Universidade do Porto
Faculdade de Engenharia
FEUP

Ricardo Manuel Soares Batista

Implementação e Segurança de Redes de Dados

Siemens, S.A.

Setembro, 2004

Faculdade de Engenharia da Universidade do Porto

Licenciatura em Engenharia Informática e Computação

Implementação e segurança de redes de dados

SIEMENS, S.A.

Relatório do Estágio Curricular da LEIC 2004

Ricardo Manuel Soares Batista

Orientador na FEUP: Prof. Raul Oliveira

Orientador na SIEMENS: Engº Pedro Paz

Setembro de 2004

"A false sense of security is worse than insecurity."

(A falsa sensação de segurança é pior que insegurança)

– Steve Gibson

Resumo

O trabalho desenvolvido, com o título "Implementação e segurança de redes de dados", insere-se no âmbito do estágio curricular para a conclusão da licenciatura de Engenharia Informática e Computação da Faculdade de Engenharia da Universidade do Porto. Foi levado a cabo na Siemens Portugal, durante a realização de um projecto para um cliente.

O estágio possui três vectores principais, nomeadamente: a avaliação do estado de arte da segurança de redes, a implementação e gestão de redes, e a análise de segurança de redes.

A avaliação do estado de arte permite a familiarização com a importância da segurança e ameaças existentes à informação. São apresentados também mecanismos e tecnologias de segurança, bem como, aplicações que podem ser utilizadas na manutenção da segurança de redes. Esta avaliação termina com um conjunto de informação gráfica que permite sintetizar o estado actual da segurança de redes.

A implementação e gestão de redes apresenta uma matéria mais prática da área das redes. A rede de intervenção é descrita de forma simples e ilustrativa, sendo expostos os mecanismos de gestão da implementação, assim como aplicações para a gestão da própria rede. Apresenta-se também uma ferramenta desenvolvida, *IP Account Alert*, que permite a detecção de vírus numa rede através da identificação de estações com comportamento anormal. A finalizar, é demonstrado como foi concretizada a segurança desta rede ao nível dos equipamentos activos.

A análise da segurança de redes é o resultado do cruzamento entre a avaliação do estado de arte da segurança e da implementação e gestão da rede em causa. É um tópico que foi simplificado através de uma breve narração dos problemas encontrados na rede implementada e respectivas soluções.

Por inferência, o resultado destes seis meses de estágio é um documento com uma forte componente teórico-prática de segurança de redes, onde se pode encontrar, com clareza, os principais pontos deste tema e a sua demonstração prática.

Agradecimentos

Ao Engº Pedro Paz, orientador do estágio na Siemens, S.A., pela sua compreensão, disponibilidade, conselhos e acompanhamento, bem como, autonomia e responsabilidade concedida.

A todos os elementos da ESO – *Enterprise Solutions*, em especial ao Engº Fernando Romão e Engº Vitor Oliveira, pelos meios concedidos e apoio demonstrado, bem como à Administração pela oportunidade oferecida e pelo voto de confiança.

Ao Professor Raul Oliveira e a todos os elementos da LEIC – Faculdade de Engenharia da Universidade do Porto, pela sua disponibilidade e boa vontade.

Índice de Conteúdos

Índice de figuras

Índice de tabelas

Lista de Acrónimos

Acrónimo	Designação
ACL	*Access Lists*
BGP	*Border Gateway Protocol*
CERT	*Computer Emergency Response Team*
DHCP	*Dynamic Host Configuration Protocol*
FTP	*File Transfer Protocol*
HTTP	*Hyper Text Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
HSRP	*Hot Standby Redundancy Protocol*
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
IOS	*Internetworking Operating System*
LAN	*Local Area Network*
MAC	*Media Access Control*
NTP	*Network Time Protocol*
POP	*Post Office Protocol*
SFTP	*Secure File Transfer Protocol*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SQL	*Structure Query Language*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
UPS	*Uninterruptible Power Supply*
VLAN	*Virtual Local Area Network*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
WEP	*Wired Equivalent Privacy*
WPA	*Wi-Fi Protected Access*

1 Introdução

A competitividade no mercado empresarial não permite às organizações qualquer tipo dè negligência.

Na era de Informação, a informação é o bem mais valioso que uma organização pode possuir. Actualmente, uma empresa que não proteja a sua informação não sobrevive muito tempo.

A informação é, de facto, o coração de uma organização. Como tal, a segurança da informação torna-se uma preocupação real, prevenindo e combatendo ataques que podem afastar uma organização do mercado empresarial.

1.1 Objectivo

O presente documento surge no âmbito da realização do estágio curricular levado a cabo na Siemens Portugal, S.A. pelo estagiário Ricardo Batista, desde Março até Agosto de 2004.

O estágio tem como principais objectivos: a avaliação do estado de arte da segurança de redes, a implementação e gestão de redes, e a análise de segurança de redes.

O trabalho apresentado, surge sobre o título de "Implementação e Segurança de Redes" desenvolve-se a partir da prestação de serviços, de apoio a um evento, por parte da entidade de estágio a um cliente.

A importância crescente do tema abordado e a intenção de conhecer mais sobre o mesmo, foram factores decisivos na escolha deste tema, a segurança de redes.

Além de expôr o trabalho realizado durante o período de estágio, este documento pretende ainda apresentar elementos essenciais à compreensão desta área em franca expansão.

Ao longo deste relatório não é referido o nome do cliente por motivos de confidencialidade, pois o seu conteúdo poderia comprometer a sua rede IP.

1.2 Siemens – A empresa

"Quando os ventos sopram, uns constroem abrigos e outros constroem moinhos"

Em 1905, foi fundada a Companhia Portuguesa Siemens-Schuckert com sede em Lisboa e uma delegação técnica no Porto.

A sede da Siemens, S.A. é nas instalações de Alfragide, onde se concentra a Administração, os *Operating Groups* (OG – grupo operacional), as *Divisions* (divisões), *Corporate Centers* (centros corporativos) e as Assessorias. A única excepção é o *Operating Group Medical Solutions* (grupo operacional de soluções médicas) que, apesar de também estar representado em Alfragide, tem a sua sede na região Norte. A estrutura completa pode ser visualizada na figura seguinte:

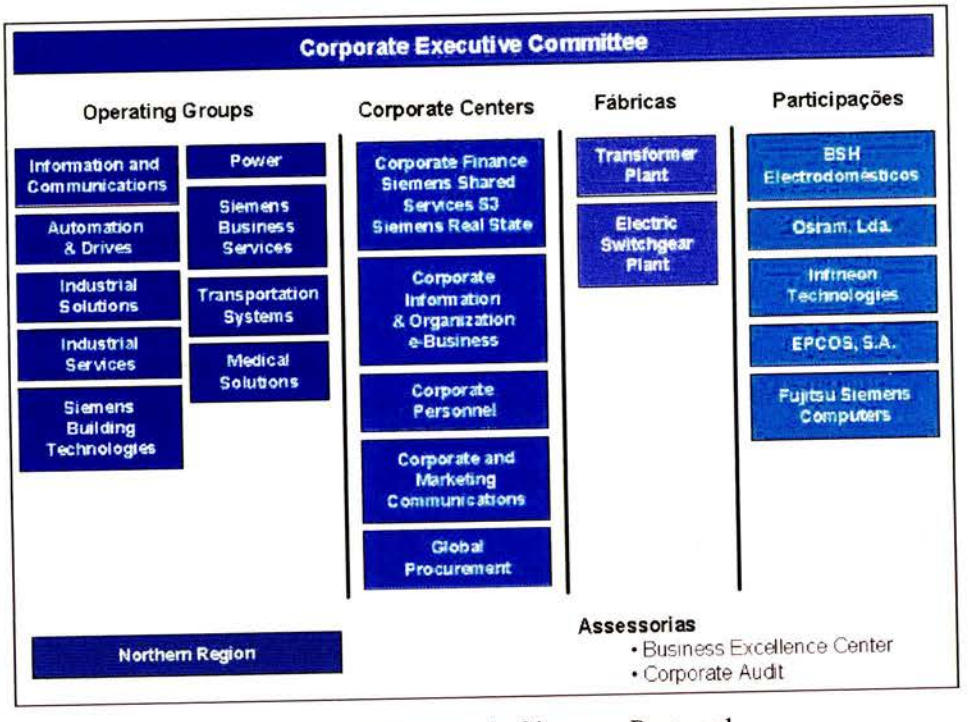


Figura 1: Estrutura da Siemens Portugal

A história da Siemens

A actividade mais antiga de que se tem conhecimento no nosso país remonta a 1876 e revolucionou por completo uma das primeiras actividades industriais em Portugal, a Indústria Vidreira da Marinha Grande.

Foram os irmãos Siemens que inventaram os primeiros fornos contínuos com regeneração do calor (tarde desenvolveram-se também para as indústrias do ferro e aço) permitindo, assim, o aumento substancial das produções em série.

Werner Von Siemens

Sir William Siemens

Como um inventor brilhante e um homem de visão da segunda metade do século XIX, Werner Von Siemens (1816-1892), contribuiu não apenas para a nova disciplina de engenharia eléctrica, como também para o desenvolvimento da indústria eléctrica. Com a construção do seu telégrafo com ponteiros, Werner fundou a "*Siemens & Halske Telegraph Construction Company*".

Wilhelm Von Siemens (1823-1883), irmão mais novo de Werner foi o responsável pelo estabelecimento da empresa nos mercados internacionais, através das suas actividades em Inglaterra. A partir de 1850, Wilhelm trabalhou como um agente para a "*Siemens & Halske*" em Londres, fundando, em 1858, a subsidiária inglesa "*Siemens, Halske & Co.*" para a produção e implementação de cabos no mar.

Siemens, nos dias de hoje

" O cliente é para nós a peça mais importante do puzzle!"

Praticamente nenhuma empresa é tão internacional como a Siemens, que está representada em quase todos os países do mundo.

A Siemens Portugal é constituída por diversos OG's onde se encontra o IC (*Information and Communications* – Informação e Comunicações). O OG IC tem como orientação estratégica a liderança nos mercados IP, Mobilidade e *E-business*. É com este posicionamento estratégico que a Siemens Portugal tem actuado no mercado nacional, caracterizado pela liberalização total do sector das telecomunicações, pela acrescida competitividade, dinamismo de mercado e uma complexidade elevada do negócio.

As diversas iniciativas deste OG conducentes à consolidação da sua posição de liderança, em vários domínios do sector das Tecnologias de Informação e Telecomunicações, contribuiram para o fortalecimento e solidez do Grupo Siemens em Portugal.

A filosofia da Siemens não é somente disponibilizar soluções inovadoras aos seus clientes e parceiros, como também aplicar com sucesso essas soluções na própria empresa.

O OG IC por sua vez contém várias áreas. A ESO é uma das áreas que constituem o IC, na qual foi realizado o estágio. A ESO é responsável pela implementação de soluções empresariais e prestação de serviços ao mercado empresarial.

Para melhor compreensão da organização do OG IC é apresentado pelo seguinte organigrama:

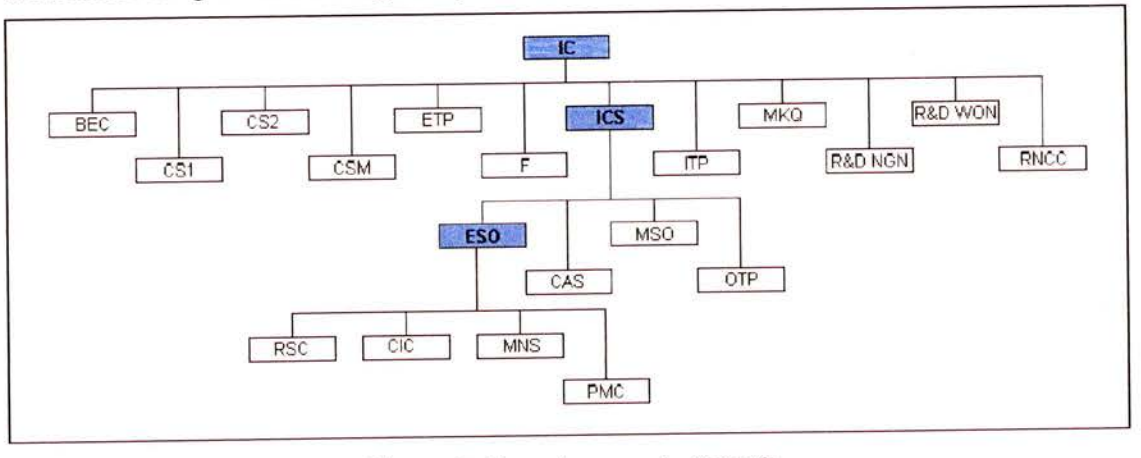


Figura 2: Organigrama do OG IC

A figura 2 apresenta todas as áreas que fazem parte do OG IC. Os níveis superiores são todos expansíveis mas, neste caso, apenas se expandiu a área onde se insere o estágio.

Além do grupo IC existem outros grupos, tais como:

- **A&D – Automation & Drives:** Oferece uma vasta gama de produtos e soluções que vai desde a aparelhagem de baixa tensão, a uma gama completa de equipamentos para instalações eléctricas de edifícios ou para os mais diversos ramos da indústria.

- **COMP – Components:** Representa, em Portugal, uma vasta gama de componentes electrónicos dirigidos à indústria de produção de módulos e aparelhagem electrónica.
- **I&S – Industrial Solutions:** Nos segmentos de mercado indústria, infra-estruturas e obras públicas, o OG IS oferece soluções inovadoras e eficazes com elevados padrões de qualidade que criam valor acrescentado para os seus clientes.
- **MED – Medical Solutions:** Como contributo significativo para cuidados de saúde mais eficientes, os produtos, sistemas e soluções Siemens optimizam processos nas clínicas, centros de saúde e hospitais, ajudando a tornar o diagnóstico mais rápido e preciso, facilitando a terapia.
- **P – Power:** A actividade empresarial da Siemens no sector de energia desenvolve-se em dois grandes segmentos de mercado, por um lado a produção – *Power generation* – e, por outro, o transporte e distribuição – *Power Transmission and Distribution* – de energia eléctrica.
- **SBS – Siemens Business Services:** A SBS posiciona-se como um fornecedor de soluções que abrangem a gestão, operação e manutenção de infra-estruturas de sistemas e redes, a concepção, desenvolvimento e integração de aplicações e ainda, a consultoria de processos e de sistemas.
- **TS – Transportation Systems:** Líder mundial em projectos chave-na-mão de transportes e sistemas ferroviários, o OG TS oferece aos seus clientes todo o tipo de soluções totalmente integradas para este mercado.

Grupo Siemens

Para além da empresa Siemens S.A, existem em Portugal outras empresas que pertencem ao grupo Siemens, como é possível constatar na seguinte figura:

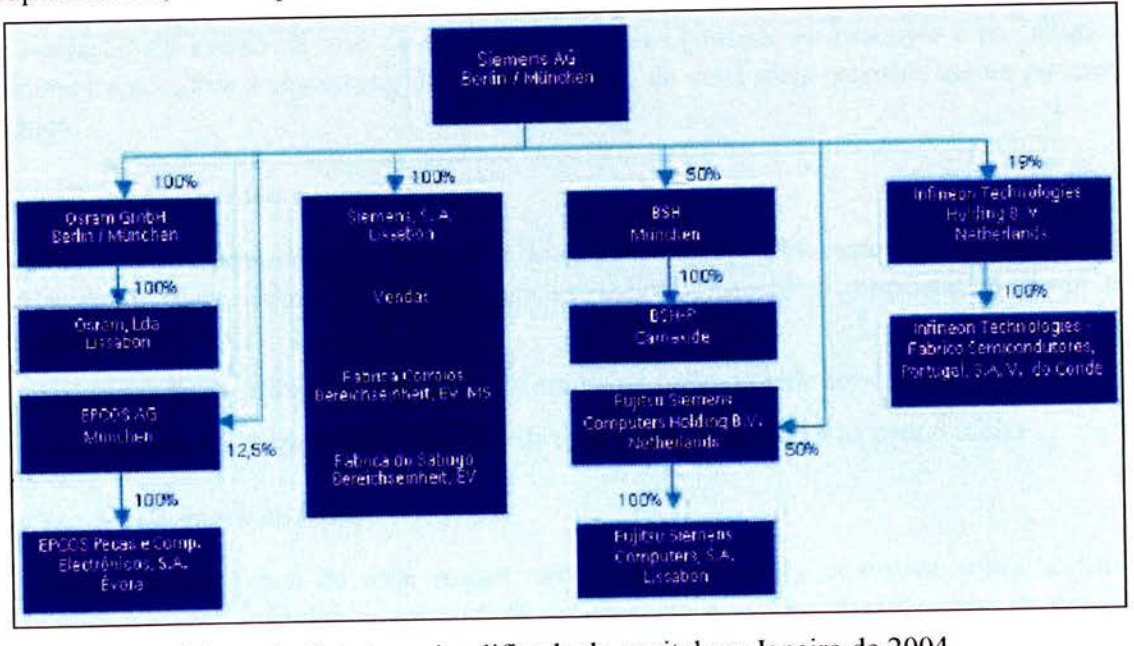


Figura 3: Estrutura simplificada do capital em Janeiro de 2004.

Alguns dados sobre o grupo Siemens:

- Volume de negócios de 77.013 milhões de doláres.

- Mais de 400 mil colaboradores em todo o mundo.
- Mais de 45 mil patentes/marcas.
- Em seis áreas de negócio: *Information and Communications* (Informação e Comunicações), *Automation and Control* (Automação e Controlo), *Power* (Energia), *Transportation* (Transportes), *Medical* (Saúde) e *Services* (Serviços).
- Presente em mais de 190 países.

1.3 Implementação e Segurança de Redes – O Estágio

O projecto de estágio abrange a implementação de uma rede de dados, a sua gestão e a respectiva análise de segurança, sendo integrado num projecto da Siemens para apoio a um cliente.

O estágio é dividido em quatro grandes fases: avaliação do estado de arte da segurança de redes, implementação e gestão da rede no cliente, análise de segurança da rede implementada e escrita do relatório de estágio.

As fases são escalonadas segundo o diagrama apresentado na figura seguinte:

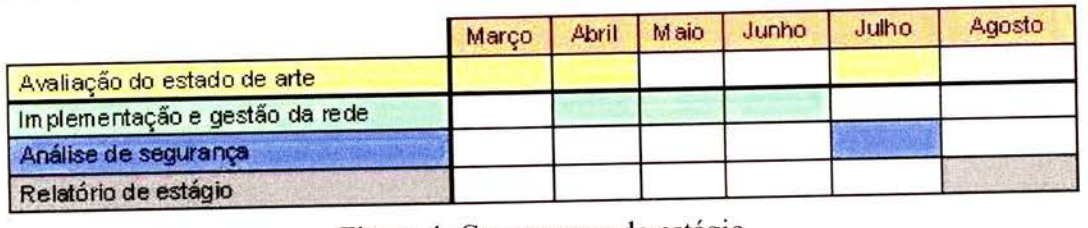


Figura 4: Cronograma do estágio.

Avaliação do estado de arte da segurança de redes

A avaliação do estado de arte da segurança de redes consiste na pesquisa e na leitura de documentação sobre a segurança, desde o seu ponto de vista mais genérico até ao pormenor técnico.

Implementação e gestão da rede

Esta fase envolve uma intensiva leitura de documentação dos fabricantes dos equipamentos a implementar, bem como de documentação sobre protocolos proprietários e o seu funcionamento.

Após a aquisição de informação, segue-se a implementação da rede concebida.

A gestão da rede é realizada com o auxilío de aplicações desenvolvidas para o efeito.

Análise de segurança de redes

A análise de segurança da rede requer, além de uma leitura exaustiva sobre auditoria informática e seus métodos, a capacidade de observar e avaliar situações que se revelem perigosas. É necessário ter sempre presente o compromisso entre segurança, acessibilidade e custos.

1.4 Organização dos capítulos

O presente relatório inicia-se com um capítulo de introdução cujo objectivo é a apresentação do documento, da instituição de estágio e do estágio propriamente dito.

O segundo capítulo pretende definir os principais conceitos do tema em questão, seguindo-se a análise do estado de arte da segurança de redes onde é possível conhecer as tecnologias mais recentes desta área, ataques, ferramentas e algumas previsões para o futuro.

O capítulo quatro incide sobre a rede implementada e analisada. Neste capítulo, é possível analisar a rede, os equipamentos envolvidos e as aplicações utilizadas na sua gestão, assim como, a aplicação concebida durante o período de estágio, a "*IP Account Alert*". É ainda efectuado um resumo de como a rede se encontra ao nível da segurança.

O quinto capítulo revela a análise de segurança, expondo os problemas encontrados durante o processo de análise.

Por último, o relatório culmina numa conclusão sobre o tema em estudo e o trabalho desenvolvido.

Em anexo, é possível encontrar um estudo realizado sobre as normas da segurança informática existentes, o código-fonte da aplicação "*IP Account Alert*" e um exemplo das configurações dos equipamentos de rede.

2 Conceitos de Segurança

Este capítulo pretende dar a conhecer a segurança enquanto conceito. Será analisado o que é segurança, como se define segurança informática e o conceito de segurança de redes.

Por fim, são apresentados os tipos de ataques que podem ocorrer nas redes.

2.1 Segurança

A definição de segurança não é clara, pois não existe uma única definição. No entanto, neste documento e de acordo com a recomendação X.800[1], assume-se que **segurança é a minimização das vulnerabilidades de bens e recursos**, ou seja, protecção de bens. Um **bem** é algo com valor e **vulnerabilidade** é uma fraqueza que pode ser explorada para violar o sistema ou a informação contida no mesmo. Uma **ameaça** é uma potencial violação de segurança.

Deste modo, a segurança sugere a criação e o cumprimento de medidas protectoras em relação aos objectos de protecção, ou seja, uma política de segurança.

Estas medidas estão classificadas da seguinte forma [1]:

- **prevenção**: conjunto de medidas que visam reduzir a probabilidade de concretização das ameaças existentes.
- **detecção**: conjunto de medidas que visam inspeccionar e detectar possíveis ameaças aos bens protegidos, de forma a minimizar o impacto das ameaças aquando da sua concretização.
- **reacção**: conjunto de medidas que visam recuperar os bens danificados em ameaças concretizadas.

Exemplo 1:

As medidas podem ser ilustradas, considerando a protecção dos bens guardados numa casa:

- prevenção: tranca-se portas e janelas, e coloca-se um muro à volta da propriedade. (prevenir a entrada de ladrões)
- detecção: coloca-se um alarme e um circuito de televisão fechado; caso contrário, só se detectará no dia seguinte. (detectar a entrada de ladrões)
- reacção: chamar a polícia e/ou repôr os bens retirados; a polícia pode recuperar algum bem e entregar-lhe. (reagir ao roubo)

Apesar deste caso ajudar a perceber os princípios da segurança informática, nem sempre é possível fazer-se estes paralelos.

Exemplo 2:

No caso de uma encomenda efectuada *online*, com cartão de crédito:

[1] No anexo A, é possível encontrar mais informação sobre esta recomendação.

- prevenção: usar encriptação quando a encomenda for colocada; confiar que a loja irá fazer algum tipo de verificação do cartão antes de aceitar a encomenda; não usar o número do cartão de crédito na Internet.
- detecção: aparecimento de uma transacção não autorizada no extracto do cartão de crédito.
- reacção: pedir um novo cartão; reclamar o custo da transacção não autorizada à loja virtual.

Neste caso, a vítima nunca deixa de possuir o cartão de crédito, apesar de ter sido "roubado". De facto, o bem roubado não foi o cartão, mas os dados do mesmo que possibilitaram a sua utilização indevida.

Políticas

Uma **política de segurança** é, portanto, o conjunto de regras classificadas pelas medidas referidas, onde se deve encontrar discriminado quem acede a quê, em que condições são realizados os acessos, o que fazer em caso de falha e o que implementar para prevenir um ataque. Ao conjunto de políticas de segurança, dá-se o nome de **modelo de segurança**.

Os modelos de segurança visam expressar formalmente as políticas de segurança. Os modelos mais conhecidos são [1]:

- *Bell-LaPadula*: preocupado com a concepção de sistemas operativos multi-utilizador seguros e apostando na confidencialidade do controlo de acessos;
- *Harrison-Ruzzo-Ullman* (HRU): define os sistemas de autorização, permitindo a alteração de permissões de acessos.
- *Chinese Wall* (muro chinês), de Brewer e Nash: sugere a inexistência de fluxo de informação que provoque conflito de interesses.
- *Biba*: visa a integridade em termos de acessos.
- *Clark-Wilson*: estabelece requisitos de segurança para aplicações comerciais.

Princípios

Apesar dos modelos e medidas, existe uma questão de equilíbrio e compromissos a ter em conta aquando do desenho de uma solução de segurança. Assim sendo, é possível afirmar que a segurança assenta no seguinte conjunto de princípios [3]:

- **Relação custo/benefício**: Traduz a necessidade de garantir um equilíbrio entre os custos associados à implementação de medidas de segurança e o retorno do investimento em matéria de prevenção, protecção e reacção. É um princípio frequentemente esquecido pelas dificuldades inerentes à avaliação do valor dos bens em causa. No entanto, existem fórmulas que permitem calcular o retorno do investimento e o seu benefício.
- **Concentração**: Defende a concentração dos bens a proteger em função da sua sensibilidade. Com este princípio é possível melhorar a eficiência da gestão das medidas de protecção, pois reduz duplicações através da classificação dos bens em causa.

- **Protecção/defesa em profundidade**: Requer que os bens e respectivas medidas de protecção sejam dispostos de forma concêntrica seguindo um modelo de camadas. Ou seja, os bens mais sensíveis no centro e os menos sensíveis no perímetro. Cada camada ou anel é uma barreira de protecção, aumentando o grau de dificuldade de acordo com o grau de profundidade. Este princípio permite organizar as medidas de segurança transformando-as numa sequência de obstáculos adaptados aos fins a que se destinam. A seguinte figura é ilustrativa deste princípio:
- **Consistência**: Este princípio alerta à necessidade da protecção homogénea face à sensibilidade dos bens protegidos. Ou seja, a protecção dos bens deve estar de acordo com a sua importância. O princípio chama a atenção para a falta de cuidado, evitando a situação clássica de ter porteiro e câmaras na porta da frente, enquanto que a porta das traseiras está destrancada.
- **Redundância**: Dita a necessidade de empregar mais do que uma forma de protecção do mesmo bem, de modo a impedir que exista pontos de falha. Por exemplo, se a energia numa sala de bloco operatório estiver assente em apenas um circuito de energia sem um gerador de apoio, temos, claramente, um único ponto de falha e crítico!

Este conjunto de conceitos é a base da segurança, definindo os principais vectores desta área. Todos estes conceitos são aplicados a todas as áreas da segurança, como, por exemplo: segurança física de edifícios (protecção de casas ou lojas) e segurança pessoal (protecção de pessoas importantes).

A seguinte figura permite uma visualização gráfica de como estes conceitos estão relacionados:

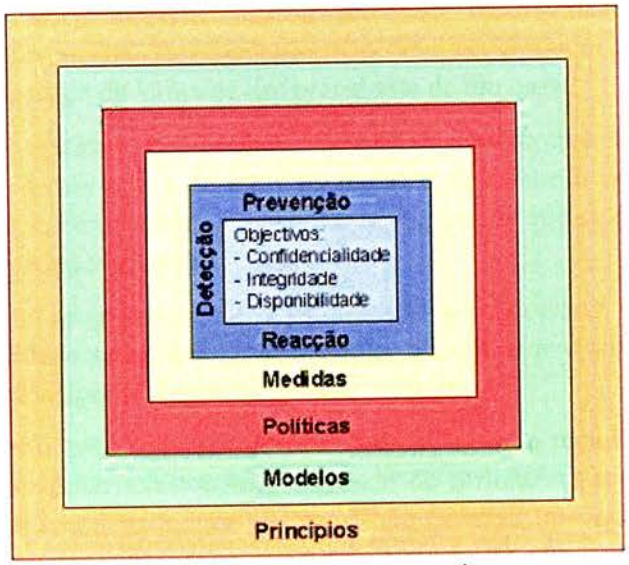


Figura 5: Relação de conceitos.

2.2 Segurança informática

A informática é o tratamento racional e automático da informação (armazenamento, análise, organização e transmissão), o qual se encontra associado à utilização de computadores e respectivos programas. Assim, o objecto mais valioso da informática é a informação que é tratada e processada.

Sendo segurança a protecção de bens, podemos afirmar que a **segurança informática** é a protecção da informação nas suas componentes de armazenamento, análise, organização e transmissão.

A segurança informática deve proteger a informação em três importantes aspectos:

- **confidencialidade**: prevenir o acesso não autorizado à informação.
- **integridade**: prevenir a alteração não autorizada da informação.
- **disponibilidade**: prevenir a impossibilidade de acesso autorizado à informação quando solicitado.

No entanto, quando se está a pensar na vertente de transmissão (comunicações), é necessário acrescentar-se a **autenticidade**, ou o **controlo de acessos** se o interesse for na área aplicacional (armazenamento, análise e organização).

O seguinte quadro permite uma rápida assimiliação deste conceito:

Segurança Informática	Geral	Confidencialidade
		Integridade
		Disponibilidade
	Comunicações	Autenticidade
	Aplicações	Controlo de Acessos

Tabela 1: Segurança Informática

A **confidencialidade** deve impedir utilizadores não autorizados de conhecerem ou aprenderem informação sensível. Por exemplo, não deve ser possível que terroristas tenham acesso ao plano de segurança da visita de um presidente de um país.

A **integridade** implica garantir que nenhum utilizador, mesmo que autorizado, do sistema modifique registos de forma a que os bens ou registos de controlo de uma empresa sejam perdidos ou corrompidos. Por exemplo, um banco deve garantir que os dados bancários de um cidadão não sejam alterados por outrém.

A **disponibilidade** é a propriedade de a informação ser acessível e utilizada quando é solicitada por uma entidade autorizada. Por exemplo, impedir que o sistema de facturação de uma gasolineira esteja indisponível.

A **autenticidade** possui três vectores-mestre: validação, não-repúdio e autenticação. A **validação** pretende confirmar a verdadeira entidade do utilizador, impedindo que esta seja utilizada indevidamente, ou negada, por exemplo, não permitir que um novo colaborador de da empresa seja autenticado como administrador do sistema. O **não-repúdio** permite prevenir a rejeição da origem ou veracidade da informação. A **autenticação** é o reconhecimento do utilizador como verdadeiro; deste modo, a autenticação pode ser realizada com base em um ou num conjunto de três factores: algo que se sabe (p.e., uma *password*), algo que se possui (p.e., um *smartcard*) ou algo que se é (p.e., impressão digital).

O **controlo de acessos** surge no sentido de atribuir permissões aos utilizadores no sistema e manter o registo dos acessos efectuados, como por exemplo, registar as entradas num armazém de equipamento informático.

A necessidade e facilidade actual de contacto com sistemas informáticos, assim como, a informação mantida e transferida através destes sistemas, levanta questões pertinentes em relação à segurança destes sistemas, principalmente nos aspectos referidos anteriormente. Quem tem acesso a informação crítica? E se alguém de má fé obter essa informação? Quais as consequências se essa informação for alterada? E se não for possível ter acesso à informação quando se pretende? Como se verifica que quem acede à informação é mesmo quem diz ser? E não se controla quem tem acesso a quê? E se existir informação que desapareça ou seja "roubada"?

A segurança informática pretende colmatar estas questões, tornando-se um "mal necessário" para os gestores e um investimento que, quando não é bem realizado, pode trazer graves prejuízos.

A segurança informática nasce, portanto, dos sistemas informáticos e da necessidade de salvaguardar a informação que viaja e reside nestes sistemas.

2.3 Segurança de redes

A segurança de redes é a componente de transmissão, comunicação e interligação de sistemas da segurança informática. Consiste em minimizar as ameaças de ataques à informação quando esta se encontra em trânsito na rede.

Apesar de ser uma componente da segurança informática, com o aumento do número de atacantes, da informação disponível na Internet, do surgimento de novas tecnologias e protocolos de segurança, a diversidade de meios de transporte, bem como, as vulnerabilidades existentes no protocolo normalizado TCP/IP, trata-se de uma componente com um elevado grau de complexidade.

Como explicado anteriormente, a segurança de redes assenta em quatro aspectos principais: confidencialidade, integridade, disponibilidade e autenticidade.

A segurança de redes pretende garantir que a transferência de dados num sistema, e mesmo entre sistemas, seja realizada sem que alguém possa ter acesso aos dados ou alterá-los durante a comunicação. Mais, a segurança de redes pretende validar e certificar de que o emissor e o receptor dos dados são legítimos, ou seja, que ambos são quem dizem ser, impossibilitando o roubo dos dados aquando da sua transferência. A segurança de redes pretende ainda garantir a possibilidade de transferir informação sempre que necessário ou solicitado.

Sendo assim, o objectivo da segurança de redes é prevenir ataques e minimizar o seu impacto em caso de concretização.

2.4 Tipos de ataques

Os ataques podem ter origem interna ou externa à organização e são realizados de acordo com os seguintes dois modos de actuação:

- **ataques passivos**, onde a informação/comunicação é visualizada e/ou copiada;
- **ataques activos**, onde a informação/comunicação é alterada e/ou desviada.

A seguinte figura pretende apresentar graficamente a estrutura dos tipos de ataques:

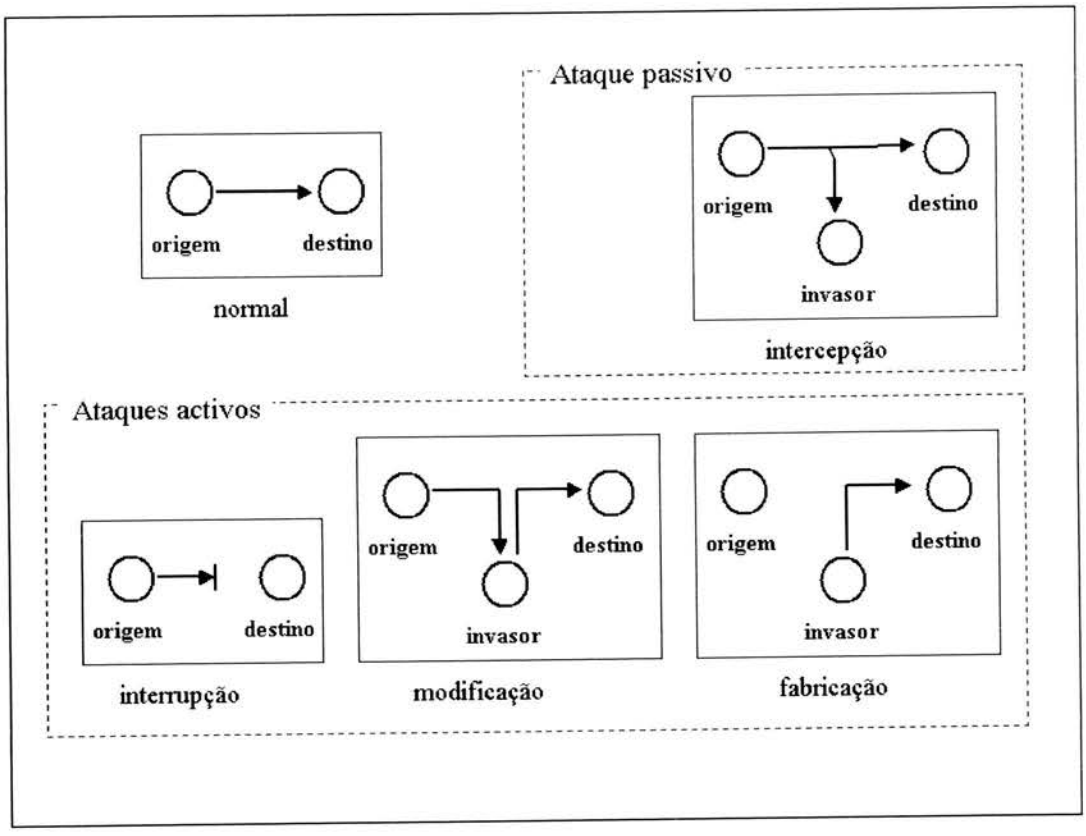


Figura 6: Tipos de ataque

Antes de explicar os ataques mais comuns, é apresentada uma tabela ilustrativa do seu contexto:

Passivos	Intercepção	*Snooping*
		Eavesdropping
		Intercepção
Activos	Interrupção	*Informação*
		Aplicações
		Sistemas
		Comunicação
	Modificação	*Alteração*
		Inserção
		Remoção
	Fabricação	*Masquerading*
		Negação de um evento

Tabela 2: Ataques

A intercepção é um ataque passivo que visa a tentativa de obter e/ou copiar informação sem autorização. Este ataque pode ocorrer onde a informação reside ou durante a sua transmissão. É um ataque que atenta à *confidencialidade* da informação e pode ocorrer nas seguintes formas:

- *Snooping (procura)*: procura de algo interessante pelos ficheiros de informação.
- *Eavesdropping (escuta)*: escuta de uma conversação à qual o atacante não faz parte.
- *Intercepção*: o atacante, ao interceptar informação, coloca-se no caminho do fluxo podendo examinar a informação e permitir, ou não, a sua passagem.

A interrupção é um ataque que nega a utilização dos recursos e/ou o acesso à informação pelos seus legítimos utilizadores. Além de ser considerado um acto de vandalismo, atenta contra a *disponibilidade* da informação e pode ocorrer nas seguintes formas:

- *Informação*: a interrupção da informação é impossibilitar a sua visualização, quer seja através da destruição ou indisponibilidade.
- *Aplicações*: trata-se de um ataque directo às aplicações, tornando-as inacessíveis à organização.
- *Sistemas*: é um ataque ao sistema que indisponibiliza os seus recursos, aplicações e informação.
- *Comunicações*: este ataque tem como alvo os meios de comunicação em si através da injecção excessiva de tráfego na rede, impossibilitando o acesso às aplicações e à informação.

A modificação é a tentativa de modificar informação, sem autorização para tal. É um ataque que pode ocorrer onde a informação reside (é armazenada) ou durante a sua transmissão. A alteração indevida da informação atenta à *integridade* da informação e pode ocorrer das seguintes formas:

- *Alteração*: é a modificação da informação tornando-a incorrecta. Por exemplo, a alteração da data de validade de um passaporte.
- *Inserção*: consiste na adição de informação falsa no sistema. Por exemplo, adicionar uma transacção num sistema bancário de modo a mover fundos entre contas bancárias.
- *Remoção*: trata-se de apagar informações. Por exemplo, registos históricos de acontecimentos.

A fabricação tem como objectivo a criação indevida de informação, bem como a tentativa de fornecer informação falsa. Trata-se de um ataque contra a *autenticidade* da informação e pode ocorrer nas seguintes formas:

- *Masquerading (mascarar)*: tentativa de agir como se fosse outro utilizador ou outro sistema.
- *Negação de um evento*: é a negação que um evento e/ou acção aconteceu como está nos registos do sistema.

3 Estado de arte da segurança de redes

O presente capítulo pretende, em primeiro lugar, transmitir a importância da segurança nos dias de hoje, referindo as ameaças existentes. Posteriormente, surge uma breve explicação das soluções e mecanismos actuais da segurança de redes, seguindo-se uma análise mais detalhada das tecnologias aplicadas. Este capítulo termina com uma listagem de ferramentas de *software* que permitem ajudar no processo de segurança de redes e com uma secção dedicada à situação actual, possibilitando uma visão global do ponto de situação da segurança e dos perigos existentes nas redes.

3.1 Importância da segurança

A Internet é, sem dúvida, a maior rede do planeta. É composta por milhares de computadores, é pública e tem como objectivo a possibilidade de estabelecer e facilitar relações pessoais, académicas e/ou empresariais. Torna-se assim, uma plataforma de fácil acessibilidade que permite a comunicação nos diversos níveis referidos. Mas, com esta acessibilidade, surgem novas ameaças ao nível da segurança.

Apesar da desconfiança e da insegurança aparente da Internet, é preciso referir que com o surgimento dessas novas ameaças, também emergiram tecnologias de segurança de combate. As tecnologias de segurança actuais permitem que seja mais seguro colocar dados pessoais na Internet do que fornecê-los a um hotel.

Actualmente, as empresas olham para a Internet como grande potencial para expandirem e melhorarem o seu modo de fazer negócio. Cada vez mais as empresas criam *extranets*[2] para lidarem com os seus parceiros, fornecedores e clientes; e *intranets*[3] para os seus colaboradores.

Embora seja uma forma optimizada de realizar o seu negócio, as empresas, através da Internet, expõem-se substancialmente, necessitando de se prevenir contra possíveis ataques. A prevenção visa impedir, por exemplo, roubos de informação (de clientes e fornecedores), paragens no negócio e sabotagem do negócio.

As empresas devem elaborar políticas e planos de segurança, bem como realizar uma intensa divulgação dessas políticas junto dos seus clientes, parceiros e colaboradores. Um ataque bem sucedido tem um impacto significativo nas organizações.

A indústria da informática já desenvolveu *standards* para ajudar a proteger a informação e certificar que a informação está segura.

Com a existência de *standards* e tecnologias de segurança, as empresas podem manter os seus sistemas quase imunes a ataques.

---

[2] Rede privada que permite a partilha segura de informações de negócio e operações com fornecedores, vendedores, parceiros, clientes e outros negócios.

[3] Rede privada contida na própria organização. Tipicamente, possui informação interna à empresa, permitindo a partilha de informação entre colaboradores e facilitando o trabalho em grupo.

É preciso frisar que, a maioria das quebras de segurança são concretizadas através de falhas na implementação das políticas de segurança, pela utilização de ferramentas disponíveis na Internet e pela falta de sensibilização para esta questão por parte dos utilizadores dos sistemas.

3.2 Ameaças à informação

As ameaças à privacidade e integridade da informação provêm de uma minoria de vândalos, tal como qualquer outro crime. No entanto, a grande diferença reside em que enquanto um assalto a um carro é realizado a apenas um carro, um ataque a partir de um computador pessoal pode prejudicar muitas redes e sistemas em todo o mundo.

Segundo especialistas da área da segurança, as ameaças são, normalmente, internas às organizações. Ou seja, colaboradores zangados, despedidos ou maliciosos que procuram danificar a rede da sua organização, bem como a informação da mesma.

Com as novas tecnologias, as organizações tendem a ligar-se directamente a parceiros e a possibilitar o acesso remoto à sua rede. Esta funcionalidade suscita novos pontos de ameaça, principalmente se as redes não forem monitorizadas e seguras por peritos.

Quem são os inimigos?

Hackers: Entusiastas que sentem prazer em ganhar acesso às redes e computadores de outrém. Não avisam e não são previsíveis quanto aos pontos de ataque.

Pessoal não-sensibilizado: Desprezam a segurança, deixando, por exemplo, *passwords* escritas debaixo do teclado. Esta falta de percepção pode permitir a injecção de vírus na rede ou perdas de informação importante. As organizações devem sensibilizar os seus colaboradores para a necessidade e importância da segurança no seu meio, bem como de estarem atentas aos erros humanos.

Pessoal insatisfeito: Colaboradores zangados, reprimidos, despedidos ou dispensados são especiais e potenciais atacantes. Além da sua insatisfação, possuem conhecimento sobre a rede e a importância da informação da organização.

Curiosos: Existem dois grupos de curiosos: os que querem satisfazer a sua curiosidade pessoal e os que fazem espionagem.

O que podem fazer os inimigos?

Vírus, é a ameaça mais conhecida devido à sua cobertura pelos meios de comunicação social. Vírus são programas de computador concebidos para se auto-replicarem e infectarem computadores na ocorrência de um determinado evento. Existem dois tipos de vírus: benignos e malignos[4]. Os primeiros são inofensivos e apenas mostram mensagens aborrecidas no visor. Os segundos já causam graves estragos como apagar informação, danificar o *hardware* ou atrasar o processamento do sistema.

[4] Os chamados *worms* inserem-se nesta categoria de vírus malignos, pois ao se duplicarem causam atrasos e lentidão nos sistemas.

Cavalos de tróia (trojan horse[5]*)*, são programas que contêm código destrutivo. São normalmente disfarçados como programas inofensivos (brincadeiras, jogos simples, etc.) ou úteis. Entre outras acções, podem apagar mensagens de correio electrónico, informação, abrirem pontos de ataque no sistema (portos) e enviarem-se a si próprios para toda a lista de endereços de correio electrónico (mais comum). Vírus e *trojans* espalham-se, comumente, através de anexos nas mensagens de correio electrónico.

Vândalos, são indivíduos que criam aplicações que destroem informação e colocam em sítios *web* para os utilizadores descarregarem. Estas aplicações também podem aproveitar vulnerabilidades conhecidas nos servidores *web* para alterarem a página principal de organizações, por exemplo.

Spam, é correio electrónico não solicitado. Implica perca de tempo (pela quantidade e lentidão que provoca nas caixas de correio) e espaço ocupado desnecessariamente nas caixas de correio.

Intercepção de informação, consiste em capturar a informação transmitida através dos diversos meios sem autorização (*IP Spoofing*[6]).

Engenharia social, consiste na obtenção de informação sem meios técnicos.

Ataques, são classificados em três categorias gerais: reconhecimento, acesso e negação de serviço.

- Reconhecimento: Ataques que consistem na obtenção de informação. Essa informação será utilizada para comprometer a rede. Existe *software* para capturar informação da rede (*sniffers*), para ver os serviços prestados (portos abertos) pelo sistema (*scanners*) e para detectar falhas/vulnerabilidades de segurança nos serviços prestados.
- Acesso: São conduzidos no sentido de explorar vulnerabilidades em aplicações que permitem o acesso ao sistemas, normalmente serviços de autenticação. Para este efeito, utilizam-se pequenos programas denominados *exploits*.
- Negação de serviço: Previnem o acesso aos sistemas. Consistem no envio de grandes volumes de tráfego incorrecto para um computador ligado a uma rede corporativa ou à Internet.

3.3 Mecanismos de segurança

Um mecanismo de segurança permite evitar e/ou proteger a informação de eventuais ataques. A aplicação destes mecanismos é diversa. No entanto, salienta-se o princípio de protecção-em-profundidade, como se pode observar na figura seguinte:

[5] O termo tem a sua origem na mitologia grega. De acordo com a lenda, os gregos ofereceram aos habitantes de Tróia um grande cavalo de madeira, dentro do qual tinham escondido os seus guerreiros. Durante a noite, os guerreiros sairam do cavalo de madeira e tomaram a cidade.

[6] Ver mais em: http://www.secwiz.com/Default.aspx?tabid=42

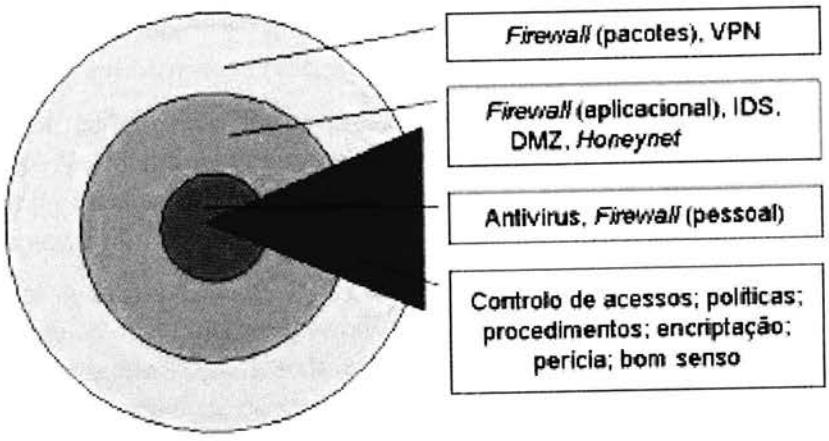


Figura 7: Defesa em profundidade – Mecanismos de segurança

Os mecanismos referidos na figura permitem aumentar gradualmente a segurança da rede recorrendo a tecnologias e medidas de segurança apropriadas. Assim sendo, segue-se uma breve explicação de como estes mecanismos podem contribuir para a concepção de uma solução de segurança.

- A implementação de *firewalls* permitirá a filtragem de tráfego de entrada e/ou de saída, evitando, por um lado, acessos externos não autorizados à rede e, por outro lado, alguns tipos de ataques à rede como, por exemplo, *SQL Injection*[7]. A instalação de *firewalls* pessoais permitem aos utilizadores filtrarem tráfego indesejado. A *firewall* é como uma fechadura, tratando-se de um *hardware* ou solução de *software* implementada na estrutura da rede que obriga ao cumprimento das políticas de segurança da organização ao restringir o acesso a recursos específicos da rede.
- A existência de *honeynets* possibilita simular a rede com o intuito de apanhar e registar todos os passos dos atacantes, permitindo, *à posteriori*, uma análise detalhada dos ataques. Este mecanismo revela-se muito útil no que diz respeito à prevenção e tomada de medidas correctivas nos sistemas ou nas políticas da organização.
- A utilização de IDS permite a detecção de intrusões, possibilitando uma reacção automática em tempo real, baseada na análise de padrões detectados no tráfego. Este mecanismo funciona como uma câmara de vigilância, tal como as *honeynets*. No entanto, a segurança de uma rede não se centra em apenas uma tecnologia ou equipamento, pelo que a utilização do IDS não dispensa a análise humana dos registos criados e dos eventos despoletados.
- A aplicação de VPNs possibilita a existência de interligações entre locais geograficamente distantes com segurança e custos reduzidos.

[7] Ataque que consiste na injecção de comandos SQL em aplicações *web*, com o objectivo de detectar e/ou explorar falhas do sistema *web*.

- A instalação de antivírus, nos computadores e servidores, evita a propagação de vírus através da sua detecção e remoção automática. Quando bem localizados, os antivírus podem evitar problemas de rede, normalmente relacionados com congestão[8] da rede.

  A constante actualização dos pacotes de antivírus permitem combater a grande maioria dos vírus. No entanto, é preciso ter em atenção que são criados milhares de vírus por mês, sendo estas actualizações destes pacotes de extrema importância na manutenção da segurança.

- A criação de zonas estanques, que consiste em separar zonas da rede de acordo com departamentos ou funções, permite isolamentos na rede (p.e., Internet, extranet, intranet, perímetro (DMZ), rede interna, wireless, modems). O principal objectivo é diminuir a probabilidade de uma falha numa zona da rede influenciar outra zona. Uma boa prática na aplicação deste mecanismo é não permitir acessos do exterior à rede interna.

- A encriptação (ou criptografia) possibilita a confidencialidade, integridade e autenticidade da informação na rede. Os certificados digitais e as assinaturas digitais diminuem a probabilidade de concretização de ataques à informação.

  A encriptação das comunicações permite a confidencialidade e integridade. No correio electrónico, por exemplo, possibilita confidencialidade e integridade da informação, bem como, a autenticidade do emissor das mensagens (através da assinatura digital). Os certificados digitais são muito utilizados no estabelecimento das redes virtuais privadas e na autenticidade de sítios *web*; podem ser comparados a um passaporte.

  A encriptação pode ser vista como a blindagem de um carro blindado, pois assegura que as mensagens (conteúdos do carro) não possam ser interceptadas ou lidas por alguém não autorizado.

- O estabelecimento e cumprimento de procedimentos revela-se essencial à manutenção da segurança da rede. Alguns procedimentos de exemplo são:
  - Aplicação e actualização de correcções de falhas (*patches*) nos sistemas operativos, aplicações e serviços de rede.
  - Análise rotineira de vulnerabilidades, comparando-as entre si e actualizando a lista de vulnerabilidades da aplicação de análise.
  - Procedimentos de escalada de risco, de acordo com os níveis de alerta.
  - Análise rotineira da rede, compara-se à ronda do guarda pelo edifício. Os analisadores de rede permitem compilar um inventário electrónico dos bens e das vulnerabilidades detectadas que podem conduzir ao compromisso da segurança. Permite, aos gestores da rede, identificarem e corrigirem falhas nos seus sistemas.

- O estabelecimento e cumprimento de políticas quanto à utilização e segurança da rede, permite educar, sensibilizar e responsabilizar os utilizadores. As políticas são regras que, electronicamente programadas e guardadas em equipamentos de controlo de

[8] Existem vírus que, além de se replicarem, tentam estabelecer contacto com dispositivos na *Internet*, gerando muito tráfego.

áreas, definem o privilégio de acessos. Existem políticas verbais, de regulamento e de segurança.

As políticas devem ser completas e aprovadas pelo topo da hierarquia da instituição, bem como, documentadas para posterior leitura de todos os colaboradores. A instituição deverá ainda obrigar à assinatura de um compromisso de confidencialidade dos seus fornecedores, parceiros e colaboradores. A revisão periódica das políticas de segurança é benéfica pois estas vão sendo actualizadas de acordo com novas necessidades e ameaças. Uma boa prática é a máxima "*O que não é explicitamente permitido, é proibido!*".

No caso das políticas de segurança, o objectivo é controlar quem tem acesso a que áreas da rede e como os utilizadores não autorizados são prevenidos de entrar nas áreas restritas. Com o desenvolvimento de políticas de segurança e implementação de salvaguardas, torna mais fácil a identificação da origem das ameaças e os tipos de ataques que podem ocorrer.

A gestão destas políticas deve ser entregue a um indíviduo ou grupo de pessoas de confiança. A difusão e comunicação das políticas definidas às pessoas é um ponto fulcral deste mecanismo. Após a definição das políticas é preciso identificar os métodos e tecnologias a aplicar no seu cumprimento.

- O controlo de acessos é também equivalente a uma fechadura (só entra quem tem a chave). Este mecanismo serve para validar a identidade do utilizador e determinará a que áreas e/ou informação este tem acesso, de acordo com o seu perfil. O controlo de acessos pode ser realizado, por exemplo, com o conhecimento de uma palavra-passe ou código, com a utilização de um *smart-card*[9], ou recorrendo à biometria[10].
- A perícia pode ser vista como um patrolhamento da área e de edifícios. Enquanto que as ferramentas de detecção de vulnerabilidades são úteis na rede, estas devem ser acompanhadas por uma avaliação da segurança realizada por peritos. Uma avaliação de segurança consiste numa análise concentrada da postura de segurança da rede, identificando fraquezas ou vulnerabilidades que necessitem de melhoramentos. Revela-se extremamente útil quando a rede sofre alterações.
- O bom senso é o principal mecanismo de segurança. É necessário avaliar correctamente o compromisso existente entre segurança, custo/benefício e acessibilidade dos recursos. A avaliação incorrecta deste compromisso pode resultar em graves prejuízos para a instituição. Por exemplo, uma entidade bancária que disponibilize *homebanking* aos seus clientes não aposta na segurança deste sistema em virtude da redução de custos; a existência de uma quebra de segurança pode provocar danos irreparáveis.

Além de todos estes mecanismos, é preciso ter sempre presente a principal regra da segurança: "*A segurança da rede é igual à segurança do seu ponto de acesso mais fraco.*"

[9] É um cartão de plástico do tamanho de um cartão de crédito, o qual contém um *microchip* (circuito integrado) embebido para guardar informação.

[10] Neste contexto, é a tecnologia que permite a análise de características humanas como impressões digitais ou a retina.

Existem, assim, várias soluções e mecanismos de segurança, desde a utilização de pacotes de aplicações de antivírus até *hardware* dedicado à segurança de redes, como *firewalls* e IDS.

3.4 Tecnologias de segurança de redes

Esta secção tenciona revelar um breve estudo que expõe, de forma genérica, as principais tecnologias de segurança de redes. O estudo dá a conhecer as tecnologias de base, o seu funcionamento e a sua possível aplicação. As tecnologias em causa são: *firewalls*, redes virtuais privadas (VPN), sistemas de detecção de intrusões (IDS) e encriptação.

Firewall

Uma *firewall* (parede-de-fogo) é um dispositivo de controlo de acessos de redes que foi concebido para negar todo o tráfego, à excepção daquele explicitamente autorizado. As *firewalls* podem ser configuradas para negar tráfego com base: no serviço solicitado, no endereço IP de origem ou destino, e/ou na identificação do utilizador que solicita o serviço; bem como, para registar todo o tráfego. Podem ser um pacote aplicacional a ser executado sobre um sistema operativo ou um dispositivo *hardware* de um fabricante.

A gestão de uma *firewall* é, normalmente, centralizada, ou seja, numa única configuração, o administrador de segurança pode definir a política pré-definida para o tráfego da rede. Uma *firewall* possui duas ou mais cartas de rede, e analisa o tráfego, de acordo com uma lista de regras, quando este passa de uma carta para outra. Normalmente, cada carta está ligada a uma rede diferente.

Existem dois tipos de *firewall*: de camada de aplicação e de filtragem de pacotes.

- *Camada de aplicação:* Também conhecida como *proxy firewall*. Neste tipo de *firewall*, as regras são forçadas através da utilização de *proxies*[11]. Para que determinado protocolo seja permitido, é necessário que este tenha o seu próprio *proxy*. A utilização deste tipo de *firewall*, implica que todas as ligações terminam na *firewall*. Ou seja, quando um utilizador pretende aceder a um servidor remoto, solicita à *firewall*, a qual iniciará a ligação com o servidor. A figura seguinte é uma demonstração gráfica deste conceito:

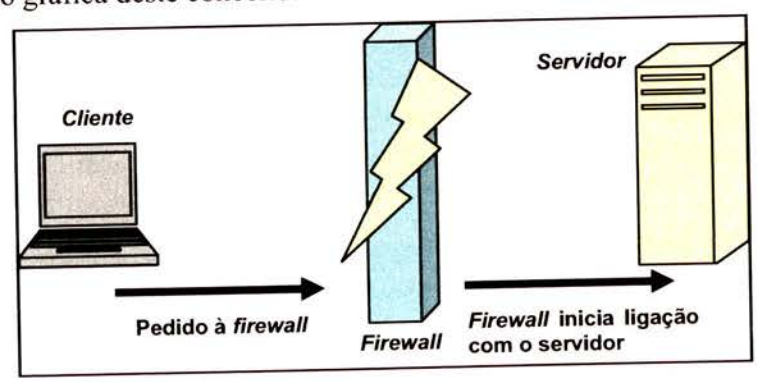


Figura 8: Funcionamento de uma *firewall* de aplicação

[11] Um *proxy* é uma aplicação ou *hardware* que possui autoridade para agir por conta de outrém, ou seja, age como intermediário entre a estação de trabalho de um utilizador e a Internet, assegurando algum nível de segurança e controlo de acessos.

Esta arquitectura permite também esconder os endereços dos sistemas atrás da *firewall*.

- *Filtragem de pacotes:* Neste tipo de *firewall*, as regras são forçadas a partir do uso de filtros de inspecção de pacotes. Os filtros examinam os pacotes e determinam se o tráfego é permitido, baseando-se nas regras definidas e no estado do protocolo (*stateful inspection*). Se o protocolo da aplicação está sobre TCP, então a determinação do seu estado é simples, visto que o TCP mantém o estado. Neste caso, quando o protocolo se encontra num determinado estado, apenas certos pacotes são esperados, sendo os restantes rejeitados pela *firewall*. No caso do UDP ser utilizado, sempre que existe um pacote para a *firewall* encaminhar, esta fica à espera de uma resposta num determinado intervalo de tempo. Portanto, as ligações não terminam na *firewall*, sendo estabelecidas directamente com o servidor, como se pode observar na figura seguinte:

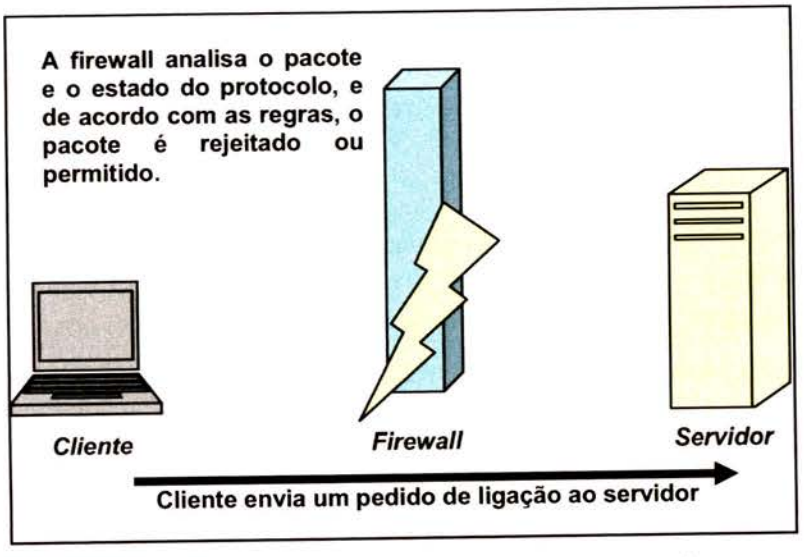


Figura 9: Funcionamento de uma *firewall* de filtragem de pacotes

Virtual Private Network (VPN)

As redes virtuais privadas (VPN) são uma forma de utilizar a infraestrutura pública de comunicações, como a Internet, para permitir o acesso seguro entre organizações ou utilizadores remotos e a rede corporativa. A VPN é uma solução de baixo custo que pode ser contrastada pelo sistema dispendioso de linhas próprias ou alugadas, as quais só podem ser utilizadas por uma organização.

A VPN funciona utilizando a rede pública, mantendo a privacidade através de procedimentos de segurança e protocolos de túneis, tal como o *Layer Two Tunneling Protocol* (L2TP). Com efeito, os protocolos, encriptando a informação no envio e desencriptando na recepção, enviam informação através de um túnel que não "aceita" informação que não tenha sido apropriadamente encriptada.

Existem dois tipos de VPN: *user-VPN* e *site-VPN*. A diferença reside no modo como a VPN é utilizada. Enquanto que a *user-VPN* é uma rede privada virtual entre o computador de um utilizador individual e a rede de uma organização; a *site-VPN* é entre localizações remotas de uma mesma organização ou entre organizações.

Uma VPN exige quatro componentes-chave:

- Servidor VPN: computador que actua como ponto final da VPN.
- Algoritmos de encriptação: devem ser escolhidos os mais fortes (3DES ou AES).
- Sistema de autenticação: deverá ser um sistema de dois-factores, ou seja, algo que se sabe e algo que se tem.
- Protocolo VPN: o protocolo *standard* de VPN é o IPSec.

Ao nível da implementação, existem três tipos de sistemas VPN:

- *Hardware*: dispositivo físico que actua como servidor VPN e executa software do fabricante, com vantagens de rapidez (alguma encriptação pode ser realizada ao nível do *hardware*) e segurança (sistema optimizado).
- *Software*: aplicações desenvolvidas para serem executadas num computador, o qual poderá ser dedicado.
- *Web-based*: nestes sistemas, a VPN é acedida via SSL. Ou seja, a VPN é uma aplicação *web* onde o cliente poderá realizar as tarefas pretendidas, sendo estas limitadas às funcionalidades implementadas.

IDS

Os sistemas de detecção de intrusão, IDS (*Intrusion Detection Systems*), são sistemas de *software* ou *hardware* que automatizam o processo de monitorização de ocorrência de eventos num computador ou numa rede, analizando-os à procura de sinais de problemas de segurança.

A detecção de intrusão é o processo de monitorização de eventos que ocorrem num sistema e de análise de intrusões, também definidas como tentativas de comprometer a confidencialidade, integridade e disponibilidade ou de passar pelos mecanismos de segurança do sistema. As intrusões são causadas por: atacantes que acedem ao sistema a partir da Internet; utilizadores autorizados nos sistemas que tentam ganhar privilégios adicionais aos quais não tem direito; e utilizadores autorizados que utilizam indevidamente os privilégios que possuem. Um IDS é um produto que automatiza este processo de monitorização e análise.

Os IDS's ajudam as organizações a protegerem os seus sistemas de ameaças que surgem com o aumento da conectividade da rede e com os sistemas de informação.

Estes sistemas permitem:

- Prevenir problemas, aumentando a percepção do risco da descoberta dos atacantes.
- Detectar problemas que não são prevenidos por outras medidas de segurança.
- Detectar o preâmbulo dos ataques.
- Documentar a existência de uma ameaça.
- Controlo de qualidade para a concepção e administração da segurança.
- Reunir informação útil sobre intrusões actuais.

Actualmente, existem diversos tipos de IDS que são caracterizados por diferentes aproximações de monitorização e análise. Agrupando os IDS por fontes de informação, existem três tipos:

- NIDS – *Network-based IDS*: Estes IDS detectam ataques através da captura e análise de pacotes da rede. Os NIDS consistem num conjunto de sensores ou dispositivos

colocados em vários pontos da rede. Estas unidades monitorizam o tráfego da rede, analisam localmente esse tráfego e enviam os relatórios dos ataques para uma consola de gestão central.

- HIDS – *Host-based IDS*: Os HIDS operam sobre a informação recolhida de um sistema individual, por exemplo, um computador. Desta forma, os HIDS analisam somente as actividades nos sistemas individuais com grande fiabilidade e precisão, determinando quais os processos e utilizadores do sistema operativo que estão envolvidos num ataque em particular. Estes IDS conseguem ainda detectar uma tentativa de ataque, pois monitorizam directamente os ficheiros e os processos do sistema.
- AIDS – *Application-based IDS*: AIDS são um subconjunto especial dos HIDS que analiza os eventos de uma determinada aplicação de *software*. Estes IDS detectam comportamentos suspeitos através do abuso de privilégios de utilizadores autorizados.

Encriptação

A encriptação é simplesmente a ofuscação da informação, permitindo a sua visualização por apenas indivíduos autorizados.

Trata-se de uma importante ferramenta de segurança, pois permite mecanismos que garantem a confidencialidade e integridade da informação. No entanto, é preciso ter a noção que esta ferramenta apenas atrasa a concretização de um ataque, ou seja, o ataque realizar-se-á assim que a cifra for quebrada.

A partir da encriptação é possível obter três serviços de segurança:

- Confidencialidade: a encriptação pode ser utilizada para esconder a informação de indivíduos não autorizados, quer a informação esteja em trânsito ou guardada.
- Integridade: a encriptação pode ser utilizada para identificar alterações na informação quando esta se encontra em trânsito ou guardada.
- Autenticidade: a encriptação pode ser utilizada para autenticar a origem da informação e prevenir a repudiação.

A encriptação consiste em dois tipos primários:

- Encriptação com chave privada (simétrica): Este tipo de encriptação requer que todas as partes, autorizadas a aceder à informação, possuam a mesma chave. Denomina-se encriptação simétrica porque a mesma chave é utilizada para encriptar e desencriptar informação, tal como se pode observar na figura seguinte:

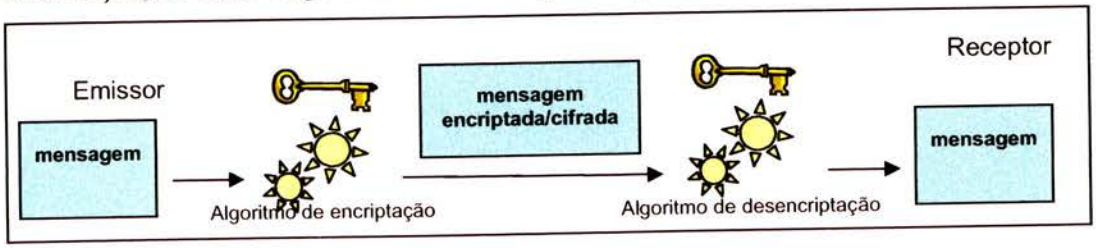


Figura 10: Encriptação simétrica

Alguns algoritmos deste tipo de encriptação são: DES, 3DES, *Unix password encryption*, AES, IDEA, RCS, *Blowfish* e CAST-128.

- Encriptação com chave pública (assimétrica): A encriptação com chave pública requer a utilização de duas chaves, uma para encriptar e a outra para desencriptar a informação, daí designar-se encriptação assimétrica. As chaves são consideradas como um par, ou seja, estão directamente relacionadas. No par, existe uma chave privada e uma chave pública. A chave privada fica sempre na posse do proprietário, enquanto que a chave pública é publicada junto da informação do seu proprietário. Com este modelo, a confidencialidade é conseguida através da encriptação da mensagem com a chave pública do receptor e da desencriptação com a chave par (chave privada do receptor); a autenticidade é alcançada através da encriptação com a chave privada do emissor, sendo validada com a sua chave par; a integridade é obtida em ambas as operações. A seguinte figura mostra o funcionamento deste modelo:

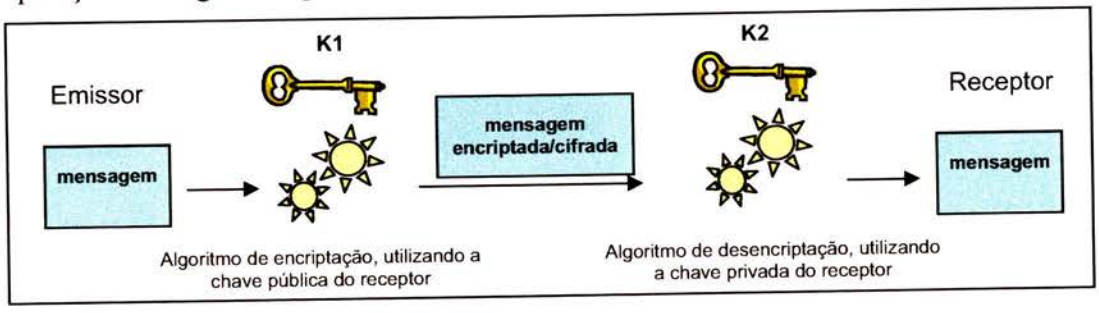


Figura 11: Encriptação assimétrica

Este tipo de encriptação é mais lento e mais intensivo ao nível computacional do que a encriptação simétrica. Alguns algoritmos utilizados são: *Diffie-Hellman Key Exchange*, RSA (*Rivest-Shamir-Adleman*) e DSA (*Digital Signature Algorithm*).

A encriptação contribui ainda para a existência da assinatura digital.

A assinatura digital é um método de autenticação de informação electrónica através da encriptação. Ou seja, a encriptação assimétrica possui duas chaves que possibilitam verificar se as mensagens são alteradas durante o seu envio, através da desencriptação (caso esta falhe, a mensagem foi modificada); a assinatura digital pretende certificar que a mensagem não foi alterada após a sua recepção e desencriptação.

A certificação da mensagem é realizada com base numa função de *hash* que cria um *checksum* da informação. O *checksum* é encriptado com a chave privada do emissor e o resultado desta operação (assinatura) é enviado junto com a mensagem original. Na recepção, o receptor executa a mesma função de *hash* sobre a informação obtendo um *checksum* da informação, desencripta o *checksum* (assinatura) que veio junto com a mensagem e compara os dois *checksum*'s. Se não coincidirem, então a mensagem foi modificada. A figura seguinte ilustra este processo:

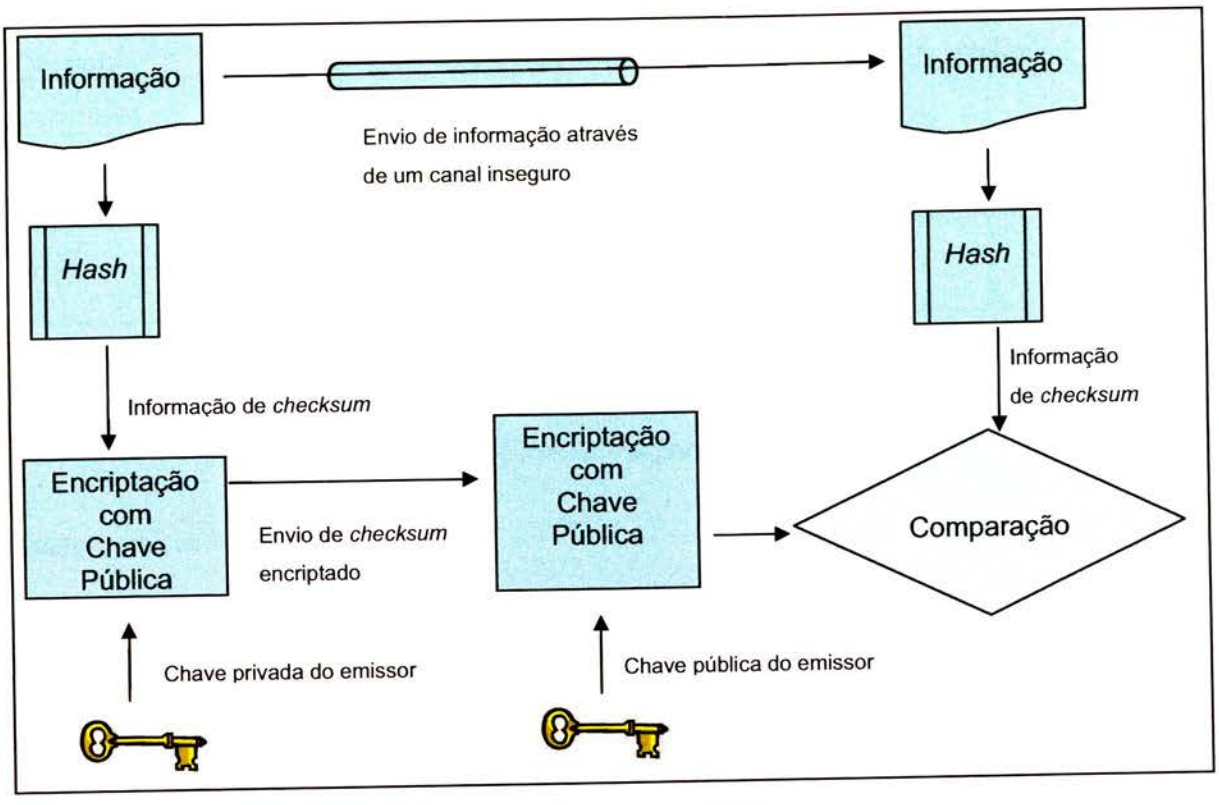


Figura 12: Assinatura digital

A segurança da assinatura digital depende de dois elementos críticos: a protecção da chave privada e a função segura de *hash* (os mais conhecidos são MD5 e SHA).

3.5 Ferramentas/Aplicações de segurança de redes

Esta secção pretende mostrar o resultado de um estudo de ferramentas de segurança de redes que permitiu reunir as ferramentas mais utilizadas na segurança de redes. As ferramentas encontram-se divididas em sete categorias, nomeadamente:

- Verificadores da integridade de ficheiros (*File Integrity Checkers*)
- Analisadores de tráfego (*Network sniffers*)
- Ferramentas para quebrar palavras-passe (*Password Crackers*)
- Ferramentas de rastreio e enumeração (*Network Scanners*)
- Ferramentas de avaliação de vulnerabilidades (*Vulnerability Assessment Tools*)
- Ferramentas de *war-dialing*
- Ferramentas para redes sem-fios (*Wireless Network Tools*)
- *Firewalls* pessoais

Verificadores da integridade de ficheiros

Ferramenta	Sítio *web*	Linux/Unix	Win32	Custo
Aide	http://sourceforge.net/projects/aide	✓		livre

Descrição	*AIDE (Advanced Intrusion Detection Environment) é um substituto do Tripwire.*			
LANGuard	http://www.gfi.com/languard/		✓	livre
Descrição	*É um utilitário que permite a detecção de intrusões através da verificação de ficheiros num sistema Windows 2000/NT.*			
Tripwire	http://www.tripwiresecurity.com/	✓	✓	livre (unix)
Descrição	*Monitoriza as alterações a ficheiros, verifica a sua integridade e notifica o administrador de violações da informação nas máquinas da rede.*			

Tabela 3: Verificadores de integridade de ficheiros

Analisadores de tráfego

Ferramenta	**Sítio *web***	**Linux/Unix**	**Win32**	**Custo**
Dsniff	http://www.monkey.org/~dugsong/dsniff/	✓		livre
Descrição	*Dsniff é uma colecção de ferramentas para auditoria de redes e testes de penetração. Dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf e webspy monitorizam passivamente a rede à procura de informação interessante (passwords, e-mails, ficheiros, etc.). Arpspoof, dnsspoof e macof facilitam a intercepção de tráfego de rede, normalmente indisponível ao atacante. Sshmitm e webmitm implementam ataques activos de "man-in-the-middle" contra sessões SSH e HTTPS através da exploração de falhas conhecidas.*			
Ethereal	http://www.ethereal.com	✓	✓	livre
Descrição	*É um analisador de protocolos de rede para Unix e Windows. Permite aos utilizadores examinar informação ao vivo de uma rede ou de um ficheiro de captura. É possível procurar de forma interactiva na informação capturada, ver informação resumida ou detalhada de cado pacote, e filtrar os pacotes visualizados.*			
Sniffit	http://reptile.rug.ac.be/~coder/sniffit/sniffit.html http://www.symbolic.it/Prodotti/sniffit.html (Windows)	✓	✓	livre
Descrição	*É um analizador de tráfego genérico para Linux, Unix e Windows.*			
Snort	http://www.snort.org/	✓	✓	livre
Descrição	*É um IDS e um analisador de tráfego genérico para Linux, Unix e Windows.*			
TCPDump	http://www-nrg.ee.lbl.gov/	✓		livre
Descrição	*É um analizador de tráfego genérico para Linux, Unix e Windows.*			
WinDump	http://windump.polito.it/		✓	livre
Descrição	*É um analizador de tráfego genérico para Windows baseado no TCPDump.*			
ettercap	http://ettercap.sourceforge.net/		✓	livre
Descrição	*É um conjunto de utilitários que permite a realização de ataques "man-in-the-middle" numa rede local. Com o ettercap é possível analisar ligações ao vivo, filtragem de conteúdos em tempo real e mais alguns truques. Suporta a disecção activa e passiva de vários protocolos, incluindo alguns cifrados.*			

Tabela 4: Analisadores de tráfego

Ferramentas para quebrar palavras-passe

Ferramenta	Sítio *web*	Linux/Unix	Win32	Custo
Crack 5	http://www.crypticide.com/users/alecm/	✓		livre
Descrição	*É um programa para adivinhar passwords, desenhado para localizar rapidamente falhas nos ficheiros de password do Unix através da análise dos conteúdos desses ficheiros. Por exemplo, utilizadores com passwords fracas.*			
John The Ripper	http://www.openwall.com/john/	✓	✓	livre
Descrição	*É um rápido quebrador de passwords, disponível em diversos sistemas operativos. O seu propósito principal é detectar passwords fracas em Unix, mas contém outros tipos de hash também.*			
L0pht Crack	http://www.securityfocus.com/tools/1005	✓	✓	€
Descrição	*É um utilitário para Windows NT, 2000 e XP que permite a quebra de passwords.*			

Tabela 5: Ferramentas de quebra de palavras-passe

Ferramentas de avaliação de vulnerabilidades

Ferramenta	Sítio *web*	Linux/Unix	Win32	Custo
CyberCop Scanner	http://www.securityfocus.com/products/126		✓	€
Descrição	*É uma ferramenta de rede que analisa as vulnerabilidades e detecta falhas de segurança nos dispositivos da rede.*			
ISS Internet Scanner	http://www.iss.net/		✓	€
Descrição	*É uma ferramenta de rede que analisa as vulnerabilidades e detecta falhas de segurança nos dispositivos da rede.*			
Nessus	http://www.nessus.org/	✓		livre
Descrição	*É uma ferramenta de rede que analisa as vulnerabilidades e detecta falhas de segurança nos dispositivos da rede.*			
SARA	http://www-arc.com/sara/	✓		livre
Descrição	*É uma ferramenta de rede que analisa as vulnerabilidades e detecta falhas de segurança nos dispositivos da rede.*			
SATAN	http://www.fish.com/satan/	✓	✓	livre
Descrição	*É uma ferramenta que ajuda aos administradores de sistemas. Reconhece diversos problemas de segurança de redes e cria relatórios dos problemas sem os explorar.*			
Retina Network Security Scanner	http://www.eeye.com/html/products/retina/index.html		✓	€

Descrição	*É uma ferramenta de avaliação de vulnerabilidades. Possui uma base de dados de vulnerabilidades para diversos sistemas.*

Tabela 6: Avaliação de vulnerabilidades

Ferramentas de war-dialing

Ferramenta	Sítio *web*	Linux/Unix	Win32	Custo
PhoneSweep	http://www.sandstorm.net/		✓	€
Descrição	*É uma aplicação comercial de "war-dialing" que suporta múltiplos modems e realiza tentativas automatizadas de penetração.*			
THC	http://www.thc.org/releases.php		✓	livre
Descrição	*É uma aplicação de "war-dialing" baseada em DOS.*			

Tabela 7: *War-dialing*

Ferramentas para redes sem fios (wireless)

Ferramenta	Sítio *web*	Linux/Unix	Win32	Custo
Aerosol	http://www.crypticide.com/users/alecm/		✓	livre
Descrição	*É um analisador de tráfego de redes sem fiso, que consegue quebrar as chaves WEP de encriptação. Monitoriza passivamente as transmissões, computando a chave de encriptação quando tiver obtido o número suficiente de pacotes.*			
AirSnort	http://airsnort.shmoo.com	✓		livre
Descrição	*É um analisador de tráfego de redes sem fiso, que recupera as chaves de encriptação. O AirSnort monitoriza passivamente as transmissões, computando a chave de encriptação quando tiver obtido o número suficiente de pacotes.*			
Kismet	http://www.kismetwireless.net	✓		livre
Descrição	*É um analisador de tráfego de redes sem fiso. Suporta quase todas as cartas sem fios em Linux.*			
NetStumbler	http://www.netstumbler.com		✓	livre
Descrição	*É uma ferramenta 802.11b que detecta redes disponíveis e regista toda a informação sobre o ponto de acesso.*			
WaveStumbler	http://www.cqure.net/tools.jsp?id=08	✓		livre
Descrição	*É uma ferramenta de consola que permite mapear a rede. Lista as características básicas da rede sem fios como o canal, WEP, ESSID, MAC, etc.*			

Tabela 8: Redes sem fios

Firewalls pessoais

Ferramenta	Sítio *web*	Linux/Unix	Win32	Custo
BlackIce	http://www.networkice.com		✓	€
McAfee Personal Firewall	http://www.mcafee.com		✓	€
Norton Personal Firewall	http://www.symantec.com		✓	€
Tiny Firewall	http://www.tinysoftware.com		✓	livre (até à v3.0)
Kaspersky Anti-Hacker	http://www.kaspersky.com/antihacker		✓	€

Tabela 9: *Firewalls* pessoais

3.6 Situação actual e evolução futura

Esta secção pretende demonstrar a situação actual e a evolução do estado da segurança informática. Serão apresentados dados sobre incidentes ocorridos deste 1990, vulnerabilidades conhecidas desde 1995, os ataques ocorridos em 2003 e os problemáticos vírus. Indicar-se-á também as tecnologias implementadas pelas organizações na prevenção e combate dos ataques, bem como, qual o factor que mais inviabiliza a aposta na segurança.

Incidentes

A evolução do número de incidentes reportados salienta uma crescente preocupação para com a segurança informática. Segundo o CERT, a difusão e o aumento do número de ferramentas de ataque propicia o crescimento verificado no gráfico seguinte:

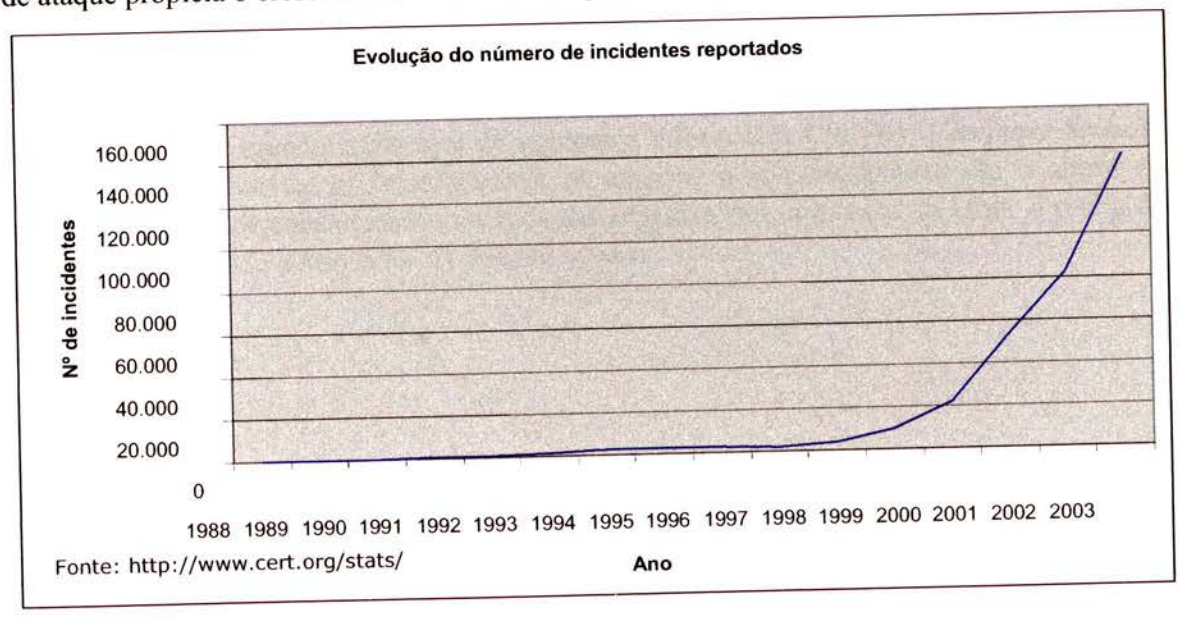


Figura 13: Evolução do número de incidentes

Nota: Um incidente pode envolver um sítio *web* ou centenas (até milhares) de sítios *web*. Alguns incidentes podem envolver uma actividade de longa duração.

Vulnerabilidades

O número de incidentes pode ser directamente associado ao número de vulnerabilidades. Conhecendo o progesso das vulnerabilidades reportadas é possível constatar a evolução da preocupação pela segurança. Os sistemas desenvolvidos estão mais seguros e mais atentos às falhas. O seguinte gráfico é a prova deste facto:

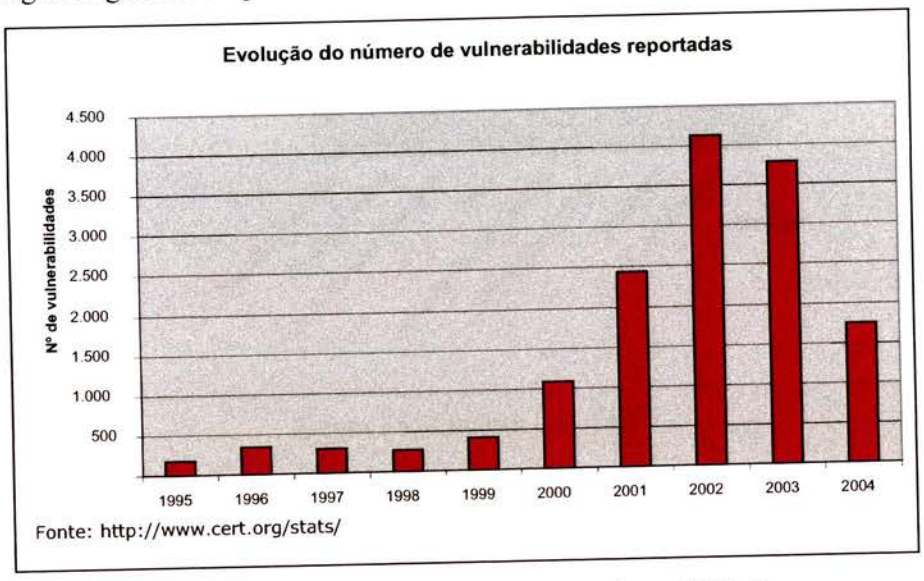


Figura 14: Evolução do número de vulnerabilidades

Nota: O número de vulnerabilidades no ano de 2004 é referente aos dois primeiros trimestres desse ano.

Ataques

O gráfico apresentado abaixo revela quais os ataques com que as organizações se depararam no ano de 2003. Segundo o instituto de segurança informática CSI/FBI (*Computer Security Institute/Federal Bureau of Investigation*), os ataques mais preocupantes são o abuso da Internet por parte de colaboradores internos das organizações, a difusão de vírus, o roubo de portátis e acessos não autorizados de pessoal interno:

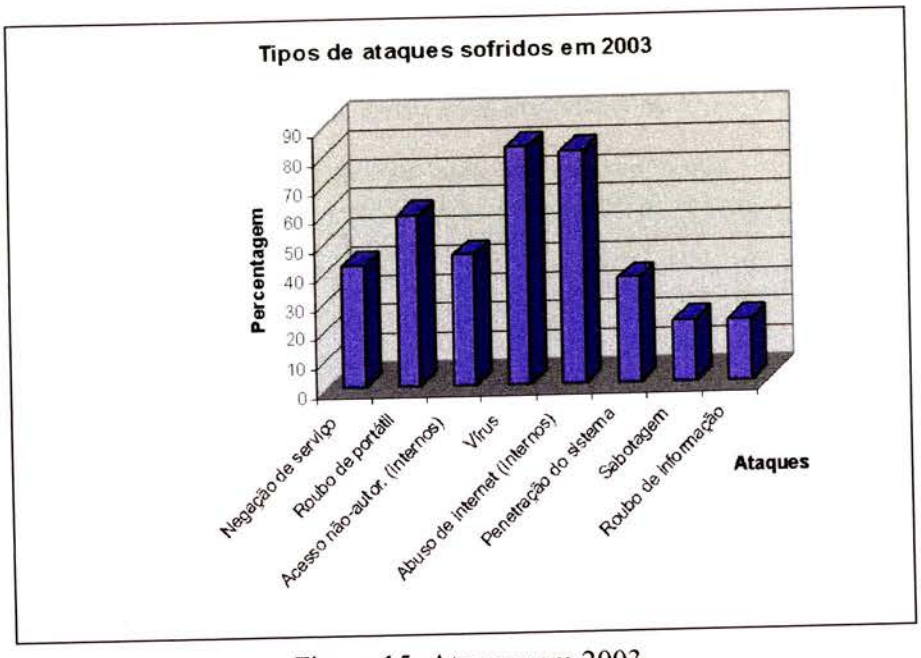


Figura 15: Ataques em 2003

A informação presente no gráfico anterior foi retirada do inquérito, conduzido pelo CSI com a participação do esquadrão de intrusões informáticas do FBI, "*2003 CSI/FBI Computer Crime and Security Survey (21 pages)*"[12].

Vírus

A razão pela qual o antivírus é a tecnologia mais utilizada encontra-se explicada pelo seguinte gráfico:

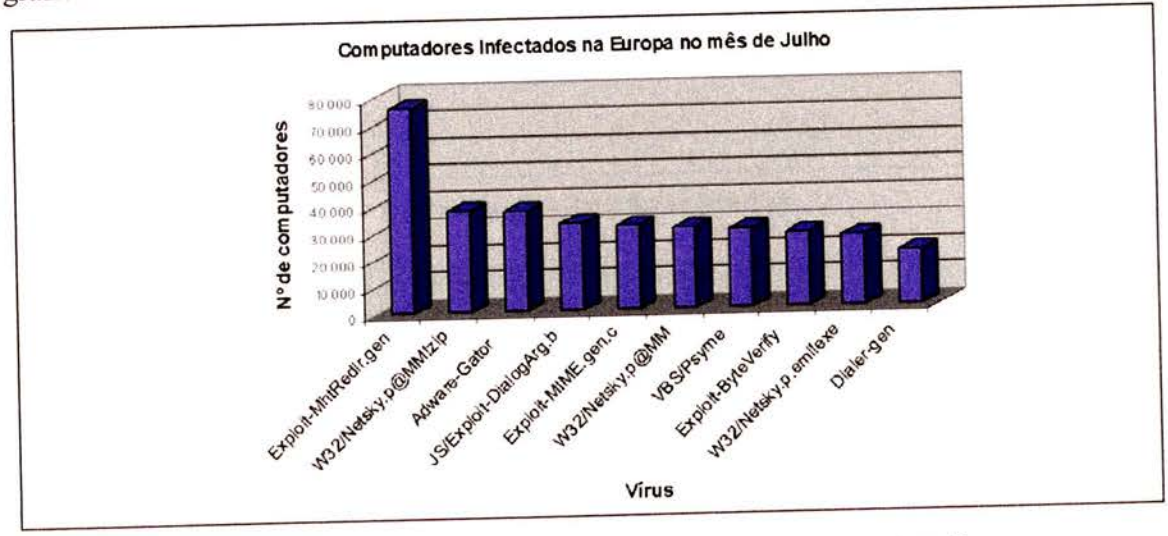


Figura 16: Computadores infectados na Europa no mês de Julho

Esta estatística retirada do sítio *web* da McAfee[13] revela o número de computadores infectados na Europa durante o mês de Julho e quais os vírus causadores da infecção.

[12] http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

[13] http://vil.mcafee.com/mast/viruses_by_continent.asp?continent_k=3&track_by=2&period_id=3

Com a crescente utilização do correio electrónico, a difusão de vírus é extremamente rápida. O gráfico seguinte é um exemplo da rapidez com que o *worm "Code Red"* se difundiu pela Internet, provocando graves prejuízos em diversas organizações.

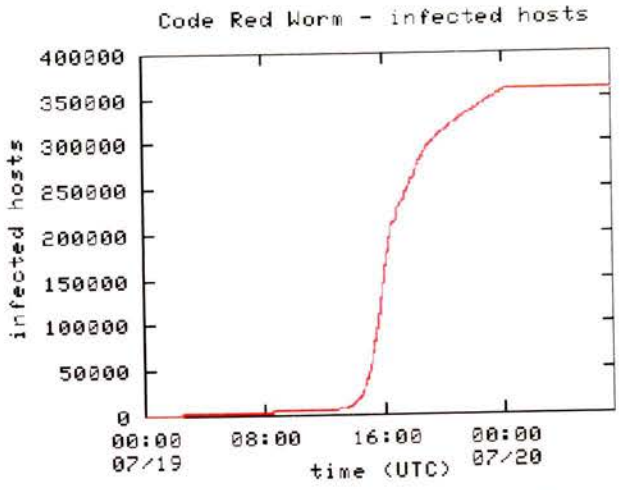


Figura 17: Computadores infectados pelo *Code Red*

Este gráfico foi retirado do sítio *web*:

http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml

Tecnologias

A empresa de consultoria Deloitte ToucheTohmatsu revelou um estudo denominado "*2003 Global Security Survey*", do qual se concluíu quais as tecnologias mais utilizadas pelas organizações, no combate aos ataques e na diminuição do prejuízo dos estragos causados. O gráfico abaixo revela que as principais tecnologias são: antivírus, VPN, IDS, filtragem de conteúdos e encriptação.

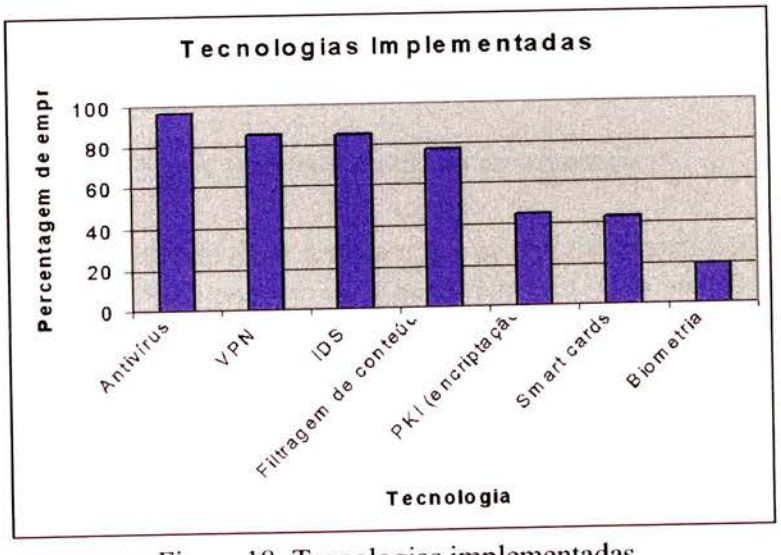


Figura 18: Tecnologias implementadas

Inviabilização da segurança

A revista "Information Security Magazine" do mês de Julho de 1999, publicou um artigo, com o resultado de um inquérito, cujo título "Top Obstacle is Budget: What is the SINGLE greatest obstacle to achieving adequate info security at your organization?"[14], ou seja, "Maior obstáculo é o orçamento: Qual é o maior obstáculo que impede as organizações de conseguir uma segurança de informação adequada?".

Um dos resultados deste artigo-inquérito é o gráfico seguinte, donde se conclui que para quase 30% das organizações inquiridas, o grande obstáculo é o orçamento:

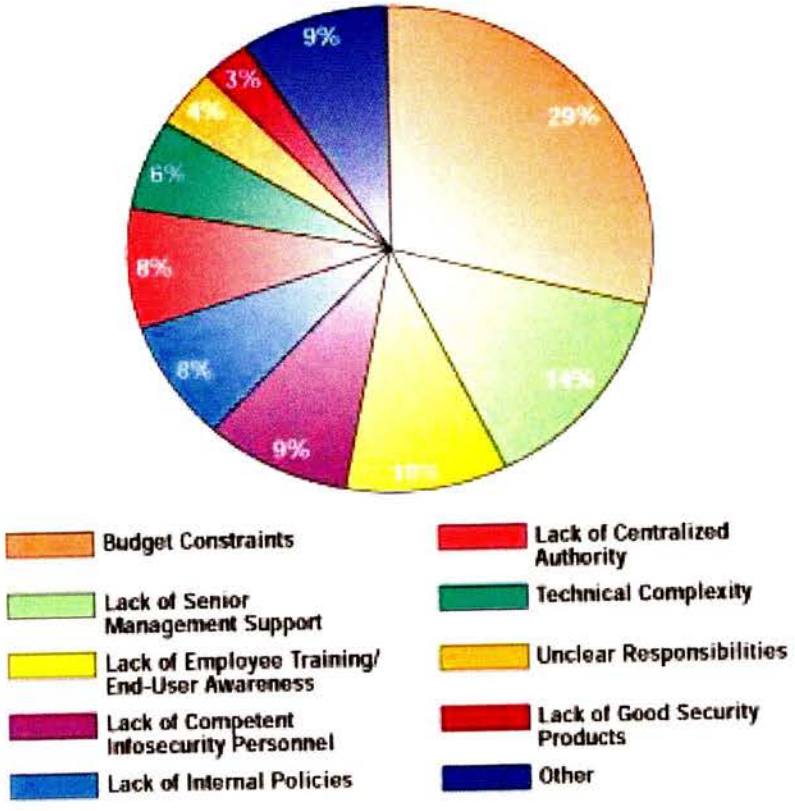


Figura 19: Maior obstáculo da segurança

A questão associada ao resultado deste gráfico e que as próprias organizações devem fazer a si próprias é: "*E de quanto é o prejuízo da organização caso haja uma falha de segurança grave?*"

3.7 Resultado

A situação actual da segurança encontra-se numa fase de sensibilização e amadurecimento. Por um lado, o número de incidentes reportados subiram de forma exponencial desde 1998,

[14] http://infosecuritymag.techtarget.com/articles/1999/enough.shtml

tendo sido sempre acompanhados pela criação e evolução das tecnologias; por outro, os investimentos realizados nesta área não são, muitas vezes, correctamente ponderados.

No que diz respeito ao futuro, com o tempo as tecnologias de segurança vão evoluindo e desenvolvendo-se com o propósito de tornar os negócios e as comunicações mais seguras.

Simultaneamente, as falhas de segurança permitem aumentar a segurança das redes. Se as empresas acompanharem as tecnologias de segurança, bem como, ameaças e perigos mais recentes, o benefício das redes evoluirá sem riscos.

4 Implementação e segurança de redes

O projecto de estágio abrangeu a implementação de uma rede de dados descrita nesta secção, bem como a sua gestão. Esta rede foi concebida para suportar serviços informáticos durante a realização de um evento. Por motivos de contrato de confidencialidade entre a Siemens e o cliente, a rede de dados em causa será referida como "Projecto Azores".

4.1 Diagnóstico do ponto de situação inicial do projecto

A implementação da rede foi realizada após a instalação de todo o equipamento passivo nas diversas localizações do projecto.

O processo de concepção do projecto não foi da responsabilidade da Siemens, sendo esta entidade apenas responsável pela implementação de equipamento activo pré-escolhido, pelo cliente, e pela gestão da rede local nos diversos sítios do projecto. A gestão centralizada foi efectuada pelo cliente.

Desta forma, o objectivo da Siemens restringiu-se à identificação, de acordo as necessidades, das localizações dos equipamentos activos, bem como, instalar, configurar e gerir as diversas redes locais durante a realização do evento. No anexo C, é possível encontrar exemplo de configurações do equipamento de um dos sítios.

4.2 Descrição da rede de dados

Com já foi referido, a rede de dados foi concebida no âmbito da realização de um evento com a finalidade de prestar serviços de comunicação para suporte a serviços informáticos.

O evento foi realizado em diversas localizações, que serão designadas neste documento por sítios (*sites*). Os sítios estão interligados entre si por uma rede IP. A figura 20 pretende apresentar uma visualização gráfica de alto nível das interligações lógicas entre os sítios:

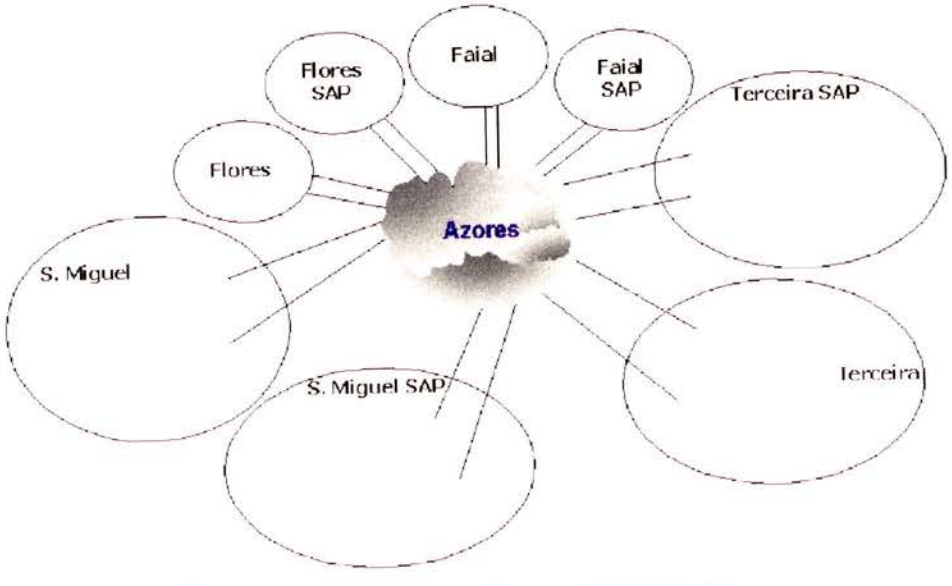


Figura 20: Rede lógica WAN do projecto Azores

A organização do evento encontra-se num local não descrito neste documento por não estar no âmbito de intervenção da Siemens.

Os utilizadores desta rede foram divididos em cinco grupos:

- Meios de comunicação social (*Media*): os utilizadores deste grupo necessitam de acesso às suas organizações através da *Internet* para colocação de notícias *online*, transferência de dados volumosos e visualização de correio electrónico.
- Organização (*Staff*): a organização carece de comunicação entre edifícios para acesso remoto a servidores de facturação, acreditação, documentos e domínio; requer ainda ligação à *Internet* para actualização do seu sítio *web online*, acesso ao correio electrónico, transferência de dados e comunicação com outros países europeus.
- Bilheteiras (*SAP/RAC*): estes utilizadores precisam de acesso a servidores dedicados alojados no sítio central da organização do evento.
- Convidados (*Guests*): este grupo apenas necessita de acesso à *Internet* para visualização de páginas *web*.
- Gestores da rede: os utilizadores que compõem este grupo necessitam de acesso a toda a rede do sítio que estão a gerir, bem como, de acesso à *Internet* para visualização de correio electrónico e visualização de sítios *web* dos fabricantes do equipamento de rede utilizado durante o evento.

O número de utilizadores por sítio (por edifício e por sala) foi fornecido pela organização do evento, a partir do qual foram alocados os equipamentos necessários.

Realizada a atribuição de gamas de endereços IP a cada um dos sítios e a alocação dos equipamentos activos, estes últimos foram instalados e configurados localmente. Durante a instalação, foi criado um documento para controlo e com o registo dos dados mais relevantes dos equipamentos. O documento pode ser visualizado na figura seguinte:

Inventário do equipamento

Local	Equipamento	Descrição	Serial	MAC	IP Gestão/Rede	Nome	Software	Obs.
S.Miguel	Cisco Router 2600		JMX0814L3Z3		172.28.254.24		12.2(15)T11tc2	1 WIC 2-T (avariado)
	Cisco Router 2600		JMX0820L2CL		172.28.254.24		12.2(15)T11tc2	1 WIC 2-T
	Cisco Router 2600		JMX0814L2C9		172.28.254.25		12.2(15)T11tc2	1 WIC 2-T e 1 PRI
1	Catalyst 3550	WS-C3350-12G	CAT0802X2X0	000ED7FAFA80	172.28.254.97	SMiguelC3550	12.1(19)EA1c	
1P1 (3)	Catalyst 2950 12p	WS-C2950G-12-EI	FHK0810Z13H	000F8F1C75C0	172.28.254.104	SMiguel-Sw2-piso1-3p1	12.1(19)EA1c	
Spare (1P1)	Catalyst 2950 12p	WS-C2950G-12-EI	FHK0810Y19W	000F24DC7AC0				velo de Terceira
Bilheteiras	Catalyst 2950 12p	WS-C2950G-12-EI	FHK0812Z1P3	000F8FD4B980	172.28.254.105			
1A1 (1)	Catalyst 2950 24p	WS-C2950G-24-EI	FOC0809X240	000F34ED2640	172.28.254.98	SMiguel-Sw1-piso1-1a1	12.1(19)EA1c	
1A1 (2)	Catalyst 2950 24p	WS-C2950G-24-EI	FOC0809X23W	000F34ED5400	172.28.254.99	SMiguel-Sw2-piso1-1a1	12.1(19)EA1c	
3P2	Catalyst 2950 48p	WS-C2950G-48-EI	FOC0810X1Q4	000F8F3D9A80	172.28.254.101	SMiguel-Sw2-piso3-3p2	12.1(19)EA1c	
3P1	Catalyst 2950 48p	WS-C2950G-48-EI	FOC0810W229	000F8F47AE40	172.28.254.100	SMiguel-Sw1-piso3-3p1	12.1(19)EA1c	
1P1 (1)	Catalyst 2950 48p	WS-C2950G-48-EI	FOC0810W1SR	000F8F300840	172.28.254.102	SMiguel-Sw1-piso1-1p1	12.1(19)EA1c	
1P1 (2)	Catalyst 2950 48p	WS-C2950G-48-EI	FOC0810W1SM	000F8F300580	172.28.254.103	SMiguel-Sw2-piso1-1p1	12.1(19)EA1c	
	GBIC 1000Base-LX	WS-G5486						Qtds: 8+2 (terceira)
	GigaStack GBIC	WS-X3500-XL						Qtds: 7 (usaram 5)
	RPS AC Power Supply Cisco 3745	PWR600-AC-RPS	ZDGN8014					
	RPS AC Power Supply Cisco 3745	PWR600-AC-RPS	ZDGN8019					
	WIC-2T (2-Port Serial WAN Interface Card Rpcm)							WIC-1T
SAP/RAC	Cisco Router 1760		FCZ0820112A		10.1.61.253			WIC-1T e 1 BRI
SAP/RAC	Cisco Router 1760		FCZ0820112U		10.1.61.252	Backup		
SAP/RAC	Catalyst 2950 24p (1)	WS-C2950G-24-EI	FOC0815W3T3	000FF75AAA00	172.28.253.148			
SAP/RAC	Catalyst 2950 24p (2)	WS-C2950G-24-EI	FOC0815X3Q1	000FF75AAA40	172.28.253.149			
ToDo						Está pronto! Tudo OK!		
						Falta configurar, trocar nº de série, etc.!		
						Em falta!		

Figura 21: Inventário de equipamento

Após a instalação e configuração dos equipamentos foram desenhados os mapas de rede de cada sítio. O exemplo que se segue é referente ao sítio "S. Miguel":

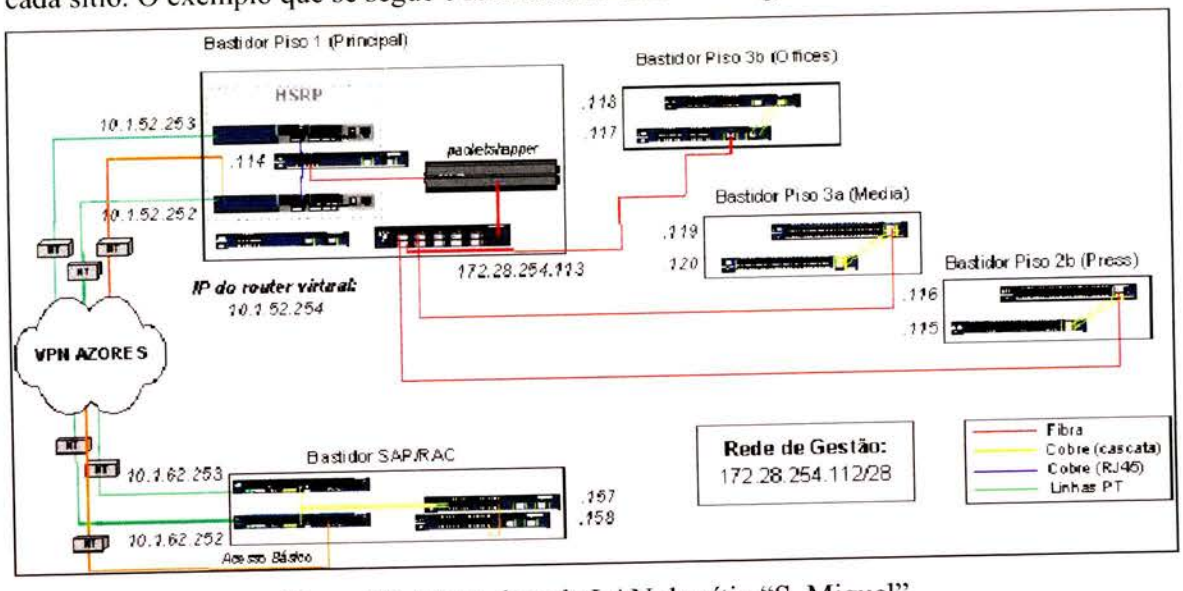


Figura 22: Mapa de rede LAN do sítio "S. Miguel"

A rede de cada sítio encontrava-se dividida em duas zonas: a SAP/RAC (área de acreditação) e a rede local do edifício. Ambas as zonas possuem ligação à VPN Azores que serve de ponto de reunião de todos os sítios do projecto.

Cada zona possui dois *routers*[15] ligados entre si através de um *switch*[16] e em redundância, utilizando o protocolo *HSRP* (proprietário da Cisco[17]). Este protocolo permite que exista apenas um endereço IP associado aos dois *routers*, embora o endereço IP de gestão para cada *router* seja diferente.

A cada *router* estão ligados 2 circuitos de 2 Mbps cada e um acesso primário ligado ao *router* de apoio (*backup*). Os *routers* têm ainda o protocolo de encaminhamento de rotas BGP activo, *traps*[18] de SNMP e sincronização de relógio através do protocolo NTP.

No caso da rede SAP/RAC, ao *switch* referido é ligado mais um *switch*, em cascata, onde se ligam os computadores que têm acesso à rede e à *Internet*.

A rede local possui ainda um *Packet Shaper* ligado entre o *switch* de interligação dos *routers* e o *router-switch* de núcleo (*core*), o Cisco 3550.

O *router-switch* Cisco 3550 interliga, por fibra, todos os *switches* distribuídos pelas salas do edifício. Existem salas com mais do que um *switch* e, neste caso, estes estão ligados em cascata.

A rede encontra-se dividida em cinco VLAN's, como está expresso na seguinte tabela:

[15] *Router* é um dispositivo de rede que permite o encaminhamento pacotes IP entre redes distinctas.

[16] *Switch* é um dispositivo de rede que permite a entrega de tramas Ethernet entre os computadores ligados.

[17] http://www.cisco.com

[18] *Trap* é um sinal que é enviado quando ocorre algum evento específico.

VLAN ID	Nome	IP
1	Gestão	172.28.254.x/28
2	Staff	10.1.5y.0
3	Press	10.1.7y.0
4	Guests	10.1.8y.0
99	Other	*«sem endereço»*

Tabela 10: VLAN's

O encaminhamento entre as VLAN's e a *Internet* é realizado pelo Cisco 3550. No entanto, o encaminhamento entre VLAN's está impedido, por motivos de segurança, recorrendo à criação de ACL's[19] no C3550.

Os computadores que se ligam à rede, recebem as suas configurações de rede de forma dinâmica, ou seja, através de DHCP e de acordo com a configuração do porto do *switch* onde estão fisicamente ligados. O serviço de DHCP era fornecido pelo C3550, no qual estão reservados endereços IP reservados para dispositivos específicos da rede (por exemplo, impressoras) e como tal, excluíndo-os das gamas de endereços IP a atribuir.

A VPN IP disponibiliza um servidor de correio electrónico que oferece POP3 e SMTP, um servidor NTP, uma estação de gestão SNMP centralizada e um servidor de registos (*syslog*).

4.3 Equipamentos

Os equipamentos activos instalados em cada sítio são:

- Cisco Router 1760 e Cisco Router 2600: Ambos equipamentos são *routers*, ou seja, encaminhadores de pacotes IP. A diferença entre estes dois modelos reside no facto do 1760 ser um *router* de acesso, enquanto que o 2600 é um *router* de acesso multiplataforma, tendo portanto mais capacidade de processamento, funcionalidades e suporte a diversas plataformas.
- Cisco Catalyst 3550: O modelo utilizado neste projecto possui 10 portos *GigabitEthernet* (1000 Mbps) para ligações em fibra óptica e mais 2 portos *GigabitEthernet* para ligações em cobre (terminações RJ-45). Trata-se de um *switch* de nível 3, ou seja, possui a capacidade de encaminhamento de pacotes IP. Este *switch* permite ainda outras funcionalidades dependendo da versão de IOS[20] instalada, tais como, servidor de DHCP, de Web, IDS, etc.
- Cisco Catalyst 2950 (12p, 24p, 48p): O Catalyst 2950 é um *switch* que suporta desde 12 a 48 portos *FastEthernet* (100 Mbps), possui 2 portos *GigabitEthernet* para ligações ópticas ou de cascata, permitindo assim obter-se uma pilha de *switch* em cascata.

[19] ACL é uma lista que permite filtrar tráfego.

[20] IOS é um sistema operativo proprietário da Cisco.

- PacketShaper: O *PacketShaper* é um produto da Packeteer[21]. Trata-se de um dispositivo aplicacional de gestão de tráfego que fornece controlo na gestão da largura de banda, assim como visibilidade ao nível 7 (camada de apresentação do modelo OSI), de forma a assegurar qualidade de serviço da rede e desempenho aplicacional. A tecnologia de modulação do tráfego ("*traffic shaping*") do *PacketShaper* permite corrigir problemas de desempenho ao nível da WAN e da Internet. O *PacketShaper* permite assegurar verdadeira qualidade de serviço para aplicações de missão crítica, como voz e vídeo, por exemplo. O *PacketShaper* é utilizado, nesta rede, para análise e modulação de tráfego.

4.4 Rede sem-fios

Durante a realização do evento é disponibilizado acesso à Internet através de uma rede sem fios instalada em cada sítio.

Esta rede permite acesso à Internet através da compra do acesso, composto por uma identificação do utilizador (*login*), uma palavra-passe (*password*) e um tempo de permanência na rede.

Quando o utilizador abre a sua primeira página *web*, o navegador *web* é automaticamente redireccionado para o sistema de autenticação da rede, no qual tem de introduzir o seu *login* e a sua palavra-passe. Após a autenticação bem sucedida, o utilizador pode navegar na Internet durante o tempo contratado.

A rede sem fios é composta por diversos pontos de acesso (*access points*) que estão ligados a um *switch* principal com acesso à Internet através de um *router*.

4.5 Aplicações de gestão da rede

Toda a gestão da rede está apoiada nos protocolos: SNMPv2, SSHv1 e HTTPS.

No acesso aos equipamentos activos através de SNMPv2 são utilizadas três aplicações:

- *IPSwitch WhatsUp Gold*: O *WhatsUp Gold* é um produto da IPSwitch[22] e é uma solução simples de mapeamento de rede, monitorização, notificação e de relatório de desempenho que ajuda os administradores de rede a detectarem e resolverem rapidamente os problemas da rede. Assim que um dispositivo da rede deixar de obter conectividade, o *WhatsUp Gold* notifica o administrador constantemente, seja por correio electrónico ou por SMS[23]. Toda a gestão é realizada por SNMP.
- *Bandwidth Monitor*: É um utilitário desenvolvido por um colaborador da Siemens (Fernando Romão) e tem como funcionalidade a monitorização de tráfego nas diversas interfaces dos *routers* através de SNMP.
- *IP Account Alert*: Trata-se de um utilitário desenvolvido pelo estagiário com o objectivo de alertar para a elevada probabilidade de um cliente da rede estar infectado com vírus. Este objectivo é conseguido através da monitorização do tráfego nos

[21] http://www.packeteer.com

[22] http://www.ipswitch.com

[23] Short Message Service

routers, avaliando, para cada endereço IP, o número de endereços de destino a que está ligado ou tentou ligar-se e o número de pacotes enviados e/ou recebidos. É com base em padrões definidos segundo estas duas variáveis que a aplicação alerta o administrador que estiver a monitorizar a rede.

O acesso aos *routers* e *switches* para a realização de comandos, adição de *acess lists*, ou outras operações, é concretizado através de SSHv1 utilizando a aplicação *SSH Secure Shell*[24].

O protocolo HTTPS é utilizado pela aplicação *Microsoft*[25] *Internet Explorer* no acesso ao serviço *web* do *PacketShaper*, para consulta de informação sobre o estado do tráfego.

Como é possível verificar na figura seguinte, o ambiente de monitorização e gestão da rede é completo e permite uma resposta eficaz e eficiente aos problemas que possam surgir:

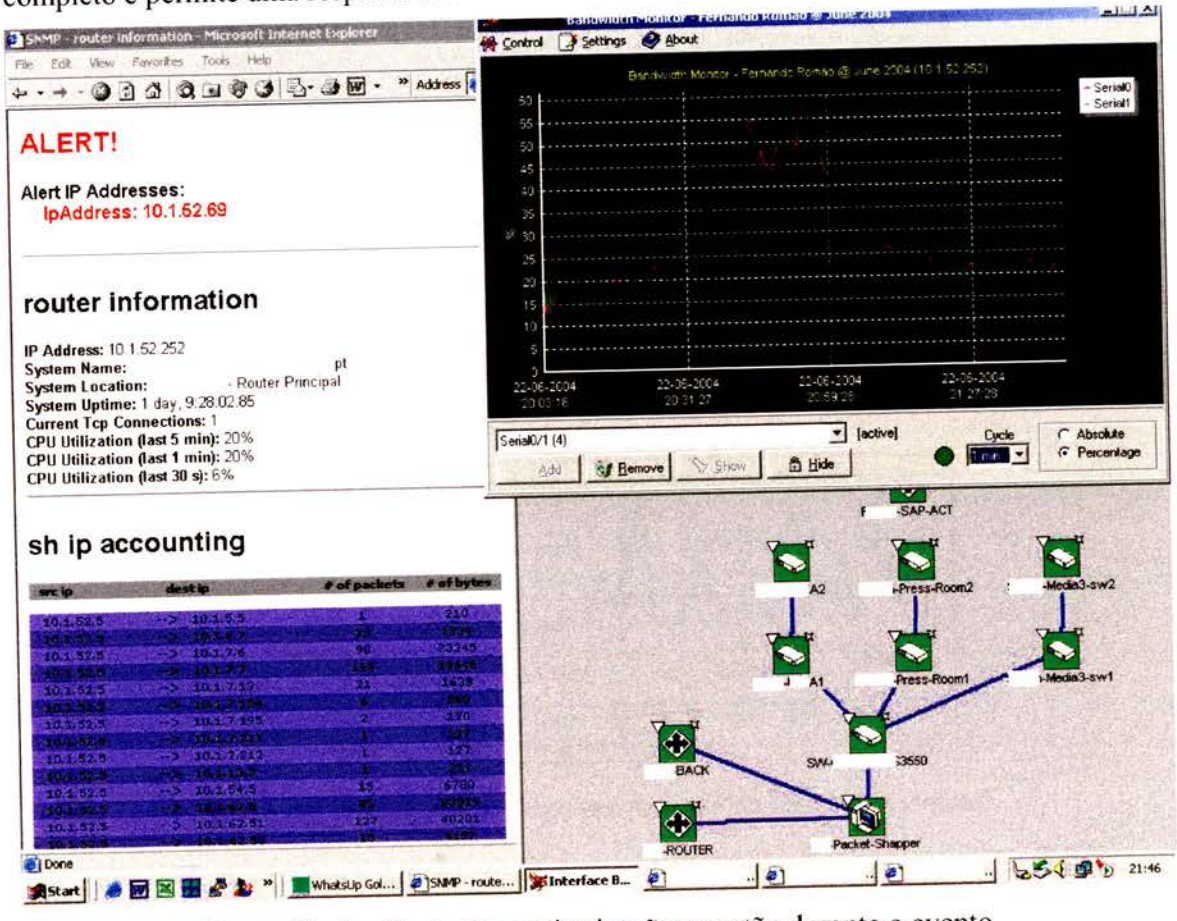


Figura 23: Ambiente de monitorização e gestão durante o evento.

A figura seguinte ilustra a aplicação *WhatsUp Gold* por completo:

[24] SSH Secure Shell é um produto da SSH Communications Security Corporation – http://www.ssh.com

[25] http://www.microsoft.com

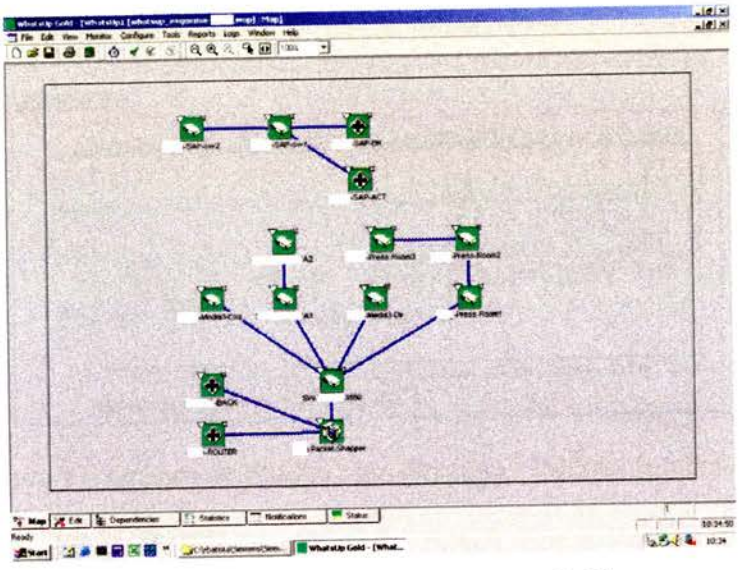


Figura 24: Aplicação *Whats Up Gold*

A consulta ao *PacketShaper* permite conhecer dados mais precisos sobre os fluxos de tráfego. As seguintes figuras mostram que tipo de tráfego que flui em direcção à Internet e à rede interna, bem como, quais os serviços mais utilizados na rede:

Inbound

Utilization

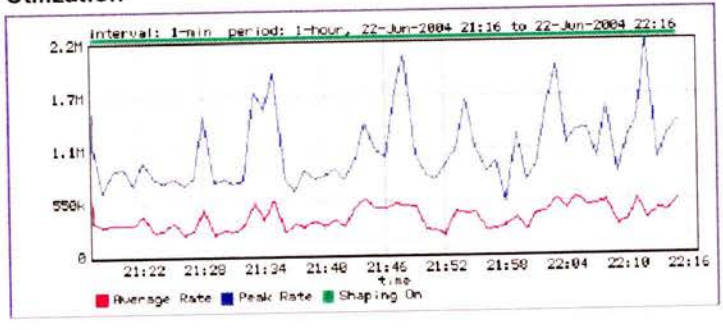
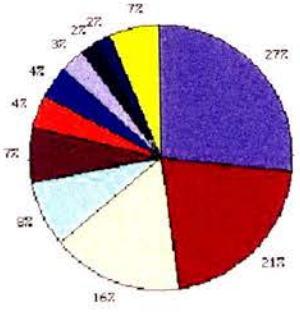


Figura 25: Gráfico de tráfego proveniente da Internet (*inbound*)

Top 10 Classes



Class Name	Average Rate (bps)	(%)
1. /Inbound/Local/Net_10_1_82_0/HTTP	106k	27
2. /Inbound/Local/Net_10_1_52_0/HTTP	81k	21
3. /Inbound/Local/Net_10_1_72_0/HTTP	60k	16
4. /Inbound/Local/Net_10_1_52_0/SNMP	29k	8
5. /Inbound/National/DC_Lisbon/DCOM	25k	7
6. /Inbound/Local/Net_10_1_82_0/Default	14k	4
7. /Inbound/Local/Net_10_1_82_0/FTP	13k	4
8. /Inbound/National/DC_Lisbon/Default	12k	3
9. /Inb...tional/DC_Lisbon/Microsoft-ds	8618	2
10. /Inbound/Local/Net_10_1_72_0/Default	7208	2
All other classes	25k	7

period: 1-hour, 22-Jun-2004 21:16 to 22-Jun-2004 22:16

Figura 26: Serviços mais utilizados a partir da Internet (*inbound*)

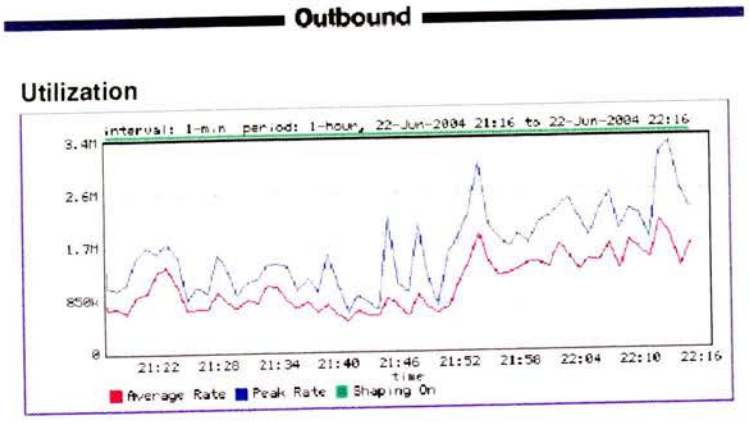


Figura 27: Gráfico de tráfego com direcção à Internet (*outbound*)

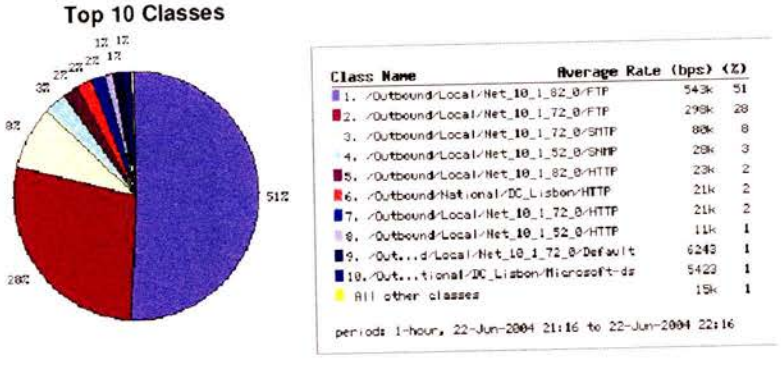


Figura 28: Serviços mais utilizados para a Internet (*outbound*)

4.6 Aplicação "*IP Account Alert*"

IP Account Alert é uma ferramenta que foi desenvolvida durante a realização do evento e nasceu com o objectivo de facilitar a detecção de vírus na rede local de cada sítio, através da identificação de estações com comportamento anormal. Trata-se de uma ferramenta baseada na arquitectura cliente-servidor, tal como figura a imagem seguinte:

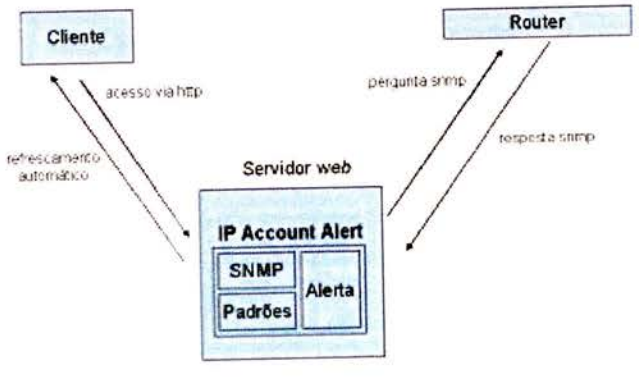


Figura 29: *IP Account Alert* – Arquitectura cliente-servidor

Antes da existência desta ferramenta, a detecção de vírus na rede só era possível quando este se tinha alastrado e causado problemas na interface externa do *router* com ligação à Internet (na realidade, à VPN), deixando a rede local muito lenta. Posteriormente, foi activado o "*IP Accounting*" nos *routers*, permitindo aos gestores da rede a visualização "crua" das ligações

efectuadas por cada endereço IP da rede local e o número de pacotes enviados. No entanto, era preciso percorrer uma lista imensa de endereços e tentar detectar que determinado endereço IP já fez demasiadas ligações com o exterior. Observada esta dificuldade e falta de eficiência deste processo, o *IP Account Alert* foi desenvolvido.

Esta ferramenta executa perguntas via SNMP aos *routers*, retirando a tabela que antes era visualizada de forma crua. A tabela é organizada e analisada de acordo com padrões pré-definidos. O padrão e a regra mais comum é: se for detectado que determinado endereço IP contactou mais que 10 endereços IP e a média dos pacotes enviados for menor ou igual a 5, então, provavelmente, esse cliente tem vírus.

Em conformidade com a análise, o *IP Account Alert* salienta o endereço IP infectado e mostra a tabela completa organizada por endereços IP de origem.

Este funcionamento interno pode ser visualizado na seguinte figura que descreve a arquitectura interna da aplicação:

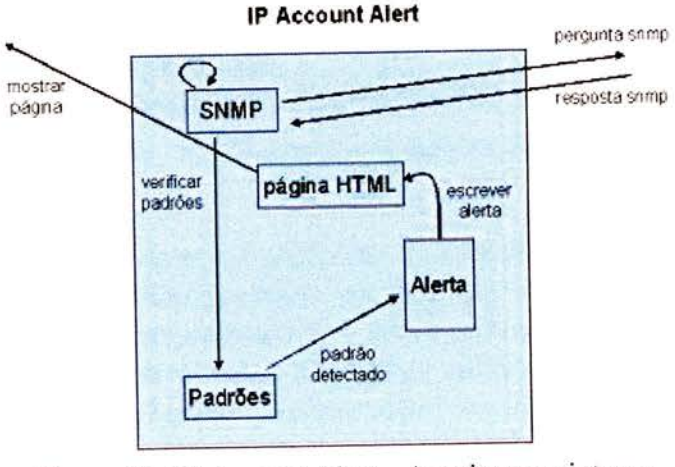


Figura 30: *IP Account Alert* – Arquitectura interna

As figuras seguintes mostram a interface gráfica desenvolvida para esta ferramenta. Nestas figuras é possível ver-se um exemplo de um alerta e da detecção de um endereço IP com vírus:

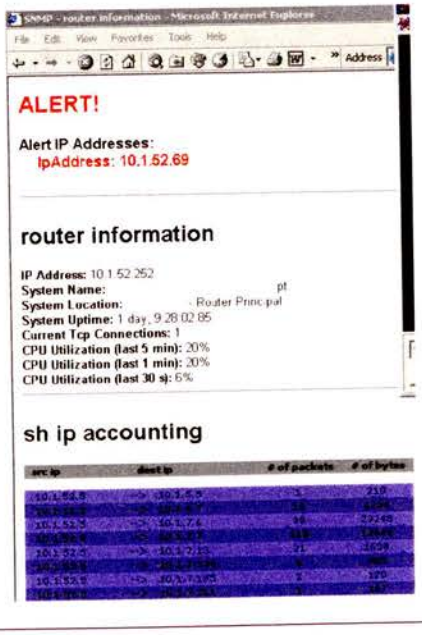


Figura 31: *IP Account Alert* – Alerta para o endereço IP infectado

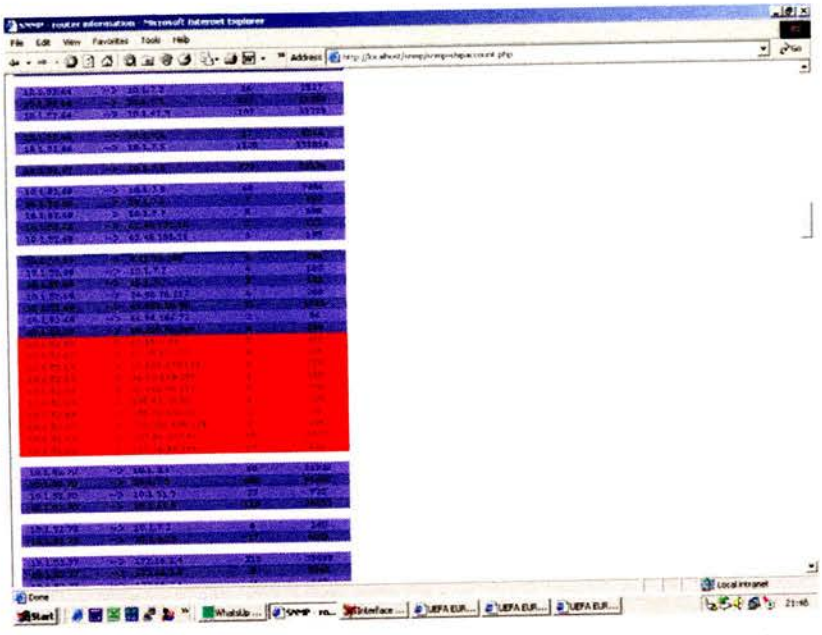


Figura 32: *IP Account Alert* – Organização e endereços contactados pelo endereço IP infectado

Assim que a ferramenta reportasse os endereços IP infectados, eram tomadas medidas de combate ao vírus. Essas medidas passavam por adicionar o endereço MAC associado ao endereço IP numa lista de endereços MAC bloqueados ao *switch* onde o cliente estava ligado e solicitando ao grupo responsável pelos sistemas de informação, uma intervenção junto do utilizador para que o vírus fosse removido com a maior brevidade possível.

O *IP Account Alert* foi desenvolvido em PHP, sendo necessário, para a sua instalação:

- Servidor *web* com suporte PHP
- MIB's de SNMP (*Management Information Base*)
- Pacote NET-SNMP[26]

O ambiente de desenvolvimento foi um Pentium II a 366 Mhz com 196 MB RAM, utilizando o sistema operativo "*Microsoft Windows 2000 Professional*", o servidor *web* "*Apache for Windows*", PHP 4.2.2 e o pacote NET-SNMP.

4.7 Segurança da rede

A segurança da rede implementada está assente em seis principais funcionalidades de segurança, das diversas que a Cisco possui:

- *Authentication, Authorization and Accounting* (AAA): AAA é, essencialmente, controlo de acessos. Ou seja, controlar quem tem acesso ao equipamento, que nível de acesso e que serviços pode usufruir. AAA é a arquitectura estrutural para a configuração de três funções de segurança independentes de forma consistente:
    - Autenticação: permite identificar utilizadores.

[26] http://net-snmp.sourceforge.net/

- Autorização: é um método de controlo de acesso remoto que permite a verificação de privilégios que determinado utilizador possui.
- Controlo: é o registo da informação do utilizador, nomeadamente, a que serviços acedeu, quando é que entrou e saíu do sistema, etc.

Esta funcionalidade pode ser encontrada nas configurações dos equipamentos através do comando:

```
aaa new-model
```

- *Access Control Lists* (ACL): As listas de controlo de acesso permitem a filtragem simples de tráfego por parte do equipamento, possibilitando o controlo do tráfego (se são encaminhados ou não). Nos equipamentos são utilizados dois tipos de ACLs: *IP* e *Extended IP*. As primeiras são simplistas e, como tal, apenas filtram o tráfego com base no endereço IP. As segundas são complexas e permitem a filtragem por protocolo de transporte (TCP, UDP), por máquina ou rede (origem e destino) e por protocolo de aplicação (telnet, ssh, http, etc.). Esta funcionalidade pode ser encontrada nas configurações dos equipamentos através dos comandos-exemplo:

  ```
  access-list 20 permit 172.28.250.0 0.0.0.15
  ```
  e

  ```
  access-list 110 permit tcp host 172.28.250.5 any eq telnet
  ```

- *Intrusion Detection System* (IDS): O sistema de detecção de intrusões permite a inspecção dos pacotes IP à procura de ataques. O IDS da Cisco descobre tipos de ataques utilizando assinaturas. Esta funcionalidade pode ser encontrada nas configurações dos equipamentos através do comando:

  ```
  ip audit po max-events 100
  ```

- *Secure Shell* (SSH): Esta funcionalidade SSH consiste numa aplicação e num protocolo. A aplicação possui um servidor e um cliente. O protocolo tem como objectivo a encriptação do tráfego gerado pela e para a aplicação. O acesso ao equipamento é realizado através do protocolo SSHv1. Esta funcionalidade pode ser encontrada nas configurações dos equipamentos através dos comandos:

  ```
  ip ssh time-out 50
  ```
  e
  ```
  transport input ssh
  ```

- *Passwords and Privileges*: A utilização de palavras-passe e de privilégios é o nível de segurança mais simples para obter controlo de acessos ao terminal do equipamento. A criação de contas de utilizadores foi realizada durante a configuração do equipamento. Esta funcionalidade pode ser encontrada nas configurações dos equipamentos através dos comandos:

  ```
  enable secret «password»
  ```
  ,

  ```
  username «username» password «password»
  ```
  e

  ```
  password «password»
  ```

  A encriptação das palavras-chave encontra-se activa em todos os equipamentos. Para activar esta função, no segundo comando (*username*), utiliza-se:

  ```
  service password-encryption
  ```

- *Network Time Protocol* (NTP): Embora não tenha uma relação directa com segurança, este protocolo permite a sincronização dos relógios do equipamento, o que é fundamental numa análise forense após um ataque. Todos os equipamentos encontram-se sincronizados com um servidor existente na VPN Azores. Esta funcionalidade pode ser encontrada nas configurações dos equipamentos através dos comandos:

  `ntp server 172.28.254.88` ,

  `ntp source loopback0` e

  `ntp clock-period 17180951`

Além das funcionalidades activas, e para uma análise eficiente e eficaz de problemas, os *routers* e o C3550 possuem activo a emissão automática de registos de eventos (*logging*) para um servidor de *syslog* remoto.

5 Análise de segurança da rede

A análise de segurança da rede é a intercepção da avaliação do estado de arte da segurança e da implementação realizada durante o trabalho desenvolvido.

Analisar a segurança de uma rede não é uma tarefa fácil, pois exige muito cuidado no compromisso entre segurança, acessibilidade e custo. A figura seguinte demonstra graficamente como se relacionam estas três variáveis:

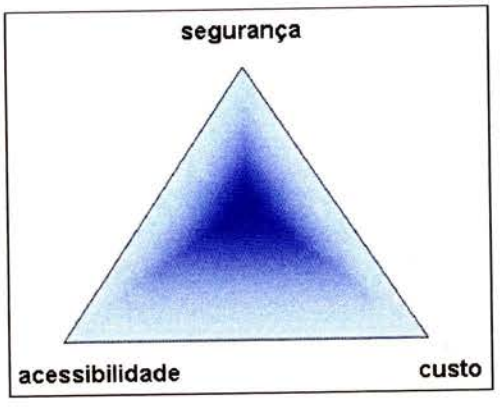


Figura 33: Compromisso entre segurança, acessibilidade e custo

A partir de uma observação atenta e cuidada, foi possível a detecção de alguns problemas na rede implementada.

Para uma exposição mais simples e clara, as falhas foram divididas em quatro níveis: infra-estrutura, equipamentos activos, servidores/impressoras e utilizadores.

5.1 Problemas ao nível da infra-estrutura

1. **Problema:** Energia.

   Descrição do problema: Cada *router* está ligado a uma RPS (*Redundancy Power Supply*) que possui duas fontes de alimentação. O problema reside no facto destas duas fontes estarem ligadas ao mesmo circuito de energia, o que implica, que em caso de corte de energia, o acesso à rede externa não é possível. Trata-se de um "ataque" de negação de serviço. Nenhum equipamento de rede está protegido com UPS.

   Solução: Utilizando as potencialidades de uma só RPS, é possível ligar os dois *routers* numa só e colocar uma UPS entre a RPS e dois circuitos de energia distinctos.

   Implicações: Planeamento e esforço financeiro.

   Aconteceu: Sim.

2. **Problema:** Ar condicionado.

   Descrição do problema: É possível encontrar bastidores em locais que não possuem as condições-ambiente necessárias ao bem-estar físico dos equipamentos, podendo resultar em sobreaquecimento do material e, por consequinte, negação de serviço e em equipamento danificado.

Alteração: Para evitar situações incómodas, dever-se-á proceder à instalação de ar condicionados nos locais onde se situam equipamentos de rede.

Implicações: Planeamento e esforço financeiro.

Aconteceu: Sim.

3. **Problema:** Posicionamento dos bastidores.

   Descrição do problema: A existência de bastidores em corredores onde passam, constantemente, pessoas é uma má política, por dois motivos: falta de ar condicionado e a acessibilidade aos equipamentos de rede. Este problema pode resultar em ataques à cablagem (corte de cabos) e aos equipamentos de rede (alteração das configurações ou roubo, por exemplo).

   Alteração: É aconselhável a deslocação destes bastidores para compartimentos adequados. No entanto, é importante salientar que a estadia do equipamento no edifício é temporária e como tal, o custo de criação de um compartimento para o efeito pode não ser justificável.

   Implicações: Planeamento e esforço financeiro.

   Aconteceu: Não.

5.2 Problemas ao nível do equipamento activo

4. **Problema:** IP Accounting.

   Descrição do problema: A detecção de ataques é efectuada através da activação da funcionalidade de "*accounting*" nos *routers*. O facto desta funcionalidade exigir muito processamento pode resultar na negação de serviço aquando da existência de vírus na rede ou da sua utilização massiva desta.

   Alteração: A colocação de um *proxy* (*squid*[27]) entre o *Packet Shaper* e o *Cisco Catalyst 3550* é recomendável. O *proxy* permitiria fazer o mesmo que a funcionalide de "*ip accounting*".

   Implicações: Planeamento, esforço financeiro e configurações.

   Aconteceu: Sim (*router* foi abaixo devido à sobrecarga de tráfego gerado por vírus).

5. **Problema:** Vírus.

   Descrição do problema: A existência de vírus na rede pode sobrecarregar a rede, concretizando-se uma negação de serviço.

   Alteração: A colocação de uma *firewall* de aplicação que filtre, por exemplo, pedidos HTTP, SMTP e FTP, diminuiria a probabilidade de intrusão de vírus na rede. Para diminuir ainda mais esta probabilidade, é aconselhável que a configuração dos

[27] http://www.squid-cache.org/

equipamentos de rede esteja segundo as normas SAFE. Por exemplo, os switches deveriam ser configurados de acordo com o documento: "*SAFE: Worm Mitigation*"[28].

Implicações: Planeamento, esforço financeiro e configurações.

Aconteceu: Sim (os *routers* pararam o seu processamento, devido à sobrecarga de tráfego gerado por vírus).

6. **Problema:** Gestão da rede.

   Descrição do problema: A gestão da rede foi realizada através da VLAN 1 (destinanda à gestão), recorrendo às tecnologias SSHv1, SNMPv2 e ACL's (o acesso aos equipamentos era filtrado por endereço IP). O uso da VLAN por defeito não é aconselhável; o uso de SSHv1 também não é recomendável pois existem aplicações que descodificam tráfego encriptado em SSHv1; e a utilização de SNMPv2 deixa a descoberto na rede todas as operações de gestão efectuadas (embora só tenha sido definido uma comunidade de leitura), pois não utiliza encriptação nem possui controlo de acessos. Deste modo, se, de algum modo, um atacante capturar o tráfego de rede vai apreender todos os dados importantes da rede, elevando o potencial de ataque.

   Alteração: Implementar SNMPv3; não utilizar a VLAN 1 para gestão; e implementar SSHv2.

   Implicações: Planeamento e configurações.

   Aconteceu: Durante testes, foi possível simular um ataque deste tipo.

7. **Problema:** *Sniffers*.

   Descrição do problema: Alterando o endereço MAC para o endereço MAC da vítima e executando uma ferramenta de análise de tráfego, como o *ethereal*, é possível visualizar o tráfego destinado a esse utilizador. Um modo mais simples, é a utilização da ferramenta *ettercap* que permite analisar tráfego de qualquer utilizador. É possível ainda obter o tráfego de todos os utilizadores de determinada rede.

   Alteração: Apelar aos utilizadores a utilização de tecnologias que usem encriptação e sensibilizar para a questão da segurança. É possível ainda utilizar ferramentas de *software* que permitem a detecção de *sniffers* (*AntiSniff*[29], por exemplo).

   Implicações: Planeamento e configurações.

   Aconteceu: Em testes.

5.3 Problemas ao nível de servidores e impressoras

8. **Problema:** Vulnerabilidades.

   Descrição do problema: Foram encontradas vulnerabilidades nos servidores, bem como, acesso remoto livre às impressoras. A existência de vulnerabilidades nos

[28] http://www.cisco.com/warp/public/cc/so/neso/sqso/safr/prodlit/sawrm_wp.pdf

[29] http://www.securiteam.com/tools/AntiSniff_-_find_sniffers_on_your_local_network.html

servidores pode implicar fuga ou roubo de informação confidencial, e alteração de informaçãoetc. O acesso remoto livre às impressoras implica a possibilidade de dispender e gastarrecursos (*toner* e papel), ou manter a impressora ocupada.

Alteração: Executar analisadores de vulnerabilidades contra os servidores e as impressoras; corrigir as falhas detectadas e manter os sistemas actualizados. Criação de um *honeypot*[30] para analisar possíveis ataques.

Implicações: Planeamento e configurações.

Aconteceu: Durante testes, foi possível a execução de um analisador de vulnerabilidades.

5.4 Problemas ao nível dos utilizadores

9. **Problema:** Portáteis.

   Descrição do problema: Além dos computadores pessoais da organização do evento, os meios de comunicação também possuiam portáteis para que pudessem trabalharem *online* durante a concretização do evento. Estes portáteis não eram previamente identificados junto da organização, implicando que qualquer atacante mais astuto conseguiria ter acesso à rede e ser bem sucedido nos seus ataques sem ser identificado. Um exemplo de ataque é o simples facto de o portátil estar infectado com vírus, prejudicando o desempenho da rede.

   Alteração: Todos os portáteis deveriam ser identificados previamente, a sua autenticação na rede deveria ser efectuada através do endereço físico da placa de rede (*MAC address*), e deveriam ser alvo de uma análise de, no mínimo, um antivírus.

10. **Problema:** Informação e sensibilização.

    Descrição do problema: A falta de informação e sensibilização dos utilizadores para as questões da segurança informática origina a utilização de protocolos inseguros como o HTTP, telnet e FTP, em vez de HTTPS, SSHv2 e SFTP. Esta falta de preocupação permite a análise simples do tráfego, pois este flui em texto (*plain-text*).

    Alteração: Incentivar à utilização de protocolos seguros, bem como de VPN's corporativas, sistemas *webmail* via HTTPS, *firewalls* pessoais e antivírus.

5.5 Problemas ao nível da rede sem fios

11. **Problema:** Encriptação e autenticação na rede.

    Descrição do problema: A rede sem fios disponibilizada durante o evento não tinha as funcionalidades de encriptação de tráfego, nem de autenticação de dispositivos na rede activas. Pelo que, recorrendo às ferramentas já descritas neste documento, é possível escutar tráfego alheio sem conhecimentos aprofundados sobre a tecnologia,

[30] Um *honeypot* é um recurso de um sistema de informação cujo valor assenta no uso não autorizado ou ilícito de um recurso. Basicamente, são utilizados para analisar como os *hackers* realizam os seus ataques. Mais informação em: http://www.tracking-hackers.com/papers/honeypots.html

podendo ser capturadas informações pessoais e/ou importantes, tais como: palavras-passe, mensagens de correio electrónico e dados de cartões de crédito.

Alteração: Apesar de ser possível quebrar o protocolo WEP, este ou outro protocolo de encriptação (com o WPA) deveria ser activado na rede. Os dispositivos deviam autenticar-se na rede com base no seu endereço físico.

No entanto, é preciso ter em atenção o compromisso entre segurança, acessibilidade e custo. Visto ser um evento de curta duração e, tendo em consideração o nível conhecimentos em informática e segurança das pessoas que o frequentam, este investimento pode não ser justificável.

6 Conclusão

A realização deste estágio implicou o estudo e a investigação sobre os equipamentos, *software* e tecnologias utilizadas, bem como, implementação de redes, criação de uma ferramenta de redes e análise de segurança de redes.

A avaliação do estado de arte da segurança de redes permite-nos concluir que, embora se esteja a ser feito um grande esforço para prevenir e diminuir as falhas de segurança das redes, não se deve negligenciar esta fonte de preocupação quotidiana.

A implementação e supervisão da rede foi um objectivo muito bem conseguido através de uma gestão eficaz da logística dos equipamentos, configurações e da documentação aliada ao projecto. Todos os problemas foram resolvidos com eficiência e eficácia, devido ao forte sentido de equipa e cooperação entre os envolvidos.

A criação da ferramenta "*IP Account Alert*" surgiu como o ponto alto do trabalho desenvolvido, permitindo a detecção de vírus na rede, através da identificação de estações com comportamento anormal. Foi de extrema importância, pois permitiu o aumento da eficácia na detecção e resolução de problemas da rede.

A análise de segurança da rede revelou-se uma tarefa árdua pela necessidade de observação constante e de um elevado sentido crítico na detecção das falhas mais subtis e na gestão dos compromissos entre segurança, acessibilidade e custos financeiros.

Deste modo, considera-se os objectivos como concluídos na sua plenitude, contribuindo para o sucesso deste projecto da entidade de estágio.

Antes de finalizar, são apresentadas quatro recomendações de segurança resultantes do trabalho efectuado:

- Toda a informação deve ser protegida de acordo com o seu valor.
- O sucesso da segurança numa organização está dependente do comportamento das pessoas, da natureza humana.
- Um bom nível de segurança pode ser atingido com uma mistura de diversas soluções e dos diversos tipos de segurança apresentados.
- A segurança não pode ser encarada como um produto, mas como um processo em constante mutação.

7 Bibliografia

7.1 Livros

[1] GOLLMAN, DIETER; *Computer Security*, Wiley, 1999.

[2] MAIWALD, ERIC; *Fundamentals of Network Security*, McGraw Hill, 2004.

[3] SILVA, PEDRO TAVARES; *Segurança dos Sistemas de Informação – Gestão Estratégica da Segurança Empresarial*, Centro Atlântico, 2003.

[4] CHAPPEL, LAURA; *Introduction to Cisco Router Configuration*, Cisco Press, 1998

[5] CHAPPEL, LAURA; *Advanced Cisco Router Configuration*, Cisco Press, 1998

[6] BONEY, JAMES; *Cisco IOS in a Nutshell*, O'Reilly, 2001

7.2 Outras publicações

- MARGI, Cíntia Borges e Ruggiero, Wilson Vicente; *Tutorial sobre Segurança em Redes*, http://www.larc.usp.br/~cbmargi/pdf/Tutorial-comdex-ot.pdf, último acesso a 24/08/2004.
- SILVA, Cândido Fonseca da; *Segurança em Sistemas de Informação*, http://ensino.univates.br/~chaet/Materiais/apres-candido-completa.pdf, último acesso a 24/08/2004.
- VERDE, Prof. Isidro Vila; *Segurança em sistemas e redes*, http://paginas.fe.up.pt/~jvv/Disciplinas/SSR/, último acesso a 24/08/2004.
- *Cisco Systems Packet magazine*, http://www.cisco.com/go/packet/, último acesso a 24/08/2004.
- ZIRING, Neal; *NSA/SNAC Router Security Configuration Guide*, NSA, 2004, http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/cisco_scg.pdf, último acesso a 24/08/2004.
- SANS Course, "*Track 7.1 - Auditing Networks, Perimeter and Systems*", SANS, 2003.
- SANS Course, "*Track 7.2 - Auditing Perimeter*", SANS, 2003.
- Cisco Systems, *A Beginner's Guide to Network Security*, 2001, http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf, último acesso a 24/08/2004.

7.3 Internet

- SecurityFocus: http://www.securityfocus.com
- SecureNet: http://www.securenet.com.br/artigos.php
- SecuriTeam: http://www.securiteam.com/
- CERT: http://www.cert.org

- FBI: http://www.fbi.gov
- Secunia: http://secunia.com/advisory_statistics
- Wireless LAN Security Site: http://www.drizzle.com/~aboba/IEEE/
- NIST: http://csrc.nist.gov/publications/nistpubs/
- HoneyPots: http://www.tracking-hackers.com/papers/honeypots.html
- Sniffing FAQ: http://www.robertgraham.com/pubs/sniffing-faq.html
- TCP Exploits: http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/TCPexploits/
- Google: http://www.google.com
- Cisco: http://www.cisco.com
- Packeteer: http://www.packeteer.com
- Insecure: http://www.insecure.org
- SANS: http://www.sans.org

ANEXO A: Estudo sobre as normas de segurança informática

Este estudo sobre as normas de segurança informática surgiu durante a análise do estado-de-arte da segurança informática. Foram realizadas pesquisas no sentido de saber se existiam normas vigentes nesta área e qual a sua finalidade. Estas pesquisas resultaram na descoberta de diversas normas, das quais foram seleccionadas as mais importantes:

- X.800 (1991)– *Security architecture for open systems*
- ISO/IEC 17799 (2000) – *Code of practice for information security management*
- BS 7799-2 (2002) – *Information security management*
- SAFE (2003) – *A security blueprint for enterprise networks*
- *Rainbow Series*
- ISO 7498-2 – *ISO Security Architecture*
- 800 Series – *NIST Specials Publications*

Existem mais normas, no entanto, ou estão obsoletas, através das descritas neste documento; ou estão mais relacionadas com a gestão da segurança.

O estudo permitiu concluir que a área da segurança encontra-se muito bem documentada ao nível de normas e *standards*. A documentação é actual e prossegue uma evolução saudável.

X.800 – Security architecture for open systems

Esta norma trata-se de uma recomendação que define elementos estruturais genéricos relacionados com segurança que podem ser aplicados nas circunstâncias onde é necessária a protecção na comunicação entre sistemas abertos (*open systems*). Estabelece, dentro da estrutura do Modelo de Referência (Recomendação X.200), guias e restrições que melhoram as recomendações existentes ou o desenvolvimento de novas no contexto do modelo OSI, permitindo comunicações seguras e uma aproximação consistente da segurança no modelo OSI.

Esta recomendação extende a recomendação X.200 (Modelo de Referência) no sentido em que cobre aspectos de segurança, os quais são elementos estruturais genéricos dos protocolos de comunicação que não são discutidos na X.200.

A X.800:

- contém uma descrição geral dos serviços de segurança e mecanismos relacionados; e
- define as posições onde os serviços e mecanismos devem estar associados, no X.200.

Os serviços e mecanismos básicos de segurança, bem como a sua colocação, foram devidamente identificados para todas as camadas do Modelo de Referência (Modelo OSI). As relações de arquitectura dos serviços e mecanismos de segurança para o Modelo OSI foram também identificadas.

A recomendação X.800 não modifica conceitos nem definições do Modelo OSI, apenas acrescenta soluções de segurança para cada camada identificada no Modelo.

ISO/IEC 17799:2000 – Code of practice for information security management

A ISO 17799 é um conjunto de recomendações para a gestão da segurança de informação para as pessoas responsáveis por iniciar, implementar ou manter a segurança na sua organização, servindo como modelo de referência.

Neste sentido, esta norma estabelece uma base comum para o desenvolvimento organizacional de normas de segurança e de práticas efectivas de gestão da segurança, estabelecendo também a confidencialidade nas relações entre organizações.

A ISO 17799 revela as melhores práticas em dez áreas de controlo da segurança, nomeadamente:

1. políticas de segurança: a necessidade de uma política de segurança, assim como, uma revisão e avaliação regular do documento.
2. segurança organizacional: como deverá ser gerida, pela organização, a função de segurança da informação.
3. classificação de bens: a necessidade de proteger devidamente ambos os bens físicos e de informação.
4. segurança de pessoal: a necessidade de gerir o risco durante o processo de recrutamento, assim como, a educação dos colaboradores.
5. segurança física e ambiental: todos os bens físicos devem ser devidamente protegidos de ladrões, fogo e outros desastres ambientais.
6. comunicações e gestão de operações: a necessidade de documentar os processos de gestão para os computadores e redes, assim como, a segurança da informação em trânsito.
7. controlo de acessos: o controlo de acessos à informação, sistemas, redes e aplicações, bem como a gestão de utilizadores e a necessidade de monitorização.
8. desenvolvimento de sistemas e manutenção: a inclusão da segurança em projectos de desenvolvimento, a necessidade de criptografia e gestão de chaves.
9. planeamento de continuidade do negócio: os riscos da interrupção da actividade e diversas alternativas para a gestão da continuidade.
10. conformidade: como a organização deve utilizar uma política e avaliar a sua conformidade.

Esta norma deve ser utilizada como ponto de partida, e como guia, no estabelecimento e criação de programas de segurança nas organizações.

BS 7799-2:2002 – Information security management systems

A BS 7799-2:2002 é uma norma Britânica, não ISO. Esta norma especifica requisitos para o estabelecimento, implementação, operação, monitorização, revisão, manutenção e melhoramento da documentação do Sistema de Gestão de Segurança da Informação (ISMS – *Information Security Management System*). Especifica ainda requisitos para a implementação dos controlos de segurança à medida dos riscos de negócio da organização. A mais valia desta norma é a certificação da infraestrutura de segurança de uma organização. A BS 7799-2:2002 baseia-se no ciclo de Planear-Fazer-Verificar-Actuar.

SAFE – A security blueprint for enterprise networks

A norma "*SAFE Blueprint*" da Cisco Systems é uma directriz para o desenvolvimento de redes seguras empresariais. O seu principal objectivo é promover as melhores práticas no desenho e implementação de redes seguras. SAFE possui uma aproximação de "defesa-em-profundidade" no desenho de segurança de redes, servindo como um guia para os responsáveis pela concepção de redes ("*network designers*") que considerem os requisitos de segurança das suas redes. Este tipo de concepção é focado em ameaças esperadas e nos seus métodos de mitigação, resultando numa aproximação em camada da segurança, onde uma falha numa das camadas não irá comprometer o resto da rede. SAFE é um conceito baseado em produtos Cisco e respectivos parceiros.

A biblioteca SAFE da Cisco é composta por diversos documentos, nomeadamente:

- *SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks*, contem informação sobre as melhores práticas na concepção e implementação de redes seguras.
- *SAFE: IPSec Virtual Private Networks in Depth*, contem informação sobre as melhores práticas na concepção e implementação de redes privadas empresarias com IPSec.
- *SAFE: Wireless LAN Security in Depth—Version 2*, contem informação sobre as melhores práticas na concepção e implementação de segurança em redes sem fios (WLAN) utilizando elementos da "*Cisco SAFE Blueprint*" para a segurança das redes.
- *SAFE: IP Telephony Security in Depth*, contem informação sobre as melhores práticas na concepção e implementação de redes telefonia IP utilizando elementos da "*SAFE Blueprint*".
- *SAFE: IDS Deployment, Tuning, and Logging in Depth*, trata-se de um guia de alto nível para a colocação de sensores *Network-Based Intrusion Detection System* (NIDS), implementação de *Intrustion Prevention System* (IPS) e registos seguros de *syslog*.
- *SAFE: Worm Mitigation*, discute técnicas e tecnologias de contaminação e mitigação.
- *SAFE: Layer 2 Best Practices*, descreve ataques de redes de nível 2, bem como, as melhores práticas de segurança de redes virtuais (VLAN).

Rainbow Series

"*Rainbow Series*" é o nome dado a uma colecção de documentos de interpretação e de orientação publicados pelo *National Computer Security Center* (NCSC). Cada documento possui uma capa de cor diferente; daí o nome "*rainbow*" (arco-íris). As linhas de orientação da *rainbow series* estão concebidas para expandir e clarificar os requisitos no *Trusted Computer System Evaluation Criteria* (TCSEC). Contudo, são apenas linhas de orientação.

Os documentos mais relevantes para a área em foco neste documento são:

- TCSEC, Orange Book
- TNI, Red Book

7.3..1 TCSEC – Trusted Computer Security Evaluation Criteria

TCSEC, também conhecido por Livro Laranja (*Orange Book*), pertence ao Departamento de Defesa (*Department of Defense - DoD*) dos Estados Unidos e foi escrito, originalmente, para sistemas militares. Este documento transpõe as categorias de segurança do DoD para a indústria da segurança informática, descrevendo-as ao pormenor.

As categorias de segurança do DoD são consideradas como certificações de segurança para os sistemas e estão classificadas de D (protecção miníma) até A (protecção verificada):

- D – Protecção miníma: Esta categoria engloba qualquer sistema que não esteja de acordo com outra categoria ou que tenha falhado na obtenção de uma classificação maior.
- C – Protecção pessoal (*discretionary*): Aplica-se em *Trusted Computer Bases* (TCB's – computadores de confiança) com um objecto opcional protegido (por exemplo, ficheiros, directórios, dispositivos, etc.).
- B – Protecção geral (m*andatory*): Esta categoria define que sistemas de protecção a TCB's devem ser genéricos e não pessoais.
- A – Protecção verificada: É o nível mais alto de segurança. Só existem três sistemas com esta certificação: *Boeing MLS LAN*, *Gemini Trusted Network Processor*, *Honeywell SCOMP*.

O TCSEC define também critérios dentro das seguintes categorias:

- Política de segurança
- Controlo de Acessos
- Garantia

7.3..2 TNI – Trusted Network Interpretation

A TNI, também conhecida por Livro Vermelho (*Red Book*) tem como objectivo endereçar a segurança de redes com conceitos e terminologia introduzida no TCSEC.

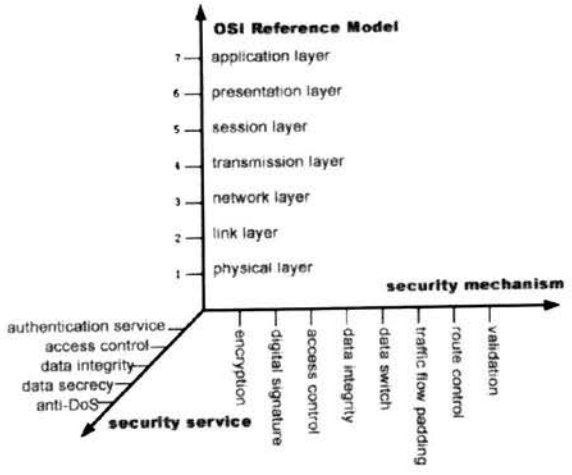
ISO Security Architecture – ISO 7498-2

O ISO 7498-2 descreve a estrutura de segurança de um sistema OSI. Trata-se de um modelo de segurança em sete camadas, tal como o ISO 7498-1, mais conhecido por Modelo de Referência OSI.

De acordo com este modelo, a infraestrutura de um sistema de informação seguro deve incluir:

- Cinco tipos de serviços de segurança
- Oito mecanismos de segurança que suportem os serviços acima
- Métodos de gestão de segurança

A figura seguinte revela a estrutura proposta por este modelo:



800 Series – NIST Special Publications

As séries 800 da NIST (*National Institute of Standards and Technology*) são documentos que visam a orientação nos diversos temas da segurança informática, nomeadamente: Criptografia, Testes, Investigação e Gestão. Estes documentos podem ser encontrados no seguinte endereço *web*: http://csrc.nist.gov/publications/nistpubs/index.html

ANEXO B: Código fonte da aplicação "*IP Account Alert*"

```
<?php
// constantes
$ripaddr = "10.1.51.252";
$system = "1";
$shipaccount = "1";

$COMMUNITY = "telepac_pje";
$HEADER_COLOR = "#999999";
$FIRST_COLOR = "#9999FF";
$SECOND_COLOR = "#7777AA";
$ALERT_COLOR = "#FF0000";
$ALERT_ALARM = 0;
$ALERT_IP = Array();
$ALERT_NPACKETS = 5;
$ALERT_NDESTIPS = 7; //5
$ALERT_MAXNPACKETS = 450;

if (isset($ripaddr) && isset($system))
{
        $host = $ripaddr;
        $sysname = snmpget($host, $COMMUNITY, "system.sysName.0");
        $sysup = snmpget($host, $COMMUNITY, "system.sysUpTime.0");
        $sysupre = substr(strrchr($sysup, ")"), 1);
        $syslocation = snmpget($host, $COMMUNITY, "system.sysLocation.0");
        $tcpcon = snmpget($host, $COMMUNITY, "tcp.tcpCurrEstab.0");
        $tcpconre = eregi_replace("Gauge32:", "", $tcpcon);

        // CPU utilization
        $cpuutilz_30s = snmpget($host, $COMMUNITY, ".1.3.6.1.4.1.9.2.1.56.0");
        $cpuutilz_1m = snmpget($host, $COMMUNITY, ".1.3.6.1.4.1.9.2.1.57.0");
        $cpuutilz_5m = snmpget($host, $COMMUNITY, ".1.3.6.1.4.1.9.2.1.58.0");
}

if (isset($ripaddr) && isset($shipaccount))
{
        $host = $ripaddr;
        // define lip accounting tables' OIDs
        $lipAccountingTable_srcIP = ".1.3.6.1.4.1.9.2.4.7.1.1";
        $lipAccountingTable_destIP = ".1.3.6.1.4.1.9.2.4.7.1.2";
        $lipAccountingTable_nPackets = ".1.3.6.1.4.1.9.2.4.7.1.3";
        $lipAccountingTable_nBytes = ".1.3.6.1.4.1.9.2.4.7.1.4";
        // get lip accounting tables
        $readLipAccSrcIP = snmpwalk($host, $COMMUNITY, $lipAccountingTable_srcIP);
        $readLipAccDestIP = snmpwalk($host, $COMMUNITY, $lipAccountingTable_destIP);
        $readLipAccNPackets = snmpwalk($host, $COMMUNITY, $lipAccountingTable_nPackets);
        $readLipAccNBytes = snmpwalk($host, $COMMUNITY, $lipAccountingTable_nBytes);

        /*
         Alarme.. se o nº médio de pacotes for inferior ou igual a 10 e o ip de origem tiver
        mais do que 5 ip's de destino, entao marcar a vermelho */
        $tmp = "";
        for ($i = 0; $i < count($readLipAccSrcIP); $i++) {
                // separador entre ip's de origem e inicialização do alarme
                if ($tmp != $readLipAccSrcIP[$i]) {
                        if ($nPackets != 0) {
                                $avgPackets = $nPackets / $nDestIPs;
                                if (($avgPackets <= $ALERT_NPACKETS || $avgPackets >=
                                        $ALERT_MAXNPACKETS) &&
                                        ($nDestIPs >= ($ALERT_NDESTIPS * 2))) {
                                        $ALERT_ALARM = 1;
                                        if (!in_array($tmp, $ALERT_IP)) {
                                                array_push($ALERT_IP, $tmp);
                                        }
                                }
                        }
                $nPackets = 0;
                        $nDestIPs = 0;
                        $avgPackets = 0;
                }
                $tmp = $readLipAccSrcIP[$i];
                // alarmistica
                $nDestIPs += 1;
                $nPackets += $readLipAccNPackets[$i];
        }
```

```
}
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Frameset//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-frameset.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="pt" lang="pt" dir="ltr">
<head>
<title>SNMP - router information</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="Refresh" content="30; shipccount.html" />
<style type="text/css">
<!--
body  {font-family: arial, helvetica, geneva, sans-serif; font-size: small}
//-->
</style>
</head>
<body>
<?php
if ($ALERT_ALARM) {
        ?>
        <h2><font color="#FF0000">ALERT!</font></h2>
        <h4>Alert IP Addresses: <br /><?php
                while (list($key, $value) = each($ALERT_IP)) {
                        echo "     <font color=\"#FF0000\"
size=\"3\"><b>".$value."</b></font><br />";
        }
        ?></h4>
        <?php
}
?>
<hr />
<h2>router information</h2>
<p />
<?php
        echo "<b>IP Address:</b> ".$host."<br /><b>System Name:</b> ".$sysname."<br />";
        echo "<b>System Location:</b> ".$syslocation."<br /><b>System Uptime:</b>
".$sysupre."<br />";
        echo "<b>Current Tcp Connections:</b>  ".$tcpconre."<br />";
        echo "<b>CPU Utilization (last 5 min):</b>  ".$cpuutilz_5m."%<br />";
        echo "<b>CPU Utilization (last 1 min):</b>  ".$cpuutilz_1m."%<br />";
        echo "<b>CPU Utilization (last 30 s):</b>  ".$cpuutilz_30s."%<br />";
?>
<hr />
<h2>sh ip accounting</h2>
<font face="Verdana, Arial, Helvetica" size="1">
<table cellspacing="0" cellpadding="0">
        <tr height="15" bgcolor="<?=$HEADER_COLOR;?>">
                <td><b>   src ip   </b></td>
                <td><b>   dest ip   </b></td>
                <td><center><b>   # of packets   </b></center></td>
                <td><center><b>   # of bytes   </b></center></td>
        </tr>
        <?php
        $bitcolor = 1;
        for ($i = 0; $i < count($readLipAccSrcIP); $i++) {
                // separador entre ip's de origem e inicialização do alarme
                if ($tmp != $readLipAccSrcIP[$i]) {
                        echo
"<tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr>";
                        $nPackets = 0;
                        $nDestIPs = 0;
                        $avgPackets = 0;
                }
                $tmp = $readLipAccSrcIP[$i];

                // variação da cor por linha
                if (($avgPackets <= $ALERT_NPACKETS || $avgPackets >= $ALERT_MAXNPACKETS) &&
                        ($nDestIPs >= $ALERT_NDESTIPS))
                        echo "<tr height=\"15\" bgcolor=\"".$ALERT_COLOR."\">";
                else {
                        if ($bitcolor)
                                echo "<tr height=\"15\" bgcolor=\"".$FIRST_COLOR."\">";
                        else
                                echo "<tr height=\"15\" bgcolor=\"".$SECOND_COLOR."\">";
                        $bitcolor = !$bitcolor;
                }

                // dados
                echo "<td>   ".substr(strrchr($readLipAccSrcIP[$i], ":"), 1)."
  </td>";
```

```
                echo "<td> <b>--></b>  ".substr(strrchr($readLipAccDestIP[$i], ":"),
1)."   </td>";
                echo "<td><center>   ".$readLipAccNPackets[$i]."
  </center></td>";
                echo "<td><center>   ".$readLipAccNBytes[$i]."
  </center></td>";
                echo "</tr>";

                // alarmistica
                $nDestIPs += 1;
                $nPackets += $readLipAccNPackets[$i];
                $avgPackets = $nPackets / $nDestIPs;
        }
        echo "</table>";
?>
<?php
if (isset($ripaddr) && isset($shipaccountcheckpoint))
{
?>
<hr />
<h2>sh ip accounting checkpoint</h2>
<table cellspacing="0" cellpadding="0">
<tr height="15" bgcolor="#999999">
<td><b>   src ip   </b></td>
<td><b>   dest ip   </b></td>
<td><center><b>   # of packets   </b></center></td>
<td><center><b>   # of bytes   </b></center></td>
</tr>
<?php
        $bitcolor = 1;
        $host = $ripaddr;

        // define lip accounting checkpoint tables' OIDs
        $lipCkAccountingTable_srcIP = ".1.3.6.1.4.1.9.2.4.9.1.1";
        $lipCkAccountingTable_destIP = ".1.3.6.1.4.1.9.2.4.9.1.2";
        $lipCkAccountingTable_nPackets = ".1.3.6.1.4.1.9.2.4.9.1.3";
        $lipCkAccountingTable_nBytes = ".1.3.6.1.4.1.9.2.4.9.1.4";

        // get lip accounting checkpoint tables
        $readLipCkAccSrcIP = snmpwalk($host, $COMMUNITY, $lipCkAccountingTable_srcIP);
        $readLipCkAccDestIP = snmpwalk($host, $COMMUNITY, $lipCkAccountingTable_destIP);
        $readLipCkAccNPackets = snmpwalk($host, $COMMUNITY, $lipCkAccountingTable_nPackets);
        $readLipCkAccNBytes = snmpwalk($host, $COMMUNITY, $lipCkAccountingTable_nBytes);

        $tmp = "";
        for ($i = 0; $i < count($readLipCkAccSrcIP); $i++) {
                // separador entre ip's de origem e inicialização do alarme
                if ($tmp != $readLipCkAccSrcIP[$i]) {
                        echo
"<tr><td> </td><td> </td><td> </td><td> </td></tr>";
                        $nPackets = 0;
                        $nDestIPs = 0;
                        $avgPackets = 0;
                }
                $tmp = $readLipCkAccSrcIP[$i];

                // variação da cor por linha
                if (($avgPackets <= $ALERT_NPACKETS || $avgPackets >= $ALERT_MAXNPACKETS) &&
($nDestIPs >= $ALERT_NDESTIPS))
                        echo "<tr height=\"15\" bgcolor=\"".$ALERT_COLOR."\">";
                else {
                        if ($bitcolor)
                                echo "<tr height=\"15\" bgcolor=\"".$FIRST_COLOR."\">";
                        else
                                echo "<tr height=\"15\" bgcolor=\"".$SECOND_COLOR."\">";
                        $bitcolor = !$bitcolor;
                }

                // dados
                echo "<td>   ".substr(strrchr($readLipCkAccSrcIP[$i], ":"), 1)."
  </td>";
                echo "<td> <b>--></b>   ".substr(strrchr($readLipCkAccDestIP[$i],
":"), 1)."   </td>";
                echo "<td><center>   ".$readLipCkAccNPackets[$i]."
  </center></td>";
                echo "<td><center>   ".$readLipCkAccNBytes[$i]."
  </center></td>";
                echo "</tr>";
```

```
                // alarmistica
                $nDestIPs += 1;
                $nPackets += $readLipCkAccNPackets[$i];
                $avgPackets = $nPackets / $nDestIPs;
        }
}
?>
</table>
</font>
<p />
</body>
</html>
```

ANEXO C: Exemplos das configurações do equipamento de rede

Cisco Router 2600:

```
PROJ-XXX#sh run
Current configuration : 4820 bytes
!
! Last configuration change at 14:56:37 PT Sun Jun 13 2004 by rdcxxx
! NVRAM config last updated at 14:56:37 PT Sun Jun 13 2004 by rdcxxx
!
version 12.3
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname PROJ-XXX
!
boot-start-marker
boot system flash c2600-ik9o3s-mz.123-9.bin
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 $1$YHBX$/ZGHfx.65fcE10GMyzdJd/
!
username rdcxxx password 7 111B1D0612071903567A7B70
memory-size iomem 10
clock timezone PT 1
no network-clock-participate slot 1
no network-clock-participate wic 0
aaa new-model
!
!
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name XXX.pt
!
ip audit po max-events 100
ip ssh time-out 50
no ftp-server write-enable
!
!
interface Loopback0
 description Gestao Inband XXX
 ip address 172.28.254.24 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.1.51.252 255.255.255.0
 no ip redirects
 no ip proxy-arp
 duplex auto
 speed auto
 standby 1 ip 10.1.51.253
 standby 1 timers 2 5
 standby 1 priority 120
 standby 1 preempt
 standby 1 track Serial0/0
 standby 1 track Serial0/1
!
interface Serial0/0
 description Interligacao VPN-IP (NNA/GECA 1001273143 2Mbps)
 bandwidth 1984
 ip address 192.168.0.94 255.255.255.252
 load-interval 30
 keepalive 5
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface Serial0/1
 description Interligacao VPN-IP (NNA/GECA 1001273144 2Mbps)
 bandwidth 1984
 ip address 192.168.1.42 255.255.255.252
 load-interval 30
 keepalive 5
!
router bgp 64578
 no synchronization
 bgp log-neighbor-changes
 network 10.1.51.0 mask 255.255.255.0
 network 10.1.71.0 mask 255.255.255.0
 network 10.1.81.0 mask 255.255.255.0
 network 10.1.91.0 mask 255.255.255.0
 network 172.28.254.96 mask 255.255.255.240
 neighbor 172.28.182.67 remote-as 15525
 neighbor 172.28.182.67 ebgp-multihop 2
 neighbor 172.28.182.67 update-source Loopback0
 neighbor 172.28.182.67 timers 15 45
 neighbor 172.28.182.67 soft-reconfiguration inbound
 no auto-summary
!
no ip http server
no ip http secure-server
ip classless
ip route 10.1.71.0 255.255.255.0 10.1.51.254
ip route 10.1.81.0 255.255.255.0 10.1.51.254
ip route 172.28.182.67 255.255.255.255 192.168.0.93
ip route 172.28.182.67 255.255.255.255 192.168.1.41
ip route 172.28.254.96 255.255.255.240 10.1.51.254
!
!
logging source-interface Loopback0
logging 10.99.99.80
access-list 20 permit 10.100.100.4
access-list 20 permit 172.31.237.1
access-list 20 permit 172.31.220.1
access-list 20 remark SNMP
access-list 20 permit 172.28.250.0 0.0.0.15
access-list 20 permit 192.168.200.0 0.0.0.255
access-list 20 permit 10.99.99.0 0.0.0.255
access-list 20 permit 172.28.254.0 0.0.0.255
access-list 20 permit 172.28.251.32 0.0.0.31
access-list 20 permit 172.28.253.128 0.0.0.127
access-list 20 permit 192.168.0.0 0.0.0.255
access-list 20 permit 192.168.1.0 0.0.0.255
access-list 20 remark rede local - IP reservados -equip-activos-XXX
access-list 20 permit 10.1.51.240 0.0.0.15
access-list 110 permit tcp host 172.28.250.5 any eq telnet
access-list 110 permit tcp host 172.31.237.1 any eq telnet
access-list 110 permit tcp host 172.31.220.1 any eq telnet
access-list 110 permit tcp 192.168.200.0 0.0.0.255 any eq telnet
access-list 110 permit tcp 10.99.99.0 0.0.0.255 any eq 22
access-list 110 permit tcp 172.28.254.0 0.0.0.255 any eq 22
access-list 110 permit tcp 172.28.251.32 0.0.0.31 any eq 22
access-list 110 permit tcp 172.28.253.128 0.0.0.127 any eq 22
access-list 110 permit tcp 192.168.0.0 0.0.0.255 any eq 22
access-list 110 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 110 permit tcp 192.168.200.0 0.0.0.255 any eq 22
access-list 110 remark rede local - IP reservados -equip-activos-XXX
access-list 110 permit tcp 10.1.51.240 0.0.0.15 any eq 22
access-list 110 permit tcp host 10.100.100.4 any eq 22
!
snmp-server community XXX RO 20
snmp-server trap-source Loopback0
snmp-server location XXX - Router Principal
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps hsrp
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps atm pvc
snmp-server host 172.28.250.5 XXX
!
```

```
!
line con 0
 password 7 153D1B09166C082821
line aux 0
 password 7 1061191C1751310705
line vty 0 4
 access-class 110 in
 exec-timeout 15 0
 password 7 002B0303161D280A06
 transport input telnet ssh
 transport output ssh
!
ntp clock-period 17180951
ntp source Loopback0
ntp server 172.28.254.88
ntp server 172.28.250.5 prefer
!
end

PROJ-XXX#sh ver
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S-M), Version 12.3(9), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 14-May-04 14:37 by dchih
Image text-base: 0x80008098, data-base: 0x81C7194C

ROM: System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1)
ROM: C2600 Software (C2600-IO3-M), Version 12.2(15)T12,  RELEASE SOFTWARE (fc1)

PROJ-XXX uptime is 2 weeks, 1 day, 0 minutes
System returned to ROM by reload at 01:05:00 PST Mon Mar 1 1993
System restarted at 12:05:47 PT Tue Jun 1 2004
System image file is "flash:c2600-ik9o3s-mz.123-9.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 2651XM (MPC860P) processor (revision 0x300) with 118784K/12288K bytes of memory.
Processor board ID JAE0817EBD2 (4192222121)
M860 processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Cisco Catalyst 3550:

```
PROJ-XXX#sh run
Current configuration : 7034 bytes
!
! Last configuration change at 15:10:08 PT Sun Jun 13 2004 by rdcxxx
! NVRAM config last updated at 15:10:08 PT Sun Jun 13 2004 by rdcxxx
!
version 12.1
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
```

```
hostname SW-XXX-3550
!
aaa new-model
enable secret 5 $1$VCk1$9YNLn48yoH2.cI0Oiplym.
!
username rdcxxx password 7 0519020C24595C064B554746
clock timezone PT 1
ip subnet-zero
ip routing
no ip dhcp conflict logging
ip dhcp excluded-address 10.1.71.254
ip dhcp excluded-address 10.1.81.254
ip dhcp excluded-address 10.1.81.1 10.1.81.20
!
ip dhcp pool pool_press
   network 10.1.71.0 255.255.255.0
   default-router 10.1.71.254
   dns-server 62.48.131.10 62.48.131.11
!
ip dhcp pool pool_guests
   network 10.1.81.0 255.255.255.0
   default-router 10.1.81.254
   dns-server 62.48.131.10 62.48.131.11
!
no ip domain-lookup
ip domain-name xxx.pt
ip ssh time-out 5
ip ssh authentication-retries 3
vtp domain proj_xxx
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
vlan 2
 name staff
!
vlan 3
 name press
!
vlan 4
 name guests
!
vlan 5
 name ticketline
!
vlan 99
 name other
!
!
interface GigabitEthernet0/1
 description Ligacao ao piso 3p2 - press
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/2
 description Ligacao ao piso 3p1 - press
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/3
 description Ligacao ao piso 1a1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/4
 description Ligacao ao piso 1p1 - escritorios
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
```

```
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/5
 description Ligacao as Bilheteiras
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/6
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/7
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/8
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/9
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/10
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/11
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
!
interface GigabitEthernet0/12
 switchport access vlan 2
 switchport mode access
 load-interval 30
 spanning-tree portfast
!
interface Vlan1
 description Gestao
 ip address 172.28.254.97 255.255.255.240
!
interface Vlan2
 description Staff
 ip address 10.1.51.254 255.255.255.0
!
interface Vlan3
 description PressTribune
 ip address 10.1.71.254 255.255.255.0
 ip access-group ACL_Permit-INTERNET in
!
interface Vlan4
 description Guest
 ip address 10.1.81.254 255.255.255.0
 ip access-group ACL_Permit-INTERNET in
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.51.253
no ip http server
!
ip access-list extended ACL_Permit-INTERNET
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip host 0.0.0.0 host 255.255.255.255
 deny   ip any 224.0.0.0 31.255.255.255
```

```
 deny   ip any 62.73.181.64 0.0.0.32
 deny   ip any 62.73.181.0 0.0.0.63
 permit ip any any
!
access-list 20 remark SNMP
access-list 20 permit 10.100.100.4
access-list 20 permit 172.31.237.1
access-list 20 permit 172.31.220.1
access-list 20 permit 172.28.250.0 0.0.0.15
access-list 20 permit 192.168.200.0 0.0.0.255
access-list 20 permit 10.99.99.0 0.0.0.255
access-list 20 permit 172.28.254.0 0.0.0.255
access-list 20 permit 172.28.251.32 0.0.0.31
access-list 20 permit 172.28.253.128 0.0.0.127
access-list 20 permit 192.168.0.0 0.0.0.255
access-list 20 permit 192.168.1.0 0.0.0.255
access-list 20 remark rede local - IP reservados -equip-activos-xxx
access-list 20 permit 10.1.51.240 0.0.0.15
access-list 20 permit 10.1.61.240 0.0.0.15
access-list 110 permit tcp 10.99.99.0 0.0.0.255 any eq 22
access-list 110 permit tcp 172.28.253.128 0.0.0.127 any eq 22
access-list 110 permit tcp 172.28.254.0 0.0.0.255 any eq 22
access-list 110 permit tcp 172.28.251.32 0.0.0.31 any eq 22
access-list 110 permit tcp 172.28.252.128 0.0.0.63 any eq 22
access-list 110 permit tcp 192.168.0.0 0.0.0.255 any eq 22
access-list 110 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 110 permit tcp 192.168.200.0 0.0.0.255 any eq 22
access-list 110 permit tcp host 10.100.100.4 any eq 22
access-list 110 remark ### Rede local-IP reservados-equip-activos-xxx ###
access-list 110 permit tcp 10.1.51.240 0.0.0.15 any eq 22
snmp-server community XXX RO 20
snmp-server trap-source Vlan1
snmp-server location Sala Principal
snmp-server enable traps snmp authentication warmstart linkdown linkup coldstart
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps bridge
snmp-server enable traps stpx
snmp-server enable traps rtr
snmp-server enable traps port-security
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps MAC-Notification
snmp-server enable traps hsrp
snmp-server enable traps cluster
snmp-server enable traps copy-config
snmp-server enable traps syslog
snmp-server enable traps bgp
snmp-server enable traps vlan-membership
snmp-server host 172.28.250.5 xxx
banner login ^C

      ------------------ .o00o. ------------------

                    Switch 3550

                     PROJ - XXX

                   Piso -2 - Bastidor 1

         ---------------------------------
         UNAUTHORISED ACCESS IS PROHIBITED
      Entradas nao autorizadas sao punidas por lei
               (lei 109/91 de 17 Agosto)
      ----------------------------------------------


^C
!
line con 0
 password 7 04741B031D676F4200
line vty 0 4
 access-class 110 in
 exec-timeout 30 30
 password 7 06291F245E082A150C
 transport input ssh
```

```
line vty 5 15
 access-class 110 in
 exec-timeout 30 30
 password 7 06291F245E082A150C
 transport input ssh
!
ntp clock-period 17180992
ntp source Vlan1
ntp server 172.28.254.88
ntp server 172.28.250.5 prefer
!
end

SW-XXX-3550#sh ver
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5K2L2Q3-M), Version 12.1(20)EA1a, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Mon 19-Apr-04 22:16 by yenanh
Image text-base: 0x00003000, data-base: 0x0095E2C4

ROM: Bootstrap program is C3550 boot loader

SW-XXX-3550 uptime is 2 weeks, 1 day, 1 hour, 54 minutes
System returned to ROM by power-on
System restarted at 10:28:57 PT Tue Jun 1 2004
System image file is "flash:/c3550-i5k2l2q3-mz.121-20.EA1a.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C3550-12G (PowerPC) processor (revision H0) with 65526K/8192K bytes of memory.
Processor board ID CAT0802X2X0
Last reset from warm-reset
Bridging software.
Running Layer2/3 Switching Image

Ethernet-controller 1 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 2 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 3 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 4 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 7 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 8 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 9 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 10 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 11 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 12 has 1 Gigabit Ethernet/IEEE 802.3 interface

12 Gigabit Ethernet/IEEE 802.3 interface(s)

The password-recovery mechanism is enabled.
384K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:0E:D7:FA:EA:80
Motherboard assembly number: 73-5526-08
```

```
Power supply part number: 34-0967-01
Motherboard serial number: CAT0802038Z
Power supply serial number: DTH07472UT7
Model revision number: H0
Motherboard revision number: A0
Model number: WS-C3550-12G
System serial number: CAT0802X2X0
Configuration register is 0x10F
```

Cisco Catalyst 2950:

```
SW-XXX-1p1-sw1#sh run
Current configuration : 9522 bytes
!
! No configuration change since last restart
!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname SW-XXX-1p1-sw1
!
aaa new-model
enable secret 5 $1$mIhN$zd1vDJHt30btm8zX4k56i/
!
username rdcxxx password 0 rdcxxx
clock timezone PT 1
!
vlan 2
 name staff
!
vlan 3
 name press
!
vlan 4
 name guests
!
vlan 99
 name others
ip subnet-zero
no ip domain-lookup
ip domain-name xxx.pt
ip ssh time-out 5
vtp domain XXX_XXX
vtp mode transparent
!
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
```

```
!
interface FastEthernet0/5
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/8
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/10
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/12
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/17
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
```

```
interface FastEthernet0/18
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/19
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/20
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/21
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/22
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/23
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/24
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/25
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/26
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/27
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/28
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/29
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/30
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/31
```

```
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/32
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/33
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/34
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/35
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/36
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/37
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/38
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/39
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/40
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/41
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/42
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/43
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/44
 switchport access vlan 3
```

```
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/45
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/46
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/47
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/48
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 1-4,99
 switchport mode trunk
 switchport nonegotiate
 no ip address
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 1-4,99
 switchport mode trunk
 switchport nonegotiate
 no ip address
!
interface Vlan1
 description Gestao
 ip address 172.28.254.102 255.255.255.240
 no ip route-cache
!
ip default-gateway 172.28.254.97
no ip http server
!
access-list 20 remark SNMP
access-list 20 permit 10.100.100.4
access-list 20 permit 172.31.237.1
access-list 20 permit 172.31.220.1
access-list 20 permit 172.28.250.0 0.0.0.15
access-list 20 permit 192.168.200.0 0.0.0.255
access-list 20 permit 10.99.99.0 0.0.0.255
access-list 20 permit 172.28.254.0 0.0.0.255
access-list 20 permit 172.28.251.32 0.0.0.31
access-list 20 permit 172.28.253.128 0.0.0.127
access-list 20 permit 192.168.0.0 0.0.0.255
access-list 20 permit 192.168.1.0 0.0.0.255
access-list 20 remark rede local - IP reservados -equip-activos-xxx
access-list 20 permit 10.1.51.240 0.0.0.15
access-list 20 permit 10.1.61.240 0.0.0.15
access-list 110 permit tcp 10.99.99.0 0.0.0.255 any eq 22
access-list 110 permit tcp 172.28.253.128 0.0.0.127 any eq 22
access-list 110 permit tcp 172.28.254.0 0.0.0.255 any eq 22
access-list 110 permit tcp 172.28.251.32 0.0.0.31 any eq 22
access-list 110 permit tcp 172.28.252.128 0.0.0.63 any eq 22
access-list 110 permit tcp 192.168.0.0 0.0.0.255 any eq 22
access-list 110 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 110 permit tcp 192.168.200.0 0.0.0.255 any eq 22
access-list 110 permit tcp host 10.100.100.4 any eq 22
access-list 110 remark ### Rede local-IP reservados-equip-activos-xxx ###
access-list 110 permit tcp 10.1.51.240 0.0.0.15 any eq 22
snmp-server engineID local 800000090300000F8F300841
snmp-server community xxx RO 20
snmp-server trap-source Vlan1
snmp-server location Piso 1p1 - SW1 - Jornalistas
snmp-server enable traps snmp authentication warmstart linkdown linkup coldstart
```

```
snmp-server enable traps config
snmp-server enable traps syslog
snmp-server enable traps entity
snmp-server enable traps rtr
snmp-server enable traps c2900
snmp-server enable traps vtp
snmp-server enable traps vlan-membership
snmp-server enable traps MAC-Notification
snmp-server enable traps envmon
snmp-server enable traps hsrp
snmp-server enable traps cluster
snmp-server host 172.28.250.5 telepac_pje
banner login ^CC

      ------------------ .o00o. ------------------

                  Switch 2950 - 48 Portas

                     PROJ - XXX

              PISO 1 - Bast 1P1 - Media

           ---------------------------------
           UNAUTHORISED ACCESS IS PROHIBITED
      Entradas nao autorizadas sao punidas por lei
              (lei 109/91 de 17 Agosto)
      -----------------------------------------


^C
!
line con 0
 password 7 080E5C4B1B5F261B1B
line vty 0 4
 access-class 110 in
 exec-timeout 30 30
 password 7 06291F245E082A150C
 transport input ssh
line vty 5 15
 access-class 110 in
 exec-timeout 30 30
 password 7 06291F245E082A150C
 transport input ssh
!
ntp clock-period 17180572
ntp source Vlan1
ntp server 172.28.254.88
ntp server 172.28.250.5 prefer
end

SW-XXX-1p1-sw1#sh ver
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(12c)EA1a, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Fri 27-Dec-02 10:46 by antonino
Image text-base: 0x80010000, data-base: 0x80664000

ROM: Bootstrap program is CALHOUN boot loader

SW-XXX-1p1-sw1 uptime is 21 hours, 39 minutes
System returned to ROM by power-on
System restarted at 14:52:51 PT Tue Jun 15 2004
System image file is "flash:/c2950-i6k212q4-mz.121-12c.EA1a.bin"

cisco WS-C2950G-48-EI (RC32300) processor (revision M0) with 19968K bytes of memory.
Processor board ID FOC0810W1SR
Last reset from system-reset
Running Enhanced Image
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:0F:8F:30:08:40
Motherboard assembly number: 73-7409-12
Power supply part number: 34-0965-01
Motherboard serial number: FOC08090PCK
Power supply serial number: DAB08072ZLT
Model revision number: M0
Motherboard revision number: A0
```

```
snmp-server enable traps config
snmp-server enable traps syslog
snmp-server enable traps entity
snmp-server enable traps rtr
snmp-server enable traps c2900
snmp-server enable traps vtp
snmp-server enable traps vlan-membership
snmp-server enable traps MAC-Notification
snmp-server enable traps envmon
snmp-server enable traps hsrp
snmp-server enable traps cluster
snmp-server host 172.28.250.5 telepac_pje
banner login ^CC

      ------------------ .o00o. ------------------

                  Switch 2950 - 48 Portas

                     PROJ - XXX

             PISO 1 - Bast 1P1 - Media

          ---------------------------------
          UNAUTHORISED ACCESS IS PROHIBITED
      Entradas nao autorizadas sao punidas por lei
               (lei 109/91 de 17 Agosto)
      -----------------------------------------


^C
!
line con 0
 password 7 080E5C4B1B5F261B1B
line vty 0 4
 access-class 110 in
 exec-timeout 30 30
 password 7 06291F245E082A150C
 transport input ssh
line vty 5 15
 access-class 110 in
 exec-timeout 30 30
 password 7 06291F245E082A150C
 transport input ssh
!
ntp clock-period 17180572
ntp source Vlan1
ntp server 172.28.254.88
ntp server 172.28.250.5 prefer
end

SW-XXX-1p1-sw1#sh ver
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(12c)EA1a, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Fri 27-Dec-02 10:46 by antonino
Image text-base: 0x80010000, data-base: 0x80664000

ROM: Bootstrap program is CALHOUN boot loader

SW-XXX-1p1-sw1 uptime is 21 hours, 39 minutes
System returned to ROM by power-on
System restarted at 14:52:51 PT Tue Jun 15 2004
System image file is "flash:/c2950-i6k212q4-mz.121-12c.EA1a.bin"

cisco WS-C2950G-48-EI (RC32300) processor (revision M0) with 19968K bytes of memory.
Processor board ID FOC0810W1SR
Last reset from system-reset
Running Enhanced Image
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:0F:8F:30:08:40
Motherboard assembly number: 73-7409-12
Power supply part number: 34-0965-01
Motherboard serial number: FOC08090PCK
Power supply serial number: DAB08072ZLT
Model revision number: M0
Motherboard revision number: A0
```

```
Model number: WS-C2950G-48-EI
System serial number: FOC0810W1SR
Configuration register is 0xF
```

Ricardo Batista

E-mail: ricardo.batista@siemens.com

Telef: 214178000 Fax: 214178044

Rua Irmãos Siemens, nº 1

2720-093 Amadora


BIBLIOTECA
F.E.
PORTO