Kerberos

Como só o Kerberos e o serviço partilham a chave privada K_s, conclui-se que a senha é autêntica. A senha contém uma nova chave de sessão privada, $K_{c,s}$, conhecida pelo cliente; esta chave pode ser usada para cifrar transações durante as sessões na vigência da senha. Para a defesa contra ataques de repetição, todos as senhas são acompanhadas por um *autenticador*:

$$K_{c,s}[A_c] = K_{c,s}[c, addr, timestamp]. \quad (2)$$

que consiste numa pequena *string* cifrada com a chave de sessão e contendo uma marca temporal (*timestamp*); se a hora não coincidir com a hora corrente dentro dos limites predeterminados, assume-se que o pedido é fraudulento.

A chave $K_{c,s}$ pode ser utilizada para cifrar e/ou autenticar mensagens para o servidor. Isto é utilizado para implementar funções tais como cópias de ficheiros cifradas, sessões de *login* remotas, etc. Alternativamente, $K_{c,s}$ pode ser utilizada para computação do MAC para mensagens que precisam de ser autenticadas, mas não necessariamente secretas.

Para serviços onde os clientes precisem de autenticação bidireccional, o servidor pode responder com

$$K_{c,s}[\text{timestamp} + 1]. \quad (3)$$

Isto demonstra que o servidor tem possibilidade de ler a *timestamp* do autenticador, e por isso conhece $K_{c,s}$, que por sua vez só está disponível na senha, a qual é cifrada com a chave privada do servidor.

As senhas são obtidas do TGS pelo envio de um pedido

$$s, K_{tgs}[T_{c,tgs}], K_{c,tgs}[A_c]. \quad (4)$$

Por outras palavras, é utilizado um par senha/autenticador; a senha é designada por senha de garantia. O TGS responde com uma senha para o servidor s e uma cópia de $K_{c,s}$, ambos cifrados com uma chave privada partilhada pelo TGS e pelo principal:

$$K_{c,tgs}[K_s[T_{c,s}], K_{c,s}]. \quad (5)$$

A chave de sessão $K_{c,s}$ é uma nova chave aleatória. A chave $K_{c,tgs}$ e a senha de garantia são obtidas no início da sessão. O cliente envia uma mensagem ao Kerberos com o nome do principal, e o Kerberos responde com

$$K_c[K_{c,tgs}, K_{tgs}[T_{c,tgs}]]. \quad (6)$$

A chave do cliente K_c é derivada por meio de uma transformação não invertível da *password* digitada pelo utilizador. Desta forma, todos os privilégios dependem em última análise desta chave. De notar que os servidores devem possuir as suas próprias chaves privadas, de forma a decifrarem as senhas. Estas chaves são guardadas numa localização segura no servidor.

As senhas e as chaves de cliente associadas são escondidas na máquina cliente. Os autenticadores são recalculados e recifrados de cada vez que a senha é usada. Cada senha tem um máximo tempo de validade; após esse período, o cliente tem de obter uma nova senha do TGS.



Figura 3.5 – O Fluxo de Dados no Kerberos

A ligação a servidores fora de um domínio é algo mais complexo. Uma senha normal não é suficiente, pois o KDC local não tem uma chave secreta para cada um da totalidade dos servidores remotos. Em vez disso, é utilizado um mecanismo de autenticação entre domínios. O KDC local deve partilhar uma chave secreta com o servidor KDC remoto; esta chave é utilizada para assinar o pedido local, confirmando ao KDC remoto que o KDC local confia na informação de autenticação. O KDC remoto utiliza esta informação para construir uma senha para utilização por um dos seus servidores.

Esta abordagem, apesar de ser melhor do que assumir um KDC gigante, ainda sofre de problemas de dimensão. Cada domínio precisa de uma chave individual para cada um dos outros domínios com os quais os seus utilizadores necessitam de se ligar. Para resolver este problema, as novas versões do Kerberos utilizam uma estrutura de autenticação hierárquica. Um KDC departamental pode comunicar com um KDC organizacional, e este por sua vez com o regional. Só os KDC's regionais precisam de partilhar chaves mutuamente numa malha completa.

3.3.1.1 Limitações

Apesar de o Kerberos ser extremamente útil, e ser bastante melhor que os métodos de autenticação baseados em endereços que a maioria dos protocolos mais antigos utilizam, tem algumas fraquezas e limitações [BelMer91].

Em primeiro lugar e mais importante, o Kerberos foi projectado para autenticação utilizador a *host*, não *host* a *host*. Isto é razoável num ambiente como o do Projecto Athena de estações de trabalho anónimas e sem dados, e servidores de ficheiros *email* de grande capacidade; mas pouco indicado para ambientes *host* a *host* onde os *hosts* têm as suas identidades próprias e precisam de aceder a recursos do seu próprio interesse. Para implementar isto no modelo Kerberos é necessário que os *hosts* mantenham as suas próprias chaves secretas, mas a maioria dos computadores são notoriamente pobres na manutenção de chaves secretas a longo prazo [DifHel76; MorrTh79].

Os autenticadores são também um ponto fraco. A não ser que o *host* mantenha informação de todos os autenticadores activos previamente utilizados, um intruso pode repeti-los dentro dos comparativamente largos limites temporais. Se o atacante conseguir levar o *host* a acreditar numa hora incorrecta, o *host* pode providenciar autenticadores pós-datados para um posterior abuso.

Os problemas mais sérios, no entanto, têm a ver com o modo como é obtido a senha inicial. O pedido inicial de uma senha de garantia não contém informação de autenticação, tal como uma cópia cifrada do nome do utilizador. A mensagem de resposta é bastante susceptível para um ataque de *cracking* de *passwords*; um atacante algures na Internet pode construir uma colecção de senhas de garantia cifradas e assaltá-la *off-line*. As últimas versões do protocolo Kerberos têm mecanismos para fazer face a este problema. Abordagens mais sofisticadas detalhadas em [LomOut94] ou [BelMer92] poderão ser usadas.

Existe também um problema relacionado com o *login*: como é que o utilizador sabe que o próprio comando *login* não foi já corrompido? A forma de enfrentar estes ataques é utilizar dispositivos de autenticação de desafio/resposta, mas estes não são suportados pelo protocolo. Existem algumas provisões para extensibilidade; no entanto, como ainda não existem *standards* para essas extensões, não existe interfuncionamento.

3.3.2 Cifragem ao Nível da Ligação

A cifragem ao nível da ligação lógica é a mais transparente forma de protecção criptográfica. De facto, é frequentemente implementada por dispositivos externos; mesmo os *device drivers*, e obviamente as aplicações, não sabem da sua existência [ChesBe94].

Como o seu nome indica, esta forma de cifragem protege uma ligação individual. Isto é uma vantagem mas também uma fraqueza. É uma vantagem, porque (para certos tipos de

hardware) todo o pacote é cifrado, incluindo os endereços fonte e destino. Isto protege contra análises de tráfego e em determinadas circunstâncias – por exemplo, a cifragem de uma ligação ponto a ponto – mesmo a existência do tráfego pode ser disfarçada.

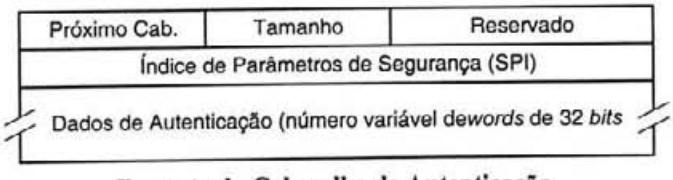
No entanto, a cifragem ao nível da ligação sofre de uma fraqueza séria: protege somente uma ligação de cada vez. As mensagens ficam expostas quando passam para outras ligações. Mesmo se estas também estiverem cifradas, as mensagens permanecem vulneráveis enquanto estiverem no nó de comutação. Dependendo de onde estiver o atacante, isto pode ser um sério revés.

A cifragem ao nível da ligação é o método de eleição para protecção estrita de tráfego local (ex.: num segmento partilhado) ou para a protecção de um pequeno número de linhas bastante vulneráveis. Circuitos de satélite são um exemplo típico, assim como circuitos de cabos transoceânicos.

3.3.3 Cifragem ao Nível de Rede e de Transporte

A cifragem ao nível de rede e de transporte são, em certo sentido, as formas mais úteis de proteger as comunicações. Tal como os cifradores ao nível de aplicação, permitem aos sistemas efectuarem conversação sobre as *internets* inseguras; tal como os cifradores ao nível da ligação, são transparentes à maioria das aplicações. No entanto, a implementação é difícil porque a função de cifragem afecta todas as comunicações entre muitos sistemas diferentes [ChesBe94], daí a necessidade de *standards*.

As versões *standard* desses protocolos disponíveis para a família de protocolos TCP/IP são definidos nos RFCs 1825 a 1829 [Atk95R25; Atk95R26; Atk95R27; Met95R28; Atk95R29]. A arquitectura de segurança proposta (IPSec) por [Atk95R25] combina técnicas criptográficas bem definidas para providenciar serviços de segurança robustos na camada IP [Doty95b].



Formato do Cabeçalho de Autenticação

Cab. IP v4	Cab. de Autent.	Protocolo Nível Sup. (TCP, UDP)

Cabeçalho de Autenticação para o IP v4

Cab. IP v6	*Hop-by-hop*/Encam.	Cab. de Autent.	Outros Cab.	Protocolo Nível Sup. (TCP, UDP)

Cabeçalho de Autenticação para o IP v6

Figura 3.6 – O Cabeçalho de Autenticação

O Cabeçalho de Autenticação – Authentication Header (AH), fornece uma forte autenticação e encontra-se no datagrama depois do cabeçalho IP e antes do protocolo do nível

superior (por exemplo o TCP). A Figura 3.6 mostra o formato do Cabeçalho de Autenticação e a sua relação com os datagramas IP v4 e IP v6.

O Próximo Cabeçalho especifica o cabeçalho do protocolo do nível superior (por exemplo TCP ou UDP) para o IP v4, ou o próximo cabeçalho que será contido no datagrama IP v6. O tamanho do AH (em *words* de 32 *bits*) deve ser especificado pois diferentes técnicas de autenticação produzem dados de tamanhos diferentes. O Índice de Parâmetros de Segurança – Security Parameters Index (SPI) é um valor pseudo aleatório utilizado como referência para qualquer informação de segurança tal como chaves de cifragem.

A Carga de Encapsulamento de Segurança – Encapsulating Security Payload (ESP) começou por providenciar somente os serviços de cifragem, providenciando actualmente quer a cifragem quer a autenticação. Os serviços ESP podem ser providenciados de duas formas, o mais simples é o modo de transporte – simples cifragem do cabeçalho de transporte mais os dados da aplicação. Mais complicado é o modo túnel – a capacidade de cifragem e encapsulamento do datagrama IP inteiro.

A Figura 3.7 mostra o formato do ESP e a sua relação com os cabeçalhos IP. Como pode ver-se na figura o AH pode ser utilizado em conjunção com o ESP para providenciar autenticação.

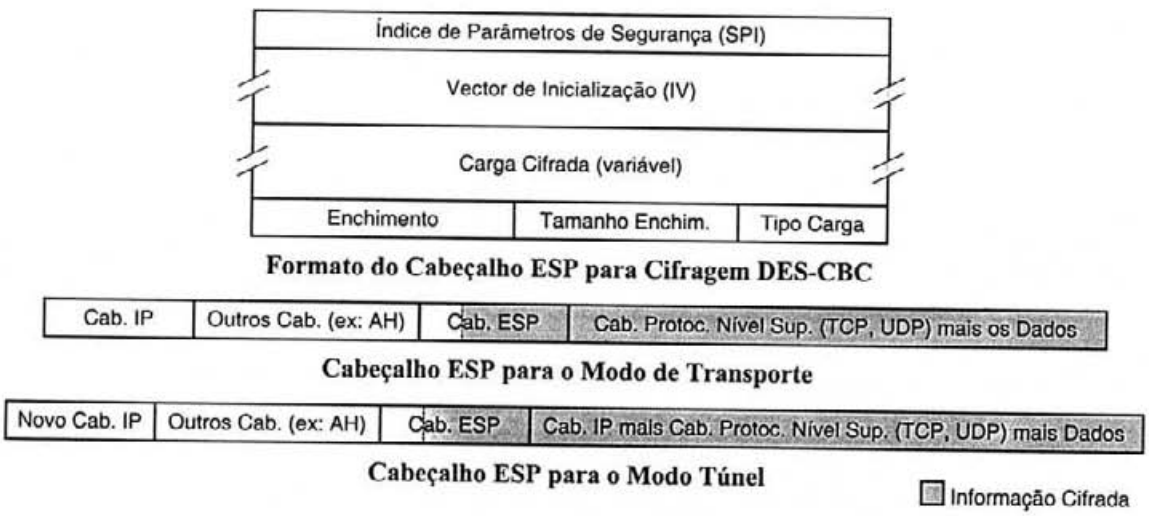


Figura 3.7 – O Cabeçalho ESP para os Modos de Transporte e de Túnel

O cabeçalho ESP é dependente da cifra particular usada para cifrar os dados. Um SPI (idêntico em forma e função ao do AH) é seguido por um Vector de Inicialização, dados cifrados e o enchimento. O carregamento cifrado é a porção de transporte do datagrama (por exemplo o cabeçalho TCP e os dados de aplicação) se for utilizado o modo de transporte, ou o datagrama IP inteiro (cabeçalho IP, cabeçalho de transporte, dados de aplicação), se for utilizado o modo túnel. De notar que toda a informação exceptuando o SPI é cifrada.

O modo de transporte assegura privacidade para qualquer aplicação que o invocar,

evitando a necessidade de implementar serviços de segurança redundantes para cada protocolo de aplicação.

O modo túnel tem duas vantagens sobre o modo de transporte. A primeira, é que torna a análise de tráfego quase impossível, se implementado num *firewall* ou *gateway* (será utilizado o endereço externo no cabeçalho IP e os endereços internos são cifrados). A segunda, as capacidades de *tunnelling* formam a base das Redes Privadas Virtuais (capítulo 5), que permitem a conectividade remota mas evitando os problemas de segurança da Internet.

3.3.4 A Cifragem ao Nível da Aplicação

Efectuar a cifragem ao nível da aplicação é a opção mais intrusiva. É também a mais flexível, porque o âmbito e força da protecção podem ser moldados para responder às necessidades específicas da aplicação. Opções de cifragem e de autenticação foram definidas para um número de aplicações de alto risco, mas até à data nenhuma foi largamente distribuída [ChesBe94].

3.3.4.1 O Protocolo *Telnet*

A área mais crítica, no sentido de um problema persistente, é o protocolo *telnet*. O risco não é tanto comprometer todo o conteúdo de uma sessão de *login* remota, apesar de poder ser suficientemente sensível, mas a forte necessidade de prevenir que as *passwords* sejam enviadas na Internet a descoberto. Naturalmente, isto pode ser prevenido pela cifragem das sessões *telnet*, mas não constitui a solução ideal por várias razões. A primeira, e a mais óbvia, a cifragem é por vezes excessiva. Em muitos casos é somente a *password* que necessita de protecção, não a conexão inteira. Não há necessidade de provocar o *overhead* durante o resto do tempo. A segunda, é que a cifragem requer a distribuição de chaves, que por sua vez requer frequentemente um processo de autenticação.

A terceira razão é porque a autenticação é necessária no *telnet* em qualquer caso. Isto providenciará conexões pré-autenticadas, na linha do *rlogin*, mas construído em bases mais flexíveis. Quer dizer, é desejável permitir aos utilizadores efectuar conexões a outras máquinas na rede sem a necessidade de repetir as *passwords*.

3.3.4.2 Autenticar o SNMP

O SNMP (Simple Network Management Protocol [CasOut90] é utilizado para controlar os *routers*, *bridges*, e outros elementos de rede. A necessidade de autenticação dos pedidos do SNMP é óbvia. O que não é tão óbvio é que alguns pacotes devem ser também cifrados, se não por outras razões, para proteger os pedidos de alteração de chaves para o protocolo de autenticação.

O primeiro problema, a autenticação, é resolvido pelo uso das funções de *hash* segu-

ras. Ambas as partes partilham uma cadeia de 16 *bytes*, a qual é adicionada no início do pedido SNMP; o MD5 é utilizado para gerar o código de *hash* de 16 *bytes*.

O secretismo é providenciado pela utilização do DES no modo CBC[5]. É efectuada uma função de *hash* na mensagem para verificação de integridade.

Para prevenir ataques de repetição, as mensagens SNMP seguras incluem uma marca temporal. As mensagens que se verifique serem antigas são descartadas.

3.3.4.3 Correio Electrónico Seguro

Com o cada vez maior recurso ao correio electrónico para os mais variados propósitos, aumenta a necessidade de serviços de autenticação e confidencialidade. Dois esquemas salientam-se como os de mais provável utilização generalizada nos próximos anos: o PGP (Pretty Good Privacy) e o Privacy-Enhanced Mail (PEM) [Stall95].

Ambos utilizam a mesma estrutura geral – as mensagens são cifradas com um sistema criptográfico simétrico, com as chaves distribuídas por um sistema criptográfico de chave pública – mas diferem significativamente no detalhe [ChesBe94].

A segurança do correio é criticamente dependente da segurança do sistema operativo subjacente. Não valerá a pena utilizar o mais forte criptosistema possível se um intruso conseguir armadilhar o servidor de correio ou escute as *passwords* enviadas na rede local. Para uma segurança máxima, qualquer sistema de correio seguro deve ser executado numa máquina de utilizador único que esteja protegida fisicamente e electronicamente.

PEM

O PEM [Linn93a; Kent93; Balens93; Kalisk93] suporta cifragem múltipla, *hash*, e algoritmos de chave pública. Nesta altura o DES é o único algoritmo de cifragem para o corpo da mensagem, embora esteja a ser desenvolvida uma versão triple-DES. O RSA é utilizado para cifrar as chaves DES e os certificados. A mensagem é sujeita a uma função de *hash* com o MD5 antes da assinatura; os certificados são sujeitos a uma função de *hash* com o MD2.

A estrutura de certificação é constituída por um grupo de ramificações. Cada raiz, conhecida por Top-Level Certifying Authority, deve efectuar certificação cruzada com todas as outras raízes. São impostos requisitos elaborados de confiabilidade e inspecção aos níveis mais baixos das autoridades de certificação, para prevenir possíveis compromissos.

Não estão ainda definidos protocolos de servidores de chaves. Os *mail agents* do utili-

[5] CBC (Cipher Block Chaining Mode) – é o mais importante modo de operação da cifragem convencional.

zador devem guardar os certificados recebidos. É definida uma forma especial de mensagem de correio, o Certificate Revocation List (CRL); essas mensagens contêm listas de certificados que já não são válidos. Qualquer autoridade que emita certificados pode gerar mensagens para cancelar os certificados emitidos.

O PEM suporta um número de diferentes modos de operação. Em primeiro lugar, o correio cifrado e assinado. Suporta também mensagens autenticadas não codificadas.

PGP

Desde o seu início, o PGP [Zimmer92] experimentou um aumento explosivo e é actualmente largamente utilizado. Está mundialmente disponível sem custos e em versões comerciais numa variedade de plataformas incluindo o DOS/Windows, UNIX, Macintosh e muitas outras. Está baseado em algoritmos comprovados e considerados extremamente seguros; especificamente, inclui o RSA para cifragem de chave pública, o IDEA para a cifragem convencional, e o MD5 para codificação de *hash*. Tem uma larga gama de aplicação desde esquemas de cifragem de ficheiros e mensagens até ao estabelecimento de comunicações seguras sobre a Internet e outras redes [Stall95].

O aspecto mais peculiar do PGP é a sua estrutura de certificação, em vez de hierárquica, o PGP suporta um "grafo de confiança" mais ou menos arbitrário. Os utilizados recebem pacotes com chaves assinadas de outros utilizadores; quando adicionam esses pacotes aos seus próprios conjuntos de chaves activas, indicam o grau de confiança que têm no assinante, e assim a presumível validade das chaves. A não ser que se tenha uma verificação independente de parte da cadeia de assinaturas, não se ganha grande segurança numa sequência longa de assinaturas, pois um atacante pode forjar uma cadeia de assinaturas [ChesBe94].

A utilização do PGP tem gerado alguma controvérsia devido à utilização não autorizada do RSA. Alguns fornecedores negociaram já acordos de licenciamento com os vários detentores de patentes, e oferecem versões comerciais para várias plataformas. O MIT disponibilizou uma versão do PGP baseada no pacote RSAREF; a utilização desta versão é legal para propósitos não comerciais.

3.3.4.4 Um API de Serviço de Segurança

O GSS-API (Generic Security Service Application Program Interface) [Linn93b; Wray93], é um interface comum para uma variedade de serviços de segurança. O objectivo é fornecer aos programadores um único conjunto de chamadas de função para utilização, e também definir um conjunto comum de primitivas que possa ser usado para a segurança das aplicações. Desta forma, as aplicações individuais não têm que implementar distribuição de chaves ou algoritmos de cifragem; basta utilizarem o mesmo mecanismo normalizado.

O GSS-API foi projectado para sistemas com base em credenciais, tal como o Kerbe-

ros ou o DASS [Kaufm93]. Não define como as credenciais devem ser obtidos, deixando isso para o sistema de autenticação subjacente.

Naturalmente, o GSS-API não garante interfuncionamento a não ser que os dois sistemas saibam respeitar as credenciais mútuas. Nesse sentido, é um tipo de *standard* pouco comum na comunidade TCP/IP: especifica o comportamento do *host*, em vez de definir o que é enviado na comunicação.

3.3.5 Desafios e Soluções para a Segurança

Existem muitos desafios na construção de um serviço completo de Intranet que forneça comunicações seguras e colaboração. O TCP/IP resolve muitos problemas de forma eficiente, no entanto, não foi projectado para oferecer serviços de comunicação seguros. Por isso, são necessárias tecnologias e políticas adicionais para resolver os problemas típicos de segurança [Hunt98].

Existem algumas tecnologias disponíveis que fornecem a base para uma grande variedade de serviços de segurança, incluindo a cifragem, a verificação de integridade de mensagens, a autenticação, e as assinaturas digitais.

Uma variedade de técnicas de cifragem e autenticação, com base nos serviços básicos da Internet, têm surgido nos últimos tempos para fornecer uma operação segura nas redes internas. Dessas técnicas as mais importantes incluem o IPSec e o Point-to-Point Tunnelling Protocol (PPTP) (descritos no capítulo 5 sobre Redes Privadas Virtuais), o *tunnelling* cifrado, o Secure Sockets Layer (SSL), o Secure Electronic Transactions (SET), e o Secure Multipart Internet Mail Encoding (S/MIME), as quais podem ser vistas na pilha protocolar na Figura 3.8. As secções seguintes fornecem uma breve descrição de como podem ser obtidas transacções seguras na Internet com a utilização destas novas técnicas.

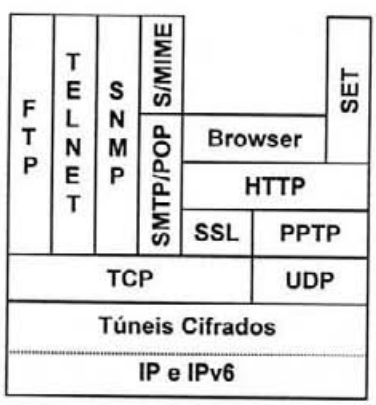


Figura 3.8 – Arquitectura Protocolar para Serviços de Transacções Seguras [Hunt98]

3.3.5.1 O Tunnelling Cifrado

A técnica do *tunnelling* cifrado tem por base o modo túnel do IPSec (secção 3.3.3) e

serve de base para as Redes Privadas Virtuais descritas no capítulo 5.

O *tunnelling* é uma técnica de encapsulamento de dados para transmissões transparentes numa rede de interligação cujos *hosts* não reconheçam os o(s) protocolo(s) encapsulados. Por exemplo, o tráfego IPX pode ser encapsulado no TCP/IP para o seu transporte numa rede que não reconheça o protocolo IPX.

Os túneis cifrados usam pacotes IP *standards*, cifram-nos e encapsulam-nos em pacotes TCP/IP para o seu transporte. As aplicações com base no IP origem e destino operam de forma normal, mas os dados entre os dois servidores do túnel são cifrados.

Frequentemente os utilizadores iniciam as ligações à Internet através dum *firewall*, mas no sentido inverso ocorrem normalmente restrições consideráveis. Quando é configurada uma Intranet utilizando túneis cifrados, o *firewall* pode ser configurado para permitir a passagem, para a rede confiável, de dados cifrados e autenticados provenientes de túneis da Internet dos clientes. Os dados *tunnelled* permanecem cifrados passado o *firewall* e dentro da rede confiável até chegarem ao servidor do túnel.

Alguns fabricantes fornecem túneis cifrados *host-a-host* ou LAN-a-LAN, enquanto outros permitem que o túnel termine no posto de trabalho. Por exemplo, pode utilizar-se *software* cliente de *tunnelling* no posto de trabalho ou, em contraste, o servidor de *tunnelling* pode servir simultaneamente múltiplos túneis clientes. As chaves de autenticação são guardadas no posto de trabalho em forma cifrada e são acessíveis pela utilização de um PIN (número de identificação pessoal). São utilizadas chaves diferentes para cada túnel configurado entre o túnel cliente e servidor.

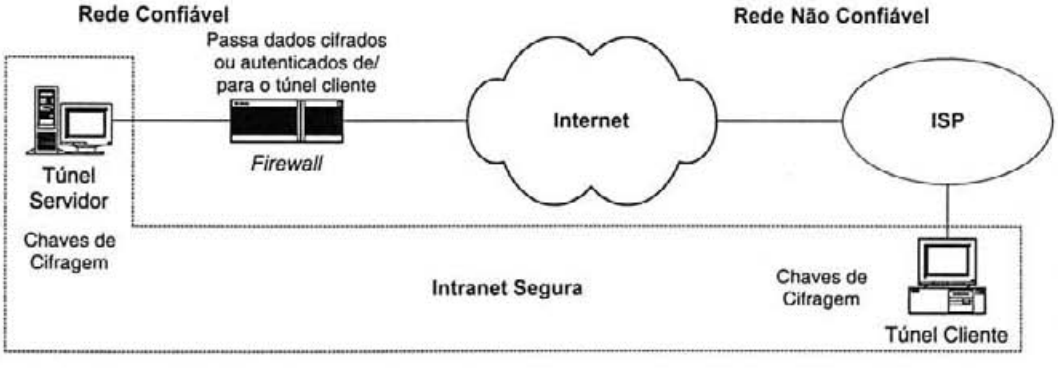


Figura 3.9 – Arquitectura de Intranet com Túneis Cifrados [Hunt98]

Os utilizadores móveis, com acesso no escritório ou em casa, podem ligar-se a um fornecedor de serviços Internet (ISP) e estabelecer um túnel seguro com a rede confiável. A autorização é baseada num PIN ou sistema de desafio/resposta (e não no endereço IP), seguido por um par de chaves de cifragem utilizada para autenticar o PC com o servidor de *tunnelling* confiável. Isto permite ao utilizador deslocar-se na rede, sem estar constrangido a um determinado endereço de *hardware* específico. Logo que seja estabelecido um túnel cifrado

com a rede confiável, o posto de trabalho pode comunicar livremente nessa rede ou pode ser restringido por políticas de segurança específicas.

Não é requerido nenhum *software* especial dentro da rede confiável já que é utilizado o encaminhamento normal logo que os pacotes deixem o túnel e sejam decifrados. Nem é necessário nenhum *software* especial no fornecedor de serviços da Internet apesar de todo o tráfego que passa por ele ser cifrado, como se pode ver na Figura 3.9.

A Operação dos Túneis Cifrados

Quando um túnel cliente (um grupo ou pessoal) deseja iniciar uma ligação com um servidor Internet Group Tunnel, é enviado um pedido de ligação ao longo da rede. O pedido pode ser endereçado a um *firewall*, o qual transmite a ligação ao servidor Internet Group Tunnel apropriado. A mensagem de pedido de ligação contém um identificador que é cifrado pelo cliente com a chave pública do servidor, e que é depois decifrado pelo servidor com a sua chave privada.

A base de dados do servidor contém uma lista de clientes autorizados a estabelecer túneis. Se o pedido tiver de ser garantido, o servidor de *tunnelling* envia uma resposta cifrada utilizando a chave pública do cliente, a qual é depois decifrada pelo cliente utilizando a sua chave privada. Depois desta sequência de autenticação, as duas partes trocam porções de uma chave de sessão, as quais são combinadas para formar uma chave de sessão secreta. As chaves de sessão são alteradas periodicamente para melhorar a segurança. Em cada túnel é utilizado um par de chaves pública/privada RSA para a autenticação e, após o estabelecimento do túnel, são trocadas chaves de sessão secretas RC4 para a cifragem do dados.

O cliente do túnel tem dois endereços, um apropriado para a rede à qual está directamente ligado, e o outro válido para a rede à qual está ligado pelo túnel. Isto evita a existência de uma *back door* para outros postos de trabalho na rede do fornecedor de serviços da Internet poderem estabelecer uma ligação com a Intranet. As tabelas de encaminhamento são configuradas de forma que todas as comunicações destinadas aos *hosts* da rede *tunnelled* são enviadas através do túnel e as comunicações destinadas aos outros *hosts* são enviadas normalmente para a rede ligada directamente.

A maioria dos *firewalls* podem ser configurados para permitir a passagem de tráfego cifrado de um túnel para uma rede interna e para o servidor de *tunnelling*. Normalmente, transmite-se o tráfego endereçado a uma porta específica do *firewall* para uma porta específica no servidor de *tunnelling*, desta forma escondendo o endereço do servidor de *tunnelling* assim como efectuando o *log* de todas as tentativas de ligações quer ao *firewall* quer ao servidor de *tunnelling*.

3.3.5.2 O Secure Sockets Layer (SSL)

Os conceitos de comércio electrónico e de transacções seguras só são válidos com um mecanismo adequado para assegurar a confidencialidade da transacção. A sua implementação da segurança na rede é alcançada no *standard* Secure Sockets Layer ou SSL.

O Secure Sockets Layer providencia um método para adicionar segurança à aplicações existentes ao incorporar a tecnologia RSA Data Security. O SSL é independente do protocolo de aplicação e fornece [Hunt98]:

- Cifragem (que cria um canal seguro).
- Autenticação.
- Utiliza certificados X.509 e assinaturas digitais para verificar a identidade das partes.
- Integridade das mensagens (que assegura que as mensagens não podem ser alteradas no percurso).

A cifragem RSA utiliza pelo SSL e pela cifragem de *tunnelling* é similar apesar de a cifragem ser executada em camadas diferentes da pilha protocolar. O SSL cifra os dados na camada de aplicação enquanto os túneis estabelecem uma ligação para todas as ligações lógicas entre as duas redes. As aplicações que precisem de cifrar uma sessão específica, tal como uma sessão de *web browser* ou Telnet, deve ser modificada para permitir o pedido de uma ligação cifrada. Com o *tunnelling*, as aplicações não precisam de ser modificadas pois todo o tráfego entre redes *tunnelled* é cifrado.

Uma vantagem do protocolo SSL é ser independente da aplicação. Os protocolos de aplicação de alto nível tal como o HTTP, FTP e Telnet colocam-se transparentemente no topo da camada SSL que pode negociar um algoritmo de cifragem e chaves de sessão, bem como autenticar um servidor antes que o protocolo de aplicação transmita ou receba dados. Todos os dados transmitidos do protocolo de aplicação são cifrados, assegurando assim a privacidade.

O SSL providencia um *handshake* de segurança que é utilizado para iniciar a conexão TCP/IP. Este *handshake* resulta no acordo entre o cliente e o servidor no nível de segurança que utilizarão, e satisfaz quaisquer requisitos de autenticação para a ligação. Depois disto, a única tarefa do SSL é cifrar e decifrar os dados utilizados da aplicação. Isto significa que toda a informação do pedido e resposta HTTP é completamente cifrada, incluindo a URL pedida, qualquer conteúdo de formulário submetido (incluindo números de cartão de crédito), qualquer informação de autorização de acesso HTTP (*usernames* e *passwords*), e todos os dados respondidos do servidor para o cliente.

O SSL fornece três serviços de segurança fundamentais (Tabela 3.7), todos eles utilizando cifragem de chave pública.

Serviço de Segurança	Tecnologia Associada	Protecção Contra
Privacidade da mensagem	Cifragem	Escuta de mensagens
Integridade da mensagem	Códigos de autenticação de mensagens (funções de *hash*)	Vândalos
Autenticação mútua	Certificados X.509	Impostores

Tabela 3.7 – Serviços de Segurança do SSL [Hunt98]

A privacidade da mensagem é obtida pela combinação de técnicas de cifragem de chave pública e de chave simétrica. Basicamente, todo o tráfego entre um cliente e um servidor é cifrado utilizando uma chave e um algoritmo de cifragem que é decidido pelo cliente e pelo servidor durante a negociação inicial da ligação [GarINET].

A integridade da mensagem certifica que o tráfego entre dois *hosts* utilizando o SSL não é modificado em trânsito. É utiliza uma função de *hashing*, decidida entre os *hosts*, a qual gera uma mensagem resumo (*digest*) dos dados a serem enviados. A mensagem resumo é adicionada aos dados a serem transmitidos e na recepção é recalculada e comparada com a original. Uma igualdade exacta indica que a mensagem não foi modificada em trânsito.

Na autenticação mútua são utilizados certificados X.509, que são trocados pelas partes no inicio da ligação. A autenticação é geralmente avançada pelo servidor, que comprova a sua identidade ao cliente, mas pode também ser pedida pelo servidor, se for necessário que o cliente prove a sua identidade.

As versões mais recentes do SSL têm algumas melhorias protocolares que incluem [Hunt98]:

- Menor número de mensagens de *handshake* e mais rápidas.
- Suporte para mais algoritmos de troca de chaves e de cifragem (particularmente, Diffie-Hellman e Fortezza).
- Suporte para *tokens* de *hardware* na forma de cartões Fortezza. Este constitui o primeiro passo para o suporte geral a *smart cards* com capacidades criptográficas.
- Melhoria no protocolo de pedido de certificados do cliente, permitindo ao servidor especificar uma lista de autoridades de certificação para enviar os certificados do cliente, evitando que o utilizador tenha de escolher um certificado para cada ligação.

O SSL foi submetido ao grupo de trabalho de segurança do W3C[6] para ser considerado um *standard* de segurança para os *browsers* WWW e servidores da Internet.

Surgiu entretanto um novo método de acesso URL, o HTTPS, para ligação a servido-

[6] O World Wide Web Consortium (W3C) é uma organização de colaboração internacional entre organizações de pesquisa, cujo objectivo é guiar a evolução da World Wide Web.

res HTTP utilizando o SSL. O HTTPS constitui a camada SSL por baixo do HTTP (Figura 3.8). O SSL/HTTP e o HTTP são protocolos diferentes e residem tipicamente em portas diferentes (443 e 80, respectivamente). O mesmo sistema servidor pode executar simultaneamente servidores HTTP seguros e inseguros.

Outra variação do mesmo esquema é o S/HTTP – uma variante do HTTP melhorada a nível de segurança. O SSL/HTTP e o S/HTTP têm motivações diferentes, enquanto o SSL constitui a camada de segurança por baixo dos protocolos de aplicação, o S/HTTP adiciona segurança baseada nas mensagens ao HTTP (projectado numa abordagem ao PEM e MIME). O SSL e o S/HTTP não são mutuamente exclusivos, ao contrário, podem coexistir de forma complementar colocando a camada S/HTTP no topo do SSL.

O Nível de Segurança do SSL

As versões internacionais (fora dos EUA) do SSL utilizam chaves de 40 *bits* para a cifragem de chave pública RSA. A utilização de métodos de "força bruta" permite "quebrar" a chave. O número de combinações que será necessário examinar é 2^{40}, que consiste em 1,099,511,627,776 chaves diferentes. No entanto, sem um número bastante significativo de recursos computacionais, uma técnica de "força bruta" não será viável. Um dos primeiros exemplos de "quebra" de uma chave de 40 *bits* utilizou uma rede de 120 computadores, bem como um número de computadores paralelos, levando cerca de 8 dias para pesquisar todo o espaço de chaves. Provavelmente, não valerá a pena gastar este tempo e esforço por um número de cartão de crédito [GarINET].

Para versões do protocolo usadas nos EUA, são utilizadas chaves de 128 *bits*. Para uma chave deste tamanho é realisticamente impossível "quebrar" por métodos de "força bruta", utilizando um computador com a tecnologia computacional actual. No entanto a utilização de mais vastos recursos poderá levar à quebra da chave como é demonstrado na secção 0 (O Poder do RSA).

3.3.5.3 A Identificação e Autenticação Fortezza

Fortezza é uma placa PCMCIA tipo II e é um componente chave do programa para o sistema de segurança do departamento de defesa da National Security Agency. É uma solução de segurança integrada que responde às necessidades de organizações civis e militares que requeiram a protecção de informação sensível mas não classificada [Hunt98].

A placa Fortezza combina uma técnica de autenticação de utilizador, que obsta às tentativas de *sniffing* de *passwords*, com a força do Digital Signature Algorithm, proposto pelo NIST, e assegura que a identificação remota não fica sujeita a escuta. A cifragem e a gestão de chaves são efectuadas de forma automática, não requerendo nunca a intervenção do utilizador.

3.3.5.4 O Secure Electronic Transactions (SET)

Em resposta à procura cada vez maior de comércio electrónico, as organizações MasterCard, Visa e um pequeno grupo de parceiros de tecnologia de chaves desenvolveram conjuntamente o protocolo Secure Electronic Transactions (SET) como um método para tornar seguras as transacções de cartões de crédito sobre redes não confiáveis. O SET define o protocolo de pagamento electrónico e o processo de gestão do certificado.

A especificação SET permite satisfazer os seguintes requisitos:

- Confidencialidade da informação – assegura que a informação do detentor do cartão só é acessível ao destinatário. O SET utiliza a cifragem de mensagens para assegurar a confidencialidade.
- Integridade dos dados – garante que o conteúdo da mensagem não é alterado durante a transmissão. São utilizadas assinaturas digitais para assegurar a integridade dos dados.
- Autenticação da conta do detentor do cartão – verifica que o detentor do cartão é o utilizador legítimo da conta bancária. O SET assegura a autenticação da conta pela utilização de assinaturas digitais e certificados do detentor do cartão.
- Autenticação do comerciante – confirma ao detentor do cartão que o vendedor pode aceitar pagamentos de cartões bancários. O SET utiliza assinaturas digitais e certificados do comerciante para assegurar esta autenticação.
- Interoperabilidade – assegura que qualquer detentor dum cartão com *software* compatível pode comunicar com qualquer comerciante que execute *software* compatível. O SET providencia protocolos específicos e formatos de mensagens que asseguram a interoperabilidade numa variedade de plataformas de *hardware* e *software*.

As principais entidades participantes no sistema de pagamento definido pelo SET interagem directa ou indirectamente da forma descrita na Figura 3.10, e são as seguintes:

- Detentor do cartão – no comércio electrónico, os consumidores e as organizações interagem com os comerciantes a partir de computadores. Um detentor de cartão utiliza um cartão de pagamento emitido por uma instituição bancária emissora. O SET assegura que nas interacções do detentor do cartão com o comerciante, a informação do cartão e da conta permanece confidencial [SET97].
- Banco emissor – é a instituição financeira que estabelece uma conta e emite o cartão de pagamento para o detentor do cartão. O banco emissor garante o pagamento para as transacções autorizadas com o cartão de pagamento.
- Comerciante – com o SET, o comerciante pode oferecer transacções electrónicas seguras. Um comerciante que aceite cartões de pagamento deve ter um relacionamento com um banco aceitante.
- Banco Aceitante – é a instituição financeira que estabelece uma conta com o comerciante e processa as autorizações de pagamento por cartão e os pagamentos.

- *Gateway* de Pagamentos – dispositivo operado por um banco aceitante, ou uma terceira parte, que processa as mensagens de pagamento dos comerciantes, incluindo as instruções de pagamento dos detentores de cartões.
- Autoridade de Certificação (CA) – entidade confiável que autentica as partes envolvidas na transação. A Autoridade de Certificação fornece certificados às entidades (com o nome e a chave pública) e que são assinados digitalmente pela CA.

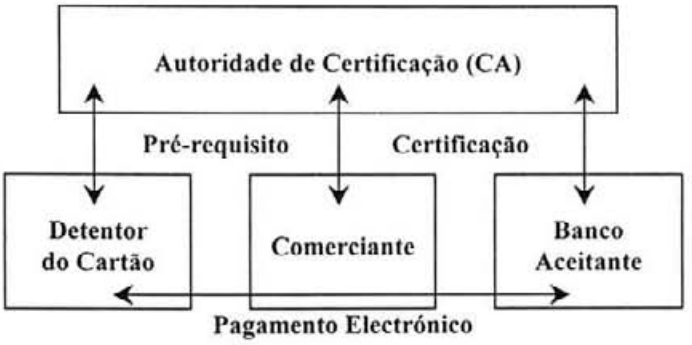


Figura 3.10 – Interacções do Sistema de Pagamento SET [Hunt98]

O SET define um conjunto de protocolos de transacções que utilizam princípios criptográficos para conduzir de forma segura o comércio electrónico. As várias transacções no processo do comércio electrónico estão esquematicamente definidas na Figura 3.10:

- Registo do detentor do cartão.
- Registo do comerciante.
- Pedido de compra.
- Autorização de pagamento.
- Captura do pagamento.

3.3.5.5 O Secure Multipart Internet Mail Encoding (S/MIME)

O S/MIME é uma especificação para correio electrónico seguro e foi projectado para adicionar segurança às mensagens de e-*mail* em formato MIME. Os serviços de segurança oferecidos são a autenticação (utilizando assinaturas digitais) e a privacidade (utilizando a cifragem de chave pública RSA). Mais importante ainda, foi projectado para ser interoperável, de forma que quaisquer duas aplicações que implementem o S/MIME podem comunicar de forma segura [Hunt98].

O S/MIME utiliza uma abordagem criptográfica híbrida para fornecer a segurança – muitas vezes referida por envelope digital. A maioria do processo de cifragem da mensagem é feita com uma cifra simétrica, e é utilizado um algoritmo de chave pública para a troca de chaves e para a assinatura digital. O S/MIME utiliza certificados digitais com base no X.509 e recomenda três algoritmos de cifragem simétrica: o DES, Triple-DES, e o RC2. O tamanho ajustável do tamanho da chave no algoritmo RC2 torna-o especialmente útil em aplicações a utilizar fora dos EUA.

Quer o S/MIME, o PGP e o PEM (ver a secção 3.3.4.3) especificam métodos de correio electrónico seguro. Todos oferecem serviços de privacidade e de autenticação.

O PGP pode ser visto como uma especificação e uma aplicação. Depende dos utilizadores para a troca de chaves e para o estabelecimento da confiança mútua. Este método informal funciona bem em para pequenos grupos de trabalho, mas pode tornar-se ingovernável para grande número de utilizadores. O S/MIME, por outro lado, utiliza hierarquias onde são formalizados os papéis do utilizador e do certificador. Isto significa que o S/MIME é mais seguro e mais escalonável do que as implementações do PGP e, para além disso, pode ser bem integrado em muitas aplicações de e-*mail*.

O *standard* PEM especifica um formato de mensagem e uma estrutura hierárquica. O formato da mensagem é baseado em texto de 7 *bits*, enquanto o S/MIME foi projectado para funcionar com as ligações binárias MIME bem como com texto. Os princípios das hierarquias são também mais flexíveis com o S/MIME, permitindo uma fácil configuração para pequenos grupos que não precisem de fazer parte de uma hierarquia geral, e também uma forma simples de integrar grupos numa hierarquia que melhor sirva as suas necessidades.

3.4 *Firewalls*

Um *firewall* é um dispositivo que arbitra o acesso entre redes, permitindo alguns tipos de tráfego e bloqueando outros, com base nas regras da política de segurança da organização. Essas regras definem essencialmente que endereços, aplicações, e utilizadores serão considerados confiáveis. Dados provenientes dessas origens poderão passar o *firewall* e todos os outros dados serão bloqueados [Doty95a].

O *firewall* é um sistema eficiente de segurança de rede. Situa-se, na maioria das vezes, no ponto onde a rede interna protegida se liga à Internet. Todo o tráfego proveniente da Internet ou com origem na rede interna passa através do *firewall* [ChapZw95].

Do ponto de vista lógico, o *firewall* é um separador, restritor, e analisador. A implementação física do *firewall* varia de *site* para *site*. Mais frequentemente, o *firewall* é um conjunto de componentes de *hardware* – um *router*, um *host*, ou uma combinação de *routers*, computadores, e subredes com o *software* apropriado.

3.4.1 Vantagens e Desvantagens dos *Firewalls*

Os *firewalls* podem fazer muito pela segurança de um *site*. Algumas das suas vantagens vão mesmo para além da segurança. Fazendo passar todo o tráfego por um único ponto, fornece a possibilidade de concentrar as medidas de segurança nesse ponto e aumentar assim a segurança de rede. Permite também reforçar a política de segurança do *site*, ao autorizar somente a passagem dos serviços aprovados e segundo as regras definidas. Ao poder separar

secções de rede, o *firewall* limita as consequências que um problema de segurança poderia trazer para a totalidade da rede. Como todo o tráfego passa pelo *firewall*, este pode efectuar o *log* eficiente da actividade entre a rede protegida e a rede externa.

Os *firewalls* oferecem excelente protecção contra ameaças, mas não são uma solução de segurança completa. Algumas ameaças estão fora do controlo do *firewall*. É necessário encontrar outras formas de protecção contra essas ameaças incorporando segurança física, segurança do *host*, e educação dos utilizadores no plano global de segurança.

Se o atacante estiver já dentro da rede protegida, o *firewall* não poderá fazer virtualmente nada. Os utilizadores do lado de dentro podem furtar dados, danificar *hardware* e *software*, e modificar programas subtilmente sem sequer chegar perto do *firewall*. Ameaças internas requerem medidas de segurança internas.

O *firewall* pode controlar efectivamente o tráfego que passa por ele; no entanto nada pode fazer acerca do tráfego que não passa por ele, por exemplo um acesso *dial-in* a um sistema interno para lá do *firewall*.

Um *firewall* é projectado para proteger contra ameaças conhecidas. Periodicamente são descobertas novas formas de ataque, utilizando serviços anteriormente confiáveis, ou utilizando ataques que simplesmente não ocorreram anteriormente.

Os *firewalls* não defendem a rede contra viroses. Apesar de muitos *firewalls* analisarem o tráfego recebido para determinar se pode passar para a rede interna, a análise é baseada nos endereços origem e destino e em números de portas, não nos detalhes dos dados. Mesmo com *software* de filtragem de pacotes ou *proxy* sofisticados, a protecção contra vírus no *firewall* é muito difícil, pois existem demasiados tipos de viroses e demasiadas formas de um vírus se esconder nos dados. A forma mais prática de resolver os problemas dos vírus é através de *software* de protecção antivírus baseado no *host*, e de educação dos utilizadores.

Apesar das limitações e desvantagens, o *firewall* é a forma mais efectiva de ligar uma rede à Internet e proteger essa rede. No capítulo 1 será descrita em pormenor a arquitectura dos *firewalls* bem como as várias variantes arquitectónicas na construção de *firewalls*.

4. Arquitecturas de *Firewall*

Uma base para definir a arquitectura de um *firewall* é o modelo OSI (Figura 4.1), o qual fornece uma imagem mais clara que o modelo TCP/IP [Hunt98].



Figura 4.1 – A Arquitectura do *Firewall* e a sua Relação com o Modelo OSI [Hunt98]

Do ponto de vista arquitectónico podem definir-se 3 tipos de *firewalls*:

- *Firewalls* ao nível do pacote – operam nas camadas de rede (exemplo: IP[1]) e de transporte. São frequentemente referidos por *screening routers* ou filtros de pacotes e bloqueiam a transmissão de certas classes de tráfego.
- *Firewalls* ao nível da aplicação – operam nas camadas de sessão, apresentação e aplicação. São normalmente implementados utilizando *hosts* dedicados executando *software* especializado e podem também ser referidos por *hosts* bastião[2] ou servidores *proxy*[3], normalmente executados sobre UNIX ou Windows NT. Podem também providenciar serviços de *relay* (transmissão) para compensar os efeitos do filtro.
- *Firewalls* Stateful Inspection – tecnologia recente que incorpora o estado da comunicação e da aplicação, e informação de contexto que é guardada e actualizada dinamicamente. Isto fornece dados cumulativos com os quais as tentativas de comunicação subsequentes podem ser avaliadas.

---

[1] Em geral, salvo afirmação em contrário, discute-se no contexto TCP/IP.

[2] *Host* Bastião – sistema computacional que deve ser bastante seguro devido à sua vulnerabilidade a ataques, normalmente porque está exposto à Internet e é um ponto principal de contacto para os utilizadores das redes internas [ChapZw95].

[3] Servidor *Proxy* – programa que comunica com servidores externos em proveito dos clientes internos. Os clientes *proxy* comunicam com os servidores *proxy*, os quais transmitem os pedidos aprovados dos clientes para os servidores externos, e transmitem as respostas de novo aos clientes [ChapZw95].

Um *firewall*, em geral, é constituído por vários componentes diferentes (Figura 4.2). Os "filtros" bloqueiam a transmissão de certas classes de tráfego. Uma *gateway* é uma máquina ou conjunto de máquinas que providenciam serviços de *relay* para compensar os efeitos do filtro. A rede ocupada pelo *gateway* é muitas vezes designada por "zona desmilitarizada" ou DMZ (*De-Militarised Zone*). Em geral, o filtro exterior pode ser utilizado para proteger o *gateway* de ataques, enquanto o filtro interno é utilizado para precaver as consequências de um *gateway* comprometido. Um ou outro dos filtros, ou ambos, podem proteger a rede interna de assaltos. Uma máquina *gateway* exposta é também designada por *host* bastião [ChesBe94].

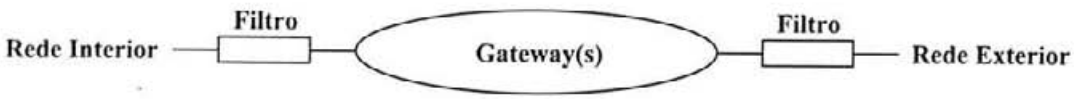


Figura 4.2 – Esquema de um *Firewall*

Nas próximas secções descrevem-se as abordagens mais importantes utilizadas para a construção de *firewalls* – sistemas de filtragem de pacotes (ao nível do pacote) e sistemas *proxy* (ao nível da aplicação), este último englobando as abordagens de *gateways* de aplicação e *gateways* de circuito.

4.1 Sistemas de Filtragem de Pacotes

Os sistemas de filtragem de pacotes encaminham pacotes entre *hosts* internos e externos de uma rede, mas efectuam-no selectivamente. Permitem a passagem ou bloqueiam determinados tipos de pacotes de uma forma que reflicta a política de segurança do *site*, como é mostrado na Figura 4.3. O tipo de *router* utilizado num *firewall* de filtragem de pacotes é designado por *router* de filtragem (*screening router*).

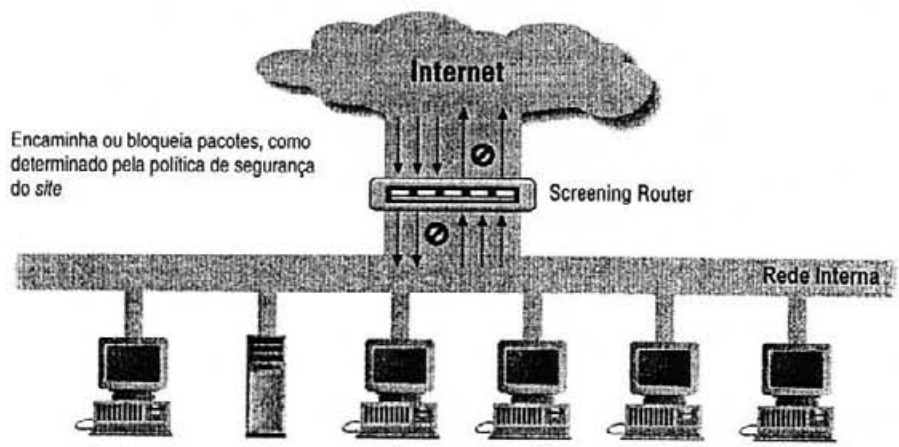


Figura 4.3 – A Utilização de um *Screening Router* na Filtragem de Pacotes [ChapZw95]

Cada pacote tem um cabeçalho próprio e encapsula cabeçalhos de protocolos de mais alto nível, que contêm determinada informação. A principal informação é a seguinte:

- Endereço origem IP
- Endereço destino IP
- Protocolo (quer o pacote seja TCP, UDP ou ICMP)
- Porta origem TCP ou UDP
- Porta destino TCP ou UDP
- Tipo de mensagem ICMP

Para além disso, o *router* sabe informação acerca do pacote que não está reflectida nos cabeçalhos, tais como:

- A interface ao qual chega o pacote
- A interface de saída do pacote

O facto de servidores de serviços de Internet residirem em determinados números de portas permite ao *router* bloquear ou permitir determinados tipos de conexões simplesmente pela especificação do número de porta apropriado no conjunto de regras definidas para a filtragem de pacotes.

Exemplos de programação de um *router* de filtragem para encaminhar pacotes selectivamente de ou para o *site* podem ser: bloquear todas as comunicações provenientes de sistemas exteriores à rede interna, com excepção de comunicações SMTP (*e-mail*) recebidas, ou permitir os serviços de *e-mail* e FTP mas bloquear todos os serviços perigosos.

Um *router* vulgar analisa o endereço de destino de cada pacote e selecciona o melhor caminho para enviar esse pacote para o seu destino. A decisão de como lidar com o pacote é baseada somente no seu destino. Se o *router* souber como enviar o pacote para o destino envia-o, se não souber devolve o pacote à origem, via uma mensagem ICMP "destino inatingível". Por outro lado, um *router* de filtragem examina os pacotes mais pormenorizadamente; para além de determinar se pode ou não encaminhar o pacote para o seu destino, também determina se deve ou não enviar o pacote, de acordo com a política de segurança do *site*.

O facto de só ser possível ter um *router* de filtragem entre uma rede interna e a Internet, como se vê na Figura 4.3, coloca uma enorme responsabilidade no *router* de filtragem. Não só realiza todo o encaminhamento e decisões de encaminhamento, mas constitui o único sistema de protecção; se o seu sistema de segurança falhar, ou cair em consequência de um ataque, a rede interna fica exposta.

Para além disso, um *router* de filtragem não pode modificar os serviços. Pode permitir ou negar um serviço, mas não pode proteger operações individuais internas de um serviço. Se um determinado serviço tiver operações inseguras, ou se o serviço é normalmente providenciado por um servidor inseguro, a filtragem de pacotes isolada não o pode proteger.

4.1.1 Vantagens da Filtragem de Pacotes

Uma das maiores vantagens da filtragem de pacotes é que um único *router* de filtragem de pacotes, estrategicamente colocado, pode ajudar a proteger uma rede inteira. Se for somente um *router* a ligar o *site* à Internet, ganha-se uma enorme vantagem na segurança de rede ao efectuar a filtragem de pacotes nesse *router*, independentemente da dimensão do *site*.

Ao contrário dos sistemas proxy, que serão descritos na secção 4.2, a filtragem de pacotes não requer qualquer *software* ou configuração das máquinas clientes, nem requer qualquer treino ou procedimentos por parte dos utilizadores. A filtragem de pacotes é "transparente" ao funcionamento normal da rede, quer isto dizer que este processo pode ser efectuado sem a cooperação, e muitas das vezes sem o conhecimento, dos utilizadores.

As capacidades de filtragem de pacotes estão disponíveis em muitos produtos de encaminhamento de *hardware* e de *software*, quer comerciais quer disponíveis livremente na Internet. Muitos dos *routers* comerciais, tais como os da Cisco Systems ou da Livingston Enterprises, incluem capacidades de filtragem de pacotes. Também existem muitos pacotes de *software* com essas capacidades.

4.1.2 Desvantagens da Filtragem de Pacotes

Apesar da larga disponibilidade da filtragem de pacotes em *hardware* e *software* diverso, as capacidades de filtragem de pacotes de muitos desses produtos partilham, em maior ou menor grau, limitações comuns:

- As regras de filtragem são por vezes difíceis de configurar;
- Uma vez configuradas, estas regras tendem a ser difíceis de testar;
- As capacidades de filtragem de pacotes de muitos dos produtos são incompletas, tornando a implementação de alguns tipos de filtros difíceis ou impossíveis;
- Como em muitas outras situações, os sistemas de filtragem de pacotes podem ter erros de implementação, os quais são mais problemáticos que os dos sistemas *proxy*. Normalmente um *proxy* que falhe simplesmente deixa de passar os dados, enquanto que um sistema de filtragem de pacotes que falhe pode permitir a passagem de pacotes que devia ter negado.

Mesmo com implementações perfeitas de filtragem de pacotes, alguns protocolos não são apropriados para a obtenção de segurança por filtragem de pacotes. Esses protocolos incluem os comandos "r" Berkeley e protocolos baseados no RPC como o NFS e NIS/YP.

Algumas políticas não podem ser implementadas pelos *routers* normais de filtragem de pacotes, já que a informação que o *router* de filtragem de pacotes tem disponível não o permite. Por exemplo, os pacotes referem de que *host* provêm, mas normalmente não de que utilizador; desta forma não é possível implementar restrições por utilizadores. De igual forma,

os pacotes referem a que porta se destinam, mas não a que aplicação; a implementação de restrições sobre os protocolos de alto nível é feita por número de porta, esperando-se que mais nada passe na porta associada a esse protocolo. Utilizadores mal intencionados da rede interna podem facilmente subverter este tipo de controlo.

4.1.3 O Processo de Filtragem de Pacotes

Para perceber a filtragem de pacotes, é necessário perceber os pacotes e como eles são tratados em cada camada da pilha protocolar do TCP/IP:

- Camada de aplicação (ex.: FTP, Telnet, HTTP)
- Camada de transporte (ex.: TCP ou UDP)
- Camada *internet* (IP)
- Camada de acesso à rede (ex.: Ethernet, FDDI, ATM)

Em cada camada, um pacote é constituído por duas partes: o cabeçalho e o corpo do pacote. O cabeçalho contém informação protocolar relevante para essa camada, enquanto o corpo do pacote contém os dados dessa camada. Cada camada trata a informação que obtém da camada superior como dados, e aplica o seu próprio cabeçalho a esses dados. Este processo de preservação dos dados enquanto se adiciona um cabeçalho é conhecido por encapsulamento.

No outro extremo da ligação, este processo é invertido. À medida que os dados são passados de uma camada para a camada superior, cada cabeçalho é retirado pela respectiva camada.

No processo de filtragem de pacotes, a informação mais importante são os cabeçalhos das várias camadas. Considerando um exemplo de um pacote TCP/IP numa rede Ethernet, serão descritos, nas secções seguintes, os diferentes tipos de pacotes e os respectivos cabeçalhos que os *routers* de filtragem de pacotes examinarão.

4.1.3.1 Protocolos Abaixo do IP

No exemplo de um "pacote" TCP/IP numa rede Ethernet, o cabeçalho da camada Ethernet, basicamente, dá-nos a seguinte informação:

- O tipo de pacote – neste exemplo é um pacote IP em oposição a AppleTalk, Novell, ou outro.
- O endereço Ethernet da máquina que coloca o pacote no segmento de rede Ethernet particular – a máquina fonte original, se ligada ao mesmo segmento; de contrário, o último *router* no caminho desde a máquina fonte até ao ponto actual.
- O endereço Ethernet destino do pacote no segmento de rede Ethernet particular – a máquina destino, se esta estiver ligada ao mesmo segmento; de contrário, o próximo

router no caminho até à máquina destino.

É teoricamente possível filtrar informação abaixo do nível IP – no exemplo, o endereço Ethernet. No entanto, muito raramente isso é útil porque em muitos casos todos os pacotes que provêm do exterior têm o mesmo endereço de hardware (o endereço do *router* que efectua a ligação à Internet). Pata além disso, muitos *routers* têm múltiplas conexões com diferentes protocolos de baixo nível.

Como resultado, a filtragem em protocolos de baixo nível requer a configuração de várias interfaces com diferentes tipos de regras para os diferentes protocolos de baixo nível. Não é possível definir uma regra que se aplique a todas as interfaces num *router* que tenha, por exemplo, duas ligações Ethernet e uma FDDI, porque os cabeçalhos dos pacotes Ethernet e FDDI, apesar de semelhantes, não são iguais. Na prática, o IP é o protocolo de nível mais baixo no qual é efectuado filtragem de pacotes.

4.1.3.2 O Protocolo IP

Do ponto de vista da filtragem de pacotes, o cabeçalho IP contém quatro componentes de informação interessantes:

- O endereço IP fonte.
- O endereço IP de destino.
- O tipo de protocolo transportado – identifica o corpo IP como um pacote TCP, UDP, ICMP ou outro tipo de pacote.
- O campo de opções IP – normalmente vazio, mas onde são especificadas opções como o IP *source route* e as opções de segurança IP, se utilizadas para um determinado pacote.

A opção IP mais comum com que um *firewall* é confrontado é o IP *source route*. O *source routing* permite que a fonte de um pacote especifique o caminho que o pacote deve tomar até ao seu destino, em vez de permitir que cada *router* do percurso utiliza as suas tabelas de *routing* para decidir o encaminhamento do pacote. Em teoria, a opção do *source route* é útil para resolver situações de *routers* com tabelas de *routing* danificadas ou incorrectas. No entanto na prática, o *source routing* é frequentemente utilizado somente por atacantes que tentam circunscrever medidas de segurança ao provocar que os pacotes sigam caminhos inesperados.

Muitos sistemas de filtragem de pacotes têm a abordagem de descartar qualquer pacote que tenha qualquer opção IP activada, sem sequer analisar qual é a opção ou o que significa. Em geral, este alternativa parece funcionar bem, sem causar quaisquer problemas em especial.

Outra consideração ao nível do IP na filtragem de pacotes é a fragmentação. Uma das

características do IP é a possibilidade de dividir um pacote grande, que de outro modo não poderia atravessar alguma subrede devido a limitações de tamanho, em pacotes mais pequenos, designados fragmentos. Os fragmentos são depois reorganizados no pacote completo pela máquina destino.

Do ponto de vista da filtragem de pacotes, o problema com a fragmentação é que somente o primeiro fragmento contém a informação do cabeçalho dos protocolos de alto nível, tais como o TCP, que o sistema de filtragem de pacotes precisa para decidir a permissão ou não da totalidade do pacote. A abordagem usual na fragmentação é permitir a passagem de qualquer fragmento subsequente ao primeiro, e efectuar a filtragem somente no primeiro fragmento do pacote. Isto é seguro porque, se o sistema de filtragem de pacotes decidir descartar o primeiro segmento, o sistema de destino não será capaz de reorganizar os segmentos restantes no pacote original e o pacote parcial não será aceite.

O facto de o *host* de destino guardar temporariamente os fragmentos em memória, à espera do fragmento em falta, torna possível que atacantes usem pacotes fragmentados num ataque de negação de serviço. Quando o *host* de destino desiste de reorganizar o pacote, envia uma mensagem ICMP "expirou o tempo de reorganização do pacote" ao *host* origem, o que informa o atacante da existência do *host*, e porque é que a conexão não teve sucesso. A única coisa a fazer contra este ataque é filtrar as mensagens ICMP para o exterior.

Os fragmentos para o exterior podem conter dados que não se deseja divulgar. Se esta situação ocorrer por acidente, não constituirá propriamente um problema, mas se alguém do interior intencionalmente utilizar a fragmentação para transmitir dados, então existem utilizadores hostis no interior do *firewall*, e nenhum *firewall* consegue lidar com sucesso com este problema.

A única situação na qual é necessário ter preocupações sobre os fragmentos para o exterior é a situação na qual se permite a entrada de um pedido mas se bloqueia a saída da resposta. Nesta situação os fragmentos da resposta subsequentes ao primeiro sairão, e o atacante tem razões para os esperar e analisar. A resolução deste problema está no cuidado da filtragem de pedidos para o exterior e não confiar na filtragem das respostas.

4.1.3.3 O Protocolo TCP

No exemplo de um pacote TCP, do ponto de vista da filtragem de pacotes, o cabeçalho TCP contém três componentes de informação importantes:

- A porta TCP de origem – um número de dois *bytes*, que especifica de que processo cliente ou servidor provém o pacote na máquina de origem.
- A porta TCP de destino – com informação semelhante à porta TCP de origem.
- O campo de *flag* TCP.

O campo de *flag* TCP contém um *bit* com interesse para a filtragem de pacotes: o *bit* ACK. Ao examinar este *bit*, um *router* de filtragem de pacotes pode determinar quando um determinado pacote é o primeiro pacote que inicia uma conexão TCP (se o *bit* ACK não estiver activado) ou é um pacote subsequente (se o *bit* ACK estiver activado). O *bit* ACK faz parte do mecanismo TCP que garante a entrega dos dados.

O TCP é o protocolo mais frequentemente utilizado nos serviços da Internet, providenciando conexões confiáveis e bidireccionais entre dois pontos. O TCP é fiável pelo facto de oferecer três garantias à camada de aplicação: o destino receberá todos os dados da aplicação, pela ordem em que foram enviados, e sem duplicados. Estas garantias implicam que os dois lados da conexão têm de trocar informação de *startup* antes que possam trocar dados e devem manter informação do estado da conexão.

Para se bloquear uma conexão TCP é suficiente bloquear o primeiro pacote da conexão. Sem este primeiro pacote e, mais importante, a informação de *startup* da conexão que ele contém, quaisquer pacotes adicionais nessa conexão não serão reorganizados pelo receptor, e a conexão nunca terá lugar.

Reconhecer os pacotes de início de conexão permite impor uma política que permita aos clientes internos ligar-se aos servidores externos, mas evita que os clientes externos se liguem aos servidores internos. Isto é implementado permitindo pacotes TCP de início de conexão (sem o *bit* ACK activo) somente no sentido para o exterior e não para o interior. Os atacantes não conseguem subverter esta abordagem simplesmente activando o *bit* ACK nos pacotes de início de conexão, porque é a ausência do *bit* ACK que identifica esses pacotes como pacotes de início de conexão.

As implementações de filtragem de pacotes variam na forma como tratam e deixam tratar o *bit* ACK. Algumas implementações fornecem acesso directo ao *bit* ACK, por exemplo, deixando incluir "ack" como uma palavra chave nas regras de filtragem de pacotes. Outras implementações fornecem acesso indirecto ao *bit* ACK, por exemplo, palavras chave que examinam este *bit*. Finalmente, algumas implementações simplesmente não permitem examinar o *bit* ACK.

4.1.3.4 O Protocolo UDP

O UDP é uma alternativa ao TCP de baixo *overhead*, pois não oferece nenhuma das garantias de confiança do TCP. Cada pacote UDP é independente, isto é os pacotes não fazem parte de uma "circuito virtual" como no caso do TCP.

Os pacotes UDP são estruturalmente muito similares aos pacotes TCP. O cabeçalho UDP contém os números de porta UDP origem e destino. No entanto, não contém nada parecido com o *bit* ACK. O *router* de filtragem de pacotes não tem possibilidade de determinar, pelo simples exame do cabeçalho de um pacote UDP proveniente do exterior, se esse pacote é

o primeiro pacote de um cliente externo para um servidor interno, ou uma resposta de um servidor externo para um cliente interno.

Algumas implementações de filtragem de pacotes, tal como o Firewall-1 da CheckPoint, o SecureConnect Router da Morning Star, e o KarlBridge/KarlBrouter, têm a capacidade de "lembrar" os pacotes UDP para o exterior que visualizaram. Podem depois permitir somente os pacotes de resposta correspondentes no mecanismo de filtragem. Para ser considerado como resposta, o pacote do exterior tem de ser do *host* e porta para os quais foi enviado o pacote de saída, e tem de ser direccionado para o *host* e porta que enviou o pacote de saída. Esta capacidade é referida por filtragem dinâmica de pacotes, porque o *router* modifica automaticamente as regras de filtragem de forma a acomodar os pacotes de retorno. Estas regras implicam uma limitação no tempo, pois só permitem a resposta dentro de alguns segundos ou minutos.

4.1.3.5 O Protocolo ICMP

O ICMP é utilizado para o estado do IP e mensagens de controlo. São exemplos de mensagens ICMP as mensagens de *echo request* – ex.: uma mensagem de *ping*, *echo response* – resposta a uma *echo request*, *time exceeded* – mensagem de retorno de um *router* quando determina que um pacote parece estar em *looping*, e *redirect* – mensagem que um *router* envia a um *host* informando sobre um caminho mais eficiente a ser utilizado da próxima vez.

Ao contrário do TCP e do UDP, o ICMP não tem portas de origem ou destino, e não serve de base a nenhum outro protocolo de nível superior. Em vez disso, é um conjunto de códigos definidos de tipos de mensagens ICMP; o código particular utilizado dita a interpretação do resto do pacote ICMP.

Muitos sistemas de filtragem de pacotes permitem filtrar pacotes ICMP com base no campo do tipo de mensagem ICMP

4.1.3.6 Protocolos da Camada da Aplicação

Na maioria dos casos, existe um protocolo adicional em cima do protocolo TCP ou UDP, específico à aplicação. Esses protocolos diferem grandemente na sua especificidade, e são em grande número, proporcionalmente ao número de aplicações de rede.

Algumas sistemas de filtragem de pacotes mais recentes fornecem a possibilidade de filtrar com base nos protocolos de camada de aplicação em aplicações particulares bem definidas. Por exemplo, podem reconhecer informações particulares numa transacção FTP de forma a activarem filtros dinâmicos, ou então podem comparar a informação de um pacote com a aplicação para que é suposto dirigir-se, para se ter a certeza que pacotes endereçados para uma porta DNS, por exemplo, são efectivamente pacotes DNS.

4.1.3.7 Protocolos não IP

Outros protocolos do mesmo nível do IP, por exemplo o AppleTalk e o IPX, fornecem tipos de informação semelhantes ao IP, no entanto os cabeçalhos e as operações para estes protocolos, e por isso as suas características de filtragem de pacotes, variam radicalmente. A maioria das implementações suportam somente a filtragem do IP, e simplesmente descartam os pacotes não IP. Alguns sistemas providenciam suporte limitado de filtragem de pacotes para protocolos não IP, sendo este suporte bastante menos flexível e capaz que o dos *routers* de filtragem IP.

Nesta altura, a filtragem de pacotes como ferramenta não é tão popular e tão desenvolvida para os protocolos não IP, presumivelmente porque estes protocolos são raramente utilizados para comunicar no exterior duma organização sobre a Internet.

Na Internet, os protocolos não IP são tratados encapsulando-os nos protocolos IP. Na maioria dos casos, ficar-se-á limitado a permitir ou negar os protocolos encapsulados de forma global; é possível, por exemplo, aceitar todas as mensagens Appletalk-em-UDP, ou rejeitá-las na totalidade. Poucos sistemas que suportam protocolos não IP podem reconhecer essas conexões quando encapsuladas e filtrá-las nos seus diversos campos.

4.2 Sistemas *Proxy*

Serviços *proxy* são aplicações especializadas ou programas servidores que são executados num *firewall host*: um *dual-homed host*[4] com um interface para a rede interna e outro para a rede externa, ou num outro *host* bastião que tenha acesso à Internet e esteja acessível às máquinas internas. Estes programas aceitam os pedidos dos utilizadores para serviços Internet e enviam-nos apropriadamente, de acordo com a política de segurança do *site*, para os servidores reais. Os *proxies* fornecem substituição de ligações e actuam como *gateways* para os serviços. Por esta razão, os *proxies* são por vezes designados por *gateways* ao nível da aplicação[5] [ChapZw95].

Os serviços *proxy* colocam-se, mais ou menos transparentemente, entre o utilizador na rede interna, e um serviço na rede externa ou na Internet. Em vez de comunicarem directamente um com o outro, cada um comunica com o *proxy*, efectuando este todas as comunicações entre os utilizadores e os serviços da Internet.

---

[4] *Dual-homed host* – computador de uso geral que tem pelo menos duas interfaces de rede.

[5] As terminologias de *firewalls* diferem. Alguns autores (essencialmente na literatura mais recente) utilizam o termo serviço *proxy* para englobar toda a abordagem de *proxy*, outros autores referem *gateways* ao nível de aplicação e *gateways* ao nível de circuito. Existem pequenas diferenças entre os significados dos dois termos.

Os serviços *proxy* são efectivos somente quando são utilizados em conjunção com um mecanismo que restringe as comunicações directas entre os *hosts* internos e externos. Esse mecanismo poderá ser um *dual-homed host* ou um sistema de filtragem de pacotes. Se os *hosts* internos puderem comunicar directamente com os *hosts* externos, não há necessidade de os utilizadores usarem os serviços *proxy*.

Para se caracterizar o funcionamento dos serviços *proxy*, considere-se a situação mais simples, onde se adicionam serviços *proxy* a um *dual-homed host*.

Como se pode ver na Figura 4.4, o serviço *proxy* requer dois componentes: um servidor *proxy* e um cliente *proxy*. O servidor *proxy* é executado no *dual-homed host*. Um cliente *proxy* é uma versão especial de um programa cliente normal (ex.: cliente FTP ou WWW) que comunica com o servidor *proxy* em vez de o fazer com o servidor real situado na Internet. O servidor *proxy* avalia os pedidos do cliente *proxy*, e decide quais autorizar e quais negar. Se o pedido for aprovado, o servidor *proxy* contacta o servidor real representando o cliente (daí o termo "*proxy*" – "procuração" em português), e transmite os pedidos do cliente *proxy* para o servidor *proxy* e as resposta do servidor *proxy* para o cliente *proxy*.

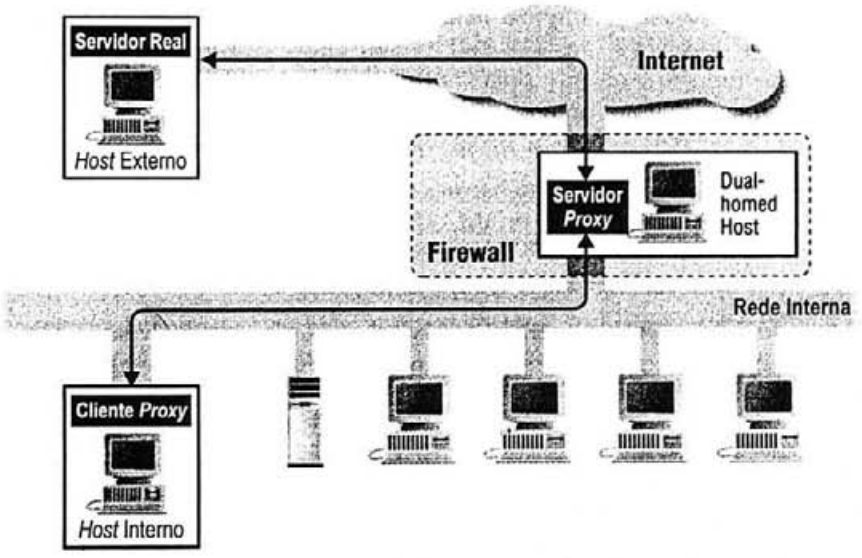


Figura 4.4 – A Utilização de Serviços Proxy com um *Dual-homed Host* [ChapZw95]

Um serviço *proxy* é uma solução de *software*, não uma arquitectura de *firewall* em si, podendo-se utilizar serviços *proxy* em conjunção com várias arquitecturas de *firewall*.

4.2.1 A Necessidade dos *Proxies*

Dual-homed hosts configurados sem *proxies* limitam a acção dos utilizadores porque o seu funcionamento não é transparente aos utilizadores, e aqueles que queiram aceder a serviços de rede não o podem efectuar directamente, têm de se validar no *dual-homed host*. A situação piora em ambientes de múltiplos sistemas operativos onde a interoperabilidade poderá ser reduzida. Para além disso, o *dual-homed host* não providencia segurança adequada, pois

torna-se quase impossível tornar segura uma máquina com muitos utilizadores, particularmente quando esses utilizadores tentam obter acesso à rede externa.

Os sistemas *proxy* evitam a limitação da acção dos utilizadores automatizando a interacção com o *dual-homed host*. O utilizador tem a ilusão de estar a comunicar directamente com o servidor na Internet, com um mínimo de interacção directa com o *dual-homed host*.

Os problemas de insegurança são tratados pelo sistema *proxy* ao evitar os *logins* dos utilizadores no *dual-homed host* e forçando as conexões através de *software* de controlo. Como o *software proxy* funciona sem o requisito de *login* do utilizador, o *host* onde ele é executado é salvaguardado da aleatoriedade de ter múltiplos *logins*. É também impossível para alguém instalar *software* não controlado para acesso à Internet; o *proxy* actua como um ponto de controlo.

4.2.2 Vantagens dos *Proxies*

A transparência é o maior benefício dos serviços *proxy*. Para o utilizador, um servidor *proxy* apresenta a ilusão de que está a comunicar directamente com o servidor real. Para o servidor real, o servidor *proxy* apresenta a ilusão de que está a comunicar directamente com um utilizador do *proxy host*. Desta forma os serviços *proxies* permitem aos utilizadores aceder aos serviços da Internet "directamente".

Como os servidores *proxy* "entendem" o protocolo de base, permitem que o *logging* seja efectuado de forma particularmente eficiente. Por exemplo, ao invés de efectuar o *log* de todos os dados transferidos, um serviço FTP *proxy* faz o *log* somente dos comandos enviados e as respostas recebidas.

4.2.3 Desvantagens dos *Proxies*

Os serviços *proxy* têm vantagem sobre os serviços não *proxies*. Apesar do *software proxy* estar largamente divulgado para os serviços mais comuns, para os serviços mais recentes ou menos divulgados é mais difícil encontrar. Até que novo *software proxy* esteja disponível, um sistema pode ter de ser colocado fora do *firewall*, abrindo assim potenciais brechas de segurança.

Poderão ser necessários servidores *proxy* diferentes para cada serviço, porque o servidor *proxy* precisa de conhecer o protocolo de forma a determinar o que deve permitir ou não permitir passar, e de forma a fazer-se passar por cliente ao servidor real e pelo servidor real ao cliente *proxy*. A instalação e configuração desses vários servidores pode ser trabalhosa.

Em muitos casos, os servidores *proxy* requerem modificações nos clientes e/ou procedimentos, o que tem desvantagens. Devido a estas modificações as aplicações *proxy* podem funcionar menos bem do que as não *proxy*, e tendem a adaptar as especificações dos protoco-

los apesar de alguns clientes e servidores serem menos flexíveis que outros.

O funcionamento do *proxy* baseia-se na possibilidade de colocação do servidor *proxy* entre o cliente e o servidor real, o que requer uma interacção relativamente simples entre os dois. Outros serviços que têm interacções complicadas podem não ser possível de implementar em *proxy*.

Sendo uma solução de segurança, o *proxy* baseia-se na possibilidade de determinar que operações de um protocolo são seguras. Nem todos os protocolos permitem formas fáceis de fazer isso. O sistema de protocolos X Windows, por exemplo, tem um grande número de operações inseguras e torna-se difícil fazê-lo funcionar ao remover essas operações. Um outro exemplo, o HTTP está projectado para operar eficientemente com servidores *proxy*, mas está projectado também para ser facilmente extensível ao passar dados que irão ser executados. É impossível ao servidor *proxy* proteger dos dados; teria de perceber os dados que são passados e determinar a sua perigosidade.

4.2.4 O Funcionamento do *Proxy*

Os detalhes do funcionamento do *proxy* diferem de serviço para serviço. Alguns serviços permitem o *proxy* facilmente ou automaticamente; para esses serviços, configura-se o *proxy* efectuando alterações de configuração aos servidores normais. Para a maioria dos serviços, no entanto, activar o *proxy* requer *software* servidor *proxy* apropriado do lado do servidor, e do lado do cliente é necessária uma das seguintes opções: *software* cliente específico ou procedimentos de utilizador pré-definidos.

Com a primeira abordagem, o *software* tem de saber como contactar o servidor *proxy* em vez do servidor real quando um utilizador efectua um pedido, e como informar o servidor *proxy* a que servidor real se deve ligar.

Existem alguns problemas associados a esta abordagem. Por vezes só existe disponível para certas plataformas *software* cliente apropriado. Mesmo se o *software* estiver disponível para as plataformas necessárias, poderá não ser o *software* preferencial dos utilizadores. Por vezes um determinado *software* que se deseja utilizar não suporta o servidor *proxy* utilizado. Uma excepção a esta regra são os programas cliente de WWW; muitos destes programas suportam *proxies* de vários tipos, pois os seus autores ao reconhecerem os ambientes nos quais eles iriam funcionar, forneceram suporte ao nível de projecto à filosofia *proxy*. Finalmente, a utilização de alterações no cliente *proxy* não torna o processo de *proxy* completamente transparente para os utilizadores, já que estes terão de efectuar configurações extra.

Na utilização da abordagem de procedimentos pré-definidos, os servidores *proxy* estão projectados para funcionar com *software* cliente normalizado, mas obriga a que os utilizadores sigam procedimentos pré-definidos. Com esta abordagem o utilizador utiliza *software* cliente normalizado para comunicar com o servidor *proxy* e informa-o para ligar ao servidor

real, em vez de se ligar directamente ao servidor real. Como poucos protocolos estão desenhados para passarem este tipo de informação, o utilizador precisa não só de saber o nome do servidor *proxy*, mas também que sintaxe especial é utilizada para passar o nome do outro *host*.

Esta abordagem tem alguns problemas pelo facto do seu funcionamento não ser transparente aos utilizadores. A utilização de procedimentos pré-definidos coloca limitações em quais os clientes a utilizar, pois alguns não permitem transmitir o nome do servidor real. O problema principal, no entanto, será conseguir informar os utilizadores de forma eficiente dos procedimentos a seguir para cada protocolo. Em qualquer organização de tamanho considerável, esta abordagem torna-se impraticável.

4.2.5 *Proxies* de Nível de Aplicação *Versus* de Nível de Circuito

Um *proxy* de nível de aplicação conhece a aplicação particular para a qual irá providenciar serviços *proxy*; entende e interpreta os comandos do protocolo de aplicação. A versão extrema de um *proxy* de nível de aplicação é uma aplicação do tipo do Sendmail, que implementa um protocolo de *store-and-forward*.

Um *proxy* de nível de circuito cria um circuito entre o cliente e o servidor sem interpretar o protocolo de aplicação. Uma versão extrema de um *proxy* de nível de circuito é um dos modernos *gateways proxy* híbridos que se parece como um *proxy* para o exterior mas como um *router* de filtragem para o interior.

Em geral, os *proxies* de nível de aplicação utilizam procedimentos modificados, enquanto os *proxies* de nível de circuito utilizam clientes modificados. Isto tem que ver com a praticabilidade do processo *proxy*, pois para efectuar uma conexão *proxy* é necessário saber o destino dessa conexão. Um *gateway* híbrido pode simplesmente interceptar as conexões, mas um *host proxy* só pode receber conexões que lhe são restritas; tudo o resto tem de informar onde deve ser feita a conexão daí para a frente.

Um *proxy* de nível de aplicação pode obter essa informação no protocolo de aplicação, quer pelas características da sua estrutura, ou pela interpretação dos dados fornecidos pelo utilizador. Como a possibilidade de utilizar clientes não modificados é uma característica útil, os *proxies* de nível de aplicação geralmente são projectados para tirarem vantagens do seu conhecimento do protocolo de aplicação, por isso utilizam procedimentos modificados.

Um *proxy* de nível de circuito não consegue interpretar o protocolo de aplicação e precisa de obter a informação que lhe é fornecida através de outros meios, por exemplo utilizando um cliente modificado que fornece ao servidor o endereço de destino. Como os *proxies* de nível de circuito normalmente não têm possibilidade de utilizar procedimentos modificados, utilizam clientes modificados.

Apesar de não haver nenhum *proxy* de nível de aplicação conhecido que tenha como

base um cliente modificado, existem *proxies* de nível de circuito baseados em procedimentos modificados. O *proxy* Plug-gw do TIS FWTK (Internet Firewall Toolkit) da Trusted Information Systems, por exemplo, utiliza procedimentos modificados (a conexão é feita ao servidor *proxy*, em vez de ao *host* de destino) e é um *proxy* de nível de circuito. Baseia as decisões de destino unicamente no endereço origem, e nas portas de origem e destino da conexão.

A vantagem de um *proxy* de nível de circuito é que providencia serviços para uma grande variedade de diferentes protocolos. A maioria dos *proxies* de nível de circuito são também servidores *proxy* genéricos; podem ser adaptados para utilização com quase todos os protocolos. No entanto, nem todos os protocolos podem ser facilmente tratados por um *proxy* de nível de circuito. Protocolos como o FTP, que comunicam dados transportados do cliente para o servidor, requerem alguma intervenção ao nível protocolar, e desta forma algum conhecimento ao nível da aplicação.

A desvantagem de um servidor *proxy* de nível de circuito é que providencia muito pouco controlo sobre o que passa pelo *proxy*. Tal como um filtro de pacotes, controla as conexões na base da sua origem e destino e não consegue determinar facilmente se os comandos que o atravessam são seguros. Os *proxies* de nível de circuito são facilmente enganados por servidores configurados com números de portas atribuídos a outros servidores.

4.2.6 *Proxies* Genéricos *Versus* Dedicados

A terminologia "nível de aplicação" e "nível de circuito" é frequentemente utilizada, mas também se pode classificar servidores *proxy* em "dedicados" e "genéricos". Um servidor *proxy* dedicado serve um único protocolo; um servidor *proxy* genérico serve múltiplos protocolos.

Na prática, servidores *proxy* dedicados são de nível de aplicação, e servidores *proxy* genéricos são de nível de circuito. Apesar de ser possível produzir um servidor *proxy* de nível de aplicação genérico (que entende uma grande gama de protocolos) ou um servidor *proxy* de nível de circuito dedicado (que fornece somente um serviço, mas não entende o respectivo protocolo), nenhuma destas situações foi considerada na prática.

4.2.7 Servidores *Proxy* Inteligentes

Um servidor *proxy* pode fazer bastante mais do que simplesmente transmitir pedidos. Os *proxies* que o fazem designam-se por servidores *proxy* inteligentes. Por exemplo, alguns servidores *proxy* HTTP efectuam o *cache* de dados, de forma que múltiplos pedidos para os mesmos dados não sejam enviados novamente para a Internet. Os servidores *proxy* (particularmente os de nível de aplicação) podem providenciar um melhor *logging* e controlo de acesso que o obtido através de outros métodos, apesar de poucos dos servidores *proxy* existentes tirarem total partido dessas oportunidades.

À medida que os servidores *proxy* se desenvolvem, as suas capacidades aumentam rapidamente. Começam a competir oferecendo novas capacidades para além da funcionalidade básica. É mais fácil tornar inteligente um servidor *proxy* dedicado, de nível de aplicação; um *proxy* de nível de circuito tem capacidades limitadas.

4.2.8 Segurança de Protocolos

Para alguns serviços, efectuar o *proxy* poderá ser tecnicamente fácil, mas sem significado do ponto de vista da segurança. Se um protocolo for inerentemente inseguro, implementar um serviço *proxy* com base nesse protocolo sem efectuar nenhuma alteração não o tornará mais seguro. Um sistema *proxy* de um *firewall* deve capturar as operações inseguras e pelo menos oferecer ao utilizador a possibilidade de as evitar. Isto seria razoavelmente possível em protocolos inseguros, mas requer um maior conhecimento da aplicação do que seria necessário para um protocolo seguro.

Se for difícil distinguir entre operações seguras e inseguras de um protocolo ou impossível utilizar o serviço se as operações inseguras forem evitadas, efectuar o *proxy* poderá não ser uma solução viável. Nesse caso, poderá não haver uma boa solução, e ficar-se-á reduzido a utilizar um *host* vítima[6]. Há quem considere o HTTP um desses protocolos, porque pode chegar a uma situação de transferência de programas que são executados transparentemente pelo cliente.

4.3 O Stateful Inspection

Stateful Inspection, por vezes também conhecido por filtragem dinâmica de pacotes, é um desenvolvimento recente de alguns fabricantes de *firewalls* e representa uma abordagem alternativa na tecnologia dos *firewalls*.

O Stateful Inspection intercepta os pacotes ao nível de rede e examina esses pacotes com base no estado da comunicação. Isto origina o armazenamento da informação do estado de um ou mais pacotes bem como o *buffering* e a reassemblagem do datagrama antes que uma decisão de acesso possa ser tomada [Hunt98].

A vantagem desta abordagem está na diversidade e capacidade de suportar uma variedade de protocolos e serviços. Por não depender na pilha nativa do *firewall host* para o pro-

---

[6] *Host* vítima – tipo especial de *host* bastião que serve para executar serviços que são difíceis de fornecer de forma segura quer com *proxies* quer com filtragem de pacotes, ou serviços bastante recentes de que não se conhecem as implicações a nível de segurança. É uma máquina sem informação importante, e não tem acesso a máquinas que um intruso possa utilizar. Ao contrário do *host* bastião quase sempre deve permitir aos utilizadores efectuarem o *login* [ChapZw95].

cessamento, e também a sua capacidade de "relembrar" a informação passada relacionada com a sessão, o Stateful Inspection pode aplicar qualquer regra baseada no próprio conteúdo da comunicação. O Stateful Inspection é normalmente implementado com suporte ao conjunto dos protocolos TCP/IP.

No entanto, o Stateful Inspection tem também algumas desvantagens, permite aos clientes externos ligações IP directas para *hosts* internos, e só suporta autenticação do utilizador com recurso a um *proxy* [AvoBla98].

4.3.1 Os Requisitos do Stateful Inspection

O Stateful Inspection fornece um grande nível de segurança ao incorporar o estado derivado da comunicação e da aplicação e informação de contexto que é guardada e actualizada dinamicamente. Isto fornece dados cumulativos com os quais as tentativas de comunicação subsequentes podem ser avaliadas. Fornece conhecimento completo da camada de aplicação sem necessitar de um *proxy* separado para cada serviço a ser seguro.

De forma a tomar decisões de controlo para os serviços baseados no TCP/IP (por exemplo, quando aceitar, rejeitar, autenticar, cifrar e/ou efectuar o *log* de tentativas de comunicação), um *firewall* deve obter, guardar, recuperar e manipular informação derivada de todas as camadas de comunicação e de outras aplicações [CheckP98].

Não é suficiente examinar os pacotes isoladamente. A informação de estado é um factor essencial na tomada das decisões de controlo para novas tentativas de comunicação. Dependendo da tentativa de comunicação, o estado da comunicação (derivada das comunicações passadas) e o estado da aplicação (derivada das outras aplicações) podem ser críticas nas decisões de controlo.

Para assegurar o nível mais alto de segurança, um *firewall* deve ser capaz de aceder, analisar e utilizar a seguinte informação:

- Informação da Comunicação – informação do pacote de todas as sete camadas.
- Estado da Comunicação – o estado derivado das comunicações prévias, por exemplo, o comando de transferência de dados para o exterior de uma sessão FTP pode ser guardado de forma que uma conexão de dados FTP do exterior possa ser verificada.
- Estado da Aplicação – a informação de estado derivada de outras aplicações, por exemplo, a um utilizador previamente autenticado será permitido aceder através do *firewall* somente aos serviços autorizados.
- Manipulação da Informação – a avaliação de expressões versáteis baseadas nos factores anteriores.

4.3.2 A Tecnologia Stateful Inspection

O Stateful Inspection cumpre todos os requisitos de segurança definidos acima. As tecnologias de *firewall* tradicionais, a filtragem de pacotes e os *proxies*, são inadequados em algumas áreas (ver a Tabela 4.1).

Capacidade do *Firewall*	Filtragem de Pacotes	*Proxies*	Stateful Inspection
Informação da Comunicação	Parcial	Parcial	Sim
Estado da Comunicação	Não	Parcial	Sim
Estado da Aplicação	Não	Sim	Sim
Manipulação da Informação	Parcial	Sim	Sim

Tabela 4.1 – Comparação das Arquitecturas de *Firewall* [CheckP98]

O Stateful Inspection ultrapassa as limitações das outras abordagens de *firewall* providenciando o conhecimento completo da camada de aplicação sem quebrar o modelo cliente/servidor. Com o Stateful Inspection, o pacote é interceptado na camada de rede, a informação relacionada com o estado, requerida para a decisão de segurança, é extraída de todas as camadas da aplicação e mantida em tabelas dinâmicas de estado para avaliação das subsequentes tentativas de ligação. Isto fornece uma solução que é bastante segura e permite grande desempenho, escalabilidade, extensibilidade e transparência.

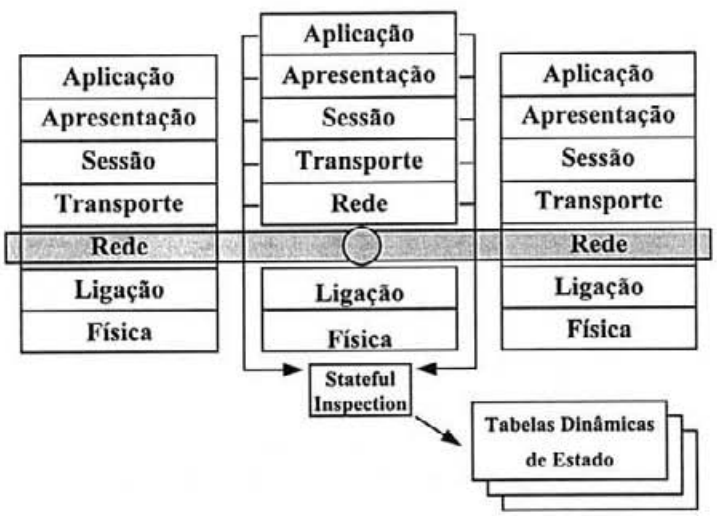


Figura 4.5 – A Arquitectura do Stateful Inspection [CheckP98]

4.3.2.1 O Exemplo FTP

O Stateful Inspection analisa a sessão FTP, examinando os dados FTP da camada de aplicação. Quando o cliente requer que o servidor gere a ligação de retorno (um comando FTP de transferência de dados), é extraído o número de porta do pedido. Os endereços IP e os números de porta do cliente e do servidor são guardados numa lista de pedidos pendentes de dados FTP.

Quando a ligação de dados FTP é tentada, o Stateful Inspection examina a lista e verifica que a tentativa é em resposta de um pedido válido. A lista de ligações é mantida dinamicamente, de forma que somente as portas FTP requeridas são abertas. Logo que a sessão é fechada as portas são bloqueadas, assegurando a máxima segurança.

4.3.2.2 A Segurança dos Protocolos *Connectionless* tal como o UDP

As aplicações baseadas no UDP são difíceis de filtrar com técnicas de filtragem de pacotes simplistas, porque no UDP não existe distinção entre um pedido e uma resposta. No passado, a opção estava entre eliminar completamente as sessões UDP ou abrir uma larga porção da gama UDP para comunicação bidireccional, e assim expor a rede interna.

A solução implementada pela Check Point segura as aplicações UDP mantendo uma ligação virtual em cima das comunicações UDP. Cada pacote de pedido UDP que é autorizado a atravessar o *firewall* é registado, e os pacotes UDP que atravessam na direcção oposta são verificados com a lista das sessões pendentes de forma a assegurar que cada pacote UDP está num contexto autorizado. Um pacote que é uma resposta genuína a um pedido é enviada e todos os outros descartados. Se uma resposta não chegar dentro do período de tempo especificado, o tempo da ligação expira. Desta forma, todos os ataques são bloqueados, enquanto as aplicações UDP podem ser utilizadas de forma segura.

4.4 Arquitecturas de *Firewalls*

A "solução ideal" para a construção de um *firewall* dificilmente se baseará numa única técnica; é normalmente uma combinação de técnicas cuidadosamente seleccionadas para resolver diferentes problemas. Os problemas a resolver dependem dos serviços que se quer fornecer aos utilizadores e qual o nível de risco que se considera aceitável correr. As técnicas utilizadas para resolver esses problemas dependem do tempo, custos, e aptidões disponíveis [ChapZw95].

Alguns protocolos podem ser melhor tratados com a filtragem de pacotes, outros são melhor tratados com *proxies*. A maioria dos *firewalls* utilizam uma combinação de *proxies* e filtragem de pacotes.

Esta secção descreve um conjunto de formas de agregar vários componentes de *firewalls*.

4.4.1 Arquitectura de *Dual-Homed Host*

A arquitectura de *dual-homed host* tem por base um computador que tem pelo menos duas interfaces de rede. Este tipo de *host* pode actuar como um *router* entre as redes a que esses interfaces estão ligados. No entanto, para implementar uma arquitectura de *firewall* tipo

dual-homed host, esta função de encaminhamento é desactivada. Desta forma, pacotes IP de uma rede (por exemplo a Internet) não são encaminhados directamente para a outra rede (por exemplo a rede interna protegida). Os sistemas no interior do *firewall* e os sistemas fora do *firewall* podem comunicar com o *dual-homed host*, mas estes sistemas não conseguem comunicar directamente entre si.

A arquitectura de rede para um *firewall* de *dual-homed host* (Figura 4.6) é bastante simples: o *host* coloca-se entre a Internet e a rede interna.

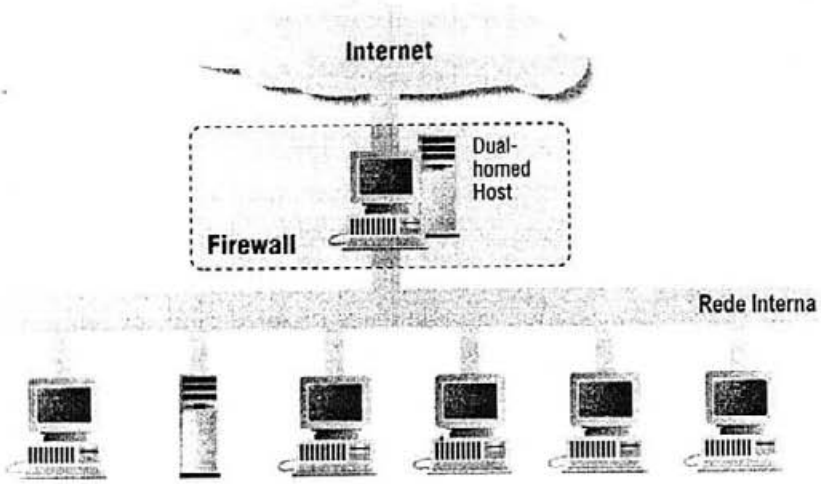


Figura 4.6 – Arquitectura de *Dual-Homed Host* [ChapZw95]

Os *dual-homed hosts* podem fornecer um nível elevado de controlo. Se não for permitido que os pacotes passem entre as redes interna e externa, é certo que qualquer pacote da rede interna que tenha uma origem externa é evidência de algum tipo de problema de segurança. Em alguns casos permite rejeitar conexões que dizem ser para um determinado serviço mas que não contêm os respectivos tipos de dados correctos; por outro lado, um sistema de filtragem de pacotes tem dificuldades com este tipo de controlo.

Um *dual-homed host* só pode providenciar serviços através de *proxy*, ou permitir aos utilizadores efectuarem o *login* directamente no *dual-homed host*. Se as contas de utilizador apresentam já problemas significativos de segurança por si próprias, apresentam especiais problemas nos *dual-homed hosts*, onde podem inesperadamente permitir serviços que sejam considerados inseguros.

Efectuar o *proxy* é muito menos problemático, mas pode não estar disponível para todos os serviços de interesse. Como já vimos anteriormente (4.2 Sistemas *Proxy*) existem formas de tornear esta situação, mas não se aplicam a todos os casos. A arquitectura de *screened host*, descrita na secção seguinte, oferece algumas opções extra para providenciar serviços novos e/ou não confiáveis.

4.4.2 Arquitectura de *Screened Host*

Enquanto uma arquitectura de *dual-homed host* providencia serviços de um *host* ligado a múltiplas redes mas com o encaminhamento desactivado, uma arquitectura de *screened host* providencia serviços de um *host* que está ligado somente à rede interna, utilizando um *router* em separado. Nesta arquitectura, a segurança é providenciada primeiramente pela filtragem de pacotes; por exemplo, a filtragem de pacotes evita que os utilizadores torneiem os servidores *proxy* para efectuarem conexões directas.

A Figura 4.7 ilustra uma versão simples de uma arquitectura de *screened host*. O *host* bastião situa-se na rede interna. O filtro de pacotes no *screening router* é configurado de forma que o *host* bastião é o único sistema da rede interna com o qual os *hosts* da Internet podem estabelecer conexões, mas somente certos tipos de conexões são permitidas. Qualquer sistema externo que tente aceder a sistemas ou serviços internos tem de ligar-se a este *host*. O *host* bastião, desta forma, precisa de manter um alto nível de segurança.

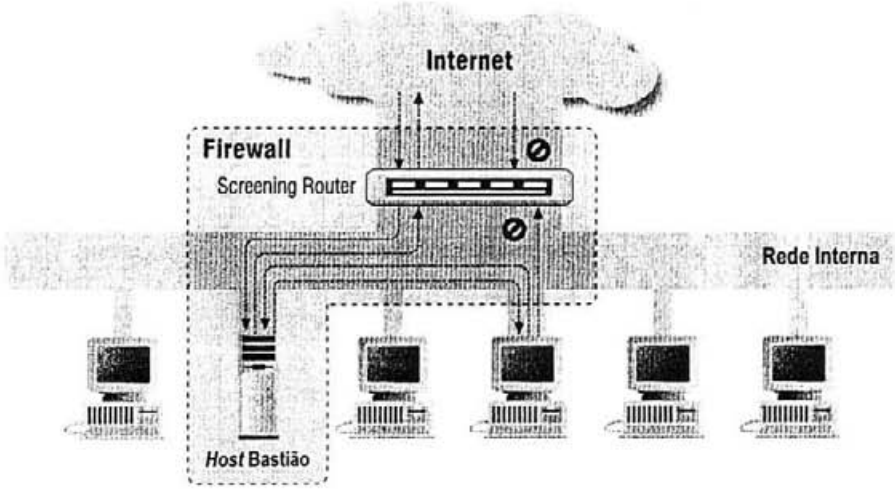


Figura 4.7 – Arquitectura de *Screened Host* [ChapZw95]

O filtro de pacotes também permite ao *host* bastião abrir conexões permitidas para o exterior, de acordo com a política de segurança do *site*. A configuração de filtragem de pacotes no *screening router* pode basear-se numa das seguintes opções:

- Permitir a outros *hosts* internos estabelecer conexões com *hosts* na Internet para certos serviços.
- Inibir todas as conexões dos *hosts* internos, forçando-os a usar serviços *proxy* através do *host* bastião.

É possível combinar estas duas abordagens para diferentes serviços; alguns podem ser permitidos directamente por filtragem de pacotes, enquanto outros podem ser permitidos somente indirectamente por *proxy*.

Como esta arquitectura permite que pacotes passem da Internet para as redes internas, pode ser considerada mais arriscada do que a arquitectura de *dual-homed host*, que é projectada de forma que nenhum pacote externo possa chegar à rede interna. Na prática, a arquitectura de *dual-homed host* também está sujeita a falhas que deixem passar os pacotes da rede externa para a rede interna. Para além disso, é mais fácil defender um *router*, que fornece um conjunto muito limitado de serviços, do que é defender um *host*. Para a maioria dos propósitos, a arquitectura de *screened host* fornece melhor segurança e melhor utilização do que a arquitectura de *dual-homed host*.

Comparada com outras arquitecturas, no entanto, tal como a arquitectura de subrede *screened* descrita na secção seguinte, tem algumas desvantagens. A maior é que se um atacante conseguir entrar no *host* bastião, não resta mais nada em termos de segurança da rede entre o *host* bastião e o resto dos *hosts* internos. O *router* também representa um único ponto de falha; se o *router* ficar comprometido, a rede inteira fica disponível a um atacante. Por esta razão, a arquitectura de subrede *screened* tem-se tornado cada vez mais popular.

4.4.3 Arquitectura de Subrede *Screened*

A arquitectura de subrede *screened* fornece uma camada extra de segurança à arquitectura de *screened host* adicionando uma rede de perímetro[7] que isola mais a rede interna da Internet.

Pela sua natureza, os *hosts* bastião são as máquinas mais vulneráveis da rede. Apesar dos esforços que se efectuem para as proteger, são as máquinas mais propícias para serem atacadas, porque são as máquinas que podem ser atacadas. Se, tal como na arquitectura de *screened host*, a rede interna estiver aberta ao ataque a partir do *host* bastião, então este é um alvo muito tentador. Não existem outras defesas entre o *host* bastião e as outras máquinas internas.

Isolando o *host* bastião numa rede de perímetro, é reduzido o impacto de uma entrada forçada no *host* bastião. O intruso obtém algum acesso, mas não o acesso total.

No tipo mais simples de arquitectura de subrede *screened* (Figura 4.8), existem dois *screening routers*. Um situa-se entre a rede de perímetro e a rede interna, e o outro situa-se entre a rede de perímetro e a rede externa. Para forçar a entrada neste tipo de arquitectura, um atacante terá de conseguir passar ambos os *routers*. Mesmo se o atacante conseguir entrar no *host* bastião, ele terá ainda de passar o *router* interior. Desta forma não existe um ponto vulnerável único que comprometa a rede interna.

---

[7] Rede de perímetro – rede situada entre uma rede protegida e uma rede externa, de forma a providenciar uma camada adicional de segurança. A rede de perímetro é por vezes designada por "zona desmilitarizada".

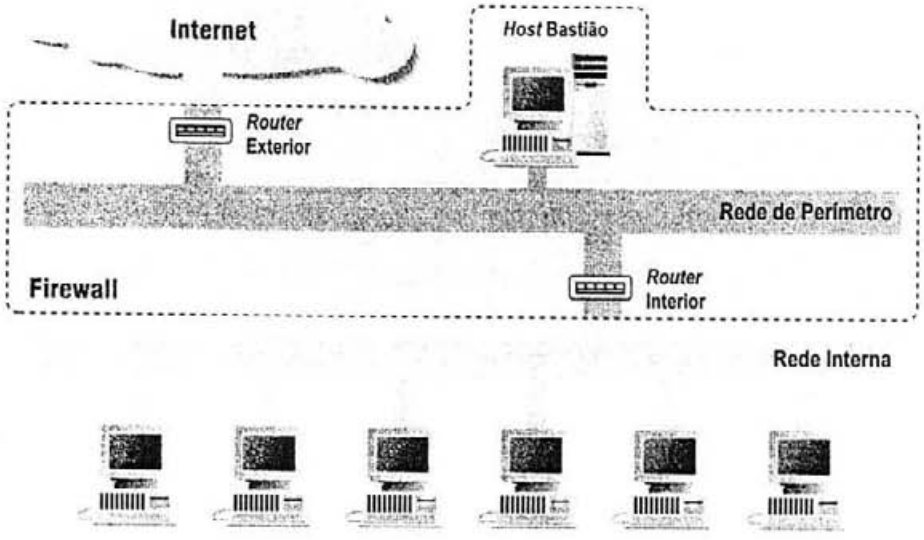


Figura 4.8 – Arquitectura de Subrede *Screened* (utilizando dois *routers*) [ChapZw95]

Alguns *sites* vão mais longe ao criar séries de camadas de redes de perímetro entre o exterior e as suas redes internas. Os serviços menos confiáveis e mais vulneráveis são colocados nas redes de perímetro mais exteriores. A ideia é que um atacante que force a entrada numa máquina de uma rede de perímetro exterior terá muitas dificuldades para atacar com sucesso as máquinas interiores devido às camadas adicionais de segurança entre o perímetro exterior e a rede interna. No entanto, isto só é verdade se existir algum significado nas diferentes camadas; se os sistemas de filtragem entre cada camada permitirem a passagem das mesmas coisas entre todas as camadas, as camadas adicionais não providenciarão qualquer segurança adicional.

4.4.3.1 A Rede de Perímetro

A rede de perímetro constitui uma camada de segurança adicional. Se um atacante conseguir quebrar a camada externa do *firewall*, a rede de perímetro oferece uma camada adicional de protecção entre o atacante e os sistemas internos.

Na maioria das tecnologias de rede é possível a alguém, a partir de uma máquina, espiar o tráfego de rede, quer a tentar apanhar *passwords*, a visualizar os conteúdos dos ficheiros, a ler *email* interessante, etc. Todo o tráfego da rede de perímetro é de e para o *host* bastião, ou de e para a Internet. Como o tráfego estritamente interno não passa para a rede de perímetro, ficará a salvo de alguém que espie o tráfego se o *host* bastião ficar comprometido.

Obviamente, o tráfego de e para o *host* bastião, ou o tráfego externo, continuará visível. Parte do trabalho no projecto de um *firewall* está em assegurar que este tráfego não é em si suficientemente confidencial que a sua leitura por alguém possa comprometer o *site* no seu todo.

4.4.3.2 O *Host* Bastião

Com a arquitectura de subrede *screened*, liga-se um *host* (ou *hosts*) bastião à rede de perímetro; este *host* é o ponto principal de contacto para as conexões provenientes do exterior, por exemplo sessões de *email* provenientes do exterior destinados ao *site*.

Os serviços de clientes internos para servidores na Internet são tratados de uma das seguintes formas:

- Configurar a filtragem de pacotes nos *routers* exterior e interior para permitir aos clientes internos aceder aos servidores externos directamente.
- Configurar servidores *proxy* a serem executados no *host* bastião para permitir aos clientes internos aceder aos servidores externos indirectamente. Também deverá ser configurada a filtragem de pacotes para permitir aos clientes internos comunicar com os servidores *proxy* no *host* bastião e vice versa, mas inibir as comunicações directas entre os clientes internos e o exterior.

Em ambos os casos, a filtragem de pacotes permite ao *host* bastião ligar-se a, e aceitar conexões de *hosts* na Internet; que *hosts*, e para que serviços, é ditado pela política de segurança do *site*.

Muita da actividade do *host* bastião é agir como um servidor *proxy* para vários serviços, quer executando *software* servidor *proxy* especializado para protocolos particulares (tal como HTTP ou FTP), ou executando servidores normalizados para protocolos *proxy* por si próprios (tal como o SMTP).

4.4.3.3 O *Router* Interior

O *router* interior protege a rede interna da Internet e da rede de perímetro. Efectua a maioria da filtragem de pacotes do *firewall* e permite os serviços seleccionados da rede interna para a Internet. Esses serviços são os serviços que o *site* pode, de forma segura, suportar e providenciar utilizando filtragem de pacotes em vez de *proxies*.

Devem limitar-se os serviços entre o *host* bastião e a rede interna de forma a reduzir o número de máquinas (e o número de serviços dessas máquinas) que podem ser atacadas do *host* bastião, se este ficar comprometido. Devem limitar-se, na medida do possível, ao permitir os serviços somente de e para *hosts* internos particulares; por exemplo, o serviço SMTP deve ser limitado a conexões entre o *host* bastião e o servidor ou servidores de *mail* internos. A segurança dos *hosts* internos e serviços que podem ser contactados pelo *host* bastião, deve ser tida em especial atenção, pois estes *hosts* e serviços serão o alvo posterior do atacante se este conseguir forçar a entrada no *host* bastião.

4.4.3.4 O *Router* Exterior

Em teoria, o *router* exterior protege a rede de perímetro e a rede interna da Internet. Na prática, os *routers* exteriores tendem a permitir quase todo o tráfego para o exterior da rede de perímetro, e geralmente efectuam pouca filtragem de pacotes. As regras de filtragem de pacotes para proteger as máquinas internas deverão ser essencialmente as mesmas em ambos os *routers*; se existir um erro na definição das regras que permita o acesso ao atacante, o erro estará provavelmente presente em ambos os *routers*.

Frequentemente, o *router* exterior é fornecido por um grupo externo (normalmente o fornecedor da Internet), e o seu acesso poderá ser limitado. O grupo externo que efectua a gestão do *router* provavelmente quererá configurá-lo com algumas regras gerais de filtragem de pacotes, e não quererá manter um conjunto complicado ou frequentemente alterável de regras de filtragem. A confiança no *router* poderá também não ser a mesma da dos *routers* da própria organização.

As únicas regras de filtragem de pacotes que são realmente especiais no *router* exterior são as que protegem as máquinas na rede de perímetro (os *hosts* bastião e o *router* interior). Os *hosts* da rede de perímetro são protegidos primeiramente por segurança de *host*, complementada pelas regras de filtragem de pacotes do *router* exterior (a redundância é importante).

As restantes regras que se poderão inserir no *router* exterior são duplicados das regras do *router* interior. São as regras que impedem o tráfego inseguro entre os *hosts* internos e a Internet. Para suportar os serviços *proxy*, onde o *router* interior deixa que os *hosts* internos enviem alguns protocolos desde que estejam a comunicar com o *host* bastião, o *router* exterior pode deixar passar esses protocolos desde que provenham do *host* bastião. Estas regras são desejáveis por constituírem um nível extra de segurança, mas os pacotes que elas bloqueiam só existirão se o *router* interior falhar ou alguém ligar uma máquina à rede de perímetro.

Uma das tarefas de segurança que o *router* exterior pode efectuar, e que dificilmente poderá ser efectuado por outro componente, é a filtragem de quaisquer pacotes provenientes da Internet que tenham endereços fonte forjados, dizendo provir da rede interna. O *router* interior podia fazer isso, mas não pode garantir que os pacotes que dizem ser da rede de perímetro não são forjados. O *router* exterior está numa fronteira clara, pois se o atacante pudesse forjar pacotes a partir da rede de perímetro teria a maioria dos benefícios de um *host* bastião comprometido.

4.4.4 Variações das Arquitecturas de *Firewalls*

Nas secções anteriores foram descritas as arquitecturas de *firewalls* mais comuns. Convém, no entanto, caracterizar algumas das variações de arquitecturas mais importantes, tendo em vista o aumento da flexibilidade na combinação dos componentes de *firewalls*, de forma a melhor conjugar o *hardware* existente, o orçamento disponível, e a política de segu-

rança da organização.

4.4.4.1 Subrede *Screened* com Múltiplos *Hosts*

Poderá fazer sentido utilizar múltiplos *hosts* bastião na configuração de *firewall* de subrede *screened*, tal como se pode ver na Figura 4.9. As razões para esta opção incluem o desempenho, a redundância, e a necessidade para separar dados ou servidores.

Poderá optar-se por ter um *host* bastião que providencia os serviços importantes para os utilizadores da rede interna (tal como servidor SMTP, servidores *proxy*, etc.), enquanto outro *host* providencia os serviços da Internet. Desta forma, o desempenho dos serviços da rede interna não é prejudicada pela actividade dos utilizadores externos.

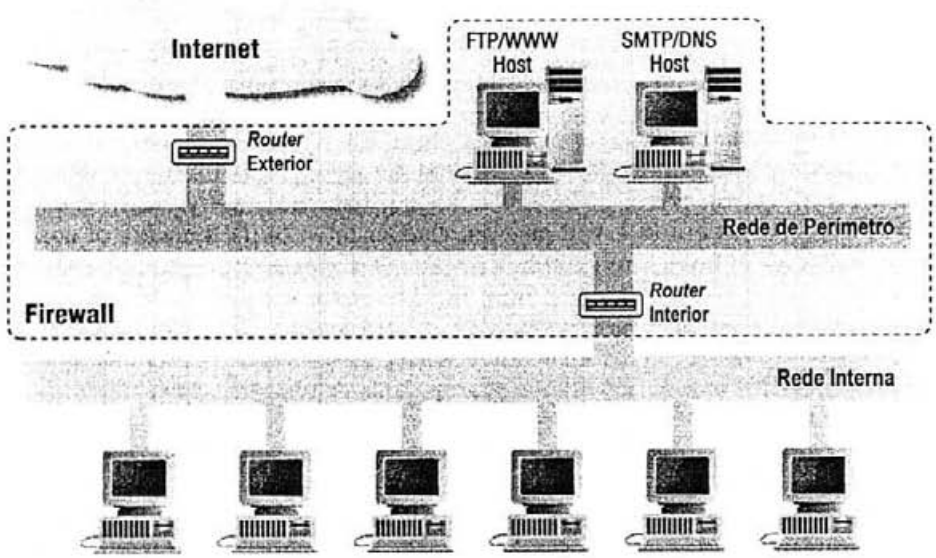


Figura 4.9 – Subrede *Screened* com *Host* Bastião e Servidor de Internet [ChapZw95]

Existem por vezes razões de desempenho para a utilização de múltiplos *hosts* bastião mesmo que não se forneçam serviços de Internet. Alguns serviços têm uma utilização intensiva de recursos, e é possível também utilizar vários *hosts* bastião para os mesmos serviços por razões de desempenho.

Se a configuração de *firewall* incluir vários *hosts* bastião, é possível configurá-los para redundância, de forma que se um falhar, os serviços podem ser fornecidos por outro. No entanto, nem todos os serviços suportam esta abordagem.

Pode optar-se também por utilizar múltiplos *hosts* bastião para evitar que os conjuntos de dados dos serviços interfiram uns com os outros, não só por razões de desempenho mas também por poderem existir razões de segurança para a sua separação. De igual forma, pode optar-se por separar serviços, para eliminar a possibilidade de um serviço poder ser utilizado para atacar o outro.

4.4.4.2 Subrede Screened com *Dual-Homed Host*

A combinação da arquitectura de *dual-homed host* com a arquitectura de subrede *screened* permite obter um aumento significativo de segurança relativamente à arquitectura base. O *host* bastião é, nesta configuração, um *dual-homed host* que divide a rede de perímetro em duas redes (Figura 4.10).

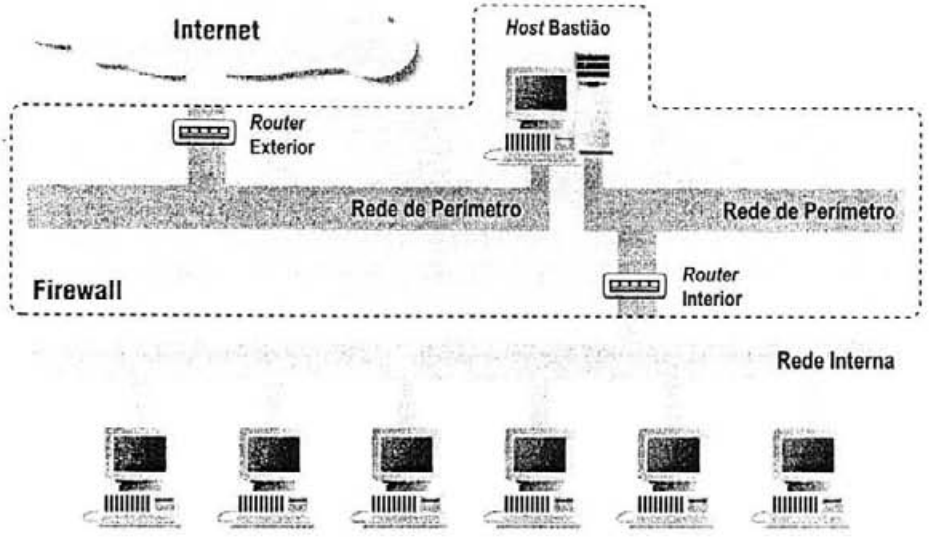


Figura 4.10 – Subrede *Screened* com *Dual-Homed Host* (adaptada de [ChapZw95])

Os *routers* fornecem protecção relativamente aos actos de forja de informação, e protegem de falhas quando o *dual-homed host* encaminha o tráfego. O *dual-homed host* providencia um controlo mais fino nas conexões do que a filtragem de pacotes.

Este *firewall*, também designado por *belt-and-suspenders*, providencia uma excelente protecção multicamada, no entanto requer uma cuidadosa configuração do *dual-homed host* de forma a tirar total proveito de todas as possibilidades.

4.4.4.3 Subrede *Screened* com *Routers* Interior/Exterior Combinados

Na arquitectura de subrede *screened* é possível combinar os *routers* interior e exterior num só *router*, mas somente com um *router* suficientemente flexível e capaz. É necessário um *router* que permita especificar os filtros de entrada e de saída em cada interface.

Ao combinar os *routers* interior e exterior, como se pode ver na Figura 4.11, continuamos a ter uma rede de perímetro (numa interface do *router*) e uma conexão para a rede interna (noutra interface do *router*). O tráfego permitido pelas regras de filtragem configuradas no *router* flui directamente entre a rede interna e a Internet, e o tráfego que é manipulado pelos *proxies* flui entre a rede de perímetro e a Internet ou entre a rede de perímetro e a rede interna.

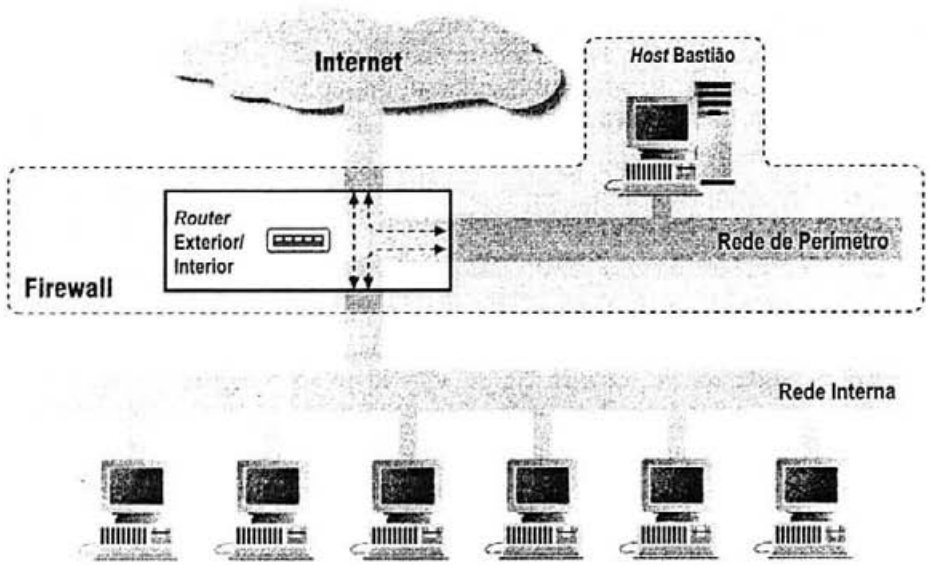


Figura 4.11 – Subrede *Screened* com *Routers* Interior/Exterior Combinados [ChapZw95]

Esta arquitectura, tal como a arquitectura de *screened host*, torna o *site* vulnerável ao comprometimento de um único *router*. Em geral, os *routers* são mais fáceis de proteger do que os *hosts*, mas não são impenetráveis.

4.4.4.4 Subrede *Screened* com *Host* Bastião *e Router* Exterior Combinados

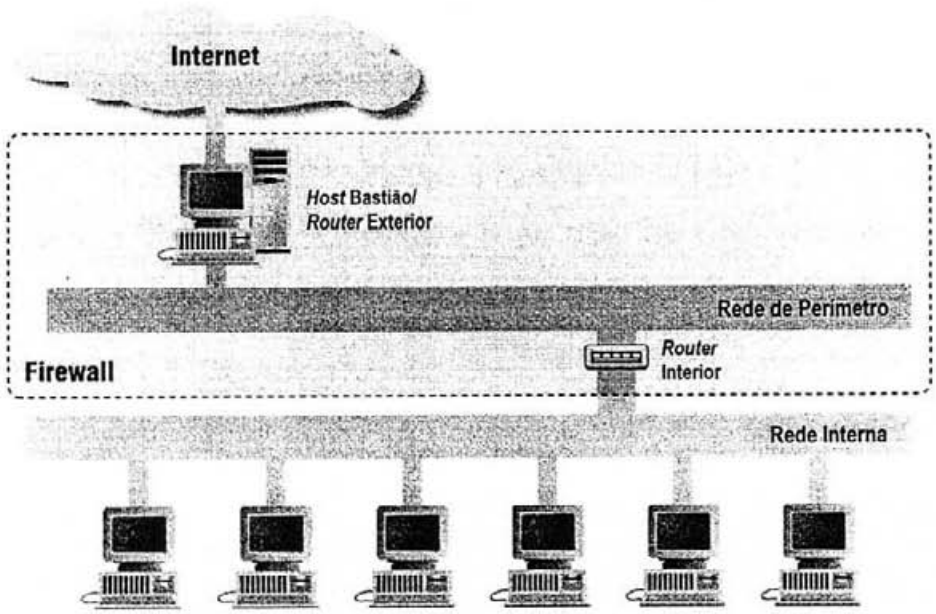


Figura 4.12 – Subrede *Screened* com *Host* Bastião *e Router* Exterior Combinados [ChapZw95]

Em determinadas casos utiliza-se uma máquina *dual-homed* como *host* bastião *e router* exterior. Por exemplo, se a única ligação disponível à Internet for uma ligação *dial-up* SLIP ou PPP, e se se executar no *host* bastião um servidor de partilha da ligação *dial-up*, ele irá actuar como *host* bastião e *router* exterior. Isto é funcionalmente equivalente à configura-

ção de três máquinas (*host* bastião, *router* interior e *router* exterior) da arquitectura de subrede *screened.*

Utilizando-se um *dual-homed host* para encaminhar o tráfego não permite obter o desempenho ou a flexibilidade de um *router* dedicado, mas não será necessário muito para uma ligação de baixa largura de banda. O pacote de *software* utilizado deverá ter a capacidade de efectuar filtragem de pacotes, mas como o *router* exterior não tem de efectuar uma filtragem de pacotes exigente, o pacote de *software* não terá de ter grandes capacidades de filtragem de pacotes.

Ao contrário da combinação dos *routers* interior e exterior, a combinação do *host* bastião com o *router* exterior (Figura 4.12), não acarreta vulnerabilidades significativas. Nesta arquitectura, o *host* bastião está mais exposto à Internet, protegido somente pela filtragem do seu próprio pacote de *software* de filtragem, e será necessário um cuidado extra para o proteger.

4.4.4.5 Subrede *Screened* com *Host* Bastião e *Router* Interior Combinados

A combinação do *host* bastião e do *router* interior (Figura 4.13) não salvaguarda a segurança da rede.

O *host* bastião e o *router* exterior efectuam tarefas de protecção distintas; complementam-se mas não se salvaguardam um ao outro. O *router* interior funciona em parte como a salvaguarda dos dois.

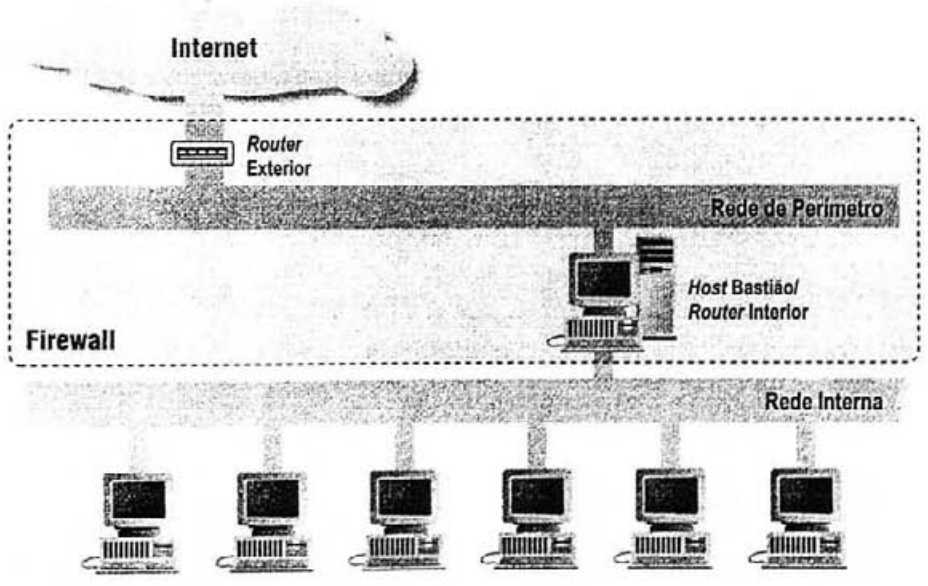


Figura 4.13 – Subrede *Screened* com *Host* Bastião e *Router* Interior Combinados [ChapZw95]

A combinação do *host* bastião e do *router* interior pode alterar a configuração do

firewall de forma drástica; se o *host* bastião não for combinado com um *software* de filtragem de pacotes, deixamos de ter a rede de perímetro e obtemos uma arquitectura de *screened host*, com a segurança de rede bastante comprometida.

Desta forma, esta variante deverá utilizar um *host* bastião (*dual-homed host*) que execute um *software* de filtragem de pacotes com as regras de filtragem devidamente configuradas.

Neste tipo de configuração, o tráfego interno é protegido de escuta mesmo que o *host* bastião fique comprometido; para chegar à rede interna, o atacante precisa ainda de passar o *router* interno. Na configuração com a combinação de um *host* bastião e um *router* exterior, a rede de perímetro continuará a existir com o *software* de filtragem de pacotes, desta forma o atacante precisará de ultrapassar dois níveis de protecção.

No entanto, um dos princípios principais da rede de perímetro é evitar que o *host* bastião possa espiar o tráfego interno. Mover o *host* bastião para o *router* interior torna todo o tráfego interno visível para ele.

4.4.4.6 Subrede *Screened* com Várias Redes Internas

A utilização de vários *routers* internos para interligar a rede de perímetro a várias partes da mesma rede interna pode causar muitos problemas, e é geralmente uma má ideia devido a problemas de encaminhamento. É difícil também manter múltiplos *routers* interiores correctamente configurados. O *router* interior é o que tem o mais importante e o mais complexo conjunto de regras de filtragem de pacotes e, tendo dois, duplicam as hipóteses de se terem as regras de filtragem erradas.

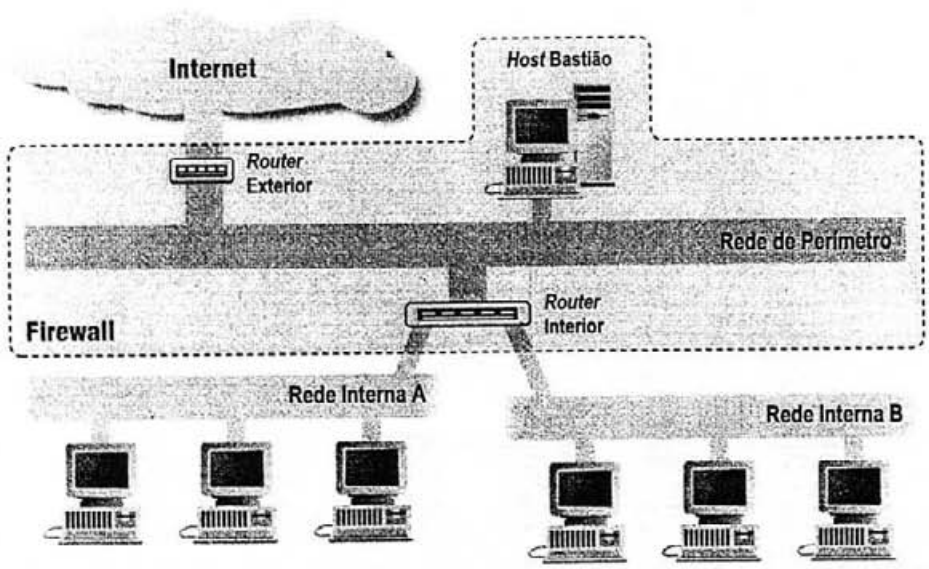


Figura 4.14 – Múltiplas Redes Internas Ligadas a Interfaces Diferentes do Mesmo *Router* [ChapZw95]

Se houver a necessidade de múltiplas redes internas por razões técnicas, organizacionais, ou políticas, a forma mais simples de acomodar essas redes será atribuir-lhes interfaces separados num mesmo *router*, como pode ser visualizado na Figura 4.14. Esta configuração complica a configuração do *router* consideravelmente, mas não produz os riscos de uma configuração de múltiplos *routers* internos.

Se existirem demasiadas redes internas para um único *router*, ou se a partilha do *router* não for aceitável por outras razões, pode construir-se um *backbone* interno onde se ligam as redes internas pelo respectivo *router*, ligando-se o *backbone* à rede de perímetro através de um único *router* interno.

4.4.4.7 Subrede *Screened* com Vários *Routers* Exteriores

Existem algumas situações nas quais faz sentido ligar vários *routers* exteriores à mesma rede de perímetro, como podemos ver na Figura 4.15.

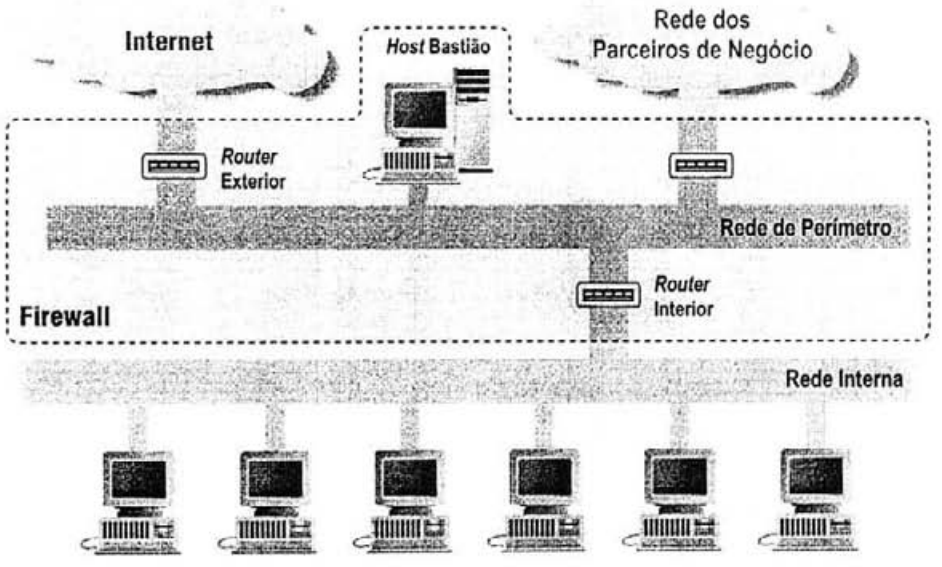


Figura 4.15 – Arquitectura que Utiliza Vários *Routers* Exteriores [ChapZw95]

Se a organização dispuser de múltiplas ligações à Internet, por exemplo, através de diferentes *service providers* para redundância, ou se dispuser de uma ligação à Internet e outras ligações a outros *sites*. Nestes casos, é possível ter um *router* exterior com várias interfaces de rede exteriores.

Ligar vários *routers* exteriores para a mesma rede externa (por exemplo, dois diferentes Internet *providers*) não é um problema de segurança significativo. Podem ter diferentes conjuntos de regras de filtragem, mas isso não é crítico em *routers* exteriores. Existem duas vezes mais hipóteses de ataque, mas o comprometimento de um *router* exterior não é particularmente ameaçador.

As coisas são mais complexas se as ligações são para diferentes redes (por exemplo uma para a Internet e outra privada). Será necessário questionar se alguém conseguir comprometer o *host* bastião, poderá o atacante aceder a tráfego sensível da rede privada? Se sim, então talvez seja melhor equacionar a alternativa de instalar redes de perímetro separadas em vez de vários *routers* exteriores numa única rede de perímetro.

4.4.4.8 Subrede *Screened* com Várias Redes de Perímetro

Podem ser utilizadas várias redes de perímetro por razões de redundância. Não faria muito sentido utilizar duas ligações à Internet, e utilizá-las através do mesmo *router* ou *routers*. Utilizando dois *routers* exteriores, duas redes de perímetro, e dois *routers* interiores assegura-se que não existirá um ponto único de falha entre a organização e a Internet.

Podem também ser utilizadas várias redes de perímetro por razões de privacidade, de forma que se enviem dados confidenciais através de uma, e utilizar uma ligação à Internet através de outra. Nesse caso, poder-se-ia mesmo ligar ambas as redes de perímetro ao mesmo *router* interior.

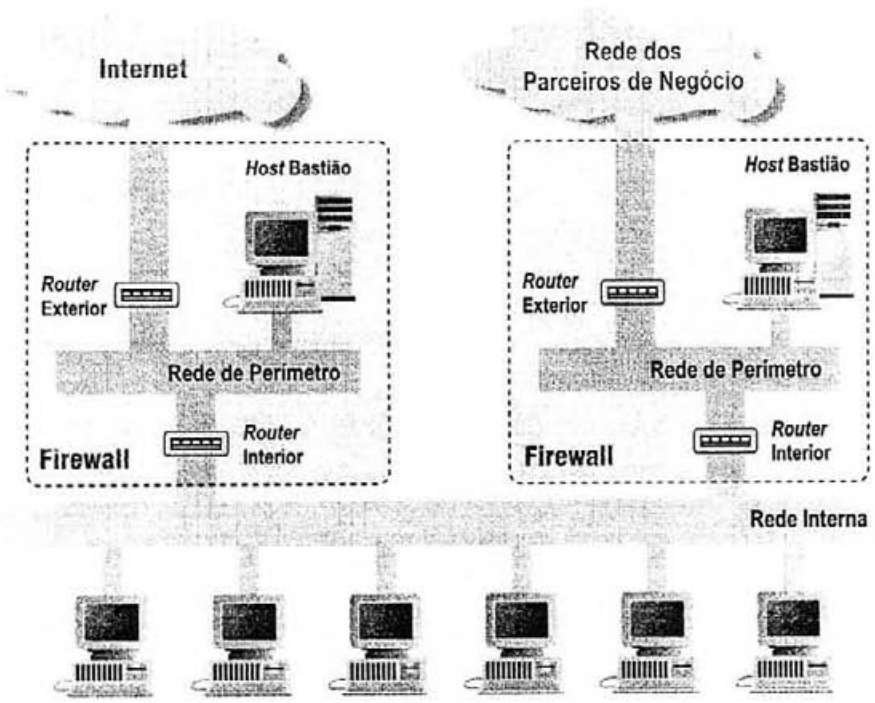


Figura 4.16 – Arquitectura que Utiliza Várias Redes de Perímetro [ChapZw95]

Ter várias redes de perímetro é menos arriscado do que ter vários *routers* interiores a partilhar a mesma rede interna, mas é também um problema na manutenção devido aos vários pontos de fraqueza possíveis. Estes *routers* devem ser geridos com cautela de forma a manter políticas de segurança apropriadas; se ambos estão ligados à Internet, devem aplicar a mesma política.

4.5 *Firewalls* Internos

As situações descritas até este ponto sobre *firewalls* retractam *firewalls* para proteger a rede interna da Internet. No entanto, em algumas situações pode ser necessário proteger partes da rede interna em relação a outras. Existem várias razões pelas quais se pode optar por efectuar isso:

- A necessidade de separar redes de teste ou de laboratório.
- Redes do *site* são menos seguras que o resto do *site*, por exemplo, redes de demonstração ou de ensino.
- Redes que são mais seguras do que o resto do *site*, por exemplo, projectos de desenvolvimento secretos ou redes onde é processada informação financeira ou de qualificações.

Muitas vezes faz sentido manter uma parte da organização separada das outras, pois nem todos os utilizadores precisam dos mesmos serviços ou informação, e a segurança é frequentemente mais importante em algumas partes da organização do que noutras.

Muitas das ferramentas e técnicas utilizadas para construir *firewalls* da Internet são também úteis para construir os *firewalls* internos. No entanto, existem algumas considerações especiais a fazer para construir *firewalls* internos.

4.5.1 Redes Laboratório

As redes de laboratório e teste são normalmente as primeiras a serem consideradas para separação do resto da organização via um *firewall*. A não ser que o trabalho englobe os *routers*, este tipo de *firewall* pode ser bastante simples. Nem uma rede de perímetro nem um *host* bastião são necessários, pois pelo facto de todos os utilizadores serem internos não é necessária a preocupação com a escuta de informação, e como as máquinas não são máquinas de utilizadores não será necessário providenciar muitos serviços. Na maioria dos casos, será necessário um *router* de filtragem de pacotes que permita qualquer conexão do exterior, mas somente as conexões que sejam seguras no sentido da rede.

Se forem testados os *routers*, será mais inteligente utilizar uma rede separada; ou então evitar que o *router* escute as actualizações de encaminhamento do resto da rede. É possível efectuar isto de várias formas, dependendo da configuração da rede, dos testes a efectuar, e dos *routers* disponíveis. Pode utilizar-se um protocolo de encaminhamento diferente do que o que está em teste e desactivar o protocolo em teste; ou configurar o *router* para não aceitar quaisquer actualizações de encaminhamento da interface em teste e filtrar os pacotes do protocolo de encaminhamento; ou especificar de que *hosts* o *router* aceitará actualizações.

Se houver várias redes de teste, poderá ser aconselhável instalar uma rede de perímetro para as redes de teste e um *router* para ligar cada uma à rede de perímetro, activando a

maior filtragem no *router* entre a rede de perímetro e a rede principal. Se os testes envolverem conexões externas, a rede de teste deve ser tratada como uma rede externa.

4.5.2 Redes Inseguras

As redes de teste são perigosas, mas não necessariamente menos seguras que outras redes. Muitas organizações têm também algumas redes que são intrinsecamente menos seguras do que a maioria. Por exemplo, redes universitárias de acesso aos estudantes, redes de organizações para demonstrações ou de treino, podem ser particularmente inseguras. Apesar disso, essas redes inseguras precisam de mais interacção com o resto da organização do que uma rede puramente externa.

Este tipo de redes, onde utilizadores externos têm acesso prolongado e a possibilidade de utilizar as suas próprias ferramentas, são realmente tão inseguras como as redes externas e devem ser tratadas dessa forma. Devem ser posicionadas numa nova ligação do *router* externo ou deve ser instalada uma nova rede de perímetro para essas redes. A única vantagem que estas redes oferecem sobre as redes puramente externas é que é possível fazer executar *software* particular nessas redes, o que significa que se pode utilizar a cifragem de forma efectiva.

As redes de demonstração e treino, onde os utilizadores externos têm um acesso supervisionado relativamente breve e não podem utilizar as suas próprias ferramentas, podem ser mais confiáveis, mas continua a ser necessário utilizar um *router* de filtragem de pacotes ou um *dual-homed host* para evitar que o tráfego confidencial flua ao longo dessas redes. Deve-se também limitar essas redes a conexões a servidores considerados seguros.

4.5.3 Redes de Alta Segurança

A maioria das organizações têm também pontos que são particularmente sensíveis à segurança. Em universidades, determinados projectos de investigação, ou a informação da avaliação; em companhias comerciais, novos produtos em desenvolvimento; em qualquer organização, a informação financeira requer protecção especial; e algum trabalho governamental não classificado também requer protecções especiais.

As redes para trabalho classificado – a qualquer nível de classificação – não só precisam de ser mais seguras, mas também precisam de cumprir as regulamentações governamentais mais importantes. Terão de ser redes separadas das redes não classificadas, pois os *firewalls* tradicionais não cumprem os requisitos.

Para cumprir os requisitos de segurança extra pode optar-se entre cifragem do tráfego que passa na rede interna normal, ou configurando redes separadas para o tráfego seguro. Redes separadas é uma solução tecnicamente mais fácil desde que existam máquinas separadas. Quer dizer, num projecto seguro que possui alguns computadores, e se os utilizadores efectuam o *login* nessas máquinas para o trabalho nesse projecto, é razoavelmente simples

configurar um *firewall* simples de uma única máquina (um *router* de filtragem de pacotes). Esse *firewall* trata a rede normal como o universo externo inseguro. Se não forem necessários muitos serviços no projecto, o *host* bastião poderá não ser necessário, e uma rede de perímetro só será necessária para as situações de maior requisitos de segurança.

Nas situações em que o trabalho dos utilizadores tem requisitos de segurança, e não existem máquinas separadas para esse trabalho, é mais difícil de implementar uma rede separada. Se essas máquinas forem colocadas numa rede mais segura, os utilizadores não conseguirão trabalhar com facilidade com o restante *site*. Neste caso, será necessário um *host* bastião e provavelmente uma rede de perímetro para operacionalizar todos os serviços. A ligação das máquinas às duas redes, a segura e a insegura, de forma que possam transmitir dados confidenciais sobre uma e no resto do *site* com a outra, é uma configuração complicada. Se estiverem ligados às duas redes ao mesmo tempo, cada *host* será um *firewall dual-homed host* com todos os problemas de manutenção e de segurança inerentes por poderem ser desconfigurados pelos utilizadores de forma que impliquem problemas de segurança. Se só puderem estar ligados a uma rede de cada vez será mais seguro. No entanto, a configuração das máquinas torna-se complexa e alternar de uma para outra rede é incómodo para os utilizadores.

Numa universidade, que em princípio não terá somente uma rede coerente, colocar os serviços de académicos e financeiros em redes seguras, separadas por *firewall* do resto da universidade, provavelmente funcionará. Numa companhia ou instituição governamental, onde a maioria dos utilizadores trabalham no mesmo ambiente, a solução mais apropriada será a utilização de cifragem.

4.5.4 *Joint Venture Firewalls*

Por vezes, as organizações juntam-se em situações determinadas e limitadas, como projectos de cooperação; precisarão de partilhar máquinas, dados, e outros recursos durante a duração do projecto. Apesar de as duas partes decidirem confiar mutuamente para os propósitos do projecto, continuam a ser duas organizações diferentes e possivelmente competidoras. As organizações quererão continuar a proteger a maioria dos seus sistemas e informação, pois não confiam inteiramente na outra nem no seu sistema de segurança.

Um *firewall* interno limita a exposição nestas situações, ao providenciar um mecanismo para partilhar alguns recursos e proteger a maioria desses recursos. Antes de configurar o *firewall* interno, é necessário definir quais os serviços a partilhar e a proteger; definir se é necessário criar um ambiente comum de trabalho para o projecto, e neste caso serão necessários dois *firewalls*: um entre a rede do projecto de cooperação e cada uma das organizações; e determinar exactamente o que se pretende realizar e os requisitos de segurança, que determinarão que tecnologias de *firewall* serão utilizadas.

Redes de perímetro partilhadas são uma boa solução para a abordagem de redes de cooperação. Cada parte instala o seu próprio *router*, sobre o seu próprio controlo, numa rede de

BIBLIOTECA F.E. PORTO

perímetro entre as duas organizações. Nalgumas configurações, esses dois *routers* podem ser as únicas máquinas na rede de perímetro, sem *host* bastião. Neste caso a "rede" pode ser uma linha série entre os dois *routers*. Utilizar uma ligação ponto a ponto como a rede de perímetro entre duas organizações, em vez de uma rede de perímetro multicliente partilhada, evita que o tráfego seja visto por uma terceira organização.

A decisão sobre a necessidade de um *host* bastião depende dos serviços que são requeridos pelo *firewall* e do nível de confiança entre as organizações. Se as organizações têm uma razoável confiança uma na outra e, consequentemente, na segurança mútua, poderá ser aceitável estabelecer uma filtragem de pacotes de forma que os clientes do outro *site* possam ligar aos serviços internos. Se as organizações não têm essa confiança mútua, podem ambas instalar o seu próprio *host* bastião na rede de perímetro, sobre o seu próprio controlo e gestão. O tráfego fluirá do sistema interno de uma organização para o seu *host* bastião, passando para o *host* bastião da outra organização, e finalmente para o sistema interno da outra organização.

4.6 O Futuro dos *Firewalls*

Os sistemas *firewalls* designados por "*firewalls* de terceira geração", que combinam as características e capacidades de filtragem de pacotes e de sistemas *proxy* em algo mais do que as duas tecnologias juntas, começaram a tornar-se disponíveis.

Cada vez mais as aplicações clientes e servidoras disponibilizam suporte nativo para ambientes *proxy*. Por exemplo, muitos clientes WWW incluem capacidades *proxy*, e muitos sistemas são fornecidos com suporte em *run-time* ou *compile-time* para sistemas *proxy* tal como o SOCKS. Por outro lado os sistemas baseados no Stateful Inspection começam a impor-se fornecendo a capacidade de suportar uma variedade de protocolos e serviços e poder aplicar qualquer regra baseada no próprio conteúdo da comunicação. Ultrapassam as limitações dos sistemas de filtragem de pacotes mantendo o mesmo nível de desempenho mas fornecendo um grande nível de segurança.

Os principais fabricantes dividem-se na aposta nas tecnologias mais promissoras – *proxies* e *stateful inspection*. No entanto, a evolução poderá estar na disponibilização de *firewalls* híbridos com a combinação das melhores características das duas tecnologias, como é o caso do Firewall-1 da Check Point.

Enquanto se trabalha nos bastidores na resolução das limitações do tamanho de endereços do protocolo de base da Internet, o IP, as pessoas que projectam o novo protocolo IP (muitas vezes referido por IPng – de "IP *next generation*", e que será o *standard* IPv6) estão a aproveitar a oportunidade de efectuar outros melhoramentos no protocolo. Alguns desses melhoramentos têm o potencial de causar alterações profundas no modo como os *firewalls* serão construídos e operados.

5. As Redes Privadas Virtuais (VPNs)

As organizações reconheceram já a Internet como um meio para a troca rápida e eficiente de dados de negócio e informação, aumentando a flexibilidade do acesso a parcerias de negócio, e reduzindo significativamente os custos da comunicação. No entanto, muitas organizações têm evitado a Internet ou restringem severamente a sua utilização devido às ameaças que são do conhecimento geral. Essas ameaças têm sido contrapostas com produtos de segurança que minimizam os riscos das redes.

As redes privadas virtuais, ou VPNs, são uma ferramenta cada vez mais importante porque são capazes de resolver um largo espectro de problemas de segurança da Internet. A tecnologia das VPNs utiliza técnicas modernas de criptografia para cifrar as comunicações de rede de forma que somente as comunicações autorizadas são possíveis [KerTIS].

Geralmente, uma VPN liga de forma segura duas ou mais redes geograficamente separadas através de uma rede pública intermédia (tipicamente a Internet) ou uma rede insegura, cifrando todos os dados enviados por uma rede e decifrando os dados recebidos na outra rede. A cifragem dos dados que são enviados na Internet tem várias vantagens, incluindo as seguintes:

- Controlo de Acesso – o acesso aos recursos de rede pode ser restrito aos utilizadores ou processos que possuem a chave criptográfica apropriada.
- Autenticação Mútua – esta característica estabelece uma forma pela qual ambos os extremos de uma comunicação de rede podem confiar na identidade mútua.
- Privacidade – o tráfego cifrado não está sujeito a "escuta" ao passar na Internet.
- Integridade – o tráfego cifrado não pode ser modificado acidentalmente ou maliciosamente sem detecção.
- Não Repúdio – este processo assegura que o emissor não pode negar ser a origem da comunicação.

Existem variações arquitectónicas VPN que merecem consideração. Considere-se os elementos descritos na Figura 5.1.

Ligações Cifradas *Firewall* a *Firewall* – Implementar cifragem entre o *Firewall* A e o *Firewall* B assegura que todo o tráfego que cruza a Internet entre ambos é privado e seguro, e que esta protecção adicional é completamente transparente aos utilizadores ou *software* de aplicação em ambas as redes.

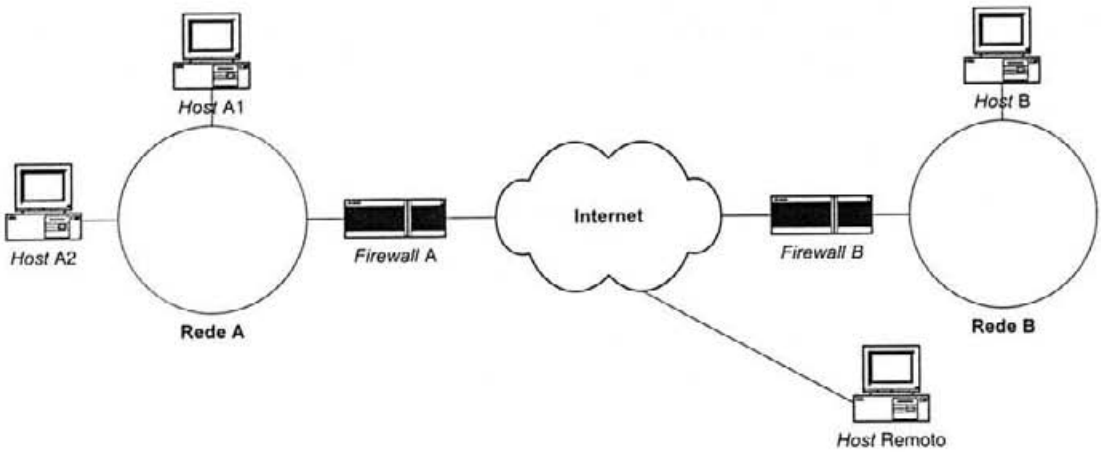


Figura 5.1 – Componentes de uma Arquitectura VPN

Ligações Cifradas *Host* a *Host* – Os dados são cifrados entre *hosts* ponto a ponto. Por exemplo, uma ligação cifrada entre o *host* A1 e o *host* B fornece privacidade e segurança quanto a intercepções não autorizadas em qualquer ponto da rede A, da Internet, ou da rede B. As ligações cifradas entre o *host* A1 e o *host* A2 evitará que utilizadores legítimos mas curiosos da rede privada A vejam ou modifiquem dados importantes.

Ligações Cifradas de um *Host* Remoto a um *Firewall* – Frequentemente é desejável fornecer a utilizadores ou parceiros acesso seguro e privado (cifrado) a recursos na rede privada, a partir de um *host* remoto isolado na Internet. Isto pode ser conseguido de três formas:

1. Uma ligação cifrada do *host* remoto até ao *host* final (o *host* A2, por exemplo). Constitui um exemplo de uma ligação cifrada *host* a *host* descrita acima. Tem a vantagem de restringir o acesso do *host* remoto a uma única máquina da rede privada sem haver a necessidade de um serviço específico *proxy* no *firewall*.
2. Uma ligação cifrada do *host* remoto até à interface interna do *dual-homed firewall* A. Como a interface interna do *firewall* é semelhante a todos os outros *hosts* da rede privada A, o *host* remoto tem assim acesso completo a todos os *hosts* e serviços da rede privada. Este modelo tem a vantagem de permitir acesso completo sem a necessidade de um serviço específico *proxy*. É geralmente descrita como ligação cifrada "confiável".
3. Uma ligação cifrada do *host* remoto até à interface externa do *dual-homed firewall* A. A interface externa do *firewall* está de facto ligada à Internet, e os pacotes que são decifrados nesse interface devem estar conformes com as regras dos *firewalls proxies*. A vantagem deste modelo é que o tráfego entre o *host* remoto e o *firewall* é privado porque é cifrado, mas os *proxies* podem ser utilizados para restringir o acesso do *host* remoto a recursos da rede privada. É geralmente descrita como ligação cifrada "privada".

5.1 As Tecnologias VPN

São utilizadas várias tecnologias para implementar as VPNs. Nas secções seguintes serão descritos os *standards* emergentes que são utilizados pelos fabricantes na implementação das VPNs.

5.1.1 O Protocolo de Cifragem da Ligação SwIPe

Para ligar de forma segura e privada duas redes através de uma rede pública, as opções mais comuns têm sido linhas dedicadas ou uma ligação VPN cifrada passando pela Internet. Se for escolhida a VPN, as duas redes utilizarão métodos *out-of-band* tal como uma ligação telefónica ou correio registado para trocar uma chave secreta partilhada que cada rede utilizará para cifrar e decifrar o tráfego IP entre elas [KerTIS].

A cifragem do tráfego IP nesses casos é razoavelmente simples. Um protocolo de cifragem da ligação tal como o swIPe[1] (*software IP encryption*) é utilizado em conjunção com um algoritmo de cifragem tal como o DES para cifrar e decifrar cada pacote IP (quer o cabeçalho quer os dados) antes que seja colocado na Internet. É afixado um novo cabeçalho ao pacote cifrado que contém a informação necessária para encaminhar o pacote até ao seu destino e o identifica como um pacote cifrado no destino. O swIPe geralmente utiliza chaves instaladas manualmente e o algoritmo de cifragem DES (56 *bits*) e é considerado bastante seguro. No entanto, protocolos tais como o swIPe são úteis somente quando o número de *hosts* participantes é relativamente pequeno, tipicamente menor do que 100.

5.1.2 O IPSec

O *standard* IPSec (arquitectura descrita na secção 3.3.3) desenvolvido pelo IETF (Internet Engineering Task Force) permite fornecer um sistema básico para interoperacionalidade entre fornecedores. Muitos fornecedores interoperam actualmente através do IPSec [AvoTIS].

Em situações que exijam uma solução VPN que se comporte bem num ambiente onde as organizações têm de gerir um maior número de ligações cifradas (até às dezenas de milhar), e para além disso, deva ser possível para as partes em cada ponto da comunicação poderem confiar na identidade da parte no outro ponto e possam confiar que os dados comunicados não são modificados acidentalmente ou maliciosamente e que o emissor não possa mais tarde negar ter enviado os dados, o IPSec é uma resposta a esses requisitos [KerTIS].

O IPSec reúne um conjunto de protocolos de segurança numa estrutura básica flexível,

[1] SwIPe é um protocolo de segurança de camada de rede. Funciona pela afixação de um autenticador criptográfico a cada pacote IP e cifrando os dados no formato IP em IP.

escalonável, e normalizada que é similar de certa forma ao protocolo swIPe mas que é bastante mais rico nos serviços que pode providenciar e nas técnicas de cifragem que pode utilizar. O IPSec está estruturado em dois componentes fundamentais: o Cabeçalho de Autenticação – Authentication Header (AH) – e a Carga de Encapsulamento de Segurança – Encapsulating Security Payload (ESP). Cada um serve propósitos ligeiramente diferentes. Podem ser utilizados separadamente, ou podem ser combinados para respeitar requisitos de segurança mais complexos.

O Cabeçalho de Autenticação contém os campos necessários para autenticar ambos os pontos de uma conexão e proteger a transmissão contra as modificações (integridade); adicionalmente, quando utilizado com determinados algoritmos, fornece o não repúdio. Não fornece a privacidade com base na cifragem dos dados.

A Carga de Encapsulamento de Segurança fornece a autenticação de ambos os pontos da conexão, protege a transmissão contra modificação, e fornece privacidade pela cifragem dos dados. Não fornece a função de não repúdio. O AH e o ESP podem ser utilizados independentemente ou em combinação. Quando é utilizado o IPSec, o cabeçalho IP tradicional é substituído pelo cabeçalho AH ou ESP antes de ser transmitido na Internet.

As diferenças conceptuais entre as VPNs baseadas em swIPe e as VPNs que respeitam o IPSec são relativamente pequenas. Ambas utilizam a cifragem para "esconder" os dados, e ambas utilizam um cabeçalho IP modificado para transmitir os pacotes na Internet e identificar a natureza cifrada dos pacotes à chegada. As diferenças de implementação entra as duas tecnologias é enorme.

5.1.2.1 Caracterização da Tecnologia IPSec

O conceito de Associação de Segurança é provavelmente o elemento mais importante a entender no IPSec. Quando dois *hosts* querem estabelecer uma ligação cifrada, devem em primeiro lugar trocar informação para determinar o que cada *host* é capaz em termos de algoritmos de cifragem, modos de cifragem, chaves, etc. Logo que tenham acordado num conjunto complementar de parâmetros, designado por Índice de Parâmetros de Segurança – Security Parameters Index (SPI), a combinação do SPI e do endereço de destino identifica unicamente uma determinada Associação de Segurança e torna-se a base para o estabelecimento da ligação cifrada.

Qualquer implementação do Cabeçalho de Autenticação ou da Carga de Encapsulamento de Segurança deve suportar este conceito de Associação de Segurança. Os *hosts* participantes devem negociar a seguinte informação para o Índice de Parâmetros de Segurança:

- Algoritmo de autenticação e modo do algoritmo
- Chaves utilizadas com o algoritmo de autenticação
- Algoritmo de cifragem, modo do algoritmo, e a transformação

- Chaves utilizadas com o algoritmo de cifragem
- Duração da chave
- Campo do vector de inicialização para o algoritmo de cifragem
- Duração desta Associação de Segurança
- Endereço(s) fonte da Associação de Segurança
- Nível de sensibilidade para sistemas seguros multinível

O Cabeçalho de Autenticação foi projectado para fornecer integridade e autenticação mas sem confidencialidade para os datagramas IP. A ausência de confidencialidade assegura que implementações do AH estarão largamente disponíveis na Internet, mesmo em localizações onde a exportação, importação, ou uso da cifragem para providenciar a confidencialidade esteja regulada.

A Carga de Encapsulamento de Segurança está projectada para providenciar a integridade, autenticação, e confidencialidade dos datagramas IP, pelo encapsulamento do datagrama inteiro (modo Túnel), ou somente dos dados do protocolo da camada superior (modo Transporte), cifrando a maior parte do conteúdo do ESP, e depois adicionando um novo cabeçalho IP ao agora cifrado ESP (ver secção 3.3.3). Este cabeçalho IP não cifrado é utilizado para transportar os dados protegidos pela *internetwork*.

A combinação da utilização do Cabeçalho de Autenticação IP com o Protocolo de Encapsulamento de Segurança pode ser efectuada para obter as desejadas propriedades de segurança. O AH fornece sempre integridade e autenticação e pode fornecer não repúdio se utilizado com determinados algoritmos de autenticação (por exemplo o RSA). O ESP fornece sempre integridade e confidencialidade e pode também fornecer autenticação se utilizado com certos algoritmos de autenticação. O ESP não fornece o não repúdio. Adicionar o AH ao datagrama IP antes de encapsular esse datagrama utilizando o ESP pode ser desejável em situações de necessidade de forte integridade, autenticação e confidencialidade, e também se for requerido não repúdio forte.

5.1.2.2 A Gestão de Chaves – Os *Standards*

Os mecanismos de troca de chaves – a decisão e a comunicação das chaves criptográficas a usar para tornar seguras as comunicações criptográficas – e a manutenção dessa troca segura (privada) é vital para as comunicações privadas e para o estabelecimento das VPNs [AvolTIS].

No sistema básico do IPSec, existem muitos protocolos que podem ser utilizados para realizar as tarefas IPSec necessárias tais como negociar a Associação de Segurança, estabelecimento das chaves de sessão, etc. Os dois principais protocolos em utilização geral que suportam as VPNs IPSec são o ISA/KMP e o Oakley [KerTIS].

O Internet Security Association Key Management Protocol (ISA/KMP) define proce-

dimentos e formatos de pacotes para estabelecer, negociar, modificar, e remover as Associações de Segurança. Esses formatos fornecem um sistema base consistente para a transferência de chaves e dados de autenticação que é independente da técnica de geração de chaves, algoritmo de cifragem e mecanismo de autenticação.

O ISA/KMP é distinto dos protocolos de troca de chaves de forma a separar eficientemente os detalhes da gestão das associações de segurança (e gestão de chaves) dos detalhes de troca de chaves. Podem existir muitos protocolos diferentes de troca de chaves, cada um com propriedades de segurança diferentes. No entanto, é requerido um sistema básico comum para o acordo no formato dos atributos da Associação de Segurança e para a negociação, modificação e remoção das Associações de Segurança. O ISA/KMP serve para este sistema básico comum.

O protocolo de determinação de chaves Oakley é utilizado para estabelecer dinamicamente uma chave de cifragem de dados que é única para cada ligação (sessão) iniciada. O protocolo Oakley permite aos *hosts* participantes trocar informação ao longo de uma rede pública, como a Internet, e acordar numa chave de sessão secreta que somente eles partilham, apesar de toda a informação que trocam passar na Internet não codificada. É utilizada uma versão modificada do protocolo Diffie-Hellman Key Agreement Protocol para providenciar segurança eficiente e suficientemente testada.

O ISA/KMP e o Oakley juntos fornecem uma forma pela qual os *hosts* participantes podem estabelecer, de forma mutuamente acordada, um conjunto de parâmetros de cifragem e depois acordar de forma segura numa chave de sessão para cada ligação entre eles que passe na Internet.

Uma alternativa ao ISA/KMP é o Simple Key Management for IP (SKIP). Estes esquemas diferem na medida em que o ISA/KMP ajuda a definir as condições para a gestão de chaves, mas não a troca das chaves é efectuada pelo Oakley. O SKIP, por outro lado, permite a distribuição de chaves ao nível do pacote IP e baseia-se no Diffie-Hellman para manter a transferência segura.

5.1.3 O PPTP

O PPTP (Point-to-Point Tunneling Protocol) foi desenvolvido originalmente como uma extensão do PPP (Point-to-Point Protocol) utilizado com o TCP/IP nas linhas série (ligações *modem dial-up*), pela Microsoft em colaboração com outros fabricantes. Os túneis PPTP encapsulam os protocolos IP, IPX, ou NetBEUI nos pacotes IP. Sendo suportado pela Microsoft nos servidores Windows NT, poderá tornar-se o protocolo *standard* para estabelecer uma VPN de um sistema remoto até uma rede privada [AvolTIS].

Conceptualmente, não existe diferença entre a utilização do PPTP como cliente de comunicações com um *firewall* e a utilização duma pilha IPSec no cliente para comunicar

com o *firewall* e estabelecer uma VPN. O PPTP suporta o *tunnelling* de protocolos não IP.

O PPTP foi projectado para resolver simultaneamente os problemas dos custos e da segurança, utilizando a Internet como uma tecnologia inter-LAN e disponibilizando os benefícios de comunicações seguras e de baixo custo. O PPTP é suportado pela Microsoft, 3Com, Ascend, Telematics e US Robotics. O protocolo equivalente da Cisco é o Layer 2 Forwarding (L2F). Forem feitas sugestões para combinar as melhores características do L2F e do PPTP num novo protocolo designado L2TP [Hunt98].

5.2 As Tecnologias das Várias Áreas VPN

O estabelecimento de VPNs requer um acordo em quatro áreas diferentes: o mecanismo de cifragem, o algoritmo de cifragem (e o tamanho da chave a utilizar), o mecanismo para a negociação das trocas de chaves, e o algoritmo a utilizar na troca de chaves. Existem vários *standards* em cada uma dessas áreas tal como está descrito na Tabela 5.1.

Mecanismo de cifragem	swIPe, IPSec, PPTP
Algoritmo de cifragem	RC2, RC4, DES, 3DES, IDEA, CAST, FWZ-1
Mecanismo para negociar a cifragem e a troca de chaves	ISA/KMP, Oakley, SKIP
Algoritmo pata cifragem da informação de troca de chaves	RSA, Diffie-Hellman

Tabela 5.1 – Os *Standards* das VPNs

Todos estes *standards* precisam de ser coordenados e comunicados. As tecnologias existentes hoje em dia, e que têm vindo a ser implementadas em VPNs baseadas em *firewalls*, fornecem esses mecanismos e permitirão o aumento da distribuição e utilização das VPNs num futuro próximo.

5.3 Perspectivas com as VPNs

Devido ao aumento da utilização da Internet nas actividades das organizações, e o aumento do número de relatórios de ataques e das tentativas de forçar entradas nas redes, a segurança é cada vez mais um requisito primordial. Apesar de não serem ainda utilizadas em larga escala, com os desenvolvimentos dos *standards* e com a automatização no estabelecimento das VPNs que eles devem fornecer, espera-se um enorme aumento na utilização das VPNs [AvolTIS].

Os *firewalls* não serão dispensados com as VPNs, pois reforçam a política de segurança de rede de uma organização e fazem parte de uma defesa de perímetro. Mesmo que fosse instalado o IPSec em todos os computadores de uma organização, este forneceria privacidade

e autenticação mas não asseguraria o reforço da política de segurança da rede (os serviços permitidos, etc.). Os *firewalls* reforçam uma política de segurança que requeira ligações privadas entre redes (*sites*) mesmo que os utilizadores não possam ou não utilizem uma ligação cifrada.

As extensões IPSec disponíveis para o novo Ipv6 resolvem problemas que precisavam de solução já à bastante tempo. O IPSec protege contra ataques de *sniffer*, *spoofing* e *hijacking*[2]. Mas, mesmo com o IPSec, os erros de configuração e implementação não desaparecem. Um *firewall* é o melhor mecanismo para este tipo de problemas limitando o número de *hosts* expostos. A combinação do IPSec com *firewalls* fornece a melhor protecção [Ellerm96].

[2] Hijacking – ataque em que alguém furta a ligação depois de o utilizador se autenticar perante o sistema.

6. Ferramentas de Monitorização e Diagnóstico

A segurança de rede não se confina aos *firewalls*, cifragem e dispositivos de autenticação. É também um processo flexível que fornece constante informação do *status* das defesas, reconhece ataques e más utilizações, e responde com reconfigurações apropriadas e contra-medidas.

Para que uma rede organizacional atinja um nível de protecção mais garantida, é necessária uma tecnologia mais activa e "inteligente". Uma tecnologia que monitore activamente a rede e reconheça o óbvio bem como os sinais subtis de comprometimento da rede, quer sejam originados do exterior quer do interior. Uma tecnologia que responda numa fracção de tempo que permita tomar acções protectoras imediatas. Uma tecnologia que assista o gestor da segurança de rede em todos as fases do ataque. E uma tecnologia que possa ser implementada e mantida sem um peso excessivo quer nos recursos de pessoal, estrutura da rede ou recursos de rede [NetGen97].

6.1 As Alternativas de Segurança

Os produtos que fornecem protecção da informação para os ambientes de sistemas abertos modernos podem ser divididos em duas categorias distintas: tecnologias passivas ou estáticas, e sistemas activos ou de tempo real.

6.1.1 A Tecnologia de Segurança Estática

Muitos dos mais populares dispositivos de segurança do mercado são categorizados como segurança passiva ou estática. Estes incluem dispositivos de protecção do perímetro – tais como *firewalls* e *wrappers* de sistema – que providenciam os mecanismos para uso de alguém que tenciona efectuar acções.

Apesar de os *firewalls* e os *logs* de sistema providenciarem informação que pode ser importante à resposta ou recuperação de um ataque, esta acção tem lugar depois do facto ocorrido. A informação é recolhida mas não existe nenhuma base de conhecimento a partir da qual identificar um ataque, nem mecanismo a seguir a partir de um alarme ou resposta. Por vezes os próprios *logs* perdem a utilidade, pois pode passar demasiado tempo ou os *backups* podem já ter sido reescritos.

As tecnologias de cifragem e de autenticação são utilizadas para prevenir a ameaça de

utilizadores não autorizados que tentem entrar na rede interna; mas desde que algum esquema de decifração ultrapasse a segurança da rede, uma vez entrando na rede interna esta fica sem protecção.

Adicionalmente, a segurança passiva sozinha tem maiores custos de manutenção e desempenho. Os dispositivos passivos não efectuam funções activas como detectar intrusos, o que deve ser efectuado por um administrador com os custos de tempo e esforço. Tem também custos em termos de dinheiro e tempo sempre que um administrador de sistema executa um *software* agente de segurança numa máquina, analisa *logs* de *firewall* na pesquisa de ataques, desliga um *router* para reconfigurar os filtros, ou estabelece um *proxy* para proteger um novo serviço.

6.1.2 A Tecnologia de Segurança Activa

A tecnologia activa é definida pela capacidade de pesquisar activamente as vulnerabilidades de rede ou brechas de segurança, muitas vezes com a capacidade adicional de envio de uma resposta automática prévia à intervenção humana.

Essas tecnologias de pesquisa activa incluem: ferramentas de auditoria e de *scanning* (exame sistemático) de vulnerabilidades das redes, sistemas, e aplicações; serviços de monitorização que alertam os gestores de rede para problemas dos *routers*, intrusões de rede ou actividades suspeitas; e detectores de vírus.

Uma categoria adicional é a detecção activa de intrusões. Combinam capacidades de procura com capacidades de resposta automática. Os detectores de intrusão empregam algoritmos para identificar actividade de determinados tipos de ataque e enviam alarmes e respostas quando são identificadas as ocorrências particulares.

6.2 A Monitorização e Controlo Tradicionais

No passado, os gestores de rede tinham como única alternativa a instalação de controlos de acesso baseados no *host* e a utilização de utilitários *add-on*, e o treino do pessoal de informática [Aberde97].

Mesmo actualmente, os gestores de rede de muitas organizações sem perceberem o risco total para as suas redes ou as muitas alternativas não tradicionais associadas com a redução desses riscos, optam pela simples implementação de defesas de segurança baseadas em *firewalls* e pelos mecanismos de segurança dos sistemas [ISS97a;ISS97b]:

- Autenticação
- Controlo de acesso
- Cifragem

Esta abordagem *ad-hoc* tradicional conhecida por "mitigação de riscos directa" significa a redução de alguns riscos mas deixa outros significativos não resolvidos.

6.2.1 Ferramentas de Protecção, Monitorização e Auditoria

Não é suficiente para uma máquina ou *firewall* serem seguros, é necessário verificar a sua segurança e se foram configurados convenientemente. Deve ser possível também, verificar o que acontecerá se a análise efectuada estiver errada – isto é, se o *gateway* não for seguro [ChesBe94].

Eis algumas das ferramentas de protecção e monitorização mais largamente utilizadas:

- TCP Wrapper [Venema92] – é o mais conhecido mecanismo para monitorar e adicionar *logging* e filtragem para muitos serviços UNIX *standard* iniciados pelo *inetd*.
- TIS Firewall Kit [AvoRan94] – é um conjunto de componentes de *software* e práticas de configuração de sistema que providenciam os componentes básicos de criação de *firewalls*, bem como ferramentas para tornar seguro o *mail* SMTP e providenciar autenticação forte de utilizadores.
- Swatch – monitor de ficheiros de *log* criados pelo *syslog*; permite ao administrador efectuar acções específicas em resposta a eventos inseridos no *log* e conjuntos de eventos.
- TCPdump – é uma ferramenta bastante conhecida para sistemas UNIX de monitorização de tráfego na rede.
- Fremont Network Mapper – programa de descoberta de topologias de rede.
- Chrootuid [Venema92] – permite executar um serviço de rede num baixo nível de privilégio e com acesso restrito ao sistema de ficheiros. Permite reduzir grandemente o impacto de possíveis problemas de segurança no *software daemon*.

A função de auditoria é extremamente importante, pois se o gestor de rede optar por não a efectuar haverá voluntários na Internet que a efectuarão por ele e não lhe comunicarão os resultados [ChesBe92]. Existem disponíveis bastantes ferramentas de auditoria que poderão ajudar a descobrir erros de configuração:

- COPS [FarSpa90] – sistema que verifica sistemas UNIX em busca de problemas de segurança comuns tais como permissões não seguras em ficheiros ou directórios importantes.
- Tiger (de Doug Schales, Texas A&M University) – ferramenta que verifica os problemas de segurança de um sistema, de forma análoga ao COPS.
- Tripwire [KimSpa93] – verificador da integridade de ficheiros. Compara um conjunto de directórios e ficheiros com informação guardada numa base de dados previamente criada.
- SATAN – Security Administrator Tool for Analysing Networks (de Wietse Venema e Dan Farmer) – ferramenta controversa pois ao contrário do COPS, Tiger e outras

ferramentas, verifica o sistema a partir do exterior, da mesma forma que um atacante. Desta forma um atacante pode utilizar o SATAN para atacar qualquer sistema. De qualquer forma ajuda os administradores de rede, reconhece vários problemas de segurança do funcionamento da rede, e relata-os sem os explorar.

- ISS – Internet Security Scanner (de Christopher William Klaus) – executado a partir de outro sistema, verifica o *bugs* de *software* e erros de configuração do sistema muitas vezes explorados pelos atacantes.

6.3 Sistemas de Auditoria de Vulnerabilidades e de Detecção de Intrusões

As ferramentas de auditoria de vulnerabilidades e de detecção têm vindo a ser utilizadas por administradores de rede e de sistemas de informação para identificar falhas de segurança e detectarem ataques, simplificando as operações de segurança e reduzindo a necessidade de especialização de conhecimentos [Aberde97]. Estas ferramentas são utilizadas também para medir a eficácia dos sistemas tradicionais de prevenção de segurança.

Os gestores de rede utilizam as ferramentas de auditoria de vulnerabilidades e de detecção para:

- Identificar e isolar intrusos e aplicações desonestas;
- Determinar o nível de segurança da infra-estrutura de rede;
- Avaliar da efectividade das respostas às necessidades de segurança;
- Aplicar as correcções para reduzir os riscos postos pela rede;
- Monitorar as actividades de organizações externas para reduzir a exposição.

6.3.1 1ª Geração: Detecção de Intrusões pelo Reconhecimento de Regularidades

Tendo ganho alguma vantagem comercial em 1993, a primeira geração de ferramentas de detecção (ver Figura 6.1) focava quase exclusivamente a identificação de intrusos na *gateway* da entrada da rede. Inicialmente avançadas para a altura, essas ferramentas comparavam incursões de rede esperadas com regularidades de *strings* nos pacotes de rede do exterior. Essas ferramentas providenciavam graus diferentes de protecção e eficiência.

Algumas dessas soluções providenciam uma imediata inspecção, análise e bloqueamento, enquanto outras providenciam a possibilidade de repetir eventos históricos. As primeiras permitem o reconhecimento imediato de problemas potenciais e ameaças à medida que estes ocorrem.

6.3.2 2ª Geração: *Scanners* Inteligentes de Detecção de Vulnerabilidades e Riscos

Actualmente, versões mais maduras das ferramentas de detecção que dependem de conjuntos de regras, retorno heurístico de respostas, e reconhecimento de regularidades ultra-

passaram muito as capacidades primitivas das primeiras ferramentas.

As primeiras ferramentas de auditoria de vulnerabilidades e riscos emergiram em 1995. Desde essa altura a tecnologia evoluiu rapidamente, permitindo a possibilidade de rapidamente identificar problemas nas redes, sistemas, servidores *web*, *firewalls* e aplicações ao longo da organização. Mas nem todas as ferramentas actuais são semelhantes. Algumas estão limitadas à identificação de fraquezas dos serviços e protocolos configurados na rede, enquanto outras chegam a qualquer dispositivo IP ligado ou aplicação. E nem todas as ferramentas identificam todos os problemas.

Os fornecedores mais importantes estão actualmente a fornecer máscaras e capacidades de relatório que permitem a iniciados na segurança facilmente identificarem os problemas mais extraordinários e as soluções recomendáveis para a resolução de graves problemas ao longo de múltiplos ambientes, incluindo: ambientes operacionais, *firewalls*, servidores *web*, *routers* e aplicações.



Figura 6.1 – Ferramentas de Auditoria de Vulnerabilidades

6.3.3 3ª Geração: Gestão de Segurança Adaptativa

Os fornecedores mais avançados começaram a fornecer ferramentas de *scanning* completo que permitem a detecção completa de intrusões, que vai bastante para além das capacidades das ferramentas de detecção de regularidades da primeira geração.

Surgindo no mercado somente em 1997, os fornecedores das tecnologias de reconhecimento de regularidades e de *scanning* centraram a atenção na integração das suas soluções com as infra-estruturas de sistemas de informação e de utilitários de gestão. Estes produtos são mais fáceis de gerir, e integram repositórios de problemas conhecidos e resoluções com retorno automático de respostas de forma a gerir os riscos ao longo da rede.

Alguns fornecedores providenciam integração com os *firewalls* mais populares de forma a reconhecerem dinamicamente controlos de acesso entre redes. Outros fornecem repo-

sitórios protegidos de falhas de segurança, resoluções e correcções que permitem reconfigurar componentes da rede, incluindo *routers*, *firewalls*, ambientes de operação de servidores de aplicações e servidores *web*. E mais importante ainda, alguns fornecedores providenciam aos utilizadores a possibilidade de decidir sobre uma resolução proposta, se houver a possibilidade desta provocar efeitos colaterais.

6.3.4 O Futuro: Segurança de Rede de Auto-Resolução

Os fornecedores líderes estão a avançar para além do conjunto desligado de factos limitados, ao desenvolverem o esforço de integração da auditoria, detecção e análises de impacto com as soluções de segurança legadas, novos servidores de autenticação e autorização, *help desk software*, ferramentas de gestão de rede e ferramentas de gestão de sistemas da organização. Estes esforços estão a ser desenvolvidos em laboratório, mas enquanto a promessa da gestão de segurança adaptativa não estiver realizada, a segurança de rede de auto-resolução permanecerá um sonho.

6.4 As Ferramentas e Serviços de Segurança Activos

Nesta secção vamos caracterizar mais em pormenor as tecnologias de segurança activas – as ferramentas e serviços de segurança activos.

6.4.1 Ferramentas de Auditoria de Vulnerabilidades

As ferramentas de auditoria de vulnerabilidades são também designadas por ferramentas de *scanning* ou *scanners*. Os auditores de vulnerabilidades são constituídos por *software* de teste que é executado sobre a rede e procura áreas de fraqueza [NetGen97].

Apesar de serem activas no sentido do teste, ainda requerem que o utilizador tome a atitude de reparar, resolver ou eliminar vulnerabilidades, e são válidas somente naquele espaço de tempo.

6.4.2 Serviços de Monitorização

Os serviços de monitorização são semelhantes às ferramentas de monitorização de falhas e de desempenho. As ferramentas de monitorização de segurança verificam continuamente a rede em busca de problemas com os *routers*, intrusões que se verifiquem na rede ou actividades suspeitas.

Apesar de serem pró-activas na acção de monitorização, estas ferramentas ainda requerem uma acção subsequente da parte do utilizador.

6.4.3 Detecção de Vírus

O *software* de detecção de vírus pode reduzir o risco de infecções indesejáveis. Mesmo redes seguras podem ser vulneráveis pois as viroses podem ser transportadas pelos programas de fabricantes, *download* de *software*, e *e-mail*.

Algum *software* de detecção de vírus pode detectar e eliminar viroses com intervenção mínima ou mesmo sem intervenção do utilizador. Apesar de ser um método efectivo de protecção, a distribuição do *software* pelos postos e servidores é demorada e custosa.

6.4.4 Detecção de Intrusões

Um dos mais poderosos tipos de tecnologia de segurança activa, os sistemas de detecção de intrusões (IDS – Intrusion Detection Systems) combinam a monitorização de rede com a captura em tempo real e análise de cabeçalhos e dados dos conteúdos dos pacotes. Utilizam algoritmos sofisticados para reconhecer tipos de "assinaturas" de ataques e, após a descoberta, enviam alarmes e tomam mesmo acções de resposta.

Alguns sistemas de detecção de intrusões são baseados em *hosts*, em cujo *software* de sistema se focalizam as actividades de nível de utilizador e autenticação, acesso a ficheiros, acções de sistema e suporte a fraquezas do sistema operativo. Tem as desvantagens de o *software* dever ser configurado em cada *host* e a sua perspectiva de focalização no *host* provoca a ausência de visibilidade global do sistema.

O outro tipo de sistema de detecção de intrusão é baseado na rede. Tipicamente consiste em sensores inteligentes distribuídos que funcionam em concertação com repositórios de informação e *software* de gestão cliente/servidor. Os sensores efectuam a maior parte da análise especializada do fluxo de dados e enviam somente dados de alarme a um gestor central, reduzindo o tráfego adicional que sobrecarrega a rede, minimizando a interferência com as operações normais. Adicionalmente, os sistemas de rede configurados para ligações promiscuas podem inserir-se nas redes existentes sem congestionamento ou reencaminhamento de informação.

Cada abordagem tem as suas vantagens e desvantagens. As vantagens da detecção baseada na rede incluem [Hurw98]:

- Detecção mais rápida – um monitor baseado na rede tipicamente detecta um problema em segundos ou milisegundos. A maioria das abordagens no *host* dependem da auditoria de *logs* com a frequência de alguns minutos.
- Menor visibilidade – Um monitor é menos visível e acessível do que um *host*, e por isso menos vulnerável ao ataque. Ao contrário de um *host*, não tem de responder a *pings*, permitir aos utilizadores executarem programas nele, ou permitir acesso a utilizadores.

- Maior perímetro – a abordagem baseada na rede pode parar um ataque no perímetro da rede, antes do atacante sequer possa aceder a um *host*.
- Menos monitores – um só monitor pode proteger um segmento de rede partilhado. Em contraste, é necessário um agente por *host*, o que pode ser caro e difícil de gerir.
- Menos recursos – não ocupa qualquer recursos no dispositivo protegido.

A abordagem baseada no *host* também tem as suas vantagens:

- Menores custos – pode ter menores custos para pequeno número de *hosts*.
- Mais granular – pode facilmente monitorar actividades tais como acesso a ficheiros sensíveis, directórios, programas, ou portas, que são difíceis de deduzir a partir de pistas baseadas nos protocolos.
- Perímetro mais restrito – se um atacante obtiver uma *password* e um nome de utilizador para um *host*, o agente baseado no *host* tem mais possibilidades de distinguir actividades maldosas de actividades normais.
- Mais configurável – a configuração de cada *host* é mais fácil com um agente por cada *host*.
- Menos *hosts* – a abordagem baseada no *host* pode não necessitar de uma plataforma de *hardware* dedicada.
- Menos sensível ao tráfego – é improvável que um agente perca qualquer actividade devido ao fluxo de tráfego.

Estas duas abordagens complementam-se mutuamente. Uma estratégia possível é implementar monitorização baseada na rede e adicionar agentes em *hosts* particularmente sensíveis.

6.4.5 Os Componentes Chave

Dadas as limitações da tecnologia passiva e da detecção de intrusões de *host*, o sistema de detecção de intrusões ideal é um sistema baseado na rede que resolva as necessidades chave de detecção em tempo real, os alarmes e as respostas. Outras características, que resolvem as necessidades de confiabilidade, segurança, transparência e recuperação, são descritas também.

6.4.5.1 Componente de Tempo real

Como a arma mais poderosa nas mãos do intruso é o tempo, é essencial um componente de tempo real em todos os sistemas de segurança.

A **detecção de tempo real** significa que uma intrusão é identificada no espaço de segundos de má utilização ou comprometimento de rede, antes que possam ser causados danos. A **resposta automática em tempo real** significa que o ataque é contraposto com uma reacção instantânea – a activação de uma função de *logging* automática, um alarme à pessoa apro-

priada via *e-mail*, *pager* ou eventos SNMP, ou resposta programada automática.

6.4.5.2 Bloqueamento de Eventos

O bloqueamento de eventos é uma função adicional que pode aumentar as facilidades de *logging* e de alarme ao desligar (ou bloquear) automaticamente uma ligação em resposta a certos ataques altamente destrutivos tais como o SYN Flooding[1] ou o TCP Hijacking.

6.4.5.3 Alarmes Inteligentes

Os alarmes não confiáveis e os falsos positivos levam os operadores dos sistemas a ignorar não só os alarmes falsos, mas também os verdadeiros. É vital minimizar os falsos positivos e permitir aos administradores de rede ajustar os dispositivos de acordo com a sua própria rede.

Por esta razão, a tecnologia de detecção de intrusões gravitou em direcção a uma tecnologia baseada na assinatura ou na má utilização – uma inteligência analítica intrínseca pode reconhecer centenas de ataques, más utilizações, e assinaturas de intrusões. Por exemplo, alguns ataques são simplesmente uma colecção de eventos menores que não seriam detectados, mas colectivamente significam uma intrusão. Um sistema inteligente sabe detectar a diferença, o que torna o sistema mais seguro e reduz a probabilidade de alarmes falsos.

6.4.5.4 Ficheiros de *Log* e de *Tracing*

Os ficheiros de *log* são essencialmente usados para efectuar o *tracing* duma intrusão. Deixam um registo da informação chave do ataque, localizando precisamente o endereço de origem e seguindo o percurso do intruso. Este ficheiro de *log* ajuda também com a resposta pós-ataque, dando assistência na recuperação e construção do caso.

Os ficheiros de *tracing* de evidências são os registos detalhados de pacotes de um endereço de ataque que pode ser automaticamente capturado logo que uma intrusão for detectada. Esses ficheiros de *tracing* de evidências seguem as "pegadas" do intruso que podem ser utilizadas para determinar as intenções, destino, e técnicas do atacante. Se capturados correctamente, os ficheiros de *tracing* podem também ser preparados para serem lidos por um *sniffer* analisador de rede, ou utilizado como prova em tribunal.

---

[1] SYN Flooding – tipo de ataque de negação do serviço, em que a máquina do *hacker* envia uma série de *requests* de ligação mas não efectua os respectivos *acknowledgements* da resposta, provocando a espera por tempo indefinido da máquina alvo. Se o processo for repetido muitas vezes, torna a porta de destino inoperante.

6.4.5.5 Transmissão Segura e Transparente

Um sistema de detecção que utilize as mais recentes tecnologias de segurança para autenticar, cifrar e gerir comunicações, ajuda a eliminar os ataques de *spoofing*, negação do serviço, e *snooping*. Adicionalmente, a tecnologia de detecção de intrusões transparente significa que um intruso bem como os utilizadores autorizados não podem determinar se estão a ser investigados.

6.5 Opiniões Críticas e Perspectivas de Evolução

De entre as ferramentas activas de segurança, as mais sensíveis e que poderão comprometer a segurança da rede se não forem suficientemente eficientes, os sistemas de detecção de intrusões (IDS) têm recebido algumas opiniões críticas relativamente à sua real capacidade de resposta aos ataques de rede.

Ptacek e Newsham da Secure Networks [PtaNew98] afirmam que os IDSs baseiam-se num mecanismo de recolha de dados – análise de protocolos passiva – que é fundamentalmente imperfeito. Salientam dois problemas básicos relacionados com a análise de protocolos passiva: o primeiro é que não existe informação suficiente na linha na qual basear conclusões sobre o que estará de facto a acontecer nas máquinas da rede; e o segundo, o facto de o sistema ser passivo torna-o inerentemente "*fail-open*", que significa que um comprometimento na disponibilidade do IDS não compromete a disponibilidade da rede.

Após testes efectuados a alguns dos mais populares IDS do mercado, que demonstraram vulnerabilidades aos ataques, concluem que os IDSs não são perfeitamente confiáveis até serem completamente redesenhados.

Marcus Ranum da Network Flight Recorder, afirma que o engano nos sistemas de detecção de intrusões é que é impossível para alguém que não conheça uma rede poder perceber o que deve ou não acontecer realmente nessa rede. Diz que a NFR opta por fornecer aos seus clientes e aos revendedores com valor acrescentado a possibilidade de integrar os seus próprios filtros eficientemente.

As críticas à abordagem tecnológica dos IDS e as possibilidades de configuração das soluções terão comprovados fundamentos, mas não retiram as grandes potencialidades e lugar próprio no espaço da segurança de rede que estas ferramentas atingiram. Pelo contrário, estas críticas obrigam a um constante aperfeiçoamento quer do ponto de vista da segurança quer do ponto de vista da gestão. Um exemplo disso são as facilidades de configuração das assinaturas dos novos ataques que as soluções mais importantes do mercado já disponibilizam.

Por outro lado, conscientes de que a detecção de intrusões sozinha não é suficiente e que será necessário combiná-la com outras soluções de segurança de rede, perspectiva-se que

o mercado dos *firewalls* e dos IDS pode vir a convergir, como é evidenciado pelas aquisições entre empresas dos dois mercados [ClarCN98]. Outro aspecto é a possibilidade de os IDSs efectuarem a reconfiguração de *routers* ou *firewalls* para bloquearem algum ataque detectado e inibir o seu acesso à rede.

A tendência das soluções de segurança poderem convergir nota-se também com os *firewalls* e VPNs, e de uma forma geral as várias soluções de segurança poderão convergir para uma solução global, colocada no perímetro da rede e em locais estratégicos, e mais flexível e fácil de gerir.

II

II. Estudo de um Caso

7. Caracterização do Caso

O caso em estudo diz respeito à rede de computadores do Instituto Politécnico do Porto (IPP). A rede de computadores do IPP (Figura 7.1) interliga numa topologia em estrela as redes locais dos seus vários estabelecimentos:

- Escolas – Esc. Superior de Educação (ESE), Esc. Superior de Música e Artes do Espectáculo (ESMAE), e Esc. Superior de Estudos Industriais e de Gestão (ESEIG) – Núcleos da Póvoa do Varzim e de Vila do Conde.
- Institutos: Inst. Superior de Engenharia do Porto (ISEP), e Inst. Superior de Contabilidade e Administração (ISCAP).
- Outros estabelecimentos: Serviços Centrais (SC), e Instituto de Desenvolvimento Tecnológico (IDT).

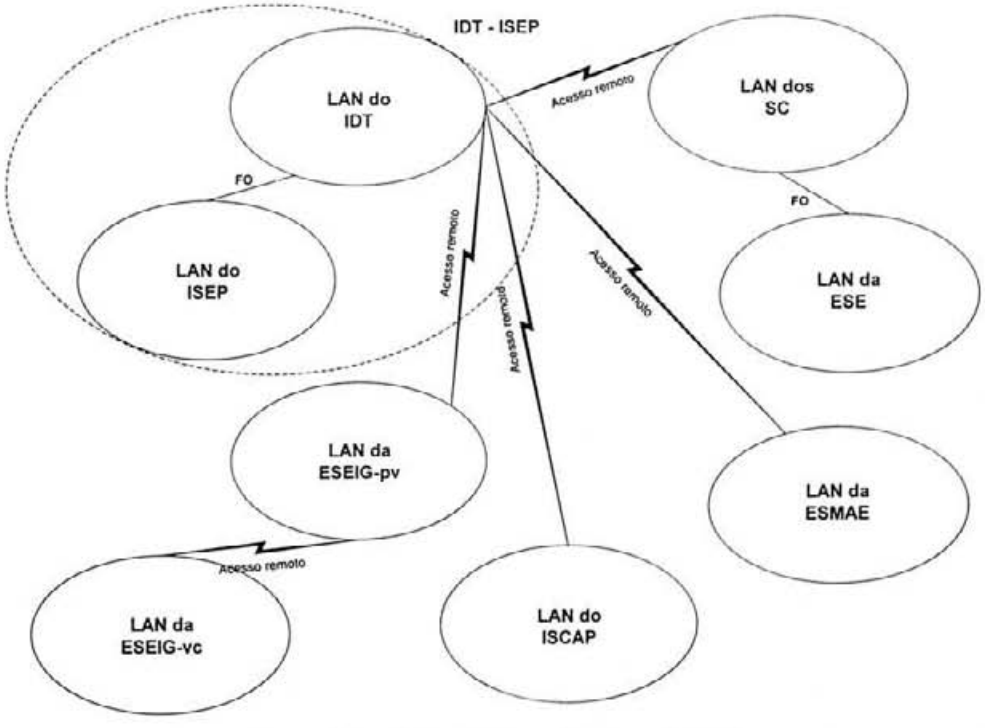


Figura 7.1 – Rede de Computadores do IPP

A rede visa interligar as várias redes locais (LANs) que fornecem serviços gerais ou específicos a alunos, professores e funcionários, considerando-se em particular todos os serviços inerentes do acesso à Internet, principalmente os serviços de WWW e de *e-mail*. Deve permitir igualmente a interligação dos vários estabelecimentos do IPP, com os outros institutos politécnicos e outros estabelecimentos de ensino superior, de investigação e científicos, e

de uma forma geral com a "rede global".

7.1 Caracterização Geral da Rede

Os vários estabelecimentos estão ligados através de fibras ópticas e linhas dedicadas, tipicamente desde algumas centenas de metros a 4 ou 5 km, havendo uma situação limite de cerca de 30 km (ESEIG).

As várias redes locais têm graus de complexidade diferentes, desde as simples LANs de um segmento de rede e com algumas dezenas de PCs (ESEIGs e ESMAE), passando pelas LANs de média dimensão com maior complexidade e cerca de uma ou duas centenas de PCs (ESE, SC, e ISCA), até à LAN de maior complexidade (ISEP-IDT) com vários segmentos departamentais e várias centenas de PCs.

As LANs são tipicamente Ethernets, de cablagem estruturada (UTP categoria 5) a operarem a 10/100 Mbits/s e de cabo coaxial fino (10Base2) nas instalações mais antigas. A LAN do ISEP-IDT tem um *backbone* constituído por várias fibras ópticas que interligam os vários edifícios.

Os equipamentos de comunicação das LANs ao nível dos nós da rede são *switches* e *hubs* Cabletron que permitem efectuar a distribuição da cablagem UTP e fibra óptica. Outros *hubs*, repetidores, e servidores de terminais completam os equipamentos de comunicação principais. Ao nível da WAN são utilizados vários *routers* Cisco 2503 e um Cisco 4500-M (no IDT) na interligação das linhas dedicadas, como já foi referido, numa topologia em estrela.

O IDT efectua a ligação à Internet através da RCCN (Rede da Fundação para o Desenvolvimento dos meios Nacionais de Cálculo Científico), por meio de uma linha dedicada digital de 256 kbits/s. As linhas dedicadas entre o IDT e os vários estabelecimentos são digitais a 64 kbites/s.

A rede do IPP tem uma configuração de rede aberta, suportando várias arquitecturas protocolares. Mas vários factores justificam a utilização do TCP/IP como o principal protocolo de comunicação: o ser o *standard* da Internet, as várias redes locais estarem interligadas numa perspectiva de ligação à Internet, e por ser o protocolo de melhor implantação simultaneamente nos universos UNIX e Windows e facilitar assim a intercomunicação. São utilizados também outros protocolos ao nível das redes locais como o NetBEUI, IPX, LAT, etc.

Os tipos de máquinas existentes são na sua grande maioria PCs IBM compatível com sistema operativo Windows 95, e em menor número Windows NT e 3.1, máquinas Digital UNIX, Macintosh com MacOS, e na situação particular do ISEP-IDT máquinas Ultrix, VMS, Novell e outras.

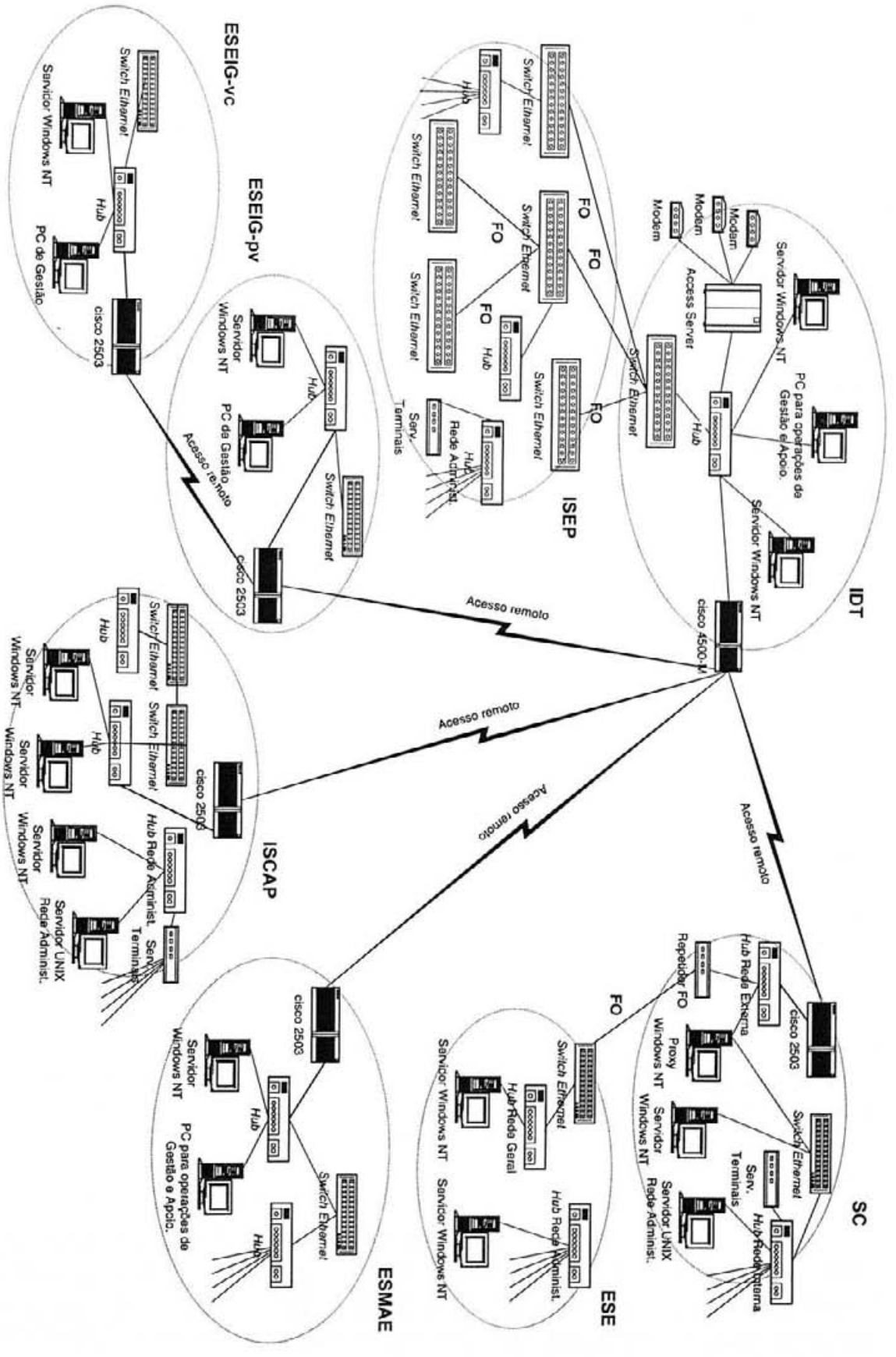


Figura 7.2 – Esquema Detalhado da Rede de Computadores do IPP

O IDT disponibiliza os servidores de DNS e de WWW, suportando desta forma o acesso à Internet das redes locais e às páginas Web do IPP. A gestão da rede é efectuada também no IDT, tendo por base o protocolo SNMP.

7.2 Um Problema de Segurança

Na perspectiva dos objectivos da rede, surgiu desde o início um problema de segurança que tem que ver com a segurança da informação dos serviços administrativos dos vários estabelecimentos, particularmente a informação dos serviços académicos relacionada com a avaliação e com as propinas.

Este problema caracteriza-se pela falta de confiança dos responsáveis dos vários estabelecimentos nos mecanismos de segurança de rede, que tem como origem o desempenho das soluções convencionais de segurança de *host* e de rede. Esta situação é reforçado pelas notícias ocasionais de "quebra" de sistemas considerados seguros, ocorridas em vários países e diferentes tipos de organizações.

O perfil dos *hackers* acentua ainda mais o problema, já que o IPP tem estabelecimentos em que os alunos têm bastantes conhecimentos, como é o caso de engenharia, dos protocolos das redes de computadores e de ferramentas de monitorização e de *hacking*.

7.3 Perspectivas para uma Solução do Problema

Foram definidas duas subredes constituintes da rede do IPP, designadas: Rede Geral e Rede Administrativa. A primeira engloba as LANs ou segmentos de rede de utilização geral ou com requisitos de segurança menos sensíveis e a segunda, mais restrita, engloba os segmentos de rede com as máquinas mais sensíveis e que exigem maiores requisitos de segurança, nomeadamente dos serviços administrativos e académicos.

A Rede Administrativa é constituída por máquinas Alpha Digital Unix nos estabelecimentos de maior dimensão (ISEP e ISCA) e nos SC, que administra financeiramente os outros estabelecimentos (ESE, ESMAE e ESEIGs), os quais acederão remotamente à máquina dos serviços centrais (SC). Os postos de trabalho são terminais Unix nos estabelecimentos SC, ISEP e ISCA, e máquinas com Windows 95 e *software* de emulação de terminal em todos os estabelecimentos. Existem também máquinas Windows NT como servidores das aplicações Windows.

Numa solução transitória e após a instalação das linhas dedicadas que permitiram a ligação das redes locais, os segmentos de rede da Rede Administrativa de cada um dos estabelecimentos ficaram isoladas, ou através do isolamento físico da restante rede local ou então pela implementação de um *firewall* para esse segmento da rede local.

A solução definitiva do problema foi adiada para uma altura em que o desenvolvimento e distribuição das aplicações de *software* administrativo e de alunos justifique a interligação da Rede Administrativa.

As duas alternativas que foram sendo consideradas são, por um lado a implementação de uma solução que garanta a segurança da rede de computadores, por outro lado uma solução drástica que leva à separação física das duas subredes.

7.3.1 A Opção de Separação Física das Duas Subredes

A perspectiva de solução que tem vindo a ganhar maior aceitabilidade entre as opiniões dos responsáveis técnicos da área de telecomunicações do IPP é a opção pela separação física das duas subredes. Ficando a Rede Administrativa fisicamente separada da Rede Geral e sem qualquer acesso à rede exterior. Considerando-se a hipótese de um mesmo serviço ou departamento ter diferentes postos de trabalho ligados a uma ou a outra das subredes (nunca em simultâneo), para permitir aos seus utilizadores acederem aos diferentes serviços de cada uma das subredes.

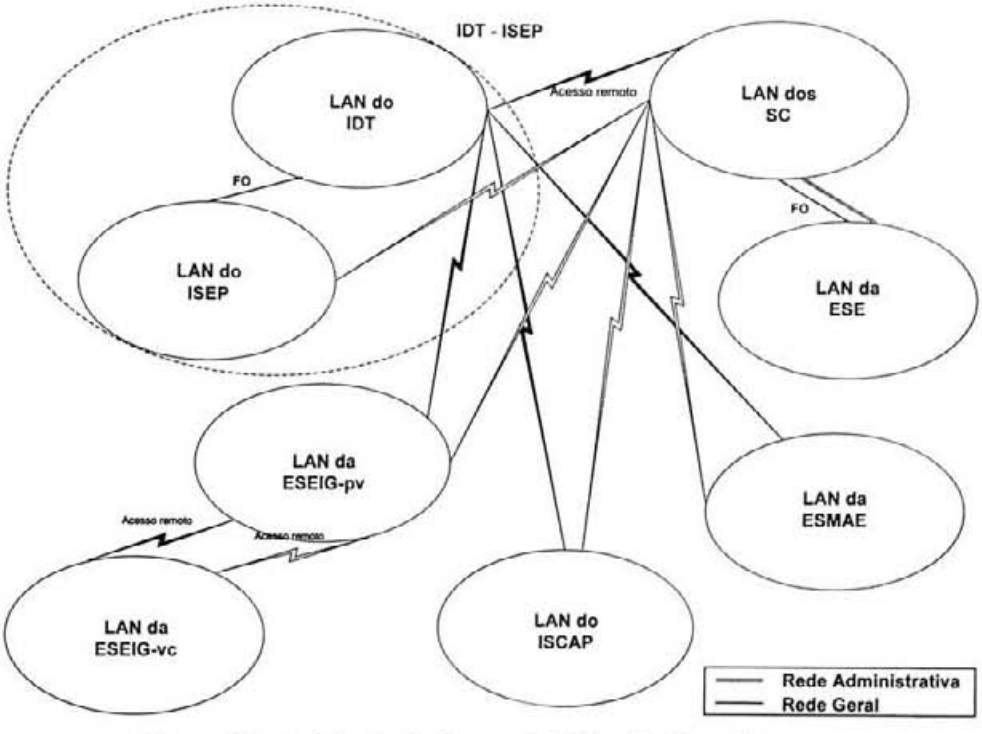


Figura 7.3 – A Solução da Separação Física das Duas Subredes

A solução da separação física das duas subredes (Figura 7.3) obriga à duplicação das linhas dedicadas e fibras ópticas. A Rede Administrativa, tendo uma topologia idêntica à Rede Geral, teria como nó central os Serviços Centrais e extremos as escolas e institutos, reflectindo a hierarquia e distribuição dos serviços académicos e administrativos (esta solução é subscrita pela presidência do IPP).

Constituindo uma solução que à primeira vista resolve o problema de segurança de uma forma definitiva por constituir uma solução drástica na separação dos universos de utilizadores, constata-se por outro lado que essa solução é somente aparente. Pois se a separação das subredes resolve o problema de segurança a nível das redes locais, já com a utilização de linhas públicas de dados o problema subsiste, ficando somente reduzida a "visibilidade" da Rede Administrativa mas nem por isso mais segura.

Por outro lado, coloca-se a questão da interoperabilidade entre as duas redes. Se o objectivo é isolar a Rede Administrativa e inibir a comunicação com o exterior, como é que um utilizador da Rede Administrativa, por exemplo, utiliza o correio electrónico? Fica assim extremamente limitada a operação eficiente nesta rede, tendo os seus utilizadores de se socorrerem de um computador da outra rede para poderem tirar partido de todos os serviços disponíveis. Este problema é agravado com o cada vez maior leque de serviços e a sua integração.

A questão da duplicação dos recursos informáticos é também bastante importante, já que principalmente a duplicação do número de linhas públicas de dados, dos elementos activos de rede e dos meios computacionais implicará consideráveis custos financeiros. A duplicação do esforço e dos recursos para a gestão das duas redes será também considerável.

7.3.2 A Opção de Implementação de um Sistema de Segurança de Rede

Os desenvolvimentos e resultados obtidos na área da segurança de rede perspectivam a implementação de soluções fiáveis. Por isso deverá sempre ser considerada a opção de implementação de um sistema de segurança baseado em soluções tecnológicas comprovadas e que garantam uma total fiabilidade.

Os *firewalls* poderão ser uma primeira linha de defesa, e a adição de cifragem das ligações (VPNs) e de ferramentas de segurança adaptativa (*scanning* e detecção de intrusões) permitem formar um conjunto de ferramentas complementares e que constituam uma solução de segurança bastante coesa. Novas soluções de autenticação e controlo de acessos permitem reforçar a base da segurança a nível do *host*.

8. Proposta de uma Solução

Neste capítulo aponta-se uma solução que constitui a proposta a adoptar para o sistema de segurança de rede, tema central desta dissertação de mestrado. Um dos objectivos deste estudo era também verificar se a solução responde aos requisitos de segurança pretendidos ou se se deverá optar pela alternativa de separação física das redes Geral e Administrativa do IPP.

A solução proposta será caracterizada e será feito o estudo e selecção das ferramentas a utilizar.

8.1 Arquitectura da Solução a Implementar

A solução a implementar baseia-se na complementaridade de várias ferramentas de segurança: *firewall* para o controlo de acessos e encaminhamento, VPN para a cifragem das ligações e autenticação mútua, e sistema de detecção de intrusões como uma segunda barreira activa para salvaguardar hipotéticas falhas de segurança ou de configuração dos primeiros.

A arquitectura de *firewall* e os principais elementos activos de rede existentes na espinha dorsal dos nós da rede determinam a arquitectura dos segmentos de rede local a implementar. Os elementos activos de rede e as suas características técnicas (anexo A) constituem assim uma restrição técnica, pois esse material foi adquirido recentemente para a constituição dos nós da rede do IPP.

Tendo por base a arquitectura de *Firewall* de Subrede *Screened*, a que respeita os maiores requisitos de segurança, definiram-se duas alternativas consideradas as mais seguras para a arquitectura base do sistema de segurança (Figura 8.1).

As características base da arquitectura do sistema de segurança são as seguintes:

- A rede de perímetro constitui uma camada de segurança adicional para a rede interna (Rede Administrativa) e para o *host* bastião. Todo o tráfego da rede de perímetro é de e para o *host* bastião, ou de e para a Internet.
- O *router* exterior constitui a primeira barreira à Internet e ao segmento local da Rede Geral. Efectua a ligação da Internet à Rede Geral e à rede de perímetro e faz a filtragem de tráfego para a rede de perímetro protegendo o *host* bastião e a rede interna.

- A solução de *firewall* seleccionado (secção 8.2.2) determina que o *router* interior seja um *dual-homed host*. Este *firewall gateway* interior é a segunda barreira de protecção à rede interior.
- O *host* bastião constitui o ponto de contacto para as conexões autorizadas provenientes do exterior e dos serviços dos clientes internos para servidores na rede externa. Age como um servidor *proxy* para vários serviços da Internet (HTTP, FTP, etc.) e executa serviços para a rede interna e para a Internet (servidor HTTP, FTP, SMTP, etc.). O serviço SMTP funciona como intermediário entre o servidor de *e-mail* (rede interna) e a Internet.

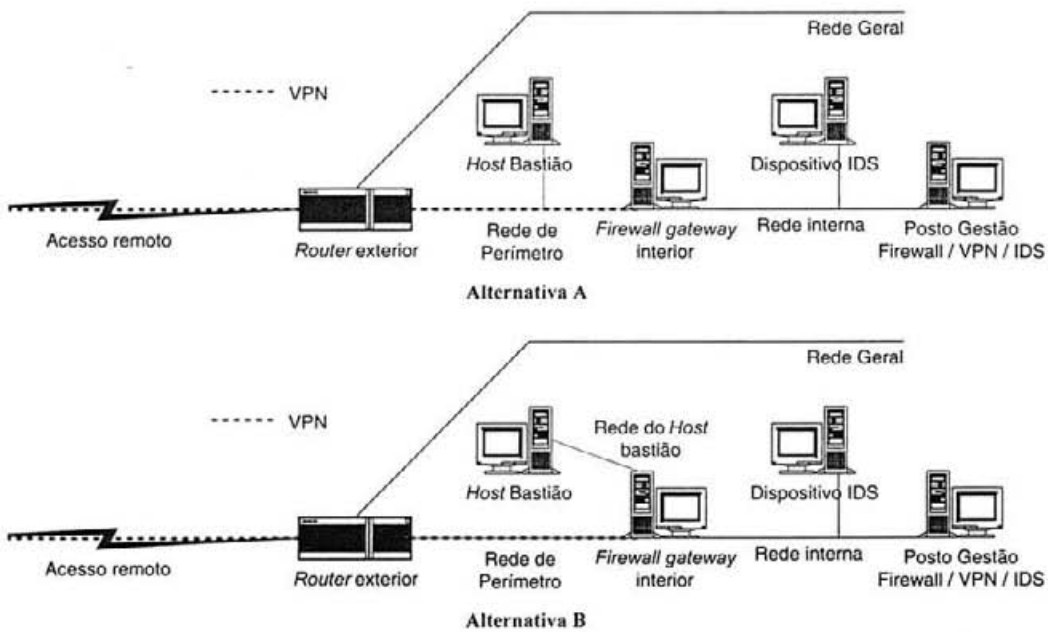


Figura 8.1 – Alternativas da Arquitectura do Sistema de Segurança

- Para assegurar os requisitos de privacidade das comunicações entre os segmentos da Rede Administrativa, são estabelecidas ligações cifradas *firewall* a *firewall*. São implementadas VPNs para a cifragem da linha a partir do *firewall gateway* interior, através das redes de perímetro e das linhas públicas de dados até ao *firewall gateway* interior do outro extremo.
- O dispositivo IDS (Intrusion Detection System), actuando com um interface de rede em modo promíscuo, detecta em tempo real todos os ataques conhecidos e implementa medidas para os terminar, desligando conexões e inclusive reconfigurando o *firewall gateway* ou o *router*, notificando o gestor de rede através de *pager*, *e-mail*, ou outro.
- O posto de gestão é um posto centralizado para a gestão do sistema com reconfiguração e gestão remota dos componentes que o permitam.

A arquitectura de *firewall*, baseada num *router* exterior (*hardware*), eficiente na filtragem do tráfego, e em *software* de *firewall* num *gateway* interior, com funções avançadas e enorme flexibilidade na gestão, permite obter uma arquitectura com dois componentes dife-

rentes mas complementares e que se salvaguardam mutuamente em caso de falha.

8.1.1 As Alternativas do Sistema de Segurança

A diferença entre as duas alternativas (Figura 8.1) está na posição do *host* bastião. Na alternativa "A" situa-se na rede de perímetro, na alternativa "B" situa-se numa segunda rede protegida ligada à terceira interface do *firewall gateway*, obtendo uma protecção reforçada.

A alternativa "A" representa a configuração base da arquitectura de *Firewall* de Subrede *Screened*, tem as vantagens de ser mais simples e permitir um maior desempenho do sistema.

A alternativa "B" acrescenta uma maior complexidade e reduz o desempenho do *firewall gateway* pelo facto de as ligações com destino ao *host* bastião serem recebidas num interface do *firewall gateway*, transmitidas para o *host* bastião, e a resposta deste novamente transmitida para o *firewall gateway* que a direcciona para uma das outras interfaces. Por outro lado a segurança do *host* bastião é salvaguardada em caso de comprometimento do *router* exterior, ficando o *host* bastião seguro pelo *firewall gateway*. Pelo facto do *host* bastião ficar mais seguro permite que, por exemplo, seja o servidor de um serviço com grandes requisitos de segurança como é o *e-mail*, e libertando assim um servidor para o efeito na rede interior.

Como a diminuição de desempenho introduzido no *firewall gateway* não é muito significativa, e o próprio desempenho não é uma prioridade pois o tráfego entre os segmentos da Rede Administrativa será de baixo débito, e ainda pelo facto da solução "B" acrescentar um factor de segurança ao sistema (no *host* bastião), que é o principal requisito da rede, conclui-se que a melhor alternativa arquitectónica é a "B".

8.1.2 Configurações Particulares

As características particulares das várias redes locais determinam algumas adaptações à solução de base descrita.

A ESMAE, por ser um estabelecimento de menor dimensão e não dispor do seu próprio servidor Unix para as aplicações administrativas, não justifica ter uma máquina IDS e o seu próprio servidor para os serviços da Internet (*host* bastião); opta-se assim por utilizar o *firewall gateway* para a disponibilização dos serviços da Internet aos clientes internos, e a execução de serviços (por exemplo o HTTP) será realizada pelo servidor do IDT.

As ESEIGs não justificam a arquitectura de *firewall* de base pois terão somente um ou dois postos cada na Rede Administrativa e não terão qualquer servidor. Como somente as sessões remotas para os servidores dos SC constituem pontos sensíveis a defender, opta-se por uma arquitectura mais simples mas que garante a segurança.

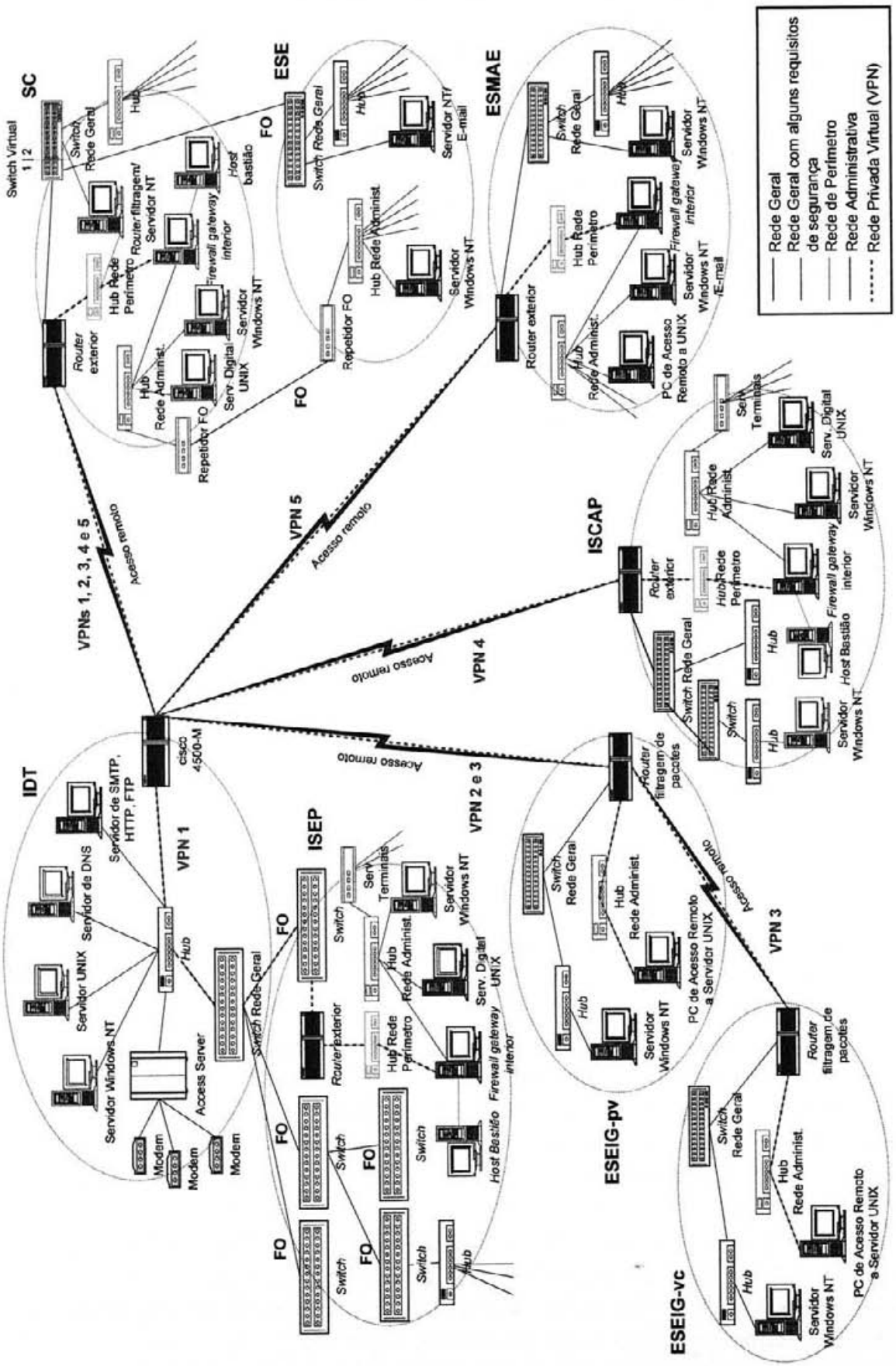


Figura 8.2 – Esquema Geral da Solução a Implementar

A arquitectura de *firewall* a adoptar nas ESEIGs baseia-se no *router* de filtragem de pacotes que efectuará a filtragem do tráfego. A cifragem da ligação, através de um *software* de cifragem de cliente remoto, irá até ao posto de acesso remoto. Como os postos de acesso remoto têm aqui um papel importante na cifragem e na autenticação opta-se por um sistema operativo mais seguro – o Windows NT.

Nos SC existe a situação particular de um segmento de rede geral com requisitos de segurança médios. Como é um segmento sem acesso aos alunos e por isso mais confiável poderá ser ligado à rede de perímetro através de um *dual-homed host*. Como o *host* bastião não fica situado na rede de perímetro este solução não constitui um problema. Este segmento de rede fica protegida pelo *router* de filtragem de pacotes e utilizará os serviços do *host* bastião, mas não terá qualquer acesso à Rede Administrativa pois a filtragem de tráfego do *firewall gateway* só permitirá o acesso aos serviços do *host* bastião.

Obviamente que a solução indicada para este segmento poderia passar pela sua ligação a uma interface suplementar do *firewall gateway*, no entanto o número elevado de postos a defender por aquele iria aumentar grandemente os custos do licenciamento do *firewall* e os requisitos de segurança do segmento não o justificam.

Visto que a ESE se situa no mesmo *campus* dos SC e por existirem duas fibras ópticas que a ligam aos SC, prolongam-se os dois segmentos de rede dos SC até à ESE, poupando-se recursos, deste modo.

8.2 Selecção das Ferramentas do Sistema de Segurança de Rede

Com base na arquitectura proposta em 8.1 e nas ferramentas tipo indicadas, é necessário efectuar a selecção das ferramentas de entre as do mercado que demonstrarem maior eficácia na resposta aos requisitos de segurança definidos para cada ferramenta tipo: *firewall*, VPN, e ferramenta de detecção de intrusões.

Devido à enorme variedade de ferramentas disponíveis dos tipos seleccionados, torna-se extremamente difícil, devido às limitações de tempo e recursos, efectuar uma análise e testes correctamente fundamentados com vista à selecção das melhores tendo por base os critérios definidos. Pelo que se optou por uma pesquisa de "Testes de Laboratório" efectuadas por revistas conceituadas na área das telecomunicações.

8.2.1 Teste de Laboratório de *Firewalls*

Seleccionámos os dois mais recentes "testes de laboratório" sobre *firewalls* da revista Data Communications – "Firewalls: Don't Get Burned" de Março de 1997 [NewDC97f], e "NT Firewalls: Tough Enough" de Abril de 1998 [NewDC98f] e um da revista Byte – "Firewall Software for NT and Unix" de Junho de 1997 [SeacBt97].

Apesar de o primeiro ser o mais abrangente relativamente ao número de *firewalls* participantes e à gama de sistemas operativos (o teste de Abril de 98 está restrito a *firewalls* NT e o de Junho a 6 *firewalls* Unix e 3 NT), o teste de Abril de 98 é o mais actual quer relativamente às ferramentas e metodologias de teste quer relativamente às versões mais actuais dos *firewalls*. Além disso, a maioria dos fornecedores para a plataforma Windows NT tem versões equivalentes para vários ambientes UNIX ou outros.

O teste de Abril de 98 será assim o teste de base à análise e os outros dois servem de termos de comparação. No anexo C.1 é descrito o teste de laboratório, nomeadamente os *firewalls* testados, a metodologia de teste, os resultados do teste, e as tabelas com os resultados dos três testes de laboratório.

8.2.1.1 A Escolha do Teste

Dois produtos mereceram a "escolha do teste": o Firewall-1 da Check Point Software Technologies e o Guardian da Netguard.

O Firewall-1 tem uma segurança excelente, bom desempenho, e uma óptima interface de gestão. Qualidades que colocam o Firewall-1 na posição da melhor opção. O produto é especialmente fácil de gerir remotamente. O *stateful inspection* permite configurar regras de acesso virtualmente para qualquer condição. Nos testes de desempenho obtém um lugar intermédio, talvez por o seu NAT[1] ser lento. No entanto, o desempenho é bem menos importante do que a segurança ou a gestão – e o *firewall*-1 é excelente em ambos.

A segurança, velocidade, e facilidade de gestão são as marcas de qualidade do Guardian. Combina *proxies* de aplicação e *stateful inspection*, e é bastante fácil de configurar. A sua interface é muito boa, permitindo efectuar facilmente as tarefas chave. Obteve também uma posição entre os mais rápidos no teste de desempenho.

No teste de Março de 97 (Tabela 10.5 no anexo C.1.4) foram classificados para a "escolha do teste" o Firewall-1 da Check Point Software Technologies, o Cyberguard Firewall da Cyberguard, o Watchguard Security Management System da Seattle Software Labs, e o Sunscreen EFS da Sun Microsystems.

No teste de Junho de 97 da revista Byte (Tabela 10.6 no anexo C.1.4), o CyberGuard Firewall obteve vantagem relativamente aos maiores competidores (Check Point FireWall-1 e AltaVista Firewall 97).

[1] *Network address translation* – mecanismo que esconde os endereços IP internos da rede externa de forma a não permitir aos atacantes a apreensão da topologia de rede [NewDC98f].

8.2.2 As Opções de *Firewall* Seleccionadas

Os critérios dos testes de laboratório (segurança, gestão e desempenho) são idênticos aos requeridos pelo caso em estudo, e pela mesma ordem já que à segurança é dada a maior importância e o desempenho, embora importante, é menos determinante. Considerando-se também a qualidade dos testes e as entidades conceituadas que os realizaram, os resultados dos testes podem ser uma óptima base para a selecção do *firewall*.

O Firewall-1 da Check Point Software Technologies ocupa as posições cimeiras em todos os testes, obtém a "escolha do teste" nos testes da Data Communication e somente é ultrapassado no teste da Byte por deficiências na configuração e gestão. Os resultados do teste de Abril de 98 demonstram que essas deficiências foram entretanto ultrapassadas. Desta forma pode concluir-se que a primeira opção é sem dúvida o Firewall-1 que é também o líder do mercado.

Outras opções, igualmente fiáveis e seguras são de considerar, como o Cyberguard Firewall que obteve a melhor classificação em dois dos testes, e o Netguard a melhor classificação no teste mais recente (resolveu os problemas detectados no teste de Março de 97. Na hipótese de surgirem constrangimentos de ordem técnica (no decorrer do estudo do caso) ou económica há a possibilidade de se considerar estas opções.

Os constrangimentos económicos poderão também ser importantes pois o custo das opções seleccionadas é substancial. Para o cálculo dos custos tomou-se como base os preços indicados nos testes de laboratório para uma LAN com 25 utilizadores que é o número de utilizadores, com uma margem de segurança, para cada segmento da Rede Administrativa.

Para uma LAN com 25 utilizadores o custo do Firewall-1 é de cerca de 550 contos, o Guardian custa cerca de 450 contos, enquanto o Cyberguard custa cerca 1.100 contos.

O Proxy Server ocupa nas condições económicas uma excelente posição. Para além de ter o preço mais baixo (cerca de 180 contos), é incluído no pacote Microsoft BackOffice que é adquirido pelo IPP para os servidores Windows NT, o que torna a sua utilização sem custos.

8.2.3 Teste de Laboratório de VPNs

Seleccionamos dois "testes de laboratório" sobre VPNs da revista Data Communications – "VPNs: Security With an Uncommon Touch" de Setembro de 1997 [ShaDC98v], e "VPNs: Safety First, But What About Speed?" de Julho de 1998 [NewDC98v], e um da revista Byte – "Extend Your Net with VPNs" de Novembro de 1997 [SterBt97].

De forma semelhante ao "teste de laboratório" de *firewalls* toma-se como referência a metodologia de teste da Data Communications. O teste de Setembro de 97 é mais abrangente relativamente ao número de produtos VPN e de soluções (*software* e *hardware-software*),

pelo que será a base da análise. O teste de Julho de 98 é dedicado somente a VPNs de *hardware-software*, e o teste da Byte de Novembro de 97 é dedicado a soluções de *software*. Com os três testes teremos assim termos de comparação para ambas as soluções.

No anexo C.2 é descrito o teste de laboratório, nomeadamente as VPNs testadas, a metodologia de teste, os resultados do teste, e as tabelas com os resultados dos três testes de laboratório.

8.2.3.1 A Escolha do Teste

Quatro produtos merecem a "escolha do teste": o Firewall-1 da Check Point Software Technologies, o Infocrypt Enterprise da Isolation Systems, o Sunscreen EFS da Sun Microsystems, e o Permit Security Gateway da Timestep.

O Check Point Firewall-1 tem-se salientado pela sua simples gestão de segurança, e agora estendeu essa facilidade às VPNs. Aos gestores de rede é possível configurar parâmetros VPN através da mesma interface utilizada para definir as regras do *firewall* – de facto, as regras do *firewall* são regras VPN. O Firewall-1 suporta todas as características VPN importantes, como o DES e o Triple DES; autenticação baseada em *token*; e autenticação IPSec e cifragem.

O Isolation da Infocrypt Enterprise é literalmente uma "caixa preta" – um produto de *hardware* fechado com funcionalidades de *firewall* e VPN integradas. A configuração do dispositivo e das VPNs é bastante simples. O *software* de gestão do Infocrypt para o Windows 95 e NT afixa todas as VPNs duma rede num único ecrã, e a selecção de qualquer dispositivo ou túnel disponibiliza informação como os parâmetros de rede e o tipo de cifragem utilizada. Utiliza o IPSec para autenticação e cifragem e permite a escolha entre o DES e o Triple DES.

O Sunscreen EFS da Sun Microsystems distingue-se pelo seu *software* cliente. Com o Sunscreen for Windows 95, mesmo utilizadores inexperientes conseguem facilmente utilizar VPNs. O produto testado não suporta configurações servidor-a-servidor. Funciona em ambiente Solaris e utiliza SKIP, autenticação MD5 e cifragem DES ou Triple DES.

O Permit Secure Gateway da Timestep é o único produto não *firewall* a merecer a escolha do teste. Entre os produtos que utilizam CAs, é o mais simples de configurar. A maioria dos parâmetros podem ser introduzidos no dispositivo, o que constitui uma grande poupança de tempo especialmente em redes grandes.

No teste de Julho de 98 da Data Communications (Tabela 10.9 no anexo C.2.4) as escolhas do teste foram ciPro-VPN da Radguard, que oferece uma segurança comprovada e funcionalidades de gestão para uma organização complexa, e o VSU 1010 da VPNet Technologies que oferece grande segurança e funcionalidades de gestão e foi o de melhor desempenho do teste.

No teste de Novembro de 97 da Byte (Tabela 10.10 no anexo C.2.4), o Aventail VPN impressiona pela sua flexibilidade, suporte extensivo de métodos de cifragem, e variedade de opções de autenticação.

Dois outros produtos tiveram uma óptima classificação: o FireWall-1 da Check Point e o Eagle NT da Raptor Systems. Ambas adicionam um nível extra de segurança ao integrarem funções VPN com a funcionalidade de *firewall*; desta forma é possível fornecer vários níveis de controlo de acesso ao utilizadores VPN uma vez autenticados.

8.2.4 As Opções VPN Seleccionadas

Com base nos mesmo critérios do teste de *firewalls* (segurança, gestão, e desempenho) a selecção da solução VPN só não é baseada numa análise mais profunda da segurança. O teste mais abrangente no número de soluções de *software* e de *hardware-software* só considerou uma análise da segurança e não o seu teste rigoroso. O teste de laboratório que o efectuou foi o de Julho de 98, também da Data Communications, mas estava restrito a soluções de *hardware-software*.

Considerando-se que os próprios fabricantes são as maiores autoridades na segurança dos dispositivos VPN, assume-se que esta estará à partida salvaguardada. No dia a dia, os erros de configuração e novos ataques são lugar comum, por isso os compradores devem considerar a segurança um processo contínuo e devem executar testes frequentes utilizando dispositivos de *scanning* e sistemas de detecção de intrusão [NewDC98v].

Relativamente a uma preferência entre as soluções de *software* e as de *hardware-software*, estas últimas têm uma vantagem clara no desempenho já que a cifragem efectuada em *software* é geralmente considerada muito lenta para ligações que operam a velocidades de 1.5 Mbit/s ou superior. No entanto, para o caso em estudo este problema não se coloca pois as necessidades de largura de banda para a Rede Administrativa não são exigentes. Por outro lado as soluções de *software* têm vantagem na flexibilidade de actualizações de novas versões e nos custos inerentes.

As conclusões a tirar dos resultados dos testes analisados são menos evidentes que no caso dos *firewalls*. No entanto destacam-se o Firewall-1 da Check Point com a "escolha do teste" no teste de Setembro de 97 e segundo lugar nos outros dois testes, neste caso não por ausência de funcionalidades ou questões técnicas, na comparação com as escolhas do teste, mas pela sua utilização ser mais acessível a profissionais. O Firewall-1 tem uma enorme vantagem para selecção como solução VPN, pois foi considerado como primeira opção para *firewall* e as funções complementares dos *firewall* e VPNs tornam-no uma solução integrada com vantagens irrefutáveis.

O Aventail VPN, a "escolha do teste" no teste de Novembro de 97 da Byte, teve uma excelente evolução relativamente à versão testada no teste de Setembro de 97 e poderá ser

considerado também uma excelente opção de VPN.

Das soluções de *hardware-software* o ciPro-VPN da Radguard e o VSU 1010 da VPNet Technologies foram os que se destacaram no teste de Julho de 98 tendo sofrido uma nítida evolução relativamente ao teste de Setembro de 97. Constituem óptimas alternativas, principalmente num cenário com grandes requisitos de desempenho.

O custo da licença do componente de VPN do Firewall-1 para uma rede de 25 postos é de cerca de 200 contos, e o custo do Aventail VPN é de cerca de 1.450 contos. Das soluções de *hardware-software* o ciPro-VPN custa cerca 1.500 contos e o VSU 1010 cerca de 1.380 contos.

Apesar do componente de VPN do Firewall-1 ter um custo bastante acessível, uma solução sem custos seria, pelas mesmas razões do *firewall* Microsoft Proxy 2.0, o Microsoft Routing and Remote Access Service, mas que na versão actual não oferece ainda funcionalidades VPN e características técnicas consideradas mínimas (ver teste da Byte – Tabela 10.10 anexo C.2.4).

8.2.5 Teste de Laboratório de Sistemas de Detecção de Intrusão

Para a selecção de um sistema de detecção de intrusões (IDS) seleccionamos os "testes de laboratório": "Intrusion Detection Systems: Suspicious Finds" de Agosto de 1998 da revista Data Communications [NewDC98i], e "Network intrusion-detection solutions" de Maio de 1998 da revista InfoWorld [BroIW98i]; e várias análises individuais de produtos IDS da revista PCWeek do 1° semestre de 1998 [KenPW98a; KenPW98a; SurPW98a; SurPW98b].

Pelas vantagens da abordagem na rede relativamente à de *host*, referidas em 6.4.4, e por no sistema em estudo se pretender defender uma rede constituída por segmentos locais delimitados por *firewalls* e por segmentos públicos cifrados, a opção por um sistema IDS baseado na rede parece ser mais adequada.

Toma-se como referência o teste da Data Communications por testar as versões mais actuais dos produtos IDS. Ambos os *labs* efectuaram testes pormenorizados à capacidade de detecção e resposta de ataques dos IDSs bem como outras características relevantes. Com as várias análises individuais de produtos IDS obtém-se um termo de comparação adicional.

8.2.5.1 A Escolha do Teste

O teste da Data Communications considerou o Netranger da Cisco e o RealSecure da ISS as melhores soluções IDS. No entanto, evidenciando a importância dos aspectos de segurança – a detecção de ataques, que constitui o requisito principal para o caso em estudo, considera-se que, com base nos resultados do teste, as soluções RealSecure da ISS e o Flight Jacket da Anzen constituem as melhores soluções (Tabela 10.12 e Tabela 10.13 no anexo

C.3.4). Os custos beneficiam também estas duas opções.

O RealSecure oferece a melhor relação de potencialidades de configuração e de grande facilidade de utilização dos IDS testados. O produto inclui centenas de assinaturas de ataques pré-configurados e permite a definição de novas assinaturas de ataques. Tem uma interface de utilizador eficiente e simples, e pode reconfigurar dinamicamente o Check Point Firewall-1 ou *routers* Cisco para filtrar tráfego de uma dada origem, em resposta a um ataque. A versão em produção 2.1 falhou dois dos ataques em teste, mas a versão beta 2.5 detectou-os.

O Flight Jacket não é instalado com muitas assinaturas de ataques pré-configuradas. No entanto, a linguagem de *scripting* Ncode, torna-o extremamente versátil em termos da detecção de virtualmente qualquer assinatura conhecida. Mas para isso, existe muita programação e especialização de segurança associado ao Flight Jacket. A interface gráfica baseada em Java precisa ainda de ser melhorada, mas isso é compensado pelo seu desempenho: foi o melhor produto com os tráfegos mais pesados.

No teste de Maio de 98 da InfoWorld (Tabela 10.15 no anexo C.3.4) evidenciaram-se também o RealSecure da ISS e o Flight Jacket da Anzen. O Flight Jacket foi a melhor solução na detecção de ataques tendo obtido excelentes resultados, o RealSecure foi o que obteve melhores resultados na correcta identificação e resposta aos ataques e nas ferramentas de relatório.

8.2.6 As Opções de Sistema de Detecção de Intrusões Seleccionadas

Com base nos resultados dos testes e nos critérios de segurança, gestão, e desempenho, a selecção da solução IDS deverá ser entre o RealSecure da ISS e o Flight Jacket da Anzen, as melhores soluções nas pontuações alcançadas, em particular nos aspectos de segurança, tendo sido as "escolhas do teste".

A solução IDS mais equilibrada e poderosa nos vários critérios é o RealSecure da ISS. Tem evoluído no decorrer das várias versões nos aspectos de detecção de ataques, atingindo um excelente nível na versão 2.5 pelo que será esta versão a indicada para selecção.

O Flight Jacket da Anzen é também uma excelente solução e será uma segunda opção. Menos forte nos aspectos de gestão, mas bastante eficiente nos da detecção de ataques, tem vantagem particular na questão dos custos.

Para um universo de postos a defender, no caso em estudo, de cerca de 25 em cada LAN, os custos do Flight Jacket são de cerca de 1.000 contos enquanto o RealSecure custará cerca de 1.600 contos.

Se existirem constrangimentos económicos, uma solução de baixo custo será o SessionWall-3 que custa cerca de 270 contos. Tem capacidades multifacetadas, efectuando audi-

toria, detecção de intrusões e más utilizações, bloqueia viroses de *e-mail* e *applets* perigosos. Evidenciou algumas limitações na detecção de ataques e nas facilidades de configuração, mas relativamente ao primeiro aspecto foi prejudicado por ter sido fornecido numa plataforma de teste de desempenho limitado, justificando-se desta forma ser também uma boa solução.

8.2.7 Constrangimentos e Requisitos Técnicos

Seleccionadas as melhores opções das ferramentas do sistema de segurança, tendo em linha de conta requisitos gerais de segurança, funcionalidades e gestão, e desempenho, é agora necessário analisar a existência de possíveis constrangimentos técnicos entre as ferramentas seleccionadas para a configuração do sistema, bem como requisitos técnicos mais específicos.

Principalmente a combinação de *firewall* e VPN requer uma cuidada análise devido à complementaridade mas também sobreposição de funções e a necessidade de gestão comum para uma segurança mais efectiva. A solução de *firewall* e VPN do Firewall-1 da Check Point constitui a melhor opção, no entanto um requisito técnico introduziu um novo factor na selecção: o tamanho da chave de cifragem.

Conforme descrito na secção 3.2.4, os EUA impõem actualmente fortes restrições à exportação da cifragem, 56 bits para o tamanho das chaves DES e 40 bits para as restantes. No entanto esta cifragem não garante os requisitos mínimos de segurança pois como foi descrito estas chaves foram já quebradas.

A capacidade da cifragem VPN é especialmente importante pois estará sujeita a ataques do exterior e poderá por em causa a confidencialidade e integridade da informação. Pelo que se equacionou a selecção de uma alternativa VPN à primeira opção (Firewall-1 VPN) que garantisse uma capacidade de cifragem pelo menos correspondente ao Triple DES que corresponde a uma capacidade real de 112 bits. Com esta capacidade de cifragem obtém-se uma perspectiva de médio prazo quanto à eficácia da segurança da chave.

A melhor solução está na pesquisa de produtos provenientes de países não sujeitos a essas restrições e se possível dentro da gama de opções seleccionadas. Desta forma, efectuou-se a pesquisa das capacidades de cifragem do *firewall* e VPN Guardian da Netguard Ltd. (Migdal Ha-Emek, Israel), e das VPNs CIPro da Radguard Ltd. (Tel Aviv, Israel), e Permit Security Gateway da Timestep Corp. (Ontário, Canadá). Como a própria Check Point, fornecedora do Firewall-1, é sediada em Israel e foi também inquirida.

Tendo-se aprofundado a informação técnica acerca das capacidades de cifragem e mesmo contactado por *e-mail* (anexo C.4) as sedes das organizações obtiveram-se os seguintes resultados:

- O Guardian é exportado com o Triple DES e o RC4 de 128 *bits*, no entanto como a

sua cifragem é baseada no CryptoAPI do Windows NT que está sujeito a restrições de exportação, fica restrito a chaves de tamanho máximo de 48 *bits* RC4.

- O CIPro é exportado com o Triple DES, bastando para isso uma autorização do governo Israelita para a organização que utilizar o produto.
- O Permit Security Gateway é exportado com o Triple DES.
- O Firewall-1 actualmente é exportado nas opções de 48 *bits* FWZ-1 ou 56 *bits* DES. No entanto, a Check Point prevê começar a disponibilizar o Firewall-1 com cifragem Triple DES de 168 bits a partir de Outubro de 98. É necessária uma autorização do governo Israelita.

8.2.8 As Ferramentas Seleccionadas

Com o aumento do tamanho da chave de cifragem do Firewall-1 reúnem-se os requisitos para a sua selecção como uma solução integrada *firewall* e VPN, permitindo uma mais eficiente gestão do sistema.

Para o componente de detecção de intrusões, a ferramenta seleccionada é o Real Secure da ISS, partindo-se do princípio que o preço não constituirá um constrangimento. A sua capacidade de reconfiguração do Firewall-1 e de *routers* Cisco aumenta a integração do sistema de segurança de rede e as capacidades de gestão do sistema de segurança de rede.

8.3 A Auditoria do Sistema de Segurança de Rede

Por mais seguro que seja um sistema de segurança de rede, é necessário efectuar auditorias de segurança periódicas para a verificação da existência de falhas de segurança ou erros de configuração nos *firewalls*, servidores, *routers* e restantes componentes da rede.

A auditoria de segurança da rede faz a verificação de quão segura ou insegura é uma rede. Efectuar auditorias regulares da segurança dos sistemas de uma rede e o conhecimento e disponibilização da informação relativa às novas falhas de segurança detectadas constitui a melhor defesa para prevenir e enfrentar os riscos de segurança

As ferramentas de *scanning* permitem efectuar a auditoria de segurança que tem por objectivo informar a localização das vulnerabilidades, o seu grau de severidade, e o que é necessário efectuar para as resolver.

A disponibilização de uma ferramenta de *scanning* permite por um lado validar a solução de segurança de rede antes do início da sua exploração, e por outro lado efectuar verificações periódicas para manter a integridade do sistema de segurança de rede. Constitui assim uma ferramenta complementar ao sistema de segurança de rede definido.

8.3.1 A Selecção da Ferramenta de Auditoria de Segurança

Para a selecção da ferramenta de auditoria de segurança seleccionámos os testes de laboratório: "Holy Intruders!: IP-Based Security Auditing Tools" de Julho de 1998 da revista Network Computing [ShiNC98], "Network security checkup" de Maio de 1998 da revista InfoWorld [BroIW98s], e "Beating back the hackers" de Outubro de 1997 da revista Network World [KatNW97].

Por ser o artigo que efectuou o teste comparativo das ferramentas mais pormenorizado e também por ser o mais recente, toma-se como referência o teste da revista Network Computing.

8.3.1.1 A Escolha do Teste

O Internet Scanner recebeu a escolha do teste por uma simples razão: encontrou as falhas que se esperava encontrar e detectou algumas que eram desconhecidas para a equipa do teste, de forma mais precisa do que os outros *scanners*. Inclui o conjunto mais completo de verificações do NT, e verifica também as *passwords* que podem ser facilmente adivinhadas. Tem também uma gama ampla de verificações UNIX, testes IP de baixo nível e algum conhecimento de falhas VAX/VMS. Consiste em três módulos integrados para o *scanning* de *intranets*, *firewalls*, e servidores *web*. O Internet Scanner é um produto completo e bem desenvolvido.

No entanto, como os outros produtos, tem também os seus defeitos, incluindo algumas falhas de segurança não detectadas e um processo de actualização não automático e lento.

Entretanto, a ISS lançou já as actualizações 5.0.1 e 5.2, tendo resolvido alguns *bugs* e introduzido novas funcionalidades: 40 novas verificações de vulnerabilidades, novos relatórios de gestão e um sistema de actualização automática de informação que verifica a versão correcta da base de dados e se estão carregados os últimos serviços e vulnerabilidades, efectuando uma série de actualizações incrementais se for necessário.

De igual forma, nos outros dois testes o Internet Security Systems é considerado a melhor solução. Utilizando uma lista de vulnerabilidades detalhada e completa, o que não é demonstrado por qualquer dos outros produtos.

8.3.2 A Ferramenta de Auditoria de Segurança Seleccionada

Com base nos resultados dos testes a solução de auditoria de segurança deverá ser o Internet Security Systems da ISS.

De salientar no entanto que o teste da InfoWorld [BroIW98s] (ver anexo C.5.3) recomenda a utilização quer de ferramentas de segurança de rede quer de segurança do *host*, para obter

uma imagem correcta da segurança da rede durante a auditoria, obtendo-se uma perspectiva global da segurança mais completa. Como o objecto do presente trabalho é o de propor uma solução numa perspectiva de segurança de rede, deixa-se em aberto a utilização de uma ferramenta adicional de auditoria de *host* (na secção 8.5 analisam-se os aspectos de segurança de *host*).

Para o universo de postos do caso em estudo (cerca de 25 em cada LAN) os custos do Internet Security Scanner são de cerca de 900 contos.

Na possibilidade de existirem constrangimentos económicos, o SessionWall-3 (ver teste de detecção de intrusões no anexo C.3) embora não tendo sido testado em nenhum dos testes de auditoria de segurança, tem capacidades multifacetadas, efectuando auditoria, detecção de intrusões e más utilizações. Embora tendo algumas limitações em ambas as áreas constitui uma solução de baixo custo, cerca de 270 contos para cada LAN de 25 utilizadores.

8.4 A Plataforma/Sistema Operativo do Sistema

Sem entrar numa análise de qual o melhor sistema operativo, é necessário indicar qual o que terá mais vantagens para o caso em estudo. Devido a inegáveis vantagens de gestão, será sempre conveniente ser o mesmo SO para as várias ferramentas do sistema de segurança de rede bem como para a ferramenta complementar de auditoria.

O Firewall-1 da CheckPoint tem soluções para Windows NT, Solaris, SunOS, HP-Unix e IBM-AIX. O RealSecure da ISS permite a alternativa entre o Windows NT e o Solaris. A ferramenta de *scanning* Internet Security Scanner da ISS tem soluções para Windows NT, Solaris, SunOS, HP-Unix, IBM-AIX e Linux. Os sistemas operativos comuns nas várias ferramentas são o Windows NT e o Solaris.

Por ser o sistema operativo mais utilizado na rede em estudo e por ser o ambiente com maiores perspectivas de utilização generalizada e por isso maiores garantias de suporte técnico, o Windows NT é a opção seleccionada.

8.5 Pontos de Vulnerabilidade na Segurança de *Host* e Física

O nível de segurança que a solução de segurança de rede proposta permite atingir pode ser comprometido com deficiências na segurança do *host* e mesmo na segurança física.

Analisando o tipo de utilizadores da Rede Administrativa – essencialmente pessoas com reduzidos conhecimentos de informática e pouca sensibilidade para os problemas da segurança – podemos concluir que a segurança da rede poderá ficar comprometida por situações não detectadas pelas ferramentas do sistema de segurança de rede, do género:

- Confidencialidade das *passwords* não garantida pela sua anotação ou descuido.
- Transmissão das *passwords* a terceiros mesmo que de forma não intencional.
- Disponibilização dos postos de trabalho a terceiros com sessões autenticadas.
- Etc.

Para uma rede com elevados requisitos de segurança a opção por uma solução *smart card*, permitiria a resolução dos problemas descritos, introduzindo as características de segurança adicionais para uma elevada segurança de *host*: certificados digitais e pares de chaves pública/privada. Existem várias alternativas comerciais como a SecurID da Security Dynamics (suportada pelo Firewall-1), a NetSign da Litronic. Cada *smart card* tem um custo médio de cerca de 25 contos.

Outra alternativa será um dispositivo biométrico, por exemplo por impressões digitais, também com soluções comerciais disponíveis como é o caso do Digital Persona U.are.U e o Sony Fingerprint Identification Unit. Estes dispositivos têm um custo médio de cerca de 25 contos cada.

Analisando as condições da segurança física da rede, não se colocam problemas da importância dos descritos acima relativos à segurança do *host*. Passa pela intervenção dos gestores de rede a implementação de regras de segurança física como a localização e acesso aos servidores da rede, *firewalls* e elementos activos de rede; a manutenção de *backups* do sistema e dados em locais seguros e afastados da localização dos servidores; etc. A relativa falta de segurança dos postos de trabalho, sendo menos sensível por não guardarem dados importantes, poderá ser colmatada pela utilização dos dispositivos *smart cards* ou biométricos.

Finalmente, a hipótese deixada em aberto na secção anterior da utilização de uma ferramenta de auditoria de segurança baseada no *host* (ver anexo C.5.3), permite reforçar a segurança de rede, detectando as falhas de segurança de *host*. Uma boa alternativa para a ferramenta de auditoria de *host* pode ser o Enterprise Security Manager (ESM) da Axent Technologies (referenciado no teste de ferramentas de auditoria de segurança, anexo C.5) e que tem o custo de cerca de 600 contos para um gestor e dois agentes, um para NT e outro para Unix.

8.6 O Teste da Solução Proposta

O objectivo do estudo nesta secção é o de descrever a implementação de uma plataforma de teste da arquitectura de segurança e de propor uma metodologia de teste da solução a adoptar, e implementar e descrever os testes a realizar.

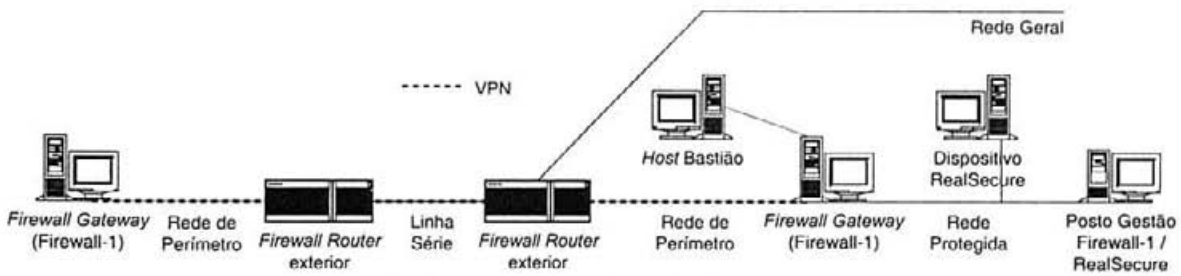
A realização dos testes permitirá a validação da solução implementada pela utilização da ferramenta complementar de *scanning* de segurança, a simulação de alguns ataques de vários tipos e o teste da solução num ambiente de exploração mais prolongado.

8.6.1 A Plataforma de Teste

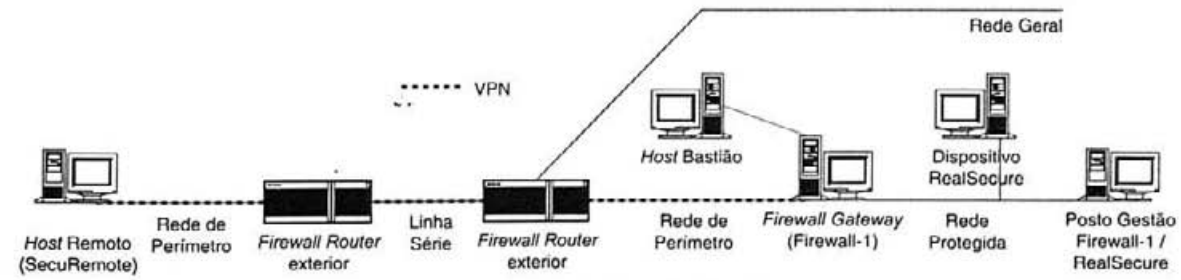
Para poder ser realizado o teste da solução de segurança de forma mais conveniente, foram reunidos os componentes necessários para recriar a arquitectura da solução de segurança numa infra-estrutura de rede independente da rede em exploração, sem interferir assim com o seu funcionamento normal.

Definiram-se duas configurações de teste (Figura 8.3) que permitem testar as arquitecturas de segurança com VPN *firewall* a *firewall* (entre SC e ISEP, ISCAP e ESMAE) e com VPN *firewall* a *host* remoto (entre SC e ESEIG-pv e ESEIG-vc). Os componentes utilizados são os seguintes:

- *Routers* exteriores – Cisco 2503 interligados por um cabo série, simulando uma WAN a 2 Mbit/s.
- *Firewall Gateway* (da rede principal), *Host* Bastião e Dispositivo RealSecure – Dell PowerEdge 2300 com Pentium II a 350 MHz e 128 Mbytes de RAM, e Windows NT 4.0.
- *Host* Remoto/*Firewall Gateway* (da segunda rede) – Dell Optiplex GX1 com Pentium II a 330 MHz e 64 Mbytes de RAM, e Windows NT 4.0.
- Posto de Gestão – CHIPT7 Pentium II 266 MHz e 64 Mbytes de RAM.



Configuração com VPN *Firewall* a *Firewall*



Configuração com VPN *Firewall* a *Host* Remoto

Figura 8.3 – A Plataforma de Teste

8.6.2 A Metodologia de Teste

A metodologia de teste baseia-se na implementação faseada de um conjunto de operações para a validação da solução de segurança e, com base nos resultados obtidos, concluir se a solução corresponde aos requisitos de segurança propostos.

Começando-se pela implementação da plataforma de teste (Figura 8.3) baseada na arquitectura de segurança proposta, recria-se numa rede de laboratório as combinações possíveis a encontrar na rede do caso em estudo, incluindo a instalação de versões de demonstração das ferramentas seleccionadas.

O passo seguinte será a configuração dessas ferramentas, tirando partido das suas capacidades de reforço da segurança. Com a ferramenta *firewall*/VPN a implementação das regras de segurança, a selecção dos mecanismos de autenticação, e a configuração do esquema de cifragem e mecanismo de troca de chaves nas VPNs. Com os *routers/firewalls* a implementação das regras de filtragem de pacotes de forma articulada com os *firewalls gateways*. E com a ferramenta de detecção de intrusões a configuração e activação do sistema na detecção de todos os tipos de ataque conhecidos por este.

Com a plataforma de teste instalada e configurada utiliza-se a ferramenta de auditoria de segurança no *scanning* exaustivo aos serviços de rede e configurações do sistema operativo das máquinas sensíveis da rede, nomeadamente máquinas *firewall*, *host* bastião, máquina IDS e posto de gestão (na rede real seria necessário auditar também os servidores da rede protegida).

O passo seguinte na validação da solução será a simulação de alguns ataques dos vários tipos e analisar o comportamento da segurança do sistema. E também a capacidade de resposta das ferramentas IDS e de auditoria numa situação de algum novo ataque que entretanto possa surgir.

E finalmente, presumindo-se satisfatórios, os resultados dos testes anteriores indicam o teste da solução num ambiente de exploração mais prolongado que precederá a aceitação final da solução de segurança.

9. Conclusões

Devido aos constrangimentos do tempo disponível para a realização da tese, os testes propostos no final do capítulo 8 (secção 8.6) da solução de segurança proposta, só poderão ser realizados após a entrega da dissertação, no trabalho a prosseguir no contexto do problema de segurança da Rede Administrativa do IPP. Espera-se vir a documentar esses resultados logo que disponíveis.

No entanto, poderão desde já ser tiradas conclusões relativamente ao problema em estudo – a segurança de uma subrede de computadores que se distribui por uma WAN. Foram estudadas soluções de segurança – arquitecturas de *firewalls*, VPNs, ferramentas de detecção de intrusões e de auditoria, e sistemas evoluídos de autenticação ao nível do *host*. Todos eles tendo na sua base diversos protocolos de segurança e uma tecnologia com grandes desenvolvimentos e forte aposta da investigação, e de enorme relevo na confidencialidade e integridade da informação na computação – a cifragem da informação e os mecanismos associados de autenticação (com chaves privadas e as assinaturas digitais). Efectuou-se assim, com base neste estudo, uma proposta de arquitectura de solução a adoptar, e uma selecção de ferramentas comerciais fundamentada em testes de laboratório exaustivos de publicações conceituadas.

A arquitectura da solução proposta reuniu o conjunto de ferramentas consideradas mais eficazes na protecção da rede, mantendo a conectividade – o *firewall*, a rede privada virtual (VPN) e o sistema de detecção de intrusões (IDS). Uma ferramenta complementar foi também proposta, de auditoria de segurança, que permite validar as configurações de segurança a nível do sistema operativo, *firewalls* e *routers*.

Os testes de laboratório, que incidiram sobre a segurança, facilidade de configuração e desempenho, garantem as funcionalidades e capacidade de resposta das ferramentas testadas, com especial realce a segurança. De salientar a simulação de ataques reais efectuados com base na protocolo IP e que obtiveram excelentes prestações das ferramentas mais avançadas.

No entanto, o teste *in loco* da arquitectura proposta numa implementação de rede simulando o caso em estudo é importante. É necessário testar o comportamento das ferramentas no seu conjunto e de acordo com as características particulares da rede e, bastante importante, a eficácia dos mecanismos de segurança. O primeiro aspecto perspectiva-se que não constitua problema devido à complementaridade das ferramentas e características de funcionamento; o *firewall* e VPN operam em conjunto e a ferramenta IDS actua em modo passivo. Relativamente à eficácia dos mecanismos de segurança, os bons resultados individuais obtidos nos

testes de laboratório pelas ferramentas isoladamente e com base também na complementaridade das ferramentas garantem à partida a reunião das suas capacidades de segurança. O teste da solução será ainda assim aconselhável.

Como conclusão final deve referir-se que a segurança de rede mais do que uma excelente solução encontrada em determinado momento, é um processo contínuo de constante actualização relativamente às novas realidades tecnológicas das redes e aos novos ataques de rede. Não se compadece com soluções baseadas em ferramentas não profissionais e que não sejam intensivamente testadas, pois o completo domínio das várias áreas de vulnerabilidade dos sistema e redes e a constante actualização da gama de novos ataques é vital para o sucesso na implementação da segurança de rede.

III

III. Apêndices

A. Técnicas de Cifragem

1. O DES

O esquema de cifragem mais largamente utilizado é definido no Data Encryption Standard (DES) adoptado desde 1977 pelo NIST (National Institute of Standards and Technology), como FIPS PUB 46. O NIST recomenda o uso do DES para aplicações que não visem a protecção de informação classificada [Stall94a].

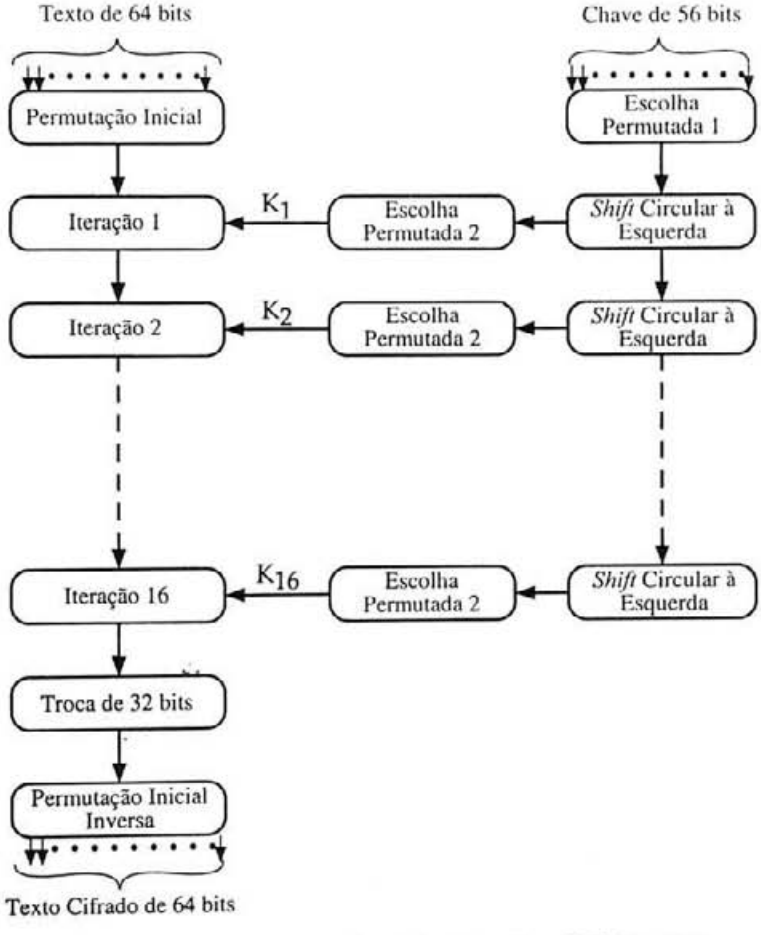


Figura 10.1 – Descrição Geral do Algoritmo DES [Stall95]

O esquema para a cifragem DES está ilustrado na Figura 10.1. Tal como em qualquer esquema de cifragem, existem duas entradas para a função de cifragem: o texto corrente a ser cifrado e a chave. Neste caso, o texto deve ter tamanho 64 *bits* e a chave 56 *bits*.

1.1 Cifragem

O processamento do texto corrente realiza-se em três fases. Em primeiro lugar, o texto de 64 *bits* passa por uma permutação inicial (IP) que rearranja os *bits* para produzir o *input permutado*. A isto segue-se uma fase que consiste em 16 iterações da mesma função. O *output* da última iteração consiste em 64 *bits* que é uma função do texto corrente de *input* e da chave. As metades esquerda e direita do output são trocadas para produzir o *preoutput*. Finalmente, o *preoutput* sofre uma permutação (IP^{-1}) que é a inversa da função da permutação inicial, para produzir o texto cifrado de 64bits.

A porção do lado direito da Figura 10.1 mostra a forma pela qual a chave de 56 *bits* é utilizada. Inicialmente, a chave é passada através de uma função de permutação. Depois, por cada uma das 16 iterações, é produzida uma subchave (K_i) pela combinação de um *shift* circular à esquerda e uma permutação. A função de permutação é a mesma para cada iteração, mas gera uma subchave diferente por causa do *shifting* repetido dos *bits* da chave.

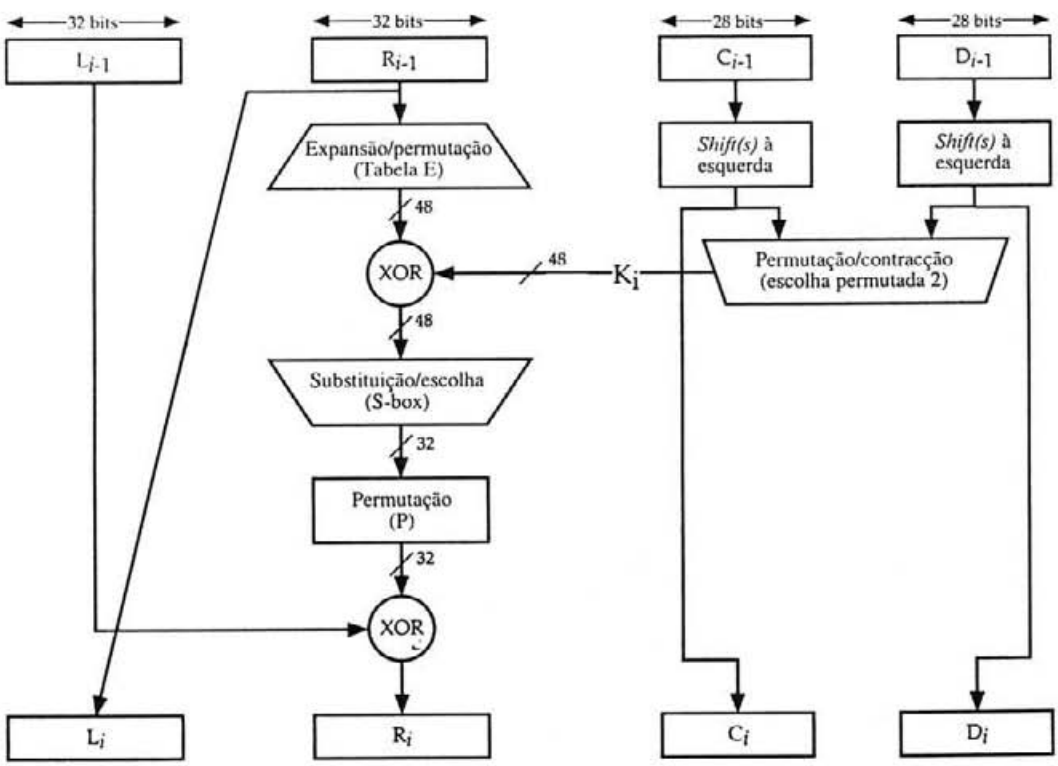


Figura 10.2 – Iteração do Algoritmo DES [Stall95]

A Figura 10.2 descreve mais em pormenor o algoritmo para uma só iteração. O *input* permutado de 64 *bits* passa por 16 iterações, produzindo um valor intermédio de 64 *bits* no final de cada iteração. As metades esquerda e direita de cada valor intermédio de 64 *bits* são tratadas como quantidades de 32 *bits* separadas, designadas por L (left) e R (right). O processamento total de cada iteração pode ser sumariado nas fórmulas seguintes:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \text{ Ø } f(R_{i-1}, K_i)$$

onde Ø representa a função XOR (OU exclusivo).

O *output* do lado esquerdo de uma iteração (L_i) é igual ao *input* do lado direito dessa iteração (R_{i-1}). O *output* do lado direito (R_i) é o OU exclusivo de L_{i-1} e uma função complexa f de R_{i-1} e K_i. Esta função complexa envolve permutações e operações de substituição. As operações de substituição são representadas por tabelas designadas *S-boxes*, que mapeiam cada combinação de 48 *bits* de *input* numa de 32 *bits*.

Na Figura 10.2 vemos que a chave de 56 *bits* utilizada como *input* do algoritmo é inicialmente sujeita a uma permutação. A chave de 56 *bits* resultante é depois tratada como duas quantidades de 28 *bits*, designadas C_0 e D_0. Em cada iteração, C e D são sujeitas separadamente a um *shift* circular à esquerda de 1 ou 2 *bits*. Estes valores servem como *input* para a próxima iteração e para outra função de permutação, que produz um *output* de 48 *bits* que serve como *input* para a função f (R_{i-1}, K_i).

1.2 Decifração

O processo de decifração no DES é essencialmente o mesmo do processo de cifragem. A regra é a seguinte: utilizar o texto cifrado como *input* do algoritmo DES, mas utilizar as chaves K_i em ordem inversa, quer dizer, utilizar K_{16} na primeira iteração, K_{15} na segunda iteração, e assim sucessivamente.

1.3 O Poder do DES

Desde a sua adopção como *standard*, tem havido preocupações prolongadas sobre o nível de segurança providenciado pelo DES. Estas preocupações são de dois tipos: a natureza do algoritmo e o tamanho da chave.

Durante muitos anos, a preocupação mais importante era a possibilidade de explorar as características do algoritmo do DES para efectuar criptanálise. O foco da preocupação eram as oito tabelas de substituição, ou *S-boxes*, que são utilizadas em cada iteração. Porque o critério do projecto destas caixas, e mesmo de todo o algoritmo, nunca foram tornados públicos, existe a suspeita de que as caixas foram construídas de forma que a criptanálise é possível para um oponente que saiba a fraqueza nas *S-boxes*. Ao longo dos anos têm sido descobertas um número de regularidades e comportamentos inesperados das *S-boxes*. A despeito disto, ninguém até agora foi bem sucedido na descoberta da suposta fraqueza fatal das *S-boxes*.

À medida que os avanços nas técnicas criptanalíticas têm ocorrida, a força subjacente do algoritmo DES tornou-se mais aparente. Não foi ainda publicado nenhum método de ataque prático ao DES. Dado que o algoritmo sobreviveu a anos de exame rigoroso, é provavel-

mente seguro dizer que o DES é um dos mais fortes algoritmos de cifragem já idealizados.

A maior preocupação actual é o tamanho da chave. Com um tamanho da chave de 56 *bits*, existem 2^{56} chaves possíveis. Em face disto, um ataque de força bruta parece impraticável. Assumindo que em média metade do espaço das chaves tem de ser pesquisado, uma só máquina efectuando uma cifragem DES por micro-segundo levará mais de mil anos a quebrar a cifra[1].

No entanto, a assumpção de uma cifragem por micro-segundo é bastante conservadora. Uma análise rigorosa do problema foi feita por [Wiener93] e é baseada na assumpção que o atacante tem pelo menos um par (texto corrente, texto cifrado).

[Wiener93] propõe o projecto de um *chip* que usa técnicas de *pipeline* de forma a obter um factor de pesquisa de chaves de 50 milhões de chaves por segundo. Utilizando custos de 1993, desenhou um módulo que custa $100,000 (dólares americanos) e contém 5.760 *chips* de pesquisa de chaves. Com este desenho, foram obtidos os seguintes resultados:

Custo da Máquina de Pesquisa de Chaves	Tempo de Pesquisa Esperado
$100,000	35 horas
$1,000,000	3.5 horas
$10,000,000	21 minutos

Tabela 10.1 – Resultados do Estudo de [Wiener93]

O desenho de [Wiener93] representa o culminar de anos de pesquisa sobre a segurança do DES e pode ter sido um ponto de viragem. Nesta altura ainda parece razoável confiar no DES para aplicações pessoais e comerciais. Mas este tempo permitiu investigar alternativas para a cifragem convencional. Duas das mais promissoras candidatas para a substituição do DES são o Triple DES e o IDEA.

2. IDEA

O IDEA (International Data Encryption Algorithm) é um algoritmo de cifragem convencional orientado ao bloco, desenvolvido em 1990 por [LaiMas90]. Foi apresentada uma versão revista do algoritmo [LaiMas91], desenhada para fazer frente aos recentes avanços nos ataques criptanalíticos.

O esquema global da cifragem IDEA está ilustrado na Figura 10.3. O IDEA é um cifrador de bloco que utiliza uma chave de 128 *bits* para cifrar dados em blocos de 64 *bits*.

[1] Como é demonstrado na secção 0 (O Poder do RSA) existem formas de contrariar esta afirmação.

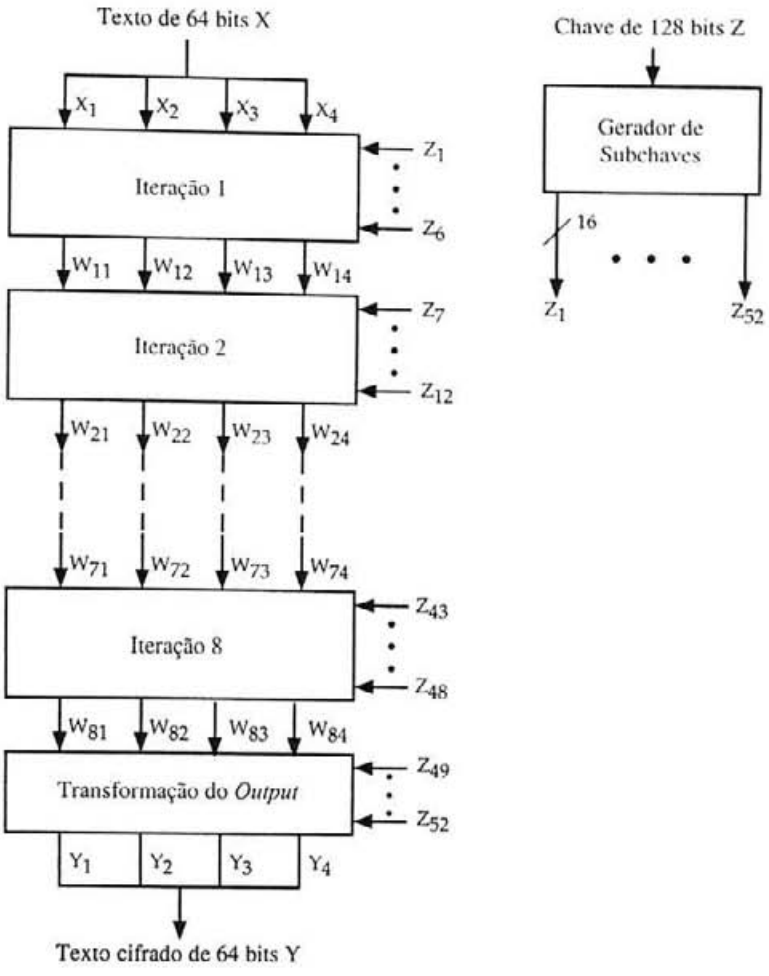


Figura 10.3 – Esquema Geral do IDEA [Stall95]

2.1 Iterações

O algoritmo IDEA consiste em oito iterações, seguidas por uma função de transformação final. O algoritmo divide o bloco de *input* em quatro subblocos de 16 *bits*. Cada uma das iterações utiliza quatro subblocos de 16 *bits* de *input* e produz quatro blocos de 16 *bits* de *output*. A transformação final também produz quatro blocos de 16 *bits*, os quais são concatenados para formar o texto cifrado de 64 *bits*. Cada uma das iterações também utiliza seis subchaves de 16 *bits*, enquanto a transformação final utiliza quatro subchaves, para um total de 52 subchaves. O lado direito da Figura 10.3 indica que essas 52 subchaves são geradas da chave de 128 *bits* original.

Cada iteração do IDEA utiliza três operações matemáticas diferentes. Cada operação é efectuada em dois blocos de *input* de 16 *bits* para produzir um único *output* de 16 *bits*. As operações são:

- OU exclusivo *bit* a *bit*, representado por Ø.
- Adição de inteiros módulo 2^{16} (módulo 65536), os *inputs* e *outputs* são tratados como inteiros de 16 *bits* sem sinal. Esta operação é representada por ß.

- Multiplicação de inteiros módulo $2^{16} + 1$ (módulo 65537),), os *inputs* e *outputs* são tratados como inteiros de 16 *bits* sem sinal, excepto um bloco de zeros que é tratado como 2^{16}. Esta operação é representada por °.

Estas três operações são incompatíveis, pois não satisfazem as leis distributiva e associativa.

A utilização destas três operações combinadas fornece uma transformação complexa do *input*, tornando a criptanálise muito mais difícil do que algoritmos como o DES, o qual se baseia somente na função XOR.

A Figura 10.4 mostra a primeira iteração do algoritmo; as iterações subsequentes têm a mesma estrutura mas com diferentes *inputs* de subchave e texto corrente derivado.

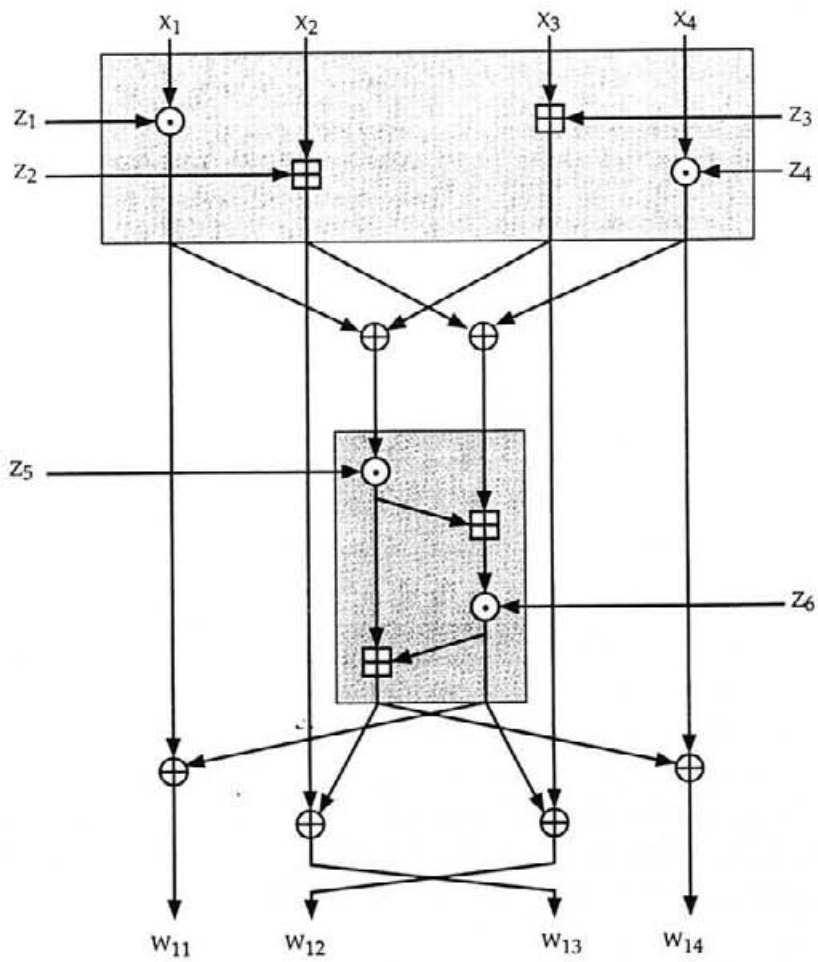


Figura 10.4 – Iteração do IDEA (primeira iteração) [Stall95]

A iteração começa com uma transformação que combina os quatro subblocos de *input* com quatro subchaves, utilizando as operações de adição e multiplicação. Esta transformação é representada pelo rectângulo sombreado da parte de cima da imagem. Os quatro blocos de *output* desta transformação são depois combinados utilizando a função XOR para formar dois

blocos de 16 *bits* que são *input* para a transformação representada pelo rectângulo sombreado de baixo, a qual também utiliza duas subchaves como *input* e combina esses *inputs* para produzir dois *outputs* de 16 *bits*.

Finalmente, os quatro blocos de *output* da primeira transformação são combinados com os dois blocos de *output* da transformação anterior, utilizando-se o XOR para produzir os quatro blocos de *output* desta iteração. De notar que a grande mistura dos *bits* processados torna o algoritmo mais resistente à criptanálise.

A nona etapa do algoritmo, designada na Figura 10.3 etapa de transformação do *output*, tem a mesma estrutura da primeira zona sombreada das iterações precedentes (Figura 10.3). A única diferença é que os segundo e terceiro *inputs* são trocados antes de serem aplicados às unidades operacionais. Isto tem o efeito de desfazer a troca no final da oitava iteração. A razão para esta troca adicional é devida a que a decifração tem a mesma estrutura que a cifragem.

Finalmente, as subchaves para cada iteração são geradas por séries de *shifts* da chave de 128 *bits* original.

O IDEA demonstra ter um número de vantagens sobre o DES ou mesmo o Triple DES. O tamanho da chave de 128 *bits* torna-o mais resistente aos ataques de pesquisa de chaves de força bruta. A estrutura interna do IDEA torna-o mais resistente à criptanálise que o DES. Finalmente, o IDEA foi desenhado para facilitar quer as implementações em *software* quer em *hardware*. Para implementações comparáveis do IDEA e do Triple DES, o IDEA deve executar em muito menos tempo.

3. MD5

O MD5 (Message-Digest Algorithm) foi desenvolvido por Ron Rivest [Rivest92]. O algoritmo tem como *input* uma mensagem de tamanho arbitrário e produz como *output* uma mensagem resumida (*digest*) de 128 *bits*. O *input* é processado em blocos de 512 *bits*.

A Figura 10.5 descreve o processamento geral de uma mensagem para produzir o "resumo". O processamento consiste nos passos seguintes:

- Adicionar *Bits* de *Padding*: A mensagem é aumentada de forma que o seu tamanho em *bits* fique congruente com 448 módulo 512, quer dizer, o tamanho da mensagem aumentada é 64 *bits* menor que um inteiro múltiplo de 512 *bits*. O enchimento é sempre efectuado, mesmo que a mensagem tenha já o tamanho necessário, por exemplo, se a mensagem tiver 448 *bits* de tamanho, é aumentada de 512 *bits* para um tamanho de 960 *bits*.

- Adicionar Tamanho: Uma representação de 64 *bits* do tamanho em *bits* da mensagem original é adicionada ao resultado do primeiro passo. Se o tamanho original for maior que 2^{64}, então somente os 64 *bits* de ordem mais baixa são utilizados.

  O resultado dos dois primeiros passos é uma mensagem com tamanho múltiplo de 512 *bits*, representada na figura por uma sequência de blocos de 512 *bits* $Y_0, Y_1, \ldots, Y_{L-1}$. O resultado é um múltiplo de 16 *words* de 32 *bits*.

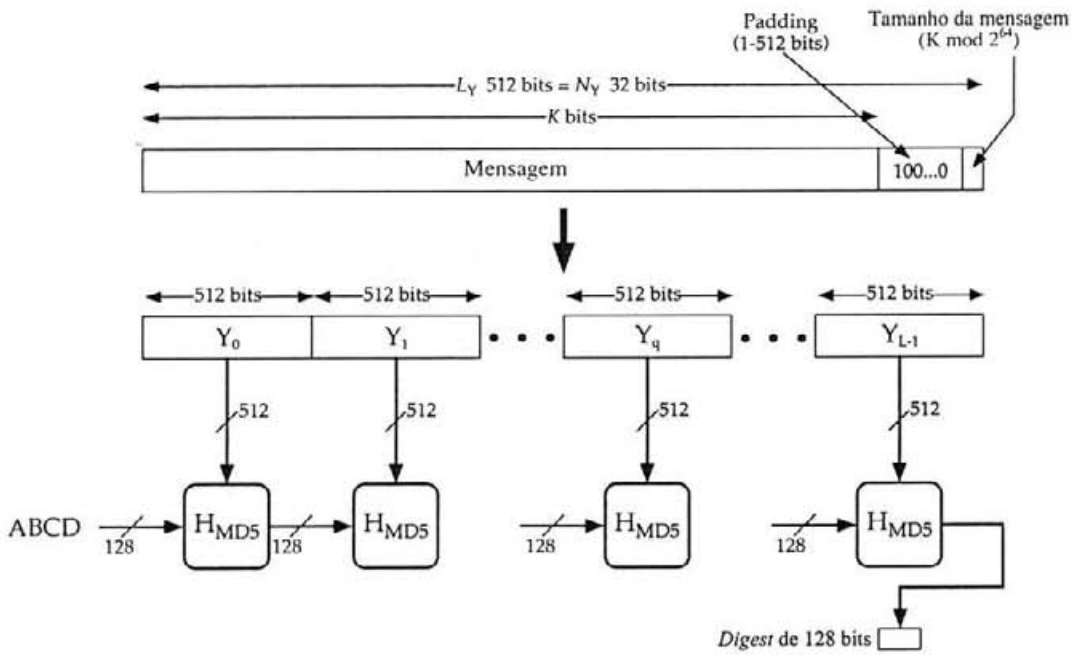


Figura 10.5 – Geração da Message Digest Utilizando o MD5 [Stall95]

- Inicializar o *Buffer MD*: É utilizado um *buffer* de 128 *bits* para guardar os resultados intermédios e finais da função de *hash*. O *buffer* é constituído por quatro registos de 32 *bits* (A, B, C, D), que são inicializados com os seguintes valores hexadecimais:

```
A = 01234567
B = 89ABCDEF
C = FEDCBA98
D = 76543210
```

- Processar a Mensagem em Blocos de 512 *Bits* (*Words de 16*): O núcleo do algoritmo é um módulo que consiste em quatro etapas de processamento, designado H_{MD5} na Figura 10.5, e a sua lógica está ilustrada na Figura 10.6. Cada etapa tem a mesma estrutura funcional mas cada uma utiliza uma primitiva de função diferente – f_F, f_G, f_H, f_I.

  Cada etapa toma como *input* o bloco actual de 512 *bits* a ser processado (Y_q) e o *buffer* de 128 *bits* e actualiza o conteúdo do *buffer*. Cada etapa utiliza também um

quarto da tabela de 64 elementos T[1 . . . 64], construída a partir da função seno.

O elemento *i* de T, designado T[*i*], é igual à parte inteira de $2^{32} \times \text{abs}[(\sin(i)]$. Como abs[(sin(*i*)] é um número entre 0 e 1, cada elemento de T é um inteiro que pode ser representado com 32 *bits*. A tabela fornece um conjunto de elementos "aleatórios" de 32 *bits*, que deve eliminar qualquer regularidade dos dados de *input*.

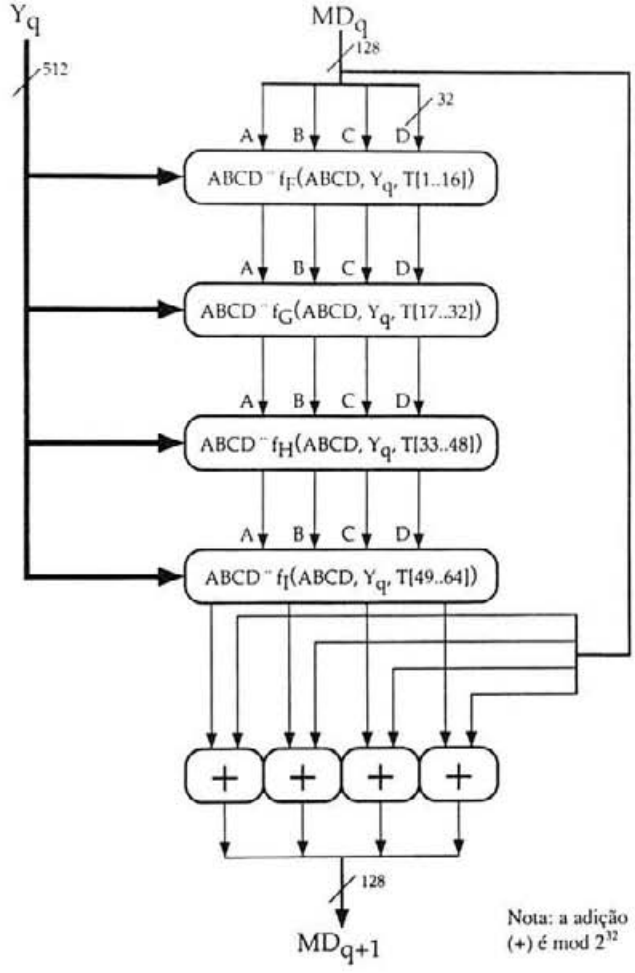


Figura 10.6 – MD5: Processamento de um Único Bloco de 512 *bits* (HD_{MD5}) [Stall95]

Generalizando, para o bloco Y_q, o algoritmo tem como *inputs* Y_q e um valor "resumo" intermédio MD_q. O MD_q é colocado no *buffer* ABCD. O *output* da quarta etapa é adicionado a MD_q para produzir $MD_{(q+1)}$.

- O *Output*: Depois de todos os *L* blocos de 512 *bits* terem sido processados, o *output* da etapa *L* é a mensagem "resumo" de 128 *bits*.

O algoritmo MD5 tem a propriedade de cada *bit* do código de *hash* ser função de todos os *bits* de *input*. A repetição complexa das funções básicas (F, G, H, I), origina que seja improvável que duas mensagens escolhidas aleatoriamente, mesmo que exibam regularidades similares, tenham o mesmo código de *hash*. Rivest conjectura no RFC que o MD5 é tão forte

quanto possível para um código de *hash* de 128 *bits*, nomeadamente a dificuldade de surgirem duas mensagens com a mesma mensagem resumo é da ordem de 2^{64} operações, enquanto a dificuldade de encontrar uma mensagem com uma dado "resumo" é da ordem de 2^{128} operações.

4. Regulações da Cifragem em Alguns Países

Apresenta-se uma tabela com as regulações da cifragem em alguns países mais representativos da União Europeia, Portugal, e também Israel que é um país exportador desta tecnologia.

País	Importações	Exportações	Utilização com fio	Utilização sem fio
França	Requerida licença se o tamanho da chave exceder 40 bits e se o produto for de fora da União Europeia	Requerida licença	Requerida licença para tamanhos de chave superiores a 48 bits, a não ser se as chaves sejam depositadas numa organização independente	Requerida licença para tamanhos de chave superiores a 48 bits, a não ser se as chaves sejam depositadas numa organização independente
Alemanha	Permitido	Restrições das N. U.	Permitido	Permitido
Israel	Requerida licença	Requerida licença	Requerida licença	Não permitido
Portugal	Permitido	Restrições das N. U.	Permitido	Permitido
Espanha	Permitido	Requerida licença	Permitido somente para bancos	Não permitido
U.K.	Permitido	Requerida licença	Permitido	Permitido

Tabela 10.2 – Regulações da Cifragem em Alguns Países

B. Principais Elementos Activos de Rede

As características técnicas mais relevantes dos principais elementos activos de rede do IPP são as seguintes:

- *Router* do IDT (nó central) – Cisco 4500M:
  - *Router* modular configurável suportando até 3 módulos de processador de rede (NPM) com Cisco IOS, de entre as opções: Ethernet, Token Ring, Fast Ethernet, ATM, FDDI, ISDN BRI e PRI, e várias opções série.
  - Suporte a uma vasta gama de protocolos de encaminhamento através do *software* Cisco IOS, incluindo IP, IPX, AppleTalk, CLNS, XNS, e outros.
  - Suporta características tais como compressão (TCP/IP *header*, DEC LAT, *link* e X.25 Packet Payload), Priority Output Queuing, Custom Queuing, Access Lists e Cisco Protocol Translation.

- *Routers* dos outros estabelecimentos – Cisco 2503:
  - Combina 1 ligação LAN (Ethernet), 2 portas WAN série síncronas (até 2 Mbps) e uma porta ISDN BRI.
  - Suporta uma grande variedade de serviços WAN, desde linhas alugadas, Frame Relay, ISDN, X.25 e SMDS.
  - Suporte a uma vasta gama de protocolos de encaminhamento através do *software* Cisco IOS, incluindo IP, IPX, AppleTalk, CLNS, XNS, e outros.
  - Permite gestão de largura de banda e optimização e características de segurança que incluem compressão de dados e filtragem de pacotes.

Pelo facto deste *router* ter somente 1 porta LAN, não permite grandes possibilidades numa arquitectura de *firewall*, por exemplo na arquitectura de *firewall* de subrede *screened* não permite efectuar a separação do tráfego entre duas LANs no *router* exterior.

Uma boa solução para este problema está em combinar o *router* Cisco 2503 e o Cisco 1005 que existe em alguns dos estabelecimentos.

- Cisco 1005, características:
  - Tem 1 ligação LAN (Ethernet) e uma porta WAN série síncrona (até 2 Mbps) .
  - Suporta uma grande variedade de serviços WAN, desde linhas alugadas, Frame Relay, ISDN, X.25 e SMDS.
  - Suporta o *routing* e *bridging* do IP, IPX, e AppleTalk sobre linhas alugadas, Frame Relay, Switched 56, SMDS, e X.25.

Combinam-se os *routers* interligando-os pela porta série do Cisco 1005 e pela segunda porta série do Cisco 2503 (Figura 10.7), obtendo-se um canal de 2 Mbps. De outra forma teria de ser inserido um *dual-homed host* adicional com três interfaces de rede para se implementar uma arquitectura de subrede *screened*. Esta solução teria maiores custos do que a aquisição de um *router* Cisco 1005 para os estabelecimentos que não o tiverem (cerca de 150 contos).

A filtragem do tráfego não fica comprometida de forma alguma, cabendo ao Cisco 2503 efectuá-la, entre as três redes – Internet, rede de perímetro e Rede Geral.

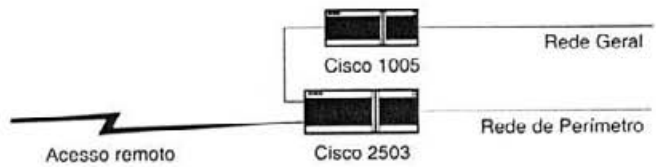


Figura 10.7 – Combinação de 2 *Routers* para Obtenção de 2 Portas LAN

Uma outra opção está na aquisição do *router* Cisco 2514, da mesma gama dos existentes, e que dispõe de duas portas LAN e duas série e que tem o custo de cerca de 550 contos.

- *Switches* – Cabletron FN100:
  - Arquitectura de comutação escalável de alta velocidade e latência mínima. Suporta taxas de transferência até 2.56 Gbps, mais do que suficiente para 16 portas de 100 Mbps.
  - Suporta os *standards* 10BASE-T, 100BASE-TX, e 100BASE-FX;
  - Suporta a auto-negociação IEEE 802.3u entre 10BASE-T e 100BASE-TX.
  - Permite configurar até 4 *switches* virtuais e definir grupos de trabalho virtuais para optimizar o tráfego de rede. Suporta o *trunking* entre dois *switches* na combinação de até 8 linhas para uma largura de banda total de 800 Mbps.
  - Configuração e gestão utilizando o SNMP, in-band ou out-of-band.
  - Contém a funcionalidade de *full store-and-forward* e é transparente aos protocolos, permitindo efectuar o *bridge* de diferentes tipos de tráfego de rede, independentemente do protocolo de rede.
  - Suporta o Algoritmo de Spanning Tree (IEEE 802.1(d)) que permite o desenho de topologias Fast Ethernet perfeitamente redundantes.
  - Suporta mais de 8000 endereços MAC, com constante aprendizagem das entradas associadas com cada porta. Protege contra *multicast storms*.

C. Testes de Laboratório

1. Testes de Laboratório de *Firewalls*

Uma equipa formada pela Data Communications e pela National Software Testing Laboratories Inc. (NSTL) realizou testes exaustivos aos *firewalls* reunidos no teste de laboratório.

Depois de anos de debate sobre a melhor tecnologia de *firewall* – *firewalls* de filtragem de pacotes ou *firewalls proxies*, os fabricantes estão a começar a fornecer ambas as abordagens. Mesmo a Check Point, o primeiro fabricante a fornecer um produto *stateful inspection*, agora também oferece *proxies* [NewDC98f].

Muitos *firewalls* suportam também características VPN como a autenticação e a cifragem. Estas características não foram avaliadas, pois as VPNs pela sua importância justificam um teste separado.

1.1 A Metodologia de Teste

Catorze dos mais importantes fornecedores de *firewalls* foram convidados a fornecer um *firewall* que suportasse o Windows NT Server 4.0 Service Pack 3, 2 interfaces 100Base-T (um para a rede interna e outro para a rede pública), gestão remota, e *network address translation*[1] (NAT). A Data Communications conseguiu reunir os seguintes fornecedores de *firewalls*:

- Check Point com o Check Point Firewall-1 v. 3.0,
- DEC com o Altavista Firewall 97 v. 3,
- Fortress com o Netfortress Heatseeker Pro v. 1.0,
- Microsoft com o Proxy Server v. 2.0,
- Netguard com o Guardian v. 3.0,
- Raptor com o EagleNT, version 5.0.1,
- Secure com o Secure Computing Firewall for NT, version 3.1.

[1] *Network address translation* – mecanismo que esconde os endereços IP internos da rede externa de forma a não permitir aos atacantes a apreensão da topologia de rede [NewDC98f].

Devido à falta de suporte de componentes utilizados no teste, ou por não terem as versões requeridas do *firewall* ainda disponíveis ou ainda não testadas nas condições propostas, declinaram o convite: Cisco Systems (Global Internet), CyberguardCorp (Cyberguard Firewall), Network-1 Software and Technology (Firewall/Plus), Cycon Technologies (Cycon Labyrinth Firewall), Milkyway Networks (Black Hole), Trusted Information Systems (Gauntlet Internet Firewall), e Ukiah Software (Netroad Firewall).

Para assegurar uma comparação justa, todos os produtos foram testados no mesmo *hardware* e passados para um disco duro diferente em cada entrada do teste. O sistema de teste foi um Pentium Pro 200 MHz de duplo CPU com 256 Mbytes de RAM.

Os *firewalls* foram testados no que respeita à segurança, gestão, e desempenho (Tabela 10.3 na secção A.1.4). Para testar a segurança foi utilizado o Safesuite 5.0 da Internet Security Systems (ISS) que foi configurado para executar cerca de 300 tentativas de penetração em cada *firewall*. O Safesuite foi executado numa máquina no segmento público, e foi utilizado o seu *output* como a base principal para os relatórios de segurança. Foi verificado também se os *firewalls* capazes de bloquearem páginas Web contendo objectos Java ou ActiveX de facto o fazem.

Nos testes da gestão, foram definidos três cenários comuns que surgem aos gestores de rede – administração remota, controlo de acesso, e o *logging* – e foi anotado como é que os *firewalls* tratam cada situação.

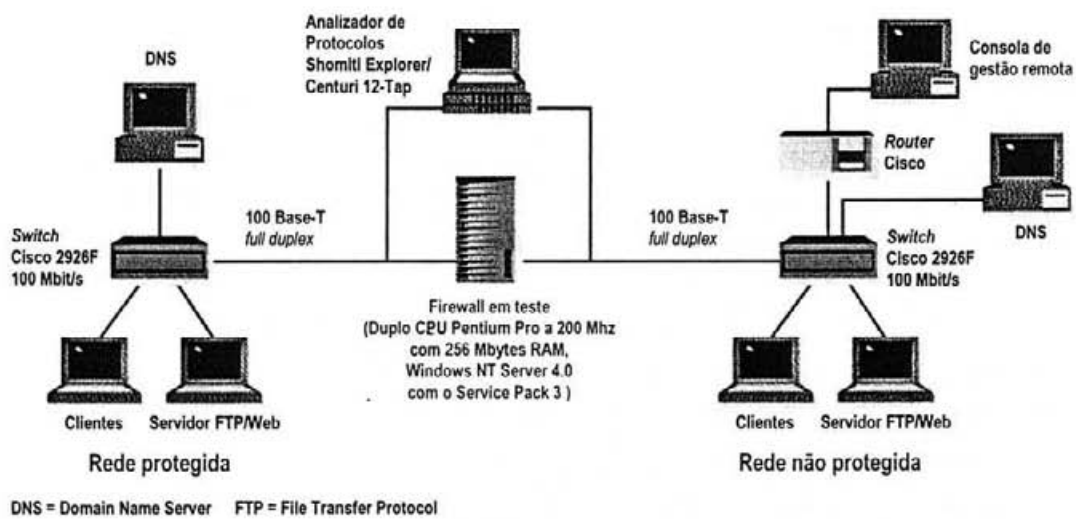


Figura 10.8 – Configuração da Plataforma de Teste [NewDC98f]

No primeiro cenário, um atacante tenta uma infiltração através de um *firewall* e é avaliado se o *firewall* notifica o gestor de rede (por e-mail ou *pager*) e permite a este desactivar o *firewall* de um segmento de rede remoto. É verificado também se as comunicações entre o segmento remoto e o *firewall* são cifradas. No segundo cenário, um gestor de rede configura duas políticas de segurança – uma permitindo acesso baseado em endereço IP (verificando se

permite restrições de horas do dia) e outra baseada num ID de utilizador. No terceiro cenário, são examinados vários aspectos do *logging* de *firewall*. Verifica-se o suporte à recolha de dados específicos dos *log* de cada *firewall* para criar dois relatórios – um que lista todos as tentativas de acesso não autorizado ordenadas por endereço IP de origem, e o outro que lista todos os pedidos HTTP de um dado endereço IP de origem num período de 24 horas.

Verificou-se também como é que cada *firewall* se comporta quando o espaço do *log* e do disco duro enche. Existindo quatro possibilidades: reiniciar o *log*, reescrevendo as entradas mais antigas; continuar a operar sem *logging*; desligar o acesso; ou permitir aos gestores de rede definirem uma dessas opções. Finalmente, foi determinado quando e como o *logging* é efectuado, e se o tamanho do *log* pode ser definido pelo utilizador quer no mesmo sistema do *firewall* ou em sistemas externos. Em produtos que suportassem o *logging* externo, verificou-se se o *firewall* transmitia as entradas do *log* em formato cifrado.

Para a avaliação do desempenho, foi utilizado o InterMark, uma aplicação desenvolvida pela NSTL para o teste de aplicações da Internet, para gerar os pedidos HTTP e FTP. Foi configurada uma plataforma de teste com dois servidores FTP e Web – um em cada lado do *firewall*, cada um com duas interfaces 100Base-T e cada uma com um único endereço IP. Utilizaram-se também duas máquinas cliente, novamente colocadas uma em cada lado do *firewall* e configuradas com duas interfaces 100Base-T com um único endereço IP. Para assegurar o máximo *throughput* a cada *firewall*, os servidores e clientes foram ligados a *switches* Fast Ethernet, que por sua vez ligam a cada interface do *firewall*. Foram utilizadas ligações *full-duplex*, e assegurou-se a oferta de cargas de 100 Mbit/s simultaneamente em ambas as direcções e sem colisões. Foram colocados geradores de tráfego para lá dos *switches*, capazes da oferta de dados a 100 Mbit/s.

Como os *firewalls* baseados em arquitecturas *proxy* podem ter diferentes características de desempenho para diferentes protocolos, foram configurados testes diferentes para medir o desempenho Web e FTP. Em ambos os casos, os quatro "clientes virtuais" (geradores de tráfego de 100 Mbit/s), dois de cada lado do *firewall*, efectuaram o pedido de recursos aos servidores através do *firewall*. O tráfego foi configurado bidireccional mas não emalhado, as interfaces de cliente 1 e 2 solicitaram dados das interfaces do servidor 1 e 2, respectivamente.

O Intermark registou o número de transações por minuto completadas com sucesso. Foi depois calculado o *throughput* médio dividindo a quantidade de dados transferidos pelo tempo que demorou a completar cada teste.

1.2 Os Resultados do Teste

O Safesuite quase não registou vulnerabilidades, quer no código do *firewall* ou nas configurações do Windows NT. No teste de Março de 97, que incluía produtos Unix, foram executados cerca de 100 ataques e encontradas dezenas de falhas. Neste teste, executaram-se 288 formas de ataque, e encontraram-se sete vulnerabilidades num *firewall* (Altavista Fi-

rewall 97), mas todas elas foram falsos positivos.

Somente o Heatseeker Pro da Fortress Technologies não tem o NAT *built-in*, mas pode ser combinado com um dispositivo NAT. Ao invés de servir de barreira no perímetro da rede, o Heatseeker Pro reside em cada PC da rede e intercepta as chamadas a cada *driver* Winsock de cada computador. Um módulo de gestão central permite aos gestores de rede definir as políticas e aplicá-las globalmente. No entanto, a sua dependência do Winsock significa que não poderá ser utilizado em plataformas não Windows, o que o elimina da aplicação ao caso em estudo.

Deve ser notado que o aumento de popularidade de produtos como o Safesuite, que é fornecido como uma forma de validação da configuração do *firewall*, pode ser uma razão para os óptimos resultados encontrados. Os fabricantes de *firewalls* poderão ter salvaguardado as vulnerabilidades mais conhecidas que o Safesuite verifica.

Estes *firewalls* efectuam um trabalho excelente na procura de potenciais vulnerabilidades no próprio Windows NT. As rotinas de instalação tomam medidas para aumentar a segurança do NT, tal como substituir o *driver* de serviços por defeito por um *driver* compacto sem os serviços desnecessários.

Não quer isto dizer que estes produtos sejam perfeitos. Os testes revelaram bastantes possibilidades de melhoria na gestão, especialmente nos *logs* de auditoria do *firewall*. Os testes de desempenho mostram que o *network address translation* diminui significativamente o desempenho.

Os fornecedores dos *firewalls* configuraram-nos para ataques localizados e bem definidos num ambiente de laboratório cuidadosamente controlado. Apesar de ser uma forma válida de demonstrar a funcionalidade dos *firewalls*, não significa que esses *firewalls* sejam absolutamente seguros. De facto, isso não existe, esses produtos podem ser vulneráveis a novos ataques ou, mais frequentemente, a más configurações que colocam a rede em risco. É por isso que se deu quase tanta ênfase na gestão dos *firewalls* como se deu à segurança.

Nos testes de gestão (Tabela 10.4 na secção A.1.4) foram encontrados bastantes diferenças entre os produtos, especialmente em termos de auditoria dos *logs* – uma capacidade crítica na descoberta dos atacantes. Essas diferenças devem-se em primeiro lugar, às diferenças entre as interfaces dos *firewalls*, e existem diferenças substanciais no que cada interface permite efectuar aos gestores de rede.

O desempenho dos *firewalls* é importante, mas considerou-se secundário relativamente à segurança ou à gestão. O *firewall* mais rápido com o NAT activado foi o Microsoft's Proxy Server, que atingiu os 62.57 Mbit/s com tráfego FTP (Figura 10.9). O factor de comparação deste desempenho é o máximo teórico deste teste que é de 200 Mbit/s (*throughput* agregado). A Microsoft teve também o melhor resultado com o tráfego Web, com uma velo-

cidade de 56.17 Mbit/s. Os seguintes melhores desempenhos foram da Netguard, Secure Computing, e Check Point. O NAT claramente degrada o desempenho.

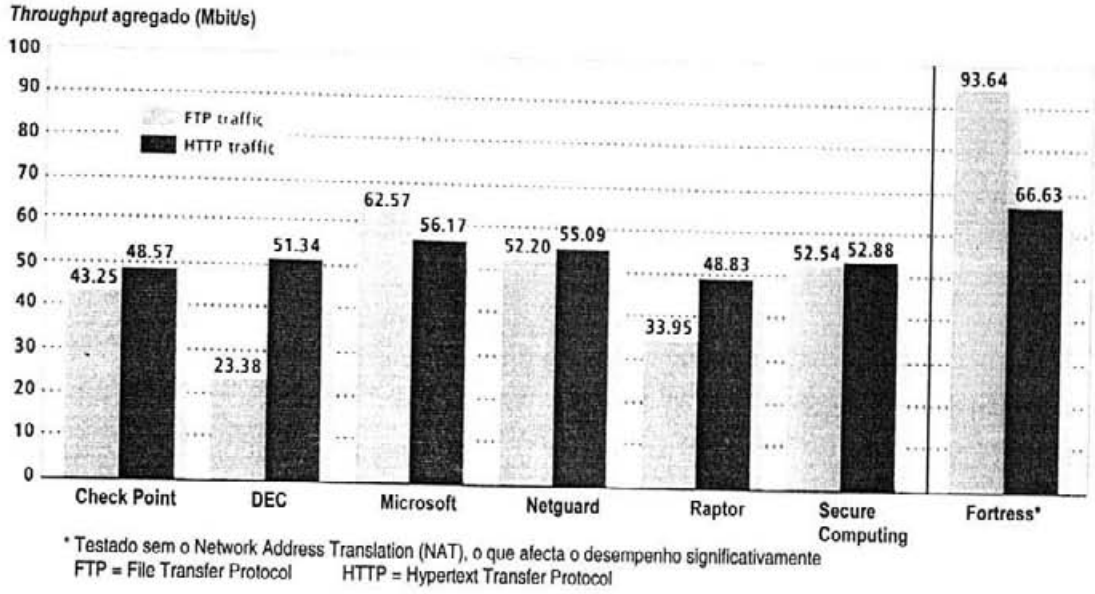


Figura 10.9 – Teste de Desempenho dos *Firewalls* [NewDC98f]

Um factor que não foi medido neste teste foi o número máximo de ligações concorrentes que o *firewall* pode suportar.

Uma forma de melhorar o desempenho do *firewall* é com o *load balancing*. Neste teste, quatro produtos – da Check Point, Microsoft, Netguard e Secure Computing – permitem que um grupo de *firewalls* trabalhem em conjunto, com um dispositivo gerindo os pedidos para os outros. O *load balancing* é uma técnica chave para o aumento do desempenho da rede.

1.3 As Conclusões dos Outros Testes de Laboratório

Será útil analisar também as conclusões dos outros dois testes de laboratório. O teste de Março de 97 da Data Communications, como se disse é mais abrangente na gama de sistemas operativos e na quantidade de *firewalls* e o de Junho de 97 da Byte é um teste comparativo de uma fonte diferente. Será útil comparar as classificações dos *firewalls* nos três testes, mas convém salvaguardar as evoluções de cada um dos *firewalls* ao longo de um ano.

No teste de Março de 97 foram encontradas vulnerabilidades em alguns produtos, a maioria delas resultado de configurações deficientes. As capacidades de gestão excederam as expectativas, e alguns *firewalls* não suportaram as pesadas cargas dos testes de desempenho o que leva a preocupações sobre a real segurança de cada um.

Apresenta-se na Tabela 10.5 na secção A.1.4 a tabela comparativa dos *firewalls* deste teste, tendo sido seleccionados somente aqueles que estão também presentes no teste de Abril de 98 juntamente com os que foram a "escolha do teste".

No teste de Junho de 97 da revista Byte (Tabela 10.6 na secção A.1.4), o CyberGuard Firewall empatado com o Check Point FireWall-1, o AltaVista Firewall 97, e o Firewall/Plus obtiveram uma pontuação de segurança quase perfeita, mas obteve vantagem relativamente aos maiores competidores (Check Point FireWall-1 e AltaVista Firewall 97) com a combinação das melhores funcionalidades, facilidade de gestão, e bom desempenho.

O Check Point Firewall-1, neste teste, ao seu conjunto de funcionalidades completo e a um óptimo desempenho são contrapostas as ferramentas de configuração longe da perfeição. O AltaVista Firewall 97 compensa a sua relativa falta de funcionalidades com óptimo desempenho e uma interface de gestão simples.

1.4 Tabelas dos Testes de Laboratório de *Firewalls*

Apresentam-se nas próximas páginas as tabelas com os resultados dos testes de laboratório de *firewalls*: Tabela 10.3 – Os *Firewalls* em Teste, Tabela 10.4 – Cenários de Gestão do *Firewall*, Tabela 10.5 – Os *Firewalls* do Teste de Laboratório de Março de 97, e Tabela 10.6 – Os *Firewalls* do Teste de Laboratório de Maio de 97.

Fabrican.	Produto	Arquitectura	Max interf./ interfaces suportados	Filtros de Log	Cifragem/ autenticação	Filtragem ActiveX/ Java	Suporte 24 hor., 7 dias	Load Balan-cing	Preço para 25/100 utilizad.
Check Point	Check Point Firewall-1, v. 3.0	Stateful inspection, proxy	32/ dependente do sistema	Serviço, tempo, origem, destino, tracing de pacotes	DES, RC4, FWZ-1/Kerberos, MD5, Radius, SecurID, SHTTP, Socks, SSL, Tacacs+, IPSec AH, S/Key, firewall passwords	Sim/Sim	Sim[1]	Sim	$2,995/ $7,995
DEC	Altavista Firewall 97, v. 3	Filtragem de pacotes, proxy de aplicação, circuit relay	2/Ethernet, fast Ethernet, token ring, FDDI, T1/E1, T3/E3, ATM	Serviço, tempo, origem, destino	RC4/SecurID, NT domain password	Não/Não	Sim[1]	Não	$2,495/ $3,995
Fortress	Netfortress Heatseeker Pro, v. 1.0	Filtragem de pacotes; circuit relay em todos os postos	Dependente do sistema	Serviço, tempo, origem, destino	Nenhum	Sim/Sim	Não	Não	$1,944/ $5,190
Microsoft	Proxy Server, v. 2.0	Filtragem de pacotes, proxy de aplicação, circuit relay	Dependente do sistema	Nenhum	MPPE, PPTP/NT authentication, Radius, SHTTP, SSL	Não/Não	Sim	Sim	$995/$995
Netguard	Guardian, v. 3.0	Filtragem de pacotes, proxy de aplicação, stateful inspection	Dependente do sistema/ Ethernet, fast Ethernet, token ring, FDDI, T1/E1, T3/E3, ATM	Serviço, tempo, origem, destino, tracing de pacotes	DES, triple DES, RC4, All CryptoAPI compatible/MD5	Sim/Sim	Sim	Sim	$2,480/ $3,980
Raptor	EagleNT, v. 5.0.1	Proxy de aplicação	64/Ethernet, fast Ethernet, token ring, FDDI, T1/E1, T3/E3	Serviço, tempo, origem, destino, tracing de pacotes	DES, triple DES, RC4/MD5, Radius, SecurID, SHTTP, Socks, SSL, Tacacs+, IPSec AH	Sim/Sim	Sim[1]	Não	Não aplic./ $3,995 (s/ VPN); $6,500 (c/ VPN)
Secure	Secure Computing Firewall for NT, v. 3.1	Filtragem de pacotes, proxy de aplicação, circuit relay	3/Ethernet, fast Ethernet, T1/E1, T3/E3	Serviço, tempo, origem, destino	PPTP/MD5, Radius, Safeword	Sim/Sim	Sim[2]	Sim	$3,000[3]/ $7,000[4]

1. Com custo adicional
2. Por opção do revendedor
3. Preço para 50 utilizadores
4. Preço para 400 utilizadores
DES = Data encryption standard
E1 = 2.048 Mbit/s
E3 = 34 Mbit/s
IPSec AH = IP security authentication header
MD5 = Message digest 5
MPPE = Microsoft point-to-point encryption
PPTP = Point-to-point tunneling protocol
Radius = Remote authentication dial-in user service
SHTTP = Secure hypertext transfer protocol
SSL = Secure sockets layer
Tacacs = Terminal access controller access control system
T1 = 1.544 Mbit/s
T3 = 45 Mbit/s

Tabela 10.3 – Os *Firewalls* em Teste [NewDC98f]

Tarefas	Check Point	DEC	Fortress	Microsoft	Netguard	Raptor	Secure Computing
Cenário 1: Gestão Remota							
Notificação de tentativa de acesso não autorizado	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Facilidade da tarefa (acesso não autorizado)	4	4	3	4	4	5	4
Desactivar remotamente o acesso do exterior	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Facilidade da tarefa (Desactivar remotamente o acesso do exterior)	4	4	3	4	5	4	4
Cifragem da ligação remota	Sim	Sim	No	Sim	Sim	Sim	Sim
Cenário 2: Controlo de Acesso							
Limita os endereços IP recebidos	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Restrições por hora do dia	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Facilidade da tarefa (Restrições por hora do dia)	5	5	5	4	5	4	5
Limita as ligações baseadas no ID do utilizador	Sim	FTP, telnet	Sim	Sim	Sim	Sim	Sim
Facilidade da tarefa (limita as ligações)	4	4	3	4	4	4	4
Cenário 3: Capacidades de Logging							
Listar as tentativas de acesso não autorizado, ordenadas por endereço IP	Sim	Sim	Sim	Não	Sim	Sim	Sim
Facilidade da tarefa (listar as tentativas de acesso não autorizado)	3	3	4	0	3	3	3
Listar os pedidos HTTP, dos endereços IP fonte dados	Sim	Sim	Sim	Não	Sim	Sim	Sim
Facilidade da tarefa (listar os pedidos HTTP)	4	3	4	0	4	3	3
Log cheio	Desactiva o logging	Efectua o Shutdown	Desactiva o logging	Remove o log antigo, e escreve o novo log	Efectua o Wrap do log	Remove o log antigo, e escreve o novo log	Efectua o Wrap do log
Disco cheio	Desactiva o logging	Efectua o Shutdown	Desactiva o logging	Definido pelo utilizador	Efectua o Shutdown	Remove o log antigo, e escreve o novo log	Efectua o Wrap do log
Definição pelo utilizador do tamanho do log no mesmo sistema	Não	Não	Não	Sim	Sim	Sim	Sim
Permite o logging num sistema diferente	Sim	Não	Sim	Sim	Sim	Sim	Sim
Definição pelo utilizador do tamanho do log num sistema diferente	Não	Não	Não	Sim	Sim	Sim	Sim
Permite o logging no mesmo sistema	Sim	Não	Não	Não	Sim	Sim	Não

Pontuação: 0 = Não suportado; 1 = Deficiente; 2 = Positivo; 3 = Bom; 4 = Muito Bom; 5 = Excelente.

FTP = File transfer protocol; HTTP = Hypertext transfer protocol.

Tabela 10.4 – Cenários de Gestão do *Firewall* [NewDC98f]

Fabricante	Produto	Arquitectura	Sistema/ SO testado	SOs suportados	Max interfaces/ interfaces suportados	Filtros de Log	Cifragem/ autenticação	NAT	Filtragem ActiveX/ Java[1]	Preço 25/100/ 1000 utl.
Altavista Software Inc.	Altavista Firewall 97 version 3.0 (beta)	Filtragem de pacotes, proxy de aplicação, circuit relay	Alpha/ Digital Unix	BSDI Unix, Digital Unix/ Ultrix, Windows NT 3.51 ou 4.0	2/Ethernet, token ring, FDDI, ATM a 25 ou 155 Mbit/s, fast Ethernet, 100VG Any LAN, série até T1/E1, T3/E3, assíncrono., ISDN	Serviço, tempo, origem, destino	MD5, SecureID, SHTTP, SSL, Tacacs+, Securenet Key, Cryptocard, Watchword, S/Key, nome de utilizador e password para acesso exterior	Sim	Sim/não	$3,995 (50 nós)/ $7,995 (200 nós)/ $14,995 (s/ limite)
Check Point Software Technologies Inc.	Check Point Firewall-1 version 2.1	Stateful inspection	Sparc Ultra 143, 128 Mb RAM/ Solaris	HP-UX, Solaris, SunOS, Windows 95, Windows NT 3.51 ou 4.0	N/D/Ethernet, token ring, FDDI, ATM a 25 ou 155 Mbit/s, fast Ethernet, 100VG Any LAN, série até T1/E1,T3/E3, assíncrono, ISDN	Serviço, tempo, origem, destino	MD5, Radius, SecureID	Sim	Sim/não	$2,995/ $7,997/ $18,990
Cyberguard Corp.	Cyberguard Firewall version 3.0	Filtragem de pacotes, proxy de aplicação, circuit relay, stateful inspection	Intel Pentium Pro/ Cyberguard MLS Unixware 2.1	Cyberguard MLS Unixware 2.1, AT&T SVR4 Unix, SCO Unix	Sem limite/Ethernet, FDDI, fast Ethernet	Serviço, tempo, origem, destino	MD5, SecureID, Socks, SSL	Sim	Não/não	$9,995/ $14,995/ $19,995 (s/ limite)
Netguard Ltd.	Guardian version 2.0	Stateful inspection	Pentium Pro 200-MHz / Windows NT 4.0	Windows NT 4.0 , OS/2, Windows NT 3.51	Dependente do SO/Ethernet, token ring, FDDI, ATM a 25 ou 155 Mbit/s, fast Ethernet, 100VG AnyLAN, série até T1/E1, T3/E3, assíncrono, ISDN, adaptador com driver NDIS	Serviço, tempo, origem, destino	Kerberos, MD5	Sim	Não/não	$3,980/ $6,980/ $6,980
Raptor Systems Inc.	EagleNT version 4.0	Proxy de aplicação, circuit relay	Compaq Prosignia 200/ Windows NT 4.0	HP-UX, Solaris, Windows NT 4.0, DG-UX, Sinux	N/D/Ethernet, token ring, FDDI, fast Ethernet, 100VG-AnyLAN	Serviço, tempo, origem, destino	MD5, Radius, SecureID, Tacacs+, Cryptocard, Assurenet Pathways, S/Key, NT Domain Controller, multiuse gateway password	Sim	Sim/não	$6,500/ $11,000/ $15,000
Seattle Software Labs Inc.	Watchguard Security Management System version 2.10.03	Filtragem de pacotes, proxy de aplicação, circuit relay, stateful inspection	Pentium PC/ Linux	Linux, Windows 95, Windows NT 3.51, Windows NT 4.0	3/Ethernet	Serviço, tempo, origem, destino	Nenhum	Sim	Sim/sim	$3,495/ $3,495/ $3,495

(Contin.) Fabricante	Produto	Arquitectura	Sistema/ SO testado	SOs suportados	Max interfaces/ interfaces suportados	Filtros de Log	Cifragem/ autenticação	NAT	Filtragem ActiveX/ Java[1]	Preço 25/100/ 1000 util.
Secure Computing Corp.	Secure Computing Borderware Firewall Server version 4.0.1	Filtragem de pacotes, proxy de aplicação, circuit relay	100-MHz Pentium PC, 32 Mbytes RAM/BSD I Unix 1.1	Hardened BSDI Unix 1.1	3/Ethernet, token ring, FDDI, fast Ethernet, serial up to T1/E1	Serviço, tempo, origem, destino	MD5, SecureID, Socks, SSL, Cryptocard, Activecard, Enigma Logic, DES Gold, passthrough authentication	Sim	Não/não	$4,000/ $7,000/ $7,000
Secure Computing Corp.	Sidewinder Security Server version 3	Proxy de aplicação	PC Pentium 100-MHz, 32 MB RAM/ Hardened BSD/OS 2.1	Hardened BSD/ OS 2.1	4/Ethernet, FDDI, fast Ethernet	Serviço, tempo, origem, destino	Radius, SecureID, Tacacs+, Enigma Logic Safeword, Cryptocard	Sim	Sim/não	$6,995/ $10,995/ $19,995
Sun Microsystems Inc.	Sunscreen EFS version 1	Filtragem de pacotes, stateful inspection	Sparc Ultra/ Solaris 2.5	Solaris 2.5, Solaris	N/D/Ethernet, fast Ethernet	Serviço, origem, destino	MD5	Sim	Não/não	$1,495/ $4,995/ $14,995

1. Filtragem de Java não verificada no teste.
2. Filtragem ActiveX não verificada no teste.
E1 = 2.048 Mbit/s
E3 = 34 Mbit/s
N/D = Não disponível
NAT = Network Address Translation
Radius = Remote authentication dial-in user service
SHTTP = Secure hypertext transfer protocol
SSL = Secure Sockets Layer
Tacacs+ = Terminal Access Controller System
T1 = 1.544 Mbit/s
T3 = 45 Mbit/s

Tabela 10.5 – Os *Firewalls* do Teste de Laboratório de Março de 97 [NewDC97f]

Fabricante	Produto	Segurança	Gestão	Funcionalidades Relevantes	Desempenho	Tecnologia	Pontuação Geral
Cyberguard Corp.	CyberGuard Firewall	5	4	5	4	5	5
Altavista Software Inc.	AltaVista Firewall 97	5	4	3	5	4	4
Milkyway Networks	Black Hole	3	2	3	1	3	3
Global Internet Software Group	Centri Firewall	3	2	1	4	4	3
Check Point Software Technologies Inc.	Check Point FireWall-1	5	3	5	5	3	4
Raptor Systems	Eagle NT Firewall	3	3	3	1	4	3
Network-1 Software and Technology	Firewall/Plus	5	1	2	1	2	2
Trusted Information Systems	Gauntlet Internet Firewall	4	3	4	1	3	3
Secure Computing Corp.	Sidewinder Security Server	4	3	3	1	3	3

Pontuação: 0 = Não suportado; 1 = Deficiente; 2 = Positivo; 3 = Bom; 4 = Muito Bom; 5 = Excelente.

Tabela 10.6 – Os *Firewalls* do Teste de Laboratório de Maio de 97 [SeacBt97]

2. Testes de VPNs

Novamente em colaboração com a National Software Testing Laboratories Inc. (NSTL), a Data Communications realizou uma avaliação completa de soluções VPN. Foram reunidos 14 produtos em condições de configuração comuns e cenários administrativos, e foram determinadas as penalizações de desempenho que implicam.

Os vários produtos VPN são bastante diferentes uns dos outros. Desta forma foi necessário categorizar as várias implementações VPN. Foram definidas duas grandes categorias: cliente/servidor e servidor/servidor. As VPNs cliente/servidor têm uma correspondência um para um de clientes e túneis cifrados. Servidor/servidor, em contraste, envolve um túnel cifrado com múltiplos clientes.

Alguns produtos são soluções de *software*, enquanto outros são uma combinação de *hardware* e *software*. Alguns incluem funções de encaminhamento e *firewall* (controlo de acesso); outros focalizam somente na autenticação e cifragem. Alguns implementam o IPSec (secção 5.1.2), um *standard* de autenticação e cifragem, enquanto outros não. Como complemento, os fornecedores suportam uma grande variedade de métodos de autenticação, incluindo cartões de autenticação *token*, servidores Radius[2], e um grande número de algoritmos de cifragem.

2.1 A Metodologia de Teste

Foram convidados 26 fornecedores de VPNs, dos quais 12 declinaram a participação, alegando a não disponibilização de um produto apropriado ou constrangimentos de recursos. Os que declinaram o convite foram: ANS Core Systems, Certicom, Cylink, Data Fellows, DSN Technology, Milkyway Networks, Network Systems, Secure Computing, Securicor 3Net, Sterling Commerce, Tradewave, e Trusted Information Systems. A Data Communications conseguiu reunir os seguintes fornecedores de VPNs:

- Altavista com o Altavista Tunnel 97,
- Aventail com o Aventail VPN Server 2.03,
- Check Point com o Check Point Firewall-1 3.0,
- IBM com o IBM Firewall for AIX 3.1,
- Sun com o Sunscreen EFS 1.1,
- V-One com o Smartgate NT Server 2.3,
- Cisco com o Cisco PIX Firewall,

[2] Radius (Remote Authentication Dial-In User Service), desenvolvido pela Livingston, permite aos gestores de rede configurar e administrar parâmetros de segurança para múltiplos RASs (Remote Access Servers) de um único *site*. Muitos servidores de autenticação externos suportam o Radius.

- Compatible com o Intraport Network Access Server,
- IRE com o Safenet LAN VPN Encryptor,
- Isolation com o Infocrypt Enterprise,
- Radguard com o CIPro,
- Redcreek com o Ravlin 10,
- Timestep com o Permit Security Gateway,
- VPNet com o VSU 1010.

Neste teste os produtos foram testados do ponto de vista de gestão e desempenho. A segurança foi analisada pela comparação dos produtos e soluções disponibilizadas. No teste de Julho de 98 a segurança foi também testada, tendo sido utilizado o Safesuite 5.0 da Internet Security Systems (ISS) que executou mais de 200 tentativas de penetração contra cada dispositivo. A plataforma de teste ligava duas subredes IP privadas sobre uma rede pública emulada. O Safesuite foi executado do lado público de cada dispositivo VPN e foram anotadas as vulnerabilidades.

Para avaliação das funções de gestão (do teste base da análise), foram criados quatro cenários cobrindo considerações comuns: acesso a utilizador remoto, gestão de chaves, regras internacionais, e gestão remota.

O cenário de acesso remoto envolveu uma tentativa de estabelecimento de uma ligação segura a partir de uma localização externa. Foram examinados os métodos de autenticação do utilizador, a possibilidade do utilizador activar e desactivar a cifragem, e a revogação e renovação de chaves. Foi verificado se cada sistema efectuava estas tarefas, iniciando uma sessão cifrada e revogando e renovando chaves. Estas últimas tarefas foram classificadas numa escala de 1 a 5 da facilidade de utilização.

Para a gestão de chaves, foi criado um cenário no qual duas companhias ligam as suas redes via um túnel cifrado. Utilizando o Century LAN Analyzer da Shomiti Systems, foi verificado se cada sistema pode trocar chaves automaticamente e se a frequência de revisão de chaves é automática, manual, ou definido pelo utilizador. A facilidade de cancelamento de uma chave foi também classificada numa escala de 1 a 5.

O cenário de regras internacionais envolveu uma ligação VPN entre países cujas leis no tamanho das chaves diferem. Foi verificado se cada sistema podia suportar múltiplos tamanhos de chave e se faz o ajuste por omissão para a chave de menor tamanho. Foi também examinado o mecanismo para a distribuição de chaves noutros países.

No cenário de gestão remota, pesquisaram-se as tarefas comuns de gestão de rede, tal como a configuração de parâmetros para vários *sites* em simultâneo e o cancelamento de chaves e acesso de rede remotamente. Foi verificado também como é que o sistema responde quando o ficheiro de *log* fica cheio.

Na avaliação do desempenho, foi utilizada uma plataforma de teste de duas subredes IP, uma com um PC servidor e a outra com PC cliente. Os PCs tinham CPUs Pentium a 150 MHz, 64 Mbytes de RAM, e placas de rede Etherexpress 10/100 da Intel Corp. Todos os PCs executavam ou Windows NT Server 4.0 ou o Windows 95. Sempre que possível, o teste foi efectuado em segmentos 100Base-T; se não, em segmentos 10Base-T. Em dispositivos que não suportam encaminhamento, foi fornecido um *router* de *software* executado em Windows NT Server 4.0. Começou-se por efectuar medições de base da plataforma de teste sem nenhum sistema a testar.

Utilizando a ferramenta de geração de tráfego Intermark da NSTL, o sistema em teste foi sujeito a tráfego unidireccional e bidireccional. No teste unidireccional, o cliente solicitava continuamente um ficheiro de texto de 1.6 Mbyte ao servidor até que a sua *cache* estivesse completamente cheia e fosse atingido um estado estável; foi depois medido o *throughput* na linha utilizando o analisador Shomiti, e na camada de aplicação o Intermark. O teste bidireccional é semelhante, excepto que o cliente envia um fluxo contínuo de pacotes SNMP ao servidor. Todos os testes foram executados nos modos cifrado e texto corrente.

2.2 Os Resultados do Teste

Foram detectadas muitas diferenças em como os utilizadores são autenticados. Alguns produtos utilizam o algoritmo MD5, outros utilizam certificados X.509 que são verificados por uma autoridade de certificação, enquanto outros utilizam *tokens* e *passwords* atribuídas pelo gestor de rede. Alguns esquemas baseados em *token* também utilizam o MD5. Neste caso, a informação de segurança é salvaguardada pois é atribuída *out of band*, antes de qualquer tentativa de autenticação.

Foi requerido que todos os produtos cifrassem os dados de forma a garantir a confidencialidade e prevenir qualquer tipo de ataque de *man-in-the-middle*[3]. Todos os produtos examinados têm um módulo de cifragem automática, e somente dois não permitem aos utilizadores desligarem-no: o Intraport da Compatible Systems e o Safenet LAN VPN Encryptor da Information Resource Engineering.

Neste cenário particular procurou-se saber quais as funcionalidades se as chaves de cifragem e os mecanismos de autenticação ficarem comprometidos. Especificamente, qual a facilidade com que um gestor pode revogar uma chave e atribuir uma nova. Os produtos da Check Point, Isolation, Sun, e Timestep receberam classificações de 5.

Verificou-se também quais os produtos que permitem a cifragem na LAN. Mas todas as soluções VPN assumem que a rede local é confiável e por isso não permitem a cifragem.

[3] Man-in-the-midle – ataque que consiste em forjar uma conversação fazendo-se passar pelo *host* confiável.

No cenário de duas companhias ligadas por um túnel cifrado, verificou-se a facilidade de configurar controlos de acesso (para os recursos de cada parceiro) e como é que as chaves seriam trocadas. Para os produtos *firewalls* da Check Point, Cisco, IBM, Isolation, e Radguard, isto não constitui um problema, pois uma função primária dos *firewalls* é o controlo de acesso. Os produtos da Aventail, Compatible Systems, IRE, V-One, e VPNet tratam o controlo de acesso de acordo com o endereço IP, o Altavista baseia-o no servidor do túnel. Os produtos da Redcreek e Timestep não suportam controlo de acesso.

A maioria dos produtos testados efectuam algum tipo de gestão de chaves automática, geralmente um dos protocolos de gestão de chaves: ISA/KMP e o SKIP. Os que suportam o ISA/KMP são a Cisco, IRE, Isolation Systems, Radguard, e Timestep. Os que suportam o SKIP são a Check Point, Sun, e VPNet. Os outros produtos utilizam técnicas manuais ou proprietárias.

No cenário da gestão remota, verificou-se a facilidade com que o gestor de rede poderá, por exemplo, remotamente cancelar uma chave comprometida. Todos os produtos permitem efectuar esta tarefa remotamente. No entanto, determinados requisitos devem ser preenchidos previamente: deve existir uma VPN entre a localização do gestor de rede e o servidor, e o gestor de rede deve dispor de *software* de gestão.

Outra verificação teve que ver como o produto VPN trata as tentativas de entrada no sistema de utilizadores sem chaves válidas. Para isso, estabeleceu-se uma ligação segura com o servidor remoto e no meio da sessão fez-se a troca de chaves. Os produtos que detectaram imediatamente o cancelamento da chave foram os da Check Point, Radguard, e Sun.

Na verificação da resposta do sistema quando o ficheiro *log* fica cheio os resultados variaram. Alguns produtos simplesmente reescrevem as entradas antigas – os produtos da Altavista, Check Point, Compatible, Redcreek, Sun, e VPNet. Outros efectuam o *backup* do *log* para um dispositivo secundário e reescrevem o *log* – os produtos da Aventail, IBM, IRE, and V-One. O produto da Radguard permite ao gestor de rede decidir o que fazer quando o *log* encher, enquanto que o da Timestep simplesmente efectua o *shutdown* do dispositivo. Os produtos da Cisco e da Isolation utilizam o *syslog* para efectuar as funções de *logging*. Pelo menos nenhum deles continua a funcionar sem nenhum *log*, o que seria tão mau como funcionar sem segurança nenhuma.

O teste final deste cenário envolveu a configuração de múltiplos *sites*. Os únicos produtos com esta capacidade são os da Altavista, Check Point, IBM, Radguard, Sun, Timestep, e VPNet.

O teste do desempenho enfrentou alguns problemas. Devido às diferenças entre os produtos foi necessário criar diferentes plataformas de teste. Cinco fornecedores providenciaram dispositivos com interfaces 100Base-T, enquanto os restantes providenciaram interfaces 10Base-T. O gerador de tráfego não fornecia pacotes à velocidade da linha, de forma que

seria possível aos produtos com maior desempenho obterem maiores taxas se confrontados com um tráfego mais pesado.

Para efectuar a comparação mais justa possível, tomou-se como referência o desempenho das próprias plataformas de teste. Utilizou-se o gerador de tráfego Intermark e foram registados as taxas de transferência de referência, para o tráfego unidireccional foram de 8.88 e 57.88 Mbit/s nas redes 10Base-T e 100Base-T respectivamente, e para o tráfego bidireccional 8.72 e 11.60 Mbit/s. Estes valores representam o *throughput* da camada de aplicação, sendo a taxa de transferência na linha substancialmente maior.

Foi colocado cada produto na plataforma de teste e medido o *throughput*. Devido às dificuldades inerentes à comparação entre os produtos 10 e 100-Mbit/s, os resultados foram normalizados apresentando-os como percentagens do *throughput* de referência.

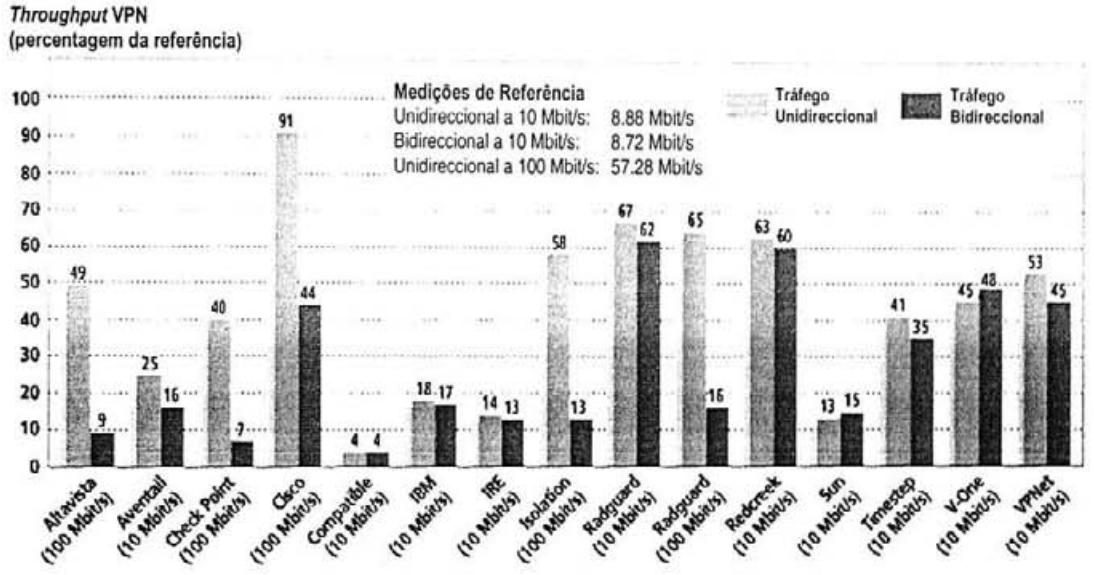


Figura 10.10 – Avaliação do Desempenho VPN [ShaDC98v]

Quase todos os produtos obtiveram um maior desempenho com tráfego unidireccional do que com bidireccional (Figura 10.10). Isto sugere que as VPNs afectam o desempenho. Mas a maioria das aplicações são bidireccionais por natureza, e o facto de o desempenho bidireccional ser na maioria dos casos bastante menor indica que o comportamento da aplicação provavelmente mascarará qualquer penalização que a VPN introduza.

2.3 As Conclusões dos Outros Testes de Laboratório

No teste de Julho de 98 da Data Communications (Tabela 10.9 na secção A.2) foram testadas somente soluções de *hardware-software*. Todos os produtos testados passaram o desafio de segurança – a passagem em mais de 200 tipos de ataque. Na maioria dos casos a gestão remota dos dispositivos é fácil. Mas o desempenho provou ser problemático, especialmente para ligações T1 (1.544 Mbit/s) ou superiores. No pior caso do teste de *stress*, os dis-

positivos perderam de 50 a 85 por cento do tráfego gerado.

No teste de Novembro de 97 da Byte (Tabela 10.10 na secção A.2), o Aventail VPN impressiona pela sua flexibilidade, suporte extensivo de métodos de cifragem, e variedade de opções de autenticação. A cifragem e autenticação podem ser controlados num nível de serviço a serviço, e podem ser utilizados filtros adicionais para limitar o acesso do utilizador ou protegê-lo de Java ou ActiveX potencialmente hostis. É extremamente versátil no suporte a múltiplas plataformas em clientes e servidores.

Neste teste, salienta-se no FireWall-1 o permitir ao administrador criar ligações VPN com acesso irrestrito ao protocolo de rede, ou com um nível extra de segurança ao permitir ao *firewall* restringir ou permitir certos tipos de tráfego. A configuração VPN do FireWall-1 é mais acessível a profissionais, mas é também muito mais flexível que a maioria e suporta uma grande variedade de opções de cifragem e autenticação.

O Eagle NT obteve uma boa classificação graças ao seu suporte para múltiplos esquemas de cifragem e autenticação, bem como à sua possibilidade de selectivamente controlar o acesso a recursos internos através das regras de acesso do *firewall*. As suas capacidades de monitorização e de *logging* impressionam.

2.4 Tabelas dos Testes de Laboratório de VPNs

Apresentam-se nas próximas páginas as tabelas com os resultados dos testes de laboratório de VPNs: Tabela 10.7 – VPNs do Teste de Laboratório de Setembro de 97, Tabela 10.8 – Cenários de Gestão da VPN, Tabela 10.9 – VPNs do Teste de Laboratório de Julho de 98, Tabela 10.10 – As VPNs do Teste de Laboratório de Novembro de 97.

Fabric.	Produto	Topologias	Firewall Integrado	Portas de LAN	Autenticação	Cifragem	Gestão de Chaves	Tunneling	Config. Remota segura	Resol. Log cheio	Sistema Operativo	Preço (serv. E 100 lig.)
Plataformas de Software												
Altavista	Altavista Tunnel 97	Server to server, client-server	Sim	N/A	MD5, RC4	DES, RC4	RSA B-Safe	Proprietário	Não	Rotação	BSDI Unix; Digital Unix; Ultrix; Windows 95, NT 3.51, 4.0	$9,905
Aventail	Aventail VPN Server 2.03	Server to server, client-server	Não	N/A	MD5, PAP, CHAP, Radius, SSL 3.0, SecurID	DES, Triple DES, RC4, SSL 3.0, RSA, Diffie-Hellman	Chave pública/ privada	PPTP, L2TP, L2F	Sim	Backup e Rotação	AIX; HP UX; DEC Unix; Solaris; WFW 3.x; Windows 95, NT 3.51, 4.0	$20,095
Check Point	Check Point Firewall-1 3.0	Server to server, client-server	Sim	N/A	MD5, S-Key, SecurID, Zxent	Ipsec, DES, Triple DES	ISA/ KMP, SKIP, FWZ, Ipsec manual	PPTP, L2TP, L2F	Sim	Rotação	DEC Unix; SCO Unix; AIX; MS DOS; PC DOS; Windows NT 4.0	$4,995 (50 util.) $18,990 (ilimit.)
IBM	IBM Firewall for AIX 3.1	Server to server, client-server	Sim	N/A	MD5, Passphrase, SecurID, Assurenet Pathways S/net Key, Open API	Ipsec, DES, CDMF	Manual, IBM firewall –firewall protocol, propriet. Dynam. Protocol over SSL	Nenhum	Sim	Backup e Rotação	AIX; OS/2; Windows 95	$8,840
Sun	Sunscreen EFS 1.1	Client-server	Sim	N/A	SKIP authentication	RC2, RC4, DES, Triple DES	SKIP	SKIP	Sim	Rotação	Solaris 2.4, 2.5, 2.6; Windows 95; X86	$4,995
V-One	Smartgate NT Server 2.3	Client-server	Não	N/A	MD5, Smartgate Mutual authentication	DES, RC4	Process o de registo Online	Smartgate Tunneling	Sim	Backup e Rotação	BSDI; HP-UX; Irix; Mac OS; Sun OS; Solaris; Windows 95, NT 3.51, 4.0	$5,595
Plataformas de Hardware/Software												
Cisco	Cisco PIX Firewall	Server to server	Sim	10 Base-T, 100 Base-T	Radius, Tacacs+	DES	Manual	Ipsec-ESP	Sim	Via OS	N/A	$9,000[1]
Compatible	Intraport Network Access Server	Client-server	Não	10 Base-T	MD5	Personal Level Encryp-tion	None	Generic routing encapsula-tion, STEP	Sim	Rotação	Windows 95	$38,935
IRE	Safenet LAN VPN Encryptor	Server to server, client-server	Não	10 Base-T	Safenet Smartcard, password	DES	ANSI X9.17	IETF RFC 1631	Sim	Backup e Rotação	Windows 95, NT 4.0	$20,990

(Contin.) Fabric.	Produto	Topologias	Firewall Integra-do	Portas de LAN	Autenticação	Cifragem	Gestão de Chaves	Tunneling	Config. Remota segura	Resol. Log cheio	Sistema Operativo	Preço (serv. E 100 lig.)
Isolation	Infocrypt Enterprise	Server to server, client-server	Sim	10 Base-T, 100 Base-T	MD5, PAP, CHAP, Radius, SSL 3.0, SecurID	Ipsec, DES, Triple DES	Certifi-cados digitais, Diffie-Hellman	Isolation Tunneling	Sim	Via OS	Windows 95, NT 4.0	$9,950
Radguard	CIPro	Server to server, client-server	Sim	10 Base-T, 100 Base-T, token ring	MD5, SHA-1, certificate authority, hardware tokens	Ipsec, DES, Triple DES	ISA/ KMP, Diffie-Hellman, certifi-cados digitais	Ipsec-ESP	Sim	User-defined	Windows 95, NT 4.0	$9,950
Redcreek	Ravlin 10	Server to server, client-server	Não	10 Base-T	MD5, X.509, DSS, PAP, CHAP, Radius	DES, Triple DES, IDEA	ISA/ KMP	Ipsec-ESP	Sim	Rotação	Windows 95, NT 3.51, NT 4.0	$6,500
Timestep	Permit Security Gateway	Server to server, client-server	Não	10 Base-T	MD5, certificados, passwords	DES, RCA	Timeste p Security Associ-ation Protocol	None	Sim	Shutdo wn	Windows 95, NT 3.51, NT 4.0	$21,804
VPNet	VSU 1010	Server to server, client-server	Não	10 Base-T	MD5	DES, Triple DES, RC4	SKIP	Ipsec-ESP	Sim	Rotação	Windows 95	$4,995

1. 66 ligações
CHAP = Challenge authentication protocol
DES = Data Encryption Standard
ESP = Encapsulating security payload
IDEA = International Data Encryption Algorithm
ISA/KMP = Internet Security Association & Key Management Protocol
L2F = Layer 2 Forwarding
L2T = Layer 2 Tunneling
N/A = Não aplicável
PPTP = Point-to-point tunneling protocol
SKIP = Simple Key Management for IP
SSL = Secure Sockets Layer

Tabela 10.7 – VPNs do Teste de Laboratório de Setembro de 97 [ShaDC98v]

	Alta-Vista	Aven-tail	Check Point	Cisco	Com-patible	IBM	IRE	Isola-tion	Rad-guard	Red-creek	Sun	Time-step	V-One	VPNet
Cenário 1: Acesso Remoto														
Tipo de autenticação	Passwd	Passwd/ tokens	Passwd/ tokens	N/A	Passwd	Passwd	Passwd/ tokens	Tokens	Passwd/ tokens	Passwd	MD5/ Passwd	Passwd/ tokens	Smar-tgate Mutual Authen-tication	Passwd/ Radius/ SecurID
Cifragem automática	Verific.	Verific.	Verific.	N/A	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.
Facilidade de revogação da chave	4	3	5	N/A	4	4	3	5	4	N/A	5	5	3	4
Facilidade de atribuição de chaves	4	3	5	N/A	4	4	3	5	4	N/A	5	5	3	4
Cenário 2: Gestão de Chaves														
Limitar o acesso	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Não	Sim	Sim
Troca de chaves automática	Verific.	Verific.	Verifed	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.
Frequência de revisão chaves automática	Verific.[1]	Verific.	Verific.	N/A	Verific.	Verific.	Verific.	Verific.[1]	Verific.[1]	Verific.[1]	Verific.[1]	Verific.[1]	Verific.	Verific.
Facilidade de cancelamento de uma chave	4	3	5	2	4	4	3	4	4	N/A	5	5	3	4
Reconhecimento do algoritmo	Não	Não	Não	Não	Não	N/A	Não	Não	N/A	N/A	Não	Não	Não	N/A
Cenário 3: Regras Internacionais														
Gestão de tamanho chaves diferenciados	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.[1]	Verific.
Distribuição de chaves internacional	Manual	Autom.	Manual	Manual	Manual	Manual	Manual	Autom.	N/A	Manual	Autom.	Autom.	Manual	Autom.
Cenário 4: Gestão Remota														
Cancelar chaves	Verific.[1]	Não Verific.[2]	Verific.	N/A	Verific.	Verific.	Verific.	Verific.	Verific.	N/A	Verific.	Verific.	Verific.	Verific.
Negar acesso à rede	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.	Verific.
Cancelar detecção de chaves	4	N/A	5	3	3	4	3	4	5	N/A	5	3	3	4
Profiling Genérico	Verific.	Verific.	Verific.	Não	Verific.	Verific.	Verific.	Verific.	Verific.	Não	Verific.	Verific.	Não	Verific.
Configurações Simultâneas	Verific.	Não	Verific.	Não	Não	Verific.	Não	Não	Verific.	Não	Verific.	Verific.	Não	Verific.

1. Definido pelo utilizador
2. Suportado em versão Unix (não verificado)
Facilidade da tarefa: 1 = menos fácil, 5 = mais fácil
N/A = Não aplicável

Tabela 10.8 – Cenários de Gestão da VPN [ShaDC98v]

Fabric.	Produto/ versões de software testadas	Interfaces suportados/ Max interfac. Ethernet	Firewall/ IP router	Cifragem	Gestão de chaves	Autenticação do utilizador	CA	Gestão de rede	Software cliente	Preço por cliente	Preço por dispos. VPN[1]
Internet Devices	Fort Knox Policy Router/4.0	Half- e full-duplex Ethernet, half- e full-duplex fast Ethernet/3	Sim/sim	DES, triple DES, 40- e 128-bit RC4	IKE	CA externa (3Q98), passwords, Radius 3Q98), cartões de autenticação token (3Q98)	Não	Web-based	Windows 95, Windows 98, Windows NT 4.0 (3Q98)	$40 (25 util.), $20 (1000 ou +)	$5,990 (3 interf.)
Radguard	cIPro-VPN/3.05	Half- e full-duplex Ethernet, half- e full-duplex fast Ethernet/2	Sim/sim	DES, triple DES	IKE draft version 9	CA integrada ou externa, cartões de autenticação token	Sim	HP Openview	Windows 95, Windows NT 3.51, 4.0	$100	VPN: $5,950; CA: $5,950
Redcreek	Ravlin 10/2.2x	Half- e full-duplex Ethernet/2	Não/não	DES, triple DES (3 chaves ou 168-bits)	IKE draft version 9, Ipsec manual keying	CA externa, Radius, cartões cartões de autenticação token	Não	CA Unicenter, Castle Rock SNMPc, HP Openview, IBM Netview e TME 10, Sun Solstice	Windows for Workgroups 3.11, Windows 95, Windows NT 4.0	$20 a $45	$3,500
Shiva	LANrover VPN Gateway/6	Async, half- e full-duplex Ethernet, half- e full-duplex fast Ethernet, V.35/2	Sim/sim	DES, triple DES	IKE, Shiva Smart Tunneling	CA externa, CHAP, PAP, Radius, cartões de autenticação token	Vend. Sepa-rad.	CA Unicenter	Windows 95, Windows 98, Windows NT 4.0	Dep. Quant.	$9,250
Timestep	Permit Gate 4520/1.00	Half- e full-duplex Ethernet/2	Não/sim	Blowfish, CAST, DES, triple DES, IDEA, RC5	IKE draft version 7	CA integrada ou externa, Radius (3Q98), cartões de autenticação token	Sim	HP Openview, qualquer sistema baseado em SNMP	MacOS, Windows 95, Windows NT 4.0	$40 (1000 util.)	$5,495
VPNet	VSU 1010/2.0	Half-duplex Ethernet, EIA-232/2	Não/sim	DES, triple DES	IKE draft version 9, SKIP	CA externa, CHAP, Radius, cartões cartões de autenticação token	Não	CA Unicenter, Castle Rock SNMPc, HP Openview, IBM Netview e TME 10, Sun Solstice	Windows 95, Windows NT 4.0	$99 (1 util.) a $22 (600 ou +)	$4,995 (2 interf.)

1. Preço por dispositivo VPN assume-se um interface Ethernet, um interace V.35, e todo o software necessário.

CA = Certificate authority

CAST = Carlisle Adams and Stafford Tavares

CHAP = Challenge authentication protocol

DES = Data encryption standard

IDEA = International Data Encryption Algorithm

IKE = Internet Key Exchange

ISAKMP = Internet Security Association and Key Management Protocol

PAP = Password authentication protocol

Radius = Remote authentication dial-in user service

RC = Ron's code

SKIP = Simple Key Exchange Internet Protocol

Tabela 10.9 – VPNs do Teste de Laboratório de Julho de 98 [NewDC98v]

Fabricante	Produto	Tecnologia	Funcionalidades e Funções VPN	Implementação	Facilidade de Utilização	Pontuação Geral
Aventail	Aventail VPN 2.5	4	4	4	4	4
Check Point	Check Point FireWall-1 3.0a	4	4	4	3	4
Raptor Systems	Eagle NT 4.0	4	4	4	3	4
Microsoft	Microsoft Routing and Remote Access Service	3	2	3	3	3
Secure Computing	BorderWare Firewall Server 4.1	4	3	3	2	3
Sun Microsystems	SunScreen SKIP 1.1	3	3	3	2	3
Trusted Information Systems	Gauntlet 4.0	3	3	3	3	3
AltaVista	AltaVista Tunnel 97	2	2	4	3	2
Data Fellows	F-Secure Virtual Private Network 1.1	3	2	2	2	2
FTP Software	Secure Client 3.0	3	2	2	2	2

Pontuação: 0 = Não suportado; 1 = Deficiente; 2 = Positivo; 3 = Bom; 4 = Muito Bom; 5 = Excelente.

Tabela 10.10 – As VPNs do Teste de Laboratório de Novembro de 97 [SterBt97]

3. Testes de Sistemas de Detecção de Intrusões

Em colaboração com a NSTL, a Data Communications sujeitou os vários produtos IDS a várias formas de ataque, avaliou as capacidades de gestão, e efectuou o *benchmark* do desempenho.

Os IDSs identificaram os ataques em redes sem tráfego bem como em segmentos *Ethernet* com bastante tráfego, mas num segmento Fast Ethernet largamente utilizado a vigilância desaparece; de facto nenhum produto detectou todos os ataques quando a rede estava largamente utilizada.

3.1 A Metodologia de Teste

A Data Communications convidou oito fornecedores IDS a participarem no teste, tendo reunido os seguintes:

- Abirnet com o Session Wall-3 Release 3,
- Anzen com o Anzen Flight Jacket 1.2 (Network Flight Recorder v. 1.6.2),
- Cisco com o Netranger 2.1.1,
- ISS com o RealSecure 2.1,
- Internet Tools com o ID-Trak 2.0.

A Axent Technologies, a Network Associates, e a Security Dynamics declinaram o convite alegando que os seus produtos se destinam a detecção de intrusões em *hosts* e não em redes, o que constitui o objectivo do teste. Foi solicitado aos fabricantes o fornecimento de um sistema de detecção de intrusões (IDS) e *hardware*, incluindo uma interface 10/100Base-T para monitorar e um interface 10Base-T para gestão *out-of-band*.

Foi avaliada a segurança, o desempenho, e a facilidade de utilização. Nos testes de segurança, foi verificado se cada produto era capaz de reconhecer formas de ataque comuns. Os ataques foram executados a partir de uma subrede 100Base-T através de um *router* para a subrede 100Base-T monitorada pelo IDS.

Foram executados 10 ataques: o *ping sweep*, que executa *pings* para todos os *hosts* de uma dada gama de endereços; o *port scan*, que verifica as respostas das portas UDP; o *dig*, que questiona um servidor DNS sobre informação acerca de *hosts*; o *SYN flood*, que bombardeia um *host* com inúmeros pedidos para abrir *sockets* TCP; o *ping of death*, que envolve um pacote *echo* ICMP extremamente grande; o *land*, que envolve um pacote com o mesmo endereço IP de origem e destino e número de porta TCP; *floods* ICMP e UDP, que carregam um *host* com tantos pedidos que pedidos legítimos não são respondidos; o *supernuke*, um ataque que bloqueia algumas máquinas Windows que escutam a porta 139; e o *teardrop 2*, onde um pacote UDP formado impropriamente provoca o bloqueio do *host*. Foi observado se o IDS

detectava cada ataque na subrede monitorada.

Para avaliar o desempenho, foram executados os mesmos ataques mas a linha foi submetida a tráfego bidireccional em *background*. Foram submetidos dois tipos de tráfegos; o primeiro consistia num igual número de pacotes TCP de 64, 128, 256, e 512 *bytes*. Foi depois submetido tráfego bidireccional que consistia somente de pacotes de 64 *bytes*. Ambos os tráfegos foram submetidos a taxas agregadas de 10%, 20%, e 40%, e foram anotados os ataques detectados pelo IDS.

Para avaliar a facilidade de utilização, foram desenvolvidos alguns cenários que representam tarefas chave do IDS e foram classificadas as facilidades de cada produto para completar essas tarefas. No primeiro cenário, tentou-se definir uma nova "assinatura" de ataque e adicioná-la ao IDS. No segundo, tentou-se produzir um relatório contendo o número, frequência, e origem dos ataques detectados pelo IDS. Foram classificadas cada uma das tarefas: geração do relatório, alteração do intervalo coberto pelo relatório, e adição ou remoção de itens do relatório. Finalmente, foi avaliado a interface e clareza da documentação para cada produto. Foi utilizada uma escala de 1 a 5.

3.2 Os Resultados do Teste

A maioria dos produtos deste teste consiste num monitor de uma estação de gestão que recebe dados do monitor (Tabela 10.11 na secção C.3.4). O Sessionwall-3 da Abirnet, que é gerido localmente, é a excepção. Ao contrário dos produtos RMON (*remote monitoring*), os IDSs não utilizam o SNMP (que não suporta facilidades de segurança na sua versão actual) para transmitir informação do monitor para o gestor. Em vez disso, utilizam vários meios de autenticação e cifragem. Uma outra característica de segurança, as interfaces de gestão de todos os produtos com excepção do ID-Trak da Internet Tools são passivas, de forma que um atacante não tem possibilidade de detectar quando é que o IDS está a escutar.

Todos os produtos incluem rotinas pré-definidas para a detecção de ataques específicos, e todos permitem adicionar rotinas que detectam novos ataques à medida que são descobertos. O mais flexível de todos é Flight Jacket da Anzen, que inclui uma poderosa linguagem de *scripting* que permite a definição de virtualmente qualquer evento.

Uma limitação em todos os produtos é que funcionam somente em segmentos de acesso partilhado, e não em redes comutadas. Os fabricantes estão a tentar introduzir a tecnologia IDS nos *switches*, mas por agora recomendam a colocação dos monitores IDS nos segmentos chave de acesso partilhado e ligar *hubs* aos *switches* sempre que tráfego comutado deva ser monitorado.

O teste de desempenho serviu não só para descrever o desempenho em redes de produção mas também para encontrar o limite do desempenho do sistema. A situação de maior carga (40% de utilização, ou cerca de 60.000 pacotes por segundo) não se encontra em redes

de produção.

Os vários produtos, na operação a 10% ou 20% de utilização, comportaram-se exactamente como em redes sem tráfego. Somente o RealSecure da ISS falhou dois ataques, mas a versão beta do próximo lançamento (RealSecure 2.5) detectou-os (Tabela 10.12 na secção C.3.4).

Mas ao subir a fasquia para 40%, somente com duas excepções, todos os produtos falharam cada um dos ataques. Isto significa que os ataques podem passar despercebidos desde que exista tráfego suficiente na rede.

Os resultados pioraram ainda mais com tráfego de pacotes de 64 *bytes* (Tabela 10.13 na secção C.3.4). A utilização de poderosas configurações de *hardware* ajuda grandemente na detecção de ataques em situações de grande carga na rede, no entanto, isso não é o suficiente. O Flight Jacket da Anzen foi o único produto a detectar ataques a 40% de carga na rede, tendo utilizado um poderoso Pentium II a 400 MHz. Mas Marcus Ranum da Network Flight Recorder referiu que a versão do *software* utilizada foi optimizada para segmentos com grande utilização. O Netranger da Cisco, apesar de ter um sensor IDS de *hardware/software*, detectou só 5 ataques com 20% de carga da rede e nenhum com 40%.

Será motivo de preocupação o facto de os IDSs não detectarem ataques em períodos de grande utilização da rede. Talvez não se encontrem redes de produção com as cargas oferecidas, mas pequenos picos de tráfego são bastante comuns. Desta forma o IDS pode ser vítima de um ataque de negação de serviço, que constitui o tipo de ocorrências que em primeiro lugar é suposto evitar ou pelo menos identificar.

Apesar disso, todos os IDSs detectaram a generalidade dos ataques com 10% de carga na rede com vários tamanhos de pacotes, o que é equivalente a um segmento de rede Ethernet com carga máxima. Desta forma responderão bem em segmentos Ethernet de 10 Mbit/s com grande carga.

Os fabricantes direccionam agora a atenção para o aperfeiçoamento do desempenho dos seus produtos, quer pela optimização de *software* ou por embeberem código em *hardware*. Enquanto isso não acontecer o desempenho não será compatível com a segurança, e a alternativa com garantia de segurança será a utilização de segmentos de 10 Mbit/s.

Foi também avaliada a interface de cada produto e as ferramentas de relatório e verificou-se a facilidade de gestão. No primeiro cenário, a configuração do IDS para reconhecer um novo ataque, todos os produtos permitem definir as rotinas de reconhecimento do ataque e todos de forma fácil (Tabela 10.14 na secção C.3.4). Os produtos da Abirnet, Cisco, e ISS são os mais fáceis de gerir neste aspecto. Os produtos da Anzen e Cisco são os melhores em termos de flexibilidade.

No segundo cenário, a criação de um relatório utilizando o IDS, novamente todos os produtos foram muito bons ou excelentes, enquanto os produtos da Anzen, ISS, e o Internet Tools são os mais fáceis de utilizar. O RealSecure da ISS tem a interface mais fácil de utilizar, com um ecrã de alto nível que ordena os alertas de segurança pelo nível de risco e lista os *hosts* monitorados.

3.3 As Conclusões dos Outros Testes de Laboratório

No teste de Maio de 98 da InfoWorld (Tabela 10.15 na secção C.3.4), alguns dos critérios utilizados na classificação das soluções não eram adequados para o caso em estudo (custos, interoperabilidade e facilidade de configuração) pelo que, de acordo com os dados obtidos no teste, foram redefinidos de forma a reflectirem as suas importâncias para o caso em estudo.

Das soluções testadas evidenciaram-se o RealSecure da ISS e o Flight Jacket da Anzen. O Flight Jacket foi a melhor solução na detecção de ataques tendo obtido excelentes resultados, o RealSecure foi o que obteve melhores resultados na correcta identificação e resposta aos ataques e nas ferramentas de relatório.

O terceiro conjunto de soluções (Tabela 10.16 na secção C.3.4), são análises da revista PC Week sobre as características técnicas e não incluem testes aos produtos. Constituiu assim um conjunto de dados comparativos.

3.4 Tabelas dos Testes de Laboratório de IDSs

Apresentam-se nas próximas páginas as tabelas com os resultados dos testes de laboratório de sistemas de detecção de intrusões: Tabela 10.11 – Sistemas de Detecção de Intrusões do Teste de Laboratório de Agosto de 98, Tabela 10.12 – Ataques Detectados em Redes com Tráfego, Tabela 10.13 – Teste de *Stress* do IDS, Tabela 10.14 – Gestão IDS do Teste de Laboratório de Agosto de 98, Tabela 10.15 – Resultados do Teste de Laboratório de Maio de 98 e Tabela 10.16 – Resultados dos Testes Individuais.

Fabric.	Produto	Sistema testado	Sistema operativo	Topologias	Configura-ção remota	Métodos de reconf. Remota do sistema	Opções de alerta	Frequênc. updates da BD de ataques	Preço (25/100/ 1,000 nós)
Abirnet	Session Wall-3 Release 3	266-MHz Pentium II, 64 Mbytes RAM, Windows 95	Windows 95, Windows 98, Windows NT 4.0	Half- e full-duplex Ethernet, half- e full-duplex fast Ethernet, token ring, FDDI	Não suportado	Configura cada dispositivo separada-mente	Inserção no log, tom audí-vel, e-mail, fax, pager, envio de trap ao NMS, exec. de DLL ou comando	Download a partir do Web site	$1,495/ $4,950/ $14,950
Anzen	Anzen Flight Jacket 1.2 (Network Flight Recorder v. 1.6.2)	400-MHz Pentium II, 128 Mbytes RAM, BSDI Unix 3.1	BSDI Unix, FreeBSD, HP-UX, Linux, NetBSD, OpenBSD, Solaris, Windows NT 4.0	Half- e full-duplex Ethernet, half- e full-duplex fast Ethernet, FDDI	Data Fellows' SSH; SSL para acesso Web	Download dos novos ficheiros de config. p/ múltiplos dispositivos com um comando	Inserção no Log, e-mail, fax, pager, envio de trap ao NMS, um alerta para utilizador	3 vezes por ano	$5,500/ $5,500/ $5,500
Cisco	Netranger 2.1.1	Sensor: Dual-CPU 266 MHz Pentium II, 128 Mbytes RAM, Solaris 2.6; director: Sparc Ultra 5, 128 Mbytes RAM, Solaris 2.6	Sensor: Solaris; director: AIX, HP-UX, Solaris	Full-duplex Ethernet, full-duplex fast Ethernet, token ring, FDDI	IKE ou SKIP na gestão de chaves; DES ou triple DES na cifragem; SHA-1 ou MD5 na autenticação	Configura cada dispositivo separada-mente	Inserção no log, tom audí-vel, e-mail, fax, pager, envio de trap ao NMS, um alerta para utilizador	Com cada nova release; mensal-mente com início em Outubro	$25,000/ $25,000/ $25,000[1]
ISS	RealSecure 2.1	333-MHz Pentium II, 128 Mbytes RAM, Windows NT Server 4.0 com SP 3	Solaris, Solaris x86, Windows NT 4.0	Half-duplex Ethernet, half-duplex fast Ethernet, token ring, FDDI	RSA ou cifragem elliptic curve (chaves até 163-bit); autenticação de troca de chave desafio	Configura cada dispositivo separada-mente	Inserção no log, tom audí-vel, e-mail, fax, pager, envio de trap ao NMS, alarme em tempo real ao NMS	Mensal-mente	$8,995/ $8,995/ $8,995
Internet Tools	ID-Trak 2.0	300-MHz Pentium II, 64 Mbytes RAM, Windows NT Server 4.0 com SP 3	Windows 95, Windows 98, Windows NT 3.51, Windows NT 4.0	Half- e full-duplex Ethernet, half- e full-duplex fast Ethernet	Cifragem de 64-bit; autenticação MD5	Download dos novos ficheiros de config. p/ múltiplos dispositivos com um comando	Inserção no log, tom audí-vel, e-mail, fax, pager, envio de trap ao NMS, terminar a sessão do intruso	À medida que forem conheci-dos novos ataques	$3,999 (50 nós)/ $5,499/ $9,999

1. Preço cobre o hardware e software para um sensor e software de gestão. MD5 = Message digest 5
DES = Data encryption standard NMS = Network management system
DLL = Dynamic link library SHA-1 = Secure hashing algorithm 1
IKE = Internet Key Exchange SSL = Secure sockets layer

Tabela 10.11 – Sistemas de Detecção de Intrusões do Teste de Laboratório de Agosto de 98 [NewDC98i]

	Abirnet			Anzen			Cisco			ISS			Internet Tools		
	10%	20%	40%	10%	20%	40%	10%	20%	40%	10%	20%	40%	10%	20%	40%
Ping sweep	●	●	⊗	●	●	●	●	●	⊗	●	●	⊗	●	●	⊗
Port scan	●	●	⊗	●	●	●	●	●	⊗	●	●	⊗	●	●	⊗
Dig	●	●	⊗	●	●	●	●	●	⊗	⊗[1]	⊗[1]	⊗	●	●	●
SYN flood	●	●	⊗	●	●	●	●	●	⊗	●	●	⊗	●	●	⊗
Ping of death	●	●	⊗	●	●	●	●	●	⊗	●	●	⊗	●	●	⊗
Land attack	●	●	⊗	●	●	●	●	●	⊗	●	●	⊗	●	●	⊗
ICMP flood	●	●	⊗	●	●	●	●	●	⊗	●	●	⊗	●	●	⊗
UDP flood (loop infinito)	●	●	⊗	●	●	●	●	●	⊗	●	●	⊗	●	●	⊗
UDP flood (porta inatingível)	●	●	⊗	●	●	●	●	●	⊗	●	●	⊗	●	●	⊗
Supernuke	●	●	⊗	●	●	●	●	●	⊗	●	●	⊗	●	●	⊗
Teardrop 2	●	●	⊗	●	●	●	●	●	⊗	⊗[1]	⊗[1]	⊗	●	●	⊗

● - Detectado
⊗ - Não detectado

1. Detectado com o Realsecure v. 2.5 (beta)

Streams bidireccionais de pacotes de 64, 128, 256, e 512 *bytes* submetidos como tráfego em *background*.

Tabela 10.12 – Ataques Detectados em Redes com Tráfego [NewDC98i]

	Abirnet			Anzen			Cisco			ISS			Internet Tools		
	10%	20%	40%	10%	20%	40%	10%	20%	40%	10%	20%	40%	10%	20%	40%
Ping sweep	⊗	⊗	⊗	●	●	●	●	⊗	⊗	●	●[2]	⊗	⊗	⊗	⊗
Port scan	⊗	⊗	⊗	●	●	⊗	●	●	⊗	●	●[2]	⊗	⊗	⊗	⊗
Dig	⊗	⊗	⊗	●	●	⊗	●	⊗	⊗	⊗[1]	⊗[1]	⊗	⊗	⊗	⊗
SYN flood	⊗	⊗	⊗	●	●	⊗	●	●	⊗	●	●[2]	⊗	●	⊗	⊗
Ping of death	⊗	⊗	⊗	●	●	⊗	●	●	⊗	●	●[2]	⊗	⊗	⊗	⊗
Land attack	⊗	⊗	⊗	●	●	●	●	⊗	⊗	●	●[2]	⊗	⊗	⊗	⊗
ICMP flood	⊗	⊗	⊗	●	●	⊗	●	●	⊗	●	●[2]	⊗	⊗	⊗	⊗
UDP flood (loop infinito)	⊗	⊗	⊗	●	●	⊗	●	⊗	⊗	●	●[2]	⊗	⊗	⊗	⊗
UDP flood (porta inatingível)	⊗	⊗	⊗	●	●	●	●	●	⊗	●	●[2]	⊗	⊗	⊗	⊗
Supernuke	⊗	⊗	⊗	●	●	⊗	●	⊗	⊗	●	●[2]	⊗	⊗	⊗	⊗
Teardrop 2	⊗	⊗	⊗	●	●	⊗	●	⊗	⊗	⊗[1]	⊗[1]	⊗	⊗	⊗	⊗

● - Detectado
⊗ - Não detectado

1. Detectado com o Realsecure v. 2.5 (beta)
2. Detectado e efectuado o *log*, não foi despoletado o alarme.

Streams bidireccionais de pacotes de 64 *bytes* submetidos como tráfego em *background*.

Tabela 10.13 – Teste de *Stress* do IDS [NewDC98i]

	Abirnet	Anzen	Cisco	ISS	Internet Tools
Definição de novos ataques	5	4	5	5	4
Geração de relatórios	4	5	4	5	5
Alterar os limites intervalos dos relatórios	4	4	4	5	4
Adicionar/remover itens nos relatórios	5	4	5	5	5
Documentação	4	4	4	4	4
Interface do *software*	4	3	4	5	4
Pontuação total	4.33	4	4.33	4.83	4.33

Pontuação: 0 = Não suportado; 1 = Deficiente; 2 = Positivo; 3 = Bom; 4 = Muito Bom; 5 = Excelente.

Tabela 10.14 – Gestão IDS do Teste de Laboratório de Agosto de 98 [NewDC98i]

Fabric.	Produto	Arqui-tectura	Reconhe-cimento Ataques	Respos. Ataques e Relatórios	Admin. e Segu-rança	Configu-ração e Manuais	Interope-rabilidade[1]	Custos	Pont. Geral	Custos[2] *software/ hardware*	Fonte/ Data
			20%	20%	20%	15%	15%	10%	100%		
Abirnet	Session Wall-3 2.1	Baseada na rede	2	2	3	3	3	5	2,8	$1,495 $800	Info World Maio/98
IBM	IERS (NetRanger)	Baseada na rede	2	3	4	3	3	1	2,8	$195,000	Info World Maio/98
Internet Security Systems	RealSecure 2.0	Baseada na rede	2	4	3	3	4	4	3,3	$8,995 $3,100	Info World Maio/98
Network Flight Recorder/ Anzen	NFR/Anzen Flight Jacket	Baseada na rede	5	3	2	2	3	3	3,1	$15,070	Info World Maio/98

1. Salienta-se a interoperabilidade com Digital Unix e Windows NT. Se baseado na rede considera-se suficiente o suporte a uma das versões dos S.O. referidos; se baseado no *host* considera-se essencial o suporte aos dois S.O. e Windows 95 (*hosts*).
2. Custos do *software* (e licenças) e de *hardware* (e *software* de base) para um segmento de rede com 1 servidor Digital Unix, 1 servidor Windows NT e 25 postos/utilizadores.

Tabela 10.15 – Resultados do Teste de Laboratório de Maio de 98 [BroIW98i]

Fabric.	Produto	Arqui-tectura	Tecnol. e funciona-lidades	Desempe-nho	Gestão	Facilda-de Utili-zação	Interope-rabilidade[1]	Custos	Pont. Geral	Custos[2] software/ hardware	Fonte/ Data
			20%	20%	20%	15%	15%	10%			
Internet Tools	ID-Trak 2.0	Baseada na rede	4	4	3	3	4	4	3,7	$4,000 $1,800	PC Week Ago/98
Arbinet	Session Wall-3 v1 Release 3	Baseada na rede	4	4	4	4	3	5	4,0	$1,495 $1,800	PC Week Ago/98
Network Associates	CyberCop Network (NetRanger)	Baseada na rede	4	4	1	3	4	2,0	3,1	$24,000 $8,000	PC Week Jul/98
Centrax Corp.	Entrax 2.0	Baseada no *host*	4	4	4	5	2	3,0	3,8	$12,995 $1,800	PC Week Jun/98
Axent Technologies	OmniGuard/ ITA 3.0	Baseada no *host*	4	4	1	4	5	4,0	3,6	$7,355 $1,800	PC Week Mar/98
Internet Security Systems	RealSecure 2.0	Baseada na rede	4	4	4	4	4	4,0	4,0	$8,995 $3,100	PC Week Fev/98

3. Salienta-se a interoperabilidade com Digital Unix e Windows NT. Se baseado na rede considera-se suficiente o suporte a uma das versões dos S.O. referidos; se baseado no *host* considera-se essencial o suporte aos dois S.O. e Windows 95 (*hosts*).
4. Custos do *software* (e licenças) e de *hardware* (e *software* de base) para um segmento de rede com 1 servidor Digital Unix, 1 servidor Windows NT e 25 postos/utilizadores.

Tabela 10.16 – Resultados dos Testes Individuais

4. Constrangimentos e Requisitos Técnicos

Apresenta-se a seguir uma tabela com as restrições da exportação da cifragem de vários produtos VPN e *firewall*.

		Tamanho Máximo da Chave		
		Nos EUA	Fora dos EUA	
Vendedor	Produto		Sem recuperação de chave	Com recuperação de chave
Hardware VPN				
Radguard Ltd. Tel Aviv, Israel, http://www.radguard.com	CIPro	Triple DES	112-bit DES	Não oferecido
Timestep Corp. Kanata, Ontario, http://www.timestep.com	Permit Enterprise	Triple DES, 168-bit RC5	Triple DES, 56-bit RC5	Não oferecido
VPNet Technologies Inc. San Jose, Calif., http://www.vpnet.com	VSU-1000, VSU-1010	Triple DES	56-bit DES	Não oferecido
Firewalls				
Check Point Software Technologies Inc. Redwood City, Calif., http://www.checkpoint.com	Firewall 1	56-bit FWZ-1, 56-bit DES	40-bit FWZ-1	Não oferecido
Netguard Ltd. Migdal Ha-Emek, Israel, http://www.netguard.com	Guardian	Triple DES, 128-bit RC4	Triple DES, 128-bit RC4	Não oferecido
Network Associates Santa Clara, Calif., http://www.nai.com	Gauntlet	Triple DES	56-bit DES	Triple DES

Tabela 10.17 – Restrições da Cifragem

Apresentam-se a seguir os *e-mails* das respostas dos fabricantes relativamente às restrições da exportação da cifragem dos produtos VPN e *firewall*.

De: **Luis Cardoso [SMTP:lusocresa@telepac.pt]**
Enviada em: Quinta-feira, 20 de Agosto de 1998 19:11
Para: 'jestrela@sc.ipp.pt'
Assunto: RE: VPN key size

...

Use any encryption engine you choose
Guardian's VPN supports Microsoft's CryptoAPI, which is becoming a global standard for encryption applications. As a result, you may select any encryption module that is compatible with CryptoAPI. The Windows NT package includes two encryption engines by RSA: RC2 and RC4. These Windows engines support key length of 42 to 48 bit and comply with US export regulations. In the local US edition of Windows NT, 128 bit encryption engines are provided. The customer may use any other encryption engine that is compatible with Cryp-

toAPI according to his preference and local regulations.

De: **Avi Rembaum [SMTP:avi@radguard.com]**
Enviada em: Segunda-feira, 24 de Agosto de 1998 9:48
Para: José Estrela
Assunto: Re: Question about clPro.

...

RADGUARD can and does export to Europe Triple DES encryption systems. We are required to obtain permission from the Israeli government to do so, but obtaining such approval does not in any way involve back door or key escrow options. We are not limited by US export restrictions.

De: **Hamutal Einhorn [SMTP:hamutal@checkpoint.com]**
Enviada em: Quarta-feira, 26 de Agosto de 1998 10:51
Para: José Estrela
Cc: hamutal@checkpoint.com; herveb@checkpoint.com
Assunto: Re: FWZ-1 key length

...

Check Point FW-1 v3 supports 2 types of encryption schemes:
VPN: FWZ1 48 bit
VPN-DES: 56 bit
Check Point can freely export FW-1 type FWZ1 to Portugal. End users that would like to obtain FW-1 VPN DES need to receive specific export license (requires end user declaration). Around October this year Check Point FW-1 will include strong encryption 3DES (168 bit).

...

Check Point products are produced in Israel and therefore subject to the Israeli export control. 3DES can be exported to Portugal provided that the end user receives an export license.

5. Testes de Ferramentas de Auditoria de Segurança

A Network Computing testou quatro soluções de auditoria de segurança em múltiplos *sites*:

- NetSonar Vulnerability Scanner and Network Mapping System 1.0 da Cisco Systems,
- Internet Scanner 5.0 da Internet Security Systems (ISS),
- Netective Site 1.0 da NETECT,
- Ballista Security Auditing System 2.4 da Secure Networks.

Antes do teste dos *scanners* de segurança, foram consideradas as necessidades de segurança – *scanning* preciso, relatórios informativos, uma base de dados de exploração actualizável e um processo de *scanning* eficiente.

5.1 A Metodologia de Teste

O ambiente de teste consistiu num *array* de dispositivos e plataformas: *routers* Bay Networks e Cisco Systems, *hubs* e *switches*; e ambientes AIX, Linux, Netware, Solaris e Windows NT. Não só se reuniu uma diversidade de sistemas operativos, mas também várias versões.

Foram reunidas máquinas executando *jobs* de produção e máquinas cuidadosamente camufladas com falhas de segurança conhecidas. Foi assegurado que alguns dos sistemas operativos foram actualizados com os *patches* e versões de resolução de problemas, enquanto outros continham somente a instalação base. Foi utilizada uma combinação de máquinas de produção e máquinas operadas por utilizadores, e combinou-se um conjunto de falhas conhecidas com problemas desconhecidos e deixou-se para as ferramentas de auditoria de segurança o trabalho de *scanning*.

5.2 Os Resultados do Teste

A solução dos problemas de segurança de rede não passam somente por uma defesa completa de *firewall*, mas também por um conjunto de sistemas segurança de próxima geração, tais como os *scanners* de segurança examinados no teste. Tendo evoluído de ferramentas como a SATAN de Farmer e Venema e o ISS de Klaus, estas soluções fazem uma verificação da configuração de segurança de rede, utilizam verificações internas e análise de regularidades para testar os *hosts* designados, procurando falhas e más configurações.

As funcionalidades gerais encontradas nos *scanners* de segurança são bastante impressionantes (ver Tabela 10.18 e Tabela 10.19 na secção 5.4), no entanto têm também alguma imaturidade. Cada produto é particularmente forte em pelo menos uma área e algo limitado noutras. Salienta-se a interface e a pormenorização de relatórios do Internet Scanner, as verificações e flexibilidade do Ballista, o trabalho de base nas actualizações automáticas e verificação de integridade do Netective, e a flexibilidade de relatórios do NetSonar.

O *scanning* geral do Internet Security Scanner impressionou. Dispõe de uma variedade de verificações e um dispositivo de relatórios detalhado. É a ferramenta de auditoria de segurança mais completa que foi testada, sendo rivalizada somente pelo Ballista da Secure Networks.

Tal como o Ballista, o Internet Scanner conduz múltiplos *scans* simultaneamente o que contribui para a eficiência geral. No teste de rede, o *scanning* de 20 *hosts* foi completado em menos de 15 minutos.

A outra ferramenta que se destacou foi o Ballista Security Auditing System. Oferece um grande conjunto de verificações com algumas opções de configuração. Oferece algumas excelentes funcionalidades, incluindo ferramentas para o *cracking* pró-activo de *passwords* e

fortes capacidades de configuração. No entanto, tem duas fraquezas importantes. A primeira, os mecanismos de relatório precisam de um profundo reformulação. Segundo, a verificação de falhas pode ser esporádica, pois não detectou algumas das falhas de segurança mais importantes.

5.3 As Conclusões dos Outros Testes de Laboratório

No teste de Março de 98 da InfoWorld [BrolW98s], apesar de não apresentar tabelas comparativas das soluções testadas, o Internet Scanner da ISS é o mais elogiado. Demonstrando uma lista de vulnerabilidades impressivamente detalhada e completa, e relatórios das vulnerabilidades apelativos. Estes resultados são incomparáveis nos outros produtos. No entanto, precisa de ferramentas adicionais quando acede à segurança de uma rede empresarial, particularmente ferramentas baseadas no *host*.

A outra solução que se evidenciou, o Enterprise Security Manager (ESM) 4.4 da Axent utiliza um mecanismo gestor/agente, em oposição à abordagem de teste remoto do Internet Scanner. O ESM identifica as falhas de segurança baseadas no *host* que o Internet Scanner pode ter falhado. Tem agentes para quase todos os tipos de Unix, VMS, NT, e Netware, incluindo agentes para bases de dados Oracle e AS/400, e planeia disponibilizar agentes para *firewalls*, *routers*, e servidores da Web.

O Internet Scanner pesquisa cada serviço executado na rede e detecta mesmo algumas falhas potenciais do NT, e analisa também os *firewalls*. O ESM não está preparado para identificar esses problemas. Ao contrário, analisa uma enorme quantidade de falhas baseadas no *host* (por exemplo integridade e privilégios de ficheiros e objectos, integridade de contas e analise de *passwords*, etc.), comparando-as com os parâmetros do utilizador. Desta forma com o ESM, não existem vulnerabilidades per si, somente excepções à política de segurança definidas.

Por esta razão, é recomendado utilizar quer ferramentas de segurança de rede quer de segurança do *host*, para obter uma imagem correcta da segurança da rede durante a auditoria. E não somente pela perspectiva global da segurança que isso oferece, mas por ser uma boa forma de obter uma *defence in depth* com múltiplos *checkpoints* através dos quais um atacante terá de passar e também menores hipóteses de alguma falha de segurança passar despercebida.

No teste de Outubro de 97 da Network World, (Tabela 10.20 na secção 5.4), confronta novamente o Internet Security Scanner e o Enterprise Security Manager, tendo sido novamente o primeiro a obter melhores resultados, com evidência para a detecção de falhas de segurança de rede e funcionalidades gerais.

5.4 Tabelas dos Testes de Laboratório de Auditoria de Segurança

Apresentam-se a seguir as tabelas com os resultados dos testes de laboratório de sis-

temas de auditoria de segurança: Tabela 10.18 – As Ferramentas de Auditoria de Segurança da Network Computing, Tabela 10.19 – Características de *Scanning* de Segurança e Tabela 10.20 – As Ferramentas de Auditoria de Segurança do Teste de Outubro de 97.

Fabricante	Produto	Precisão/ Funcionalidades	Relatórios	Política de Actualizações	Preço	Pontuação Total
	Ponderação	40%	30%	20%	10%	
Internet Security Systems	Internet Scanner 5.0	4,5	4	2,5	4	3,9
Secure Networks	Ballista Security Auditing System 2.4	4	2	4	4	3,4
Cisco Systems	NetSonar Vulnerability Scanner and Network Mapping System 1.0	3	3,5	2,5	4	3,15
NETECT	Netective Site 1.0	1	3	5	4	3,7

Pontuação: 0 = Não suportado; 1 = Deficiente; 2 = Positivo; 3 = Bom; 4 = Muito Bom; 5 = Excelente.

Tabela 10.18 – As Ferramentas de Auditoria de Segurança da Network Computing [ShiNC98]

	NetSonar Vulnerability Scanner and Network Mapping System 1.0	Internet Scanner 5.0	Netective Site 1.0	Ballista Security Auditing System 2.4
Características				
Plataformas suportadas	Solaris (SPARC e x86)	NT, AIX, HP-UX, Solaris, Linux	Solaris (SPARC)	NT, Solaris, BSD, Linux
***Scanning* de segurança:**				
Verificações Unix	●	●	●	●
Verificações NT	●	●	●	●
Verificações VAX/VMS	⊗	●	⊗	⊗
Verificação de integridade Binária	⊗	⊗	Somente Solaris	⊗
Verificações de negação de serviço	●	●	⊗	●
Agente de *Firewall*	⊗	●	⊗	●
Actualizações Automáticas	⊗	⊗	●	⊗
Capacidades de *scripting* configuráveis	●	⊗	⊗	●
Password cracking	⊗	⊗	⊗	●
Escalonamento de tarefas	●	⊗	⊗	⊗
Preço:				
Classe-C	$2,995/$6,995	$4,995	$3,995	$4,000/ano
Ilimitado (valor anual)	$34,000			$10 (mais de 2000 dispositivos)

● - Sim
⊗ - Não

Tabela 10.19 – Características de *Scanning* de Segurança [ShiNC98]

Fabricante	Produto	Resultados	Funcionalidades	Administração	Instalação e configuração	Total
		40%	25%	25%	15%	
Internet Security Systems, Inc.	Internet Scanner 4.3.3	5	4,5	4,5	4	4,6
Axent Technologies, Inc.	OmniGuard/ Enterprise Security Manager (ESM) 4.4	4	3,5	4,5	4	4,0
Trusted Information Systems, Inc.	Stalker 2.1	4	3,5	4	3	3,7
Shareware	COPS 1.04	2,5	2,5	2	3	2,5
Shareware	Asmodeus 0.22	2,5	2	2,5	2	2,3

Tabela 10.20 – As Ferramentas de Auditoria de Segurança do Teste de Outubro de 97 [KatNW97]

Bibliografia

[Aberde97] AberdeenGroup, "Vulnerability Assessment: Empowering IS to Manage Actual Risk", An Executive White Paper, September 1997.

[Anoni97] Anónimo, "Maximum Security – A Hacker's Guide to Protecting your Internet Site and Network", Sams.net, 1997.

[AvolTIS] Avolio, Frederick M. "Firewalls and Virtual Private Networks", Network Security White Paper, Trusted Information Systems.

[AvoBla98] Avolio, Frederick M.; e Blask, Chris; "Application Gateways and Stateful Inspection", A Brief Note Comparing and Contrasting, Trusted Information Systems, January, 1998.

[AvoRan94] Avolio, Frederick M.; e Ranum, Marcus "A Network Perimeter with Secure External Access", In Proceedings of the Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February, 1994.

[Balens93] Balenson, David "Privacy Enhancement for Internet Electronic Mail: Part III: Algoritms, modes, and identifiers", RFC 1423, February, 1993.

[BelMer91] Bellovin, Steven M., e Merrit, Michael "Limitations of the Kerberos Authentication System", USENIX Conference Proceedings, Inter, 1991.

[BelMer92] Bellovin, Steven M., e Merrit, Michael "Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks", Proceedings IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, May, 1992.

[BroIW98i] Broderick, John; McClure, Stuart; e Scambray, Joel; "Network intrusion-detection solutions", Test Center Comparison, InfoWorld Electric, May 4, 1988.

[BroIW98s] Broderick, John; McClure, Stuart; e Scambray, Joel; "Network security checkup", Test Center Analysis, InfoWorld Electric, March 16, 1988.

[Bryant88] Bryant, B., "Designing an Authentication System: A Dialogue in four scenes",

February, 1988.

[CasOut90] Case, Jefrey; Fedor, Mark; Schoffstall, Martin; e Davin, James, "Simple Network Management Protocol (SNMP)", RFC 1157, May, 1990.

[ChapZw95] Chapman, D. Brent, e Zwicky, Elizabeth D., "Building Internet Firewalls", O'Reilly & Associates, 1995.

[CheckP98] Check Point Software Technologies Ltd., "Stateful Inspection Firewall Technology", TECH NOTE, 1998.

[ChesBe94] Cheswick, William R., e Bellovin, Steven M., "Firewalls and Internet Security – Repelling the Wily Hacker", Addison-Wesley, 1994.

[ClarCN98] Clark, Tim "Web site alarms boost security ", CNET NEWS.COM, January 26, 1981.

[DenSac81] Dennig, Dorothy E.; e Sacco, Giovanni M., "Timestamps in Key Distribution Protocols", Communications of the ACM, August, 1981.

[DifHel76] Diffie, W., e Hellman, M., "New Directions in Cryptography", IEEE Transactions on Information Theory, November, 1976.

[DornDC98] Dornan, Andrew, "Encryption – Seeing Through Keyholes ", Data Communications, July, 1998.

[Doty95a] Doty, Ted, "A Firewall Overview", ConneXions, Vol. 9, n° 7, July, 1995.

[Doty95b] Doty, Ted, "Towards Real Internet Security", ConneXions, Vol. 9, n.° 12, December, 1995.

[Ellerm96] Ellerman, Uwe, "IPv6 and Firewalls", http://www.cert.dfn.de/eng/team/ue/fw/ipv6fw/home.html, DFN-CERT, 1996.

[FarSpa90] Farmer, Dan; e Spafford, Eugene, "The COPS Security Checker System", In USENIX Conference Proceedings, Anaheim, CA, Summer, 1990.

[GarINET] Gardner, James, "Security On The Internet and SSL", Paper, I-net, Australia.

[Haller94] Haller, Neil M., "The S/Key one-time password system", Proceedings of the Internet Society Symposium on Network and Distributed System Security, February, 1994.

[Hunt98] Hunt, Ray, "Network Security", Tutorial, 7th IFIP/ICCC Conference on Information Networks and Data Communications, Aveiro, Portugal, June 15-17, 1998.

[Hurw98] Hurwicz, Michael, "Cracker Tracking: Tighter Security with Intrusion Detection", Byte, May, 1998.

[ISO91] ISO, "Information Technology – Telecommunications and Information Exchange Between Systems – Transport Layer Security Protocol", Draft International Standard (DIS) 10736, October, 1991.

[ISO92] ISO, "Information Technology – Telecommunications and Information Exchange Between Systems – Network Layer Security Protocol", Draft International Standard (DIS) 11577, November, 1992.

[ISS97a] Internet Security Systems Inc. (ISS), "Adaptive Security Model: A Model Solution – A Solution Model", White Paper, Atlanta, GA, September, 1997.

[ISS97b] Internet Security Systems Inc. (ISS), "Real-time Attack Recognition and Response: A Solution for Tightening Network Security", White Paper, Atlanta, GA, 1997.

[Kalisk93] Kaliski, Burt, "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services", RFC 1424, February, 1993.

[KatNW97] Kates, Jim, "Beating back the hackers", Product Testing, Network World, October 27, 1998.

[Kaufm93] Kaufmam, Charles, "DASS – Distributed Authentication Security Service", RFC 1507, September, 1993.

[KenPW98a] Phillips, Ken "OmniGuard/ITA thwarts insider attacks – Axent Technologies' software blocks hack attempts in real time", PC Week Labs, PC Week, March 11, 1998.

[KenPW98b] Phillips, Ken "Detectors blanket network with security – SessionWall-3 provides overall protection; ID-Trak concentrates on threats from outside", PC Week Labs, PC Week, August 10, 1998.

[Kent93] Kent, Stephen, "Security Options for the Internet Protocol", RFC 1108, November, 1991.

[KerTIS] Ker, Keith, "GVPN White Paper", Network Security White Paper, Trusted

Information Systems.

[KimSpa93] Kim, Gene; e Spafford, Eugene, "The Design and Implementation of Tripwire: A File System Integrity Checker", Technical Report CSD-TR-93-071, Purdue University, 1993.

[KohlNe93] Kohl, John; e Neuman, Cliff, "The Kerberos Network Authentication Service (V5)", RFC 1510, September, 1993.

[LaMOdl91] LaMacchia, Brian A.; e Odlyzko, Andrew M., "Computation of Discrete Logaritms in Prime Fields", Designs, Codes and Cryptography, 1991.

[Lampor81] Lamport, Leslie, "Password Autentication with Insecure Communications", Communications of the ACM, November, 1981.

[LaiMas90] Lai, X., e Massey, J., "A Proposal for a New Block Encryption Standard", Proceedings, EUROCRYPT '90, Springer-Verlag, 1990.

[LaiMas91] Lai, X., e Massey, J., "Markov Ciphers and Differential Cryptanalysis", Proceedings, EUROCRYPT '91, Springer-Verlag, 1991.

[Leutw94] Leutwyler, K., "Superhack", Scientific American, July, 1994.

[Linn93a] Linn, John, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", RFC 1421, February, 1993.

[Linn93b] Linn, John, "Generic Security Service Application Program Interface", RFC 1508, September, 1993.

[LomOut94] Lomas, Mark.; Gong, Li; Saltzer, Jerome; e Needham, Roger, "Reducing Risks from Poorly Chosen Keys", Proceedings of the Twelfth ACM Symposium on Operating Systems Principles, SIGOPS, December, 1989.

[MilOut87] Miller, S. P.; Neuman, B. C.; Schiller, J. I.; e Saltzer, J. H., "Kerberos Authentication and Authorization System", Project Athena Tecnical Plan, MIT, December, 1987.

[Morr85] Morris, Robert, "A Wekness in the 4.2 BSD Unix TCP/IP Software", Computing Science Technical Report 117, AT&T Bell Laboratories, Murray Hill, NJ, February, 1985.

[MorrTh79] Morris, Robert; e Thompson, Ken "Unix Password Security", Communications of the ACM, November, 1979.

[NeeSch78] Needham, R. M.; Schroeder, M., "Using Encryption for Authentication in Large Networks of Computers", Communications of the ACM, December, 1978.

[NeeSch87] Needham, R. M.; Schroeder, M., "Authentication Revisited", Operating Systems Review, January, 1987.

[NetGen97] Network General, "Protecting Your Network: The Choice Between Active and Static Security Technologies", A Network Visibility Guide, October, 1997.

[NewDC97f] Newman, David; Holzbaur, Helen; e Bishop, Kathleen; "Firewalls: Don't Get Burned", Lab Test, Data Comunications, March 21, 1997.

[NewDC98f] Newman, David; Holzbaur, Helen; e Carter, Michael; "NT Firewalls: Tough Enough", Lab Test, Data Comunications, April, 1998.

[NewDC98i] Newman, David; Giorgis, Tadesse; e Yavari-Issalou, Farhad; "Intrusion Detection Systems: Suspicious Finds", Lab Test, Data Comunications, August, 1998.

[NewDC98v] Newman, David; Giorgis, Tadesse; e Yavari-Issalou, Farhad; "VPNs: Safety First, But What About Speed?", Lab Test, Data Comunications, July, 1998.

[Pfleeg97] Pfleeger, Charles P. "Security in Computing", Prentice Hall, 1997.

[PtaNew98] Ptacek, Thomas H.; e Newsham, Timothy N., "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection", Secure Networks, Inc., January, 1998.

[RiShAd78] Rivest, R.; Shamir, A.; e Adleman, L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communications of the ACM, February, 1978.

[Rivest92] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April, 1992.

[SDNS388] SDNS, "Secure Data Networking System Security Protocol 3 (SP3)", Technical Report Revision 1.3, SDNS Protocol and Signalling Working Group, SP3 Sub-Group, July 1988.

[SDNS488] SDNS, "Secure Data Networking System Security Protocol 4 (SP4)", Technical Report Revision 1.2, SDNS Protocol and Signalling Working Group, SP4 Sub-Group, July 1988.

[SeacBt97] Seachrist, David; Holzbaur, Helen, "Firewall Software for NT and Unix", Byte Software Lab Report, Byte, June, 1997.

[SET97] SET Secure Electronic Transaction LLC Website, "The SET Standard Book 1 Business Description", The SET Standard Technical Specifications, May, 1997.

[ShaDC98v] Shah, Deval; e Holzbaur, Helen; "VPNs: Security With an Uncommon Touch", Lab Test, Data Comunications, September 21, 1997.

[ShiNC98] Shipley, Greg, "Holy Intruders!: IP-Based Security Auditing Tools", Product Testing, Network Computing, July 15, 1998.

[Stall94a] Stallings, W., "Cryptographic Algorithms, Part I: Conventional Cryptography", ConneXions, Vol. 8, nº 9, September, 1994.

[Stall94b] Stallings, W., "Cryptographic Algorithms, Part II: Public-key Encryption and Secure Hash Functions", ConneXions, Vol. 8, nº 10, October, 1994.

[Stall95] Stallings, W. "Network and Internetwork Security – Principles and Practice", Prentice Hall, 1995.

[SteOut88] Steiner, Jennifer; Neuman, Clifford; e Schiller, Jeffrey, "Kerberos: An Authentication Service for Open Networked Systems", Proceedings of the Winter 1988 USENIX Conference, February, 1988.

[SterBt97] Stern, Morgan, "Extend Your Net with VPNs", Byte Software Lab Report, Byte, November, 1997.

[SurPW98a] Surkan, Michael "RealSecure fends off network attacks – Version 2.0 is even better at defending against IP attacks in real time", PC Week Labs, PC Week, February 25, 1998.

[SurPW98b] Surkan, Michael "Entrax lags server guards – NT intrusion detector from Centrax lacks rivals' features", PC Week Labs, PC Week, June 17, 1998.

[Tuchm79] Tuchman, W., "Hellman Presents No Shortcut Solutions to DES", IEEE Spectrum, July, 1979.

[Venema92] Venema, Wietse, "TCP WRAPPER: Network Monitoring, access control and booby traps", In Proceedings of the Third Usenix UNIX Security Symposium, Baltimore, MD, September, 1992.

[WeilNW98] Weil, Nancy, "U.S. govt.'s encryption standard cracked in record time", IDG News Service, Network World Fusion, July 20, 1998.

[Wiener93] Wiener, M., "Efficient DES Key Search", Proceedings, Crypto '93, Springer-Verlag, 1993.

[Wray93] Wray, Jonh, "Generic Security Service API: C-bindings", RFC 1509, September1993.

[Zimmer92] Zimmerman, Philip, "PGP User's Guide", September, 1992.

FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Departamento de Engenharia Electrotécnica e de Computadores

ANEXO

Segurança em Redes de Computadores – Estudo de um Caso

José Manuel Moreira Estrela

Mestrado em Engenharia Electrotécnica e de Computadores
pela Faculdade de Engenharia da Universidade do Porto

Dissertação submetida para satisfação parcial dos
requisitos do grau de mestre
em
Engenharia Electrotécnica e de Computadores
(Área de especialização de Telecomunicações)

Dissertação realizada sob supervisão de
Professor Doutor José Ruela,
do Departamento de Engenharia Electrotécnica e de Computadores
da Faculdade de Engenharia da Universidade do Porto

Porto, Dezembro de 98

Índice

1. Introdução 1

2. Validação da Solução de Segurança de Rede 3

2.1 A Plataforma de Teste 3

2.2 A Configuração da Plataforma de Teste 4

2.2.1 A Implementação do *Firewall* e VPN 4

2.2.2 A Configuração do Dispositivo IDS 6

2.2.3 A Configuração da Ferramenta de Auditoria 6

2.3 A Auditoria de Vulnerabilidades 6

2.3.1 Os Resultados da Auditoria com o Internet Scanner 6

2.3.2 Os Resultados do IDS e a Simulação de Ataques ao Sistema 8

2.4 Conclusões 10

Apêndice A. Relatórios de Vulnerabilidades 11

1. Relatório de Vulnerabilidades do *Firewall Gateway* 11

2. Relatório de Vulnerabilidades do *Router* 13

3. Relatório Final de Vulnerabilidades do *Host* Bastião 15

Direitos Legais do Software Utilizado 17

Índice das Ilustrações

Figura 2.1 – A Plataforma de Teste 3
Figura 2.2 – A Política de Segurança Implementada 5
Figura 2.3 – A Política de Segurança para os Routers 6
Figura 2.4 – Ataques Detectados pelo RealSecure 10

1. Introdução

Este anexo à dissertação de mestrado visa a documentação dos testes realizados à arquitectura de segurança de rede proposta na dissertação e que só foi possível realizar após a data da entrega da mesma.

A necessidade de efectuar o teste da solução para a sua aplicação real no âmbito da actividade profissional associada à necessidade de completar o estudo da arquitectura proposta comprovando-a, motivaram a realização deste anexo.

Começa-se por caracterizar a plataforma de teste, descrevendo-se de seguida a implementação e configuração das ferramentas, incluindo a definição da política de segurança da rede que implementa as *firewall gateways* e as VPNs.

Descreve-se depois a auditoria realizada, detalhando-se as vulnerabilidades detectadas no *firewall gateway*, *host* bastião e *router*, e a respectiva resolução. Finalmente simulam-se ataques de forma a comprovar a eficácia do *firewall* e do dispositivo IDS.

2. Validação da Solução de Segurança de Rede

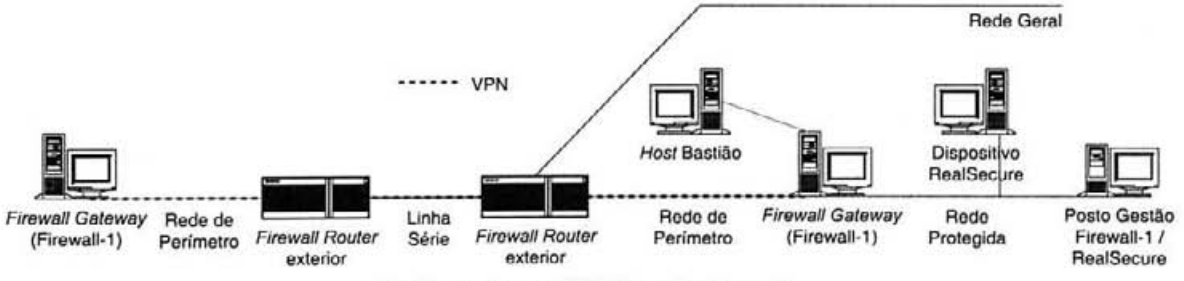
Neste capítulo descreve-se a implementação da plataforma de teste da arquitectura de segurança e depois de aplicada a metodologia de teste são descritos os testes realizados.

Como foi referido na dissertação os testes permitem a validação da solução implementada pela utilização da ferramenta *scanning* e pela simulação de alguns ataques à rede.

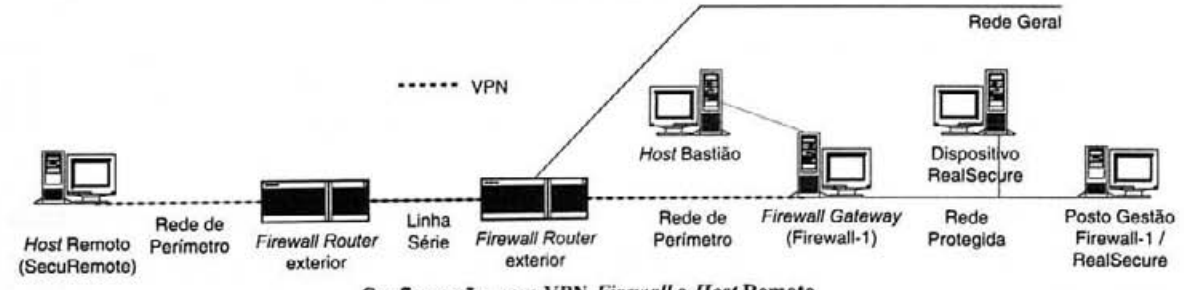
2.1 A Plataforma de Teste

Apresenta-se novamente, a arquitectura de teste da solução de segurança. Definiram-se duas configurações de teste (Figura 2.1) que permitem testar as arquitecturas de segurança com VPN *firewall* a *firewall* (entre SC e ISEP, ISCAP e ESMAE) e com VPN *firewall* a *host* remoto (entre SC e ESEIG-pv e ESEIG-vc). As configurações dos componentes utilizados são as seguintes:

- *Routers* exteriores – Cisco 2503 com IOS 11.2.
- *Firewall Gateways* – com Windows NT Server 4.0, o módulo do Firewall-1, e para além do SNMP mais nenhum serviço de rede instalado.



Configuração com VPN *Firewall* a *Firewall*



Configuração com VPN *Firewall* a *Host* Remoto

Figura 2.1 – A Plataforma de Teste

- *Host* Bastião - com Windows NT Server 4.0, o serviço de Mail Microsoft Exchange 5.5, o Internet Information Server disponibilizando os serviços de WWW e FTP, e Microsoft Proxy 2.0.
- *Host* Remoto, Posto de Gestão e Dispositivo RealSecure – Windows NT Workstation 4.0.

2.2 A Configuração da Plataforma de Teste

Partindo-se da plataforma de teste e das versões (*full functional*) das ferramentas seleccionadas, aplicou-se a metodologia previamente definida. As ferramentas e as respectivas versões foram as seguintes:

- Firewall-1 3.0b (VPN) para Windows NT da CheckPoint.
- RealSecure 2.5 para Windows NT da Internet Security Systems.
- Internet Scanner 5.4 para Windows NT da Internet Security Systems.

Após a instalação e configuração do *hardware* da plataforma de teste, iniciou-se uma fase de instalação, configuração e experimentação das ferramentas. Após o domínio do funcionamento e potencialidades das ferramentas iniciou-se então a configuração final, com vista à validação da plataforma de teste.

2.2.1 A Implementação do *Firewall* e VPN

O Firewall-1 utiliza o protocolo SNMP para a obtenção automática das propriedades na definição dos objectos da rede (máquinas, redes, *routers*, etc.), em particular a definição dos *routers* e das máquinas com o módulo de *firewall* (*gateways*).

Para os *gateways* define-se também as características de cifragem: o método de cifragem (somente disponível o FWZ), os domínios de cifragem (quais os segmentos de rede que terão as suas comunicações cifradas), e gerando-se a chave CA (Autoridade de Certificação) para o posto de gestão e obtendo-se deste as chaves Diffie-Hellman para as *gateways*, que servirão para a autenticação entre as máquinas.

Definidos os objectos, a definição da política de segurança torna-se bastante intuitiva, pela simples selecção das origens e destinos dos dados e pelas respectivas acções a executar. As regras da política de segurança são definidas numa perspectiva global do *site*, depois cada *gateway* interpreta cada regra somente nos aspectos que lhe dizem respeito.

A política de segurança que serve como ponto de partida para as exigências definidas para o caso em estudo está traduzida na Figura 2.2, e que ao mesmo tempo traduz as regras de filtragem dos *firewall gateways* e implementa as VPNs.

No.	Source	Destination	Service	Action	Track	Install On
1	Any	IPPGateways	Any	reject	Alert	Dst
2	IPPGateways	Any	Any	reject	Alert	Src
3	HostBastiao	NTServer	smtp	accept	Short	Gateways
4	RedesProtegidas	RedesProtegidas	Any	Encrypt	Long	Gateways
5	RedesProtegidas	Any	Any	accept	Short	Gateways
6	Any	RedeDMZ	ftp http smtp	accept	Short	Gateways
7	UtilExter@AcessosExter	IPPServer	telnet	User Auth	Long	Gateways
8	UtilExter@PostosRemotos	IPPServer	telnet	Client Encrypt	Long	Gateways
9	Any	Any	Any	reject	Long	Gateways

Figura 2.2 – A Política de Segurança Implementada

O conjunto de regras relativas à política de segurança (Figura 2.2), tem a seguinte interpretação:

- Regra 1 – Evita qualquer acesso (utilizadores internos e externos) aos serviços das máquinas *firewall gateway*, tornando-as "transparentes".
- Regra 2 – Para proteger completamente os *firewalls gateway* inibe-se também as comunicações com origem na *gateway*.
- Regra 3 – O tráfego SMTP com origem no *host* bastião pode ser encaminhado para o servidor de *mail* interno.
- Regra 4 – O tráfego entre as redes protegidas é cifrado de *firewall gateway* a *firewall gateway*.
- Regra 5 – Os utilizadores das redes protegidas podem aceder à Intranet e à Internet.
- Regra 6 – Os utilizadores não locais só podem aceder à rede do servidor da Internet (*host* bastião) e aos serviços FTP, HTTP e SMTP.
- Regra 7 – Especifica que os utilizadores autorizados dos acessos exteriores poderão utilizar o serviço Telnet e terá de ser efectuada a autenticação (através das opções de cartões SecurID, S/Key, *password* de NT ou Unix, etc.).
- Regra 8 – As sessões (Telnet) iniciadas pelos utilizadores autorizados dos postos remotos são cifradas.
- Regra 9 – Rejeita e efectua o *log* de todas as outras comunicações.

De igual forma, o conjunto de regras da política de segurança referentes aos *routers* estão definidas na Figura 2.3.

No.	Source	Destination	Service	Action	Track	Install On
1	RedesProtegidas	RedesProtegidas	Any	accept		Routers
2	RedesProtegidas	Any	Any	accept		Routers
3	Any	RedeDMZ	smtp ftp http	accept		Routers
4	Any	Any	Any	reject		Routers

Figura 2.3 – A Política de Segurança para os *Routers*

2.2.2 A Configuração do Dispositivo IDS

O dispositivo IDS (RealSecure), por ser baseado numa larga base de dados de intrusões e extensivamente testado para os ambientes Windows NT e Unix, tornou a implementação bastante simples já que tem uma configuração de base que se aplica à generalidade das situações.

Para a sua exploração basta a ligação da máquina com o respectivo serviço activo utilizando o interface de rede em modo promíscuo.

2.2.3 A Configuração da Ferramenta de Auditoria

O Internet Scanner, também com uma configuração de base para uma auditoria padrão, permite efectuar o *scanning* de segurança de rede, local ou a qualquer dispositivo "visível" da rede, quer sejam máquinas NT ou Unix, *firewalls* ou *routers*.

Para o ambiente Windows NT, permite também a auditoria da segurança a nível do próprio sistema operativo. As suas potencialidades podem também, se configuradas para o efeito, provar categorias de ataques de negação de serviço e outras, que podem por em causa o normal funcionamento da máquina auditada.

2.3 A Auditoria de Vulnerabilidades

As máquinas submetidas à auditoria foram, no segmento de rede principal (para o outro segmento o processo seria idêntico), o *firewall*, o *host* bastião e o *router*, por serem aquelas potencialmente mais vulneráveis aos ataques. As máquinas NT foram configuradas com os requisitos mínimos de sistema exigidos: o Windows NT 4.0 com o Service Pack 3. Com esta configuração iniciou-se a auditoria.

2.3.1 Os Resultados da Auditoria com o Internet Scanner

No primeiro *scanning* detectou-se uma extensa gama de vulnerabilidades, no *Firewall*

gateway 7 vulnerabilidades de alto risco, 18 de médio risco e 33 de baixo risco. No *Host* Bastião, por disponibilizar vários serviços de rede, encontraram-se ainda mais vulnerabilidades, 11 de alto risco, 15 de médio risco e 58 de baixo risco. No *router* auditou-se 1 vulnerabilidade de médio risco e 4 de baixo risco.

Apresentam-se nos apêndices Apêndice A.1 e Apêndice A.2 os relatórios emitidos pelo Internet Scanner e que descrevem todas as vulnerabilidades detectadas no *firewall gateway* e *router*, bem como a respectiva resolução para cada um dos problemas. Sinteticamente listam-se algumas das mais importantes vulnerabilidades detectadas nas três máquinas:

- Getadmin – ataque de alto risco no qual um utilizar local pode obter privilégios de administrador ao executar o utilitário "getadmin".
- SecHole – utilitário que permite a um utilizador obter acesso de *debug* num processo do sistema.
- Teardrop Modificado – vulnerabilidade de médio risco que explora a forma como a pilha TCP/IP trata certas situações de excepção causadas por cabeçalhos UDP mal constituídos.
- Out of Band DoS – ataque de negação de serviço provocado pelo envio de dados Out of Band através do protocolo TCP.
- Ssping – é possível para um atacante provocar o *crash* do *host* ao enviar pacotes ICMP mal constituídos.
- Utilizadores Listados Através de uma "Sessão Nula" – o estabelecimento de uma sessão NetBios sem parâmetros que providenciem a lista de utilizadores, fornecendo a base para um futuro ataque de "força bruta".
- Negação de Serviço ao Windows NT – ataque de negação de serviço quando é feito um pedido de *logon* ao serviço SMB mal constituído, a máquina bloqueia ou reinicia.
- Serviço de *Routing* Activo (no *router*) – fornece a um intruso a informação de *routing*, e permitindo ao intruso o envio de pacotes RIP falsos que causem o envio dos dados para a máquina do intruso.
- Serviço *Messenger* Activo – vulnerabilidade de baixo risco que permite que um utilizador envie mensagens *pop-up* aos outros utilizadores, o que pode ser utilizado para ataques de "relacionamento social".
- Ataque de Negação de Serviço Land – vulnerabilidade que permite a um utilizador provocar um excesso de carga no CPU pelo envio de um pacote *spoofed* para uma porta que diz originar dessa mesma porta.
- Posix Activado – o Windows NT tem a classificação de segurança C2 se tiver o subsistema Posix desactivado. Com este subsistema activo é possível sujeitar o sistema a ataques de Cavalo de Tróia.
- Traceroute permitido – permite descobrir rotas até um *host* de rede.

A maioria destas vulnerabilidades foram resolvidas pela aplicação do Service Pack 4 do Windows NT (editado em Outubro de 98), e que substitui componentes do sistema com

bugs de segurança e outros. As outras vulnerabilidades foram resolvidas pela restrição de permissões a componentes do sistema, pela reconfiguração, remoção ou desactivação de serviços inseguros ou pela alteração de definições da política do sistema.

Após aplicadas as correcções referidas, foram efectuados novos processos de *scanning* que comunicaram a ausência de vulnerabilidades para o *firewall gateway* e *router*, mas que detectaram ainda algumas vulnerabilidades no *host* bastião (ver anexo Apêndice A.3). Estas vulnerabilidades ou se verificaram ser falsos positivos ou se referem a serviços desconhecidos do Internet Scanner nomeadamente do Microsoft Exchange e Microsoft Proxy. Analisando algumas das vulnerabilidades:

- FPNWCLNT.DLL tem *checksum* incorrecto (alto risco) – esta DLL alterada permitiria o acesso em texto corrente às novas *passwords*; no entanto o *checksum* só é dado como incorrecto porque a DLL foi substituída pelo SP4 do Windows NT.
- Utilizador com Privilégio de Actuar como Sistema (alto risco) – falso positivo já que é o utilizador "administrator" que actua como sistema para executar os serviços do Microsoft Exchange.
- Log do Windows NT Acessível (alto risco) – também falso positivo pois foi o utilizador "administrator" que executou o *scanner* no acesso ao *log* do sistema, e só ele tem acesso ao *log*.

As restantes vulnerabilidades são na sua generalidade falsos positivos, merecendo um estudo mais aprofundado as que dizem respeito ao serviço de Mail do Microsoft Exchange, já que este serviço, não tendo sido auditado, poderá conter algumas eventuais vulnerabilidades.

Da análise deste relatório de vulnerabilidades e com base em hipotéticas vulnerabilidades referentes a serviços *proxy* no *host* bastião, concluiu-se da necessidade de considerar uma alternativa de uma das configurações na arquitectura de segurança: o *host* bastião deixar de constituir o ponto de contacto para os serviços dos clientes internos para servidores na rede externa (servidor *proxy* serviços da Internet – HTTP, FTP, etc.), passando estes serviços a ser fornecidos pelo *firewall gateway*.

Nesta perspectiva, o Firewall-1 com os seus serviços de segurança (HTTP, FTP, etc.) que fornecem autenticação e segurança de conteúdo, permitiria a obtenção de uma maior segurança do sistema já que deixa de ser necessário um segundo componente (*host* bastião), possivelmente menos seguro, como intermediário entre os utilizadores internos e os serviços da Internet, cabendo somente ao *firewall gateway* essa função. O *host* bastião continuaria a fornecer os serviços da Internet (HTTP e FTP) e no serviço SMTP funciona como intermediário entre o servidor de *e-mail* da rede interna e a Internet.

2.3.2 Os Resultados do IDS e a Simulação de Ataques ao Sistema

Após a auditoria do sistema efectuou-se a prova da sua segurança através da simulação

de ataques do exterior do *firewall gateway* para verificar a eficácia deste, e a partir do segmento de rede protegida considerando uma hipotética falha do *firewall*.

Foi utilizado o Internet Scanner e o seu conjunto de testes (ataques) de negação de serviço e de "força bruta":

- UDP Bomb (ataque de negação de serviço) – pacote UDP construído de forma incorrecta que provoca que alguns sistemas operativos mais antigos tenham um *crash* quando o recebem.
- Windows Out of Band (OOB) Check (ataque de negação de serviço) – verificação que reconhece um ataque out-of-band a uma máquina Windows. Este ataque provoca um *crash* ou perda de conectividade de rede em máquinas vulneráveis.
- Ping Bomb
- Ping of Death (ataque de negação de serviço) – agregando uma grande quantidade de informação a um pacote *ping*, um atacante pode provocar o *overflow* do *buffer* do *kernel* no *host* alvo quando este tenta responder, provocando o *crash* do sistema.
- SYN Storm
- Data Flood
- Log Flood
- Back Orifice Check (tentativa de acesso não autorizado) – ataque "back door" ao Windows 95 e Windows 98, permite a utilizadores remotos obterem controlo total da máquina.
- Kerberos IV User Snarf Check (tentativa de acesso não autorizado) – o Kerberos versão 4 contém uma vulnerabilidade que permite a um atacante remoto obter informação do nome de utilizador e de domínio ao passar um pacote mal constituído ao servidor. Esta informação pode ser utilizada para futuras tentativas para forçar o sistema.
- Portscan Detection Check (teste de pré-ataque) – esta verificação reconhece um *scan* a uma porta que tenha lugar na rede. O intruso pode determinar qual a melhor forma de atacar o sistema, determinando quais os serviços que estão activos no *host*.

Na primeira situação, ataque do exterior do *firewall gateway*, o Internet Scanner não foi bem sucedido, já que não conseguiu passar o *firewall gateway* e reportando um *scanning* sem sucesso. A ferramenta System Status do Firewall-1, reportou um conjunto de alertas relativos às tentativas de penetração do *firewall gateway*.

Na segunda situação, a partir do interior da rede protegida, o Internet Scanner efectuou os ataques referidos a uma máquina Windows NT 4.0 com SP4. O dispositivo RealSecure detectou os seguintes ataques (ver Figura 2.4):

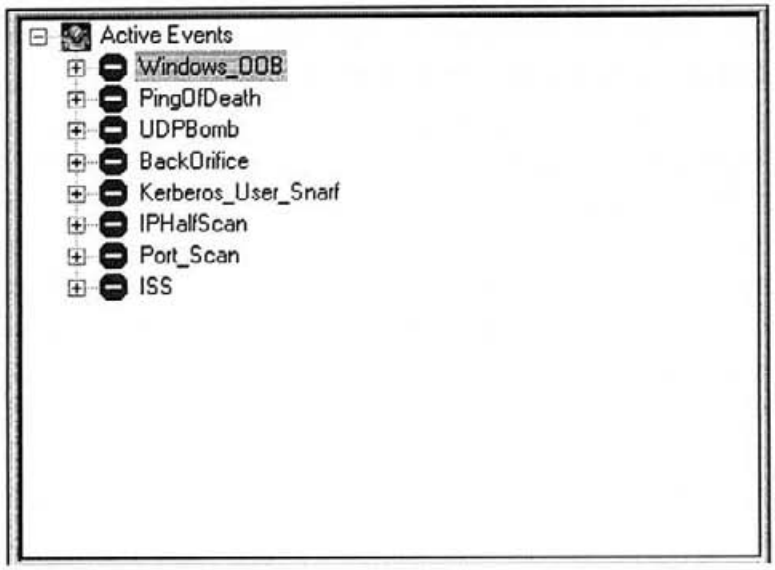


Figura 2.4 – Ataques Detectados pelo RealSecure

2.4 Conclusões

Como tinha sido referido nas conclusões da dissertação, a realização dos testes que são aqui descritos é fundamental para a validação da arquitectura de segurança proposta, e o teste duma implementação de rede simulando o caso em estudo é fundamental.

Conforme foi descrito, a configuração e funcionalidades das ferramentas são bastante satisfatórias, correspondendo às expectativas deixadas pelos testes de laboratório. O comportamento das ferramentas a nível dos mecanismos de segurança é bastante eficaz, como o demonstram a simulação de ataques (ainda que algo restrita). Os resultados da auditoria efectuada demonstram também que a ferramenta de *scanning* é uma *mais valia* para a verificação da ausência de vulnerabilidades do sistema quer a nível do sistema operativo quer a nível das máquinas do *firewall* ou máquinas mais sensíveis.

Pode concluir-se assim que a arquitectura de segurança de rede proposta é uma solução fiável, garantindo os requisitos de segurança para a situação definida. No entanto, pode tirar-se também uma conclusão menos positiva como a ferramenta de auditoria o demonstra, o nível de segurança do sistema auditado está dependente do domínio da maior quantidade de ataques conhecidos e do seu pronto reporte e actualização das ferramentas. E nesta perspectiva, os atacantes estão sempre um passo à frente dos fabricantes das ferramentas de segurança.

Apêndice A. Relatórios de Vulnerabilidades

1. Relatório de Vulnerabilidades do *Firewall Gateway*

Apresentam-se nas próximas páginas (21 páginas) o primeiro relatório de vulnerabilidades de rede obtido pela auditoria ao *firewall gateway*. O relatório está ordenado por grau de risco (alto, médio e baixo) e apresenta a descrição de cada vulnerabilidade bem como a respectiva resolução.

Network Vulnerability Assessment Report

Sorted by Vulnerability Severity and Name

October 13, 1997

Report Description:

This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggested corrective action. Vulnerabilities are classified as high, medium and low. High risk vulnerabilities are those which provide authorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

Session Name:	Session1	**Session ID:**	2
Comment:	Tese	**Template:**	Heavy IPP
File Name:	Session1_971002A	**Termination Status:**	Finished
Scan Summary Information			
Hosts Scanned:	3	**Scan Start:**	1997/10/02 19:38:13
Hosts Active:	3	**Scan End:**	1997/10/02 19:48:55
Hosts InActive:	0	**Elapsed:**	00:10:42

Vulnerability Name:
Getadmin Patch not applied

Severity:
High

Description:
An unpatched version of Windows NT has been found. It is possible for a local user to obtain administrator privileges by running getadmin. See Microsoft Knowledge base article Q146965 for details.

Fix:
Apply the post-SP3 getadmin patch, or SP4 when available. For the patch and the Knowledge Base article, see ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/getadmin-fix/ .

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
LSA Patch not applied.

Severity:
High

Description:
This system has an unpatched version of the Local Security Authority (LSA) subsystem. It is possible for an attacker to display sensitive security information. In addition, account lockout events as a result of exceeding the Bad Logon Attempts limit are not logged at Domain Controllers. Although the latter is not a vulnerability, it does create an inconvenience for administrators wanting to locate the computer where the bad password attempts originated.

Fix:
Apply Windows NT 4.0 Service Pack 3 (SP3). Then apply the post-SP3 lsa2-fix patch, or wait for Windows NT service Pack 4. Microsoft Knowledge Base Article Q182918 "Account Lockout Event also Stored in Security Event Log on DC" at http://support.microsoft.com/support/kb/articles/q182/9/18.asp orftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/nt40/hotfixes-postSP3/lsa2-fix/Q182918.txt. Microsoft Knowledge Base Article Q184017 "Administrators can Display Contents of Service Account Passwords" at http://support.microsoft.com/support/kb/articles/q184/0/17.asp or ftp://ftp.microsoft.com/bussys/winnt/winnt public/fixes/usa/nt40/hotfixes-postSP3/lsa2-fix/Q184017.TXT. Patches: Available at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ hotfixes-postSP3/lsa2-fix/

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
SecHole Lets Non-administrative Users Gain Debug Level Access

Severity:
High

Description:
The host is vulnerable to the Sechole exploit. A utility, Sechole.exe, is being circulated on the Internet that allows a non-administrative use to gain debug-level access on a system process. Using this ut ility, the non-administrative user may run some code in the system security context and thereby acquire local administrative privileges on the system.

Fix:
Windows NT 4.0 users, apply Windows NT 4.0 Service Pack 3 (SP3). Then apply the post-SP3 priv-fix patch, or wait for Windows NT service Pack 4. Microsoft Knowledge Base Article Q190288 "SecHole Lets Non-administrative Users Gain Debug Level Access" at http://support.microsoft.com/support/kb/articles/q190/2/88.asp or ftp://ftp.microsoft.com/bussys/winnt/winnt public/fixes/usa/NT40/hotfixes-postSP3/priv-fix/Q190288.TXT Patches: The priv-fix for Windows NT 4.0 is available at ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/nt40/h otfixes-postSP3/priv-fix/Windows NT 3.51 customers can download from ftp://ftp.microsoft.com/bussys/winnt/winnt public/fixes/usa/NT351/hotfixes-postSP5/priv-fix/.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
SNMP_Set Used Public Community Name to Change System Information

Severity:
High

Description:
The SNMP default Public community name is specified on the host, allowing anyone the ability to change the host's system information i they use this default value. An attacker can use SNMP to obtain valuable information about the machine, such as information on network devices and current open connections. Note: This check may report a false positive if only the system c ontact information is writable.

Fix:
If you need SNMP for network management, ensure that it is properly configured with private community names. Windows: Below are general directions to identify and remove public names. Detailed information is available from the Microsoft Knowledge Base article "How to: Configure SNMP security" at http://support.microsoft.com/support/ntserver/serviceware/10140298.asp. 1 Click the Services tab. 2 Click SNMP Service. 3 Click Properties. 4 Click the Security tab. 5 Verify that your configuration contains the following sec ur settings: - At least one Accepted Community Name exists. Empty lists cause SNMP to accept requests from anyone. (See Microsoft Knowledge Base article Q99880, "How to: Configure SNMP security" at http://support.microsoft.com/support/kb/articles/q99/8/80.asp.) - The Accepted Community Names are not default or easily guessed names, such as public. - The Only Accept SNMP Packets from Thes Hosts option is selected, and one or more IP Host or IPX address are specified. - Each host and community name in the lists is a valid destination. 6 In addition to securing SNMP from the control panel, you will want to secure it from the Registry. See the Windows NT SNMP Community Name topic for more information. Windows: If SNMP is not required, disable the service as follows: 1 Open the Network control panel. 2 Click the Services tab. 3 Click SNMP Service. 4 Click Remove. 5 Click Yes to confirm removal. Unix: To change the community name, refer to your documentation. If SNMP is not required, disable the service as follows: 1 Edit the /etc/inetd.conf (or equivalent) file. 2 Locate the line that controls the daemon. 3 Type a # at the beginning of the line to comment out the daemon. 4 Restart inetd from the command line by typing kill -HUP pid, where pid is the inetd's process ID number.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.0.5	FIREWALLGATEWAY			2
192.168.1.1	FIREWALLGATEWAY			2
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
SSL Patch Not Installed

Severity:
High

Description:
The host has an unpatched version of the Secure Sockets Layer (SSL). This vulnerability allows an attacker to formulate a complex structured attack that could potentially decode an Internet transaction encrypted using SSL. This knowledge would not give the attacker an advantage in decoding any other transactions that had been made by the server, nor would it necessarily give the attacker an advantage in decoding any other transactions performed by the user. A web site operator could detect an attack through observations such as abnormal network activity or high CPU utilization.

Fix:
Apply Windows NT 4.0 Service Pack 3 (SP3). Microsoft Knowledge Base Article Q148427 "Generic SSL (PCT/TLS) Upd ates for IIS and Microsoft Internet Products" at http://support.microsoft.com/support/kb/articles/q148/4/27.asp or ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/NT40/hotfixes-postSP3/ssl-fix/Q148427.TXT. Microsoft Security Bulletin MS98-002 "Updates available for the 'The Error Message Vulnerability' against secured Internet servers" at http://www.microsoft.com/security/bulletins/ms98-002.htm CERT Advisory CA-98.07 "Vulnerability in Some Usages of PKCS#1" at ftp://ftp.cert.org/pub/cert_advisories/CA-98.07.PKCS or http://www.cert.org/ftp/cert_advisories/CA-98.07.PKCS. Patches: The ssl-fix is available at ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/NT40/hotfixes-postSP3/ssl-fix/ Residents of the US and Canada can download the North American (128-bit) version of Schannel.dll from http://mssecure.www.conxion.com/cgi-bin/ntitar.pl

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Windows Key with Incorrect Permissions

Severity:
High

Description:
The HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion key is set to allow any user to modify the subkeys. This allows members of the "Everyone" group to create an entry under the Run and RunOnce keys that contains the name of a program to run when the computer starts.

Fix:
Set the registry permissions to allow read access to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion. Set registry permissions as follows: 1. From the Start Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. 2. Select HKEY_LOCAL_MACHINE. 3. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion. 4. From the 'Security' menu, choose 'Permissions' 5. Allow only read access to the 'Everyone' group.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Windows NT Security Log Accessible

Severity:
High

Description:
This vulnerability enables an intruder to read the Security Log on a Windows NT computer. This indicates that the user has administrative access, and that possibly the Guest account is enabled with network access. If the user running the Scanner legitimately has administrative access to the host, this is not a vulnerability.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. From the Policies menu, select 'User Rights.' Check administrative rights on the machine, and the state of the network access rights for the guest account.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
All Access NetBIOS Share - Everyone

Severity:
Medium

Description:
A NetBIOS share has been found with no access control. This allows anyone full access to any resources provided, and can also allow access to the entire hard drive on unpatched versions of Windows 95.

Fix:
WINDOWS NT: Set the permissions explicitly as follows: LOCAL MACHINE (GUI): Navigate to the NetBIOS share, right-click on the shared directory and select 'Properties.' On the 'Sharing' tab, set the permissions to allow access only to approved users. -OR- Remove th share as follows: LOCAL MACHINE (CLI): Type 'net share sharename /delete.' REMOTE HOST (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/Server Manager. Select the host. From the Computer menu, select 'Shared Directories.' Selec the NetBIOS share and click 'Stop Sharing.' UNIX: Consult your Samba documentation. This condition may require changes to Samba authentication procedures.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY	ISS Reports		2

Vulnerability Name:
Chargen Patch not Applied

Severity:
Medium

Description:
An unpatched version of Windows NT Simple TCP/IP services has been found. It is possible for an attacker to cause a network denial of service by sending broadcast UDP packets to the Windows NT chargen service. See Microsoft Knowledge base article Q154460 for details

Fix:
Apply the post-SP3 simp-tcp patch, or SP4 when available. For the patch and the Knowledge Base article, see ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix/

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Echo Service

Severity:
Medium

Description:
The Echo service was found. The Echo service can be exploited to send packets to the chargen service to create a denial of service attack. The attack can eat increasing amounts of network bandwidth causing loss of performance or even total shutdown of the affected network segments.

Fix:
UNIX: Disable the echo service by commenting out the echo entry in the /etc/inetd.conf file, then restarting the inetd process. WINDOWS The echo service is not native to Windows, but may be present. Disable it as follows: LOCAL MACHINE (GUI): From the Start menu, choose Settings/Control Panel/Services. Select the 'Simple TCP/IP' Services service and click 'Stop.' If you wish to disable only the echo service, open the registry editor, select the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SimpTcp\Parameters key and set EnableTcpEcho and EnableUdpEcho to 0 and restart the Simple TCP/IP service.

IP Address	DNS Name	Associated Info	More Info	Session ID

192.168.0.5	FIREWALLGATEWAY	2
192.168.1.1	FIREWALLGATEWAY	2
193.136.57.4	FIREWALLGATEWAY	2

Vulnerability Name:
Modified teardrop vulnerability

Severity:
Medium

Description:
This issue is a modified version of an attack that appeared on the Internet a few months ago called "teardrop." This new issue is caused by a problem with the way the Microsoft TCP/IP stack handles certain exceptions caused by misformedUDP header information. This situation does not occur in properly formed TCP/IP packets and must be generated by a program with malicious intent.

Fix:
Obtain patch: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/ for Windows NT 4.0 and ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT351/hotfixes-postSP5/teardrop2-fix/ for Windows NT 3.5.1

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
NetBIOS Information Available From SNMP

Severity:
Medium

Description:
By default, Windows NT provides information which is normally available only to administrators via SNMP. If your security policy does not allow publishing information about Windows NT services, users, and shares via a protocol with very minimal security, disable SNMP or this feature.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. Open th HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents key, locate the value which contains SOFTWARE\Microsoft\LANManagerMIB2Agent\CurrentVersion' and remove it.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Out of band DoS

Severity:
Medium

Description:
This machine was found to be vulnerable to the OOB denial-of-service attack on port 139.

Fix:
Apply the teardrop2 patch at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/ (which supersedes the oob patch) after applying Service Pack 3. For more information about teardrop2, see Microsoft Knowledge Base article Q179129 at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/Q179129.txt

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Regedit Is Associated With .reg Files

Severity:
Medium

Description:
Regedit.exe was found associated with registry files.

Fix:
Remove notepad association in the NT registry. Remove the association as follows: 1. From the Start menu, choose 'Run' 2. Type 'regedt32' and click 'OK'. This opens the Registry Editor. 3. Navigate to HKEY_LOCAL_MACHINE/Software/Classes/regfile/shell/open/command. 4. Edit your key value name to remove the notepad association.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Regfile Associations Can Be Changed By Non-Admins

Severity:
Medium

Description:
Improper permissions were found on the registry key valuename specifying a command association with registry files.

Fix:
Restrict non-Administrators write access for the command key in the NT registry. Restrict write access as follows: 1. From the Start menu, choose 'Run' 2. Type 'regedt32' and click 'OK'. This opens the Registry Editor. 3. Navigate to HKEY_LOCAL_MACHINE/Software/Classes/regfile/shell/open/command. 4. From the Security menu, choose 'Permissions' 5. Restrict non-Administrators write access.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Repair Directory Readable

Severity:
Medium

Description:
The %systemroot\repair directory is by default readable by everyone. It is possible to extract usernames and potentially the hashes of the passwords from the sam._ file. Set the permissions on this directory to full control for administrators and system and remove permissions for everyone.

Fix:
Restrict access to the %systemroot\repair directory to administrators only. LOCAL MACHINE (GUI): From Windows Explorer, right-click on the selected directory and select 'Properties.' Change access under 'Security.' LOCAL MACHINE (CLI): Type 'cacls c:\winnt\repair /g administrators:F.'

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
RRAS Patch Not Installed

Severity:
Medium

Description:
The host has an unpatched version of the Routing and Remote Access Service (RRAS). This patch includes an enhancement to TCP/IP that will improve the performance of TCP-based applications over high latency networks, demand dial filtering to better control dialing interfaces, fragmented IP packet filtering to drop malformed or unauthorized packets, and other security fixes.

Fix:
Note: This patch requires that you already have Routing and Remote Access Service for Windows NT 4.0 Server installed on your system. You must first apply the Windows NT 4.0 PPTP Upgrade before applying RRAS Upgrade 3.0 (it is important not to reboot your machine in-between installations of the Windows NT PPTP upgrade & the RRAS upgrade). For more information, please see Microsoft Knowledge Base article Q189595 "PPTP Performance & Security Upgrade for WinNT 4.0 Release Notes" Apply Windows NT 4.0 Service Pack 3 (SP3). Then apply the post-SP3 rras30-fix patch, or wait for Windows NT service Pack 4. Microsoft Knowledge Base Article Q168469 "RRAS Upgrade for WinNT Server 4.0 Hotfix Pack 3.0 Release Notes" at http://support.microsoft.com/support/kb/articles/q189/5/94.asp or ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/NT40/hotfixes-postSP3/rras20-fix/Q189594.TXT

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Scheduler Key Has Incorrect Permissions

Severity:
Medium

Description:
The HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Schedule key controls the schedule service. Server Operators have permission to write to this registry tree, which would allow them to manually schedule jobs to be run by the schedule service, which normally executes under the system user context. This can be used to raise the Server Operator's access level to Administrator.

Fix:
Remove Server operator write access to the schedule key in the NT registry. Remove write accessas follows: 1. From the Start menu, choose 'Run' 2. Type 'regedt32' and click 'OK'. This opens the Registry Editor. 3. Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Schedule. 4. From the Security menu, choose 'Permissions'. 5. Remove Server Operator write access.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Shares Enumerated Through A Null Session

Severity:
Medium

Description:
Users or shares were detected on this host using a null session. A null session is a NetBIOS connection established with a zero length string as user, password, and domain name, which is designed to enable enumeration of shares and users. This capability has always been present in Windows NT, but was recently discovered to allow access to the registry with the same level of permissions as the Everyone group. It is a low risk vulnerability (similar to finger) that allows users and shares to be enumerated.

Fix:

To remove the vulnerability, Windows NT users must restrict anonymous connections. Windows NT users should remove all unnecessary shares and apply the sec-fix patch described later in this section. Windows 95 users must remove all shares to avoid flagging this vulnerability. If shares are needed and must be secure, consider upgrading to Windows NT running NTFS. Windows 95: Remove all share or upgrade to Windows NT. Windows 95 provides no way to resolve this vulnerability, and the vulnerability will be flagged if any shares are detected, even if they are not accessible. Windows 95 and Windows NT: To remove a share from the command line, type net share sharename /delete. Windows NT: If your Windows NT version is at Service Pack 2, apply the sec-fix patch available at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ hotfixes-postSP2/sec-fix/ --OR- Apply Windows NT 4.0 Service Pack 3 --AND- To restrict anonymous connections, perform the following steps after you apply the patch or Windows NT 4.0 Service Pack 3. WARNING: Incorrectly using Registry Editor may cause severe and irreparable damage and may require you to reinstall your operating system. Internet Security Systems cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. 1 If you have not already done so, apply Windows NT 4.0 Service Pack 3 or the sec-fix patch. 2 Start the Registry Editor. 3 Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA. 4 From the Edit menu choose Add Value. The Add Value window appears. 5 In the Value Name field, type RestrictAnonymous. 6 Select REG_DWORD as the Data Type. 7 Click OK. The DWORD Editor appears. 8 In the Data field, type 1. (The Radix setting does not matter in this case.) 9 Click OK. Registry Editor adds the key to the registry. 10 Reboot the system to apply the changes. Note: Changing the Registry entries is only effective after the patch or Service Pack 3 have been applied.

IP Address	DNS Name	Associated Info	More Info	Session I
192.168.0.5	FIREWALLGATEWAY			2
192.168.1.1	FIREWALLGATEWAY			2
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Ssping Patch not Applied

Severity:
Medium

Description:
An unpatched version of Windows NT has been found. It is possible for an attacker to cause the host to crash by sending improperly forme ICMP packets. See Microsoft Knowledge base article Q154174 for details.

Fix:
Apply the teardrop2 patch at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/ (which supersedes the icmp patch) after applying Service Pack 3. For more information about teardrop2, see Microsoft Knowledge Base article Q179129 at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/Q179129.txt

IP Address	DNS Name	Associated Info	More Info	Session I
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Users enumerated through a null session

Severity:
Medium

Description:
Users were enumerated through a null session. Account names may be acquired, providing the foundation for a Brute Force attack.

Fix:
After applying the patch and Service Pack 3, then: From the Start menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA. On the Edit menu, click 'Add Valu and use the following entries: Value Name: RestrictAnonymous Data Type: REG_DWORD Value: 1. Reboot the system to apply the changes. Also, upgrade to Service Pack 3. NOTE: The winreg key will not be present if Service Pack 3 is not installed. Resetting the Registry entries is only effective after the patch and Service Pack 3 have been applied. For more information see Microsoft Knowledge Base article Q155363. To apply Service Pack 3, access ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/, choose the desired country abbreviation, then select nt40/, then choose ussp3/. Depending on whether you have an Intel or ALPHA CPU, choose i386/nt4sp3_1.exe or choose alpha/nt4sp3_a.exe respectively.

IP Address	DNS Name	Associated Info	More Info	Session I

192.168.0.5	FIREWALLGATEWAY	2
192.168.1.1	FIREWALLGATEWAY	2
193.136.57.4	FIREWALLGATEWAY	2

Vulnerability Name:
Windows NT denial of service attack

Severity:
Medium

Description:
Windows NT servers (including those with Service Pack 3 when all hotfixes applied) are vulnerable to a denial of service attack. When a logon request is initiated to access the SMB/CIFS service and the SMB logon packet is incorrectly processed, memory corruption results in the NT kernel. When this happens, a blue screen error message appears and the machine has to be rebooted.

Fix:
Apply patch from microsoft: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/srv-fix

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Winlogon Key Has Incorrect Permissions

Severity:
Medium

Description:
The HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon key has two values which can be used to cause a process to execute upon either system bootup, or when a user logs on. The programs pointed to by the System value run under the system user context after boot, and could be used to change a user's rights or access level. The UserInit value runs applications when a user logs in. The default settings for this key allow Server Operators to write these values, either of which could be used to raise a System Operator's access level to Administrator.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. Throug the Security menu, remove write access to the Winlogon key for Server Operators.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
WINS Patch not Applied

Severity:
Medium

Description:
An unpatched version of Windows NT WINS has been found. It is possible for an attacker to cause WINS to fail by sending invalid UDP packets. See Microsoft Knowledge base article Q155701 for details.

Fix:
Apply the post-SP3 wins-udp patch, or SP4 when available.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
WINS Update Patch Not Installed Header

Severity:
Medium

Description:
The host has an unpatched version of the Windows Internet Naming Service (WINS). Invalid UDP frames directed to any computer runnin WINS raises an exception in WINS causing it to terminate silently. When WINS is no longer running, problems related to domain synchronization, browsing, or connectivity may occur.

Fix:
Apply Windows NT 4.0 Service Pack 3 (SP3). Then apply the post-SP3 winsupd-fix patch, or wait for Windows NT service Pack 4. Microsoft Knowledge Base Article Q155701 "Invalid UDP Frames May Cause WINS to Terminate" at http://support.microsoft.com/support/kb/articles/q155/7/01.asp or ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/NT40/hotfixes-postSP3/winsupd-fix/Q155701.TXT

IP Address	DNS Name	Associated Info	More Info	Session I
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Account Management Auditing not Enabled

Severity:
Low

Description:
Account Management Auditing is not enabled. Account Management auditing records when new users and groups are created or changed. Since these events are highly sensitive, it is recommended that these events always be audited.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. Select Policies, Aud and enable User and Group Management auditing as required by your security policy.

IP Address	DNS Name	Associated Info	More Info	Session I
193.136.57.4	FIREWALLGATEWAY	Failure		2
193.136.57.4	FIREWALLGATEWAY	Success		2

Vulnerability Name:
Alerter and messenger services

Severity:
Low

Description:
The Windows NT Alerter service enables a user to send pop-up messages to other users, which could be used for social engineering attacks A side effect of running this service is that it causes the name of the current user to be broadcast in the NetBIOS name table, which gives th attacker a valid user name to use in brute force attempts.

Fix:
Disable the Alerter service. Disable the Alerter service as follows: 1. From the Start menu, select 'Settings', 'Control Panel', 'Services'. 2. Select the Alerter service and click the 'Stop' button. 3. Also click 'Disable' to stop the service from restarting at the next reboot.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
DCOM is Enabled.

Severity:
Low

Description:
DCOM was found to be enabled. DCOM may be used to execute programs remotely.

Fix:
Disable DCOM in the NT registry. Disable DCOM as follows: 1. From the Start menu, choose 'Run' 2. Type 'regedt32' an click 'OK'. This opens the Registry Editor. 3. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Ole. 4. Open EnableDCOM key and change the value to N. 5. Click 'OK'.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
DCOM RunAs Value Writeable

Severity:
Low

Description:
The DCOM RunAs Value was found to be writeable. DCOM calls are executed under the security context of the calling user by default. If the RunAs key has been altered, the DCOM calls can be executed under the user context of the currently logged in user, or as a third user. I this ability is not controlled very carefully, it could provide a network user with the ability to execute arbitrary code under another user context. The RunAs key is writeable by the Interactive (console) user by default, which implies that if the console user were tricked into executing a trojan which altered the registry, or if someone other than the normal user were to log on locally, then DCOM calls could be executed under the console user's context by a remote user. If the console user was of a higher access level than the network user, a security breach could result.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. Locate HKEY_LOCAL_MACHINE\Software\Classes\AppID key, and remove write permissions for the Interactive user, and propagate these permissions down that portion of the registry tree.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Default NT Administrator Userid Exists

Severity:
Low

Description:
An account named Administrator was found. This default account cannot be locked out by too many incorrect login attempts, and can be vulnerable to a Brute Force attack if a poor password is chosen.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. Within User Manager, the following options can be used to correct this vulnerability: 1. Select the Administrator account. From the User menu, select 'Rename' and change the name of the Administrator account. 2. From the User menu, select 'New.' Add a new user named Administrator, with an unguessable password, who is a member only of the Guest group. 3. From the Policies menu, select 'Account.' Enable auditing of failed login attempts, and monitor any attempts to log in as Administrator very carefully. Also, under 'Policies/User Rights,' you can remo from the Administrator account the right to log in from the network. This would force any brute force attempt to come from the console, and only users who can be locked out (if enabled) can access the computer from the network.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.0.5	FIREWALLGATEWAY			2

192.168.1.1	FIREWALLGATEWAY	2
193.136.57.4	FIREWALLGATEWAY	2

Vulnerability Name:
Forced Logoff Not Enabled

Severity:
Low

Description:
Forced logoffs are not enabled. If this is not enabled, users will not be forced to log out once their allowed login hours expire.

Fix:
Enable forced logoffs. LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager Select the account. From the Policies menu, click Account. Click the "Forcibly Disconnect Remote Users From the Server When Logon Hours Expire" check box. This option is visible only when the server is Primary Domain Controller.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.0.5	FIREWALLGATEWAY			2
192.168.1.1	FIREWALLGATEWAY			2
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Internet Explorer is outdated

Severity:
Low

Description:
Internet Scanner has detected an outdated version of Internet Explorer. All versions of Internet Explorer prior to 4.01 are known to have security issues. Note: This check requires specific privileges in order to function successfully. At a minimum, the account performing the scan must be able to connect to and read the target host's "HKEY_LOCAL_MACHINE" registry key. It is suggested that the scan be performed from an account with domain administrator privileges or local administrator privileges on the target host.

Fix:
Obtain the latest released version and patches for Internet Explorer at http://www.microsoft.com/ie.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
IP Forwarding Enabled

Severity:
Low

Description:
The host has IP forwarding enabled. If this machine is outside of the firewall, this could allow access to internal networks.

Fix:
If IP forwarding is not allowed by your security policy, follow these steps: LOCAL MACHINE (GUI): From the Start menu, choose Settings/Control Panel/Network/Protocols, and select TCP/IP, Properties. Select the Routing tab, and disable IP forwarding. If you wish to disable this function remotely, open the registry on the remote host and locate the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters key and set the IPEnableRouter value to zero. You will then need to reboot the system to allow this change to take effect.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Lan Manager Security

Severity:
Low

Description:
LAN Manager-style hashes are enabled for network authentication. LM hashes are relatively easily broken through a brute force attack, and the stronger Windows NT style hashes should be used. For more information see the online help topic entitled LAN Manager Security.

Fix:
Windows NT can be patched to change the Registry so that it accepts only NT-to-NT authentication. For more information on disabling LM Security authentication, see Microsoft Knowledge Base article Q147706.txt at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/lm-fix/Q147706.txt NOTE: Service Pack 3 must be applied first for the Registry patch to work correctly. For the patch, see ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/lm-fix. To apply Service Pack 3, access ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/, choose the desired country abbreviation, then select nt40/, then choose ussp3/. Depending on whether you have an Intel or ALPHA CPU, choose i386/nt4sp3_1.exe or choose alpha/nt4sp3_a.exe respectively.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Land denial of service attack

Severity:
Low

Description:
Internet Scanner discovered an outdated version of tcpip.sys. This vulnerability allows an attacker to cause a high CPU load by sending a spoofed packet to a port which claims to have originated from that port. Variations on this attack can cause Windows NT machines to lock up. For more information see Microsoft Knowledge Base article Q165005.txt at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/land-fix/Q165005.txt.

Fix:
Apply Windows NT 4.0 Service Pack 3, and apply the teardrop2 patch at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/ (which supersedes the land patch) after applying Service Pack 3. For more information about teardrop2, see Microsoft Knowledge Base article Q179129 at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/Q179129.txt Note: Applying router of firewall rules which deny all incoming packets which claim to originate from the internal network is good practice, and will stop this attack.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Logon Auditing not Enabled

Severity:
Low

Description:
Logon Auditing is not enabled. It is important to audit logon and logoff success and failure to be able to detect and track unauthorized access attempts.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. Select Policies, Audit and enable Logon and Logoff auditing as required by your security policy.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY	Success		2

Vulnerability Name:
Missing PowerPoint Security Patch

Severity:
Low

Description:
This check detected the absence of the PowerPoint security patch. If missing, Internet Explorer will execute an application from within PowerPoint without warning the user.

Fix:
Apply the security patch, which is available from: http://www.microsoft.com/msdownload/iesecurity/iepptsecurity.htm PPT security patch

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Multihomed Host

Severity:
Low

Description:
The Scanner has detected that the host has more than one network card installed. Under ordinary circumstances, this is not considered a serious risk. If the host is placed outside the firewall, it could provide an entry point for an intruder. Note - this vulnerability was determined by reading the Windows NT registry.

Fix:
If multihomed hosts are outside of your security policy, remove the additional network adapter. Consult your firewall documentation for more information.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
NetBIOS share found

Severity:
Low

Description:
This vulnerability indicates that a NetBIOS share has been found. If the share has the proper access controls, this is a very low risk vulnerability.

Fix:
LOCAL MACHINE: Set the permissions explicitly as follows: 1. Navigate to the share in Windows Explorer. 2. Right-click on the share, select 'Properties'. 3. Under the 'Sharing' tab, review the permissions. 4. Allow access only to approved users. 5. Click 'OK'. -OR- Open the command line, remove the share as follows: 1. From the Start menu, select Run. 2. Type 'cmd', then click 'OK'. This opens the command line. 3. Type 'net share sharename /delete.' where sharename is the name of the share. 4. Type 'exit' to return to the Windows NT desktop. REMOTE HOST (GUI): Remove the share as follows: 1. From the 'Start' menu, select 'Programs/Administrative Tools (Common)/Server Manager'. 2. Select the host. From the 'Computer' menu select 'Shared Directories.' 3. Select the share and click 'Stop Sharing.'

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY	ADMIN$		2
193.136.57.4	FIREWALLGATEWAY	C$		2
193.136.57.4	FIREWALLGATEWAY	D$		2
193.136.57.4	FIREWALLGATEWAY	IPC$		2

193.136.57.4	FIREWALLGATEWAY	ISS Reports	2

Vulnerability Name:
Object Auditing not Enabled

Severity:
Low

Description:
Object Auditing is not enabled. Object access includes files and registry keys. Auditing of these events must be enabled both by the security descriptor on the object and in the auditing settings.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. Select Policies, Audit and enable File and Object Access auditing as required by your security policy.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY	Success		2

Vulnerability Name:
OS/2 Subsystem Enabled

Severity:
Low

Description:
Windows NT was C2 evaluated with the OS/2 subsystem disabled. Enabling the OS/2 subsystem can allow a process to persist across logins.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. Open th System\CurrentControlSet\Control\Session Manager\SubSystems key, remove the Os2 value, and the file which is pointed to be the value data.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Page File not Cleared at Shutdown

Severity:
Low

Description:
The Windows NT pagefile can contain sensitive information, and should be cleared upon shutdown if required by your security policy. Some versions of the Netware authentication module will store the user name and password in clear-text, and this can be extracted from the pagefile.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. Open th HKLM\System\CurrentControlSet\Control\Session Manager\Memory Manager key, locate the ClearPageFileAtShutdown value, and set it t 1.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name: **Severity:**
Performance Monitor Readable **Low**

Description:
The permissions on the Software\Microsoft\Windows NT\CurrentVersion\Perflib key are incorrect. This allows non-administrators to read performance counters, and monitor which processes are running. Under NT 4.0, registry access from the network can be denied completely.

Fix:
Restrict registry access and/or reset permissions. Restrict registry access as follows: 1. From the Start Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. 2. Select HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Perflib. 3. From the Security menu, choose 'Permissions'. 4. Restrict access to all or set permissions to allow access to approved Administrators only.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name: **Severity:**
Policy Auditing not Enabled **Low**

Description:
Policy Auditing is not enabled. Policy auditing records when security policy changes are made. Since these events are highly sensitive, it is recommended that these events always be audited.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. Select Policies, Audit and enable Security Policy Changes auditing as required by your security policy.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY	Success		2

Vulnerability Name: **Severity:**
Posix Enabled **Low**

Description:
Windows NT was C2 evaluated with the POSIX subsystem disabled. Enabling the POSIX subsystem can also subject a host to trojan horse attacks, since it is possible to create a file with a lower case name which will be found in a search prior to a file with an upper case name.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. Open the System\CurrentControlSet\Control\Session Manager\SubSystems key, remove the POSIX value, and the file which is pointed to be the value data.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Privilege Auditing not Enabled

Severity:
Low

Description:
Privilege Auditing is not enabled. Privilege auditing records when any user rights (such as the right to backup and restore files) are granted to a user or process.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. Select Policies, Audit and enable Use of User Rights auditing as required by your security policy.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY	Failure		2
193.136.57.4	FIREWALLGATEWAY	Success		2

Vulnerability Name:
Process Auditing not Enabled

Severity:
Low

Description:
Process Auditing is not enabled. Process auditing records when processes are started and stopped. Auditing these events typically produces a large number of event logs, and is not normally enabled.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. Select Policies, Audit and enable Process Tracking auditing as required by your security policy.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY	Failure		2
193.136.57.4	FIREWALLGATEWAY	Success		2

Vulnerability Name:
Readable NT Application Log

Severity:
Low

Description:
This vulnerability enables an intruder to read the Application Log on a Windows NT computer. This may indicate that the Guest account is enabled, possibly with network access rights. If the user running the scan is an authorized user, this may not indicate a vulnerability.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. From the Policies menu, select 'User Rights' and examine which users are allowed to log on from the network. Also, check whether the Guest account is enabled.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name: SNMP
Severity: Low

Description:
An intruder can use SNMP (Simple Network Management Protocol) to gain valuable information about the machine (such as information or network devices, current open connections, etc.) when SNMP uses default words, such as public or private, for the community word. If no community is specified, then the SNMP server responds to queries from any host. See RFC 1157 "A Simple Network Management Protocol" at ftp://ftp.isi.edu/in-notes/rfc1157.txt for additional information.

Fix:
If you need SNMP for network management, ensure that it is properly configured with private community names. If SNMP is not required, disable the service as follows: WINDOWS: LOCAL MACHINE (GUI): From the Start menu, choose Settings/Control Panel/Network/Services. Select the SNMP service and click 'Stop.' UNIX: Disable snmp by putting # at the beginning of the snmp line in the inetd.conf file (usually located in /etc) and restart inetd.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.0.5	FIREWALLGATEWAY			2
192.168.1.1	FIREWALLGATEWAY			2
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name: SNMP Community Name Is World Readable By Default
Severity: Low

Description:
Windows NT exports information such as valid user names, shares, and the status of running services via SNMP. An attacker can use this information to exploit the computer in a number of ways. The only validation required to read this information is contained in the community name.

Fix:
Edit the Registry to permit only approved users access to the SNMP Community Name. Edit the registry as follows: 1. From the Start menu, select 'Run.' 2. Type 'regedt32.exe' and click 'OK.' This opens the Registry Editor. 3. Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\S NMP\Parameters\ValidCommunities 4. From the Security menu, choose 'Permissions'. 5. Set the permissions to permit only approved users access.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name: SNMP_Get Able to Retrieve Public Community Name
Severity: Low

Description:
The SNMP default Public community name is specified on the host, allowing anyone the ability to receive responses to queries from the host if they use this default value. An attacker can use SNMP to obtain valuable information about the machine, such as information on network devices and current open connections.

Fix:

If you need SNMP for network management, ensure that it is properly configured with private community names. Windows: Below are general directions to identify and remove public names. Detailed information is available from the Microsoft Knowledge Base article "How to: Configure SNMP security" at http://support.microsoft.com/support/ntserver/serviceware/10140298.asp. 1 Click the Services tab. 2 Click SNMP Service. 3 Click Properties. 4 Click the Security tab. 5 Verify that your configuration contains the following sec ure settings: - At least one Accepted Community Name exists. Empty lists cause SNMP to accept requests from anyone. (See Microsoft Knowledge Base article Q99880, "How to: Con figure SNMP security" at http://support.microsoft.com/support/kb/articles/q99/8/80.asp.) - The Accepted Community Names are not default or easily guessed names, such as public. - The Only Accept SNMP Packets from These Hosts option is s elected, and one or more IP Host or IPX address are specified. - Each host and community name in the lists is a valid destination. 6 In addition to securing SNMP from the control panel, you will want to secure it from the Registry. See the Windows NT SNMP Community Name topic for more information. Windows: If SNMP is not required, disable the service as follows: 1 Open the Network control panel. 2 Click the Services tab. 3 Click SNMP Service. 4 Click Remove. 5 Click Yes to confirm removal. Unix: To change the community name, refer to your documentation. If SNMP is not required, disable the service as follows: 1 Edit the /etc/inetd.conf (or equivalent) file. 2 Locate the line that controls the daemon. 3 Type a # at the beginning of the line to comment out the daemon. 4 Restart inetd from the command line by typing kill -HUP pid, where pid is the inetd's process ID number.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.0.5	FIREWALLGATEWAY		Hardware: x86 Family 6 Model 5 Stepping 1 AT/AT COMPATIBLE - Software: Windows NT Version 4.0 (Build 1381 Uniprocessor Free)	2
192.168.1.1	FIREWALLGATEWAY		Hardware: x86 Family 6 Model 5 Stepping 1 AT/AT COMPATIBLE - Software: Windows NT Version 4.0 (Build 1381 Uniprocessor Free)	2
193.136.57.4	FIREWALLGATEWAY		Hardware: x86 Family 6 Model 5 Stepping 1 AT/AT COMPATIBLE - Software: Windows NT Version 4.0 (Build 1381 Uniprocessor Free)	2

Vulnerability Name:
System Auditing not Enabled

Severity:
Low

Description:
System Event Auditing is not enabled. System events include startup and shutdown.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. Select Policies, Audit and enable Restart, Shutdown and System auditing as required by your security policy.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY	Success		2

Vulnerability Name:
Traceroute

Severity:
Low

Description:
Traceroute prints the route packets take to get to networked host.

Fix:
Prevent or limit external tracerouting into internal networks via packet filtering. UNIX: The UNIX version of the Scanner uses UDP packets to conduct a traceroute. Disallow incoming UDP packets with high-numbered destination ports. For more information, consult your firewall documentation. ICMP packets are not found by UNIX. WINDOWS NT: The NT version of the Scanner uses ICMP to conduct a traceroute. Disallow incoming ICMP packets with high-numbered destination ports. For more information, consult your firewall documentation. UDP packets are not found by NT. NOTE: Because the UNIX and NT versions of the Scanner use different methods for traceroute, this vulnerability may occasionally be found by one version of the Scanner and not the other.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.0.5	FIREWALLGATEWAY		Route: 192.168.1.1 -> 192.168.0.5	2
192.168.1.1	FIREWALLGATEWAY		Route: 192.168.1.1 -> 192.168.1.1	2
193.136.57.4	FIREWALLGATEWAY		Route: 192.168.1.1 -> 193.136.57.4	2

Vulnerability Name:
Unknown NT Service

Severity:
Low

Description:
A service was found which was not known to ship with Windows NT. Services can be used to install back doors, or provide unauthorized network access. Any service which is not approved by your security policy should be removed.

Fix:
Use instsrv from the Windows NT Resource Kit to remove the unwanted service. Remove the service as follows: 1. From the 'Start' menu, choose 'Run'. 2. Type 'cmd' and click 'OK'. This opens the command line. 3. At a command prompt type 'instsrv [service name] remove' and press <ENTER>. 4. Type 'exit' and press <ENTER> to return to Windows.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY	FW1SVC		2

Vulnerability Name:
Windows NT Messenger service running

Severity:
Low

Description:
The Windows NT Messenger service enables a user to send pop-up messages to other users, which could be used for social engineering attacks. A side effect of running this service is that it causes the name of the current user to be broadcast in the NetBIOS name table, which gives the attacker a valid user name to use in Brute Force attempts.

Fix:
Disable the Messenger Service. Disable the Messenger Service as follows: 1. From the Start menu, select 'Settings', 'Control Panel'. 2. Open the 'Services' icon. 3. Select the 'Messenger' service and click 'Stop.'

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Windows NT Registry opened remotely

Severity:
Low

Description:
This indicates that the Scanner is able to open the registry remotely. This may indicate that permissions are not set properly, or that possibly the guest account is enabled with network access rights. An attacker could alter file associations, permitting the introduction of a trojan horse, or otherwise seriously compromise the machine. If the host running the scan is a trusted host, this may not indicate a vulnerability.Under NT 4.0, registry access from the network can be denied completely.

Fix:
Restrict registry access and/or reset permissions. Restrict registry access as follows: 1. From the Start Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. 2. Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg. 3. From the Security menu, choose 'Permissions'. 4. Restrict access to all or set permissions to allow access to approved Administrators only.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Windows NT System Log Accessible

Severity:
Low

Description:
Windows NT System Log was found to be accessible. This vulnerability enables an intruder to read the System Log on a Windows NT computer. This may indicate that the guest account is enabled, possibly with network access rights. If the user running the scan is a authorized user, this may not indicate a vulnerability.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. From the Policies menu, select User Rights. Check administrative rights on the machine, and the state of the network access right for the guest account.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

Vulnerability Name:
Year 2000 Patch Not Installed

Severity:
Low

Description:
The Year 2000 (y2k-fix) patch is not installed on the host. This patch resolves date issues with the Find Files or Folders feature, leap year usage in the User Manager program, incorrect saved dat es in the document properties viewer, and day skipping in the Date/Time control panel.

Fix:
Apply Windows NT 4.0 Service Pack 3 (SP3). Then apply the post-SP3 y2k-fix patch, or wait for Windows NT service Pack 4. Microsoft Knowledge Base Article Q175093 "User Manager Does Not Recognize February 2000 As a Leap Year" at http://support.microsoft.com/support/kb/articles/q175/0/93.asp or ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/y2k-fix/Q175093.TXT Microsoft Knowledge Base Article Q180122 "After Changing the Time, Windows NT May Skip a Day" at http://support.microsoft.com/support/kb/articles/q180/1/22.asp or ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/NT40/hotfixes-postSP3/y2k-fix/Q180122.TXT Microsoft Knowledge Base Article Q183123 "Find Files Displays Garbled Date if Year i s 2000 or Greater" at http://support.microsoft.com/support/kb/articles/q183/1/23.asp or ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/NT40/hotfixes-postSP3/y2k-fix/Q183123.TXT Microsoft Knowledge Base Article Q183125 "Shell Doc Property Dialog Custom Date Incorrect After Year 2000" at http://support.microsoft.com/support/kb/articles/q183/1/25.asp or ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/NT40/hotfixes-postSP3/y2k-fix/Q183125.TXT

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.4	FIREWALLGATEWAY			2

2. Relatório de Vulnerabilidades do *Router*

Apresentam-se nas próximas páginas (3 páginas) o primeiro relatório de vulnerabilidades de rede obtido pela auditoria ao *router*. O relatório está ordenado por grau de risco (alto, médio e baixo) e apresenta a descrição de cada vulnerabilidade bem como a respectiva resolução.

Network Vulnerability Assessment Report

Sorted by Vulnerability Severity and Name

October 13, 1997

Report Description:

This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggested corrective action. Vulnerabilities are classified as high, medium and low. High risk vulnerabilities are those which provide authorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

Session Name:	Session1	**Session ID:**	12
Comment:	Tese	**Template:**	Heavy IPP
File Name:	Session1_971009	**Termination Status:**	Finished
Scan Summary Information			
Hosts Scanned:	6	**Scan Start:**	1997/10/09 13:24:59
Hosts Active:	6	**Scan End:**	1997/10/09 13:42:27
Hosts InActive:	0	**Elapsed:**	00:17:28

Vulnerability Name: Routed Service Active

Severity: Medium

Description:
The routed service was detected. This provides an intruder your routing information. It opens up the possibility that an intruder can send false RIP packets, causing your data to be routed to the intruder's machine.

Fix:
If you are using a simple gateway, use a default route. Most sites are connected through a single point of entry to the Internet with a simple infrastructure. These sites do not need to run routed. Disable routed from running on the machine: Comment out routed from the /etc/inetd.conf file by putting a '#' at the beginning of the line and sending a HUP signal to the inetd (# kill -HUP <inetd.pid>).

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.1			10.0.0.0 metric (hop count): 1	12

Vulnerability Name: Finger Service

Severity: Low

Description:
The Finger service was found running. Finger gives an intruder information such as login accounts and trusted hosts.

Fix:
Disable finger, or install a finger daemon that limits the type of information provided. UNIX: Disable the finger daemon by commenting it out of /etc/inetd.conf and restarting inetd. Use GNU Finger to configure the type of information gatherable from finger. For more information on GNU finger, see: ftp://prep.ai.mit.edu/pub/gnu/finger-1.37.tar.gz GNU Finger. WINDOWS: The Finger service is not native to Windows, but may be present. Disable it as follows: LOCAL MACHINE (GUI): From the Start menu, choose Settings/Control Panel/Services. Select the service and click 'Stop.'

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.1				12

Vulnerability Name: SNMP

Severity: Low

Description:
An intruder can use SNMP (Simple Network Management Protocol) to gain valuable information about the machine (such as information o network devices, current open connections, etc.) when SNMP uses default words, such as public or private, for the community word. If no community is specified, then the SNMP server responds to queries from any host. See RFC 1157 "A Simple Network Management Protocol" at ftp://ftp.isi.edu/in-notes/rfc1157.txt for additional information.

Fix:
If you need SNMP for network management, ensure that it is properly configured with private community names. If SNMP is not required, disable the service as follows: WINDOWS: LOCAL MACHINE (GUI): From the Start menu, choose Settings/Control Panel/Network/Services. Select the SNMP service and click 'Stop.' UNIX: Disable snmp by putting # at the beginning of the snmp line in the inetd.conf file (usually located in /etc) and restart inetd.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.1				12

Vulnerability Name:
SNMP_Get Able to Retrieve Public Community Name

Severity:
Low

Description:
The SNMP default Public community name is specified on the host, allowing anyone the ability to receive responses to queries from the host if they use this default value. An attacker can use SNMP to obtain valuable information about the machine, such as information on network devices and current open connections.

Fix:
If you need SNMP for network management, ensure that it is properly configured with private community names. Windows: Below are general directions to identify and remove public names. Detailed information is available from the Microsoft Knowledge Base article "How to: Configure SNMP security" at http://support.microsoft.com/support/ntserver/serviceware/10140298.asp. 1 Click the Services tab. 2 Click SNMP Service. 3 Click Properties. 4 Click the Security tab. 5 Verify that your configuration contains the following sec ure settings: - At least one Accepted Community Name exists. Empty lists cause SNMP to accept requests from anyone. (See Microsoft Knowledge Base article Q99880, "How to: Con figure SNMP security" at http://support.microsoft.com/support/kb/articles/q99/8/80.asp.) - The Accepted Community Names are not default or easily guessed names, such as public. - The Only Accept SNMP Packets from These Hosts option is s elected, and one or more IP Host or IPX address are specified. - Each host and community name in the lists is a valid destination. 6 In addition to securing SNMP from the control panel, you will want to secure it from the Registry. See the Windows NT SNMP Community Name topic for more information. Windows: If SNMP is not required, disable the service as follows: 1 Open the Network control panel. 2 Click the Services tab. 3 Click SNMP Service. 4 Click Remove. 5 Click Yes to confirm removal. Unix: To change the community name, refer to your documentation. If SNMP is not required, disable the service as follows: 1 Edit the /etc/inetd.conf (or equivalent) file. 2 Locate the line that controls the daemon. 3 Type a # at the beginning of the line to comment out the daemon. 4 Restart inetd from the command line by typing kill -HUP pid, where pid is the inetd's process ID number.

P Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.1			Cisco Internetwork Operating System Software ..IOS (tm) 2500 Software (C2500-I-L), Version 11.2(9)P, RELEASE SOFTWARE (fc1)..Copyright (c) 1986-1997 by cisco Systems, Inc...Compiled Tue 30-Sep-97 17:08 by ccai	12

Vulnerability Name:
Stock Fingerd Running

Severity:
Low

Description:
The Finger service was found running. Finger gives an intruder information such as login accounts and trusted hosts.

Fix:
UNIX: Disable the finger daemon by commenting it out of /etc/inetd.conf and restarting inetd. WINDOWS: Fingerd is not native to Windows, but may be present. Disable it as follows: LOCAL MACHINE (GUI): From the Start menu, choose Settings/Control Panel/Services. Select the service and click 'Stop.'

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.1			Line User Host(s) Idle Location	12

Vulnerability Name:
Traceroute

Severity:
Low

Description:
Traceroute prints the route packets take to get to networked host.

Fix:
Prevent or limit external tracerouting into internal networks via packet filtering. UNIX: The UNIX version of the Scanner uses UDP packets to conduct a traceroute. Disallow incoming UDP packets with high-numbered destination ports. For more information, consult your firewall documentation. ICMP packets are not found by UNIX. WINDOWS NT: The NT version of the Scanner uses ICMP to conduct a traceroute. Disallow incoming ICMP packets with high-numbered destination ports. For more information, consult your firewall documentation. UDP packets are not found by NT. NOTE: Because the UNIX and NT versions of the Scanner use different methods for traceroute, this vulnerability may occasionally be found by one version of the Scanner and not the other.

IP Address	DNS Name	Associated Info	More Info	Session ID
193.136.57.1			Route: 192.168.0.5 -> 193.136.57.1	12

3. Relatório Final de Vulnerabilidades do *Host* Bastião

Apresentam-se nas próximas páginas (5 páginas) o relatório final de vulnerabilidades de rede obtido pela auditoria ao *router*. O relatório está ordenado por grau de risco (alto, médio e baixo) e apresenta a descrição de cada vulnerabilidade bem como a respectiva resolução.

Network Vulnerability Assessment Report

Sorted by Vulnerability Severity and Name

October 13, 1997

Report Description:

This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggested corrective action. Vulnerabilities are classified as high, medium and low. High risk vulnerabilities are those which provide authorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

Session Name:	Session1	**Session ID:**	17
Comment:	Tese	**Template:**	Heavy IPP
File Name:	Session1_971011B	**Termination Status:**	Finished
Scan Summary Information			
Hosts Scanned:	1	**Scan Start:**	1997/10/11 18:09:16
Hosts Active:	1	**Scan End:**	1997/10/11 18:22:50
Hosts InActive:	0	**Elapsed:**	00:13:34

Vulnerability Name:
FPNWCLNT.DLL has Incorrect Checksum

Severity:
High

Description:
The FPNWCLNT.DLL was found with an incorrect checksum. An altered DLL may allow access in plain text to all new passwords. Each time a password is changed or a user is added, this DLL gets called with the userids and plaintext password.

Fix:
Apply Windows NT 4.0 Service Pack 3 (SP3), convert to NTFS, verify the ACL allows proper access, make sure all values are for password filter packages are legitimate . Set the permissions properly. If an unauthorized security provider has been installed, and remove FPNWCLNT value or validate the FPNWCLNT.DLL. Apply SP3 as follows: 1. From the Start menu, choose 'Run'. 2. Type 'ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes' 3. Choose the desired country abbreviation. 4. Choose 'nt40/' 5. Choose 'ussp3/' or 'sp3/' 6. Choose i386/nt4sp3_1.exe for an Intel processor or ALPHA/nt4sp3_a.exe for an Alpha processor. -AND- If using FAT system, convert to NTFS as follows: 1. From the Start menu, choose Run. 2. Type 'cmd' and press ENTER. This opens the command prompt. 3. Type 'convert c: /fs:ntfs' and press ENTER. 4. Reboot your system. 5. Run chkdsk to make sure no errors are present. -AND- Verify the ACL key as follows: 1. From the Start Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. 2. Select HKEY_LOCAL_MACHINE. 3. Navigate to SYSTEM/CurrentControlSet/Control/Lsa/ 4. From the Security menu, choose 'Permissions'. 5. Verify that the permissions allow write access to Administrators and System. -AND- Verify password filter packages as follows: 1. From the Start Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens th Registry Editor. 2. Select HKEY_LOCAL_MACHINE. 3. Navigate to SYSTEM/CurrentControlSet/Control/Lsa/Notification Packages 4. Verify that all values in this key are for password filter packages that Setup intended to install. -OR- If you do not use FPNW or DSMN, remove the FPNWCLNT value as follows: 1. From the Start Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. 2. Select HKEY_LOCAL_MACHINE. 3. Navigate to SYSTEM/CurrentControlSet/Control/Lsa/Notification Packages 4. Click on FPNWCLNT and press delete. 5. Verify deletion. -OR- If you use FPNW or DSMN, validate the version of FPNWCLNT.DLL is dated 05/01/97 and is size of 35,088.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO			17

Vulnerability Name:
Inappropriate User with Act as System Privilege

Severity:
High

Description:
A user has been detected with Act as System privileges. This right is not normally granted to any users, and can be used to attain administrative rights.

Technician

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. Select Policies, User Rights, enable Show Advanced User Rights, then verify that this right is set in accordance with your security policy.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO	MasterAlfa		17

Vulnerability Name:
Windows NT Security Log Accessible

Severity:
High

Description:
This vulnerability enables an intruder to read the Security Log on a Windows NT computer. This indicates that the user has administrative access, and that possibly the Guest account is enabled with network access. If the user running the Scanner legitimately has administrative access to the host, this is not a vulnerability.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. From the Policies menu, select 'User Rights.' Check administrative rights on the machine, and the state of the network access rights for the guest account.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO			17

Vulnerability Name:
All Access NetBIOS Share - Everyone

Severity:
Medium

Description:
A NetBIOS share has been found with no access control. This allows anyone full access to any resources provided, and can also allow access to the entire hard drive on unpatched versions of Windows 95.

Fix:
WINDOWS NT: Set the permissions explicitly as follows: LOCAL MACHINE (GUI): Navigate to the NetBIOS share, right-click on the shared directory and select 'Properties.' On the 'Sharing' tab, set the permissions to allow access only to approved users. -OR- Remove the share as follows: LOCAL MACHINE (CLI): Type 'net share sharename /delete.' REMOTE HOST (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/Server Manager. Select the host. From the Computer menu, select 'Shared Directories.' Select the NetBIOS share and click 'Stop Sharing.' UNIX: Consult your Samba documentation. This condition may require changes to Samba authentication procedures.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO	maildat$		17

Vulnerability Name:
Sendmail %style relaying.

Severity:
Medium

Description:
Internet Scanner has determined that your SMTP server supports third-party or %style mail relaying. Third-party mail relaying occurs when a mail server processes a mail message where neither the sender nor the recipient is local to the server's mail domain. While third party relaying has some legitimate purposes, such as allowing mail messages to be routed around known mail problems, e-mail hijackers (or spammers) primarily use it to obscure their identity while sending large amounts of junk mail.

Fix:

Re-configure your SMTP server to enforce that all mail messages must either originate or terminate locally (on the mail host). General References: Information about anti-spam provisions and references is available at http://www.sendmail.org/antispam.html. The Mail Abuse Protection System (MAPS) home page is at http://maps.vix.com. Techniques and organizations dedicated to fighting junk e-mail are at http://spam.abuse.net/. For information about disabling third-party or %style relaying for specific mail servers refer to http://maps.vix.com/tsi/ar-fix.html.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO			17

Vulnerability Name:
HTTP Proxy Detected

Severity:
Low

Description:
A HTTP proxy was detected on the host. Some older proxy server may have vulnerabilities that allow an intruder to execute commands remotely.

Fix:
Disable the service. UNIX: Comment out the httpd entry in /etc/inetd.conf. Place a '#' at the beginning of the line and send a HUP signal to the inetd. (# kill -HUP <inetd.pid>). WINDOWS NT: LOCAL MACHINE (GUI): From the Start menu, choose settings/Control Panel/Services. Select the HTTP service and click 'Stop.' -OR- Review your proxy rules. Consult your firewall documentation for more information.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO			17

Vulnerability Name:
NetBIOS share found

Severity:
Low

Description:
This vulnerability indicates that a NetBIOS share has been found. If the share has the proper access controls, this is a very low risk vulnerability.

Fix:
LOCAL MACHINE: Set the permissions explicitly as follows: 1. Navigate to the share in Windows Explorer. 2. Right-click on the share, select 'Properties'. 3. Under the 'Sharing' tab, review the permissions. 4. Allow access only to approved users. 5. Click 'OK'. -OR- Open the command line, remove the share as follows: 1. From the Start menu, select Run. 2. Type 'cmd', then click 'OK'. This opens the command line. 3. Type 'net share sharename /delete.' where sharename is the name of the share. 4. Type 'exit' to return to the Windows NT desktop. REMOTE HOST (GUI): Remove the share as follows: 1. From the 'Start' menu, select 'Programs/Administrative Tools (Common)/Server Manager'. 2. Select the host. From the 'Computer' menu select 'Shared Directories.' 3. Select the share and click 'Stop Sharing.'

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO	Add-ins		17
192.168.1.2	HOSTBASTIAO	Address		17
192.168.1.2	HOSTBASTIAO	ADMIN$		17
192.168.1.2	HOSTBASTIAO	C$		17
192.168.1.2	HOSTBASTIAO	connect$		17
192.168.1.2	HOSTBASTIAO	D$		17
192.168.1.2	HOSTBASTIAO	IPC$		17

192.168.1.2	HOSTBASTIAO	maildat$	17
192.168.1.2	HOSTBASTIAO	NETLOGON	17
192.168.1.2	HOSTBASTIAO	Resources	17
192.168.1.2	HOSTBASTIAO	tracking.log	17

Vulnerability Name:
Readable NT Application Log

Severity:
Low

Description:
This vulnerability enables an intruder to read the Application Log on a Windows NT computer. This may indicate that the Guest account is enabled, possibly with network access rights. If the user running the scan is an authorized user, this may not indicate a vulnerability.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. From the Policies menu, select 'User Rights' and examine which users are allowed to log on from the network. Also, check whether the Guest account is enabled.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO			17

Vulnerability Name:
Traceroute

Severity:
Low

Description:
Traceroute is a utility used to determine the path a packet takes between two endpoints.Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

Fix:
Prevent or limit external tracerouting into internal networks via packet filtering. UNIX: The UNIX version of the Scanner uses UDP packets to conduct a traceroute. Disallow incoming UDP packets with high-numbered destination ports. For more information, consult your firewall documentation. ICMP packets are not found by UNIX. WINDOWS NT: The NT version of the Scanner uses ICMP to conduct a traceroute. Disallow incoming ICMP packets with high-numbered destination ports. For more information, consult your firewall documentation. UDP packets are not found by NT. NOTE: Because the UNIX and NT versions of the Scanner use different methods for traceroute, this vulnerability may occasionally be found by one version of the Scanner and not the other.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO		Route: 192.168.1.2 -> 192.168.1.2	17

Vulnerability Name:
Unknown NT Service

Severity:
Low

Description:
A service was found which was not known to ship with Windows NT. Services can be used to install back doors, or provide unauthorized network access. Any service which is not approved by your security policy should be removed.

Fix:
Use instsrv from the Windows NT Resource Kit to remove the unwanted service. Remove the service as follows: 1. From the Start' menu, choose 'Run'. 2. Type 'cmd' and click 'OK'. This opens the command line. 3. At a command pror ype 'instsrv [service name] remove' and press <ENTER>. 4. Type 'exit' and press <ENTER> to return to vindows.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO	MSExchangeDS		17
192.168.1.2	HOSTBASTIAO	MSExchangeDX		17
192.168.1.2	HOSTBASTIAO	MSExchangeES		17
192.168.1.2	HOSTBASTIAO	MSExchangeFB		17
192.168.1.2	HOSTBASTIAO	MSExchangeIMC		17
192.168.1.2	HOSTBASTIAO	MSExchangeIS		17
192.168.1.2	HOSTBASTIAO	MSExchangeMSMI		17
192.168.1.2	HOSTBASTIAO	MSExchangeMTA		17
192.168.1.2	HOSTBASTIAO	MSExchangeSA		17
192.168.1.2	HOSTBASTIAO	ProtectedStorage		17

Vulnerability Name:
Windows NT Registry opened remotely

Severity:
Low

Description:
This indicates that the Scanner is able to open the registry remotely. This may indicate that permissions are not set properly, or that possibly the guest account is enabled with network access rights. An attacker could alter file associations, permitting the introduction of a trojan horse, or otherwise seriously compromise the machine. If the host running the scan is a trusted host, this may not indicate a vulnerability.Under NT 4.0, registry access from the network can be denied completely.

Fix:
Restrict registry access and/or reset permissions. Restrict registry access as follows: 1. From the Start Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor. 2. Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg. 3. From the Security menu, choose 'Permissions'. 4. Restrict access to all or set permissions to allow access to approved Administrators only.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO			17

Vulnerability Name:
Windows NT System Log Accessible

Severity:
Low

Description:
Windows NT System Log was found to be accessible. This vulnerability enables an intruder to read the System Log on a Windows NT computer. This may indicate that the guest account is enabled, possibly with network access rights. If the user running the scan is a authorized user, this may not indicate a vulnerability.

Fix:
LOCAL MACHINE (GUI): From the Start menu, choose Programs/Administrative Tools (Common)/User Manager. From the Policies menu, select User Rights. Check administrative rights on the machine, and the state of the network access right for the guest account.

IP Address	DNS Name	Associated Info	More Info	Session ID
192.168.1.2	HOSTBASTIAO			17

Direitos Legais do Software Utilizado

Agradece-se à Check Point Software Technologies Ltd e à sua representante em Portugal a SOL-S a disponibilização do software Fireall-1 3.0b (VPN).

Agradece-se à Internet Security Systems Inc. e à sua representante em Portugal Pararede a disponibilização do RealSecure 2.5 e do Internet Scanner 5.4.

Fireall-1 3.0 para Windows NT é uma marca registada da Check Point Software Technologies Ltd., 1991 a 1998.

RealSecure 2.5 para Windows NT é uma marca registada da Internet Security Systems Inc. 1991 a 1997.

Internet Scanner 5.4 para Windows NT é uma marca registada da Internet Security Systems Inc. 1991 a 1997.

Microsoft Windows NT 4.0, Internet Information Server, Microsoft Exchange Server 5.5 e Microsoft Proxy 2.0 são marcas registadas da Microsoft Corporation.

