Universidade do Porto
Faculdade de Engenharia
FEUP

Helder Bruno Moreira Coelho

EXPLORAÇÃO E GESTÃO DE LOGS DE EQUIPAMENTOS DE NETWORKING E SEGURANÇA

o, 2005

Faculdade de Engenharia da Universidade do Porto
Licenciatura em Engenharia Informática e Computação

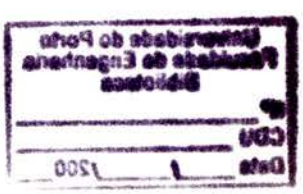
Exploração e Gestão de Logs de Equipamentos de Networking e Segurança no Banco BPI

Relatório do Estágio Curricular da LEIC 2004/2005

Helder Bruno Moreira Coelho

Orientador na FEUP: Prof. Raul Oliveira
Orientador no Banco BPI: Dr. Armando Pinto

Setembro de 2005



Para a minha Mãe, Pai e para a minha Natércia

Resumo

O presente relatório documenta o estágio realizado na instituição Banco BPI, inserido no projecto "Exploração e Gestão de Logs de Equipamentos de Networking e Segurança", no âmbito do Estágio Curricular da Licenciatura em Engenharia Informática e Computação da Faculdade de Engenharia da Universidade do Porto.

O projecto consistiu no estudo das diferentes tecnologias que permitem centralizar os *logs* gerados pelos equipamentos de *networking* e segurança, num único sistema. Inicialmente foi feito o levantamento dos equipamentos a abranger pelo projecto, definida a arquitectura de recolha dos *logs* e implementados os processos para a importação dos *logs* para o concentrador de *logs* . Noutra fase do projecto foi definido um processo para armazenar os *logs* a longo prazo devido ao grande volume de dados gerados pelos equipamentos. Para gerir todo o processo foi desenvolvida uma aplicação que efectua uma cópia semanal dos *logs* da semana passada para dois DVDs. Na última parte do projecto foram analisadas várias soluções existentes para análise de *logs* em tempo real, de forma, a gerar alertas e correlacionar os eventos gerados pelos diferentes equipamentos. Foram eleitos os três melhores produtos que se adaptam à infra-estrutura do Banco BPI.

A implementação deste projecto veio trazer melhorias óbvias na administração dos sistemas do Banco BPI, reforçando a segurança da informação, considerado um factor crítico em qualquer instituição financeira. Com o desenvolvimento do projecto é também facilitada a gestão e detecção de anomalias.

A análise, teste, aquisição e implementação de soluções de análise de *logs* será o desenvolvimento futuro do presente projecto completando assim a única carência.

Agradecimentos

Apresento os meus agradecimentos ao Dr. Armando Pinto e Eng. Mário Fernandes que me orientaram e receberam no Banco BPI e sempre se disponibilizaram para me ajudar durante o estágio. Agradeço também a todas as pessoas na DSI do Porto do Banco BPI que de várias formas me ajudaram a realizar o meu trabalho e que contribuíram à minha rápida adaptação.

Um obrigado aos meus colegas estagiários do Banco BPI, que me ajudaram neste projecto e contribuíram para um óptimo ambiente de trabalho.

Agradeço ao professor Raul Oliveira, que orientou o estágio por parte da faculdade e que me inspirou durante o curso.

Quero por fim agradecer a minha família que me apoiou durante todo o curso e sem os quais seria muito mais difícil concretizar o sonho de ser Engenheiro, aos meus colegas e amigos de curso.

Especial agradecimento à Natércia.

Índice de Conteúdos

Lista de Figuras

1 Introdução

O presente relatório, pretende dar a conhecer o trabalho desenvolvido durante os 6 meses de estágio curricular realizados no Banco BPI.

Este primeiro capítulo está dividido em 3 secções, na primeira apresenta-se a entidade acolhedora de estágio, na seguinte o projecto realizado e por último a organização do relatório.

1.1 O Banco BPI

O Banco BPI é uma das principais instituições da Banca portuguesa. É a unidade principal do Grupo BPI que é o 4º maior grupo financeiro português.

O Banco BPI serve mais de 1.3 milhões de Clientes - particulares, empresas e institucionais - através de uma rede de distribuição multicanal, composta por mais de 500 balcões de retalho, 15 centros de investimento, serviço de homebanking (BPI Net), banca telefónica (BPI Directo), balcões especializados e estruturas dedicadas ao segmento empresas e institucionais.

O Banco Português de Investimento, matriz original do grupo BPI, desenvolve a actividade de banca de investimento - Acções, Corporate Finance e Private Banking - na qual o BPI detém uma posição de liderança.

Surgiu a meio dos anos 80, focando-se exclusivamente na Banca de Investimento. Durante os anos 90 o Banco passou a ter componente comercial, com a aquisição do Banco Fonsecas & Burnay e mais tarde, do Banco Borges & Irmão e do Banco de Fomento e Exterior.

Depois de em 1997 e 1998, o Grupo BPI ter procedido à integração dos quatro bancos adquiridos (BFB, BBI, BFE e Banco Universo) e ter criado um banco comercial único (Banco BPI), em 1999 e 2000 o BPI focalizou-se na criação de uma plataforma de distribuição multicanal, plenamente integrada, na afirmação da marca BPI como uma das principais do sistema bancário.

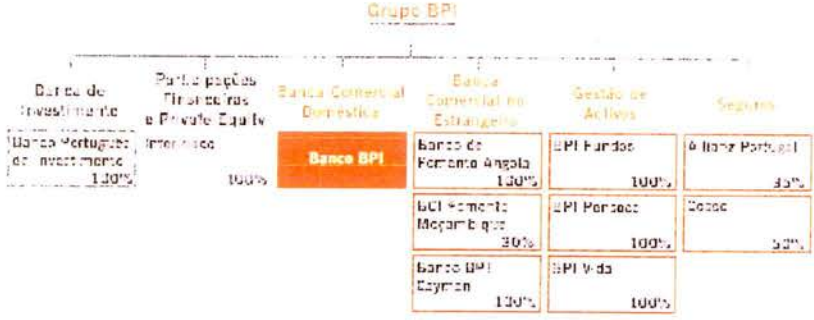


Figura 1 – Principais entidades do grupo BPI

A partir desse momento, uma das grandes preocupações foi a uniformização dos sistemas e procedimentos do Banco. Este processo culminou no início de 2003 com a fusão da parte de investimento com a parte comercial. Ao nível dos sistemas de informação, a uniformização assentou numa sofisticada rede de dados que está disponível desde 1998.

A Direcção de Sistemas de Informação (DSI), é o departamento que trata de todo o suporte informático do BPI, e que produz a grande maioria do software utilizado no Banco. Está

organizada em quatro grandes áreas: Área de Análise de Soluções, Área de Desenvolvimento, Área de Infra-Estrutura e Área de Planeamento, Qualidade e Segurança.

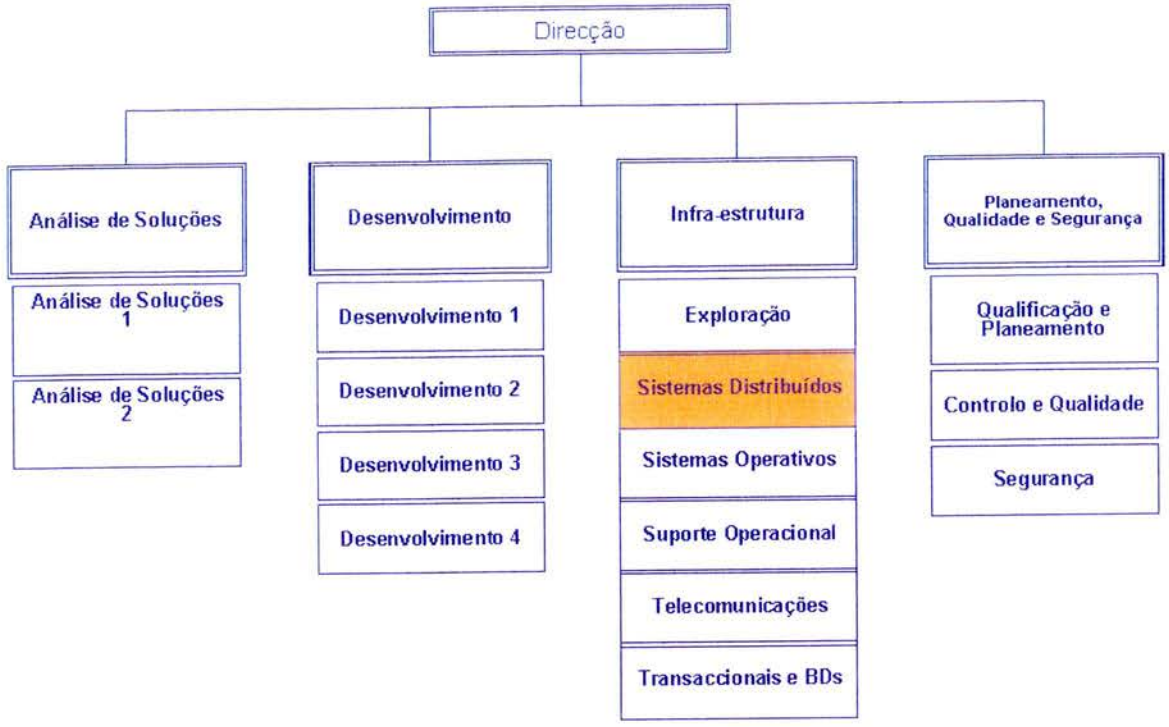


Figura 2 – Equipas da DSI

Da figura acima destaca-se, dentro da Infra-Estrutura, a área de Sistemas Distribuídos devido ao projecto estar inserido nesta equipa. Com mais detalhe é possível observar na figura abaixo a equipa dividida em duas áreas, destacando a de Web e Segurança por estar inserido na mesma.

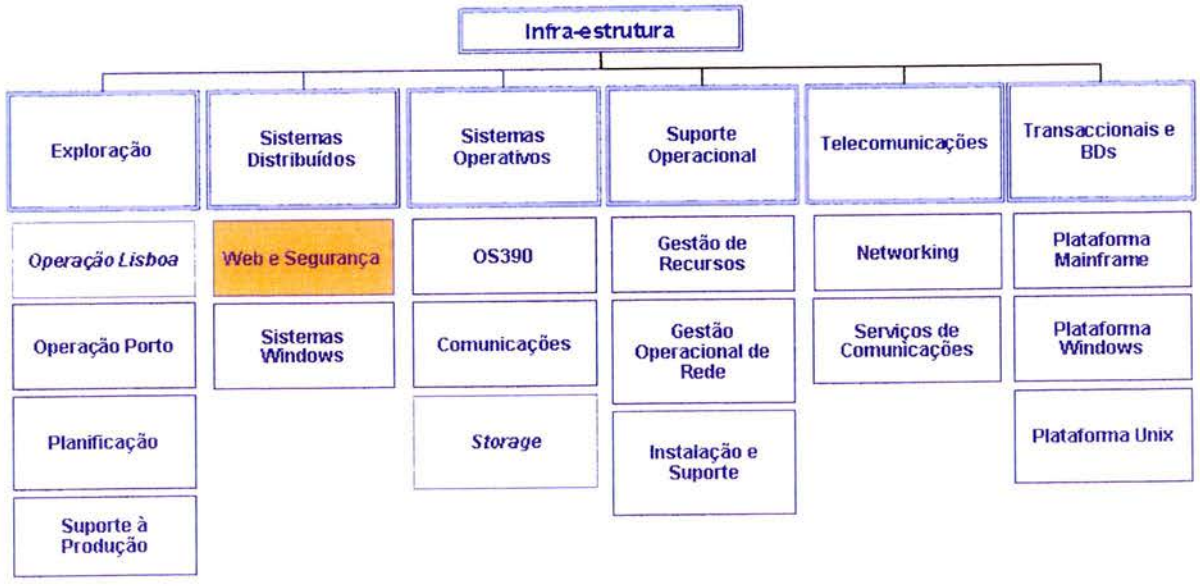


Figura 3 – Equipas da Área de Infra-Estrutura

A Área de Infra-Estrutura é responsável por disponibilizar as soluções em ambiente de produção, garantir a replicação das passagens a produção para o ambiente de formação,

preservar a operacionalidade global das soluções informáticas, gerir os ambientes de desenvolvimento e qualidade, participar noutras actividades executadas por outras áreas.

Como metodologia de implementação de software, o Banco BPI segue uma filosofia de múltiplos ambientes. De um modo geral, existem três ambientes com âmbitos diferentes, mas complementares: o ambiente de desenvolvimento, onde se criam as aplicações e são executados os primeiros testes de validação funcional; o ambiente de qualidade, em que elementos de equipas especializadas no controlo de qualidade testam extensivamente as funcionalidades da aplicação, bem como o seu comportamento perante situações anormais; finalmente, há ainda o ambiente de produção, que é o ambiente final da aplicação, ou seja, já com interacção dos utilizadores finais. Estes três ambientes não são obrigatórios em todos os casos, podendo haver aplicações apenas com dois e outras com quatro ou mais.

1.2 O Projecto: "Exploração e Gestão de Logs de Equipamentos de Networking e Segurança" no Banco BPI

Actualmente, as redes internas (*intranets*) e a Internet representam uma forma de melhorar a produtividade, pois permitem a partilha de informação e a comunicação entre pessoas de uma organização e entre esta e o exterior. As redes permitem a disponibilização de informação e serviços cada vez mais diversificados, permitindo às organizações tornarem-se mais eficientes, reduzirem os custos e chegar a um maior número de pessoas. A informação atempada e rigorosa é dos activos de maior valor para quem tem de decidir rápida e eficientemente numa economia crescentemente globalizada e em constante mutação.

A ligação das organizações a redes públicas e globais, como a Internet, não representa unicamente benefícios, mas também alguns riscos que advêm da abertura de mais uma porta da organização para o mundo exterior. Alguns dos riscos a ter em conta são: o acesso ilegítimo aos sistemas informáticos, é o uso abusivo, a falsificação de informação, entre outros possíveis. Não é que estes riscos não existam já dentro das empresas, mas com a ligação com outras redes, aumenta o número de pessoas com más intenções e consequente crescimento das falhas de segurança exploradas. A facilidade de utilização das ferramentas de ataque a sistemas informáticos, permite a pessoas com poucos conhecimentos explorar falhas de segurança, e com isso causar prejuízos às organizações. Ferramentas que permitem atacar milhares de endereços por hora e penetrar em sistemas desprotegidos. Analisando a facilidade de exploração de falhas existentes e o grande número de pessoas interessadas em explorá-las, as organizações necessitam de tomar medidas para se protegerem de forma a minimizar os riscos a que estão expostas.

Devido à natureza de certas informações nas organizações, a segurança da informação é um requisito crítico. Para estes casos é necessário analisar os aspectos básicos da segurança da informação:

- Autenticidade – o controlo de autenticidade está associado com a identificação correcta de um utilizador ou computador. O serviço de autenticação deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo.
- Confidencialidade – consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação.

- Integridade – consiste em proteger a informação contra modificação sem permissão explícita do proprietário da informação.
- Disponibilidade – consiste na protecção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis, assegurando ao utilizador o acesso à informação sempre que precisar.

Nas instituições financeiras como é o caso do Banco BPI, pela natureza da sua actividade, a segurança da informação é considerado um factor crítico. O valor da informação é dos mais elevados em comparação com outro tipo de organizações e o acesso ilegítimo a essa informação implica prejuízos tangíveis, mas ainda mais de prejuízos intangíveis, também mais difíceis de prever. Para além de estar em jogo o dinheiro da instituição, está o dinheiro dos clientes e respectivos dados confidenciais.

A implementação de mecanismos de controlo de acessos, garante acesso selectivo às redes de comunicações privadas e detecta possíveis ataques às respectivas redes. Os diferentes equipamentos existentes numa rede de computadores, como *firewalls, routers, switch,* permitem definir diferentes níveis de segurança, assegurando a segmentação da rede em várias partes. Este tipo de divisão da rede permite fazer o que se chama de defesa em profundidade, em que cada segmento possui o seu nível de acesso a diferentes recursos e que se um nível for comprometido, o nível seguinte ainda terá de ser ultrapassado e assim sucessivamente até atingir os sistemas críticos da organização.

A experiência "diz" que um sistema 100% seguro não existe, é só uma questão de tempo até alguém conseguir descobrir uma falha. Portanto, quando alguém conseguir obter acesso a um sistema ilicitamente é necessário saber o que foi feito, até onde o invasor conseguiu ir, o que conseguiu ver, em suma, até que ponto o sistema foi comprometido.

Os diversos equipamentos que constituem o sistema informático de uma organização registam as operações que são efectuadas. As aplicações permitem registar informações como entradas e saídas das mesmas. Os *routers* registam as ligações que recebem, com a origem e destino. As *firewalls* listam os acessos realizados e as tentativas de acesso negadas. Com estas facilidades parece fácil de resolver o problema de saber a que ponto um sistema foi invadido, mas se não houver o cuidado de assegurar a integridade dos registos gerados e o seu armazenamento de forma segura, a sua utilidade será nula.

Como qualquer organização o Banco BPI necessita de lidar com esta situação. O projecto com o titulo: "Exploração e gestão de logs de equipamentos de networking e segurança" pretende solucionar o problema. Antes do projecto, os eventos gerados pelos diferentes equipamentos eram armazenados em ficheiros de texto e/ou numa base de dados com pouco valor acrescentado. Estes, tinham como destino diferentes máquinas o que resultava na dispersão dos recursos e consequente dificuldade em gerir e relacionar os mesmos. Devido também ao pouco tempo disponível pelos administradores dos sistemas, a análise dos *logs* é feita de forma reactiva, quando existe algum problema vai-se analisar o que aconteceu. Se os registos estiverem dispersos em diferentes sistemas, a análise será um processo moroso, principalmente se for feito relacionando dados de diferentes fontes. Com a centralização dos eventos gerados pelos diferentes equipamentos num único sistema, ganha-se em facilidade de gestão, análise e poupança de tempo. Com a concentração dos fluxos gerados pelos *logs* na rede informática é necessário definir a arquitectura ideal e o processo de transporte desde os equipamentos até à máquina de destino, tendo em conta factores como eficiência e robustez.

Devido ao grande volume de dados que os diversos equipamentos monitorizados geram, é necessário definir um processo eficaz para armazenamentos dos eventos para análise a curto e longo prazo. Antes do projecto, o processo estabelecido era moroso devido aos vários sistemas dispersos, não oferecia garantia quanto à integridade dos dados armazenados e não tinha nenhuma politica definida, sendo esporádico e dependente do administrador responsável pelos equipamentos. Necessita-se portanto de especificar um processo que tenha em conta a especificidade do problema e se adeqúe à nova arquitectura montada.

Depois de montados os processos de recolha de eventos e armazenamento, põe-se o problema da análise dos mesmos. Devido ao enorme volume de dados, ao pouco tempo disponível dos administradores e à difícil "descodificação" dos *logs* em diferentes formatos, de diferentes equipamentos em locais com contextos diferentes é necessário encontrar formas automáticas de processamentos dos dados. Devido à complexidade envolvida, optou-se por analisar soluções já existentes que abrangem diferentes equipamentos e que estão preparados para lidar com grandes volumes de dados e extrair informação valiosa, poupando tempo e facilitando a gestão de infra-estruturas complexas como é o caso do Banco BPI.

1.3 Temas Abordados e Organização do Relatório

No presente relatório tentou-se seguir a estrutura proposta, mas devido à especificidade do projecto este foi reestruturado principalmente no que diz respeito aos capítulos sobre o trabalho desenvolvido.

Após este capítulo introdutório, em que se apresentou a entidade que acolheu o projecto de estágio, o contexto em que se insere o projecto e a estrutura adoptada. Será apresentado com maior pormenor, o problema a solucionar com o desenvolvimento do projecto.

De seguida, é especificado com um maior detalhe o problema concreto que o projecto pretende resolver. Quais as partes em que o projecto se divide e que tipo de equipamentos são abrangidos.

No terceiro capítulo são apresentadas as várias tecnologias relacionadas com o projecto, principalmente as várias opções a usar para efectuar o *logging* tais como o Syslog ou o SNMP (Simple Network Management Protocol).

No capítulo seguinte, expõem-se o desenvolvimento do projecto, dividido por 3 partes. A primeira sobre a arquitectura e implementação da recolha dos *logs*. A seguinte centra-se no armazenamento a longo prazo dos eventos para posterior análise. Na última parte faz-se a análise de soluções para a gestão de eventos de segurança.

Por último efectua-se o balanço do projecto de estágio, analisando os resultados finais e conclusões.

Em anexo, segue documentação relativa à aplicação que se desenvolveu para o *backup* dos *logs*.

2 Contexto do Projecto e Problema a Resolver

A segurança dos sistemas de informação de uma organização é de uma importância fulcral e requisito básico para que tenha alguma utilidade. A informação, matéria-prima dos sistemas de informação, deve ser protegida de forma a ser unicamente acedida pelos seus legítimos originários e destinatários; qualquer outro interveniente colocará a utilidade da informação em risco.

Os dados tratados nos sistemas informáticos passados de equipamento em equipamento estão sujeitos a anomalias de ordem técnica, a tentativas de intromissão de terceiros, a catástrofes, a defeitos, a uso indevido e muitos outros problemas possíveis. Com mil e um aspectos para pensar a ter em conta na implementação de qualquer sistema, esta tarefa é de uma complexidade deveras elevada. Para além dos problemas de ordem técnica, é necessário pensar em aspectos de natureza económica, já que o recurso Dinheiro é dos mais importantes a ter em conta e dos mais escassos.

Um factor a ter em conta na segurança da informação é o facto de muitas das vezes o valor da informação não compensar o investimento em sistemas para a sua protecção. Portanto, uma organização na implementação de qualquer sistema deve pesar todos os benefícios daí resultantes, bem como estudar o investimento a efectuar na implementação do mesmo. Os serviços de suporte também devem ser contabilizados, principalmente os serviços que garantem a segurança da informação, caso seja considerado um requisito essencial.

Outro conceito bastante pertinente na segurança da informação, adaptado da economia é a análise de risco, em que se identificam os activos da informação que a organização possui, bem como as ameaças e as vulnerabilidades que podem afecta-los, determinando a sua probabilidade de ocorrência e estimando o impacto no negócio. Os resultados da análise de risco ajudarão a organização a direccionar e determinar acções e prioridades mais adequadas, para uma gestão dos riscos de segurança da informação e a seleccionar os controles a serem implementados para a protecção contra estes riscos.

Sintetizando, na implementação de um sistema de informação e no que diz respeito à sua segurança devem ser tidos em conta os três aspectos seguintes:

- Riscos associados à falta de segurança;
- Benefícios;
- Custos de implementação dos mecanismos.

Num mundo digital e global como o de hoje, o dinheiro e o comércio possuem outra perspectiva que não a material. Os milhões de transacções, compras e vendas do dia a dia são efectuadas em grande parte sem recurso ao dinheiro físico, mas sim a ordens executados através de teclas e botões que originam um movimento de electrões que correspondem a bits e resultam numa troca de poucos a biliões de cêntimos. Devido a esta virtualização do dinheiro, as instituições financeiras necessitam de se certificar da segurança dos seus sistemas de informação em prejuízo de perderem clientes e consequente capital. Estas organizações possuem preocupações especiais ocupando um papel de destaque no investimento em segurança da informação.

Numa instituição como um banco, a segurança é cada vez mais uma prioridade, sendo necessário criar barreiras para proteger as transacções de informação internas e externas ao

banco. As comunicações electrónicas podem ser interceptadas e os dados copiados ou alterados, o que pode causar danos tanto através da invasão da privacidade dos colaboradores, como através da exploração dos dados interceptados. O acesso não autorizado a computadores e o software malicioso, como os vírus, podem incapacitar computadores e apagar ou alterar dados. Estes eventos externos podem comprometer a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos através da rede do banco.

Para além dos ataques externos, também existem factores internos de risco. O controlo de acessos a dados confidenciais e os processos de autenticação/autorização podem ser violados por utilizadores do próprio banco, mesmo que inadvertidamente. Esta situação tem originado tantos problemas às instituições, quanto as ameaças externas e que tem vindo a aumentar nos últimos tempos, mas mesmo assim é um dos problemas menos tidos em conta quando se monta uma estratégia de segurança de informação. A maior parte das organizações investe em equipamentos de segurança para fortalecer a periferia da sua rede interna, evitando estranhos de acederem aos recursos reservados aos colaboradores. Embora não possuam controlo sobre o que cada colaborador acede, negligenciando uma componente da segurança de informação fundamental. Actualmente, a maior parte das organizações preocupadas com as questões de segurança possui os seguintes sistemas implementados: *firewalls*, antivírus e as Virtual Private Networks (VPN); fundamentais na salvaguarda da segurança da informação, mas que possuem várias limitações em controlar o que se passa nos sistemas de informação como um todo.

A maioria dos sistemas de segurança como *firewalls*, IDS (Intrusion Detection Systems), encriptação, anti-virus possuem a abordagem de prevenir o acesso a pessoas estranhas a determinado recurso, da mesma forma que uma porta previne o acesso a uma casa. O problema está quando alguém pretende entrar na casa e vai conseguir por algum meio abrir a porta, obtendo acesso ao que se desejaria restrito. Caso haja algum mecanismo que detecte o comprometimento dos sistemas de prevenção, a intrusão será detectada e será efectuada uma acção de resposta, de forma a eliminar o acesso indevido. Se por outro lado não estiverem implementados mecanismos de detecção, o intruso não terá qualquer problema em efectuar as suas acções ilegítimas. A prevenção nos sistemas de informação efectuada com mecanismos falíveis está condenada ao insucesso, enquanto que os mecanismos de monitorização permitem alertar como que um alarme, para depois se poder responder activamente na fonte do problema de forma a corrigir qualquer falha e eliminar a ameaça.

A melhor forma de ter um sistema de informação o mais protegido possível, será através da implementação de sistemas de prevenção complementados por sistemas que monitorizem a rede, tal como as câmaras controlam as entradas e saídas de pessoas através de uma porta. Na ocorrência de qualquer falha na prevenção, deve-se despoletar acções de correcção e de contenção do problema. Portanto as três acções fundamentais inerentes à garantia de segurança num sistema informático serão: a prevenção, detecção e resposta.

O Banco BPI, como instituição financeira que é possui necessidade de assegurar a integridade dos seus sistemas de informação, sendo essencial a protecção dos dados relativos aos clientes e respectivas contas bancárias. Uma eventual falha relativamente à segurança acarreta prejuízos quanto à falha em si, mas também afecta a imagem da instituição caso o publico em geral tome conhecimento da ocorrência. A má publicidade gerada por um incidente de segurança de informação poderá ter consequências graves na relação dos clientes com a

instituição. Desta forma o Banco BPI implementou uma infra-estrutura que previne e controla os acessos aos sistemas de informação.

O universo de sites disponibilizados ao público por parte do Banco BPI é variado: www.bpinet.pt (site de *homebanking*), www.bpinetempresas.pt (*internet banking* para empresas), www.bpionline.pt (site de serviços de investimento), www.bancobpi.pt (informações sobre o banco, serviços e produtos), só referindo os de maior importância. Para além dos sites públicos, o Banco BPI possui uma intranet unicamente disponível para os seus colaboradores com diversas aplicações de acesso condicionado consoante as funções do utilizador. Quanto aos balcões, existe um acesso dedicado entre cada balcão e os pólos principais da rede (Porto e Lisboa) com acesso às aplicações bancárias. Os postos de trabalho e a maior parte dos sistemas de suporte assenta sobre a tecnologia Microsoft, mas também existem base de dados Oracle, sistemas baseados em HP-UX e em Mainframe.

O Banco BPI, devido à variedade de sites, de sistemas e complexidade de infra-estrutura, montou um sistema de informação que garante o acesso do público em geral, dos clientes e dos colaboradores de forma diferenciada, e protegendo a informação dos acessos ilícitos. A maneira encontrada para que isso funcione é através da implementação de sistemas que controlam o acesso dos utilizadores legítimos e recusam o acesso a pessoas não autorizadas. Ao nível da rede, os sistemas existentes para implementação da segurança são vários: segmentação da rede, *routers* com listas de acesso, *firewalls*, *proxys*, entre outros. Ao nível aplicacional existem as *passwords* de acesso aos diferentes sistemas, encriptação, certificados, para referir só os mais utilizados.

Para que uma rede de comunicações seja pensada de modo a defender a segurança dos dados em transmissão devem ser considerados as várias partes constituintes. Sendo assim, uma rede deve ser dividida nas seguintes partes: *router* de periferia que faz a primeira filtragem de pacotes da Internet, zona DMZ (Demilitarized Zone), que contem a parte pública da rede permitindo acessos vindo da Internet, rede interna onde correm as aplicações internas da empresa e rede de gestão.

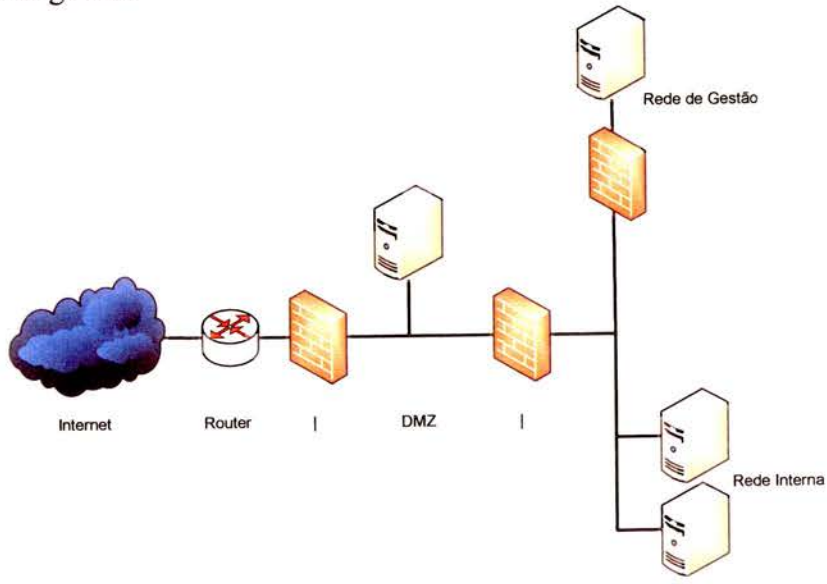


Figura 4 – Principais partes de uma rede

Para uma defesa em profundidade é necessário que cada uma dessas partes sejam separadas, protegidas e reforçadas, a ideia que o *router* de periferia com o *firewall*, por si só protegem a rede não faz sentido.

O Banco BPI na implementação da sua rede informática seguiu a mesma filosofia da defesa em profundidade, com uma arquitectura de rede constituída por diversas zonas com diferentes níveis de segurança. Por ordem crescente de segurança existe a rede pública em que se pode considerar a sua segurança nula pois não é possível controlar qualquer aspecto de quem acede ao quê. Um nível maior de segurança consegue-se entre o *router* e a primeira *firewall*, pois já se consegue implementar listas de acesso, mas muito pouco restritas. Entre a primeira *firewall* e a segunda *firewall* estão situados os servidores de acesso público como os serviços de DNS (Domain Name Service), correio electrónico e os sites públicos. De seguida pode-se encontrar a rede onde se encontram os servidores de suporte aos sites (*midleware*) como é o caso dos servidores de componentes COM. Por sua vez a camada de *midleware* acede aos servidores de base de dados que devem possuir o maior grau de segurança. Para além das redes de suporte ao negócio do banco, existe a rede destinada aos colaboradores do banco. Outra rede com um grau de segurança mais apertado é a rede de gestão, que é paralela às redes acima descritas, em que se situam as estações de gestão e de monitorização que possuem o objectivo de gerir e monitorar os vários equipamentos.

Devido à arquitectura montada os vários sistema necessitam de várias interfaces de rede, em que cada uma é ligada a uma parte da rede com funções distintas. O mais comum será que um equipamento possua três interfaces de modo a uma ficar ligada à rede mais insegura, outra a uma rede de maior segurança e a ultima ligada à rede de gestão. O tráfego que flui através de cada uma tem objectivos diferentes. A primeira serve para receber os pedidos vindos de equipamentos que possuem um nível de segurança inferior, as respostas saem pela mesma interface; a segunda permite ao equipamento direccionar o pedido para um equipamento com maior nível de segurança caso o pedido seja aceite; a terceira permite que o administrador aceda ao equipamento de forma segura para a sua configuração. Esta também serve para que os dados de monitorização sejam enviados para as estações de gestão.

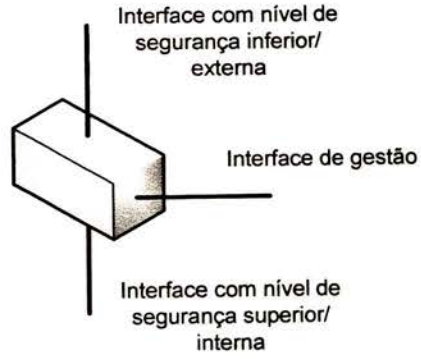


Figura 5 – Interfaces típicas de um equipamento numa rede

Na administração dos sistemas informáticos do Banco BPI as redes de gestão devem possuir um grau de segurança elevado, devido a uma intrusão aos sistemas aí localizados permitirem um acesso e alteração dos serviços de toda a rede. O tráfego que circula nestas redes é importante, também devido à informação que transporta sobre a própria infra-estrutura.

No presente projecto a infra-estrutura objecto de estudo, foi a rede que suporta o acesso dos colaboradores do Banco BPI aos serviços relacionados com ligação à Internet, como é

exemplo do acesso *web* e correio electrónico. Para além da rede de acesso à Internet, o projecto beneficiou a rede que suporta o site público www.bpionline.pt, alojado na cidade do Porto e que sofreu uma reestruturação durante a realização do estágio. Com esta reestruturação da rede do Banco BPI surgiu a necessidade de melhorar a monitorização da mesma, garantindo uma maior segurança da sua infra-estrutura.

O Banco BPI na sua infra-estrutura possui várias redes, cada uma com os seus recursos e objectivos. Por causa do modelo de implementação de sistemas de informação existentes no banco em que um projecto passa por várias etapas, desde o desenvolvimento, qualidade, pré-produção e produção; existe a rede de produção com o site www.bpionline.pt de acesso público e existe uma outra rede de pré-produção onde está reflectida a rede de produção e esta serve para efeitos de testes de procedimentos de actualização e a testes de carga.

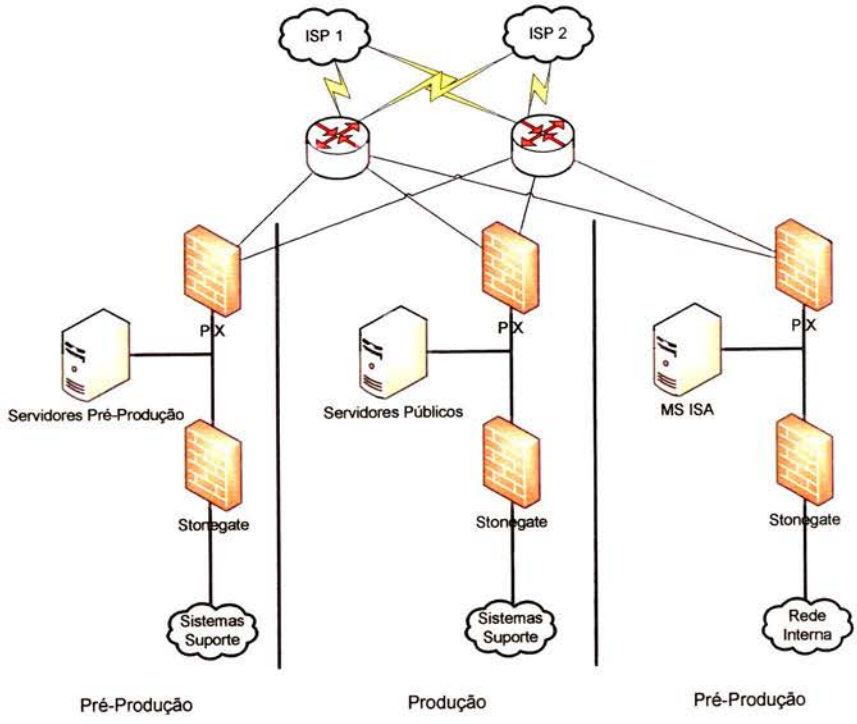


Figura 6 – Esquema simplificado da rede Banco BPI do Porto

A monitorização de uma rede de computadores é efectuada através de vários serviços que cada equipamento disponibiliza para o efeito. Uns dos mais importantes são os *logs*, disponíveis nos mais diversos equipamentos desde *routers*, *firewalls*, aplicações, servidores, entre outros. Mas afinal o que é um *log*? Nada mais do que um conjunto de dados que indicam o momento exacto em que determinada acção aconteceu num sistema. Por exemplo, numa *firewall* um *log* conterá a hora a que determinado IP acedeu a um determinado IP, isto se for tráfego permitido. Geralmente um *log* é apresentado como texto standard ASCII com vários campos, que segue um formato próprio do equipamento que o gerou e também com um significado particular. Devido à variedade de equipamentos com capacidade de *logging* não existe um formato 100% aceite. Para complicar, os *logs* gerados não são de fácil leitura e só quem estuda em pormenor determinado equipamento e os seus *logs*, os pode perceber.

Os *logs* possuem dados vitais para o diagnóstico de problemas e para a monitorização dos sistemas de informação. Estes são a fonte onde o administrador vai beber quando detecta alguma anomalia. Caso não tenha *logs*, não saberá o que aconteceu e não poderá resolver ou

prevenir uma nova falha. A análise dos *logs* é uma tarefa fundamental na administração de qualquer sistema devido à informação preciosa que disponibiliza sobre a correcta utilização dos recursos informáticos e como tarefa fundamental, deveria de ser efectuada numa base no mínimo semanal. O problema é que são poucos os administradores de sistemas que se dão ao trabalho de olhar para os *logs*, principalmente porque muitos não os percebem e também porque possuem outras tarefas que lhes parecem mais importantes e mais urgentes. Desta forma os *logs* na maior parte dos casos são consultados quando se detecta qualquer problema. Um factor que não abona a favor da consulta dos *logs* é a elevada complexidade e tempo necessário para filtrar o que interessa. Esta situação é grave porque certos problemas só são detectados pelos utilizadores muito depois de terem ocorrido as acções que originam a anomalia, e esta prolonga-se até ser detectada. Situação que se agrava mais quando de segurança de informação se trata.

Como existem os mais diversos equipamentos e aplicações a gerar *logs*, por muito poucos bytes que cada um crie, esse valor multiplicado por muitos, causa problemas no armazenamento desses eventos a longo prazo e também de largura de banda disponível, pois passava-se a necessitar de mais tráfego para monitorização, afectando o desempenho da rede para o negocio que a organização desenvolve. Portanto é necessário encontrar o equilíbrio entre a informação que se pretende com os *logs* e a percentagem da capacidade a usar para efeitos de monitorização. Relativamente ao armazenamento a longo prazo terá interesse que os *logs* sejam guardados por vários anos porque possuem valor como meio de prova para apresentar em instâncias legais caso haja algum acesso ilegítimo ou como prova que certo acesso foi efectuado a certo equipamento.

Embora o Banco BPI possuísse um conjunto de equipamentos a efectuar a monitorização e armazenamento dos *logs* dos equipamentos de segurança e de rede, a sua utilização não era a melhor, existindo diversos problemas que se tentaram solucionar com o presente projecto.

Em termos de equipamento de rede e de segurança o Banco BPI possui vários equipamentos. Os que possuem maior importância na monitorização da segurança do sistema são os *routers* da Cisco, as *firewalls* Cisco PIX, as *firewalls Stonegate* da Stonesoft e o Microsoft Internet Service Acelerator (ISA) que possui funcionalidades de *firewall* e de proxy. Para além destes existem ainda *switches*, servidores com serviços de suporte como DNS, ou com serviços desde *mail* até aos servidores de web para o site público, todos com capacidades de gerar *logs* das suas actividades.

Antes do projecto os administradores dos sistemas configuravam os equipamentos de forma isolada. A título de exemplo, existem várias Cisco PIX e estas encontravam-se a enviar os *logs* para vários servidores que recebiam os *logs* através do protocolo de syslog, que se explica de seguida em pormenor. Para além das PIX, existem os produtos *stonegate* que faziam o *logging* unicamente para um servidor de *logs* do próprio produto e também existia o MS ISA 2000 que fazia o seu *logging* para ficheiros de texto.

Devido a existirem diversas abordagens foi mais fácil para os administradores configurar a monitorização dos equipamentos de forma isolada, em que cada um envia ou armazena os *logs* à sua maneira. Com esta situação levanta-se o problema da gestão destes vários equipamentos a reportar para locais diferentes, em que para fazer uma análise completa de uma situação será necessário muito tempo a percorrer as várias máquinas a analisar *logs* complexos e tentar relacionar os dados que cada um reporta. Com esta situação chega-se a uma conclusão óbvia, que são os benefícios que resulta da implementação de uma

arquitectura que centraliza o envio dos *logs* para um único sistema, facilitando a análise e gestão dos *logs*.

Com a centralização dos *logs* para um único sistema existem questões que necessitam de ser analisadas. Inicialmente tem que se determinar quais os equipamentos que são relevantes enviarem os *logs*, dependendo do seu tipo, mecanismos de enviar os *logs* para outros equipamentos e da sua importância na segurança da rede. Outro problema que é necessário resolver é o transporte dos *logs* desde os equipamentos que os geram até ao servidor final, em que é necessário determinar se existe capacidade em termos de largura de banda, as particularidades dos métodos de transporte de *logs* de cada equipamento e a robustez e segurança do processo. Em suma, qual a melhor arquitectura que deve ser montada na centralização dos *logs*. Esta questão necessita de ser bem pensada devido aos mecanismos de monitorização serem um dos alvos de ataque dos invasores de sistemas por causa das pistas que deixam nos *logs*.

Uma outra questão que é relevante na gestão dos *logs* é a informação que estes possuem sobre acessos por parte dos utilizadores dos sistemas e da relevância destes para a prova de situações anómalas, como a intrusão num sistema. O Banco BPI na sua actividade sente a necessidade de monitorar os vários equipamentos para que se algo de mal acontecer e caso seja necessária a intervenção de entidades fiscalizadoras, judiciárias ou outras existam dados que contenham valor como prova apresentável nas instâncias judiciais. Por causa desta necessidade existe o problema extra de guardar de forma racional em termos de espaço físico e economicamente viável os *logs* gerados em vários anos por vários equipamentos. Este problema coloca-se porque dependendo do detalhe do nível de *logging* um único equipamento é capaz de gerar centenas de MB de *logs* por dia, portanto, no final de uma semana resulta em GB e em vários anos pode chegar a vários TB. A questão quanto ao armazenamento dos *logs* a longo prazo possui custos e processos próprios que a cópia de segurança de uma base de dados não levanta. Ter os *logs* dos equipamentos de segurança e de *networking* armazenados por vários anos é uma segurança que o Banco BPI deve ter, caso seja detectado um problema com algum tempo e que mereça prova oficial.

Antes deste projecto os *logs* das *firewalls* PIX e Stonegate, bem como os *logs* do Microsoft ISA, eram armazenados de forma mais ou menos periódica, mas através de um processo manual. Portanto não existia uma política de cópias de segurança definida, a não ser a cópia dos *logs* para DVD, de uma forma manual e em que só a pessoa que executou essa cópia é capaz de saber onde encontrar determinados *logs*, caso seja necessário recuperar para análise. Outro problema com a cópia dos *logs* para um único DVD é o risco que se corre de perder os *logs*, se acontecer alguma falha no processo de gravação ou falha no próprio suporte de armazenamento. Pretende-se que haja um processo bem definido, que resolva alguns problemas, que melhore os processo montados e que seja transparente para todos os intervenientes na administração destes sistemas.

Embora as questões de arquitectura de armazenamento dos *logs* a curto e longo prazo sejam necessárias e de importância capital para o sucesso do projecto, a componente de análise automática de *logs* e em tempo real possui mais valias, comparativamente à analise dos *logs* efectuada de uma forma manual. Devido à complexidade envolvida e na diversidade de *logs* existentes, o projecto possui uma outra componente de análise de soluções existentes no mercado que solucionam a análise em tempo real dos *logs* dos diversos equipamentos existentes na infra-estrutura do Banco BPI. Mesmo depois de implementados os processos de centralização e armazenamento, o processo de análise encontra-se dependente do tempo

disponível dos administradores dos sistemas para olharem para os *logs*. Devido à grande complexidade dos *logs* será necessário investir sempre muito tempo na análise destes. Se for implementada uma solução que analise os *logs* em tempo real e que gere alertas com diferentes prioridades, os administradores poderão atempadamente efectuar respostas aos incidentes que estejam a ocorrer naquele momento e conter a situação num nível de pouco comprometimento. Desta maneira, as ferramentas existentes no mercado necessitam de ser avaliadas e caso as funcionalidades se adaptem às necessidades dos sistemas de informação do banco BPI, deverão ser testadas e recomendas para aquisição.

De uma forma geral a problemática de gestão de *logs* numa infra-estrutura necessita de ser abordada por ser fundamental para a resolução e prevenção de imensos problemas. O Banco BPI com o presente projecto pretende melhorar os processos de modo a não ter surpresas desagradáveis, e colocar em perigo um bem essencial para uma organização como são os recursos informáticos e a informação que flui através destes.

3 Revisão Tecnológica

Para que se percebam muitas das questões que se levantam com os procedimentos de recolha, transporte, armazenamento e análise dos *logs* é necessário que se apresentem as diversas tecnologias que se relacionam com a gestão de todos estes processos. Existem certos protocolos que se devem entender as suas particularidades para que se chegue a uma solução óptima do problema. Apresentam-se também alguns equipamentos existentes na infra-estrutura do Banco BPI, que são objecto de monitorização, analisando em maior detalhe os mecanismos que disponibilizam para o *logging* de eventos.

3.1 TCP versus UDP

As redes baseadas no protocolo IP (Internet Protocol) são as mais utilizadas actualmente e com maior ascensão nos últimos anos. A infra-estrutura implementada no Banco BPI, serve-se do protocolo IP para ligar os vários equipamentos, isto ao nível da camada de rede. Geralmente acima do IP tem-se os protocolos de transportes TCP (Transmission Control Protocol) e UDP (User Datagram Protocol) que entregam os dados desde a origem até ao destino, cada um com as suas vantagens e defeitos.

O protocolo TCP é um protocolo baseado em conexões, inicialmente estabelece-se a ligação com o destino, faz-se a transferência de dados e por ultimo termina-se a conexão. Este possui mecanismos de controlo quanto à garantia de entrega dos pacotes ao destino bem como a chegada dos pacotes pela ordem correcta, para além da detecção de erros nos pacotes e de pacotes duplicados. Cada pacote possui um número de sequência e caso algum chegue fora de ordem, pede-se à origem que retransmita o pacote em falta. Para além da conexão origem-destinatário, existe outra que faz a ligação no sentido inverso, isto dependendo da aplicação. Como desvantagens o protocolo TCP não se direcciona para aplicações que necessitam de dados em tempo real, como por exemplo aplicações baseadas em *streaming* de áudio ou vídeo e o VoIP (Voice over IP) em que é preferível ignorar um pacote em falta do que esperar pelos pacotes na ordem correcta. Outra coisa contra é a implementação complexa que tem e que origina problemas na adopção em equipamentos com poucos recursos como é o caso de equipamentos baseados em circuitos e com pouca "inteligência".

Relativamente ao protocolo UDP ao contrário do anterior, não é baseado em conexões, mas sim em envio de datagramas que possuem dados suficientes para fazerem o caminho desde a origem até ao destinatário, sem necessidade de efectuar qualquer estabelecimento de conexão. O UDP não possui mecanismos como o TCP de garantia de entrega dos dados, da ordem correcta de chegada e de controlo de congestão, mas possui o mecanismo de validação de erros, embora não retransmita os pacotes com problemas. Caso se pretenda ultrapassar estas limitações será necessário implementar estas funcionalidades na camada de aplicação ou usar o protocolo TCP. Como vantagens o protocolo UDP possui uma implementação simples, é muito rápido e adapta-se bem a aplicações que necessitem de dados em tempo real.

3.2 Syslog

Syslog é um standard para encaminhamento de *logs* ao longo de uma rede IP, desde o equipamento gerador do *log*, onde aconteceu o evento, passando por várias máquinas que receberam o *log*, o guardaram e/ou reencaminharam para uma outra máquina. Este protocolo

foi implementado tendo em vista a simplicidade e flexibilidade de utilização. Originalmente foi usado em sistemas BSD, Unix e Linux, sendo actualmente usado nos mais diversos equipamentos como *router* e *firewalls*. O protocolo é baseado no protocolo UDP e normalmente a porta que usa é a 514, existem também implementações do protocolo sobre TCP para que seja mais robusto, mas ainda não existe um standard para a sua implementação. Devido a ser baseado em UDP possui as mesmas limitações deste pois não existem garantias da entrega dos *logs*, mas em contrapartida é simples e rápido.

O limite de tamanho para um pacote syslog é de 1024 bytes e este é constituído por 3 partes: no início aparece a prioridade do *log*, que é um número entre 0 e 165, em que o menor possui maior grau de urgência; a seguir vem o cabeçalho que contem a data e hora da ocorrência do evento e o IP ou nome do equipamento que gerou o *log*; por ultimo aparece o conteúdo do *log*, em que está descrito o evento que aconteceu, neste campo não existe definição rigorosa sobre o formato a seguir pois cada equipamento possui o seu tipo de *logs*. O protocolo de syslog possui a flexibilidade para ser implementada nas mais diversas arquitecturas de redes, estando até previstas no seu RFC (Request for Comment 3164) várias cenários de implementação e que se apresentam de seguida.

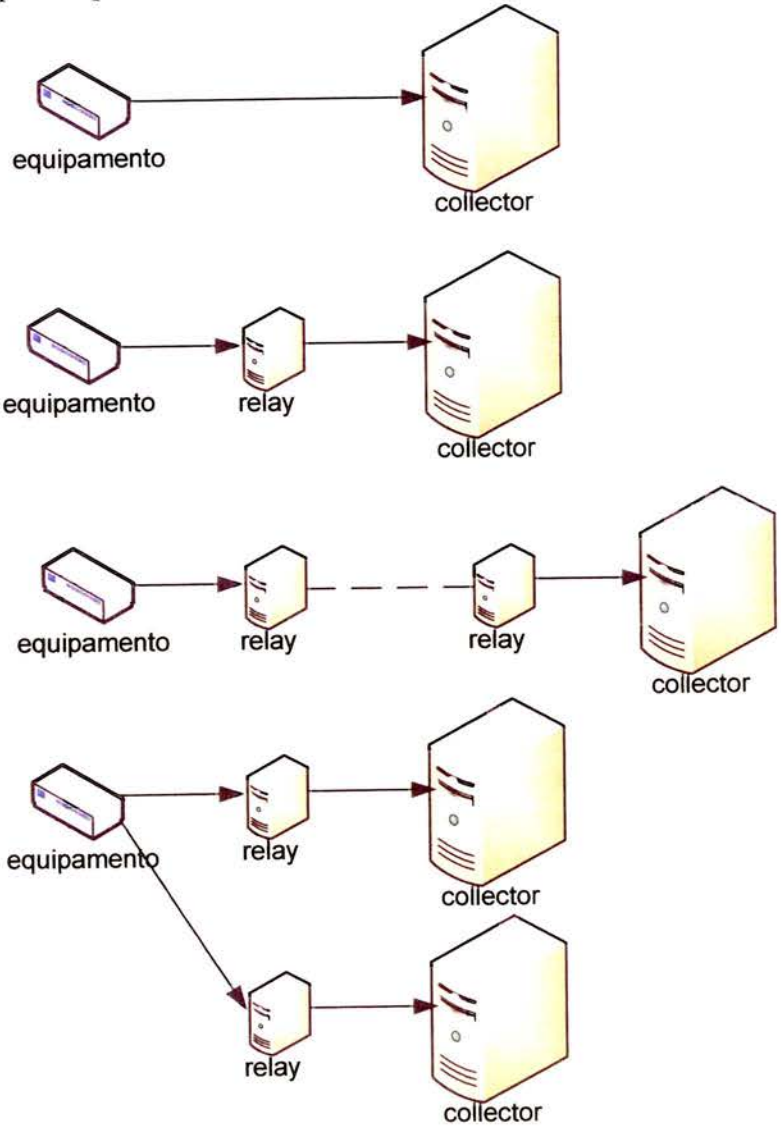


Figura 7 – Algumas arquitecturas possíveis com syslog

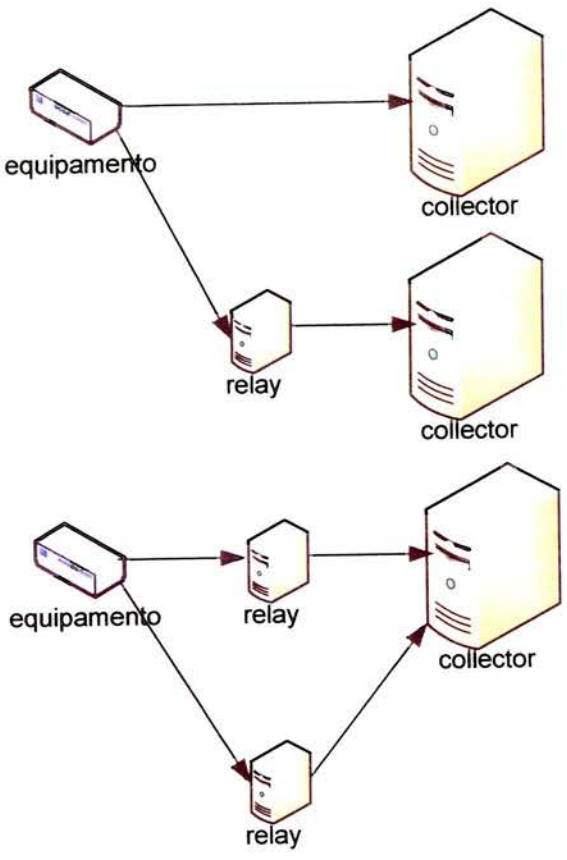


Figura 8 – Algumas arquitecturas possíveis com syslog (continuação)

O syslog apresenta determinadas desvantagens que devem ser consideradas aquando da sua implementação. Este protocolo não permite controlar por si só quais os dispositivos que vão enviar *logs* para determinado syslog server. Outra situação que pode acontecer é um equipamento estar a enviar *logs* para uma máquina que não existe ou que está com o serviço de syslog em baixo, sem que haja qualquer problema detectável para o emissor do *log*.

3.3 SNMP – Simple Network Management Protocol

O protocolo SNMP (Simple Network Management Protocol) foi desenvolvido com o objectivo de permitir a gestão e monitorização dos mais diversos equipamentos de redes de computadores. Para além da diversidade dos equipamentos foi desenhado para suportar o maior número de protocolos possíveis e permitir uma implementação generalizada em qualquer equipamento de rede. Para além do SNMP, que basicamente é o protocolo que serve para obter e alterar parâmetros de um equipamento, existem outros protocolos associados que especificam como a informação se encontra organizada. Cada equipamento que suporte SNMP possui dados relativos aos parâmetros de configuração, às estatísticas de cada interface de rede, contadores de eventos, as mais diversas informações possíveis. Os dados encontram-se estruturados numa espécie de árvore, em que cada folha possui um determinado significado. Esta organização dos dados é especificada através da notação Abstract Syntax Notation One (ASN.1) que descreve os vários objectos constituintes da MIB (Management Information Base), que é o nome dado à base de dados lógica suportada pelos equipamentos que suportam SNMP. A maior parte das MIBs é standard, mas existe a possibilidade de cada fabricante ter os seus objectos específicos dos seus equipamentos, pendurando essa informação no local reservado para esse efeito.

O SNMP possui uma arquitectura do tipo cliente-servidor, constituída por diferentes entidades, cada uma com as suas particularidades e funções. Os dispositivos geridos possuem implementado um agente SNMP que suporta os parâmetros de configuração, dados sobre o estado do equipamento e diversas estatísticas. Quando solicitado, o agente deve responder aos pedidos de outra entidade (o gestor), mas também deve reportar anomalias quando estas acontecerem. O gestor ou NMS (Network Management Station) é a entidade que gere um ou mais agentes, enviando pedidos, alterando parâmetros, recebendo as respostas a pedidos e recebendo as anomalias reportadas pelos agentes. Na interacção entre gestor e agente existe um conjunto de pedidos e respostas que estão especificadas no protocolo SNMP. Quando o gestor quer obter um objecto presente na MIB do equipamento envia uma mensagem do tipo: "*Get Request*". Com o mesmo objectivo, mas com a particularidade de enviar objectos seguidos consoante a ordem do utilizador, existe a mensagem do tipo: "*GetNext Request*". Em resposta a um pedido por parte do gestor ao agente, este último envia uma mensagem do tipo "*Get Response*" com os dados pedidos. Para alterar algum parâmetro no equipamento o gestor envia uma mensagem "*Set Request*" com o novo valor a ser tomado pelo objecto. Para o agente enviar de forma assíncrona qualquer parâmetro existe a mensagem "*Trap*" que é usada quando algum valor ultrapassa certo intervalo ou quando determinado evento ocorre. Para além deste tipo de mensagens enviadas entre agentes e gestor, com novas versões do SNMP (versão 2, versão 2c e versão 3) surgiram novos tipos de mensagens como a "*GetBulk Request*" e "*Inform*".

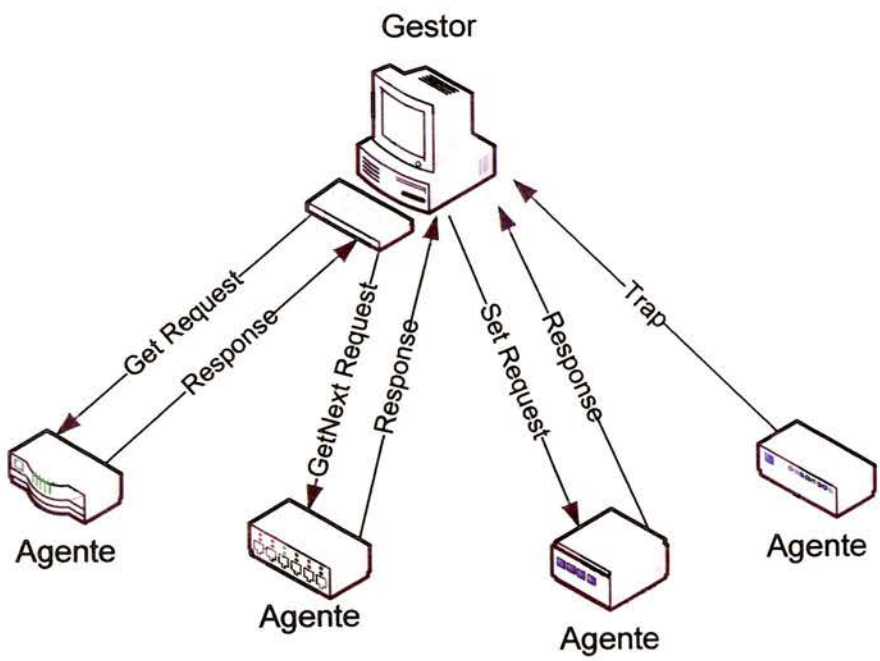


Figura 9 – Arquitectura e principais mensagens do SNMP

Ao longo da vida do protocolo SNMP têm vindo a ser feitas várias actualizações, devido a algumas falhas, maioritariamente relacionadas com a segurança. A versão 1 do protocolo usava uma *password*, conhecida como *community string*, que era transmitida em *clear text* ao longo da rede. Com a versão 2 do SNMP tentou-se incrementar a segurança, mas não foi aceite pelo mercado devido à sua complexidade. Uma outra versão do SNMP é a 2c que segue a mesma filosofia de *community string* da versão 1, acrescenta novas mensagens que permitem obter vários objectos num pedido, entre outras melhorias. O SNMP versão 3

standard com a data de 1998 acrescenta grandes alterações ao protocolo com o controlo de acesso baseado em utilizadores, faz uso de encriptação e altera a arquitectura das versões anteriores, isto a custo do aumento da complexidade do protocolo.

O SNMP como o syslog é baseado no protocolo de transporte UDP, mas também poderá ser usado sobre outros protocolos como o TCP ou X25. A porta que geralmente é usada para o agente receber os pedidos do gestor é a 161 e o gestor recebe geralmente os *traps* pela porta 162.

3.4 MD5 - Message-Digest algorithm 5

O algoritmo MD5 é um dos mais utilizados na geração de *hashes* seguras, em particular no standard de autenticação de mensagens na Internet. A sua utilização permite uma relação única entre a mensagem original e o valor de *hash*, que pode ser encarado como uma assinatura digital da mensagem. Assim, é possível substituir a autenticação de uma grande mensagem ou documento pela autenticação de um pequeno valor de *hash*.

O MD5 é um algoritmo para obter *hash* de mensagens desenvolvido por Ron Rivest no MIT. O algoritmo aceita como entrada uma mensagem de tamanho arbitrário e produz como saída 128 bits (4 palavras de 32 bits) que representam um valor de *hash* da mensagem de entrada e que pode ser encarado como uma assinatura digital da mensagem.

Calculada uma *hash* em função de determinada *string* de entrada, e caso seja necessário certificar-se que a *string* permanece inalterada, deve ser calculada a *hash* da *string* que se quer comprovar inalterada e comparada com a *hash* calculada originalmente. Caso as *hashes* sejam iguais, pode-se chegar à conclusão que a *string* é a mesma. Portanto, o algoritmo MD5 com entradas iguais gera saídas iguais e com entradas diferente gerará *hashes* diferentes, mesmo que as alterações sejam mínimas, como se pode observar nos seguintes exemplos:

- String de entrada: "log1" hash MD5: 23848b5f8ebf7d1342f06722f8f73302
- String de entrada: "log2" hash MD5: 7b1a5a4dd8df61dc8e4ea38fa24f4490
- String de entrada: "mog1" hash MD5: e637d2a2136002e352832388e69863e6
- String de entrada: "log11" hash MD5: 46fe60d33485458a4465389f13392460
- String de entrada: "log1" hash MD5: 23848b5f8ebf7d1342f06722f8f73302

Actualmente o algoritmo MD5 já não é considerado *collision free* devido a terem sido encontradas entradas diferentes, que resultam na mesma *hash*, mas tal situação não é de todo vulgar, sendo este algoritmo considerado seguro.

Para além do algoritmo MD5 existe o algoritmo MD4 que é menos seguro que o MD5, mas com maior desempenho e o SHA-1 considerado mais seguro, mas que possui pior desempenho.

3.5 Cisco Routers

Um *router* é um equipamento usado para fazer a comunicação entre diferentes redes de computadores. Este equipamento permite a comunicação entre computadores distantes entre si e até mesmo com protocolos de comunicação diferentes.

Os *routers* são dispositivos que operam na camada 3 do modelo OSI de referência. Estes têm como principal objectivo seleccionar a porta mais apropriada para encaminhar os pacotes

recebidos. Ou seja, enviar os pacotes para o melhor caminho disponível para um determinado destino. De uma forma simplista um *router* permite inter-ligar diferentes redes, ao contrário dos *switches* que ligam vários nós de uma LAN (Local Area Network).

Com o fim de distribuir pacotes, um *router* comunica com outros *routers* usando protocolos de *routing* e usa essa informação para criar e manter uma tabela com as redes que conhece e a porta de destino a usar quando pretende enviar um pacote para as mesmas. A tabela de encaminhamento armazena as melhores rotas para determinados destinos da rede, as métricas associado com aquelas rotas, e o trajecto ao *router* seguinte.

Um subtipo de *routers* existentes são os *switches* de nivel 2 e 3 que possuem as funcionalidades de um *switch* (camada 2) e de um *router* (camada 3). Existem também *routers* capazes de fazerem o *routing* entre vários protocolos, como por exemplo, entre redes IP e redes ATM (Asynchronous Transfer Mode).

Os *routers* do fabricante Cisco para além das capacidades de *routing* possuem a funcionalidade de permitir ou negar tráfego vindo de uma rede, intervalo de IPs ou até de um único IP. Os *routers* de perímetro fazem a ligação entre a rede privada e a rede pública através destas funcionalidades executando a primeira filtragem do tráfego permitido ou negado, para isso devem ser configurada devidamente as listas de acesso (*access lists*). Para além da filtragem das redes pode ser feita a filtragem sobre o protocolo, através dos cabeçalhos dos pacotes que contem as portas de destino, esta funcionalidade está implementada através das listas de acesso estendidas. Ao implementar as listas de acesso num *router* Cisco existe a possibilidade de efectuar o *logging* da aplicação de uma regra específica. A filtragem do tráfego ao nível do *router* é muito importante porque a aplicação das regras no tráfego que chega a este equipamento é feito de forma bastante rápida, poupando as *firewalls* desta tarefa isto porque são mais lentas na filtragem que fazem.

Em termos de monitorização os *routers* Cisco possuem a capacidade de gerar *logs* de diferentes tipos de eventos e grupos de eventos, consoante a prioridade e o nível de *logging* que o administrador de rede pretender. Os *logs* podem ser reencaminhados para outras máquinas através de *traps* SNMP ou através de syslog, por UDP ou TCP. O *router* pode ser configurado para enviar os *logs* para mais do que uma máquina, obtendo assim redundância de *logs*.

3.6 Cisco PIX

O equipamento Cisco PIX (Private Internet Exchange) é uma *firewall* do fabricante Cisco. Dos diferentes tipos existentes de *firewall* esta trabalha ao nível da camada de rede, mas mantém o estado das conexões de rede, portanto é considerada uma *firewall* de estado. Este tipo de *firewall* não faz a filtragem dos pacotes analisando só o trinómio origem-destino-protocolo, mas também analisa o estabelecimento das conexões, guarda o estado de cada nova conexão permitida deixando fluir os pacotes que estejam dentro da sequência e aquando da terminação da conexão elimina-a das conexões permitidas. As *firewalls* de estado possuem vantagens relativamente a outro tipo de *firewalls* relativamente à sua velocidade e consistência. As *firewalls* que analisam todos os pacotes ao nível da aplicação causam lentidão no tráfego que passa nesta devido ao tempo gasto no processamento de todos os pacotes. As *firewalls* de filtragem de pacotes devido a não possuírem controlo de estado estão sujeitas a pacotes forjados que não são detectados, mas possuem a seu favor a velocidade.

A *firewall* Cisco PIX possui diversos modelos, cada um com a sua capacidade relativamente ao número de sessões estabelecidas em simultâneo e o débito máximo de tráfego. Para além das capacidades de *firewall* este equipamento possui suporte para estabelecimento de VPNs (Virtual Private Network).

Quanto à monitorização dos eventos ocorridos na PIX, como no caso dos *routers* da mesma marca, existe suporte para os protocolos SNMP e syslog. Como nos *routers* os *logs* da PIX podem ser encaminhados para um servidor de *logs*, consoante a sua prioridade. O administrador do equipamento tem ao seu dispor a possibilidade de fazer o *logging* de todos os eventos que ocorrem no equipamento ou só os de determinado tipo ou só os de maior urgência.

3.7 Stonesoft Stonegate Firewall

A Stonegate Firewall como o nome indica é uma *firewall*, mas ao contrário da *firewall* PIX, este equipamento analisa os protocolos de aplicação e também o estado das conexões. Devido à sua arquitectura esta *firewall* permite obter o melhor das *firewalls* com estado e das *firewalls* de aplicação pois se necessário analisa todo o pacote, ou se não se justificar analisa unicamente a conexão através do seu estado e dos pacotes esperados, desta maneira permite obter bons débitos e bom nível de segurança nas comunicações mais criticas ou problemáticas. A firewall Stonegate é desenvolvida pelo fabricante Stonagete e para além das capacidades de *firewall* permite implementar VPNs baseadas em IPsec, outra funcionalidade permitida é o NAT (Network Address Translation).

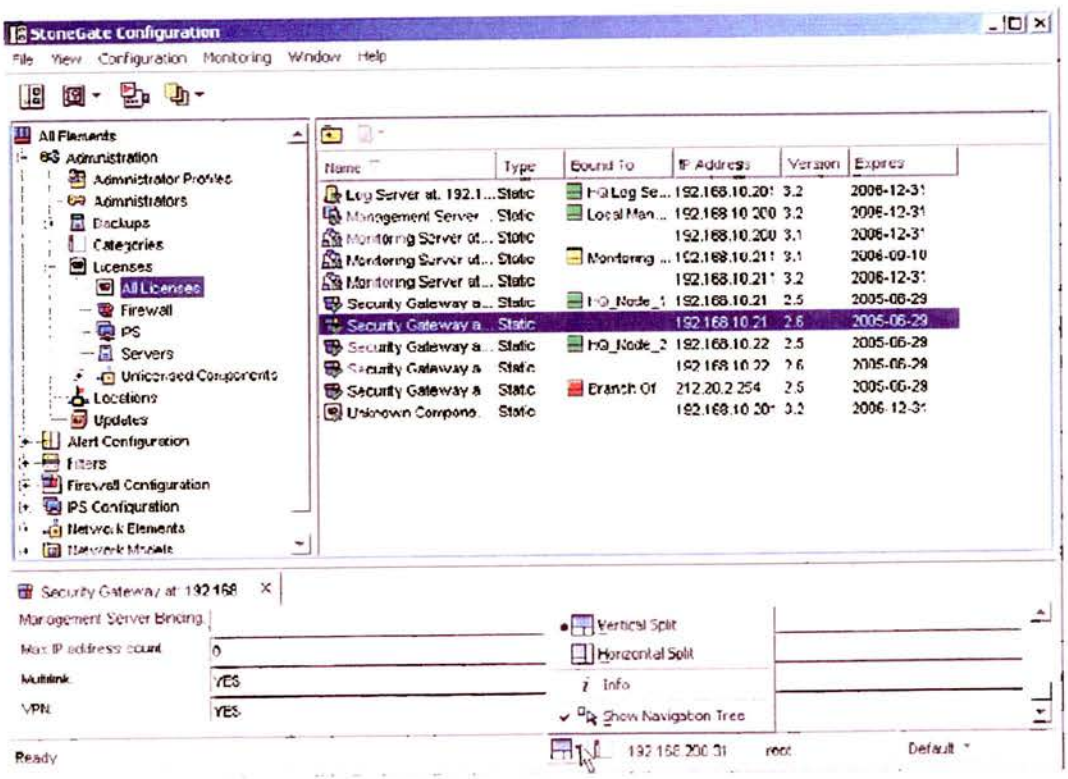


Figura 10 – Interface de configuração da *firewall* Stonegate

Ao contrário da PIX que é independente de qualquer estação de gestão e de servidor de *logs*, a Stonegate foi desenvolvida para correr num computador que corre os serviços de *firewall*, e para além desta máquina existe uma outra que gere a *firewall* e também um servidor de *logs*

dedicado para esta solução. A *firewall* em si é baseada no sistema operativo Linux e executa a filtragem dos pacotes que passam por esta. O motor da *firewall* necessita de ter ligada uma máquina que tem como função a configuração e gestão de interface entre a *firewall* e o administrador. Para alem da estação de gestão a Stonegate possui um servidor de *logs* próprio que recebe todos os *logs* do motor da *firewall* e que pode armazenar, descartar, encaminhar e arquivar os *logs*. Quando o administrador necessita de consultar os eventos ocorridos, nesta solução poderá efectuar consultas numa interface amigável que é disponibilizada, caso os *logs* estejam armazenados no servidor de *logs* próprio.

A firewall Stonegate possui a funcionalidade de enviar os *logs* que vai gerando para dois formatos: XML (Extensible Markup Language) e CSV (Comma-Separated Value), de uma forma programada. Existe também a possibilidade de encaminhar os *logs* para um servidor de *logs* externo, neste caso usando o protocolo syslog. Caso não se deseje encaminhar os *logs* para outro servidor, de *logs* da solução permite arquivar uma grande quantidade de *logs*, devido à capacidade de compressão.

3.8 MS ISA - Microsoft Internet Security and Acceleration Server

O Internet Security & Acceleration (ISA) Server 2004 da Microsoft, é um produto que engloba diversas funções, mas as que mais se destacam são as funcionalidades de *firewall*, VPN e de proxy. A Microsoft defende que os benefícios chave do ISA Server 2004 incluem as suas capacidades avançadas de protecção, a sua facilidade de utilização e o fornecimento de acesso rápido e seguro à Internet.

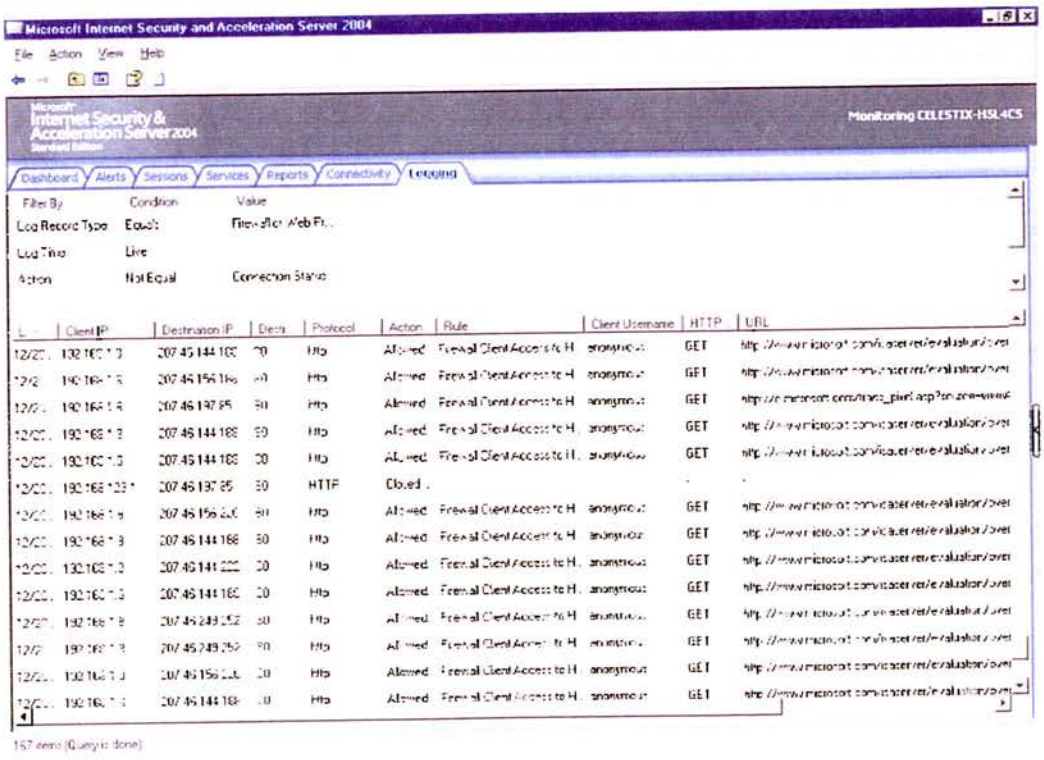


Figura 11 – Visualização de *logs* no MS ISA 2004

O ISA Server é oferecido em duas edições, Standard Edition e Enterprise Edition. Ambas possuem o mesmo conjunto de funções no entanto, a edição Standard é voltada para um servidor único, já que para implementações em larga escala com suporte para *clusters* de servidores, é necessário o ISA Server Enterprise Edition.

A componente *firewall* do MS ISA 2004, tal como a firewall Stonegate, possui uma abordagem de análise de pacotes e seu estado e inclui funcionalidades de analise de pacotes ao nível aplicação. Como já foi referido esta abordagem tem a vantagem de ser mais robusta e segura, mas tem como desvantagem a diminuição do desempenho quando a análise dos pacotes é feita de forma minuciosa.

No que diz respeito à componente de proxy o MS ISA permite optimizar a largura de banda, fazendo a cópia dos recursos mais visualizados pelos utilizadores de uma organização para *cache*, e quando for necessário aceder a esse conteúdo o proxy disponibiliza os dados locais poupando um recurso precioso como a largura de banda. Esta abordagem possui benefícios na economia de recursos e também da rapidez de acesso aos conteúdos uma segunda vez que estes já se encontram em *cache*. Para além das funcionalidades de *caching* o MS ISA na componente proxy permite filtrar determinados conteúdos acessíveis por parte dos colaboradores internos e também monitorar quais os conteúdo a que cada utilizador acede.

Os eventos que ocorrem no ISA server podem ser armazenadas de diferentes formas, através do armazenamento dos *logs* numa base de dados local que é suportada pela aplicação MSDE uma base de dados proprietária da Microsoft com algumas limitações. Outra forma de armazenamento faz uso de uma base de dados mais poderosa como o SQL Server 2000 e que deverá correr numa outra máquina. Caso se pretenda uma solução mais rápida, mas menos poderosa os *logs* podem ser enviados para ficheiros de texto, embora deixe de ser possível usar as capacidades da solução para efectuar consultas sobre os *logs*. Os processos mais expeditos para reencaminhar os *logs* para um servidor de *logs* será a exportação e importação dos ficheiros de texto com os *logs*, de forma mais ou menos automática ou através da exportação dos *logs* existentes na base de dados dos *logs*, quer em MSDE ou SQL Server 2000.

3.9 SEM (Security Event Management)

Security Event Management com a abreviatura de SEM ou também as soluções conhecidas como Security Information Management (SIM) são ferramentas que possuem como objectivo gerir e monitorar todo o tipo de eventos que os mais diversos equipamentos de um sistema de informação possa ter, desde o *router* de perímetro até aos postos de trabalho, passando pelas *firewalls*, *proxys*, IDS (Intrusion Detection System), anti-virus, servidores a base de dados. Portanto são soluções que pretendem centralizar todos os tipos de *logs* reportados pelos diversos equipamentos numa única solução.

Existem os mais diversos produtos dentro desta categoria de produtos de segurança informática, cada um com a sua filosofia. As principais funcionalidades disponibilizadas por estes produtos são:

- Centralização dos mais diversos *logs* de equipamentos do sistema de informação;
- Correlação dos eventos entre os vários equipamentos;
- Geração de alertas;
- Análise de *logs* em tempo real
- Gestão de incidentes e resolução de problemas;
- Armazenamentos dos *logs* de forma centralizada;
- Cópia de segurança dos *logs*;

- Escalabilidade e redundância na recolha de *logs*.

As soluções existentes de SEM possuem inúmeras vantagens relativamente à gestão isolada dos diversos equipamentos devido a poder ser uma única equipa a gerir todos os eventos relativos à segurança da informação, obtém-se uma visão geral de todos os componentes do sistema, uma única solução para gerir os *logs* gerados pelos mais diversos equipamentos. A análise de *logs* em tempo real, com a correlação de eventos e alertas enviados aos administradores possibilita a estes uma maior optimização das suas tarefas e consequente poupança de tempo. Com uma solução deste tipo a segurança da informação resulta na aplicação das três atitudes essenciais de prevenir, monitorar e responder.

Existem diferentes abordagens que cada fabricante adoptou, algumas soluções são implementadas através de agentes instalados nos equipamentos, outros adoptam uma posição intermédia e outros não os usam. Cada fabricante possui maior atenção sobre a segurança interna da rede monitorizando os postos de trabalho, outros concentram-se nas infra-estruturas baseadas em sistemas Microsoft Windows outros preferem concentrar-se sobre os equipamentos de rede.

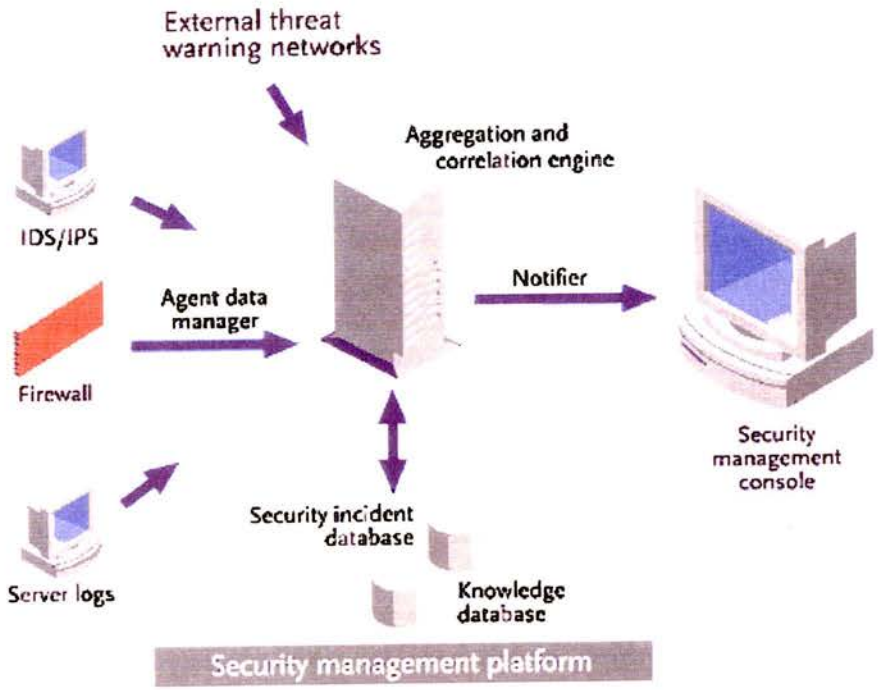


Figura 12 – Arquitectura típica de uma solução SEM

As soluções de SEM estão habilitadas a obter os *logs* dos equipamentos de diversas formas, desde o syslog, a *traps* SNMP até protocolos proprietários implementados através dos agentes. A maior parte dos produtos necessitam de uma base de dados para armazenar os *logs* recolhidos que às vezes se encontra incluída nas soluções, outras vezes não. O grande problema deste tipo de soluções é sem duvida o preço, que se encontra facilmente ao nível dos milhares de euros.

4 Desenvolvimento do Projecto

O presente projecto, devido aos diferentes pontos a solucionar, foi divido em 3 grandes partes e que se apresentam de seguida. Começa-se por descrever o problema concreto que deve ser solucionado e posteriormente descreve-se o trabalho implementado, as várias opções tomadas e respectivas justificações.

4.1 Arquitectura e Implementação da Recolha de Logs

Problema

No início do presente projecto de estágio foram definidos os principais objectivos a cumprir. Um dos objectivos estabelecidos foi a identificação dos equipamentos a abranger pelo projecto para que fossem encontradas soluções no tratamento e recolha de *logs*. O Banco BPI na sua complexa infra-estrutura possui uma enorme variedade de equipamentos. Optou-se no presente projecto, centrar atenções sobre os equipamentos sobre a alçada da equipa de segurança em que se incluem as várias *firewalls* e também os *proxyes* que efectuam o controlo de acessos à Internet dos colaboradores do Banco BPI. Para além destes equipamentos foi considerado relevante abranger também os principais *routers* que o banco tem em nesta infra-estrutura, sobre a alçada da equipa de comunicações. Inicialmente pensou-se em incluir o tratamento dos *logs* relativos aos acessos de clientes aos sites públicos bem como as transacções que estes efectuam. Tal não aconteceu devido à concentração de esforços nos equipamentos de importância critica na segurança da infra-estrutura. Durante o projecto de estágio esteve em implementação a mudança da infra-estrutura das instalações do Banco BPI para regime de *outsourcing* de instalações, portanto seria uma boa oportunidade para montar os processos necessários para a optimização da gestão dos *logs* dos equipamentos de networking e segurança.

Nesta primeira fase do projecto em que se pretende montar uma arquitectura optimizada para a recolha de *logs* dos diversos equipamentos deve ter-se em atenção os protocolos que podem ser usados para o envio dos *logs* até aos sistemas de destino. Como a largura de banda num sistema de informação é um recurso escasso deve ser racionado e portanto o processo de recolha deve ter este aspecto como fundamental. A robustez da arquitectura terá de ser boa para que se tenha confiança nos *logs* recolhidos. Se assim não for a utilidade dos *logs* reduz-se.

A tarefa de gestão e análise dos *logs* é uma tarefa que necessita de ser realizada, preferencialmente com uma periodicidade diária. Os administradores dos equipamentos são muitas vezes questionados sobre o estado de determinado equipamento em certo momento. A única maneira de estes conseguirem responder às mais diversas questões será a análise dos *logs*. A tarefa de consultar todos os equipamentos em que cada um possui o seu sistema de *logging* resulta numa tarefa morosa e complexa, principalmente se for necessário relacionar os *logs* de vários equipamentos. O presente projecto deve implementar uma solução que permita facilitar a gestão, consulta e análise dos vários equipamentos a abranger.

Solução Desenvolvida

Aquando do início do projecto de estágio foi feita uma apresentação dos mais diversos equipamentos existentes na infra-estrutura do Banco BPI. Os objectivos iniciais referem que os equipamentos objecto de análise são os equipamentos de *networking*, onde se incluem *routers* e *switches*. Para além destes devem ser abrangidos também equipamentos de segurança, como *firewalls*, IDS, entre outros.

Após a compreensão da infra-estrutura do Banco BPI, as ideias que resultaram na admissão deste projecto e também as prioridades, foi determinado que o projecto deve abranger os *logs* dos equipamentos Cisco PIX, Cisco Routers, Stonesoft Stonegate e Microsoft ISA. Chegou-se a esta conclusão devido à importância destes equipamentos na infra-estrutura do banco, porque estes são usados na ligação do Banco BPI à rede pública e que se pretende aumentar o nível de monitorização do respectivo tráfego. A implementação da nova infra-estrutura para suporte do site público www.bpionline.pt faz uso dos referidos equipamentos e necessita de ser implementado um processo coerente da gestão dos *logs*, portanto faz todo o sentido que estes equipamentos sejam abrangidos. Para além dos sistemas enunciados foi proposto inicialmente que o projecto montasse uma arquitectura para a monitorização dos servidores públicos, base de dados, incluindo as transacções que clientes efectuassem, HP-UX e também o domínio onde se encontram os colaboradores da DSI (Direcção de Sistemas de Informação) do BPI. Tal não se veio a verificar porque envolvia demasiadas equipas, não se conseguindo direccionar e obter o devido conhecimento sobre todos os sistemas, bem como a existência dos mecanismos que podem servir para monitorar os sistemas referidos. A existência de um sistema de IDS (Intrusion Detection System), foi referido como sendo uma mais valia para a análise do tráfego da infra-estrutura, mas tal sistema não foi considerado no projecto devido ao facto de ainda não ser incluído na nova infra-estrutura.

Os equipamentos Cisco Routers considerados no estágio efectuam a ligação da rede pública à rede privada da instituição, tais equipamentos possibilitam a monitorização e filtragem inicial de todo o tráfego que se faz nessa fronteira. A arquitectura da infra-estrutura de *networking* do Banco BPI foi implementada com o requisito de não haver um ponto único de falha, sendo assim existem equipamentos redundantes nos links à Internet. Como os *routers* possuem listas de acesso configuradas, sendo o primeiro nível de segurança entre rede pública e privada, faz todo o sentido que estes equipamentos sejam incluídos na gestão de *logs*.

Depois dos *routers* Cisco a rede do banco BPI possui uma primeira camada de *firewalls* Cisco PIX que faz filtragem mais fina do tráfego que é permitido e o que é negado. Neste equipamento são configuradas regras de filtragem e na aplicação destas regras resultam também os respectivos *logs* com a data, hora, IP de origem, IP de destino, se foi permitida a conexão ou se foi negado o acesso. Devido às facilidades das *firewalls* na filtragem do tráfego e também no *logging* dos eventos é critico que os *logs* estejam disponíveis para análise, consulta e monitorização.

Num nível a seguir à *firewall* Cisco PIX encontra-se a *firewall* de estado e de análise de aplicação Stonegate. Esta permite aplicar um filtro ainda mais preciso e fiável a possível tráfego que tenha chegado até esta. Pelas facilidades de gestão do equipamento, devido à estação de gestão da solução, a administração, aplicação e configuração de filtros está facilitada. Para alem da filtragem do tráfego que vem da rede pública, esta solução também permite controlar o acesso dos colaboradores às redes de gestão. A informação que esta

solução permite exportar possui valor elevado para os administradores da infra-estrutura e sendo assim foi abrangida no projecto desenvolvido.

Outro sistema que foi objecto de implementação foi o Microsoft ISA 2004 que possui as componentes de *firewall* e *proxy*. A primeira componente encontra-se em funcionamento, mas as principais funcionalidades usadas dizem respeito à componente de proxy. Esta permite controlar e acelerar os acessos dos colaboradores do banco à rede pública. Devido à política de utilização de recursos informáticos deve haver um cuidado dos colaboradores em zelar pelos sistemas que usam no local de trabalho e evitar abusos de utilização. O MS ISA permite efectuar o *logging* de todos os acessos que cada utilizador faz. Com esta informação é possível, aos administradores, saber que recursos são usados e por quem.

Estando definidos quais os equipamentos que são relevantes efectuar a sua monitorização e gestão dos *logs* gerados foram estudados os vários mecanismos que cada equipamento possui para que pudessem ser armazenados os *logs* num processo bem definido, robusto, seguro e com fácil gestão.

Os mecanismos que os *routers* Cisco possuem para encaminhar os *logs* gerados na sua actividade normal são o syslog e o protocolo SNMP, apresentados no capítulo das tecnologias. Devido a estes protocolos serem baseados no protocolo de transporte UDP é necessário ter em atenção que não existem garantias de entrega dos *logs* ao servidor de *logs*, encarregue de os receber. Se por alguma razão, muito tráfego ou quebra da ligação de rede, um pacote UDP não chegar ao seu destino, não haverá qualquer aviso sobre a não recepção de um pacote ou qualquer retransmissão. Resumindo, o pacote e respectivo *log* não será registado e nunca se saberá que aquele evento ocorreu. A solução para este problema será a implementação do servidor de *logs* perto do *router*, com uma largura de banda adequada e enviar o mesmo log para vários servidores de *logs*, para haver redundância. Desta maneira evita-se que haja um único ponto de falha, aumentando o grau de confiança em como os *logs* foram armazenados. Relativamente ao protocolo a usar, o SNMP através de *traps* permite efectuar o *logging* para uma estação de gestão e esta guardar os *logs*. As desvantagens do SNMP, em comparação com o protocolo *syslog* são as vulnerabilidades existentes e o *overhead* que possui. Portanto, será preferível o uso de syslog no encaminhamento dos *logs* do *router* até ao servidor de *logs*.

Os *routers* e a *firewall* Cisco PIX possuem os mesmos mecanismos – syslog e SNMP – para o envio de *logs*. Devido a estes protocolos serem de implementação simples, são os mais usados em equipamentos do tipo *appliance*, em que os recursos de processamento não abundam. Portanto na firewall PIX, tal como nos *routers*, é preferível usar o protocolo de syslog para efectuar o *logging*. Será útil, em alguns casos, configurar o SNMP para que envie *traps* em situações de problemas, por forma ao administrador tomar as devidas providencias.

Relativamente aos mecanismos de *logging* da *firewall* Stonesoft Stonegate existe uma maior variedade de opções no encaminhamento dos *logs* para outros sistemas. Como esta solução já possui um servidor de *logs* próprio, existe a garantia de que nenhum *log* será perdido. Essencialmente todos os eventos que acontecem são registados no servidor de *logs* proprietário, consoante a configuração definida pelo administrador. Os *logs* podem ser arquivados de forma compactada e fazerem-se consultas a esses *logs* acedendo à estação de gestão do produto. Para além de serem arquivados, os *logs* podem ser exportados para dois tipos de ficheiros: CSV ou XML como se viu no capitulo das tecnologias. Essa exportação de *logs* é efectuada de forma periódica no tempo e podem-se filtrar os *logs* a exportar. O

encaminhamento de logs em tempo real para outro sistema pode ser feita através do protocolo syslog. Tal como os outros equipamentos, caso seja usado syslog deverá haver redundância.

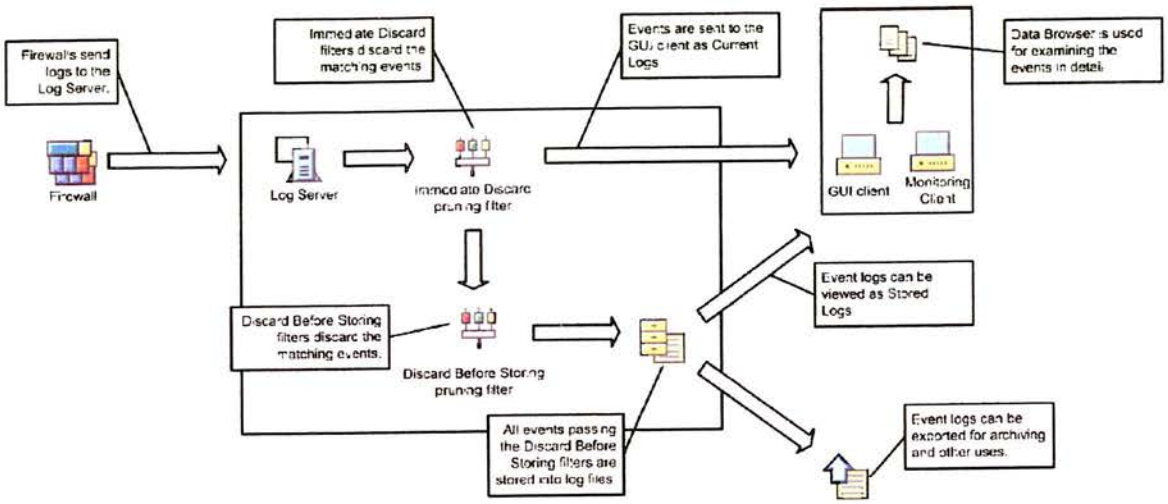


Figura 13 – Processo de encaminhamento de *logs* na *firewall* Stonegate

O produto Microsoft ISA Server com funcionalidades parecidas com a solução da Stonesoft quanto ao *logging*, permite armazenar os *logs* numa base de dados MSDE a correr localmente, pode enviar os *logs* para uma base de dados SQL Server a correr numa máquina separada do motor da *firewall* e também pode exportar os *logs* para ficheiros de texto. O MS ISA essencialmente pode ser dividido na componente *firewall* e proxy e como tal os *logs* também usam essa separação em que existe uma tabela com os *logs* da *firewall* e outra com os *logs* do proxy. Uma funcionalidade implementada é a escolha dos vários campos que podem ser guardados em determinado evento.

Das soluções que permitem a exportação para ficheiros de texto, caso seja necessário pode-se criar um processo mais ou menos automático que é capaz de transferir um determinado ficheiro de *logs* de forma periódica para um servidor de *logs*. Depois de obter o ficheiro de *logs* no servidor será necessário guardá-lo ou transformar os *logs* em ficheiros de texto para um formato mais fácil de consultar.

A vantagem de efectuar o *logging* para uma base de dados e para um servidor de *logs* proprietário será a garantia de registar todos os logs e de poder consultar os mesmos de forma amigável. O problema é que quando uma base de dados já não possui mais espaço livre em disco vai criar indisponibilidade de serviço e isso é crítico para uma empresa como o Banco BPI. Muitas das tentativas de invasão em sistemas de informação aproveita-se deste problema causando indisponibilidade de serviço ou inutilização dos mecanismos de monitorização.

Analisados os mecanismos disponíveis para o encaminhamento dos *logs* para os servidores de *logs* pode-se pensar na melhor arquitectura a montar na gestão dos *logs* dos equipamentos de rede e de segurança.

Tendo como objectivo a facilidade de gestão dos logs, a facilidade em efectuar cópias de segurança dos *logs* e a segurança conclui-se que é preferível uma arquitectura centralizada, do que uma arquitectura distribuída, em que os *logs* são armazenados de forma isolada e geridos de forma *ad hoc*. Com a centralização dos *logs* num único sistema será possível ter uma abordagem comum para todos os *logs* dos vários equipamentos, facilitando muito a consulta

dos *logs* pois estes passam a estar concentrados num único sistema, principalmente se for necessário efectuar a relação entre *logs* de diferentes equipamentos. O *backups* dos *logs* também será mais simples pois é possível fazer a cópia de todos os *logs*, de todos os equipamentos abrangidos num único sistema, ao contrário da alternativa de fazer *backup* de logs em vários equipamentos. Portanto observando estas questões, será sem duvida implementar uma arquitectura centralizada, embora haja a desvantagem de os *logs* terem de usar mais largura de banda devido ao caminho que têm de fazer desde o equipamento até ao sistema que armazena todos os *logs*.

Para que se faça a centralização dos *logs* num único sistema é necessário que haja um dimensionamento do desempenho de vários factores. Em primeiro lugar deve ter-se atenção aos volumes de tráfego relativos aos *logs* que cada equipamento gera e também a largura de banda disponível. Deve ter-se também em atenção o desempenho do servidor que vai concentrar os *logs*, principalmente aos factores: disco rígido e memória.

A opção mais obvia para o armazenamento dos *logs* no servidor central é sem duvida uma base de dados, preparada para receber grande volumes de dados e que tenha um bom tempo de resposta às consultas que se mais vulgarmente. Devido à parceria entre a Microsoft e o Banco BPI existem vantagens em termos de suporte e de custos, na implementação de uma base de dados SQL Server 2000 para o armazenamento de todos os *logs*. Como esta base de dados está preparada para receber grandes volumes de dados por hora é adequada ao problema em questão.

Observando todos os requisitos e funcionalidades desejadas a arquitectura deve evitar ter pontos únicos de falha que causam indisponibilidade na entrega dos logs no concentrador de *logs*. No caso dos *routers* e *firewall* PIX deve usar-se o protocolo syslog que envia *logs* para um servidor de *logs* primário e para um secundário, o servidor de *logs* primário reencaminha os *logs* para o concentrador que insere os *logs* na base de dados com uma estrutura própria. O servidor secundário deve também enviar os *logs* que recebeu para o concentrador de *logs*. Como este já inseriu os *logs* recebido do primário só deverão ser inseridos os *logs* que ainda não tenham sido inseridos. Desta forma garante-se que existem dois fluxos distintos de *logs* com a mesma origem e destino. Relativamente à *firewall* Stonegate a melhor forma de enviar os *logs* até ao concentrador de *logs* será a implementação de um processo que corre uma vez por dia e que exporta para ficheiros de texto em formato CSV, devido ao *overload* dos ficheiros XML, relativos ao dia anterior e faz uma transferência do ficheiro de *logs* através de SCP (Secure Copy Protocol), o concentrador que está à espera do ficheiro, importa os *logs* para a base de dados quando a transferência for concluída. Este processo tem vantagens relativamente ao protocolo syslog, porque é de fácil implementação, evitando o *parsing* do syslog recebido da Stonegate, para além da garantia de se importarem todos os *log* gerados pelo equipamento. A melhor solução encontrada na importação dos *logs* desde o MS ISA foi a criação de uma Data Transformation Service (DTS), que consiste na criação de uma ligação lógica entre a base de dados do concentrador de *logs* e do MSDE usado para armazenar os *logs* localmente. O processo correrá numa periodicidade diária e garante que os *logs* gerados são importados para o concentrador de uma forma muito simples de implementar.

Relativamente aos equipamentos que usam o syslog para encaminhar os *logs* desde o equipamento até ao concentrador de *logs*, em cada servidor que um *log* passe é feita uma cópia para disco e depois é feito o reencaminhamento do *log* para o próximo servidor de *logs* até chegar ao concentrador. Qualquer *log* que seja recebido por syslog será gravado num ficheiro com o seguinte nome: 'Syslog_<ano>-<mês>-<dia>_<hora>.txt'. A base de dados

SQL Server 2000 permite executar determinadas tarefas programadas para certo momento. Esta funcionalidade será usada para importar os *logs* do ficheiro de texto, em disco, para as respectivas tabelas de logs na base de dados. No caso dos *logs* recebidos por syslog (PIX e *routers*), foi implementado um *job* executado todas as horas ao minuto cinco. Este pegará no conteúdo do ficheiro de *logs* e consoante o tipo de equipamento, o *log* será inserido para a respectiva tabela. Para se saber qual o tipo de equipamento que gerou determinado log foi implementada uma tabela (SyslogDevice), com a correspondência entre o IP e o tipo de equipamento.

O servidor de syslog usado pela equipa de Segurança do Banco BPI é o produto Kiwi Syslog Server versão gratuita. Esta limitação implica menos funcionalidades do que a versão paga, portanto é necessário desenvolver procedimentos para efectuar a importação dos ficheiros de logs guardados em disco para a base de dados. A importação dos *logs* de todos os equipamentos é efectuada através do agendamento de tarefas com determinada periodicidade que importam os respectivos *logs*. No caso dos *logs* recebidos dos *routers*, o syslog intermediário utilizado é o Syslog-ng adoptado pela equipa de comunicações. Este possui alguns problemas ao nível do reencaminhamento dos *logs* porque não são usadas as especificações do RFC. Problemas que têm de ser resolvidos a um nível mais elevado.

Na inserção dos *logs* dos *routers* e das firewalls PIX, os equipamentos enviam os *logs* para dois servidores, o primário reenvia os *logs* para o concentrador em tempo real. O secundário deve esperar pelo final do dia para enviar os *logs* recebidos, que ficaram armazenados em disco. A ideia será inserir os *logs* recebidos do primário, hora a hora e no final de cada dia o secundário enviará os seus *logs* para concentrador que os insere na base de dados, caso ainda não tenham sido inseridos. Com este processo surge o problema de como garantir, de forma rápida e fácil que determinado *log* ainda não foi inserido. Existe a opção de efectuar o *matching* de todos os campos do *log*, mas tal situação é inviável devido ao grande volume de dados e respectivo custo na performance ao sincronizar os *logs*. A melhor maneira encontrada foi a utilização das *hash keys* MD5, que calcula uma *string* única de 128 bits consoante a entrada que recebeu. Caso existam duas *hashs* MD5 iguais é porque o *log* é o mesmo, ou ocorreram vários eventos daqueles no mesmo milissegundo e com o mesmo par origem-destino. Esta propriedade permite que seja acrescentado um campo na base de dados com a *hash* MD5 de um *log* com o objectivo de verificar se determinado *log* já existe ou não. Não existem dúvidas que é mais fácil procurar uma *string* com 32 caracteres do que efectuar uma consulta pelos vários campos.

Relativamente à *firewall* Stonegate que possui a possibilidade de exportar os *logs* para um formato de fácil importação para uma tabela de base de dados optou-se por montar um processo automático de transferência do ficheiro exportado para o concentrador de *logs* e posterior *job* que execute a importação directa do *logs*. Inicialmente os *logs* são armazenados no *log server* da própria solução e foi definido neste uma tarefa que exporta os *logs* do dia anterior, às 1:00 de cada dia para o ficheiro local: 'stonegateLog.csv'. Após 25 minutos, o ficheiro já deve ter sido exportado e então dá-se o inicio da preparação do ficheiro a enviar para o concentrador de *logs*. Portanto às 1:25 é executada a tarefa 'StonegateImport' que começa por substituir a *string* '","' por ',' em todo o ficheiro, através do utilitário sed.exe. Esta substituição é feita para que o *bulk insert* no procedimento do SQL Server do concentrador de *logs* possa ser executado com sucesso. O sed vai gerar um novo ficheiro: 'stonegateLogOk.csv', e de seguida vai-se proceder à transferência do ficheiro, através do utilitário WinSCP.

A transferência é feita através da ferramenta WinSCP que se liga ao servidor de openssh instalado no concentrador de *logs*. O WinSCP é executado em modo consola usando uma sessão guardada, esta sessão é criada fazendo um *login* inicial com um utilizador criado para este processo no servidor openssh. A sessão deve ser guardada para ser usada no *batch file*.

No *batch file* 'export.bat' para transferir o ficheiro de *log* é executado o winscp3 usando a sessão guardada e com a sucessão de comandos a executar no servidor openssh para efectuar a transferência.

Depois da transferência concluída com sucesso, é apagado o ficheiro resultante do *output* do utilitário sed e renomeado o ficheiro exportado da Stonegate para: 'stonegateLogOld.csv' (de modo a ficar com uma cópia do ficheiro, caso algo não funcione bem). Por último é criado um ficheiro 'status.log' se a transferência for executada com sucesso. Para registar qualquer problema, durante todo o processo o *output* de todas as operações é redireccionado para o ficheiro 'out2.txt'.

De forma a salvaguardar a correcta importação dos *logs* para o concentrador foi criada uma outra tarefa que deve correr 1 hora depois da transferência ter sido iniciada para verificar a existência do ficheiro 'status.log'. Se o ficheiro não existir é porque algo falhou e sendo assim é executado o *batch file* 'verify.bat' e 'verify.vbs' que envia um *mail* a informar que algo não funcionou bem. No *mail* enviado é inserido o ficheiro 'out2.txt', para que se possa ver o que falhou.

Do lado do concentrador de *logs* está definido um *job* programado para correr às 2:00 de cada dia, que faz um *bulk insert* ao ficheiro transferido. Caso ocorra algum problema, será também gerado um *mail* a informar que o processo de importação falhou. O problema pode ser resolvido usando o ficheiro 'stonegateLogOld.csv' que continua no Stonegate Log Server.

Depois de descritos os passos na importação dos *logs* dos *router*, PIX e Stonegate descreve-se qual o melhor processo encontrado para efectuar o *logging* dos eventos gerados pelo MS ISA, para o concentrador de *logs*. Como este deve fazer o seu *logging* para uma base de dados local MSDE, devido a questões de desempenho, a forma mais fácil de enviar os *logs* para o concentrador será através da construção de um DTS. Este deve ter como origem a tabela de *logs* do MS ISA e uma tabela exactamente igual do lado do concentrador de *logs*, a correr sobre o MS SQL Server 2000. O DTS deve ser configurado do lado do ISA Server porque o seu MSDE não está habilitado a receber ligações de outras máquinas. Como a Stonegate, o MS ISA Server deve efectuar a exportação dos *logs* do dia anterior e em horas com pouca actividade.

Uma funcionalidade implementada na base de dados do concentrador de *logs*, foi a resolução dos IPs de origem e destino, que aparecem nos *logs* da *firewall* PIX. Como este equipamento não possui nenhuma forma apelativa de consultar os *logs*, tal como a Stonegate. Achou-se necessária a inclusão na sua tabela de três campos que servem para extrair os IPs que se podem encontrar no *log*. A resolução dos IPs encontrados no *log* será feita durante a noite, momento em que o sistema não está muito atarefado. Para um log em particular, começa-se por extrair os IPs do *log*, efectua-se a resolução dos IPs e caso seja obtido sucesso na resolução, será trocado o IP pelo nome, caso contrário, deverá aparecer o IP original.

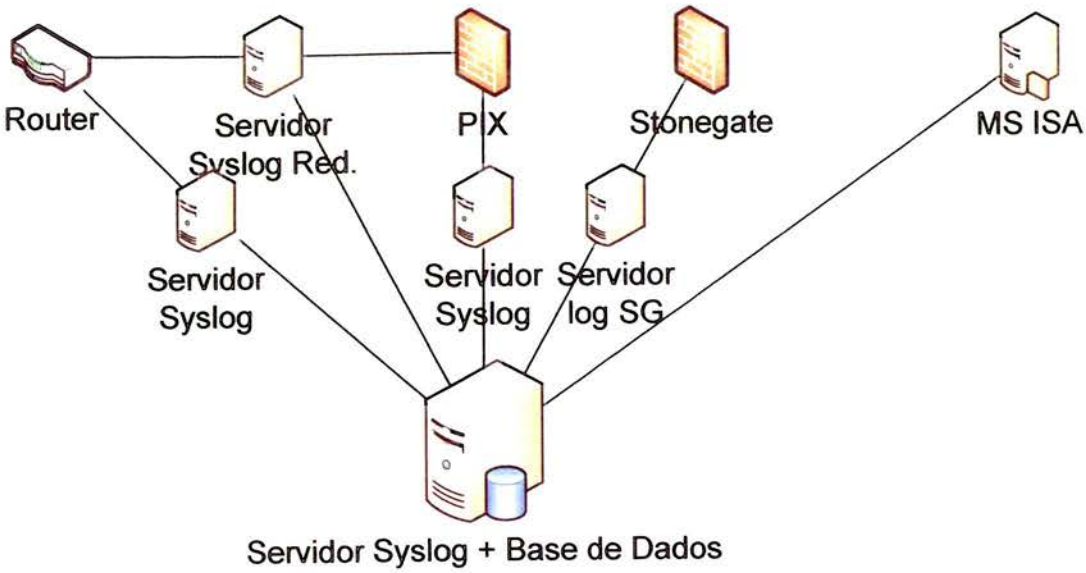


Figura 14 – Arquitectura base da concentração de *logs*

Depois de apresentados os processos de centralização dos logs na base de dados SQL Server 2000 e para que se perceba melhor a implementação da solução são descrito os procedimentos e a estrutura da base de dados que suporta o armazenamento de todos os *logs*.

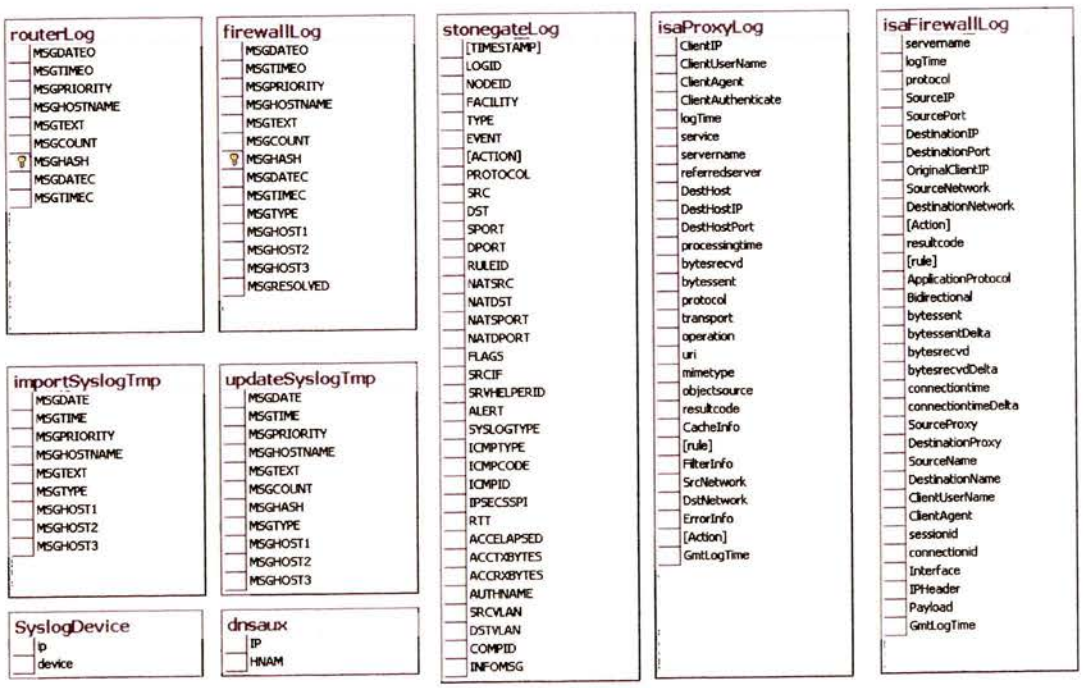


Figura 15 – Esquema das tabelas da base de dados do concentrador de *logs*

A seguir apresentam-se as principais tabelas que foram desenhadas, omitindo por outro lado as tabelas 'stonegateLog', 'isaProxyLog' e 'isaFirewallLog' por serem exactamente iguais às que se podem encontrar na respectiva solução.

SyslogDevice

[ip] [varchar] (255)

[device] [smallint]

Quando se configurar um equipamento para enviar *logs* através de syslog para o concentrador de *logs* deve primeiro inserir-se nesta tabela o IP ou *hostname* que aparece nos *logs* e no campo 'device' um 1 caso seja um router, ou 2 caso se trate de uma PIX. Os procedimentos de importação de logs baseiam-se nesta tabela para saber que formato o *log* segue.

dnsaux

[IP] [varchar] (255)

[HNAM] [varchar] (255)

Tabela auxiliar para a resolução dos IPs que se encontram nos *logs* das PIX's. Extraem-se os IPs dos *logs*, inserem-se no campo 'IP' e depois faz-se a resolução dos IPs.

firewallLog

[MSGDATEO] [datetime]

[MSGTIMEO] [datetime]

[MSGPRIORITY] [varchar] (30)

[MSGHOSTNAME] [varchar] (255)

[MSGTEXT] [varchar] (1024)

[MSGCOUNT] [int]

[MSGHASH] [char] (32)

[MSGDATEC] [datetime]

[MSGTIMEC] [datetime]

[MSGTYPE] [varchar] (16)

[MSGHOST1] [varchar] (255)

[MSGHOST2] [varchar] (255)

[MSGHOST3] [varchar] (255)

[MSGRESOLVED] [bit]

Tabela que recebe os *logs* de todas as *firewalls* PIX. Os campos 'MSGDATEO' e 'MSGTIMEO' correspondem à data e hora em que o evento ocorreu no equipamento, enquanto os campos 'MSGDATEC' e 'MSGTIMEC' à data e hora de chegada do *log* ao concentrador de *logs*. Os campos 'MSGPRIORITY', 'MSGHOSTNAME' e 'MSGTEXT' representam os campos normais existentes em qualquer *log* com o formato syslog. O 'MSGCOUNT' é o número de vezes que um *log* é repetido, 'MSGHASH' é a *hash key* MD5 do *log*, calculada a partir da *string*: 'MSGHOSTNAME,MSGPRIORITY,MSGTEXT'. O campo MSGTYPE é o tipo de eventos que a PIX gera. Por último, existem 3 campos que guardam os nomes dos IPs encontrados nos *logs*. 'MSGHOST1' possui a primeira ocorrência de um IP, transformado em nome, ou o IP caso não tenha conseguido resolver o mesmo. 'MSGRESOLVED' é igual a 1 quando já se tentou resolver os IPs desse *log*.

routerLog

[MSGDATEO] [datetime]

[MSGTIMEO] [datetime]

[MSGPRIORITY] [varchar] (30)

[MSGHOSTNAME] [varchar] (255)

[MSGTEXT] [varchar] (1024)

[MSGCOUNT] [int]

[MSGHASH] [char] (32)

[MSGDATEC] [datetime]

[MSGTIMEC] [datetime]

Tabela que armazena os *logs* dos *routers*. A estrutura é similar à usada na tabela 'firewallLog'.

importSyslogTmp

[MSGDATE] [datetime]

[MSGTIME] [datetime]

[MSGPRIORITY] [varchar] (30)

[MSGHOSTNAME] [varchar] (255)

[MSGTEXT] [varchar] (1024)

[MSGTYPE] [smallint]

[MSGHOST1] [varchar] (255)

[MSGHOST2] [varchar] (255)

[MSGHOST3] [varchar] (255)

Tabela temporária para inserir os *logs* dos *routers* e *firewalls* vindos por syslog. É usada pelo procedimento 'importSyslog'.

updateSyslogTmp

[MSGDATE] [datetime]

[MSGTIME] [datetime]

[MSGPRIORITY] [varchar] (30)

[MSGHOSTNAME] [varchar] (255)

[MSGTEXT] [varchar] (1024)

[MSGCOUNT] [int]

[MSGHASH] [char] (32)

[MSGTYPE] [smallint]

[MSGHOST1] [varchar] (255)

[MSGHOST2] [varchar] (255)

[MSGHOST3] [varchar] (255)

Tabela temporária para inserir os *logs* dos *routers* e *firewalls* recebidos por syslog. É usada pelo procedimento 'updateSyslog'.

Na implementação da base de dados foram sendo programados vários *jobs*, cada um com o seu objectivo e respectiva calendarização. Descrevem-se de seguida todos *jobs* agendados na base de dados do concentrador de *logs*.

Alerta – Ocorre quando a base de dados excede os 70 GB ou quando o seu *transaction log* excedeu os 8 GB.

CleanLogs – A correr às 3:15 de cada dia para apagar os *logs* que tenham mais de 30 dias.

ResolucaoIPs – Extrai os IPs e *hostnames* dos *logs* das PIX's e resolve os IPs. A correr todos os dias às 21:30.

StonegateLogImport – Insere os *logs* recebidos do servidor de *logs* da Stonegate. Corre numa base diária às 2:00, inserindo os *logs* do dia anterior.

Syslog_Import – Insere os *logs* recebidos via syslog. Importa os *logs* vindos de routers e PIX, inserindo-os na respectiva tabela, consoante a tabela SyslogDevice. Corre todas as horas ao minuto 5, em que insere os *logs* recebidos na hora anterior.

Optimizations Job – Corre todos os dias às 20:30 e reduz o tamanho do *transaction log* da base de dados.

Para além dos vário *jobs* agendados existem procedimentos que basicamente executam a maior parte tarefas de importação de logs, resolução de IPs ou apagam os *logs* com mais de 30 dias... Estes procedimentos ou Stored Procedures podem ser executados manualmente pelos administradores ou executados automaticamente, consoante a calendarização de um *job*. Apresentam-se de seguida os procedimentos criados. Não se inclui a sua implementação devido a serem de difícil consulta em papel.

cleanLogs – apaga os *logs* das respectivas tabelas com mais de 30 dias.

dnsLookup – recebe um IP, resolve-o e retorna o *hostname*.

exportLogs – exporta os *logs* dos últimos 7 dias para ficheiros de texto, compacta-os e move-os para um directório para efectuar backup. Pronto a correr através de um *job*.

exportLogsInt – exporta os *logs* como o procedimento anterior, mas exporta o intervalo especificado nos argumentos.

importBackup – importa os ficheiros de texto recuperados do backup.

importDir – importa os ficheiros de *logs* recebido através de syslog, existentes num directório.

importStonegate – procedimento que corre diariamente importando os *logs* da Stonegate.

importSyslog – procedimento usado para importar os *logs* recebido via syslog. Parte do princípio que não existem *logs* iguais aos que vai inserir.

importSyslogJob – procedimento executado pelo *job* que importa os *logs* dos *routers* e *firewall*.

resolveNamesAssync – resolves os nomes dos *logs* da PIX em que ainda não se tentou a sua resolução.

updateSyslog – procedimento usado quando o procedimento 'importSyslog' falha por haver um *log* repetido. Verifica se existem *logs* repetidos e caso falte inserir algum *log*, insere os *logs* em falta. Procedimento preparado para receber *logs* repetidos dum syslog secundário a

implementar e inserir unicamente os que estão em falta, gerando um registo completo dos *logs*.

updateSyslogJob – procedimento que corre quando o 'importSyslogJob' falha devido a *logs* repetidos. Está para o 'updateSyslog' como o 'importSyslogJob' está para o 'importSyslog'.

4.2 Armazenamento de *Logs* a Longo Prazo

Problema

A concentração dos *logs* dos vários equipamentos de *networking* e segurança num único sistema implica um enorme volume de dados que é armazenado em base de dados. Surge um problema relativamente à cópia de segurança dos *logs*, devido principalmente à importância que os dados possuem e à necessidade de serem armazenados por cerca de 5 anos. A capacidade da base de dados está programada para poder ter disponíveis os logs com menos de 30 dias. Passado esse intervalo de tempo, os *logs* serão apagados da base de dados. Esta situação acontece tendo em consideração o desempenho da base de dados. Desta forma deve ser encontrada a melhor maneira para serem feitas cópias de segurança aos *logs*.

Um aspecto importante nas cópias de segurança dos *logs* é a utilidade para além da salvaguarda da informação. Com os dados contidos nos *logs* e implementado algum mecanismo que garanta confiança quanto à integridade dos mesmos, estes possuem valor provatório numa situação de litígio. O Banco BPI pretende que os *logs* armazenados ao longo de 5 anos possam ser usados, caso seja necessário, para provar que determinado acesso a determinado sistema foi efectuado ou não.

Na resolução deste problema para além das questões técnicas de conseguir implementar uma forma fácil, robusta e eficiente na cópia de segurança dos *logs* é necessário ter em consideração a eficiência económica da solução e da logística inerente ao armazenamento de muitos suportes de informação por longos períodos de tempo.

Solução Desenvolvida

A concentração dos *logs* de equipamento de *networking* e segurança num único servidor origina um grande volume de dados. A presente politica de *backup* será diferente da usada para *backup* dos sistemas, devido à especificidade do problema. Como se pretende guardar registos do que aconteceu em determinado momento na rede, será mantido *off-site* cerca de 5 anos de *backups* de *logs*.

Devido ao grande volume de dados e à especificidade do problema a solução implementada foi pensada para o problema em particular. Existem soluções de *backup* implementadas no Banco BPI, mas após a sua análise concluiu-se que a filosofia de cópias de segurança de uma base de dados de clientes ou de um sistema é muito diferente do armazenamento a longo prazo de *logs* de equipamentos. Desta maneira descreve-se de seguida a solução implementada.

O concentrador de logs possui uma base de dados SQL Server 2000 constituída por várias tabelas, em que cada uma recebe os *logs* de um tipo de dispositivo.

Os equipamentos e respectiva tabela são os seguintes:

- Cisco PIX – firewallLog;

- Cisco Routers – routerLog;
- Firewall Stonegate – stonegateLog;
- Microsoft ISA Proxy- isaProxyLog;
- Microsoft ISA Firewall- isaFirewallLog.

Define-se para esta solução o início da semana como sendo a Quarta-feira. Isto deve-se ao facto de facilitar o procedimento aquando de um fim-de-semana prolongado.

Inicialmente existe um *job* que está configurado na base de dados que exporta para ficheiro de texto os *logs* da semana anterior, das cinco tabelas existentes. Cada tabela terá um ficheiro de texto com os *logs* da semana que passou. O *job* será executado todas as semanas à quarta-feira às 12:30. Os ficheiros criados terão os seguintes nomes:

- Cisco PIX - pix_<data-de-inicio>_<data-de-fim>.bck
- Cisco Routers - router_<data-de-inicio>_<data-de-fim>.bck
- Firewall Stonegate - stonegate_<data-de-inicio>_<data-de-fim>.bck
- Microsoft ISA Proxy- isaproxy_<data-de-inicio>_<data-de-fim>.bck
- Microsoft ISA Firewall- isafirewall_<data-de-inicio>_<data-de-fim>.bck

O método de exportação usado é o utilitário BCP do SQL Server 2000, executado por um Stored Procedure, chamado automaticamente à quarta-feira às 12:30. Os ficheiros exportados possuem um registo por linha e as colunas separadas por uma tabulação, de forma a facilitar a sua importação com o Bulk Insert.

Neste *job* os ficheiros depois de exportados são compactados usando o utilitário 7-Zip através da linha de comandos. Resultará um ficheiro com o seguinte nome: logs_<data-de-inicio>_<data-de-fim>.zip.

Quando o processo de geração de ficheiros ocorrer com sucesso, deve ser reportado para a aplicação de gestão *backups* servidora: o nome do ficheiro, a data de inicio que o ficheiro tem, a data de fim, o tamanho que o ficheiro possui e a *hash* MD5. A forma de reportar a informação para a aplicação é por .NET Remoting, que basicamente é uma forma de invocação remota de objectos e métodos para a *framework* .Net. Do lado do concentrador de *logs* existe a aplicação cliente desenvolvida, que envia a informação definida para a máquina responsável pelo *backup* dos *logs*.

Quando a aplicação de gestão de *backups* recebe os dados de um ficheiro, deve proceder à transferência do mesmo.

O servidor tem instalado um servidor de openssh que permite que uma máquina cliente se conecte e que de uma forma segura possa transferir ficheiros entre os dois computadores. Desta maneira o servidor de *backups* acede ao servidor openssh instalado no concentrador de *logs* e faz um get do ficheiro compactado com os *logs*, processo automatizado pela aplicação de gestão de *logs* desenvolvida.

A aplicação tendo a informação do ficheiro deve proceder à transferência para o seu disco de forma ser armazenado no dispositivo de *backup*.

Quando a transferência do ficheiro *zip* estiver concluída deve proceder-se à gravação do mesmo em DVD, mas antes verificar que o ficheiro foi transferido com sucesso e sem erros. Processo executado comparando a *hash* MD5 enviada pela aplicação cliente e a *hash* MD5

gerada do ficheiro transferido. Garantida a integridade do ficheiro transferido, será enviado à aplicação cliente (que esteve à espera de um OK), uma confirmação de que tudo correu com sucesso.

Antes de gravar o DVD o operador deve colocar o DVD com a *label* esperada. A aplicação de gestão de *logs* é responsável por informar qual a *label* para determinada semana de *logs*.

De forma a garantir que não se perdem os *logs*, confiar numa única cópia seria arriscado, isto devido a possíveis erros durante o processo de gravação ou armazenamento. Para uma maior robustez do processo, são gravados dois suportes com os mesmos dados – um primário e um secundário. Estes suportes devem ser de fabricantes diferentes (garantia que um mesmo lote não possui defeitos de fabrico), e armazenados em locais diferentes.

O sistema para identificação dos DVDs é feito de forma simples. Devem existir 520 DVDs armazenados com a label 'logs-<ordem>-1' até 'logs-<ordem>-260'. Os 520 DVDs correspondem a 5 anos de armazenamento (2 DVDs x 52 Semanas x 5 anos = 520 DVDs).

As *labels* colocadas nos suportes devem ter o seguinte formato: 'logs-<ordem>-<nr>' em que <ordem> pode ser 1 (suporte primário) ou 2 (suporte secundário) e em que <nr> é o número do backup, que varia entre 1 e 260 (um por cada semana, num total de 5 anos, 5x52 semanas = 260). Quando se chegar à semana 261, serão reciclados os suportes com as *labels* 'logs-1-1' e 'logs-2-1', continuando a mesma lógica para a semana seguinte. Como serão guardadas 2 cópias para a mesma semana serão necessários no total 2x260 DVDs, mais alguns extra, para substituir caso aconteça alguma falha.

A numeração dos *backups* teve inicio na semana de 2005-06-01 a 2005-06-07 que possui o número de backup igual a 1.

Caso ocorra algum erro com o DVD deve ser substituído por um em bom estado e colocar a *label* no novo DVD, do DVD que este veio substituir. Caso um ficheiro exceda o tamanho de um DVD single layer (4.7 GB) deverá ser feito o *backup* num DVD dual layer, com o dobro da capacidade (8.5 GB).

Como nos dados a compactar existem muitas *strings* repetidas espera-se que quando compactados os *logs* ocupem uma pequena percentagem do tamanho original. Nos testes efectuados da exportação de uma semana de *logs* originou-se 1750 MB em ficheiros de texto, compactando em formato zip, resultou um ficheiro com cerca de 218 MB.

Suporte	Capacidade (MB)	Tamanho dos *logs* (compressão a 13%) (MB)	Tamanho dos *logs* (compressão a 20%) (MB)
CD	700	5305	3500
DVD	4700	36153	23500
DVD-DL	8500	65385	42500

O operador deve sempre de uma forma manual conferir os dados da aplicação de registo de *backups* que informa qual a *label* do DVD a colocar com o DVD efectivamente colocado na *drive*. Confirmados estes dados deve dar comando para início da gravação do DVD.

Quando a gravação ocorrer com sucesso, o DVD deve ser guardado no local especificado pela aplicação ou num novo local especificado pelo operador.

Por fim o operador deve confirmar o armazenamento do DVD no sítio registado na aplicação. Desta forma, a aplicação registará a localização do ficheiro a que se efectuou o *backup*, bem como, o intervalo de tempo que ficou armazenado.

Se por alguma razão a aplicação não iniciou o processo de *backup*, será gerado um alerta para os operadores a informar que será necessário assistência no processo. Os operadores devem obter o ficheiro "zipado", do intervalo em falta e transferir o ficheiro para a aplicação servidora de *backups*. Na aplicação existe a possibilidade de importar um ficheiro manualmente, seleccionando o ficheiro e completando a informação em falta. O processo de gravação deve processar-se da forma habitual, bem como o registo na aplicação.

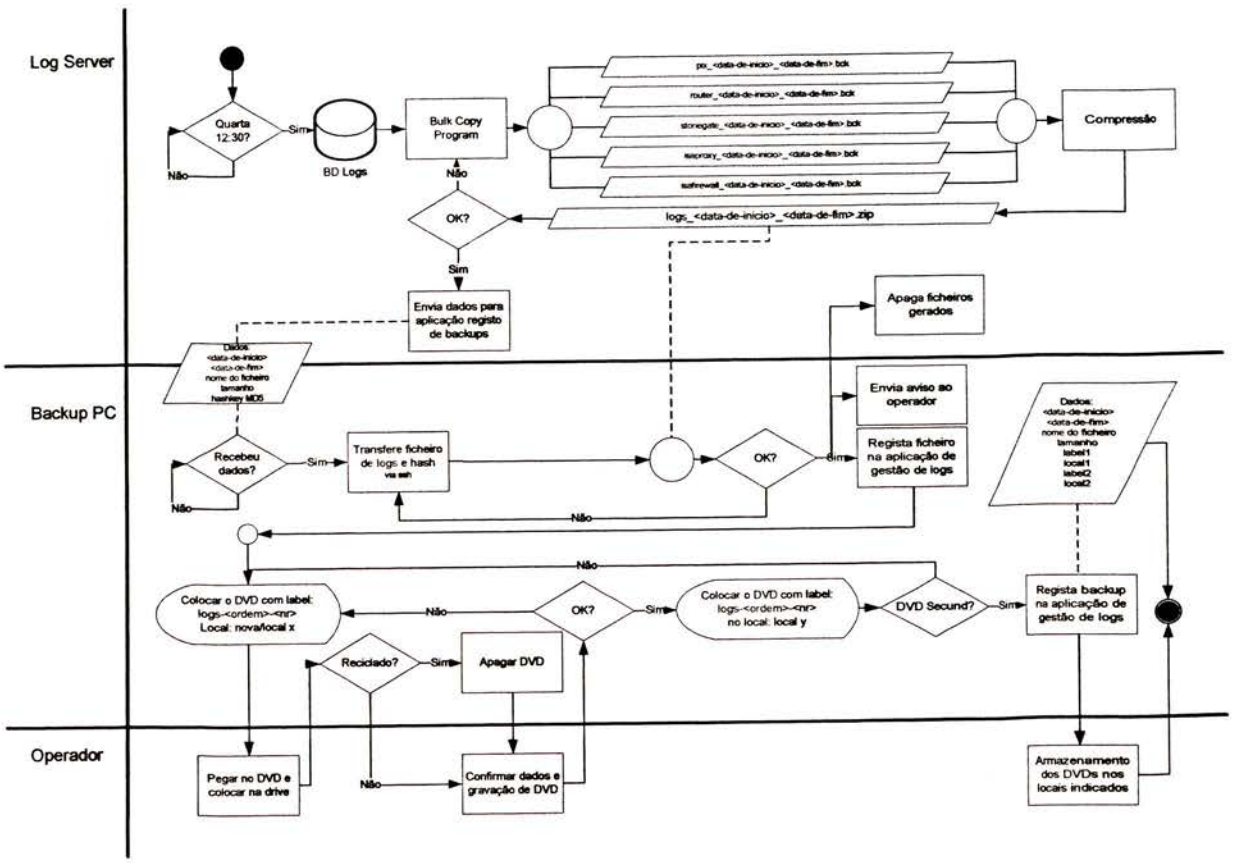


Figura 16 – Processo de *backup*

Para além do processo de *backup,* define-se o processo a executar para a recuperação dos *logs,* passando-se a explicar de seguida a solução implementada.

A base de dados que recebe todos os *logs,* possui armazenados os logs com menos de 1 mês, ou seja 30 dias anteriores ao dia actual. Para uma análise dentro deste intervalo não é necessário recuperar qualquer *backup*. Caso esta situação aconteça sugere-se que o conjunto de dias a analisar, seja exportado para uma outra base de dados, de forma a não prejudicar o desempenho da base de dados em produção. Normalmente as análises mais frequentes são feitas aos *logs* com menos de um mês.

O processo de *recover* faz-se quando for necessário analisar os *logs* dos equipamentos com mais de dois meses e menos de dois anos. Inicialmente deve haver uma indicação provável da data de possíveis problemas ou anomalias a analisar. Com as datas prováveis de inicio e fim é possível localizar os ficheiros a recuperar e qual a sua localização através da aplicação de gestão de *logs*. A aplicação deve registar que os DVDs recuperados estão em análise e quando

esta for finalizada, serão recolocados no local original e registada a sua reposição na aplicação.

Sabendo quais os DVDs a recuperar e a sua localização, o operador deve colocar os DVDs na *drive* e recuperar todos os ficheiros para um directório e descompactá-los. Durante o processo de *backup* foram registados as *hash keys* de todos os ficheiros guardados. No processo de recuperação pode-se assegurar a integridade dos ficheiros recuperados, para isso basta comparar a *hash key* registada na aplicação e as *hash keys* de cada ficheiro, no ficheiro compactado.

Para analisar os *logs* deve ser colocada uma base de dados com a mesma estrutura da de produção a funcionar, se possível numa máquina diferente. Através do procedimento 'importBackup' que usa o Bulk Insert, será feita a importação dos dados para as respectivas tabelas.

Com os *logs* recuperados faz-se a análise necessária, se não for possível analisar o pretendido deve-se recuperar outros *backups* que contenham os *logs* em falta. Depois da análise efectuada devem ser apagados os *logs* das tabelas em análise.

Quando não forem necessários os DVDs, estes devem ser colocados novamente no local onde foram retirados e o seu estado deve passar a 'armazenado' na aplicação de gestão de *logs*.

Para se perceber a informação que a aplicação de gestão de *backups* de *logs* regista e o seu funcionamento pode ser consultado, o anexo A com a respectiva descrição.

4.3 Análise de Soluções para Gestão de Logs

Problema

A implementação da centralização dos *logs* dos diversos equipamentos facilita a gestão de todo o processo de análise e de gestão dos *logs*. O problema é que a abordagem implementada não funciona em tempo real. Esta situação envolve riscos que se podem pagar caro. Por exemplo, o comprometimento de um determinado sistema na arquitectura actual, só será detectado pelos administradores, na melhor das hipóteses, após uma hora da ocorrência do problema. Isto se os administradores estiverem a analisar os *logs* de uma forma regular. O problema é que não existem recursos que estejam dedicados a tempo inteiro, à monitorização da infra-estrutura. A filosofia actual, relativamente à análise de *logs* é reactiva, em que quando é detectado algum problema ou quando alguém pede aos administradores para analisar determinada situação, é que se vai consultar o concentrador de *logs*, sobre o que terá acontecido.

A implementação de uma solução que faça a análise e monitorização em tempo real e de forma automática, será uma mais valia para a segurança da informação do Banco BPI. O que se pretende é possuir uma infra-estrutura com os mecanismos preventivos e controlo de acessos, a sua monitorização e poder responder a tempo de evitar o comprometimento dos sistemas.

Soluções

Para que a abordagem sobre a monitorização dos *logs* gerados seja efectiva e feita de forma a facilitar os administradores na gestão dos sistemas de informação, devem ser disponibilizadas

as ferramentas adequadas. Ferramentas sem as quais as, tarefas de gestão não se conseguem executar ou se mostram muito mais complicadas de concluir.

No início do projecto de estágio, um dos objectivos era o teste de soluções existentes no mercado para a análise e gestão de todos os processos relacionados com os *logs*. Devido à implementação demorada deste tipo de soluções e da necessidade da resolução de problemas concretos, foi deixada para uma próxima fase do projecto a análise exaustiva de três soluções e da sua experimentação na rede de testes. Foi feito levantamento das principais funcionalidades de cada produto e as principais potencialidades de cada um. Apresentam-se unicamente os produtos que pareceram mais direccionados para os sistemas do Banco BPI, embora tenham sido analisadas cerca de 20 produtos. As soluções apresentadas deverão ser testadas mais minuciosamente numa próxima fase e redigido um relatório minucioso de recomendação da melhor solução.

Durante o projecto de estágio foram analisadas as mais diversas informações disponíveis sobre os produtos do tipo, Security Event Management (SEM), devido a estas soluções abrangerem os mais diversos tipos de equipamentos e porque são uma solução completa sobre a gestão de todos os processos relativos aos *logs*.

As funcionalidades que se pretendem são várias, dando-se maior importância às soluções que tenham suporte local, que tenham uma boa posição no mercado e que se adaptem à infra-estrutura existem no Banco BPI.

Neste tipo de soluções existem funcionalidades que são comuns a todos os produtos:

- Arquitectura distribuída;
- Análise em tempo real dos *logs*;
- Armazenamentos dos *logs* em bases de dados;
- Relatórios pré-definidos;
- Geração de alertas;
- Correlação de eventos;
- Normalização dos *logs*;
- Existência de um motor que faz o processamento;
- Existência de consola de gestão.

Das ferramentas testadas as que mais se destacaram são as apresentadas a seguir e das quais se descrevem as principais características e diferenças entre elas.

Sentinel 5 – E-Security

Esta solução recolhe *logs* e dados de uma diversidade enorme de equipamentos, como é o caso de bases de dados, *routers*, *firewalls*, ERPs, IDSs, só enunciando alguns tipos. Possui uma arquitectura escalável, em que o processamento e monitorização são feitos de forma distribuída. A solução pode ser implementada como um *cluster*, permitindo elevadas performances.

Este produto foi o que obteve melhor avaliação entre as características necessárias e as características disponíveis, deixando liberdade para aquisição de novos equipamentos e também sendo escalável para qualquer tipo de arquitectura implementada. Nos testes efectuados por entidades externas este produto teve muito boas avaliações. Com o suporte

português por parte da empresa Cesce SI é uma escolha a fazer, para uma análise mais detalhada.

Consul Insight Suite – Consul

A principal característica que se destaca do presente produto é a sua preocupação com a certificação da empresa onde o produto for implementado nas normas de segurança ISO 17799. Este produto para além dessa preocupação possui uma vertente muito virada para a segurança interna da rede. É um produto que verifica constantemente os vários equipamentos existem sobre o cumprimento da politica de segurança estabelecida. De salientar o suporte do produto para *mainframes*.

A Consul também é representada pela Cesce SI, o que representa uma vantagem, pelo suporte nacional. Esta solução deverá ser testada devido à componente de segurança interna e externa, mas principalmente devido ao auxílio que disponibiliza na certificação das normas de segurança, obtendo desta forma vantagens competitivas com a certificação da segurança.

nFX – NetForensics

A solução da NetForensics é bastante conceituada neste tipo de soluções. Possui uma arquitectura completamente flexível e está mais direccionada para suporte a equipamentos de rede e de segurança, ao contrário das anteriores, que analisam os *logs* dos postos de trabalho e das aplicações. Esta solução permite também mapear uma intrusão, dando ao administrador a visualização do grau de comprometimento dos vários equipamentos.

Solução também com suporte nacional e que deve ser em conta caso seja necessária uma abordagem dirigida às rede e aos equipamentos de segurança.

NetIQ Security Manager - NetIQ

Relativamente ao produto da NetIQ é de referir as potencialidades que esta ferramenta possui na monitorização, essencialmente dos sistemas baseados em sistemas operativos Microsoft. Caso existem poucos recursos em termos de *hardware* esta é das soluções que menos exigências tem. O suporte nacional é também uma constante e será uma opção válida, caso se necessite de uma solução vocacionada para os sistemas Microsoft.

A grande desvantagem deste tipo de produtos é o seu preço que ronda facilmente os milhares de contos. Outra observação a fazer, é o facto de muitas das características anunciadas não corresponderem à realidade. Acrescente-se que estes produtos possuem um tempo de implementação de vários meses.

5 Conclusões e Perspectivas de Trabalho Futuro

Neste capítulo são apresentadas as conclusões retiradas de cada fase do estágio. De seguida, é feita uma avaliação dos resultados do estágio e do trabalho desenvolvido. Por fim são indicadas as perspectivas de trabalho futuro.

5.1 Conclusões do Projecto de Estágio

Um estágio curricular deveria ser regra em qualquer licenciatura de informática as vantagens que dai advêm são imensas. O projecto de estágio realizado no Banco BPI proporcionou um sem número de experiências enriquecedoras que não são possíveis de simular em nenhum meio académico. A linguagem técnica que diariamente os colegas de trabalho usam necessita de ser aprendida, o que inicialmente parece complicado, mas com o tempo se vai assimilando. Outros aspectos muito importantes no mercado de trabalho foi a percepção do escalar de decisões na hierarquia de uma empresa, também as restrições relativamente a recursos económicos e os vários ambientes que qualquer solução necessita de passar para que possa ser usada. Muitas destas questões passam despercebidas na vida académica, mas são fundamentais no mercado de trabalho.

A adaptação nesta nova etapa foi bastante rápida, contribuindo para isso o espírito de ajuda que reina entre os vários colegas. Estes proporcionaram aos vários estagiários uma boa escola sobre o verdadeiro trabalho. Uma das características mais desenvolvidas durante o estágio foi a autonomia, isto devido ao pouco tempo que as pessoas tinham para acompanhar o trabalho desenvolvido, embora fosse tirada qualquer dúvida que surgisse.

Na parte inicial do projecto foi realizado o estudo dos vários mecanismos que existem para efectuar a centralização dos *logs*, foi apresentada a infra-estrutura e compreendidos os vários problemas que se levantam com a gestão dos *logs* dos diversos equipamentos. Sem esta fase inicial de estudo e compreensão do problema, a solução não tem a melhor qualidade porque não se percebe as implicações que o projecto possui. Foram estudadas as várias opções e especificada uma arquitectura, implementada em parte, porque o *hardware* necessário não se encontrou disponível durante o estágio, mas que comprovou ser adequada ao problema de melhorar os processos que estavam em vigor antes do projecto. Prova disso é o facto do sistema montado ter passado por uma fase de testes e se encontrar em produção.

Para além de questões técnicas analisaram-se situações jurídicas, de regulamentos e de boas práticas que deveriam ser cumpridas. O caso da aceitação dos *logs* como meio de prova é exemplo de problemas que são impostos à implementação da solução, bem como o tempo que os *logs* devem ser guardados. Portanto é necessário que no desenvolvimento de qualquer projecto pensar-se nas questões não técnicas, que muitas vezes são esquecidas, e adaptar a solução para esses requisitos, correndo o risco de o trabalho desenvolvido não ter utilidade.

Na primeira fase do projecto relativa ao estudo da infra-estrutura, à definição da arquitectura, análise de soluções que ocupou bastante tempo, não foram encontras grandes dificuldades. O que causou alguma dificuldade foi a pouca informação rigorosa sobre os produtos que fazem a análise e gestão dos *logs*.

Com a segunda fase do projecto em que foi feita a instalação, configuração e implementação da recolha e concentração dos *logs* na base de dados central, foram sentidas as maiores

dificuldades. Problemas que tiveram quase sempre a mesma fonte: syslog. Este protocolo embora esteja bem documentado através do seu RFC, os fabricantes dos mais variados equipamentos insistem em não usar as especificações ou a usar uma norma, mesmo dentro dos equipamentos do mesmo fabricante. Sendo assim o *parsing* do syslog para que seja efectuada a sua importação para os respectivos campos foi uma tarefa morosa. O facto de o SQL Server não possuir mecanismos muito expeditos para efectuar manipulação de *strings* não facilitou a implementação deste processo. Outra fonte de problemas foi a garantir a eliminação de *logs* repetidos para efectuar a sincronização com os *logs* recebidos pelo servidor de *logs* secundário. Problema que tem impacto directo na performance da importação de *logs* para a base de dados. Com impacto no desempenho, existe também o procedimento que faz a resolução dos IPs dos logs recebidos da firewall PIX e que demorou bastante tempo até se encontrar a solução ideal. Com a implementação da concentração dos logs na base de dados a gestão dos logs passou a poder ser feita analisando um único sistema, obtendo benefícios práticos desse facto.

Na parte final do estágio em que se fez a implementação do processo de armazenamento dos logs a longo prazo foram encontradas algumas dificuldades. Estas começaram já na definição dos requisitos que deveriam ser atendidos e na compreensão dos sistemas já implementados no BPI (Omniback) ou em fase de implementação (BrightStor). A questão a analisar era se seria realizável montar um processo que fosse adaptado ao problema específico do armazenamento a longo prazo de grandes volumes de dados. Situação que prolongou por mais tempo do que devia acabando por ser implementada a solução descrita anteriormente. O seu desenvolvimento foi mais moroso do que o previsto, mas cumpre com todos os requisitos para os quais foi pensada.

5.2 Avaliação dos Resultados do Estágio

No final do estágio, os principais objectivos foram atingidos. Tanto a nível pessoal, como a nível profissional.

A nível pessoal, a integração na equipa de trabalho foi um sucesso. O desenvolvimento do trabalho numa área bastante interessante permitiu manter os níveis de motivação elevados e o desejo de continuar a desenvolver os conhecimentos relativos à temática da segurança e de redes de comunicações. O acesso a várias tecnologias que eram desconhecidas até então permitiu a aquisição de know-how, contribuindo para isso também o contacto com pessoas com mais experiência. Pode-se concluir assim que foi adquirida uma formação e experiência bastante extensa a vários níveis.

A nível profissional, a solução desenvolvida cumpriu os objectivos propostos e teve uma boa aceitação por parte da responsável pela gestão dos equipamentos. A solução implementada na infra-estrutura do Porto deverá ser implementada também na rede de Lisboa em que existe bastante mais tráfego. Comprovando que a solução encontrada é de qualidade e que o trabalho desenvolvido é considerado fiável.

Em termos de evolução temporal, a solução desenvolvida foi sofrendo alterações e correcções consoante a detecção de problemas. Os testes de carga efectuados ao site público ainda em pré-produção permitiu observar o comportamento da centralização dos *logs* sobre uma carga considerável. Os resultados obtidos foram óptimos não tendo sido detectado qualquer problema no desempenho pretendido.

Outro ponto forte da solução é a sua velocidade de importação de *logs*, piorando só quando se executam tarefas concorrentes, que resultam em bloqueios de partes da base de dados. É bastante rápida e consegue trabalhar com grandes quantidades de informação. Com uma base de dados com um tamanho de 40 GB a importação de *logs* ocorre sem problemas. Os tempos de consulta é que aumentam, portanto restringiu-se a base de dados a 30 dias de *logs* e o desempenho estabilizou.

Em termos de facilidade de gestão de logs os benefícios depois da solução implementada são evidentes. O administrador passa a consultar um único sistema que mantém todos os *logs* armazenados e prontos a qualquer pesquisa. O processo de *backup* deixa de ser incerto, para um processo bem documentado e que é iniciado de forma automática, cabendo ao administrador/operador o mínimo de trabalho necessário. A segurança dos *logs* é nesta solução salvaguardada, bem como a segurança da instituição, caso aconteça algum problema. Os *logs* encontram-se centralizados dificultando a eliminação de provas por parte dos invasores do sistema. Benefício que é fundamental num mundo inseguro como o actual, repleto de *hackers*, *crackers* e de pessoas mal intencionadas.

5.3 Perspectivas de Trabalho Futuro

Durante o projecto foram feitos várias mudanças ao plano inicial bem como a alguns objectivos. Esta situação originou tempo dispendido em tarefas que acabaram por não ter efeitos práticos no projecto. Por exemplo estava previsto no início do projecto que seriam feitos testes efectivos a soluções de análise de *logs*, mas tal não se veio a verificar.

Relativamente à arquitectura desenhada o envio dos *logs* desde o Microsoft ISA até ao concentrador de *logs* não foi implementado devido à falta de tempo e a outras prioridades no projecto, mas já foi testado obtendo bons resultados. Outra funcionalidade que não foi efectivamente implementada foi o sistema secundário responsável pela recepção dos *logs* e reencaminhamento para o concentrador de *logs*. Como não existia máquina disponível para efectuar a sua implementação todos os procedimentos foram montados, mas não aconteceram testes práticos.

A análise dos *logs* é a principal carência do projecto porque mesmo montados os processos de recolha e centralização dos *logs*, a análise é feita de forma manual e reactiva. Idealmente deve haver uma monitorização em tempo real, com geração de alertas. O esperado será efectuar os testes devidos às soluções recomendadas e escolher a que melhor se adapta à infra-estrutura do Banco BPI.

Referências e Bibliografia

[1] *CSI/FBI Computer Crime and Security Survey*, http://www.gocsi.com/;

[2] Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Fredrick, Ronald W. Ritchey, *Inside Network Perimeter Security*, Sams, 2002;

[2] *RFC 3164 The BSD Syslog Protocol*, 2001

[3] *Lessons About SNMP*, http://www.et.put.poznan.pl/snmp/;

[4] *SNMP Tutorial*, http://www2.rad.com/networks/1999/snmp/;

[5] *Wikipedia: SNMP*, http://en.wikipedia.org/wiki/SNMP;

[6] *Wikipedia: MD5*, http://en.wikipedia.org/wiki/Md5;

[7] *Hash Collision*, http://www.cryptography.com/cnews/hash.html;

[8] *How Routers Work*, http://computer.howstuffworks.com/router.htm;

[9] *Wikipedia: Router*, http://en.wikipedia.org/wiki/Router;

[10] *Cisco IOS SNMP Traps Supported and How to Configure Them*, http://www.cisco.com/warp/public/477/SNMP/snmp_traps.html;

[11] *Cisco PIX*, http://www.cisco.com/go/pix;

[12] *Wikipedia:Firewall*, http://en.wikipedia.org/wiki/Firewall_networking;

[13] *Norma ISO 17799*

[14] *Logging and archiving: Where storage and security needs intersect*, http://www.computerworld.com/securitytopics/security/story/0,10801,93878,00.html

[15] *Corralling Security Data* , http://www.computerworld.com/securitytopics/security/story/0,10801,83978,00.html

[16] *Microsoft Systems Architecture: Internet Data Center*, http://www.microsoft.com/resources/documentation/msa/idc/all/solution/en-us/default.mspx

[17] *Manage logging and other data collection mechanisms*, http://www.cert.org/security-improvement/practices/p092.html

[18] *MD5 Hash SQL Server Extended Stored Procedure*, http://www.thecodeproject.com/database/xp_md5.asp

[19] *SEM Systems Defend Against Information and Regulatory Overload*, http://www.csoonline.com/analyst/report2132.html

[20] *Using events-per-second as a factor in selecting Security Event Management tools*, http://www.securitydocs.com/library/2732

[21] *The Ins and Outs of System Logging Using Syslog*, http://www.securitydocs.com/library/1629

[22] *Backup Basics*, http://www.dlttape.com/DLTtape/Backup+Basics

ANEXO A: Manual da Aplicação de Gestão *Backups* de *Logs*

Ecrã Inicial

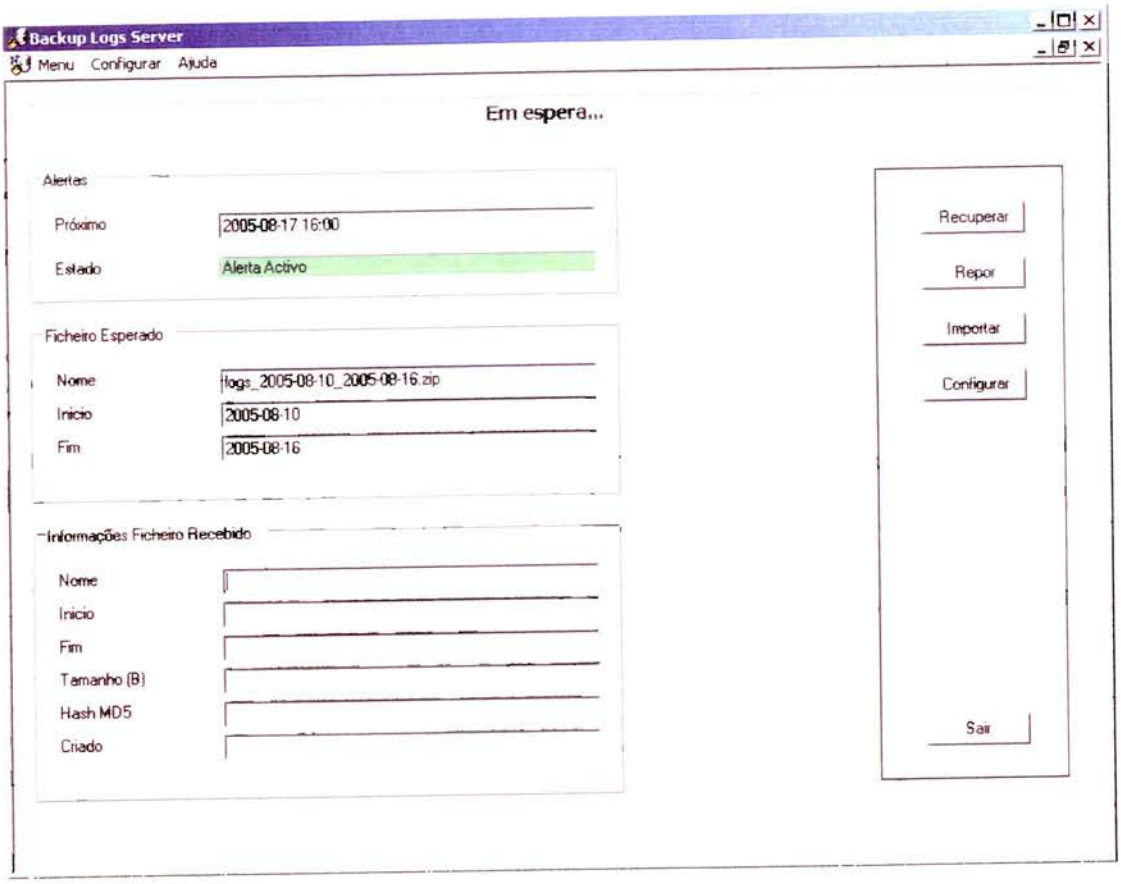


Figura 17 – Ecrã Inicial

Quando se inicia a aplicação é apresentado um formulário como o anterior. Neste, pode aceder-se a diversas funcionalidades como: recuperar suportes armazenados para analisar, repor no local de armazenamento, suportes que estavam em análise, importar ficheiros com *logs* de uma forma manual, configurar os locais de armazenamento dos suportes e também os operadores responsáveis pelo processo de *backups*, bem como as formas de serem alertados. Estas funcionalidades estão acessíveis através dos botões do lado direito e também através do menu superior.

Para além de aceder às várias funcionalidades, o ecrã inicial da aplicação apresenta informação do alerta para avisar os operadores de um *backup* em falta, informação do ficheiro que a aplicação deve receber e informações do ultimo ficheiro recebido.

Processo de *Backups*

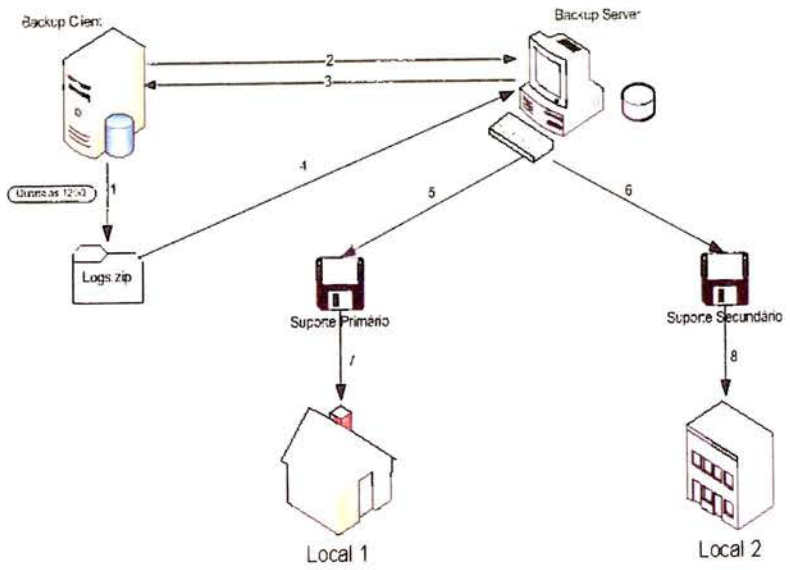


Figura 18 – Processo de *Backups*

Os *logs* dos equipamentos são exportados para uma base de dados SQL Server 2000. O processo de *backup* dos *logs* é iniciado às Quartas feiras de cada semana às 12:30, em que é executado um procedimento que gera um ficheiro comprimido no formato zip (1), com os *logs* de uma semana (da ultima 4ª feira a 3ª feira). Depois de criado o ficheiro, o mesmo procedimento executa a aplicação cliente que envia informação do ficheiro a efectuar *backup* (2). A aplicação servidora de *backups* quando recebe o pedido do cliente, acede ao servidor openssh existente no servidor de base de dados (3) e transfere o ficheiro de *logs* (4). Depois de validado o ficheiro recebido, este será gravado num DVD primário (5) e num secundário (6). Os dois suportes são validados e armazenados em locais diferentes (7 e 8). A aplicação regista o ficheiro guardado, os suportes usados e respectivo local de armazenamento.

Importação Manual de Ficheiros

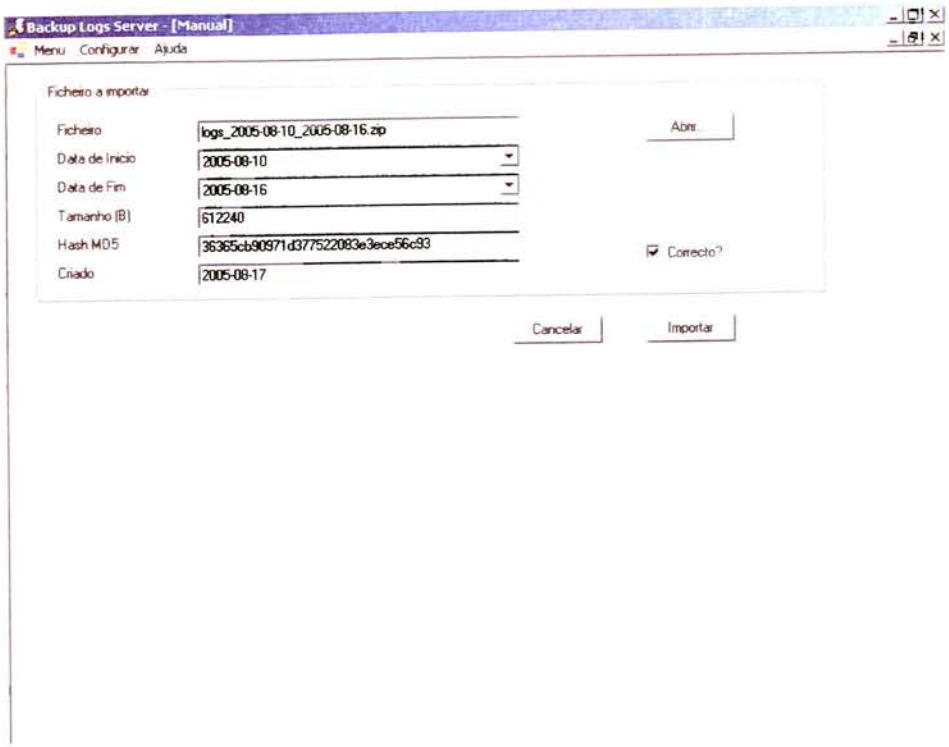


Figura 19 – Importação Manual de Ficheiros

Se por alguma razão o *backup* não poder ser feito de uma forma automática, consoante o processo definido, existe uma alternativa. No ecrã inicial da aplicação existe a opção de importar um ficheiro manualmente. Esta opção permite seleccionar um ficheiro existente no disco local, definir o intervalo de tempo de *logs* correspondente, efectuar a gravação e armazenamento do suporte. O operador deve exportar os *logs* da base de dados, e transferir o ficheiro comprimido para o servidor de *backups* e iniciar o processo de importação.

Recuperar para Análise

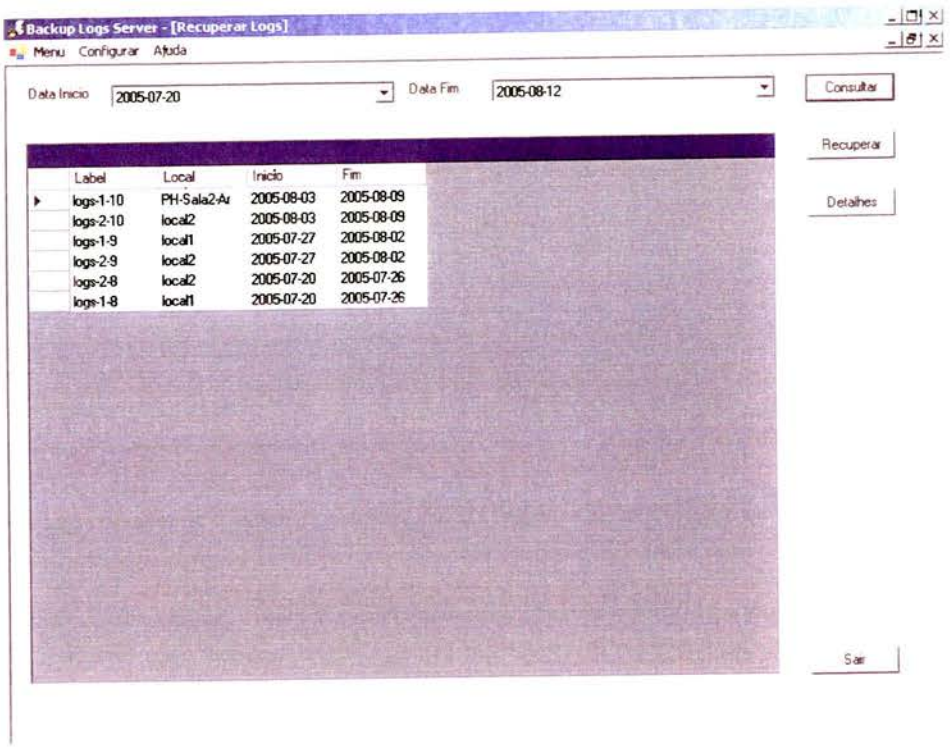


Figura 20 – Recuperar para Análise

Quando houver necessidade de se analisar os *logs* que já não se encontram na base de dados, deve ser feita a recuperação dos *backups* dos dias a analisar. Acedendo à opção de recuperação dos suportes, define-se qual a data de inicio a analisar e a data final. Clicando em "Consultar" obtém-se uma lista com os suportes e o seu local de armazenamento para o intervalo seleccionado. Para informar a aplicação de que os suportes foram recuperados e encontram-se em análise basta seleccionar os suportes e clicar em "Recuperar". Para ver os detalhes de cada suporte selecciona-se um suporte e clica-se no botão "Detalhes".

Repor Suportes em Análise

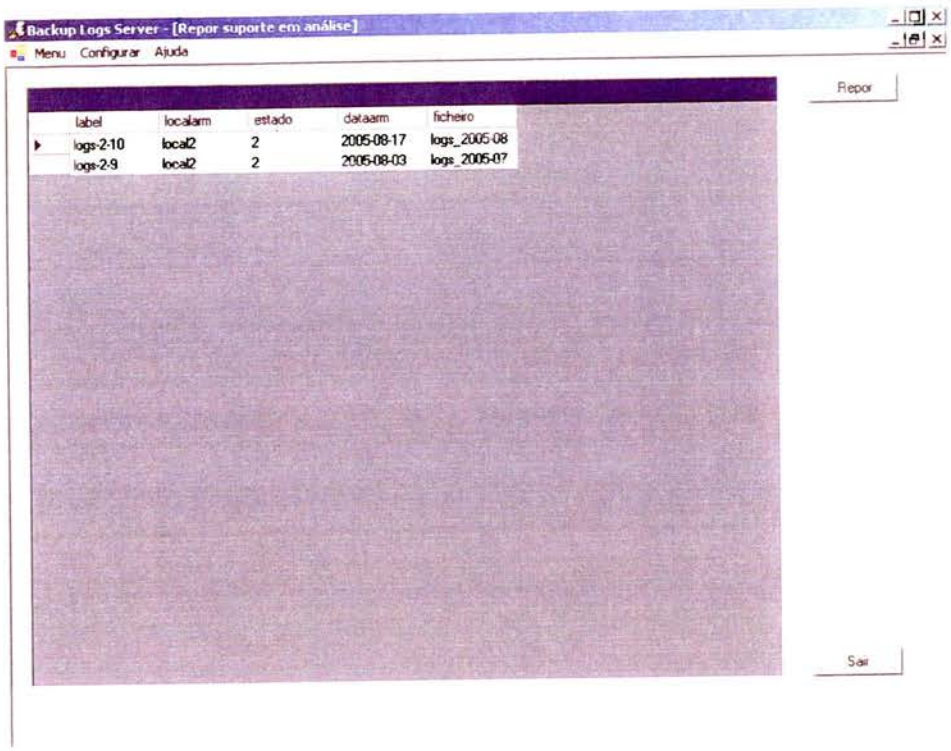


Figura 21 – Repor Suportes em Análise

Depois de serem feitas as análises pretendidas aos *logs* o operador deve recolocar os suportes nos locais onde estes se encontravam armazenados. Acedendo à opção "Repor" obtém-se uma lista com os suportes em análise e selecciona-se os suportes que serão rearmazenados nos locais originais. O operador deve colocar os suportes nos locais indicados.

Gravar Suportes

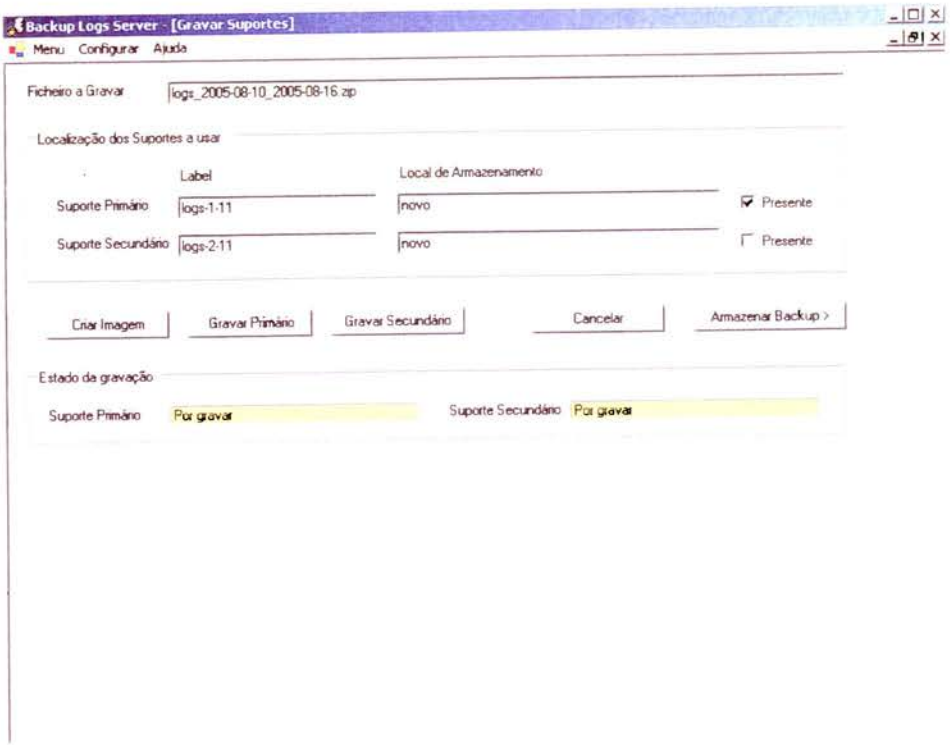


Figura 22 – Gravar Suportes

Quando se importa um ficheiro manualmente ou quando um ficheiro é transferido com sucesso para o servidor, são enviados alertas para os operadores activos e espera-se que estes dêem inicio ao processo de gravação dos suportes com os suportes esperados pela aplicação. Se for indicado um suporte novo o operador deve colocar um DVD novo, criar a imagem e iniciar a gravação. Caso o suporte indicado seja um suporte armazenado, o operador deve pegar no suporte com a *label* respectiva, que se encontra no local indicado pela aplicação e deve iniciar a gravação. Quando gravados com sucessos, devem-se armazenar os suportes em locais diferentes.

Armazenar Suportes

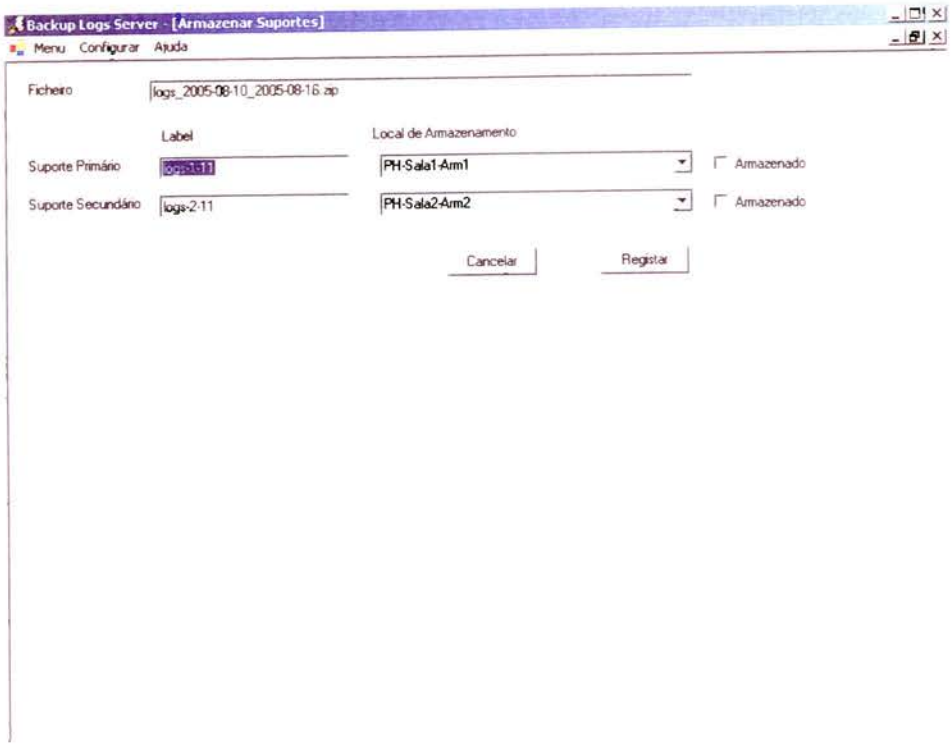


Figura 23 – Armazenar Suportes

Depois de gravados, os suportes devem ser armazenados em locais diferentes pelos operadores. Os locais indicados por defeito são os configurados na aplicação através da configuração a ver a seguir. O operador pode alterar o local de armazenamento dos suportes e deve assinalar na respectiva opção quando um suporte for armazenado.

Configurar Locais de Armazenamento

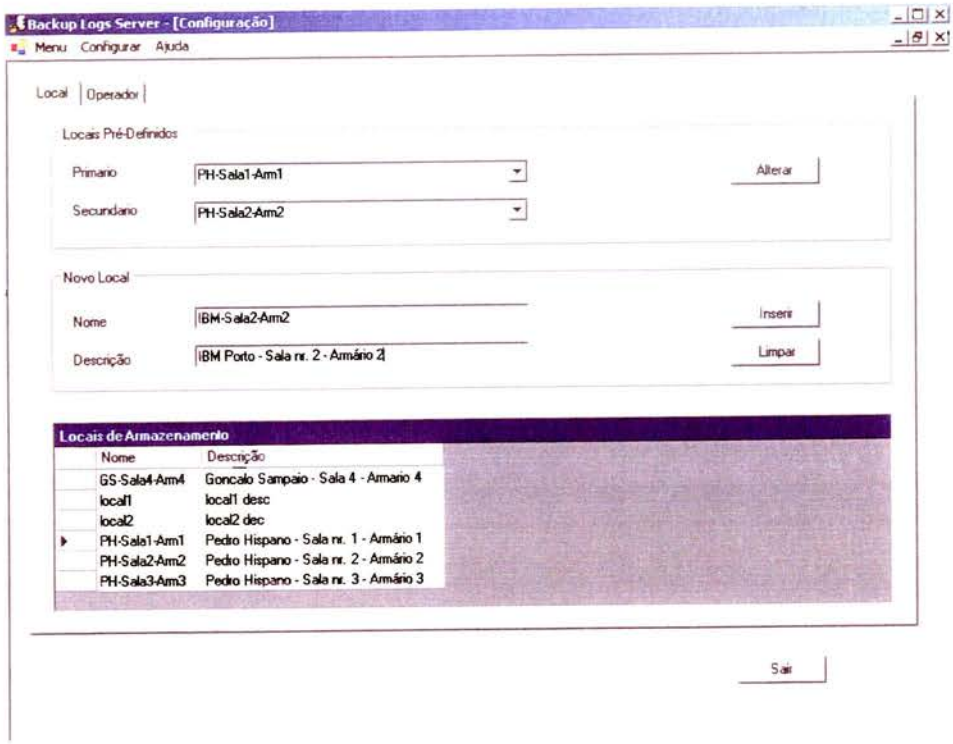


Figura 24 – Configurar Locais de Armazenamento

Para inserir novos locais de armazenamento ou para alterar os locais definidos por defeito, pode-se aceder à opção "Configurar" e seleccionar o painel "Local". Para alterar os locais pré-definidos deve-se seleccionar o local por defeito para cada suporte. Para inserir um novo local basta preencher os campos "Nome" e "Descrição", clicando em "Inserir" de seguida.

Configurar Operadores

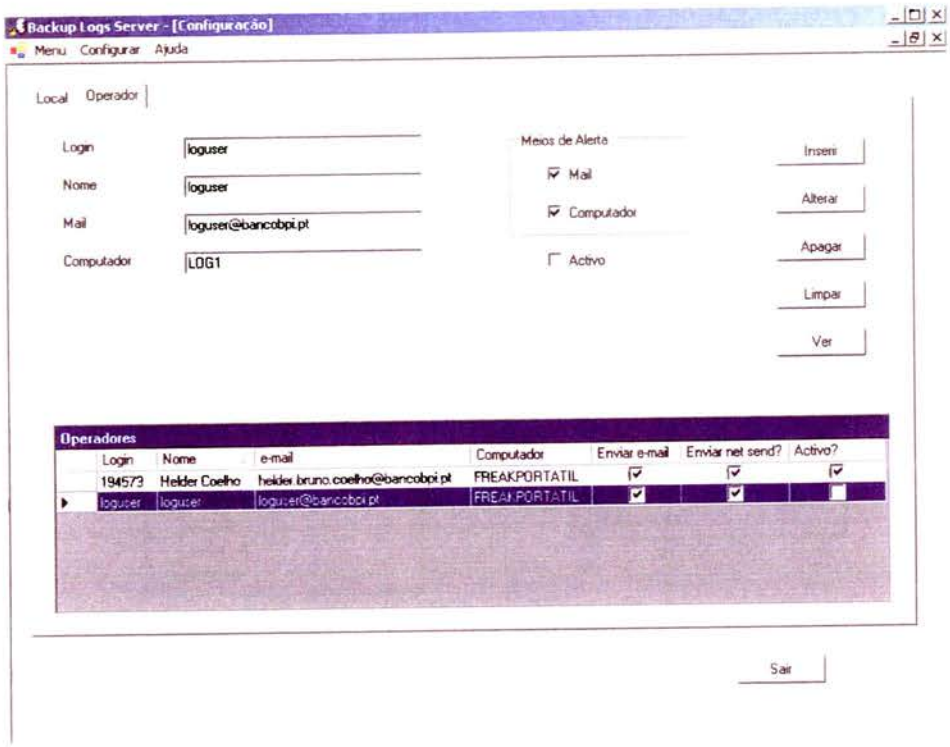


Figura 25 – Configurar Operadores

Para além de definir os locais de armazenamento é possível definir quais os operadores que serão alertados e de que forma. É possível também inserir, alterar e apagar operadores. Para apagar um operador, selecciona-se o operador pretendido e clica-se em "Apagar". Para alterar um operador, selecciona-se o pretendido, clica-se em "Ver", alteram-se os campos necessários e depois clica-se em "Alterar". Os operadores que estejam com a opção "Activo" assinalada, recebem os alertas gerados pela aplicação. Os operadores podem ser alertados via "net send" ou "e-mail", consoante os modos de alerta assinalados para cada um dos operadores.

Esquema de Base de Dados da Aplicação

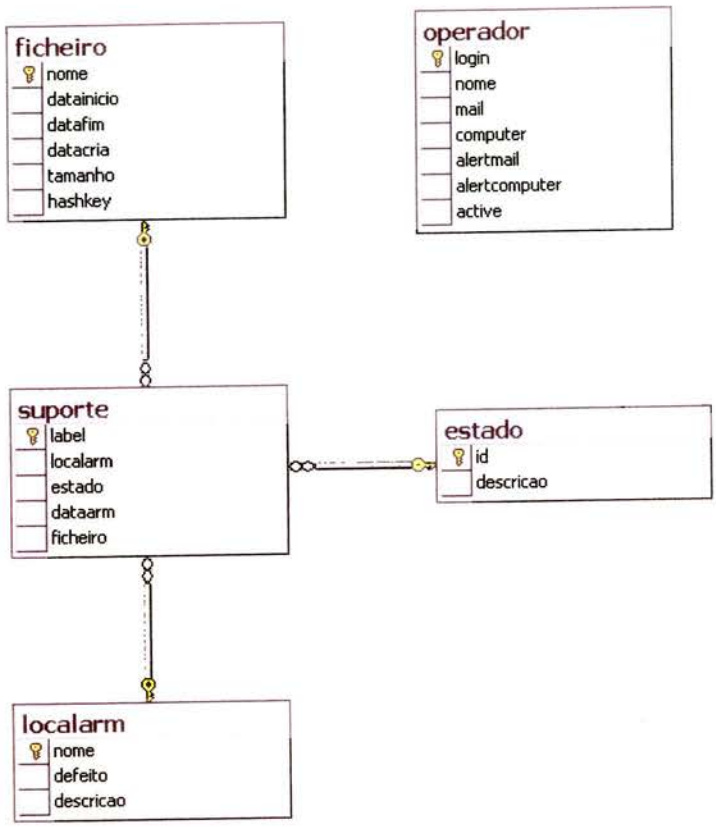


Figura 26 – Esquema de Base de Dados da Aplicação

Esquema de Base de Dados da Aplicação

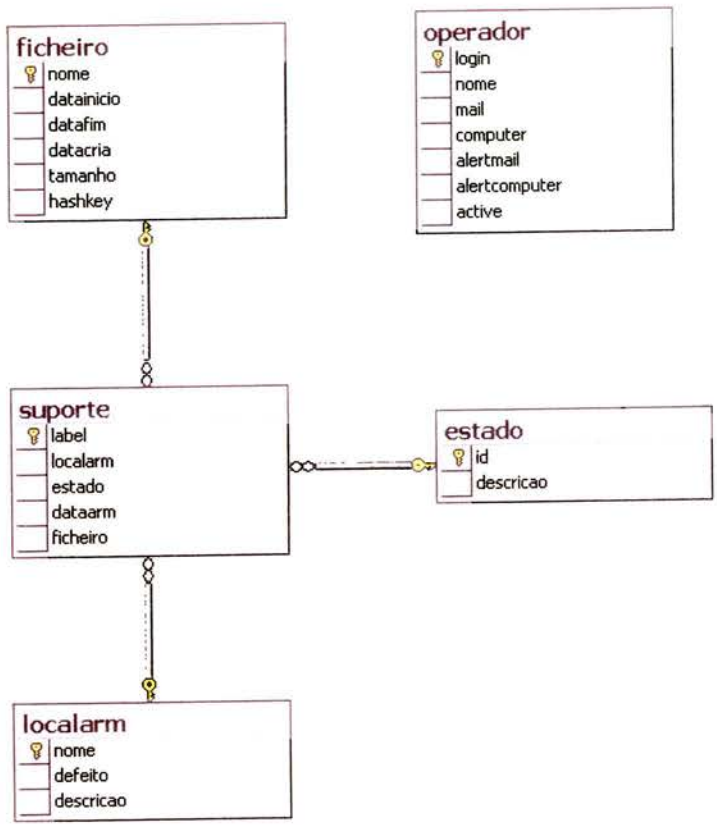


Figura 26 – Esquema de Base de Dados da Aplicação