SEGURANÇA CONTRA INTRUSÃO EM REDES INFORMÁTICAS

Nuno Filipe Lopes da Costa Duarte

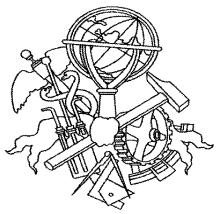
Mestrado em Engenharia Electrotécnica e de Computadores
Área de Especialização de Telecomunicações
Departamento de Engenharia Electrotécnica
Instituto Superior de Engenharia do Porto

2008

Este relatório satisfaz, parcialmente, os requisitos que constam da Ficha de Disciplina de Tese/Dissertação, do 2º ano, do Mestrado em Engenharia Electrotécnica e de Computadores

Candidato: Nuno Filipe Lopes da Costa Duarte, Nº 1980937, nfduarte@sapo.pt

Orientação científica: Jorge Botelho da Costa Mamede, jbm@isep.ipp.pt



Mestrado em Engenharia Electrotécnica e de Computadores
Área de Especialização de Telecomunicações
Departamento de Engenharia Electrotécnica
Instituto Superior de Engenharia do Porto

20 de Dezembro de 2008

Dedico este trabalho ao meu irmão e esposa, Fernando e Carla Duarte.

Agradecimentos

Este trabalho não poderia ser desenvolvido sem o apoio de algumas pessoas, às quais deixo aqui os meus sinceros agradecimentos:

Ao Professor Doutor Jorge Mamede – que aceitou a orientação desta tese – pela ajuda e aconselhamento prestados ao longo de todo o projecto. O seu auxílio e dedicação no desenvolvimento da tese foram essenciais para concluir este projecto com sucesso.

Um agradecimento especial aos meus pais, irmão e esposa, pelo apoio dado, sem o qual não seria possível embarcar neste projecto.

Finalmente, agradeço a todos os colegas e amigos que, directa ou indirectamente, colaboraram ou contribuíram, das mais diversas formas, para a conclusão da dissertação.

A todos o meu sincero muito obrigado.

Resumo

Devido ao facto de hoje em dia a informação que é processada numa rede informática empresarial, ser cada vez mais de ordem confidencial, torna-se necessário que essa informação esteja o mais protegida possível. Ao mesmo tempo, é necessário que esta a informação esteja disponível com a devida rapidez, para os parceiros certos, num mundo cada vez mais globalizado.

Com este trabalho pretende-se efectuar o estudo e implementação da segurança, numa pequena e genérica rede de testes, que facilmente seja extrapolada, para uma rede da dimensão, de uma grande empresa com potenciais ramificações por diversos locais.

Pretende-se implementar/monitorização segurança quer externamente, (*Internet service provider ISP*) quer internamente (activos de rede, postos de trabalho/utilizadores). Esta análise é baseada na localização (local, *wireless* ou remota), e, sempre que seja detectada qualquer anomalia, seja identificada a sua localização, sendo tomadas automaticamente acções de protecção.

Estas anomalias poderão ser geridas recorrendo a ferramentas *open source* ou comerciais, que façam a recolha de toda a informação necessária, e tomem acções de correcção ou alerta mediante o tipo de anomalia.

Abstract

By the fact of nowadays the information that is processed in an enterprise network, must be each time, more than confidential, it becomes necessary to protect this information. At the same time, it is necessary to provide this informatation to become available as soon as possible, for the certain partners, with the globalization of the world.

With this work, it is intended to study and implement security guard, in a small generic network prototype. In this case, is easily to export to network with a dimension of a great company, with potential ramifications, in diverse places.

It is intended to implement/monitoring external security, (Internet service to sevice provider ISP), or internal security (networking equipment, servers, hosts or users). This analizes is based in the localization (local, remote or wireless), and whenever any anomaly is detected, and it can identifyed quickly, being taken an automatically protection.

These anomalies could be managed appealing to the commercial or open source tools, which make possible to get all the necessary information, and take the necessaries measures of alerting or correcting that type of anomaly.

Índice

Índice de Figuras

Índice de Tabelas

Notação e Glossário

3DES *Triple Data Encryption Standard* – é um padrão de encriptação de dados baseado no algoritmo DES desenvolvido pela IBM em 1974.

802.1X Standard da IEEE para o controlo de acesso à rede, usado nas redes 802.11 como mecanismo de autenticação. É baseado no EAP.

AAA Authentication, Authorization, Accounting. São os três procedimentos básicos da segurança da informação. Verificar a identificação do utilizador que requere a informação; dar permissões ao utilizador para usar / modificar essa informação; controlar os acessos dos utilizadores aos recursos do sistema.

AES *Advanced Encryption Standard*

AIX *Advanced IBN Unix*

ARP *Address Resolution Protocol* – é um protocolo usado para encontrar um endereço Ethernet – *Media Access Control* (MAC) *address* – a partir do endereço IP.

ASCII *American Standard Code for Information Interchange* – é uma codificação de caracteres de sete bits baseada no alfabeto inglês

AP *Access Point* – é um dispositivo de uma rede sem fios que realiza a conexão entre todos os dispositivos móveis.

Backups O conceito de *backup* ou cópia de segurança está relacionado com a necessidade constante de guardar cópias de informação relevante, normalmente em dispositivos físicos diferentes, prevenindo situações de falhas e outros incidentes nos dados originais. Actualmente, é comum os *backups* serem guardados em localizações geográficas distantes prevenindo catástrofes maiores como incêndios, roubos e terramotos.

Bridge É o termo utilizado em informática para designar um dispositivo que liga duas ou mais redes informáticas que usam protocolos distintos ou iguais, ou dois segmentos da mesma rede que usam o mesmo protocolo.

BSS *Basic Service Set*

CCMP Counter Mode Cipher Block Chaining MAC Protocol

Cluster É um conjunto de computadores que se interligam através de um sistema não fragmentado. Tem por objectivo dividir um certo processamento de dados com outras máquinas ligadas na mesma rede para acelerar o tempo total de processamento.

DC *Domain Controler* – Controlador de Domínio da Directoria Activa da *Microsoft*

DNS *Domain Name System* – (Sistema de Nomes de Domínios) é um sistema de gestão e atribuição de nomes hierárquico.

DHCP É um protocolo que define um conjunto de regras usadas por dispositivos de comunicação tais como um *router* ou placa de rede, permitindo a estes dispositivos pedir e obter endereços IP de um servidor contendo uma lista de endereços disponíveis para atribuição.

Dial-Up É um tipo de acesso à Internet no qual uma pessoa usa um modem e uma linha telefónica para se ligar a um nó de uma rede de computadores do ISP.

DMZ Delimitarized Zone. Para a segurança de computadores, DMZ é a área de rede que permanece entre a rede interna de uma organização e uma rede externa, em geral a internet. Normalmente, uma DMZ contém equipamentos apropriados para o acesso à internet, como servidores web (HTTP), servidores de transferência de arquivos (FTP), servidores de e-mail (SMTP) e servidores DNS.

EAP-TLS Extensible Authentication Protocol (Transport Layer Security) – Protocolo de segurança usado em redes sem fios. Proporciona alta segurança a sistemas de rede *wi-fi*.

Ethernet É uma tecnologia de interligação para redes locais – *Local Area Networks* (LAN) – baseada no envio de pacotes.

Firewall É um dispositivo de uma rede de computadores que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão e/ou recepção de dados nocivos ou não autorizados de uma rede para outra.

Firmware É um tipo de software que controla directamente o hardware. É armazenado permanentemente num chip de memória de hardware, como uma ROM ou EPROM ou em memória flash tipo EEPROM. Exs.: BIOS de computador, Leitores CD, micro-ondas digital, iPod, dispositivos com display, entre outros.

Framework No desenvolvimento do *software*, uma *framework* ou enquadramento é um ambiente integrado de suporte ao desenvolvimento de projectos de *software*. Uma *framework* pode incluir programas de suporte, bibliotecas de código, linguagens de *scripting* e outros módulos para auxiliar no desenvolvimento e unir diferentes componentes de um projecto de *software*.

FTP *File Transfer Protocol* – é um protocolo de transferência de ficheiros através da Internet bastante rápido e versátil.

Gateway Um *Gateway*, ou *porta de ligação*, é uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos.

Get Um dos métodos do objecto "*form"* (GET|POST), para transmissão de informação em formulários via internet. Enquanto que o GET anexa os dados inseridos ao URL, o método POST junta-os aos cabeçalhos http.

GPL *General Public License* – é a designação da licença para software livre idealizada por Richard Stallman no final da década de 1980, no âmbito do projecto GNU da Free Software Foundation (FSF).

Hacker Hacker é o termo originário do inglês usado para designar pessoas que criam e modificam software e hardware de computadores. Actualmente, é usado para designar crackers, ou seja, pessoas que praticam actos ilegais ou sem ética.

Host Um Host pode ser considerado um qualquer dispositivo físico com capacidade de conexão a uma rede, identificando-se através de um IP, permitindo a transmissão de informação de/para outros hosts.

http *HyperText Transfer Protocol* – Protocolo de transferência de Hipertexto.

HTML *HyperText Markup Language* – Linguagem de anotação de documentos.

HP OpenView Procurve Manager *Procurve Manager Plus* (PMP) – é um produto de gestão de redes da OpenView do grupo Hewlett Packard. Este protocolo utiliza SNMP para comunicar com os componentes de uma rede, possibilitando a auto-descoberta, monitorização e controlo remotos.

HTTPS *HyperText Transfer Protocol Secure* – é uma implementação do protocolo HTTP sobre uma camada SSL ou TLS. Esta camada adicional permite que os dados sejam transmitidos através de uma conexão encriptada e verifica a autenticidade do servidor e do cliente através de certificados digitais.

ICMP *Internet Control Message Protocol* – é um protocolo integrante do Protocolo IP, definido pelo RFC 792, e utilizado para fornecer relatórios de erros à fonte original.

IEEE Institute of Electrical & Electronics Engineers, Inc.

IP *Internet Protocol* – é um protocolo usado entre duas ou mais máquinas em rede para encaminhamento dos dados.

IRIX Silicon Graphics Unix

ISEP Instituto Superior de Engenharia do Porto

ISP *Internet Service Provider* – é um fornecedor de serviços que oferece acesso à Internet.

Kerberos É o nome de um protocolo de transporte de rede, que permite comunicações individuais seguras e identificadas, numa rede insegura.

Kernel Núcleo de um sistema operativo. Representa a camada de *software* mais próxima do *hardware*, sendo responsável por gerir os recursos do sistema operativo.

LAN *Local Área Network* – Redes de Acesso Local: redes de pequena escala, reduzidas normalmente a um andar ou edifício.

Linux É o termo geralmente usado para designar qualquer sistema operativo que utilize o *kernel* Linux desenvolvido por Linus Torvalds.

MAC *Media Access Control* – é o endereço físico da interface de rede.

MD5 *Message Digest 5 Algorithm*

MITM *Man In The Middle* – técnica de forjar uma identidade, colocando-se entre duas entidades numa comunicação

MTU *Master Terminal Unit* – Unidade principal vulgo máquina central.

Multiplexer Um multiplexador, mux ou multiplexer é um dispositivo que codifica as informações de duas ou mais fontes de dados num único canal.

NTP *Network Time Protocol* – é um protocolo desenvolvido para permitir a sincronização dos relógios dos sistemas de uma rede de computadores.

Overhead O *overhead* é geralmente considerado qualquer processamento ou armazenamento em excesso, seja de tempo de computação, de memória, de largura de banda ou qualquer outro recurso que seja requerido para ser utilizado ou gasto para executar uma determinada tarefa.

PDA *Personal Digital Assistant* – Dispositivo portátil, normalmente com ecrã táctil, que tem algumas funcionalidades que o assemelham a um pequeno computador, como gestão de documentos, jogos, internet, e-mail, comunicação sem fios, entre outras. Usado em grande parte para processamento de pedidos, p. ex. em empresas de restauração.

PIN *Personal Identification Number* ou Número de Identificação Pessoal

PKI *Public Key Infrastructure* – é um órgão ou iniciativa pública ou privada que tem como objectivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de credibilidade e confiança em transacções entre partes que utilizam certificados digitais.

POP3 *Post Office Protocol version 3* – protocolo de recepção de mail

Post Método do objecto *"form"* que permite juntar os dados de um formulário aos cabeçalhos http. Os dados não persistem, como no método GET, mas por outro lado não há a limitação do tamanho do URL, dado que os dados são "invisíveis".

PPPoE *Point-to-Point Protocol over Ethernet* – é um protocolo para conexão de clientes de uma rede IP à Internet.

PPP *Point-To-Point Protocol* – é um protocolo que foi desenvolvido e padronizado através da RFC 1548 (1993) com o objectivo de transportar todo o tráfego entre 2 dispositivos de rede através de uma conexão física única.

Prompt Nos sistemas operativos que dispõe de modo de linha de comando a *prompt* é constituída por um ou mais símbolos que indicam o local a partir do qual o utilizador deve digitar uma instrução num terminal de comandos.

PSK Pre-shared Key

Radius Remote Authentication Dial In User Service – é um protocolo AAA para aplicações para acesso à rede de computadores e mobilidade através de rede IP.

RC4 É o algoritmo de encriptação de fluxos de dados muito popular utilizado em protocolos, como SSL (para proteger o tráfego Internet) e WEP (para a segurança de redes sem fios).

RPC *Remote Procedure Call* – Chamadas a procedimentos remotos

Router É um equipamento usado para fazer a comutação de protocolos, a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes entre si.

RSN *Robust Security Network*

Scripting Language É uma linguagem baseada em guiões/comandos que é interpretada linha a linha. Estes tipos de linguagens são executados por interpretadores específicos.

SHA-1 *Secure Hashing Algorithm 1*

SNMP *Simple Network Management Protocol* – é um protocolo de gestão típico de redes TCP/IP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores.

SMTP *Simple Mail Transfer Protocol* – é o protocolo padrão para envio de *e-mails* através da Internet.

SMS *Short Message Service* – Serviço de Mensagens Curtas.

Socket É o ponto terminal de uma comunicação bidireccional através de uma rede IP entre dois programas.

SSH *Secure Shell* – é simultaneamente, um programa de computador e um protocolo de rede que permite a conexão com outro computador na rede, de forma a executar comandos de uma unidade remota.

SSID *Service Set Identifier*

ODBC *Open Data Base Connectivity* – é um padrão para acesso a servidores de bases de dados.

TCP/IP Conjunto de protocolos de Internet que implementa um modelo por camadas para troca de dados.

Telnet É um protocolo cliente-servidor de comunicações usado para permitir a comunicação entre computadores ligados numa rede baseada em TCP.

TCP *Transmission Control Protocol* – é um protocolo do nível da camada de transporte (camada 4) do Modelo OSI e é sobre o qual assentam a maioria das aplicações web, como o SSH, FTP, HTTP, a *World Wide Web*.

TKIP *Temporal Key Integrity Protocol.*

TLS/SSL *Transport Layer Security / Secure Socket Layer* – são protocolos de encriptação que fornecem comunicação segura na Internet para serviços como *e-mail* (SMTP), navegação (HTTP) e outros tipos de transferência de dados.

Trojan *Trojan Horse* é um programa que entra num computador e liberta uma porta para um possível invasor (vírus).

UDP *User Datagram Protocol* – significa Protocolo de Datagramas do Utilizador e faz a entrega de mensagens independentes, designadas por datagramas, entre aplicações ou processos, em sistemas *host*.

Unix Unix é um sistema operativo multitarefa e multiutilizador originalmente criado por Ken Thompson, que trabalhava nos Laboratórios Bell (Bell Labs) da AT&T.

UPS *Uninterruptible Power Supply* – Fonte ininterrupta de tensão DC, que permite mantém máquinas ligadas durante um período de tempo aquando de falhas de corrente.

VPN *Virtual Private Network* – é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet).

WEP Wireless Encryption Protocol – sistema baseado num segredo partilhado, só conhecido entre os terminais e os Access Points. No entanto, apresenta deficiências técnicas, as quais podem ser quebradas em muito pouco tempo.

WPA O WPA surgiu como alternativa ao 802.11i, de forma a proteger eficazmente as redes Wi-Fi. O Wi-Fi é baseado no draft 3.0 do 802.11i, lançado em 2002, sendo na prática um RSN "incompleto", pois só possui TKIP sem CCMP e não possui qualquer tipo de suporte ao modo Ad-hoc.

XML *eXtensible Markup Language* – É um subtipo de SGML (*Standard Generalized Markup Language*) ou Linguagem Padronizada de Marcação Genérica capaz de descrever diversos tipos de dados.

1. INTRODUÇÃO

Este é o capítulo que dá início à tese de Mestrado que tem por tema a "Segurança contra intrusão em redes informáticas". O amplo conceito de redes, a generalização e globalização dos sistemas informáticos, está cada vez mais em voga na sociedade, e em especial, em Portugal, pela sua actual evolução neste campo. Neste capítulo introdutório, serão descritos alguns dos aspectos do desenvolvimento deste projecto e algumas características sobre o seu teor tecnológico. Também serão feitas algumas observações relativas aos objectivos propostos à organização desta tesa.

1.1. CONTEXTO

No passado, a "segurança da informação", era um termo usado para descrever as medidas de segurança físicas, usadas para manter a informação vital do governo ou negócio protegido. Esta protecção seria do alcance público, e, devia ser evidente contra consulta, alterações ou destruição. Isto foi feito, armazenando originais valiosos em armários, ou cofres fechados de arquivo, e restringindo o acesso físico às áreas onde os originais eram mantidos.

Com o crescimento do número de computadores e de meios electrónicos, a forma de obter dados mudou. À medida que a tecnologia continuou a evoluir, os sistemas computadorizados foram interligados, para dar origem às redes. Esta interligação permitiu

que os sistemas partilhassem recursos, chegando finalmente à principal rede, publicamente acessível, a Internet. Embora os métodos de assegurar a informação mudem constantemente, o conceito da segurança das redes permanece o mesmo que o da segurança da informação.

Uma vez que os computadores podem armazenar, recuperar, e processar grandes quantidades de dados, são usados em quase tudo nas nossas vidas. As redes, e a Internet, são uma parte integral de muitos negócios, e a nossa dependência dos computadores continua a aumentar. Enquanto os negócios e os indivíduos se tornam mais confortáveis com tecnologia, levam a avanços da tecnologia, sendo elaborados sistemas, cada vez mais amigáveis e mais fáceis de interligar.

Um sistema computadorizado, requer ferramentas automatizadas, para proteger os dados dos utilizadores que têm acesso local aos sistemas. Sempre que um utilizador esteja ligado a uma rede, requer que os dados processados nesse sistema estejam protegidos, não apenas do acesso local, de eventuais acessos remotos não autorizados, e, da intercepção ou alteração durante a sua transmissão.

Pretende-se então, desenvolver um estudo e apresentar algumas soluções técnicas para uma rede empresarial, de forma ir de encontro às necessidades e exigências específicas das organizações.

A partir do estudo dos requisitos do sistema, e da extensa pesquisa das soluções existentes, serão determinadas as características necessárias para as ferramentas a desenvolver. A solução encontrada deverá ir de encontro às necessidades de um modo geral das organizações em que estas se inserem.

1.2. CONTRIBUTOS

A presente Tese abrange, uma área importante da monitorização e segurança de redes informáticas. Geralmente, neste domínio, recorrem-se a ferramentas *open source* ou então proprietários (quando possível), e protocolos de comunicação padrão, para interligar equipamentos locais e remotos. Neste contexto, irão ser analisados este tipo de sistemas, e estudado o problema da segurança em rede, particularizando-se as soluções que o mercado disponibiliza. A solução a adoptar, deverá assegurar a funcionalidade, a estabilidade e minimizar o custo associado à sua exploração. Esta solução deverá aferir com eficácia, o

nível das ameaças existentes, nas redes empresariais de acesso à Internet. Por outro lado, deverá ser possível, aprender mais sobre as ferramentas, tácticas e motivos da comunidade "*hacker*".

A informação obtida, permite desenvolver estratégias para proteger de forma mais eficaz, as redes informáticas, contra as ameaças existentes, e novos tipos de ataques na Internet.

A área da segurança informática tem sido puramente defensiva. O problema inerente a esta abordagem, prende-se com o facto do intruso, ter sempre a iniciativa. Desta forma, está sempre um passo à frente, que faz com que seja difícil, proteger eficazmente uma rede de comunicações. As soluções implementadas neste projecto abordam o problema de uma forma pró-activa visando mitigar este problema.

1.3. APRESENTAÇÃO E PLANEAMENTO

A tese de Mestrado em Engenharia Electrotécnica – Área de especialização em Telecomunicações – foi elaborada no âmbito de um projecto proposto ao Instituto Superior de Engenharia do Porto (ISEP). O projecto teve a duração aproximada de um ano e foi desenvolvido no ISEP no Departamento de Engenharia Electrotécnica, e, teve como orientador o Professor Doutor Jorge Mamede por parte ISEP.

1.3.1. PLANEAMENTO DE PROJECTO

Este projecto foi organizado em seis fases, definidas da seguinte forma:

Fase 1 – Estudo dos problemas a limitar ou eliminar com a segurança;

Fase 2 – Análise de métodos e ferramentas usadas para melhoria da segurança de redes;

Fase 3 – Definição de uma rede de estudo;

Fase 4 – Implementação das soluções estudadas para segurança da rede;

Fase 5 – Definição e execução de teste à segurança da rede;

Fase 6 – Escrita da Tese.

1.3.2. REUNIÕES DE ACOMPANHAMENTO

As reuniões de acompanhamento que ocorreram ao longo deste trabalho, à medida que as datas para a previsão de conclusão das fases anteriormente definidas iam sendo atingidas, datando-se da seguinte forma:

Fase 1 – Final de Dezembro de 2007

Fase 2 – Final de Março de 2008

Fase 3 – Final de Abril de 2008

Fase 4 – Final de Junho de 2008

Fase 5 – Final de Julho de 2008

Fase 6 – Meados de Setembro de 2008

1.4. ORGANIZAÇÃO DO RELATÓRIO

Esta tese é composta pelo estudo da área de segurança e monitorização, para conhecer equipamentos existentes, soluções e tecnologias utilizadas. São apresentadas soluções, descrito o *hardware* utilizado e o *software* desenvolvido. As funcionalidades do projecto são apresentadas, seguidas de uma conclusão, onde se apresenta um estudo das ferramentas desenvolvidas, e de uma proposta de melhoramentos. De uma forma mais detalhada, relatório é composto pelos capítulos a seguir enunciados.

O capítulo 1 consiste na apresentação da tese. É definida a calendarização do trabalho e a estrutura da tese desenvolvida.

O capítulo 2 corresponde à análise de vulnerabilidades e da forma como podem ser usadas, para tirar partido do sistema por parte de terceiros. São também tratadas as ameaças mais comuns, em redes *ethernet* e *wi-fi (Local Area Network* - LAN), e enunciadas formas de evitar esses ataques.

O capítulo 3 pretende descrever, de forma extensa e pormenorizada, as regras e métodos necessários para a implementar um sistema de forma correcta e segura. São definidos conceitos de políticas de segurança, e, referidas formas para obter uma configuração óptima. Ainda neste capítulo, é visto como configurar e verificar um sistema, utilizando sistemas de monitorização e eliminando protocolos inseguros, bem como a definição e configuração de *firewalls* e acessos externos seguros.

No capítulo 4 são enunciadas estratégias, para implementar soluções físicas e lógicas para obter um melhor rendimento e desempenho do sistema, bem como implementar soluções de segurança e de restauro em caso de perdas. É feita referência às redes por *ethernet* e s/fios e como configurar ambas da melhor forma. São também enumerados os passos para a instalação do sistema, desde a criacção de partições, passando pela instalação de *software* de sistema, até à instalação e configuração de aplicações e serviços de segurança (anti-vírus, anti-spam, políticas de acesso em rede e web, prevenção de abuso de recursos, entre outros).

No capítulo 5 é definida a rede de estudo, sem segurança. O sistema escolhido para análise e implementação é aqui apresentado, e definido toda a sua configuração. Também neste capítulo é possível demonstrar como o sistema está vulnerável, face a uma configuração se segurança básica e vulnerável a ataques.

O capítulo 6 consiste na reconfiguração da rede de estudo, aplicando as correcções necessárias para eliminar as vulnerabilidades encontradas, e minimizar as possibilidades de sucesso em caso de ataques ao sistema. Estas correcções passam por instalação de *software* adicional (e-Trust), pela correcção das configurações das aplicações já instaladas (spamhaus, shorewall), pelas actualizações de sistema (*windows updates*), e autenticação dos utilizadores à infraestrutura.

O capítulo 7 corresponde às conclusões da tese, onde é referido todo o trabalho, aprendisagem, problemas encontrados e respectivas soluções, bem como uma análise pessoal do tema em causa face à actual situação dos sistemas de informação em relação à segurança informática.

2. VULNERABILIDADES E AMEAÇAS

Para compreender as vulnerabilidades e ameaças, é necessário relembrar, que os computadores, independentemente do seu avanço tecnológico, são apenas máquinas que trabalham com instruções predeterminadas. Os sistemas operativos e outros pacotes de software, são simplesmente, instruções compiladas que o computador usa, transformando *input* em *output*. Um computador, não pode determinar, a diferença entre entradas autorizadas e não autorizadas, salvo quando tal informação está escrita nas instruções. Posto isto, qualquer software que um utilizador pode modificar, ou ter acesso (que não foi especificamente concebido pelo software) é chamado vulnerabilidade. Na maioria dos casos, um intruso ou *hacker,* obtém acesso a uma rede ou computador, através da exploração uma vulnerabilidade. É possível aceder remotamente a um computador, em qualquer dos 65535 portos.

À medida que a tecnologia do hardware e software continua a evoluir, no intuito de o tornar mais segura, o "outro lado" continua a procurar a e descobrir novas vulnerabilidades. Por esta razão, a maioria dos fabricantes de software, continuam a produzir correcções (patchs) para os seus produtos, à medida que novas vulnerabilidades são descobertas.

As potenciais ameaças costumam definir-se nas duas seguintes categorias [1][4]:

- **Ameaças estruturadas** – Ameaças que são planeadas e focalizadas para um alvo específico, sendo um esforço organizado, para entrar numa rede ou numa organização específica.

- **Ameaças não estruturadas –** Esta ameaça é a mais comum, visto ser aleatória e ser o resultado dos *hackers* que procuram um alvo por oportunidade. Com a abundância de scripts que estão disponíveis na Internet, estes podem ser usados, para efectuar pesquisas às redes desprotegidas em busca de vulnerabilidades. Porque os scripts estão disponíveis livremente e funcionam com poucos recursos, na óptica do utilizador e de hardware, estes são usados extensamente através da Internet. Muitas ameaças não estruturadas, não são de uma natureza maliciosa, ou para nenhuma finalidade específica. Muitas vezes começam como de "a oportunidade faz o ladrão" se tratasse, sendo muitas vezes *hackers* principiantes que querem ver o que podem fazer.

2.1. VULNERABILIDADES DE SOFTWARE

Muitas vulnerabilidades relacionadas com software, podem ser evitadas aplicando-se técnicas de engenharia de software, durante o processo do desenvolvimento deste, antecipando possíveis ataques. Por exemplo, colocação de parâmetros de verificação, que podem ser incorporado no software para impedir ataques por *buffer overflow*.

Alguns problemas relacionados com software são descritos em seguida [1][2]:

- **Permissões sem controlo** – Se os utilizadores tiverem permissões instalar ou correr software na rede, este é mais vulnerável aos vírus, interacções inesperadas do software, e à subversão de controlos da segurança, como os cavalos de Tróia.

- **Teste de software** – Um o processo rígido e formal para testar software, é necessário para determinar a compatibilidade, com aplicações feitas ou instaladas, ou para identificar interacções não previstas. Este procedimento, deve também aplicar-se, para que se possa efectuar melhoramentos do software ou dos procedimentos de segurança deste [27].

- **Utilitários de software** – Utilitários de software, podem comprometer a integridade de sistemas e controlo de acesso, quando usados indevidamente.

Utilitários que permitem testar as vulnerabilidades de um sistema, quando usados com fins duvidosos, pode ser prejudiciais. Posto isto o uso destes utilitários deve ser controlado por políticas de segurança nomeadamente permissão ou proibição de instalar e/ou correr software nos sistemas.

- **Software de armazenamento seguro** – Uma combinação de controlo de acesso físico e lógico, deve ser implementado para assegurar que as cópias de segurança ou *backups* sendo extraviadas, não permitam o acesso aos dados. Hoje em dia, pode-se limitar o acesso ao software de armazenamento, por permissões de acesso, e encriptar os dados dos dispositivos de armazenamento, quer por software quer por hardware.

As vulnerabilidades de software, podem ser exploradas para obter acesso não autorizado aos recursos, e aos dados dos sistemas da informação. Alguns exemplos da exploração das vulnerabilidades de software podem ser [8]:

- **Sistemas Operativos "Avanced IBM Unix" (AIX) –** As palavras-chave podem ser expostas por comandos diagnósticos.

- **Servidor Novell Web** – Um intruso, pode causar um DoS *buffer overflow* enviando, uma grande quantidade de pedidos GET para a porta de administração remota. Isto, faz com que os dados enviados, que não sejam processados ficam em memória como código executável.

- **Sistemas Operativos "Silicon Graphics Unix" (IRIX) –** Uma vulnerabilidade de "*buffer overflow*" permite o acesso à raiz do sistema operativo pelo intruso.

- **Windows 9x** – A vulnerabilidade permite a um intruso localizar o sistema, e as palavras-chave do *screensaver,* fornecendo-lhe os meios necessários para obter acesso não autorizado.

- **Windows NT, XP, 2Kx** – Software de obtenção do modo de privilégio usado por um intruso, pode fazer com que obtenha acesso administrativo ao sistema operativo.

2.2. ATAQUES

Os motivos para ataques externos aos sistemas, são numerosos e variados. Estes vão do *hacker* principiante, atraído pelo desafio, ao profissional, altamente habilitado, e que visam o acesso a uma determinada organização, com uma finalidade específica (tal como o crime organizado, o espionagem industrial, ou pelo simples prazer, de conseguir expor as limitações de segurança).

As ameaças podem ser de origem externa ou interna a uma organização. As ameaças externas, visam a tentativa de acesso a uma organização pela Internet, ou através do acesso de *dialup.* As ameaças internas, originadas dentro de uma organização, são geralmente o resultado dos comportamentos dso empregados, ou outro pessoal que têm acesso autorizado, aos recursos internos da rede. Estudos existentes [3][4][8], indicam que as ameaças internas realizadas por empregados existentes, ou por antigos empregados, são responsáveis pela maioria dos incidentes da segurança da rede, na maioria de organizações.

São três os principais tipos de ataques da rede, tendo cada um o seu próprio objectivo específico:

- **Ataques por reconhecimento** – Este tipo de ataque não está projectado para ganhar acesso a um sistema ou rede, mas somente procurar e encontrar vulnerabilidades que de pode vir a explorar mais tarde.

- **Ataques por obtenção de acesso** – Este ataque está projectado, para explorar uma vulnerabilidade, e ganhar acesso a um sistema ou rede. Após ter ganho acesso, o utilizador pode:

  - Recuperar, alterar, ou destruir dados.

  - Adicionar, remover, ou alterar recursos da rede, incluindo alterações do tipo de acesso a utilizadores.

  - Instalar outras ferramentas que podem ser usadas mais tarde, para conseguir acesso à rede.

- **Ataques por negação de serviço (DoS)** – Um tipo de ataque projectado, para causar unicamente interrupções de serviço, em computadores ou redes, para depois obter acesso a estes, passando despercebido.

2.2.1. ATAQUES POR RECONHECIMENTO

O objectivo deste tipo de ataque, é executar o reconhecimento de um computador ou de uma rede. O objectivo deste reconhecimento, é determinar a composição da estrutura do computador ou da rede, a atingir, e efectuar o levantamento das vulnerabilidades existentes. Um ataque por reconhecimento, pode indicar um potencial ataque mais invasivo, ou seja, a preparação para o ataque principal. Muitos ataques por reconhecimento são feitos por scripts, que permitem que os *hackers* lancem ataques a redes apenas com alguns cliques do rato.

De seguida são apresentados alguns dos ataques mais comuns por reconhecimento:

- **Pedidos *Domain Name Service* (DNS) [3]** – Um pedido de DNS fornece ao utilizador não autorizado, informação sobre como o endereço que é atribuído a um determinado domínio e o que informações este possui, como por exemplo registos A (www), MX (mail), etc. Sites como www.DNSstuff.com, permitem obter a informação necessária relactivamente aos endereços de uma organização.

- **Ping *sweeps*** – Um ping *sweep* diz ao utilizador não autorizado, quantos *hosts* estão activos na rede. É possível bloquear os pacotes ICMP nos dispositivos activos, mas deixa-se de ter a possibilidade de detectar os defeitos da rede. Ferramentas como *Free IP Scanner by Eusing*, permitem efectuar estas análises.

- **Pesquisa vertical de portas** – Este envolve fazer uma pesquisa das portas de serviço de um único *host* e pedir serviços diferentes em cada porto. Este método permite que o utilizador não autorizado, determine que tipo de sistema operativo e serviços estão a correr no computador. Ferramentas como *Portscan ou NMAP* permitem efectuar esta pesquisa, assim como as duas seguintes.

- **Pesquisa horizontal de portas** – Este envolve efectuar uma pesquisa a uma gama de endereços para um porto ou um serviço específico. Uma pesquisa horizontal muito comum é o *scan* ao ftp. Isto é feito através de uma pesquisa a um segmento da rede, e procurar respostas às tentativas de conexão no porto 21.

- **Pesquisa por bloqueios** – Este ataque é uma combinação da pesquisa vertical e horizontal, ou seja, faz uma pesquisa a um segmento da rede e tenta establecer ligações em múltiplas portas em cada *host* desse segmento.

2.2.2. ATAQUES POR OBTENÇÃO DE ACESSO

Como o próprio nome indica, o objectivo deste ataque [4][8] é obter acesso a um computador ou a uma rede. Com este acesso, o utilizador pode executar muitas funções diferentes, funções estas, que podem ser agrupadas em três categorias distintas:

- **Intercepção** – Ao conseguir acesso não autorizado a um recurso, pode-se ter acesso a dados confidenciais, tais como registos de pessoal, folhas de pagamentos, ou projectos de pesquisa e de desenvolvimento. Logo que um utilizador ganhe acesso, pode ler, escrever, copiar, ou mover dados. Se um intruso conseguir acesso, a única forma de proteger os dados é encriptá-los o que pode pelo menos impedir que o intruso os possa ler.

- **Modificação –** Conseguindo acesso, o intruso pode alterar o recurso. Isto inclui não alterar apenas o conteúdo de um ficheiro, mas também alterar configurações de sistema, acessos não autorizados ao sistema, e alteração de privilégios [4]. O acesso não autorizado ao sistema é conseguido através da exploração das vulnerabilidades deste ou do seu software. Denomina-se por acesso não autorizado sempre que um utilizador com um de nível baixo de privilégios, tenta obter um nível mais privilegiado para conseguir informação, ou aumentar o seu nível de privilégios [4]. Isto dá-lhe um controle superior sobre o sistema ou rede que está a atacar.

- **Construção** – Com acesso a um sistema ou rede, o intruso pode criar objectos falsos e introduzi-los no ambiente. Isto pode incluir alterar dados ou introduzir façanhas empacotadas tais como um vírus, *worm*, ou *Trojan Horse* (cavalo de Troia), que faça com que possa continuar a atacar a rede por dentro.

  - Vírus – Os vírus informáticos vão desde os irritantes aos destrutivos. Consistem em código de computador que se une a outro software que corre no computador (ficheiros executáveis do sistema operativo ou e-mails, etc.). Desta forma, sempre que o software corre, o vírus reproduz-se e pode continuar a crescer até que ele bloqueie o computador infectado. Os *Chernobyl* e *Spacefiller* são exemplos de *virus* que provocam estragos elevados nas organizações.

  - *Worm* – O *worm* é um vírus que explora as vulnerabilidades em sistemas ou redes replicando-se por estas. Um *worm* faz uma pesquisa à rede, e procura um computador com vulnerabilidades específicas. Quando encontra um computador

com essa vulnerabilidade, copia-se para esse computador iniciando, de novo, o mesmo processo a partir deste. Os *Mydoom* e *Blaster*, são exemplos de *worms* em a acção é reiniciar os sistemas.

- *Trojan Horse* – Um *Trojan Horse* (Cavalo de Tróia) é um programa que geralmente reivindica o executar de uma função (tal como um jogo) mas faz algo completamente diferente (como corrupção de dados do disco duro). Os efeitos destes programas variam desde a irritação menor do utilizador, à destruição total do sistema de ficheiros do computador. Os Cavalos de Tróia são usados às vezes para explorar sistemas, criando contas de utilizador nos sistemas de modo a que um intruso possa obter acesso ou definir o seu nível de privilégios. Os *Keylogger* e *Backdoor,* são exemplos de cavalos de Tróia.

- *SPAM* – O termo ***Spam***, abreviação em inglês de "*spiced ham*" (presunto condimentado), é uma mensagem electrónica não solicitada enviada em massa. O *spam* é também a designação universal atribuída a correio electrónico (e-mail), de teor quase sempre comercial, não solicitado [1]. Normalmente é enviado em massa para dezenas, centenas e até milhares de endereços de e-mail em simultâneo, fazendo com que os servidores de *e-mail,* e linhas de comunicações fiquem sobrecarregados. Seguidamente apresenta-se um exemplo de um *e-mail de spam*:

```
Hello!
We would like to offer V_I_A_G_R_A soft tabs,

These pills are just like regular Vìagra but they are specially
formulated to be soft and dissolvable under the tongue. The pill is
absorbed at the mouth and enters the bloodstream directly instead
of going through the stomach. This results in a faster more
powerful effect which lasts as long as the normal. Soft Tabs also
have less sidebacks (you can drive or mix alcohol drinks with
them). You can get it at: http://a1medz.com/st/?coupon
No thanks: http://a1medz.com/rr.php
```

2.2.3. DENIAL OF SERVICE (DOS)

Um ataque DoS (negação de serviço) [5] tem em vista negar o acesso de utilizadores a computadores ou redes. Estes ataques geralmente têm como alvo serviços específicos ou tentativa de os desabilitar, sendo feitos inúmeros pedidos concorrentemente. Se um sistema

não está protegido e não pode reagir a um ataque DoS, ele pode ser muito facilmente bloqueado ao correr scripts que geram múltiplos pedidos.

É possível aumentar exponencialmente um ataque DoS com lançamento de vários sistemas contra um único alvo. Esta prática é chamada de um ataque de negação de serviço distribuído (DDoS) [5]. Uma prática comum pelos hackers é usar um Cavalo de Tróia para assumir o controlo de outros sistemas e sincroniza-los para um ataque DDoS. Como exemplos o *Ping flood* ou *Syn Flood*. Entre os vários tipos de ataques DoS, destacam-se os seguintes;

- ***Ping of Death -*** Também conhecido por *long Internet Control Message Protocol (*ICMP*),* envia repetidamente mensagens maiores que os 65.536 bytes permitidos pelo IP. Como exemplo de ferramenta para este ataque é o sPing.

- ***Buffer Overflow -*** Provoca um overflow no buffer do sistema atacado colocando lá mais dados do que é esperado pela aplicação**.** Foi detectada não há muito tempo uma vulnerabilidade no Outlook Express que explorava esta situação [29]. Como exemplos para este ataque são o Code Red, Slapper e Slammer.

- ***DDoS (Distributed DoS) -*** Igual ao DoS mas com um conjunto de vários sistemas semelhantes a efectuarem ataques DoS a um só sistema**.** Este tipo de ataque é mais vulgar com o advento de novas topologias de rede (ADSL, cabo, etc.)

2.2.4. COMO EVITAR ATAQUES DOS OU DDOS?

Infelizmente pouco se pode fazer para evitar este tipo de ataques. A melhor defesa actual é a prevenção e contra medidas. A maior parte dos sistemas operativos actuais implementaram já actualizações que minimizam os efeitos destes ataques [5].

2.2.5. ATAQUE "MAN IN THE MIDDLE" (MITM)

Uma das formas de por em causa a segurança de uma rede é o do ataque do MITM (*Man-In-The-Middle*), que basicamente consiste em colocar na transmissão, entre dois ou mais participantes, sem que estes se apercebam disso, um meio para escuta, alteração de dados, roubo de sessões, etc., de preferência um computador. Poderá afirmar-se que esta é uma boa forma de fazer espionagem numa rede, mas convém referir que só é possível fazê-lo em *Local Area Networks* (LANs), isto é, não é possivel efectuar este ataque, por exemplo,

entre um computador da LAN e um servidor de e-mail da Internet. Mesmo assim, com a abertura que existe hoje em dia com as redes WiFi, que em certos locais tais como universidades ou *cyber-cafes,* têm um grande volume de utilizadores, podem ser um alvo apetecível a este género de ataques [15].

2.2.6. ARP POISONING E ARP SPOOFING

O *Address Resolution Protocol* (ARP) [8] é um protocolo que permite a identificação de máquinas na rede, através da conversão do endereço na Internet (*Internet Protocol* ou IP), no endereço físico do dispositivo (Medium Access Control ou MAC). O ARP mantém uma tabela com os relacionamentos entre IPs e MACs, associando-os. Desta forma, um potencial intruso, ao tentar enviar tramas ARP adulteradas, poderá conseguir colocar-se como intermediário numa comunicação, e consequentemente, adulterar a tabela, associando, por exemplo, um IP a um endereço físico de um dispositivo seu. A partir deste momento o intruso, pode fazer-se passar pela máquina vítima. Este mecanismo é designado por ARP *poisoning*, uma vez que foram adulteradas entradas ARP, gerando ataques do tipo "*Man In The Middle"*. [5]

O processo anterior descreve o ataque quando a comunicação é efectuada na rede local. Este ataque, pode também ser efectuado quando a máquina vítima pretende estabelecer, uma comunicação para fora da rede local. Neste caso é atacada a *default gateway*, ficando a máquina que está a fazer o ataque com o controlo da comunicação, denominando-se este tipo de ataque por ARP *spoofing*, que utiliza consulta e redireccionamento de entradas ARP.

2.2.7. DHCP SPOOFING

O serviço *Dynamic Host Configuration Protocol* (*DHCP)* [5][8] é usado para a atribuição dinâmica de endereços IP às máquinas da rede, assim como informações do *dns* e do *default gateway*. Desta forma, permite que as configurações de rede das máquinas sejam atribuídas automaticamente quando o computador é ligado à rede, sendo essa gestão definida no servidor. O DHCP é um protocolo que usa UDP e não suporta qualquer tipo de autenticação. Apesar de ter alguma complexidade, para efectuar um ataque MITM basta modificar as informações da máquina vítima [5]. Por exemplo, modificar o endereço do *dns* para o endereço IP da máquina que está a efectuar o ataque (*DNS Spoofing*) ou modificar o endereço do *default gateway* para o IP do intruso.

2.2.8. DNS SPOOFING E DNS POISONING

O serviço DNS é utilizado na resolução de nomes, ou seja, é responsável por associar um nome simbólico a um endereço IP. Este serviço responde a pedidos de resolução de nomes, tanto a resolução directa (dado o nome, devolve o endereço IP) como a inversa (dado um IP, devolve o nome). O ataque MITM é baseado na modificação da resposta do *DNS.* Quando uma máquina pergunta ao DNS qual o IP para um determinado nome, a máquina que está a efectuar o ataque pode interceptar o pedido e enviar uma resposta manipulada.

Para efectuar este tipo de ataque MITM é necessário conhecer o formato dos pacotes DNS, pois vai ser necessário criar um novo pacote com o ID do pacote interceptado. Este mecanismo apenas funciona quando se intercepta a resposta porque o cliente que efectuou o pedido tem a informação do ID do pacote que vai receber, pois no caso de o ID não ser o esperado o pacote é descartado.

Ataques do tipo DNS *poisoning* podem incidir sobre a manipulação das listas de actualizações dinâmicas dos DNSs ou no envio de pedidos de actualização [3].

2.2.9. REDIRECCIONAMENTO DE ICMP

O redireccionamento do tráfego ICMP pode ser efectuado quando o intruso pretende direccionar o tráfego para o exterior. Para isso, forja um ICMP *redirect* para todos os membros da rede, forçando a que todos comuniquem, por exemplo, por ele.

Assim o intruso pode receber todas as conexões e possivelmente redireccioná-las para o exterior. É de se notar, que este ataque apenas funciona num sentido, visto o tráfego entre uma *gateway* e uma máquina da rede não poder ser redireccionado.

2.3. DETECÇÃO DE PALAVRAS-PASSE

As palavras-passe ou chaves, utilizadas para autenticar utilizadores, garantindo a sua identidade, são muitas vezes fáceis de deduzir ou descobrir utilizando ferramentas e regras, facilmente acessíveis da internet. Deste modo, deve-se pensar nas chaves previamente (para correr o risco de na altura definir uma chave demasiado simples ou então uma que se esqueça posteriormente). Estas chaves devem ser fáceis de lembrar, mas que ao mesmo tempo não façam referência a pessoas ou objectos pessoais. Devem ter um elevado grau de complexidade (não utilizar palavras, isto é, cojuntos de caracteres que perfazem uma

estrutura que se descubra com ataques do tipo dicionário), procurando utilizar letras, números e caracteres especiais (#, @, _, entre outros). Para melhor compreender este fenómeno e a importância de definir chaves seguras, vamos de seguida enunciar alguns dos tipos de ataques a palavras-passe existentes [4].

2.3.1. DEDUÇÃO

A tentativa de adivinhar as palavras-chave, é dos mecanismos mais usados para autenticar utilizadores, no acesso a um sistema de informação, sendo as palavras-chave uma aproximação comum e eficaz do ataque [9]. O acesso à palavra-chave de uma pessoa pode ser obtido, olhando em volta da sua mesa, procurando notas com a palavra-chave, ou usar a lógica para descobrir a palavra-chave de acesso. Em vez de utilizar força bruta, o *hacker* usa uma abordagem do tipo tentativa e erro, manualmente, com as palavras-chave mais prováveis. Para isso ele dispõe de três dados fundamentais:

1º.- Pelo menos 1 em cada 30 utilizadores usa o login igual a palavra-chave, ou seja de o utilizador de chama Pedro, coloca como palavra-chave "Paulo".

2º.- Grande parte dos administradores usam uma palavra-chave padrão para os sistemas, que vêm, por exemplo, com equipamentos e não são alteradas.

3º.- A maioria das palavras-chave estão relacionadas ao *login*, ou seja se o utilizador se chama Paulo Silva, é problavel que o login seja Paulo e a palavra-chave "Silva"

2.3.2. SNIFFERS DE REDES

Para acelerar a transmissão dos dados que entram nas redes, são agrupados em pacotes. O *hacker* cria ou usa programas chamados *sniffers* que monitorizam a circulação desses pacotes nas redes, e procuram palavras que possam ser *palavras-chave.* Quando encontra, o programa copia o pacote e envia-o para o computador do *hacker*. Os dados, mesmo que cheguem encriptados, é muitsd vezes possível desencripta-los e aceder à informação original [15].

2.3.3. FORÇA BRUTA

A obtenção de palavras-chave por força bruta supõe a utilização de meios para o efeito, como software que usando uma aproximação aleatória, tenta palavras-chave diferentes, na expectativa que lhe conceda a autorização necessária. Em determinados casos, alguma

lógica pode ser aplicada, para que as palavras-chave sejam relacionadas ao nome da pessoa, ao título do trabalho, aos passatempos, matrículas dos automóveis, ou a outros artigos similares [9].

2.3.4. ATAQUE DE DICIONÁRIO

O ataque de dicionário usa como base as palavras mais comuns de um dicionário, como palavra-chave, na tentativa de se obter, o desejado acesso a um computador ou à rede de um utilizador. Uma aproximação, é copiar uma linha com a palavra-chave encriptada e usar directamente essa linha directamente na tentativa de validar o acesso, ou seja, aplicando a mesmo encriptação a um dicionário de palavras-chave geralmente usadas, comparando os resultados. Este tipo de ataque pode ser automatizado [15].

2.4. ENGENHARIA SOCIAL

No que diz respeito aos ataques informáticos internos, os intrusos poderão levar os utilizadores finais a executar ataques muitas vezes sem darem por isso, em vez de perderem tempo a procurar e encontrar vulnerabilidades nos sistemas.

Este tipo de ataque usa habilidades sociais para obter informação tal como palavras-chave ou *Personal Identification Numbers* (PIN´s) (números a ser usados de encontro aos sistemas de informação). Como exemplo, um intruso pode, depois de obter contactos ou outra informação de uma organização, (ex: internet ou lista telefónica) abordar telefonicamente empregados dessa organização, muitas vezes identificando-se como "administrador de sistemas" ou "técnico da informática" pedindo as palavras-chave ou PIN´s para o uso em operações da manutenção. Os seguintes casos são exemplos adicionais de ataques de engenharia social [1]:

- Usar telefone ou *e-mail* para o intruso se fazer passar por uma pessoa (geralmente alguém do suporte técnico ou um superior da pessoa atacada) que precisa de determinadas informações para resolver um suposto problema;
- E-mails a empregados de um intruso, que pede palavras-chave porque o trabalho tem que ser feito sobre o sistema no fim-de-semana.

- E-mails ou chamadas telefónicas de um intruso, que se identifica como um oficial ou chefe, que está conduzir uma investigação para a organização, e requer palavras-chave para a investigação.

- Um técnico de reparação de computadores, que convence o utilizador que o disco duro do seu PC está danificado e é irreparável, instalando um novo disco duro para o utilizador, efectuando posteriormente um exame do disco duro original para extrair a informação e vender a informação a um concorrente ou a um governo estrangeiro

- Aproveitar informações divulgadas na Internet (lista de discussão por *e-mail*, *newsgroup*, IRC) por um administrador ou utilizador que procura ajuda para resolver algum problema na rede;

- Enviar programas maliciosos ou instruções especialmente preparadas para um administrador ou utilizador, com o objectivo de abrir novas vulnerabilidades, na segurança da rede ou obter o máximo de informação possível sobre ela (esta técnica é particularmente eficaz quando a pessoa pede auxílio pela Internet);

- Navegar por *websites* (*hypertext transfer protocol* – http) ou repositórios de ficheiros (*file transfer protocol* – ftp) em busca de informações úteis – muitas vezes é possível encontrar descrições detalhadas da infra-estrutura e/ou documentos que, por descuido ou esquecimento, não foram removidos do servidor.

A melhor defesa contra os ataques de engenharia social é uma política da segurança da informação, educando os utilizadores sobre e contra estes tipos de ataques.

2.5. CÓPIAS DE SEGURANÇA

Um dos aspectos importantes, no processo de segurança da informação da empresa, é a existência de cópias de segurança de dados, que possibilitam o funcionamento desse ambiente em situações de contingência e permitem a recuperação para situações anteriores.

Muitas vezes a organização diz-se preocupada com o assunto e implementa uma série de rotinas que efectuam cópias de segurança. Porém, essas cópias não são estruturadas, não são planeadas, revistas ou mesmo testadas. Na prática, essas informações valem muito

pouco. Quem passou pela situação de saber que dados foram gravados mas que a sua recuperação é quase impossível, compreende este facto [1].

Por outro lado quando se implementam as cópias de segurança não se pensam em aspectos que podem influenciar de modo crítico, a própria segurança. Estes aspectos podem ser o acesso por parte de intrusos que visam o roubo ou destruição, ou a inutilização devido a agentes nocivos como água ou fogo.

Algumas organizações providenciam meios para armazenar os *backups* fora das suas instalações, como cofres de bancos, por exemplo. Essa é uma boa maneira de garantir a disponibilidade dos *backups* em caso de problemas nas proóprias instalações. No entanto, isso pode comprometer a organização caso a confidencialidade e a integridade das cópias de segurança não sejam garantidas.

Para finalizar, a falta de definição de um plano de cópias de segurança, em caso de desastre, pode provocar a total desorganização na medida em não se sabe nada sobre a situação das cópias de segurança. O plano de cópias de segurança é apenas um procedimento de como, quando e onde estão as cópias de segurança. Este, pode ser apenas a definição de algo muito simples como, a definição de frequencia de mudança das “tapes” dos servidores.

2.6. REDES FÍSICAS DE COBRE OU FIBRA ÓPTICA

A segurança tem que ser uma preocupação com toda a estrutura de uma organização, nomeadamente os meios físicos.

Redes locais de cobre como UTP ou STP, ou de fibra óptica, associadas às redes Ethernet também estão sujeitas a vulnerabilidades.

As típicas formas de ataque a estas redes são as seguintes:

- **Escuta (snooping)**
    - Por derivação do meio físico (wire tapping)
    - Por derivação nos conectores
    - Por leitura da interferência electromagnética (EMI) dos cabos
    - Por escuta do espectro radio-eléctrico

- **Bloqueio (interrupção)**

- Corte do meio físico
- Através de interferência electromagnética
- Através de obstáculo

- **Desvio (hijacking)**
  - Desvio da ligação para outro equipamento emissor/receptor
  - Pode ter dois objectivos:
    - Acesso à informação por impersonificação
    - Acesso aos recursos de comunicação

A nível de cablagem UTP é geralmente instalada em tubos, calhas no interior dos edifico, em bastidores em zonas técnicas ou de circulação. Apesar de terem como vantagem a facilidade de reparação em caso de ser danificada, as vulnerabilidades deste tipo de meios são:

- O facto se serem fáceis de interceptar e de desviar
- O facto de serem fáceis de escutar através de medição de campo electromagnético
- O facto de serem fáceis de bloquear, interromper ou danificar

A nível de cablagem Fibra óptica seja ele monomodo ou multimodo, são geralmente usadas em *backbones.* Apesar de terem como vantagem a dificuldade de escuta ou intercepção (sendo necessário a interrupção do circuito para a introdução de um split óptico), no entanto apresentam as seguintes principais vulnerabilidades:

- Fáceis de bloquear, interromper ou danificar, quer por intrusos ao meio, quer por animais, nomeadamente roedores.
- Difíceis de reparar, com custo elevado.

2.7. REDES WIRELESS

As redes *Wireless Fidelity* (Wi-Fi) estão cada vez mais populares em relação as rede cabo ou cobre, devido à descida dos preços dos equipamentos, necessários para instalar este tipo de tecnologia. Além disso, a facilidade de instalação e a sua grande mobilidade tornam estas redes apetecíveis e boas alternativas às redes com fios, quer no mercado residencial como no empresarial.

As redes *wi-fi* permitem cobrir áreas alargadas, tais como campus universitários, bem como criar redes temporárias ou de custos controlados, cujos requisitos possam ser satisfeitos apenas com conectividade sem fios.

Um aspecto fundamental para a grande divulgação deste tipo de redes, foi a adesão da indústria a normas internacionais do Institute of Electrical & Electronics Engineers, Inc. (IEEE – 802.11), que permitiu a interoperabilidade entre equipamentos e a já referida concorrência e baixa de preços. Dentro das normas internacionais IEEE, existem várias versões do referido 802.11, tais como [11][17]:

- 802.11, comdébito que ronda os 2 Mbit/s, na frequência dos 2.4GHz e que utilizava o *Direct Sequence Spred Spectrum*;
- 802.11a, com o débito que ronda os 54 Mbit/s, a operar na frequência de 5GHz e que utilizava o *Orthogonal Frequency Division Multiplexing*;
- 802.11b, que tinha uma velocidade de 11 Mbit/s, a operar na frequência de 2.4GHz e que utilizava o *Direct Sequence Spred Spectrum*, juntamente com *Complementary Code Keying*;
- 802.11g, que conseguiu uma velocidade de 54 Mbit/ numa frequência de 2.4GHz, utilizando o *Orthogonal Frequency Division Multiplexing*;
- 802.11n, ainda em desenvolvimento e que irá possibilitar velocidades entre os 100 e os 640 Mbit/s.

Uma rede sem fios (802.11) é constituída por 1 ou mais BSS (Basic Service Set). Um BSS é constituído por um conjunto de estações que utilizam o mesmo MAC e compartilham a mesma área física de transmissão.

O modo de operação mais habitual das redes sem fios é o modo infra-estruturado, constituído por um conjunto de Access Points (pontos de acesso), que permitem a agregação das ligações aéreas aos terminais dos utilizadores, sejam estes portáteis, PDAs ou outro tipo de equipamentos. O principal objectivo deste modo de operação é possibilitar o acesso a uma rede exterior (Internet por exemplo), a partir de uma rede Wi-Fi, através de um Access Point ou outro dispositivo semelhante.

No caso de a rede não ter configurado quaisquer mecanismos mínimos de segurança, o

acesso à rede fica disponível, para quem estiver dentro do raio de alcance dos Access Points. Por este facto, torna-se vital que a segurança seja considerada como objectivo fundamental, na criação e implementação da rede.

Existe também um outro modo de operação sem fios, designado de Ad-hoc [30], que é utilizado para interligação entre dispositivos, tais como um PDA e um computador, para criação de uma rede entres esses mesmos dispositivos.

Para a criação de uma rede sem fios, basta a utilização do já referido *Access Point*, ligado a uma rede com fios e que irá fornecer o acesso à Internet, e um computador ou portátil que possua uma placa *Wi-Fi* que comunique com o Access Point pela rede sem fios disponibilizada.

Para criação de redes mais complexas e exteriores, terá de haver rigor na escolha dos equipamentos a utilizar, bem como um planeamento cuidado da estrutura da própria rede (visto que, nem todos os equipamentos suportam os mesmos protocolos e configurações de segurança). Pode-se inclusive recorrer à utilização de bridges para que a potência do sinal fornecido seja maior, permitindo que a rede se extenda por distâncias maiores.

No entanto, tal como todas as tecnologias sem fios, esta tecnologia é um alvo preferencial de ataques e vulnerabilidades, especialmente pelo facto de ser um meio de comunicação aberto e transmitido pelo ar, estando ao alcance de qualquer um. Desta forma, assume particular importância identificar as falhas e vulnerabilidades existentes na segurança da rede, para que se possam tomar medidas correctivas mais adequadas.

2.7.1. REDE SEM SEGURANÇA

No caso da rede [17], não ter configurados quaisquer mecanismos mínimos de segurança, o acesso à rede fica disponível, para quem estiver dentro do raio de alcance dos Access Points. Devido a isto, torna-se vital que a segurança, seja considerada como objectivo fundamental na criação e implementação da rede.

No entanto, verifica-se que quanto mais simples for a o grau de protecção das redes, menos seguras serão, dado que são mais susceptíveis a ataques. Além disto, também se verifica que os vendedores de equipamentos para redes *Wi-Fi* preferem favorecer uma postura de "facilidade de utilização" em detrimento de uma postura de "segurança", tendo o utilizador a palavra final no que concerne às configurações de segurança.

Desta forma, uma rede sem qualquer tipo de mecanismos de segurança activos é considerada uma rede aberta, podendo ser acedida por qualquer pessoa, mesmo o mais ingénuo dos utilizadores.

Outro aspecto a considerar prende-se com o facto de ser muito fácil lançar ataques aos vários elementos de uma rede, a partir do seu interior. Tendo em conta isto, qualquer intruso que consiga aceder à rede sem fios, ficará numa posição privilegiada para perpetrar qualquer tipo de ataques, como por exemplo:

- Violação da integridade de informação e serviços de rede;
- Acesso a informação confidencial e posterior chantagenm que poderá ser efectuada, por exploração da referida informação;
- Abuso da ligação à Internet e utilização da mesma às custas do proprietário incauto e para fins ilícitos;
- Destruição de dados, interferência no normal funcionamento da rede, entre outros.

Para evitar situações destas, os utilizadores poderão configurar mecanismos de segurança para este tipo de redes. Alguns destes mecanismos são o *Wired Equivalency Privacy* (WEP) e o *Wi-Fi Protected Access*, (WPA e WPA 2). No entanto, mesmo estes possuem vulnerabilidades, tal como serão apresentados em seguida.

2.7.2. REDE PROTEGIDA POR WEP

O WEP [30][17] foi criado para garantir a privacidade de informação, sendo um sistema baseado num segredo partilhado, só conhecido entre os terminais e os Access Points. No entanto, apresenta deficiências técnicas que permitem a quebra da segurança em muito pouco tempo. É possível demonstrar tal informação recorrendo a aplicações disponibilizadas na Internet e computadores com poder computacional modesto.

Por este motivo, o WEP não deve ser considerado como um mecanismo de segurança eficaz e suficiente, para impedir a penetração na rede de intrusos, cujos conhecimentos técnicos serão suficientes para contornar esta tecnologia.

A autenticação realizada numa rede sem fios com WEP tem dois modos de funcionamento:

- *Open Mode*: Sem qualquer tipo de autenticação;

- *Shared Mode*: Com autenticação, utilizando o WEP;

A autenticação é efectuada através do envio de um "desafio", por parte do Access Point para o receptor, o qual enviará a resposta cifrada com o WEP.

No que concerne ao processo de cifragem e decifragem dos pacotes, o WEP utiliza o algoritmo "*Ron's Code 4"* (RC4), inventado por Ronald Rivest, que tem como principais características:

- A sua simplicidade e rapidez funcional;
- A facilidade de implementação;
- O baixo consumo de recursos;
- O bom desempenho derivado da cifragem ser realizada apenas em cada pacote;
- Os dados que serviram de entrada ao algoritmo são uma chave secreta a ser utilizada (40 ou 104 bits);

Além destas caraterísticas, foram utilizadas também vectores de inicialização (IV) de 24 bits, que permitem variar a chave (inicialmente fixa), para que o resultado das mensagens seja diferente de cada vez que estas são enviadas. Isto permitiu uma maior segurança (embora relativa, como se verá mais à frente) e tornou mais credível a utilização do WEP numa fase inicial. O processo de cifragem e decifragem pode ser analisado na figura seguinte:

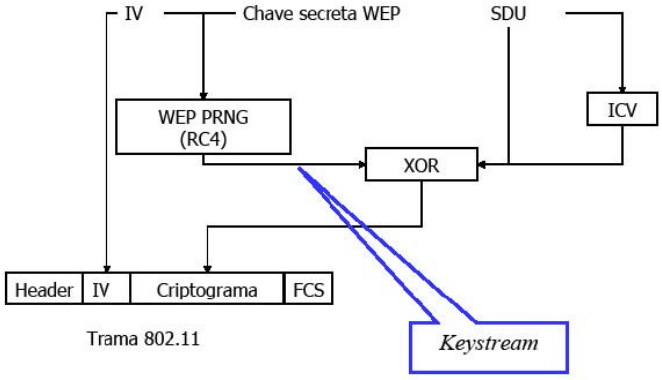


Figura 1 – Decifragem chave WEP

Na figura acima podemos verificar o funcionamento do processo de encriptação do WEP. É possível verificar a existência de uma chave partilhada secreta, que é encriptada usando o algoritmo RC4. A trama irá ser enviada e antes de reverter o processo de encriptação, é validada a chave e comparada com a chave introduzida pelo utilizador da rede.

A integridade dos mesmos pacotes era garantida através do mecanismo CRC-32 (aritmética linear), utilizado na recepção dos pacotes comparando o *Integrity Check Value* (ICV), antes e depois do envío da trama (cf. Figura 2).

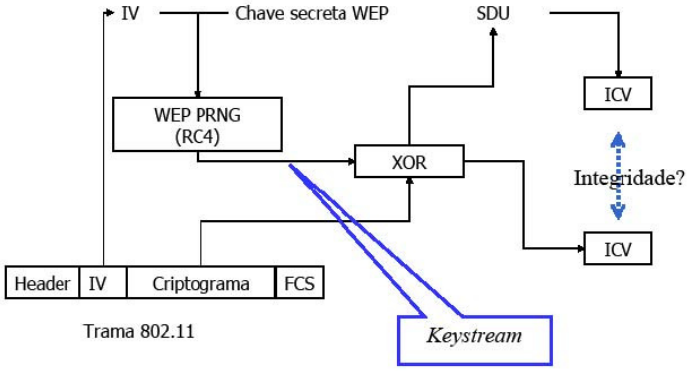


Figura 2 – Verificação da integridade de um pacote WEP

As principais vulnerabilidades do WEP são as seguintes:

- Possibilidade de interceptar o IV, visto que é enviado em texto aberto pelas comunicações, para que a chave seja conhecida em todos os pontos da rede;
- Possibilidade de reutilização da Keystream enviada, visto que a norma 802.11 permite a reutilização do IV;
- Reutilização da Keystream, juntamente com um ataque por *sniffer*s de rede, permite por exemplo, decifrar dados sem recorrer a uma chave WEP;
- O tamanho do IV bastante reduzido leva à necessidade de mudar a chave WEP, sendo que não existem mecanismos para mudança automática de chave WEP;
- É possível alterar a mensagem e o ICV do CRC32, sem que as estações se apercebam dessa diferença;
- O WEP não autentica nem garante a integridade do cabeçalho MAC, pelo que uma máquina pode alterar o seu endereço MAC, fazer-se passar por outra e enviar tramas (ataques DoS);
- Não existe qualquer controlo das sequências de tramas, pelo que os ataques de repetição podem existir;
- É possível emular um Access Point, devido ao facto do Access Point não se autenticar perante a máquina;
- A chave WEP é igual para toda a rede, pelo que o tráfego pode ser escutado/alterado por qualquer máquina na rede;

Como já foi referido, além dos IV serem enviados em *plaintext*, podem ser facilmente interceptados. Neste caso, se o intruso souber o IV que vai nos cabeçalhos (visto que são enviados abertamente), pode descobrir as chaves WEP. O ataque de Fluhrer, Martin e Shamir permite experimentar esta mesma vulnerabilidade.

Além disto, os ataques de força bruta permitem a observação do tráfego da rede, ao ponto em que será possível observar a chave utilizada na rede. Se o intruso "forçar" uma resposta de um equipamento da rede (através de um *ping*), este poderá inclusive retornar a própria chave!

Isto leva a considerar o WEP como um mecanismo de segurança inseguro. Existem também algumas ferramentas que permitem verificar estas vulnerabilidades do WEP, tais como o Aircrack, WEPCrack e o AirSnort, entre outras. Com estas ferramentas, o intruso irá conseguir ter acesso aos dados da rede e entrar nesta, ficando a rede exposta aos riscos já referidos anteriormente.

No entanto, apesar de o WEP ser quebrável, caso o Access Point não garanta outro mecanismo de protecção, este deverá ser utilizado, visto que a sua protecção é mais eficaz do que a ausência de protecção. Para melhorar a segurança, a chave da rede deve ser mudada regularmente, especialmente quando é necessário retirar o acesso à rede a um determinado utilizador.

Visto que o WEP revelou falta de segurança (comprovada pelas razões acima referidas) na protecção das redes Wi-Fi, foi proposto um novo mecanismo de segurança, o 802.11i, que apesar de ser mais eficaz, também apresenta algumas limitações, que irão ser analisadas na secção seguinte.

2.7.3. REDES PROTEGIDAS POR 802.11I

O 802.11i [11][30] surgiu com o intuito de limitar os problemas de segurança evidenciados pelo WEP. Para tal, especifica a *Robust Security Network* (RSN), que define aspectos como:

- Reutilização de protocolos já existentes;
- Cifragem de dados, utilizando:

- *Counter Mode Cipher Block Chaining MAC Protocol* (CCMP) (obrigatório);
- *Temporal Key Integrity Protocol* (TKIP) (opcional);
- *Wireless Robust Authenticated Protocol* (WRAP) (opcional);

- Autenticação/Controlo de acesso, através de:
  - 802.1X;
  - *Pre-shared Key* (PSK);
- Gestão de chaves, com:
  - 802.1X;
  - Chaves temporárias;
  - Chaves de autenticação e chaves cifradas, distintas entre si;
- Modos ad-hoc e infraestruturado;

No entanto, houve aspectos que foram negativos no RSN, tais como o facto de implicar o suporte de CCMP, que se baseia no Advanced Encryption Standard (AES) bem como o facto de o AES ter de ser implementado por hardware, visto não ser possível a sua "emulação" através de software. O AES é um algoritmo de encriptação que funciona com chaves de 128, 192 e 256 bits, com blocos de 128 bits [30].

O AES trabalha com diferentes modos de operação, que alteram a forma como o processo de crifragem é realizado. Estes modos de operação têm como objectivo principal prevenir que a mensagem, quando é cifrada, fique com o mesmo texto cifrado.

Este facto levou a uma actualização do hardware utilizado. Visto que os utilizadores e fabricantes se encontravam reticentes a efectuar esta actualização do hardware, isto implicou a criação de outro mecanismo de segurança, que retirava esta necessidade de hardware. Este mecanismo ficou conhecido como WPA [30].

2.7.4. REDES PROTEGIDAS POR WPA OU WPA2

O WPA [17] [26] surgiu como alternativa ao 802.11i, de forma a proteger eficazmente as

redes *Wi-Fi*. O *Wi-Fi* é baseado no draft 3.0 do 802.11i, lançado em 2002, sendo na prática um RSN "incompleto", pois só possui TKIP sem CCMP e não possui qualquer tipo de suporte ao modo Ad-hoc (cf.2.6).

Para evitar as limitações encontradas no 802.11i, o hardware utilizado manteve-se igual ao WEP, sendo apenas necessário efectuar uma actualização do firmware do equipamento para ter acesso a este novo mecanismo de segurança.

O WPA tem como principais características:

- Utilização do *Temporal Key Integrity Protocol* (TKIP) para cifragem de dados. É um protocolo que usa encriptação de 128 bits que altera a sua chave em cada pacote;
- Utilização do 802.1X para controlo de acesso, autenticação e distribuição de chaves. Este protocolo será explicado na secção 4.2.4 sobre protecção de redes;
- Utilização do modo infra-estruturado como modo de operação da rede;

Houve nos últimos anos uma evolução do WPA que resultou no WPA2, e que permitiu reutilizar alguns dos conceitos práticos implementados inicialmente pelo 802.11i.

O WPA2 é uma certificação disponível pela *Wi-Fi Alliance*, que certifica os equipamentos sem fios, como sendo compatível com o padrão 802.11i. O objetivo da certificação WPA2 é suportar as características de segurança imperativas adicionais do padrão 802.11i, que não são já incluídas para os produtos que suportam WPA. Como WPA, WPA2 funciona da mesma forma, oferecendo as modalidades de operação de empresa e pessoal [30].

Devido à evolução gradual do hardware utilizado, foi possível, juntamente com o WPA2, implementar funcionalidades como o AES, já incluído por hardware nos equipamentos mais recentes.

Para a grande maioria dos equipamentos recentes que não suportavam inicialmente WPA2, mas apenas WPA, a referida implementação do AES já estava realizada, pelo que bastava apenas uma actualização do *firmware* para suportar o mais recente mecanismo de segurança disponibilizado, neste caso o WPA2 [17].

Pode-se considerar assim o WPA2 como uma finalização do 802.11i, visto que implementa todas as suas principais características e conceitos práticos de segurança.

No entanto, o WPA2 é compatível quer com o WPA bem como com o WEP, sendo as certificações válidas para qualquer um deles, não deixando no entanto de ser o WEP o elo mais fraco da "cadeia".

O WPA2 apresenta características como:

- A utilização do CCMP e do TKIP para cifragem de dados;
- A utilização do 802.1X para controlo de acesso, autenticação e distribuição de chaves;
- O suporte para utilização do modo infra-estruturado e do modo Ad-hoc como modos de operação da rede;

Tanto o WPA como o WPA2 tem dois modos de gestão de chaves:

- Pessoal (sem servidor de autenticação)
    - Autenticação com PSK;
    - Distribuição e renovação de chaves através de 802.1X;
- Empresarial (com servidor de autenticação)
    - Autenticação, distribuição e renovação de chaves através de 802.1X;

No entanto, apesar de todas estas características, tanto o WPA como o WPA2 também possuem vulnerabilidades, sendo os principais:

- Susceptibilidade aos ataques de força bruta (teste de palavras-chave em sequência);
- Susceptibilidade aos ataques de dicionário (procura de palavras comuns);

Exemplos destas vulnerabilidades são as redes configuradas com palavras-chave inferiores a 20 caracteres ou equipamentos cujas palavras-chave venham originalmente com palavras-chave de 8 a 10 caracteres. Neste aspecto, quanto maior e mais complexa for a palavra-chave, maior será a dificuldade de ataques a redes com mecanismos de segurança WPA e WPA2. Juntamente com este facto, não existem aplicações publicamente conhecidas que permitam e promovam a realização de ataques de força bruta, havendo apenas a possibilidade de utilizar várias aplicações, (cujo uso é pouco intuitivo) de forma a

reunir grandes quantidades de informação sobre a rede, que possibilite a tentativa de ataque.

Para meios mais complexos, foi necessário implementar um mecanismo de segurança mais seguro que o WPA, o 802.1X. Este mecanismo de segurança será analisado mais em detalhes no capítulo seguinte.

2.8. RESUMO

Neste capítulo foram apresentadas algumas vulnerabilidades e ataques mais comuns. Foram enumerados diversos tipos de vulnerabilidades como as que exploram sistemas operativos, e falhas causadas por vírus e *spyware*. No que diz respeito a ataques, foram enunciados protocolos e serviços de rede susceptíveis a exploração, como é o caso do ARP, DHCP, DNS e ICMP. Além destas ameaças, ainda foram descritos os problemas da engenharia social e da quebra de redes *wi-fi*. Tendo em vista minimizar o efeito das vulnerabilidades face aos tipos de ataques considerados, foram apresentados alguns mecanismos de segurança para redes *ethernet* e wireless, como soluções de anti-vírus, *firewall*, e encriptação. Como foi dito, existem inúmeras vulnerabilidades e falhas nos sistemas informáticos que podem ser "aproveitadas" por pessoas ou entidades com os mais variados objectivos (aquisição de informação confidencial, destruição de documentos, ataques aos sistemas, entre outros). Normalmente, os utilizadores mal-intencionados fazem uso de aplicações facilmente localizadas na internet, com os mais diversos tipos e desígnios. Por vezes o perigo encontra-se dentro da própria empresa, e é comum haver ataques internos e espionagem por parte dos próprios colaboradores. Algumas das medidas para minimizar as probabilidades de ocorrência de falhas serão vistas nos capítulos seguintes.

3. POLÍTICAS E PROCEDIMENTOS DE SEGURANÇA DE SISTEMAS

A segurança é um dos conceitos mais importantes, senão o mais importante, na implementação de qualquer rede [1]. A protecção e confidencialidade das informações institucionais, são aspectos dependentes das medidas de segurança física e lógica da entidade gestora. Não descartando a segurança física, há perigos de cariz natural, como inundações, terramotos, incêndios, ou perigos sociais como espionagem e roubo. Aqui serão abordados aspectos relacionados com segurança lógica da informação, e algumas medidas e regras, para minimizar o impacto das vulnerabilidades de uma rede.

3.1. DEFINIÇÃO DE POLÍTICAS DE SEGURANÇA

A política de segurança da rede é o núcleo do processo de segurança de um sistema ou rede [4][14]. Cada empresa, deve ter uma política de segurança da rede, documentada e que no mínimo, deve cumprir os seguintes objectivos:

- Analisar as ameaças baseando-se no tipo de negócio exercido e no tipo de exposição da rede.
- Determinar as exigências de segurança da organização.
- Documentar a infoestrutura da rede e identificar pontos de potencial ruptura ou falha de segurança.
- Identificar os recursos específicos que requerem uma protecção e desenvolver um plano de execução.
- Deverá contemplar a segurança física dos equipamentos de forma que os intrusos não obtenham acesso local aos equipamentos.

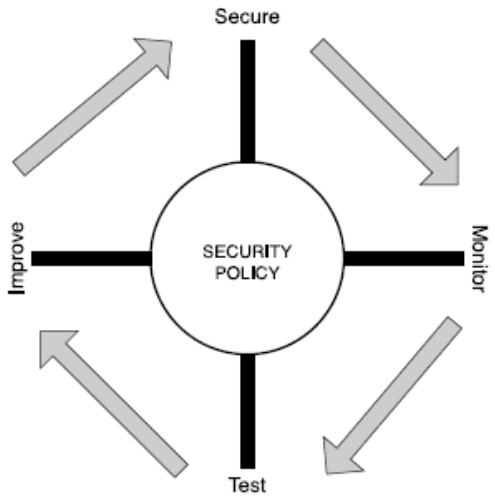


Figura 3 – Cíclo das Políticas de Segurança

Sendo elaborada uma política de segurança, esta deve ser implementada em 4 processos que se desenvolvem ciclicamente, como é apresentado na figura acima: "Implementar", "Monitorizar", "Testar" e "Melhorar".

1º Processo – Implementar

A finalidade deste processo é impedir o acesso não autorizado à rede e proteger recursos da rede. Este processo pode ser considerado, a implemantação do projecto de segurança da rede. Isto inclui o reforço dos sistemas da rede, instalando dispositivos de segurança tais como *firewalls*, sensores da detecção de intrusão, e servidores "A*uthentication, Authorization, and Accounting"* (AAA). As *Firewalls* de perímetro impedem que o tráfego

não desejado de entrar na rede. As *firewalls* internas verificam que somente o tráfego autorizado que se move entre segmentos da rede.

Este processo prevê restringir o acesso aos recursos, somente aos utilizadores autorizados, e implementar uma convenção de palavras-chave fortes (de preferência alfanuméricas). De igual modo, executar encriptação de dados para proteger a informação que passa ou esteja na rede, principalmente através de ligações não seguras (como a Internet) [4].

2º Processo – Monitorizar

Neste processo realiza-se a monitorização da rede, sendo instalandos ferramentas e/ou sensores de detecção de intrusão, nos pontos chaves da rede (perímetro) para monitorizar o tráfego interno e externo. É importante monitorizar o tráfego interno e externo, porque só assim se pode verificar se existem violações da política de segurança projectada, dos ataques internos e externos e determinar se algum deles conseguiu "minar" o sistema.

Todos os dispositivos de perímetro, como firewall, routers e sensores de detecção de intrusão devem fornecer registos de dados (ficheiros de eventos, log). Só desta forma e com uma futura filtragem se consegue detectar determinados incidentes.

3º Processo – Testar

Este processo envolve testar a eficácia do projecto da segurança. Verificar que os equipamentos de segurança são instalados, configurados e colocados a funcionar correctamente. A utilização de ferramentas utilizadas pelos chamados *hackers* são excelentes métodos para verificar as potencialidades do projecto, e determinar os pontos fortes e eventuais vulnerabilidades deste actualmente.

4º Processo – Melhorar

Este processo envolve os dados dos sensores da detecção de intrusão dos dados de teste com vista o melhorar do projecto. Uma política eficaz da segurança é sempre um trabalho em desenvolvimento e continuar a melhorar com cada ciclo do processo. Isto não significa necessariamente a implementação de novos equipamentos e tecnologia com cada ciclo. Muitas vezes basta mudar determinados procedimentos da empresa ou documentar potenciais novas ameaças e/ou vulnerabilidades. É muito importante recordar que a segurança é um processo contínuo, uma vez que, o que hoje é seguro, amanhã poderá não o ser.

3.2. FACTORES QUE INFLUENCIAM A POLÍTICA DE SEGURANÇA

Antes de se definir as políticas e/ou procedimentos de segurança, deve-se considerar vários factores que influenciam positivamente ou negativamente as políticas de segurança, e que muitas veses levam ao sucesso ou insucesso das mesmas.

Alguns factores importantes para o sucesso de uma política de segurança são [1]:

- Apoio por parte da administração superior;
- A política deve ser ampla, cobrindo todos os aspectos que envolvem a segurança dos recursos e da informação sob responsabilidade da organização;
- A política deve ser periodicamente actualizada de forma a reflectir as mudanças na organização;
- Deve haver um indivíduo ou grupo responsável por verificar se a política está a ser respeitada;
- Todos os utilizadores da organização devem tomar conhecimento da política e manifestar a sua concordância em submeter-se a ela antes de obter acesso aos recursos da organização;
- A política deve estar disponível em locais de fácil acesso aos utilizadores, tal como a *intranet* da organização.

Dos itens acima descritos, o apoio por parte da administração superior é essencial, uma vez que, é importante que os seus membros dêm o exemplo, no que diz respeito à observância da política de segurança.

Por outro lado há um conjunto de factores influenciam negativamente, na aceitação de uma política de segurança e podem levá-la ao fracasso, por exemplo [1]:

- A política não deve ser demasiadamente detalhada ou restritiva;
- O excesso de detalhes na política pode causar confusão ou dificuldades na sua implementação;
- Não devem ser abertas excepções para indivíduos ou grupos;
- A política não deve estar dependente de *software* e/ou *hardware* específico.

3.3. DEFINIÇÃO DAS POLÍTICAS E PROCEDIMENTOS DE SEGURANÇA

Uma política de segurança deve cobrir os seguintes aspectos [1]:

- Aspectos processuais:
    - Normas e regulamentos aos quais a política está subordinada;
    - Quem tem autoridade para implementar e fiscalizar o cumprimento da política;
    - Meios de distribuição da política;
    - Como e com que frequência a política é actualizada.
- Política de palavras-passe:
    - Requisitos para formação;
    - Período de validade;
    - Normas para protecção;
    - Renovação de palavras-chave;
    - Palavras-passe por omissão.
- Direitos e responsabilidades dos utilizadores, tais como:
    - Utilização de contas de acesso;
    - Utilização de *software* e informações, incluindo questões de instalação, licenciamento e *copyright*;
    - Protecção e uso de informações (sensíveis ou não), como palavras-passe, dados de configuração de sistemas e dados confidenciais da organização;
    - Uso aceitável de recursos como *e-mail*, *news* e páginas Web;
    - Direito à privacidade, e condições nas quais esse direito pode ser violado pelo administrador (a organização);
    - Uso de anti-vírus.

- Direitos e responsabilidades do administrador, como:
    - Cópias de segurança;
    - Directrizes para configuração e instalação de sistemas e equipamentos de rede, assim como definição da documentação;
    - Autoridade para conceder e revogar autorizações de acesso, conectar e desconectar sistemas e equipamentos de rede, alocar e registar endereços e nomes de sistemas e equipamentos;
    - Monitorização de sistemas e equipamentos de rede;
    - Normas de segurança física.
- Acções previstas em caso de violação da política:
    - Directrizes para tratamento e resposta de incidentes de segurança;
    - Definição de penalizações.

3.3.1. PALAVRAS-PASSE DE ADMINISTRADOR

Durante a instalação de um sistema, em determinado momento é solicitado que se defina uma palavra passe de administrador (*root* ou *Administrator*). Na maioria dos casos, é o próprio programa de instalação que solicita a escolha da palavra-chave. Noutros casos, a palavra-chave de administrador deve ser definida após o primeiro *boot* do sistema.

Deve-se estabelecer esta palavra-chave tão cedo quanto possível durante a instalação do sistema, e, de preferência, que esteja já definida pela política de segurança.

Uma chave adequada é aquela que fácil de ser lembrada e difícil de ser adivinhada, e deve respeitar, no mínimo, os seguintes critérios [1][9]:

- Ter um comprimento mínimo de 8 caracteres;
- Ser formada por letras, números e caracteres especiais;
- Não ser derivada de seus dados pessoais, tais como nomes de membros da família (incluindo animais de estimação), números de telefone, matriculas de carros, números de documentos e datas;

- Não dever ser facilmente dedutível por quem conheça suas preferências pessoais.
- Não estar presente em dicionários (de português ou de outros idiomas).

3.3.2. DOCUMENTAÇÃO DA INSTALAÇÃO E CONFIGURAÇÃO

Uma medida importante para permitir uma rápida avaliação da situação de um sistema, é a documentação da instalação e configuração. O objectivo é ter uma espécie de *bloco de notas* (ou "diário de bordo"), que detalhe os componentes instalados no sistema e todas as modificações na sua configuração global.

Este *bloco de notas* pode ser particularmente útil na identificação das versões de determinados pacotes de software instalados no sistema, ou para reconstituir uma dada instalação. Muitas vezes um administrador precisa de consultar diversas fontes e realizar várias tentativas antes de instalar e/ou configurar correctamente um determinado pacote de *software*. A existência de um documento que relate quais os passos exactos que tiveram que ser seguidos para que a instalação/configuração fosse bem sucedida, permite que esse mesmo pacote possa ser instalado correcta e rapidamente noutro sistema ou ocasião. A importância deste documento cresce à medida que a responsabilidade pela administração dos sistemas seja partilhada por diversas pessoas.

É essencial que alterações na configuração do sistema e seus componentes estejam documentadas neste *bloco de notas*. A entrada referente a estas alterações deve conter, no mínimo, os seguintes itens:

- Data da modificação;
- Responsável pela modificação;
- Justificação para a modificação;
- Descrição da modificação.

Este *bloco de notas* é um documento sensível, pois contém informações que podem ser usadas para comprometer facilmente a segurança deste sistema. Sendo assim, ele deve ser armazenado e manipulado com cuidado, de acordo com a política para documentos sensíveis da sua organização.

3.3.3. POLÍTICAS DE BACKUP E RESTAURO DE SISTEMAS

A importância dos *backups* na administração de sistemas nunca pode ser menosprezada. Sem eles, muitos dados podem ser irrecuperáveis, caso sejam perdidos devido a uma falha acidental ou a uma intrusão.

Os *backups* devem fazer parte da rotina de operação e seguir uma política determinada. O recomendavel, é, configurar os *backups* para que possam ser realizados automaticamente, e, de modo a reduzir o seu impacto sobre o trabalho dos utilizadores.

Importante também é saber ao que é que se deve efectuar backups, de modo a que não se tenha backups do que não interessa, onde são guardados, para que se saiba onde estão localizados/armazenados sempre que necessários.

A lista de itens cujo *backup* deve ser feito com frequência inclui [1]:

- Dados;
- Arquivos de configuração e sistema;
- *logs*.

Alguns cuidados devem ser tomados em relação ao local onde são guardados os *backups*[1]:

- O acesso ao local deve ser restrito, para evitar que pessoas não autorizadas roubem ou destruam *backups*;
- O local deve ser protegido contra agentes nocivos naturais (poeira, calor, humidade);
- Se possível, é aconselhável que o local seja também à prova de fogo.

Os *backups* devem ser verificados logo após serem feitos e, posteriormente, em intervalos regulares. Isto possibilita a descoberta de defeitos em dispositivos e meios de armazenamento e pode evitar que dados sejam perdidos devido a problemas com *backups* que não podem ser restaurados.

As organizações que providenciam meios para armazenar *backups* fora das suas instalações, devem procurar garantir a confidencialidade e integridade destes. Uma possível solução é encriptar o *backup* e gerar um *checksum* (MD5 ou SHA-1, por exemplo)

deste antes que seja entregue a pessoas de fora da organização. Uma verificação do *checksum* antes do restauro pode servir como prova de que o *backup* não foi alterado desde que foi feito.

Quando for necessário restaurar um sistema, isto deve ser feito com a máquina isolada ou de teste se possível. Caso o sistema em questão tenha sido comprometido, deve-se verificar a configuração após o restauro para certificar de que não fica nenhuma porta de entrada previamente instalada em caso de intrusão.

3.3.4. PRECAUÇÕES CONTRA ENGENHARIA SOCIAL

No contexto da segurança informática, Engenharia social é a técnica (ou arte) de aproveitar-se da boa fé de pessoas, para obter informações. Estas informações visam a possibilidade ou facilidade de acesso a recursos de uma organização por parte de utilizadores não autorizados. Seguidamente são indicadas algumas informações procuradas destacando-se as seguintes [1][9]:

- Palavras-passe de acesso;
- Topologia da rede;
- Endereços IP em uso;
- Nomes de *hosts* em uso;
- Listas de utilizadores;
- Tipos e versões de sistemas usados;
- Tipos e versões de serviços de rede usados;
- Dados sigilosos sobre produtos e processos da organização.

Existem diversas formas de se efectuar um ataque de engenharia social, mas todas elas têm em comum a característica de usarem basicamente psicologia e perspicácia para atingir os seus propósitos.

A principal forma de prevenir estes ataques é orientar os utilizadores e administradores de redes e sistemas sobre como agir nestas situações. A política de segurança da organização

desempenha um papel importante neste sentido, pois é nela que são definidas as normas para protecção da informação na organização.

Procurar reduzir a exposição da sua rede em fóruns públicos, por exemplo, usar endereços IP, nomes de *hosts* e utilizadores hipotéticos, e tentar não revelar mais sobre a topologia da rede do que o estritamente necessário para resolver um dado problema. Deve-se ter cuidado com orientações passadas por pessoas desconhecidas, e evitar executar programas

3.4. SINCRONIZAÇÃO DE RELÓGIOS E TIME ZONE

Os relógios de todos os sistemas (incluindo as estações de trabalho) deverão estar sincronizados, ou seja, deverão ter exactamente o mesmo horário. Para que isso aconteça, é necessário usar um protocolo de sincronização de relógios, como o NTP (*Network Time Protocol*) [5]. Este protocolo é o mais recomendado, pois existem implementações dele para os mais variados sistemas, como pode ser visto em http://www.ntp.org.

Para obter maior precisão no ajuste do relógio e para minimizar o tráfego necessário na rede, sugere-se que a sincronização via NTP seja implementada tendo em conta os seguintes pontos [5]:

1. Procurar implementar um servidor NTP local. Esse servidor irá realizar a sincronização com um servidor externo. As restantes máquinas da rede, por sua vez, terão os seus relógios sincronizados com o relógio do servidor local.

2. Muitos *ISP´s* disponibilizam um servidor NTP.

3. No caso de sistemas Unix, deve-se ajustar o relógio de *hardware* destes sistemas para a hora padrão de Greenwich (GMT) e configurar adequadamente o seu fuso horário (*timezone*) para que a hora local seja exibida correctamente

4. No caso de sistemas Microsoft, o *time zone* é definido nas opções regionais e todos os servidores e postos de utilizadores assumem automaticamente como *time server* o controlador de domínio (DC) da rede.

3.5. MONITORIZAÇÃO DE LOGS E ALERTAS

Os *logs* possibilitam o acompanhamento do que acontece com a rede e com os sistemas. Para isto, é importante que eles sejam monitorizados com frequência para permitir que eventuais problemas sejam rapidamente identificados [1][15].

Existem algumas práticas úteis no que diz respeito à monitorização de *logs*:

- Incorporar o hábito de inspeccionar os *logs* com determinada frequência;
- Efectuar a inspecção pelo menos uma vez por dia, mas tendo em mente que sistemas de grande escala ou que tratam muita informação, podem solicitar uma análise de *logs* mais frequente;
- Procurar investigar as causas de qualquer registo que pareça incorrecto ou anómalo, por mais insignificante que ele aparente ser;
- Procurar identificar o padrão de comportamento normal dos sistemas, para poder encontrar eventuais anomalias com maior rapidez;
- Procurar configurar alertas, por *e-mail*, SMS ou outros, de forma a ficar informado quando determinados eventos ocorrerem.

Na análise de *logs*, deve-se verificar o *timezone* usado para registar o hora e data dos eventos. Existem determinadas aplicações que registam eventos com a hora de Greenwich (GMT), e não com a hora local. O desconhecimento do *timezone* em que estão os *logs* pode facilmente invalidar uma análise e levar a conclusões erradas.

Uma outra opção é utilizar ferramentas que permitam monitorar *logs* em tempo real, como por exemplo o *nagios* [24] (http://www.nagios.org/). O *nagios* requer que seja especificado um conjunto de padrões a serem monitorizados (como o hardware) e as acções a serem tomadas quando um destes padrões é registado nos *logs*. As acções podem ser de diversos tipos, como por exemplo, exibir a informação registada, notificar um determinado utilizador por *e-mail* ou invocar um programa do sistema. A capacidade de execução de comandos arbitrários do *nagios* torna-o muito versátil e funcional, pois permite, por exemplo, que sejam tomadas medidas como filtragem de um endereço IP que gere determinado *log* e envio de uma mensagem de alerta *sms*.

Existem também várias ferramentas que têm por objectivo processar diversos formatos conhecidos de *logs* e que podem ser bastante úteis para o administrador. Uma grande lista dessas ferramentas, bem como documentação sobre monitorização e análise de *logs* está disponível em http://www.loganalysis.org/.

3.6. DNS

O DNS (*Domain Name System*) é um serviço fundamental para o funcionamento da Internet. Esta importância, associada à natureza das informações que possui, o tornam um dos alvos preferenciais dos *hackers*. Deste modo, uma configuração adequada dos servidores DNS é crucial para aumentar a segurança e contribui para o bom funcionamento da rede [3].

Os servidores DNS expostos à Internet estão sujeitos a uma série de riscos, de entre os quais destacam-se [3][9]:

- Extração de informação sensível sobre a rede da organização através de transferências de zonas DNS. Esta informação pode ajudar um *hacker* a identificar os pontos fracos da rede e a escolher potenciais alvos.
- Ataques de *cache poisoning* que levam um servidor a armazenarem informação falsa. Estas informações podem ser usadas para comprometer a segurança de clientes que acedam a esse servidor.
- Comprometer o servidor através de vulnerabilidades no *software* de DNS, o que pode facilitar outras quebras de segurança na restante rede da organização.

Um factor importante consiste no facto do DNS fornecer um registo que possibilita a obtenção da versão do serviço de DNS, o que pode ser usado para determinar a vulnerabilidade do serviço a um dado ataque. Por exemplo, o BIND fornece esta informação através de consultas do tipo "version.bind".

Desta forma, é aconselhável que se verifique se este tipo de registo pode ser fornecido pelo serviço de DNS. Se assim for, deve ser configurado tendo em consideração uma ou mais das seguintes medidas [3][9]:

- Bloquear toda e qualquer consulta desta natureza, originada na rede interna ou externa;

- Permitir que este tipo de consulta seja realizada apenas partindo da rede interna ou de determinados IPs, como da máquina do administrador ou do próprio servidor de DNS (*localhost*); No caso de servidores Microsoft, autorizar apenas ligações seguras.
- Efectuar o encaminhamento de pedidos públicos apenas para o ISP
- Gere registos de eventos (*logs*) para todas as consultas desta natureza.

Através de ferramentas como o *nmap, o ipscanner ou o nslookup* consegue-se obter todo o tipo de informação relativa ao DNS.

3.7. DNS REVERSO

O uso mais comum do DNS consiste na tradução de nomes em endereços IP. Por outro lado, permite também descobrir o nome associado a um determinado endereço IP. Este processo denomina-se DNS reverso, e possibilita a identificação do domínio de origem de um endereço IP [3][9].

Um DNS reverso mal configurado ou inexistente pode revelar-se problemático. Existem diversos *sites* que negam o acesso a utilizadores com endereços sem DNS reverso ou com o DNS reverso incorrecto, por exemplo no envio e recepção de *e-mail.*

As ferramentas como o *nmap, o ipscanner ou o nslookup*, também conseguem obter informações por DNS reverso.

3.8. WHOIS

Cada domínio ou gama de endereços IP registados possui uma lista de informações de contacto sobre os responsáveis pelos mesmos domínios e gamas. Existem normalmente três tipos de contactos [3][9]:

- Contacto técnico: responsável técnico pela administração e operação do domínio ou gama;
- Contacto administrativo: quem tem autoridade sobre o domínio ou gama;
- Contacto de cobrança: quem recebe correspondências de cobrança das despesas de registo e manutenção do domínio ou gama.

Os endereços de *e-mail* destes contactos devem estar sempre actualizados. No caso do contacto técnico, as mensagens enviadas devem ser recebidas por um administrador de redes responsável pela gama ou domínio, e não por pessoal administrativo ou jurídico da organização. Este contacto é usado com muita frequência para notificação de incidentes de segurança e outros problemas com a infra-estrutura de rede envolvendo o domínio ou gama.

Estas informações de contacto são mantidas numa base de dados chamada WHOIS. Esta base de dados é normalmente gerida por entidades que registaram os domínios e pelo ISP.

3.9. ELIMINAÇÃO DE PROTOCOLOS SEM CRIPTOGRAFIA

Uma medida de segurança de elevada importância na gestão de redes é a substituição de protocolos sem autenticação através de palavras-passe, ou caso exista, não tenha qualquer tipo de encriptação. Desta forma, devem ser evitados alguns protocolos, como é o caso dos seguintes [8]:

- Telnet;
- FTP;
- POP3;
- IMAP;
- rlogin;
- rsh;
- RDP

A maioria dos protocolos citados pode ser substituída pelo SSH. Esta substituição, além de fazer com que o tráfego entre cliente e servidor passe a ser encriptado, traz ainda outras vantagens, como protecção da sessão contra ataques tipo *man-in-the-middle* e roubo de sessão TCP.

Em relação ao POP3, existem diversas possibilidades de substituição [1]:

1. Usar POP3 através de um túnel SSH ou SSL. A primeira opção é interessante quando o servidor POP3 e o servidor SSH residem na mesma máquina. Para a segunda, podem ser usadas ferramentas como o "stunnel" (http://stunnel.mirt.net).

2. Alguns clientes de *e-mail* já suportam SSL directamente, não sendo necessário o uso de túneis.

3. Usar uma solução de Webmail sobre HTTPS (HTTP+SSL). Muitos acessos a webmail enviam o utilizador e palavra-passe em texto aberto, podendo ser detectadas. A implementação de https em vez de http resolve este problema.

4. Usar uma solução de RPC sobre HTTPS.

5. Usar uma solução de VPN e só depois o acesso POP3 ou RDP. Uma solução de VPN como Microsoft ISA ou OPENVPN LINUX, resolve o problema de qualquer tipo de acesso aos protocolos não seguros, uma vez que esse tipo tráfego vai encriptado no túnel VPN.

3.10. *FIREWALLS*

Uma *firewall* bem configurada é um instrumento importante para implementar a política de segurança de uma rede. Este pode reduzir externamente a informação disponível sobre a rede, ou em alguns casos, bloquear ataques a vulnerabilidades ainda não divulgadas publicamente (e para as quais ainda não existem actualizações disponíveis) na própria *firewall* ou em sistemas internos.

Por outro lado, as *firewalls* não são infalíveis. A simples instalação de uma firewall não garante que a rede esteja segura contra intrusos. Uma *firewall* não pode ser a sua única linha de defesa, sendo apenas mais um dos diversos mecanismos e procedimentos que aumentam a segurança de uma rede.

Outra limitação da *firewall* é que protege apenas contra ataques externos, não havendo controlo interno da rede [1][4][7][9].

3.10.1. A ESCOLHA DE UM FIREWALL

Existem diversas soluções de *firewall* disponíveis no mercado. A escolha de uma delas está associada a factores como custo, recursos desejados e flexibilidade. Um ponto essencial esta relacionado com a usabilidade da plataforma. A maioria das *firewalls* está disponível para um conjunto reduzido de plataformas, e a sua escolha deve restringir-se a um dos produtos com os quais os administradores da rede tenham experiência. Por exemplo, se se utilizar basicamente servidores Unix, é aconselhável que se escolha uma *firewall* desta

variante como *Shorewall* [18] ou *iptables* directamente. No caso da Microsoft, o ISA Server e no caso Cisco, o ASA ou definir VLAN´s numa infraestrutura em que o switch de core é *layer 3* com *ACL (Access Control List)* [5].

Estar familiarizado com o sistema onde a *firewall* é implementada permitirá configurá-la de forma segura. A existência de uma *firewall* instalada em sistemas inseguros pode ser até mais perigosa do que a ausência de *firewall* na rede.

As aplicações de *firewall* tendem a seguir a filosofia da plataforma onde estão inseridos. Por exemplo, a maioria das *firewalls* para Windows é configurada através de menus e janelas, ao passo que muitas *firewalls* para Unix são configuradas em linha de comandos.

Outro factor importante consiste na escolha do tipo de *firewall* que será implementada. Em algumas aplicações, destacam-se os filtros de pacotes, utilizados por muitos devido ao baixo custo associado e por estarem normalmente integrados com dispositivos como *routers* ou alguns tipos de *switches*, ou por serem facilmente integráveis ou fazerem parte do *kernel* de diversos sistemas.

3.10.2. LOCALIZAÇÃO DAS FIREWALLS

A localização das *firewalls* na rede depende normalmente da política de segurança. Entretanto, existem algumas regras que se aplicam à grande maioria dos casos [1][4][7][9]:

- Todo o tráfego deve passar pela *firewall*. Um *firewall* só pode actuar sobre o tráfego que controla. A eficácia de uma *firewall* pode ser severamente comprometida se existirem rotas alternativas para dentro da rede (modems, acessos 3G, por exemplo). Caso não seja possível eliminar todas esses caminhos, eles devem ser documentados e fortemente vigiados através de outros mecanismos de segurança.

- **Criar filtros de pacotes no perímetro da rede**. Os filtros podem estar localizados entre o *router* e o interior da rede ou no próprio *router*, se ele tiver essa capacidade. O filtro de pacotes (IDS / IPS) é importante para tarefas como bloqueio global de alguns tipos de tráfego e bloqueio rápido de serviços durante a implantação de actualizações após a descoberta de uma nova vulnerabilidade.

- **Colocar os servidores externos em áreas DMZ**. É comum colocar os servidores acessíveis externamente (Web, FTP, E-mail, etc.) num segmento de rede separado e com acesso altamente restrito, conhecido como DMZ (*DeMilitarized Zone*, ou zona desmilitarizada). A principal importância disto é proteger a rede interna contra ataques provenientes dos servidores externos, uma precaução contra a eventualidade de que um destes servidores seja comprometido. Por exemplo, supondo que um *hacker* invade o servidor Web e instale um *sniffer* na rede, e este servidor Web estiver na rede interna, a probabilidade dele conseguir capturar dados importantes (tais como palavras-passe ou informações confidenciais) é muito maior do que se estiver numa rede isolada.

- **Considerar o uso de *firewalls* internas**. Em determinados casos, é possível identificar na rede interna grupos de sistemas que desempenham determinadas tarefas comuns, tais como desenvolvimento de *software*, *webdesign* e administração financeira. Nestes casos, recomenda-se o uso de *firewalls* internas para isolar estas sub-redes umas das outras, com o propósito de aumentar a protecção dos sistemas internos e conter a propagação de ataques bem-sucedidos.

3.10.3. CRITÉRIOS DE FILTRAGEM DAS FIREWALLS

Existem basicamente dois critérios de filtragem que podem ser aplicados a *firewalls*. O primeiro é o de *default deny*, ou seja, todo o tráfego que não for explicitamente permitido é bloqueado. O segundo, *default allow*, é o contrário, ou seja, todo o tráfego que não for explicitamente proibido é permitido.

A configuração dos *firewalls* deve seguir a política de segurança da rede. Se a política permitir, é recomendável adoptar uma postura de *default deny*. Esta abordagem é, geralmente, mais segura, pois requer uma intervenção explícita do administrador para permitir o tráfego desejado, o que minimiza o impacto de eventuais erros de configuração na segurança da rede. Além disso, ela tende a simplificar a configuração dos *firewalls*.

No perímetro da rede, pelo menos as seguintes categorias de tráfego devem ser filtradas:

- Tráfego de entrada (*ingress filtering*): pacotes com endereço de origem pertencente a uma rede reservada ou a uma das gamas de endereços da sua rede interna;

- Tráfego de saída (*egress filtering*): pacotes com endereço de origem pertencente a uma rede reservada ou que não façam parte de uma das gamas de endereços da rede interna.

Um aspecto que deve ser considerado com cuidado é a filtragem do protocolo ICMP. O bloqueio indiscriminado de ICMP pode prejudicar o funcionamento da rede. Por outro lado, o ICMP pode ser usado para revelar a um possível intruso informações sobre a rede e os seus serviços. Muitas *firewalls* do tipo *stateful* permitem a passagem de mensagens ICMP de erro associadas a conexões estabelecidas, o que minimiza o impacto da filtragem.

O tráfego para a DMZ deve ser altamente controlado. As únicas ligações permitidas para os sistemas dentro da DMZ devem ser as relativas aos serviços públicos (acessíveis externamente). Ligações com origem na DMZ para a rede interna devem ser, na sua maioria, tratadas como conexões oriundas da rede externa, aplicando-se a política de filtragem correspondente.

A DMZ e a rede interna não podem estar no mesmo segmento de rede (ligadas ao mesmo *hub* ou *switch*, por exemplo). É imprescindível que estas redes estejam em segmentos de rede separados.

3.10.4. EXEMPLOS DE IMPLEMENTAÇÕES DE FIREWALLS

Existem diversas arquitecturas que podem ser empregadas para a implementação de *firewalls* numa rede [1][4][7][9]. A escolha obedece a uma série de factores, incluindo a estrutura lógica da rede a ser protegida, custo, funcionalidades pretendidas e requisitos tecnológicos.

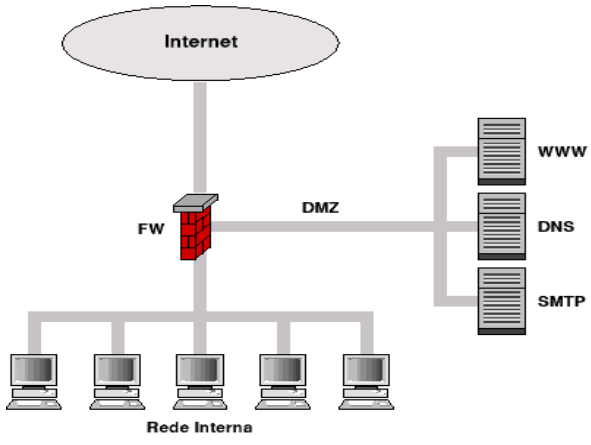


Figura 4 – Um exemplo simples de firewall

Esta secção apresenta duas destas arquitecturas. A intenção não é cobrir todas as possibilidades de uso de *firewalls*, mas fornecer exemplos de arquitecturas que funcionam e que podem eventualmente ser adoptados (na sua forma original ou após passarem por adaptações) em situações reais.

A figura acima mostra um exemplo simples de uso de *firewall*. Neste exemplo, o *firewall* possui três interfaces de rede: uma para a rede externa, uma para a rede interna e outra para a DMZ. Por omissão, esta *firewall* bloqueia tudo o que não for explicitamente permitido (*default deny*). Além disso, o *firewall* usado é do tipo *stateful*, que gera dinamicamente regras que permitam a entrada de respostas das ligações iniciadas na rede interna; portanto, não é preciso incluir na configuração do *firewall* regras de entrada para estas respostas.

O tráfego permitido no exemplo da figura acima é o seguinte:

1. Interface Externa:
    - Saída: tudo com excepção de:
        - Pacotes com endereços de origem pertencentes a redes reservadas;
        - Pacotes com endereços de origem não pertencentes a gamas da rede interna.
    - Entrada: apenas os pacotes que obedecem às seguintes combinações de protocolo, endereço e porta de destino:
        - 25/TCP para o servidor SMTP;
        - 53/TCP e 53/UDP para o servidor DNS;
        - 80/TCP para o servidor WWW.
2. Interface Interna:
    - Saída: tudo;
    - Entrada: nada;
3. Interface da DMZ:
    - Saída: portas 25/TCP (SMTP), 53/UDP e 53/TCP (DNS) e 113 (IDENT);

- Entrada: além das mesmas regras de entrada da interface externa, também é permitido o tráfego para todos os servidores na com porta de destino 22/TCP (SSH) e endereço de origem na rede interna.

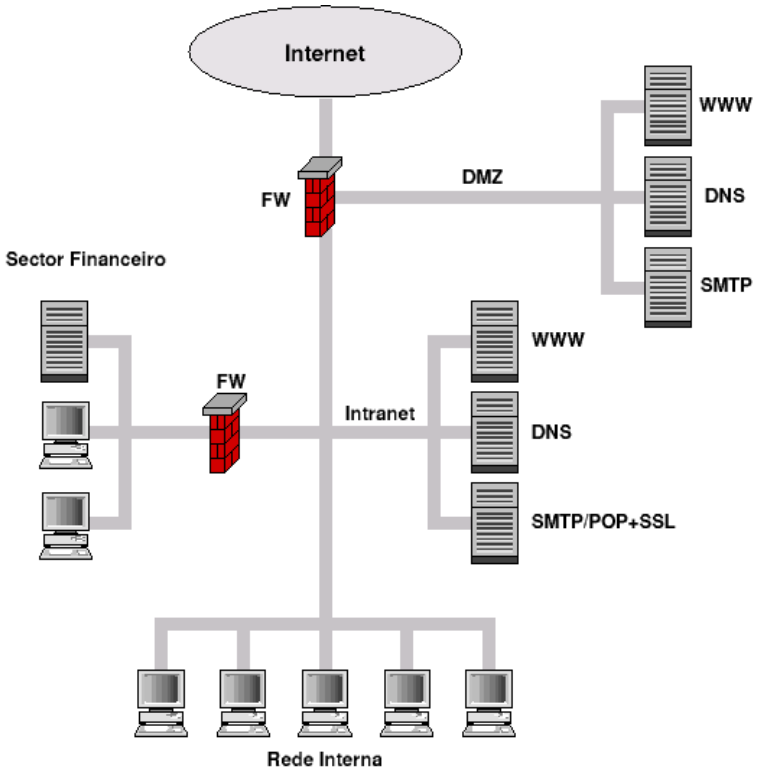


Figura 5 – Um exemplo complexo de *firewall*

A figura acima ilustra o uso de *firewalls* numa situação mais complexa do que a anterior. Neste segundo exemplo, além dos servidores externos na DMZ, há também servidores na *intranet* e no sector financeiro da organização. Devido à importância da informação mantida neste sector, a rede conta com a protecção adicional de um *firewall* interno, cujo objectivo principal é evitar que utilizadores com acesso à rede interna da organização (mas não à rede do sector financeiro) possam comprometer a integridade e/ou o confidencialidade dessas informações.

A configuração da *firewall* externa neste segundo exemplo é quase idêntica ao primeiro. Entretanto, no presente caso supõe-se que o servidor SMTP visível externamente (o da DMZ) encaminha as mensagens recebidas para o servidor SMTP da *intranet*. Para que isso seja possível, é necessário mudar a regra de filtragem para a interface interna, permitindo o tráfego do servidor SMTP da DMZ para a porta 25/TCP do servidor SMTP da *intranet*.

A configuração do *firewall* interno, por sua vez, é bastante simples. O servidor da rede do sector financeiro permite apenas acesso via HTTPS para que os funcionários da

organização possam consultar os seus recibos de vencimento; outros tipos de acesso não são permitidos. O tráfego permitido por este *firewall* é o seguinte:

1. Interface externa (rede interna):

    - Saída: tudo;
    - Entrada: apenas pacotes para o servidor do sector financeiro com porta de destino 443/TCP (HTTPS) e endereço de origem na rede interna;

2. Interface interna (rede do sector financeiro):

    - Saída: tudo;
    - Entrada: tudo (a filtragem é feita na interface externa).

3.11. SISTEMAS DE DETECÇÃO E MONITORIZAÇÃO ACTIVA

A detecção de intrusão é um conjunto de tecnicas e/ou métodos utilizados, para a detecção de actividade suspeita da organização, a nível de utilizadores e rede. A detecção de intrusão baseia-se em duas categorias básicas:

- **A detecção de intrusão dos sistemas baseada na assinatura** - Os intrusos têm assinaturas, como os vírus de computador, que podem ser detectadas com a ajuda de software, como o por exemplo o *snort*. Este tenta encontrar pacotes de dados que contêm assinaturas ou anomalias de intrusão, relacionadas, relativas a protocolos da Internet. Baseado num conjunto de regras e assinaturas, o sistema de detecção pode encontrar e registrar a atividade suspeito e gerar alertas.
- **A detecção de intrusão baseada na anomalia** – Este tipo de detecção depende das anomalias, existentes nos cabeçalhos dos pacotes. Em determinados casos, estes métodos produzem melhores resultados, comparadamente com o por assinatura. Esta sitação deve-se ao facto de que a detecção de intrusão captura os dados da rede e aplica regras para detectar as anomalias, emquanto que o por assinatura como o nome indica só procura as assinaturas.

3.11.1. IDS

(Intrusion Detection System) IDS poderá ser um software, hardware ou uma combinação dos dois, com o objective de detector actividades de intrusos. O IDS pode ter diferentes capacidades, dependendo da complexidade e da sofisticação dos seus componentes. *IDS appliances*, são a combinação do *hardware e software* que muitas empresas disponibilizam, e, usam detecção por assinaturas, anomalias ou os dois tipos. Os sistemas IDS têm como principais características [1][31]:

- Analisar o tráfego em tempo real (cabeçalhos e dados)
- Procurar pacotes IP com assinaturas específicas
- Alertar o administrador quando são detectados esses pacotes

Alguns sistemas IDS recentes têm formas de resposta activa em caso de detecção, tentando evitar o ataque informático subsequente:

- Interromper a sessão que deu origem à detecção
- Manipular as regras de filtragem do *firewall* no sentido de descartar o tráfego do potencial atacante – bloqueio temporário ou permanente

3.11.2. NETWORK IDS OU NIDS

(Network IDS) NIDS são sistemas de detecção de intrusão que conseguem capturar dados, à medida que estes são transmitidos pela infraestrutura (cabo, fibra, wireless). Ao mesmo tempo, comparam esses dados, com as bases de dados, de assinaturas na prespectiva de encontrar un intruso, sendo posteriormente gerado um alerta, ou activar de um ficheiro log.

3.11.3. HOST IDS OU HIDS

(Host-based intrusion detection systems) HIDS são sistemas ou agents de detecção de intrusão, instalados nos postos de trabalho dos utilizadores. Estes sistemas de detecção, conseguem monitorizar o sistema e ficheiros log, com o objectivo de detectar actividade maliciosa. Alguns destes sistemas podem ser reactivos, isto é, reagindo a uma tentativa ou a uma intrusão, com uma notificação ou alerta.

Por outro lado alguns HIDS são proactivos, ou seja, ao monitorizar o trafego da rede, assim que é detectada alguma anomalia, para alem originarem alertas ou notificações, também podem funcionar como actuadores, activando procedimentos em tempo real.

3.11.4. ASSINATURAS

As assinaturas são padrões que se encontram dentro dos pacotes de dados, sendo estas, utilizadas para detectar uma gama variada de ataques. Por exemplo, a presence de "scripts/iisadmin" em pacotes que são encaminhados para um servidor Web, podem indicar uma possível actividade de intrusão. As assinaturas podem estar presents em diferentes partes dos pacotes. Por exemplo, podemos encontrar assinaturas no cabaçalho ou na camada de transporte dos pacotes.

Os IDS dependem do tipo de assinaturas em que se pretende detectar actividade suspeita, e dependendo dos fabricantes, podem estar disponiveis actualizações de assinaturas.

3.11.5. LOCALIZAÇÃO DOS SISTEMAS IDS

Dependendo do tipo de topologia, pode-se optar por posicionar os detectores de intrusão, apenas num determinado local, ou em vário locais diferenciados. Isto depende que que tipo de actividades se pretende detectar/controlar, como, internas, externas, etc. Por exemplo, se o objectivo é detectar potenciais intrusões externas, coloca-se o sistema de detecção de intrusão é dentro do router ou da firewall internos. Na figura seguinte é apresentada a localização tápica para os detectores de intrusão.

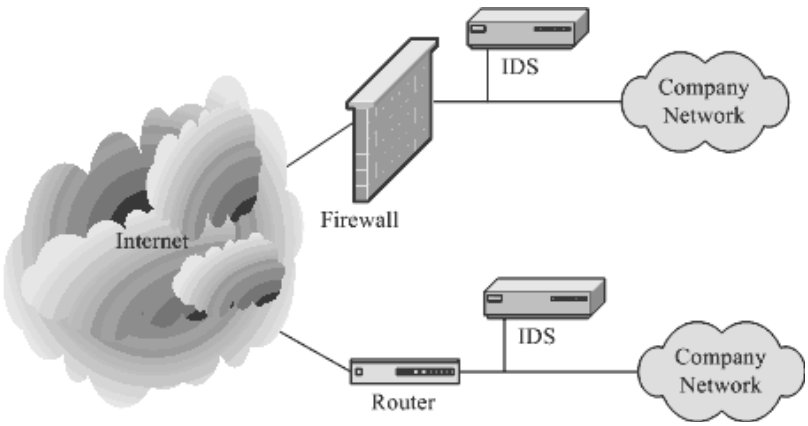


Figura 6 – Localização dos sistemas IDS

3.11.6. VULNERABILIDADES DA DETECÇÃO

Os sistemas IDSs não são infaliveis e por veses apresentam tanto detecções fidedignas como falsos resultados. Dependendo do tipo de alarmes apresentados pelos IDS são possíveis os seguintes tipod de cenários [31]:

- **Verdade positiva** — Ocorre quando um ataque real ocorrer, e o IDS responder com o alarme apropriado. Uma ação adicional pelos administradores de contra-ataque é exigida quando os alarmes positivos e verdadeiros ocorrem.
- **Verdade negativa** — Atividade normal, como esperado pelos administradores do IDS. Quando nenhum ataque acontece, o sistema de deteção de intrusão não tem nenhuma razão levantar alarmes.
- **Falso positivo** — Conhecido como falsos alarmes, estes ocorrem quando uma identificaçãofeita pelo IDS, determina trafego legítimo ou nenhuma atividade como sendo um ataque. Este é um inconveniente que pode provocar sérios problemas nos sistemas
- **Falso negativo** — Quando um potencial ou um ataque genuíno não é detectado pelo IDS. Neste cenário, à medida que aumentam as ocorrências, a sua genuidade deverá ser considerada duvidosa. Deverão ser feitas actualizações ao IDS ou considerar um eventual ataque que não está a ser detectado com a tecnologia existente.

3.11.7. RESPOSTA À DETECÇÃO DE INTRUSÃO

Os sistemas de detecção de intrusão, disparam vários tipos de alarmes e respostas, quando detectado tráfego malicioso. O grau de respostas depende do tipo de ataque realizado e do tipo de alarme gerado. Muitos alarmes falso positivos, não exigem que o administrador responda, contudo é benéfico efectuar registos, quando estes alarmes ocorrem. Dete modo a informação pode ser usada no futuro, para eventuais correcções do sistema. As modalidades activas e passivas das respostas, podem ser incorporadas nos sistemas, sendo algumas delas as seguintes [31]:

- **Bloqueio de endereço IP** — O IDS pode eficazmente obstruir o endereço IP em que originou o ataque. Este esquema pode não ser eficaz uma vez que, com a contante mudança da atribuição de endereços IP por parte dos operadores, o endereço do intruso está em constante mudança. Todavia, obstruir endereços IP é

uma forma muito eficaz de evitar servidores de envio eo Spam e aos ataques de negação de serviço.

- **Cancelar ligações ou sessões** — As ligações ou as sessões que um intruso mantem com o sistema comprometido podem ser interrompidas. O RESET dos pacotes TCP pode ser feito para que, o intruso perca as ligações ou sessões estabelecidas. Os routeres e as firewalls podem ser reconfigurados para tomar acções apropriadas, dependendo da gravidade da intrusão.
- **Adquirir informação adicional** — As respostas podem incluir a colecta de informação, sobre ou a observação do intruso durante o tempo. A ánalise dos registos ou mecanismos sensoriais podem, alertar os sistemas para trabalhar mais com cuidado, durante determinados períodos de recolha de informações. A informação recolhida pode ser usada posteriormente para analisar padrões do atacante, e, para fazer uma identificação mais robusta. Além disto, os mecanismos podem ser configurados para realizãr ações contra o intruso quando for suficiente o conhecimento sobre sua origem.

3.12. VIRTUAL PRIVATE NETWORK (VPN)

A ideia de utilizar uma rede pública como a Internet em vez de linhas dedicadas para implementar redes corporativas é denominada de Virtual Private Network (VPN) ou Rede Privada Virtual [1][12]. As VPNs são túneis encriptados entre pontos definidos, criados geralmente através da Internet, para transferência de informações, de modo seguro, entre redes, ou entre utilizadores remotos e essas redes.

A segurança é o conceito fundamental da VPN. Uma vez que dados privados serão transmitidos pela Internet, que é um meio de transmissão inseguro, deve haver um nível de protecção que impeça que esses mesmos dados sejam modificados ou interceptados.

Outro serviço disponibilizado pelas VPNs é a conexão entre empresas (Extranets) através da Internet, que possibilita a criação de ligações encriptadas que podem ser muito úteis para utilizadores móveis ou remotos, bem como filiais distantes de uma empresa.

Uma das grandes vantagens do uso das VPNs é a redução de custos com comunicações, pois elimina a necessidade de linhas dedicadas de longa distância que podem ser substituídos por linhas ADSL em cada ponto sendo configuradas VPN´s. Esta solução

pode ser bastante económica, sobretudo com o aumento das velocidades das linhas ADSL de hoje em dia.

Em resumo, duas formas de aplicabilidade de VPN´s, passam por [1][16]:

- Acesso remoto via internet
- Interligação de redes via Internet

Para a realização deste trabalho vão ser configuradas VPN´s através da aplicação "OpenVpn" [28], uma vez que apresenta as características especiais, como as seguintes:

- É *software* livre, ou seja, pode-se usar e modificar, sem qualquer problema de com licenças.
- Permite construir um túnel em qualquer subrede ou adaptador ethernet virtual, sobre uma única porta UDP ou TCP,
- Permite usar toda a encriptação, autenticação e características de certificação OpenSSL para proteger o tráfico da rede privada.
- Permite usar *cipher*, chave, ou compilador HMAC suportado pela OpenSSL,
- Permite escolher entre chave-estática baseada em encriptação convencional ou chave-pública baseada em certificação.
- Permite construir um túnel com uma rede na qual o ponto final seja dinâmico, ou seja, um DHCP ou clientes com DNS dinâmico.
- Permite controlar o OpenVPN usando uma GUI no Windows ou Mac OS X.

3.13. RESUMO

Neste capítulo foi descrita a problemática da implementação, de políticas e procedimentos de segurança numa empresa. Foram descritos os objectivos a cumprir por uma correcta política de segurança, e a importância da estruturação da mesma, antes da implementação do sistema. Para melhor compreender este processo, foram descritas as etapas do ciclo das políticas, desde a sua definição, até à fase de optimização.

Após a definição e descrição dos processos teóricos de segurança, foram enunciadas algumas características para uma correcta e segura configuração do sistema, como a

instalação lógica do sistema, atribuição palavras-chave seguras, gestão de cópias de segurança e formação no sentido de definir cuidados especiais com engenharia social.

De forma a ajudar a compreensão dos conceitos enunciados neste capítulo, foram descritas características que permitem optimizar a gestão de pessoas e máquinas, gerando simultaneamente uma mais fácil manutenção do sistema. Foram referidos aspectos relacionados com a optimização do sistema operativo, sincronização de relógios, registo de eventos e alertas do sistema, uso de servidores DNS e serviços WHOIS. Por fim, foi ainda feito um estudo aprofundado sobre o uso de *firewalls*, sistemas de detecção de intrusão e, formas de optimizar o seu funcionamento de acordo com o tipo de sistema, Para maior segurança e facilidade de acesso externo à rede interna, foi enunciada a possibilidade de uso de redes privadas virtuais ou VPNs.

4. SEGURANÇA DE INFRAESTRUTURAS E SISTEMAS

4.1. REDES DE COBRE OU FIBRA ÓPTICA

As redes de cobre ou via fibra *Ethernet* são muitas vezes deixadas ao abandono, negligenciadas por parte dos administradores, esquecendo-se que hoje em dia, num ambiente globalizado como é o empresarial, entram e saem das empresas uma série de pessoas que nada têm a ver com a organização [9], evienciando falhas graves na política de segurança implementada.

Assim sendo deve-se procurar adoptar algumas das seguintes acções:

- **Em Projecto**:
    - Documentar toda a infra-estrutura de ligações quer dos equipamentos activos, quer das tomadas de rede.

- Não existindo qualquer sistema de segurança na ligação Ethernet, implementar pelo menos a atribuição de IP via DHCP por endereço MAC ou via IP fixo.

- Implementar segurança as portas dos *switches* em que se ligam APs para que, no caso de serem roubados a porta ficar bloqueada, não ser possível a ligação de outro AP não autorizado na mesma porta sem intervenção do administrador.

- Vedar o acesso físico a bastidores ou *switches* intermédios ou zonas técnicas, de modo a que utilizadores mal intencionados, não consigam aceder à rede ou até provocar outros estragos como desligar os equipamentos.

- **Gestão e manutenção:**

  - Registar as acções de novas instalações e configurações da rede.

  - Efectuar as ligações das tomadas aos *switches*, usando apenas as estritamente necessárias. Registá-las, desactivar as portas quando não forem necessárias e manter a vigilância das áreas técnicas.

  - Realização de inventário periódico dos equipamentos ligados à rede e inspacção do estado da cablagem.

De seguida é apresentado um caso em que, através do uso aplicações como IPSCAN juntamente com AMAC, é possível clonar o endereço MAC de um utilizador com IP atribuído por DHCP baseado no endereço MAC. Sendo assim, ao configurar o DHCP para atribuir endereços por endereço MAC, é possível adicionar um nível de segurança acrescido, uma vez que o acesso à rede é limitado fisicamente, e em caso de clonagem, obriga a executar as tarefas de pequisa e clonagem apresentadas nas figuras seguintes.

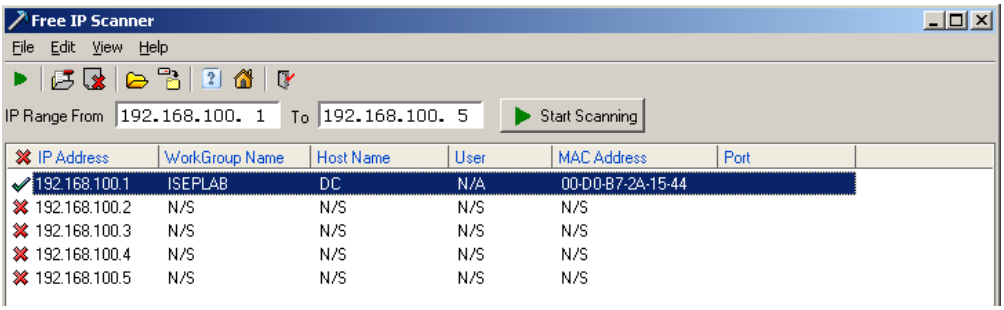


Figura 7 – Ferramenta de pesquisa de máquinas na rede

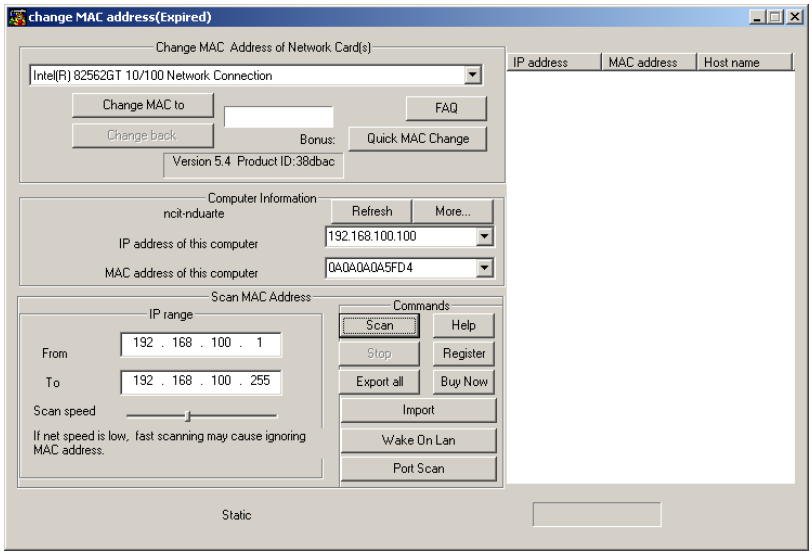


Figura 8 – Ferramenta de alteração do endereço MAC

4.2. REDES WIRELESS

Esta secção mostra alguns cuidados a ter pelos administradores aquando da instalação e operação segura das redes *wireless*.

4.2.1. POLÍTICA DE UTILIZAÇÃO DA REDE WIRELESS

É muito importante que seja definida uma política de uso da rede *wireless*, que deve ser incorporada na política de segurança da instituição [11]. Esta política deve cobrir pelo menos os seguintes itens [26]:

- Definir quem está autorizado a instalar *Access Points* (APs) nas instalações da instituição. A instalação de APs por pessoal não autorizado, e sem as devidas precauções, pode comprometer seriamente a segurança de toda rede;
- Definir quem está autorizado a utilizar a rede *wireless* da instituição;

- Prever as acções a ser tomadas em caso de roubo ou perda de equipamentos *wireless*; Por exemplo, a configuração de *port security no switch* adjacente, impede que em caso de roubo este seja reposto ou substituído, sem intervenção do administrador da rede.
- Definir que tipo de informação, pode ser transmitida pela rede;
- Descrever as configurações mínimas de segurança para APs, clientes, etc.

4.2.2. TOPOLOGIA

Existem dois factores muito importantes que devem ser considerados ao definir a topologia de uma rede *wireless*: o posicionamento dos APs e a necessidade de isolar a rede externa da rede interna.

Em relação ao posicionamento do AP, dependendo da potência da antena, uma rede *wireless* pode ter um alcance que ultrapasse os limites geográficos da instituição, o que pode potenciar um uso e uma captura não autorizadas. Esse excesso de sinal é extremamente comum e deve servir de estímulo, para o administrador implementar medidas preventivas como por exemplo, o uso de autenticação e encriptação.

Além do uso de encriptação, um posicionamento cuidadoso dos APs (mais para o centro de um prédio, longe de janelas, etc.) pode minimizar a propagação desnecessária de sinal. É importante notar que esse procedimento deve ser encarado, apenas como uma camada adicional de segurança, uma vez que um intruso pode fazer uso de uma antena amplificadora de sinal e ter acesso à sua rede *wireless* mesmo a distâncias maiores.

Em relação ao isolamento da rede *wireless* da rede interna da organização, deve ter-se em conta que as redes *wireless* não devem ser ligadas directamente, dentro de uma rede protegida por um *firewall* (devem ser consideradas "*untrusted*"). Colocar um AP directamente numa rede protegida por um *firewall,* seria equivalente à instalação de um *modem* dentro dessa rede, por exemplo.

Uma solução de topologia pode ser colocar todos os APs numa zona da rede, e colocar uma *firewall* entre essa zona e o resto da infra-estrutura de rede da instituição. Além de possibilitar o controlo de utilização, ainda se cria uma possibilidade de integração com VPNs.

Por fim, ao ligar um AP, é preferível fazê-lo a um *switch*, e não a um *hub*. O tráfego de rede num *hub* pode ser enviado para toda a rede *wireless* e eventualmente ser interceptado por algum cliente.

4.2.3. ENCRIPTAÇÃO E AUTENTICAÇÃO

Devido à facilidade com que uma rede *wireless* pode ser utilizada por pessoas não autorizadas e à facilidade com que se pode capturar o tráfego, é extremamente importante o uso de encriptação e de mecanismos de autenticação numa rede *wireless*.

O padrão 802.11 original suporta apenas dois tipos de autenticação do cliente *wireless*: "*open authentication*" e "*shared-key authentication*". No primeiro modo o cliente precisa apenas de fornecer o *Service Set Identifier* (SSID) correcto para juntar-se à rede. No modo "*shared-key authentication*" é preciso o conhecimento de uma chave WEP (*Wired Equivalent Privacy*) para que isso ocorra. É importante notar que essa autenticação é do dispositivo *wireless*, e não dos utilizadores da rede.

O padrão 802.11 define o protocolo WEP como mecanismo para codificar o tráfego entre os APs e os clientes *wireless*. Essa codificação ocorre na camada de ligação e exige que todos os participantes partilhem a mesma chave WEP estática. O WEP possui diversas fragilidades, mas apesar disso o seu uso é recomendável e deve ser encarado como uma camada adicional de segurança.

Para aumentar a segurança nas redes *wireless* deve-se escolher o maior tamanho de chave WEP possível, sendo essencial trocar as chaves WEP que venham nas configurações padrão dos equipamentos. O uso de encriptação nas aplicações, como SSH e SSL, também é recomendável para minimizar os riscos de escuta não autorizada. Além disso também deve ser considerado o uso de encriptação no próprio protocolo TCP/IP, como IPsec e o uso de VPNs em geral.

4.2.4. REDES PROTEGIDAS POR 802.1X

O 802.1X [17][26] foi concebido para oferecer autenticação, controlo de acesso e distribuição de chaves em redes locais, com ou sem fio. Apesar de ser mais utilizado para redes sem fio, não está ligado às normas IEEE 802.11, estando no entanto ligado às normas IEEE 802, relativas a todos os padrões de redes locais e metropolitanas, além de poder ser

utilizado em conjunto com diversos protocolos de autenticação localizados nas camadas superiores.

Relativamente a isto, deve-se também referir que o mecanismo de autenticação a ser utilizado no IEEE 802.11 deverá obrigatoriamente seguir o modelo do IEEE 802.1X.

O 802.1X é bastante utilizado no meio empresarial, visto que estabelece uma estrutura de autenticação sofisticado além de adaptar também o *Extensible Authentication Protocol (EAP),* que permite encapsular diversos protocolos de comunicação existentes nas camadas superiores, não definidos pelo 802.1X. Estes protocolos introduzem aspectos como autenticação por *Kerberos,* palavras-chave, certificados digitais e chaves públicas.

O protocolo 802.1X permite efectuar o controlo de acesso orientado à porta e a distribuição de chaves, quer com o WEP dinâmico, bem como no WPA e WPA2. Além disso, ele resolve um problema existente no modo "Personal" do WPA2, o qual consistia na mudança de chaves na totalidade de uma rede. No 802.1X, não é necessário realizar a alteração das chaves de uma só vez para todos os equipamentos da rede, pelo que se torna mais intuitivo e dinâmico de ser utilizado.

O 802.1X permite autenticação mútua, garantido quer a autenticação do utilizador na rede bem como a autenticação da própria rede ao utilizador (evitando redes "falsas"), além de garantir uma arquitectura de autenticação e controlo de acesso bastante fiável.

O padrão não especifica qual o tipo de arquitectura a utilizar, sendo no entanto a norma associá-lo a uma arquitectura com servidores RADIUS e base de dados de suporte. Visto que o servidor de autenticação pode estar incluído no próprio Access Point, este não é um requisito obrigatório deste protocolo.

O 802.1X apesar de oferecer uma autenticação forte, apresenta algumas vulnerabilidades, devido a alguns protocolos que introduz, o que pode levar a ataques como *session hijacking*, entre outros.

Alguns dos protocolos suportados pelas camadas superiores e que são introduzidos no 802.1X são EAP-TLS (Transport Layer Security), o PEAP (Protected Extensible Authentication Protocol), o EAP-TTLS (Tunnuled Transport Layer Security) e o LEAP (Lightweight Extensible Authentication Protocol).

4.2.5. ACCESS POINTS

Existem vários aspectos importantes que devem ser considerados na escolha e configuração de um AP:

1. **Considerações na escolha:** na escolha de um modelo de AP é muito importante determinar quais os recursos de encriptação e autenticação que são suportados [17]. Outro factor importante é saber se o AP possibilita *upgrades* de *firmware*, permitindo incorporar novos padrões e eventuais correcções desenvolvidas pelo fabricante.

2. **Alteração de configurações padrão:** muitos modelos de APs vêm com configurações de fábrica que são do conhecimento público, incluindo palavras-chave *default*. É extremamente importante que todas as configurações originais sejam mudadas pelo administrador antes de colocar o AP em funcionamento, incluindo:

    - Palavras-passe de administração;
    - SSID;
    - Chaves WEP;
    - *Communities* SNMP.

3. **Modos de configuração:** a maioria dos APs permite vários meios de configuração: HTTP, SNMP, Telnet, etc. Sempre que possível, é importante desabilitar os que não forem necessários e optar por um modo de configuração, que não seja pela própria rede *wireless*, mas sim pela rede de cobre ou via ligação série. Isso minimiza as hipóteses de que a sessão de configuração com o AP seja capturada por algum cliente *wireless*.

4. ***Broadcast* de SSID:** uma recomendação útil é desabilitar o *broadcast* de SSID pelo AP. Embora seja uma medida simples, pode dificultar o uso de alguns programas populares de mapeamento de redes *wireless* como o *Omnipeek ou Netstumbler*

5. **Filtragem por endereço MAC:** alguns APs possuem o recurso de filtragem de clientes *wireless* por endereço MAC. Embora endereços MAC possam ser falsificados, e muitas vezes não seja prático manter uma lista de endereços MAC dos clientes autorizados (e em alguns casos inviável, como por exemplo em conferências), o administrador pode considerar, o uso desse recurso como uma camada adicional de segurança do seu ambiente *wireless*.

6. **Acesso Físico**: Alguns APs possuem uma opção de *reset* físico, que faz com que todas as configurações de fábrica sejam repostas. Nesses casos, é muito importante que o AP fique num local com acesso físico controlado. Por outro lado, caso não tenha o *reset* físico pode ser substituído por um AP do intruso.

Uma última consideração diz respeito à possibilidade de desligar o Access Point quando o mesmo não estiver a ser usado, evitando que a rede esteja disponível por mais tempo do que o necessário.

4.2.6. PROTECÇÃO AOS CLIENTES WIRELESS

A educação dos utilizadores é um aspecto muito importante e eles também devem receber as orientações sobre a utilização segura das redes *wireless*. Uma rede *wireless* deve ser considerada uma rede pública e, portanto, mais susceptível a ataques. Deste modo, é recomendável que os clientes dessa rede, tais como portáteis, PDAs, estações de trabalho, etc, passem por um processo de instalação e configuração que vise o aumento de sua segurança, incluindo:

- Aplicação de *patches*;
- Uso de *firewall* pessoal;
- Instalação e actualização de anti-vírus;
- Desactivação da partilha do disco, impressora, etc.

4.2.7. MONITORIZAÇÃO DA REDE WIRELESS

Da mesma forma que muitos administradores monitorizam o seu ambiente de rede convencional (com o uso de *Intrusion Detection Systems* ou IDSs, por exemplo) [31], a monitorização da rede *wireless* também é importante. Essa monitorização pode detectar:

- Clientes ligados num dado instante (em horários improváveis ou simplesmente para acompanhamento);
- Instalação de APs não autorizados;
- Dispositivos que não estejam a usar WEP;
- Ataques contra os clientes *wireless*;
- Acessos não autorizados;
- Mudanças de endereços MAC;
- Mudanças de canal;
- DoS ou *jamming*.

A nível de monitorização, ferramentas como *nágios*, HP Procurve Manager, ou HP Procurve Mobility Manager permitem gerir, analisar, gerar e enviar alertas sobre o estado dos quaiquer equipamentos activos.

4.3. PREPARAÇÃO DA INSTALAÇÃO DE SISTEMAS

A instalação de um sistema deve ser feita com este isolado da rede. Esta operação reveste-se de maior importância, quando se pretende disponibilizar serviços para o exterior (internet).

Ainda ssim, deve-se ter em atenção alguns procedimentos como:

- Planear a instalação, definindo itens como:
    - O propósito do sistema a ser instalado;
    - Os serviços que este sistema disponibilizará;
    - A configuração de *hardware* da máquina;
    - Particionamento de disco,
- Instalar o sistema a partir de dispositivos de armazenamento locais (CD, fita ou disco), desligado da rede;

- Caso seja necessário efectuar *downloads* de actualizações, por exemplo, deve-se colocá-lo numa rede isolada, acessível apenas pela rede interna.

Caso seja possível, deve-se evitar concentrar todos os serviços de rede apenas numa única máquina, distribuindo-os por vários sistemas. Isto é desejável pois aumenta a disponibilidade dos serviços na rede e reduz o número de serviços não disponibilizados em caso de comprometimento de algum sistema.

4.4. ESTRATÉGIAS DE DEFINIÇÃO DE PARTIÇÕES

Na instalação de um sistema a definição de partições é importante. O idel é dividir o disco em várias, em vez de usar uma única partição ocupando o disco inteiro. Isto é recomendável por diversas razões [1][13]:

- Um hacker ou um programa mal construído pode encher uma partição na qual tenha permissão de escrita (áreas temporárias e de armazenamento de *logs* são susceptíveis a este problema). Se os programas estiverem noutra partição, o sistema operativo por exemplo provavelmente não será afectado, evitando que o sistema pare.

- Caso uma partição seja corrompida por alguma razão, as outras partições provavelmente não serão afectadas.

- Em determinados sistemas, é possível definir algumas características individuais para cada partição ou patilha. Por exemplo, nos sistemas Unix, algumas partições podem ser usadas em modo "só de leitura", o que é útil para partições que contenham binários que são modificados com pouca frequência. Nos sistemas Microsoft pode-se definir permissões a nível da partilha ou a nível NTFS o que aumenta a segurança.

- Em determinados casos a existência de várias partições permite múltiplas operações de disco em paralelo e/ou o uso de optimizações individuais para cada partição, o que pode aumentar o desempenho do sistema.

- O uso de várias partições geralmente facilita o procedimento de *backup* do sistema, pois simplifica funções como:

    - Copiar partições inteiras de uma só vez;

- Excluir partições individuais do procedimento;
- Fazer *backups* em intervalos diferentes para cada partição.

As partições específicas que devem ser criadas variam de sistema para sistema, não existindo uma regra que possa ser sempre seguida. No entanto, é de útil avaliar a conveniência da criação de partições separadas para as áreas onde são armazenados itens como:

- Programas do sistema operativo;
- Dados dos utilizadores;
- *logs*;
- Arquivos temporários;
- Filas de envio e recepção de *e-mails* (servidores *Simple Mail Transfer Protocol* – SMTP);
- Filas de impressão (servidores de impressão);
- Repositórios de arquivos (servidores FTP);
- Páginas Web (servidores HTTP).

As partições devem ser dimensionadas de acordo com os requisitos de cada sistema. Em determinados casos, o tamanho ocupado pelo sistema operativo é fornecido, o que pode auxiliar na determinação do tamanho de algumas partições.

Qualquer que seja a estrutura de divisão escolhida, é recomendável se tenha pelo menos um esboço desta por escrito antes de começar a instalação. Isto facilita o processo de instalação e reduz a probabilidade de fazer uma determinada escolha, sem que as suas consequências sejam antecipadamente previstas.

4.5. DESACTIVAÇÃO DE SERVIÇOS NÃO UTILIZADOS

Um procedimento importante na segurança de sistemas é a desactivação de serviços (locais e, principalmente, de rede) que não serão utilizados no sistema. A lógica por detrás desta recomendação é reduzir a exposição do sistema a vulnerabilidades externas [1][13].

Embora possa parecer que existe redundância entre esta fase e a anterior, na prática surgem situações nas quais o administrador é forçado a instalar um pacote ou componente completo para poder utilizar apenas um subconjunto das funcionalidades oferecidas por esse pacote. Além disso, muitos programas optam por maximizar as funcionalidades disponibilizadas aos utilizadores, e a configuração padrão do sistema deixa activados todos os serviços instalados. Caso uma dessas situações ocorra, as funcionalidades que não serão utilizadas deverão ser desactivadas ou mesmo removidas do sistema.

Por exemplo, no caso da instalação do IIS da Microsoft, que instala o serviço Web e FTP por omissão, se o administrador não alterar a configuração após a instalação, e caso só necessite de ter um dos serviços a funcionar, terá os dois serviços a funcionar desnecessariamente.

Caso não seja possível desactivar serviços individualmente, uma alternativa é usar um filtro de pacotes, ou firewall para bloquear as portas TCP/UDP usadas por esses serviços, impedindo que eles estejam acessíveis através da rede.

4.6. ANTI-VÍRUS E DETECTORES DE VÍRUS

A detecção de intrusão compreende uma variedade de técnicas e mecanismos. A principal operação consiste em determinar, se um sistema está infectado por um vírus ou outro tipo de código malicioso. As técnicas de "*Vírus scanning*" e prevenção de intrusões são usadas para prevenir e/ou detectar problemas, aplicando em simultâneo os mecanismos de resposta necessários, para suprimir esses ataques [2].

Os detectores de Vírus usam algoritmos de teste combinado, que podem verificar diferentes assinaturas ao mesmo tempo. Estes algoritmos incluem potencialidades de detecção de *worms*, conhecidos e desconhecidos, e cavalos de Tróia. Os detectores verificam discos e outras unidades e se encontram algum ficheiro com vírus, removem esses ficheiros para a zona de quarentena ou até os eliminam. Geralmente realizam actualizações automáticas, efectuando downloads das configurações de novos vírus que entretanto vão aparecendo.

Como ferramenta de teste para este projecto foi usado o Etrust 8.1 [26], apesar de ser comecialmente pago, quando comparado com um grátis como o clamwin, tem algumas diferenças importantes, que em muitos casos justificam o seu custo. Por exemplo:

- Dispor de uma consola de gestão e alertas para todos os equipamentos da organização
- Permitir a instalação remota do anti-vírus em qualquer computador da rede
- Utilização de vários motores de pesquisa de vírus, como o "realtime", que corre em background e verifica todos os ficheiro que não sendo executados, lidos ou escritos.
- Dispor de suporte para verificação de Java e ActiveX, SMTP, POP3, FTP e HTTP.
- Permitir actualizações automáticas das bases de dados bi-diárias e suporte 24h.

4.7. INSTALAÇÃO E VERIFICAÇÃO DE ACTUALIZAÇÕES

Depois de instalados e configurados os sistemas, é necessário verificar se não existem correcções ou actualizações [1][6] (*patches*, *fixes*, *service packs*) para vulnerabilidades conhecidas nos componentes instalados. A maioria dos fornecedores de *software* disponibiliza correcções, para problemas de segurança que sejam descobertos, sem que se tenha de esperar pela publicação da próxima versão. Na maioria das vezes, estas correcções estão disponíveis através da Internet.

No entanto, nem sempre todas as correcções disponíveis precisam ser instaladas. Deve-se limitar as correcções, aos componentes que estejam efectivamente instalados no sistema. A instalação indiscriminada de actualizações pode enfraquecer a segurança do sistema em vez de a fortalecer [13].

Muitas vezes algumas configurações do sistema são alteradas durante o processo de instalação de actualizações. Sendo assim, é recomendável que se reveja a configuração dos sistemas após instalar uma correcção, para certificar, que a instalação não tenha revertido eventuais configurações.

É bastante útil manter um repositório das actualizações que já foram utilizadas, para facilitar a instalação das mesmas noutros sistemas.

No caso da Microsoft o (*WSUS) windows update services* [6] que faz a gestão das actualizações efectuadas, a efectuar e disponíveis para aprovação. Usando WSUS, os administradores podem inteiramente controlar a distribuição das actualizações, que são

disponibilizadas através do site de actualização da Microsoft, e, definir políticas de actualização, definindo horários e actualizações a efectuar nos computadores.

4.8. PREVENÇÃO DE ABUSO DE RECURSOS

Existem alguns serviços que, quando mal configurados, podem permitir que utilizadores externos abusem dos recursos da sua rede, ainda que isso não implique na ocorrência de uma invasão. Dois destes serviços são o *e-mail* e os *proxies Web* [1][4][8].

A configuração incorrecta destes serviços pode causar vários efeitos indesejáveis. Um deles é que recursos computacionais da organização (a começar pelo *link* Internet, mas incluindo CPU, discos e memória dos servidores) são usados por terceiros sem que eles paguem por essa utilização. Em muitos casos, esses recursos são de tal forma consumidos que utilizadores legítimos não conseguem utilizar esse serviço.

Além disso, servidores mal configurados são muitas vezes usados para disseminar conteúdo ilegal, tal como pornografia envolvendo crianças. Se um conteúdo deste tipo for encontrado em sistemas da organização, existe a possibilidade de que a organização venha a ser legalmente implicada em processos-crime.

4.8.1. CONTROLE DE RELAY EM SERVIDORES SMTP

Na sua configuração padrão, muitos servidores SMTP vêm com a funcionalidade de *relay* aberto [3], permitindo que seja usados, para enviar mensagens de e para qualquer rede ou domínio, independente dos endereços envolvidos serem da sua rede ou não. Estes servidores são os mais explorados para envio de SPAM.

Além das consequências já mencionadas, diversas redes bloqueiam a recepção de mensagens, a partir de servidores que tenham sido ou estejam a ser usados para envio de SPAM, fazendo com que utilizadores do servidor com o "*relay* aberto" não possam enviar mensagens a utilizadores [4]. Há que se considerar também, que o uso de servidores SMTP de terceiros, torna mais difícil a localização e identificação dos *spammers*, diminuindo as possibilidades deles serem identificados e punidos por estes abusos.

Para resolver o problema do "*relay* aberto" é necessário configurar os servidores SMTP correctamente. A configuração adequada deve permitir apenas:

- Envio de mensagens com endereço de origem local e endereço de destino local ou externo;
- Recepção de mensagens com endereço de origem local ou externo e endereço de destino local.
- Associar ao servidor SMTP filtros anti-spam e *anti-vírus* como por exemplo *spamassassin* e *clamav.*
- Efectuar online, através de listas RBL [4], a pesquisa dos servidores em "*relay* aberto" comprometidos e bloquear a recepção de *e-mails* destes servidores.

Na maioria dos casos, é possível fechar o *relay* mesmo quando a rede possui *roaming users* (utilizadores de dispositivos móveis), usando mecanismos como POP-before-SMTP e SMTP AUTH, ou então utilizar um servidor de e-*mail Relay* que possibilite a implementação do máximo de protecções possível.

Como possibilidade existe a implementação de várias ferramentas [23], que combinadas entre si cumprem a comfiguração adequada acima anteriormente referida. As ferramentas são o Postfix, Amavis, Spamassassim e Clamav, permitindo também a possibilidade de apresentar um relatório estatístico de todo o *e-mail* processado. Este reletorio permite verificar a quantidade de *e-mail* que foi entregue sem problemas, a quantidade de *e-mail* de spam, a quantidade de *e-mail* com vírus etc.

4.8.2. CONTROLE DE ACESSO A PROXIES WEB

Assim como no caso dos servidores SMTP, *software* que faz *proxy* de Web (tais como Squid [19], Wingate e Microsoft ISA Server), também pode sofrer abusos se não forem tomadas as devidas precauções.

Um *proxy* mal configurado pode ser usado por utilizadores externos como um "trampolim" para acesso a recursos de forma anónima. Este anonimato pode ser usado para cometer crimes, tais como envio de mensagens caluniosas, difamatórias ou ameaçadoras e divulgação de pornografia infantil [1].

A configuração correcta para um *proxy* Web é aquela que permite o acesso somente aos endereços IP ou melhor ainda, aos utilizadores autorizados (pertencentes à sua rede).

Em ambientes em que o abuso é realmente um problema, ferramentas como *Sarg* [21] *ou Microsoft ISA 2006* permitem controlar todo o tráfego ou navegação do utilizador, ou seja que sites consultou, que downloads fez, quanto tempo e largura de faixa usou e a que horas acedeu a determinado recurso.

Este tipo de controlo tem que estar incluído nas políticas de segurança da organização e os utilizadores devem ser informados antes da sua implementação, visto que, para alguns utilizadores pode potenciar uma eventual invasão de privacidade.

4.8.3. FILTRAGEM DE CONTEÚDOS WEB

Apesar do controlo de acesso a nível do *Web proxy* limitar em muito o uso abusivo, hoje em dia existe uma preocupação acrescida das organizações em limitar os acessos a conteúdos Web, ora por provocarem distracção e perca de produtividade dos utilizadores ora por muitas vezes o acesso a conteúdos pouco fidedignos, pode colocar em risco a rede pois estes sites muitas vezes por intermédio de *java scripts* ou outros activam cavalos de Troia no sistema.

Esta filtragem é feita geralmente em associação e/ou com o *Web proxy* bloqueando por exemplo o acesso a sites que contenham palavras como “sex”, “sexo”, *urls* como *www.casino.net,* e que não permitem por exemplo o download de ficheiros *.mp3 Algumas das ferramentas de filtragem de conteúdos são o *squid-guard, dansguardian [20]* e *Microsoft ISA Server*.

4.9. RESUMO

Este capítulo vem enunciar alguns dos aspectos físicos das diferentes redes existentes, suas características e regras para melhor garantir um nível de segurança aceitável. Foram referidas as redes de cobre/fibra óptica e as redes sem fios, bem como as csaracterísticas e vulnerabilidades a que cada uma delas está afecta. Enunciaram-se variadas formas de configuração, e formas para reduzir a complexidade, e definir regras objectivas e implementar segurança a nível de actualizações no sistema, protocolos usados, canais de comunicação, chaves de acesso (autenticação), entre outras.

Neste capítulo, é feita também uma abordagem mais pormenorizada dos passos ideais, para uma configuração segura de uma infraestrutura em rede. Foram vistos alguns aspectos cruciais, como a instalação/configuração do sistema operativo e actualizações devem ser

feitos, com o maior cuidado e sem acesso ao exterior, pois é através de vulnerabilidades existentes nesta área, que surgirão a grande maioria dos ataques ao sistema. Após montado todo o sistema, foram referidas características ligadas à manutenção do sistema, como a instalação de software adicional, antí-vírus e anti-spam, configuração de acessos/restrições a utilizadores e criação de filtros web.

5. DEFINIÇÃO DA REDE DE ESTUDO

5.1. INTRODUÇÃO

Para definir que tipo protecção se deve implementar numa infraestrutura, primeiro, é necessário avaliar quais as vulnerabilidades existentes, para que se possa apresentar a solução mais adequada e com o menor custo. Neste capítulo é apresentada uma rede de estudo com interligação de sistemas Microsoft e Linux, protocolos e serviços implementados, como serviço *web, e-mail, webmail,* acessos remotos, entre outros. Depois de implementado o protótipo da rede é feita uma análise das falhas existentes, garantindo-se ter uma noção tão exacta quanto o possível do tipo de problemas e vulnerabilidades existentes.

5.2. ARQUITECTURA DA REDE

A arquitectura da rede de estudo tem como base uma Directoria Activa (*Active Directory*) de Microsoft, de domínio iseplab.local, constituída por um servidor controlador de domínio

(Domain Controler – DC*)* e um servidor de *e-mail* com Microsoft Exchange 2003 como se ilustra na figura seguinte.

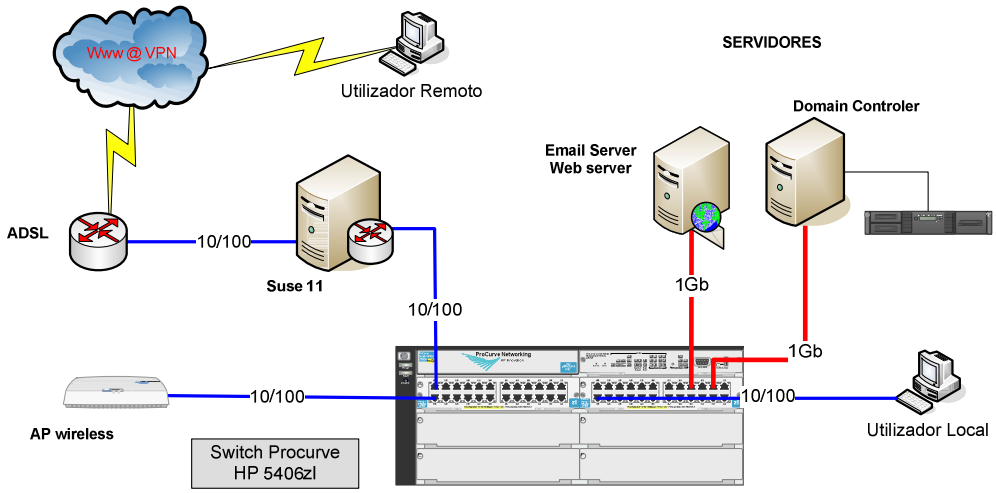


Figura 9 – Infra-estrutura física

A efectuar a interligação física de todos os equipamentos foi colocado um switch HP que fornecerá interface via Ethernet às máquinas de teste, e um ponto de acesso wireless que será o interface wireless às máquinas teste.

O DC permite validar todos os utilizadores e computadores da rede, funcionando também como servidor de ficheiros, com os dados partilhados da rede, com uma instalação normal sem aplicação de políticas de segurança.

O servidor Exchange é onde os utilizadores irão ter as suas caixas de correio, que poderão ser acedidas, interna ou externamente, por *Outlook* ou via *Webmail*.

Para interligar a rede externa à rede interna foi colocado um servidor Linux que neste cenário funcionará como router, apesar de ter instaladas algumas ferramentas que serão fundamentais para a análise de falhas e/ou vulnerabilidades. Esta medida fornece os serviços de acesso ao exterior aos utilizadores internos como internet (www), transferência de ficheiros (ftp) entre outros. Aos utilizadores externos encaminha os acessos de webmail, ftp, smtp para os servidores internos correspondentes. O servidor Linux é representado por "SUSE11.ISEP.LOCAL", no diagrama seguinte.

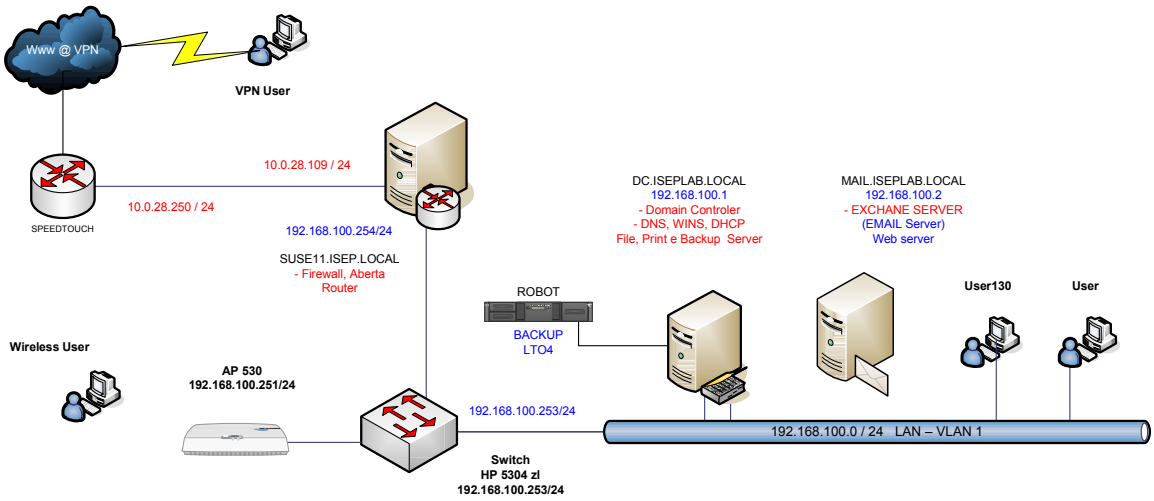


Figura 10 – Arquitectura da rede de estudo

Desta forma pretende-se implementar uma infra-estrutura básica insegura, ou com um mínimo de segurança, definindo-se, os equipamentos necessários, critérios de configurações, funções e serviços de cada um. Para a rede de estudo definiram-se as seguintes configurações:

- Endereçamento da Rede Interna (192.168.100.x / 24)
- Endereçamento da Rede Externa (cedida pelo Isep, 10.0.28.0.x / 24)
- Definição de 2 utilizadores: user e user130.
- Atribuição de IP aos pc's, por DHCP por endereços MAC
- Todos utilizadores da organização têm que ter correio interno e só alguns devem ter correio externo. O "user130" deverá ter acesso apenas ao *e-mail* interno e o "user" ao e-mail interno e externo. O endereço externo é @caramelo.com
- Os utilizadores que têm correio externo devem conseguir aceder ao correio remotamente do exterior.
- A não utilização de qualquer tipo de firewall, para comprovar a sua necessidade e, pelo facto que quando são requeridos acessos à internet por parte do ISP, este cobra o serviço de firewall à parte, que nem sempre é adjudicado.
- Configuração de um AP com chave WEP, uma vez que é o mais fácil de configurar, mas também se irá mostrar que é o mais vulnerável.

- Acesso directo a todos os recursos da internet, sem qualquer protecção de segurança, a todos os utilizadores, uma vez que quando activo o acesso à internet, todos os serviços estão disponíveis sem controlo.

Depois de implementada a infraestrutura, o objectivo neste capítulo é efectuar um levantamento das falhas de segurança existentes com a realização de demonstrações, com a ajuda das ferramentas apresentadas, para depois serem aplicadas correcções.

5.2.1. EQUIPAMENTOS

Neste projecto foram usados os seguintes equipamentos com as seguintes funções como poderemos verificar na figura 9:

- Um swich HP Procurve 5406 zl, como core switch da infra-estrutura,
    - Endereço IP interno – 192.168.100.253/24
- 3 Pc´s como servidores de teste localizados nas redes Interna.
    - Controlador de Domínio (dc.iseplab.local)

      – Servidor Windows 2003 Standard

      – Endereço IP interno – 192.168.100.1/24
    - Servidor de correiro e servidor *webmail* (mail.iseplab.local)
        - W2k3 standard, Exchange 2k3 standard
            - Endereço IP Interno – 192.168.100.2/24
    - Suse 11 – Será apenas default *Gateway* da Rede (suse11.iseplab.local)
            - Endereço IP Interno – 192.168.100.254/24
            - Endereço IP Externo – 10.0.28.109/24
- 1 Pc que será o utilizador que estará rede interna, da organização, com IP atribuído por DHCP, definido por endereço MAC, 192.168.100.101/24.
- 1 Portátil que será o utilizador externo ou remoto quando fora da empresa.

- Como gateway, que deveria ser o router do ISP, será feita a comunicação dos dados com o exterior (Internet), através do acesso cedido pelo ISEP com endereço IP 10.0.28.254/24.

- 1 Router / AP wireless que será o nosso equipamento de testes para os acessos wireless dos utilizadores à rede.

    - IP – 192.168.100.251/24

5.2.2. SERVIDORES E POSTOS DE TRABALHO

Os servidores foram instalados com software trial, sendo efectuados os downloads do respectivos sites, http://technet.microsoft.com/en-us/windowsserver/bb430831.aspx#EHD no caso da Microsoft e http://en.opensuse.org/OpenSUSE_11.0 no caso do OpenSuse.

1. DC.ISEPLAB.LOCAL

A nível do DC foi realizada uma instalação *standard*, e, como se pode verificar na figura 11, através da ferramenta de gestão dos utilizadores e computadores de um domínio Microsoft (active directory users e computers), foram criados os diferentes utilizadores, para que seja possível a realização das simulações. Na mesma figura pode-se validar, através da ferramenta de verificação se segurança do domínio (default domain security settings), que, não foram definidas quaisquer políticas de segurança, quer a nível de acessos, quer a nível de comunicações. A nível de especificações, está configurado como servidor de DNS, WINS, servidor de catálogo, *schema* e servidor de ficheiros onde os utilizadores têm as partilhas de rede.

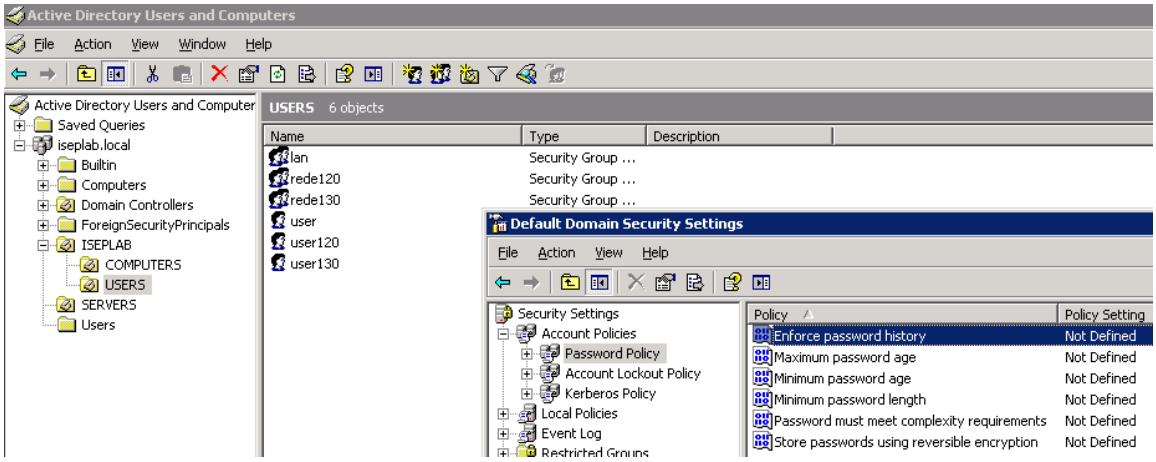


Figura 11 – (Não) Atribuição de políticas de segurança no Windows

A nível de actualizações, não se instalou qualquer tipo de software de actualizações ou correcções automáticas, assim como não se instalou qualquer software de anti-vírus, de forma a simular as vulnerabilidades da inexistência destes.

A nível de DHCP foi feita a reserva para o PC por endereço MAC como podemos verificar na figura seguinte, sendo atribuído o endereço ip 192.168.100.101. Esta configuração é ilustrada na figura 12.

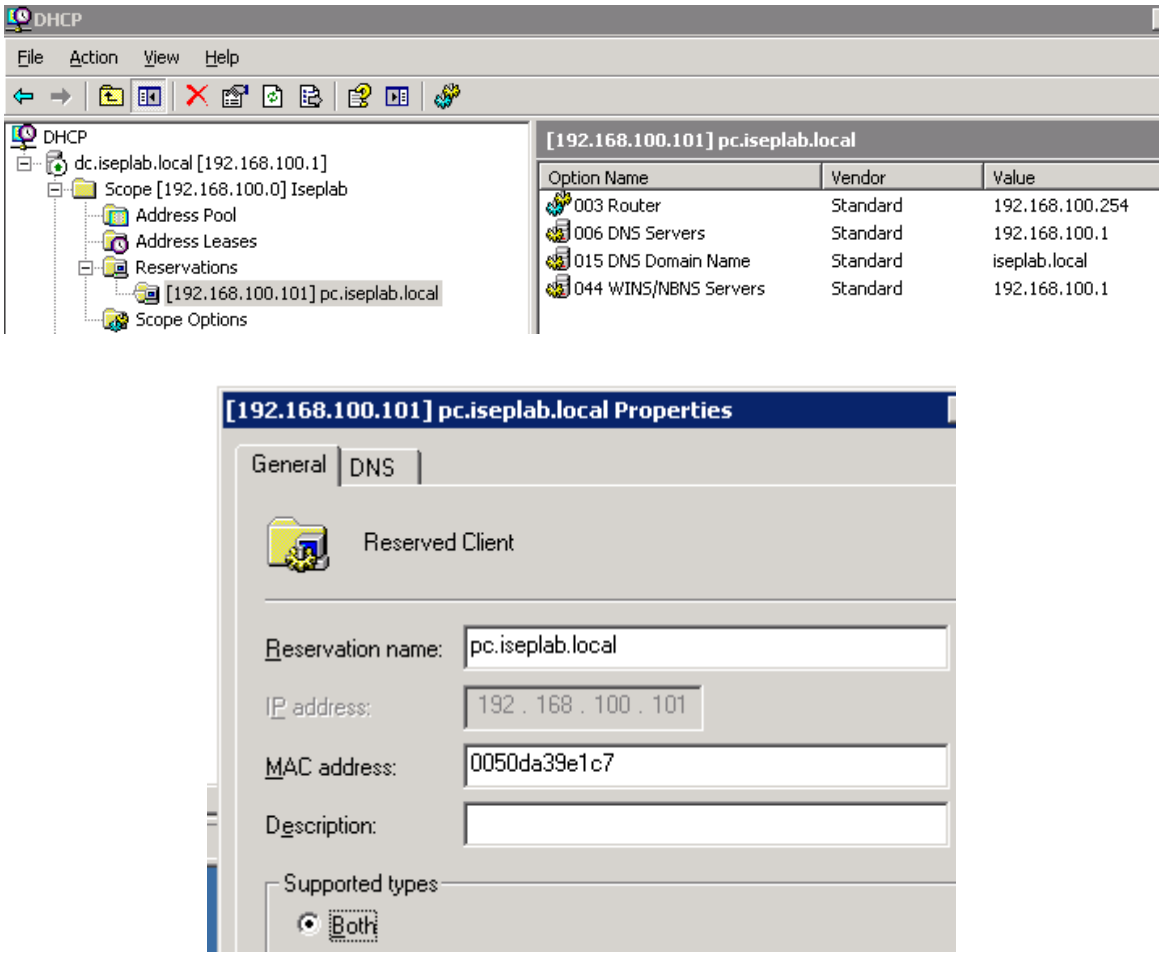


Figura 12 – Configuração do DHCP com atribuição endereços por MAC

2. MAIL.ISEPLAB.LOCAL

A nível do servidor de correio / Web, foi criada uma nova organização para o Exchange (ISEPLAB). Para obdecer aos critérios para envio / recepção de e-mail foi necessário criar dois endereços de *SMTP* como se mostra na figura 13. Destes dois endereços, o endereço @iseplab.local foi criado para que todos os utilizadores da organização possam usar o *e-mail* internamente. O endereço @caramelo.com foi criado para os utilizadores com acesso

externo ao *e-mail* conseguirem receber e-mails no domínio exigido. O protocolo SMTP é crítico uma vez que é usado como meio de envio de *spam* e vírus, de modo que deve ser configurado de forma segura.

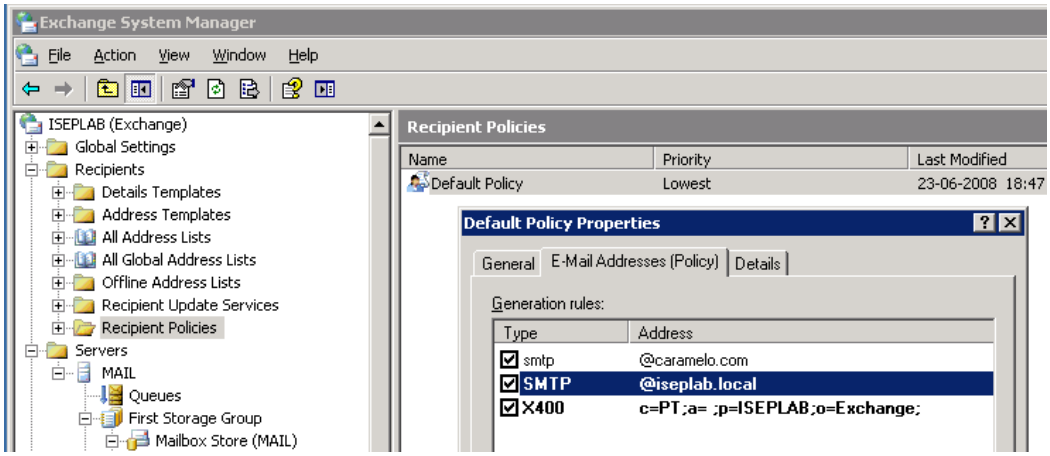


Figura 13 – Definição de política de envío de mails no Exchange

O *Exchange system manager* é o aplicativo do servidor de e-mail (Exchange) que permite efectuar as configurações de envio / recepção das mensagens para o exterior, critérios de tamanho ca caixa de correio, etc. Neste cenário, foram usadas as configurações por omissão, não sendo definido qualquer servidor para encaminhamento das mensagens (verificação de spam ou anti-virus). Isto significa que o envio de e-mails para o exterior é por DNS, não havendo qualquer limitação a nível das caixas, como limites de envio, armazenamento ou recepção.

3. SUSE11.ISEPLAB.LOCAL

O servidor Linux, que aqui funciona como router, foi configurado segundo os critérios pedidos, sendo o gateway da rede interna para a internet, reencaminhando os pedidos internos para o gateway do ISEP 10.0.28.250/24. Na figura seguinte pode-se validar a tabela de routing deste router. A rede 192.168.20.0/24 será usada como DMZ, como veremos em secções futuras.

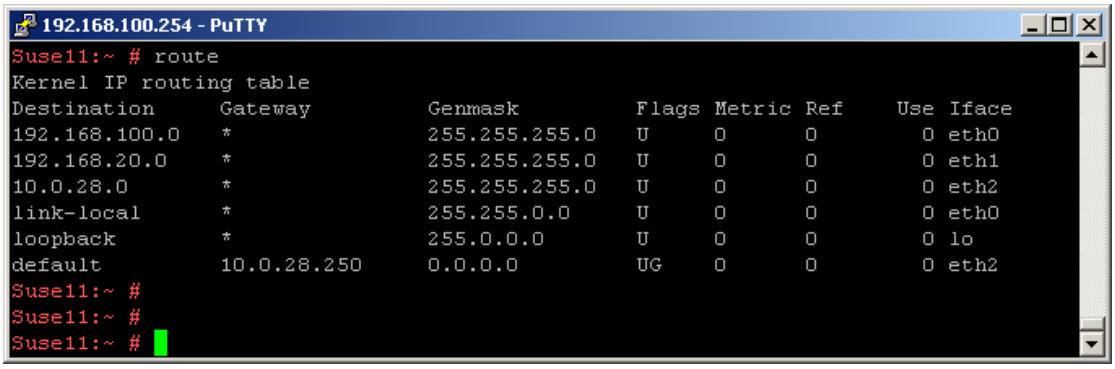


Figura 14 – Tabela de Routing das redes

A nível de resolução de nomes (hosts ou DNS), esta é realizada pelos servidores indicados pelo ISEP que fazem neste cenário de operador / ISP.

```
# vi /etc/resolv.conf
#domain iseplab.local
nameserver 192.168.100.1
nameserver 193.136.60.10
nameserver 193.136.60.2
```

4. FIREWALL de PERÍMETRO

A firewall (Shorewall) foi instalada, mas, para este cenário, está em modo aberto ou "pass through", funcionando apenas como servidor de log, para não influenciar os testes a realizar posteriormente. No entanto, não foi estruturado o processo de instalação e configuração, como a configuração das zonas da firewall e atribuição das zonas aos interfaces e consequentemente associação às redes, sendo efectuadas as configurações *standard* básicas. Como vemos a seguir (*), nas configurações do firewall, são dadas permissões para entrada de informação de todos os destinos.

```
Vi /etc/shorewall/interfaces  // Configuração dos interfaces
#############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
lan     eth0    detect
dmz     eth1    detect
wan     eth2    detect
lan     ppp+    -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE

Vi /etc/shorewall/policy
#############################################################################
#SOURCE         DEST            POLICY          LOG
#                                               LEVEL
#dmz            all             DROP            info
#lan            all             DROP            info
```

```
#wan            all             DROP            info
#all            all             DROP            info
all             all             ACCEPT          info (*)
#LAST LINE -- DO NOT REMOVE
```

Relativamente aos pedidos externos, e como este servidor funciona como router, os pedidos de *e-mail* (porta 25), *webmail* (porta 80) ou RDP (3389) têm que ser encaminhados para os servidores internos (DNAT), com os serviços associados. Neste caso o servidor mail.iseplab.local, é o destinatário dos pedidos externos. No quadro seguinte, são apresentadas as configurações (DNAT) do *shorewall* para permitir esse redirecionamento de serviços.

```
Vi /etc/shorewall/rules
#########################################################################
#ACTION  SOURCE   DEST        PROTO DEST    SOURCE       ORIGINAL
#                                          PORT    PORT(S)    DEST
## Acessos para SMTP e Webmail
DNAT     wan            lan:192.168.100.2       tcp     25      -
DNAT     wan            lan:192.168.100.2       tcp     http      -
DNAT     wan            lan:192.168.100.2       tcp     3389      -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

5. POSTOS DE TRABALHO

Neste cenário, os postos de trabalhos obtêm o IP por DHCP via endereço MAC. Como se pode verificar na figura seguinte, o IP (*IP Adress*) configurado no DHCP corresponde ao endereço MAC (*Physical Address*) do posto referido. A figura seguinte é a confirmação das configurações apresentadas na figura 12.

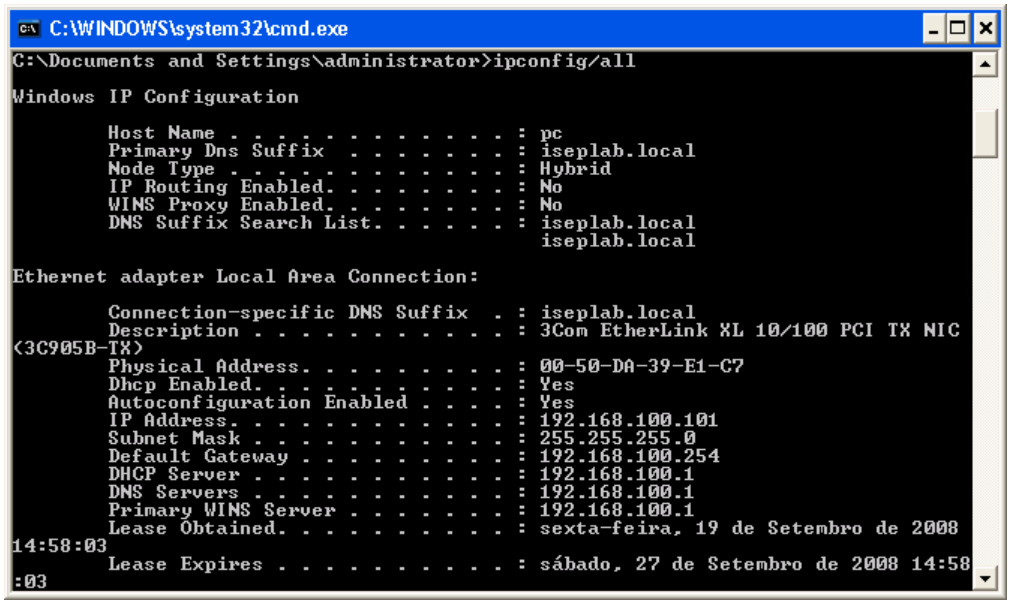


Figura 15 – Configuração da Rede Local

5.2.3. ACTIVOS DE REDE

Nesta secção serão referidos os dispositivos físicos utilizados para interligar a rede.

1. SWITCH DE REDE

O switch implementado foi um HP Procurve e, neste cenário funciona apenas como core switch da rede, sendo configurado o endereço IP 192.168.100.253 para gestão, como se pode verificar na configuração apresentada.

```
ProCurve Switch HP# show run
Running configuration:
; J8762A Configuration Editor; Created on release #H.10.38
hostname "ProCurve HP Switch "
time timezone 60
time daylight-time-rule Middle-Europe-and-Portugal
exit
ip default-gateway 192.168.100.254
sntp server 192.168.100.1
snmp-server community "isepro" Unrestricted
vlan 1
  name "rede_100"
  untagged 1-9 [1]
  ip address 192.168.100.253 255.255.255.0
  exit
spanning-tree [2]

ProCurve Switch HP#
```

[1] *Untagged* – commando que permite associar as portas referidas anteriormente a uma rede private virtual, neste caso à VLAN1.

[2] *Spanning-tree* – é um protocolo permite determiner qual o caminho mais eficiente entre cada segmento de rede, separado por *bridges* ou *switches*. Na eventualidade da ocorrência de problemas na rede, o algoritmo recalcula entre os caminhos restantes, o novo caminho mais eficiente, activando-o automaticamente.

2. PONTO DE ACESSO WIRELESS

O ponto de acesso wireless instalado usou um Dlink e foi configurado, a nível de endereços IP e gateway, com as configurações definidas nos requisitos, ficando o acesso *wireless* com WEP 64 bits (pois é o mínino possível configuravel, ficando mais vulnerável, como será demonstrado) como ilustra a figura seguinte.

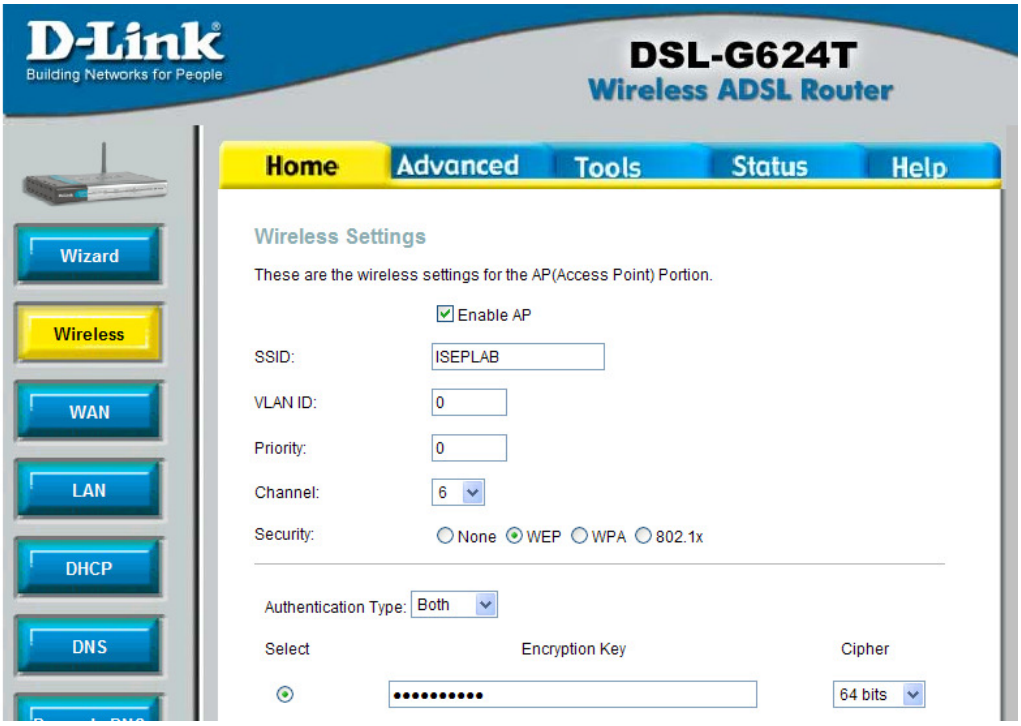


Figura 16 – Configuração Wireless do Access Point

5.3. IDENTIFICAÇÃO DE FALHAS E VULNERABILIDADES

5.3.1. INSTALAÇÃO DOS SISTEMAS

Não foi definida qualquer configuração a nível de partições. Foi usada apenas uma partição, no caso dos sistemas Microsoft e foram definidas partições específicas para logs nos casos do sistema Linux. Em caso de vírus ou corrupção de dados das partições de sistema, esta situação implica a perca de todos os dados de sistema e dados pessoais dos utilizadores.

5.3.2. RECONHECIMENTO EXTERNO

Seguidamente apresentam-se alguns exemplos de utilização de ferramentas de reconhecimento e obtenção de informação da organização. Neste cenário só se podem apresentar os exemplos, visto não ter sido possível o registo de qualquer domínio ou gama de pública de IP's. De seguida são presentadas algumas ferramentas para o efeito [8]:

- **dig** (ver http://www.madboa.com/geek/dig/):

```
dig yahoo.com A +noall +answer
dig yahoo.com MX +noall +answer
dig yahoo.com NS +noall +answer
dig yahoo.com ANY +noall +answer
dig -x 204.152.184.167 +short
```

```
dig gentoo.de +trace
dig cse.ogi.edu +nssearch
```

Este comando Unix permite questionar o servidor DNS devolvendo informação dos registos do domínio através do nome do domínio, *host*, ou endereço IP.

- **nslookup** (utilize uma máquina windows)

```
nslookup
> server 193.136.60.10
> set type=any
> dei.isep.ipp.pt
> ls –d dei.isep.ipp.pt
> exit
```

Este comando, que é comum ao Windows e Unix, assim como o comando *dig*, permite fazer a consulta dos registos de DNS de um determinado domínio, *host*, ou endereço IP.

- **nmap** (pesquisa de portas disponíveis no router)

```
nmap –PE  –v –PA21,22,23,80,3389 –sU –T4 –A 10.0.28.109
Scanning 10.0.28.109 [1000 ports]
Discovered open port 22/tcp on 10.0.28.109
Discovered open port 3389/tcp on 10.0.28.109
Discovered open port 25/tcp on 10.0.28.109
Discovered open port 80/tcp on 10.0.28.109
Discovered open port 8080/tcp on 10.0.28.109
Discovered open port 81/tcp on 10.0.28.109
Discovered open port 111/tcp on 10.0.28.109
Discovered open port 3128/tcp on 10.0.28.109
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 5.0 (protocol 2.0)
25/tcp   open  smtp          Microsoft ESMTP 6.0.3790.3959
80/tcp   open  http          Microsoft IIS webserver 6.0
81/tcp   open  http          Apache httpd 2.2.8 ((Linux/SUSE))
111/tcp  open  rpcbind
100000  2    111/udp  rpcbind
100000  2    111/tcp  rpcbind
3389/tcp open  microsoft-rdp Microsoft Terminal Service
```

O nmap é uma aplicação que consulta uma máquina em busca de portas abertas e que poderão, consequentemente, potenciar diversas vulnerabilidades.

No caso da pesquisa pelo nmap, o intruso consegue saber ao pormenor, que portas estão disponíveis para efectuar ataques, assim como as versões de sistemas operativos e tipo e versões dos sistemas utilizados para os serviços associados. Como se observa para o caso do serviço de e-mail, consegue-se verificar que o servidor é o Exchange.

5.3.3. ACESSO À REDE DE COBRE OU FIBRA

Em relação à infra-estrutura via rede de cabo de cobre ou fibra, assumiu-se que neste cenário, não é possível o acesso físico ao switch. De qualquer forma, o facto de não existir

uma conta de acesso aos equipamentos activos, é por si uma vulnerabilidade, na medida em que, remotamente, qualquer utilizador pode desligar o equipamento.

No entanto, assumindo que os endereços IP estão a ser atribuídos por endereço MAC, demonstra-se a obtenção de acesso à rede Ethernet. Para isso, o primeiro passo é detectar a gama de IP's da rede e o endereço MAC de um posto, já com endereço IP atribuído.

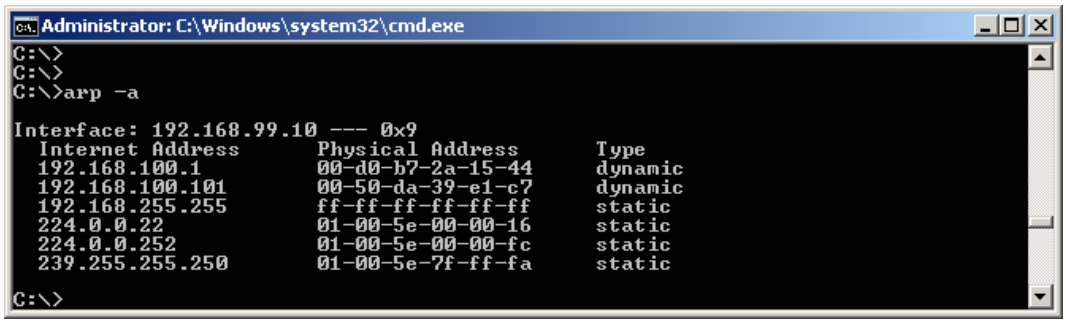


Figura 17 – Consulta de endereços IP/MAC

Numa primeira fase, como se verifica no teste da figura 17, configura-se a placa de rede com endereço 192.168.99.100/16, por exemplo, e, executando o comando "*Arp –a*" consegue-se descobrir as redes actualmente existentes e alguns endereços ip atribuídos a essa rede, como se verifica na figura seguinte.

Nesta fase, como já se sabe qual o endereço de rede, reconfigura-se o interface de rede do PC de teste com um endereço da rede que se quer obter acesso, por exemplo 192.168.100.10/24, e com o *software* "Free IP Scanner" efectua-se uma pesquisa em busca de IP's já atribuídos, com vista a obtenção dos endereços MAC dessas máquinas, como se vê na figura seguinte.

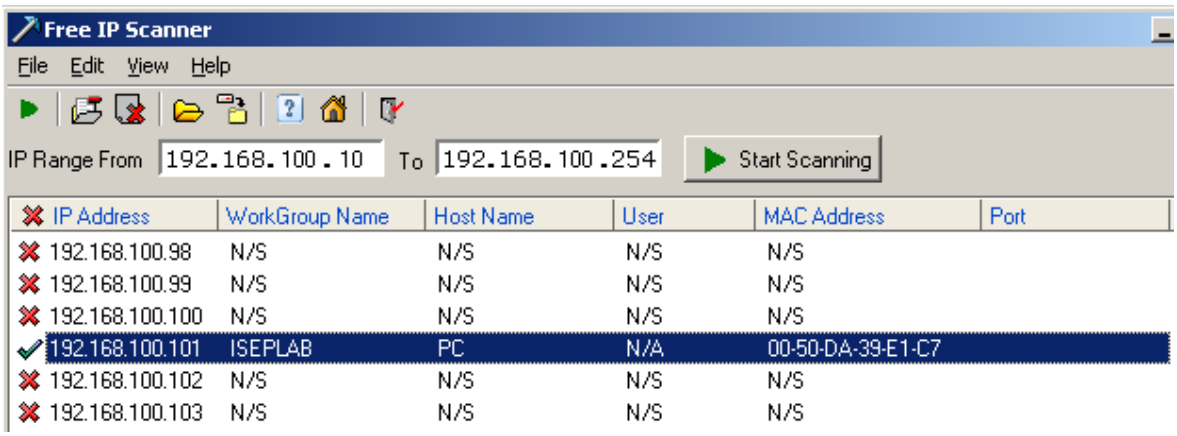


Figura 18 – Pesquisa de endereços IP já atribuídos

De seguida e com a ajuda de um emulador de endereço MAC atribui-se o endereço obtido anteriormente ao pc que se está a usar, para que seja possível obter todos os dados da infra-estrutura indicados pelo *dhcp*.

Na figura seguinte apresentam-se os dados MAC (iniciais) do PC correndo o comando ipconfig /all.

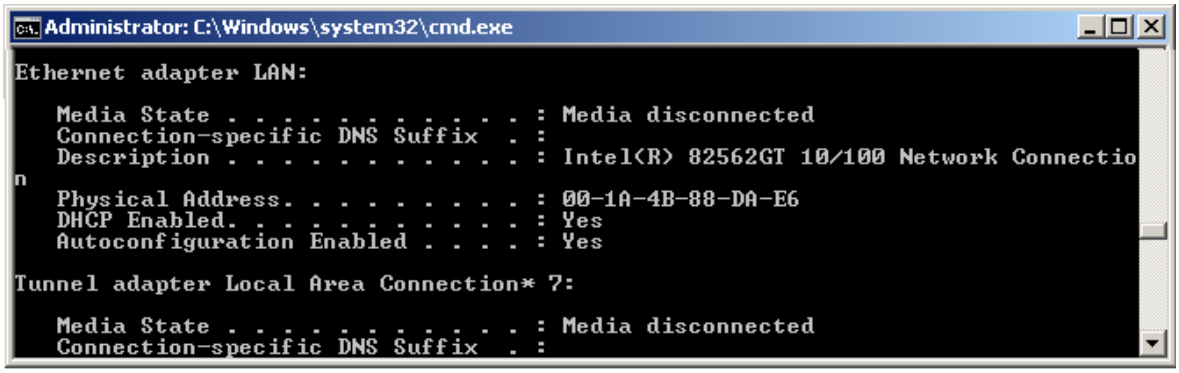


Figura 19 – Configurações da rede local

Seguidamente, usando o SMAC2.0, altera-se o endereço MAC:

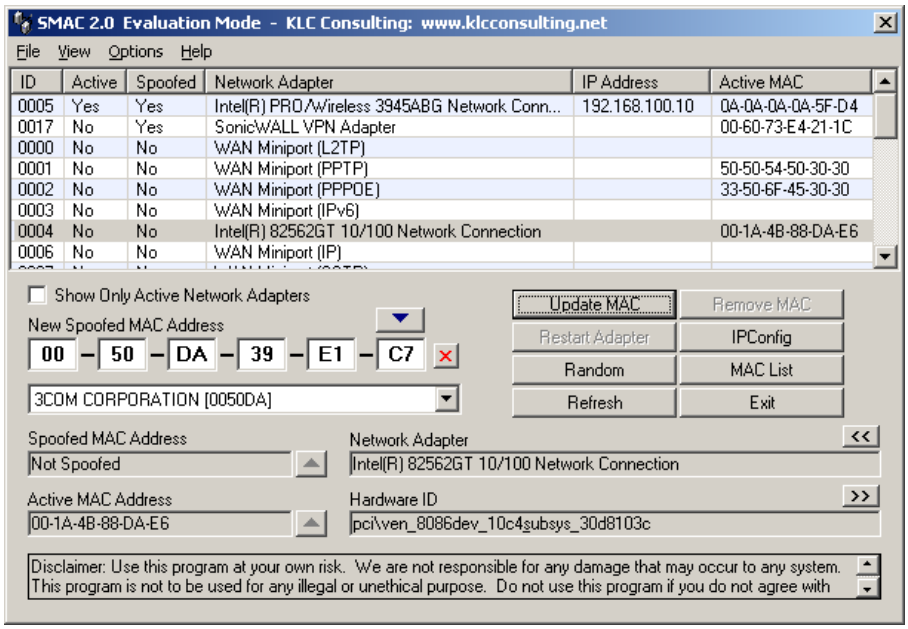


Figura 20 – Alteração do endereço MAC com o SMAC 2.0

Ao executar o comando ipconfig /all na máquina de teste, como se pode comprovar na figura seguinte, foi cedido o acesso a endereço à rede, com atribuição automática dos dados de rede, como IP, Gateway e DNS, através do servidor DNS, DHCP e WINS.

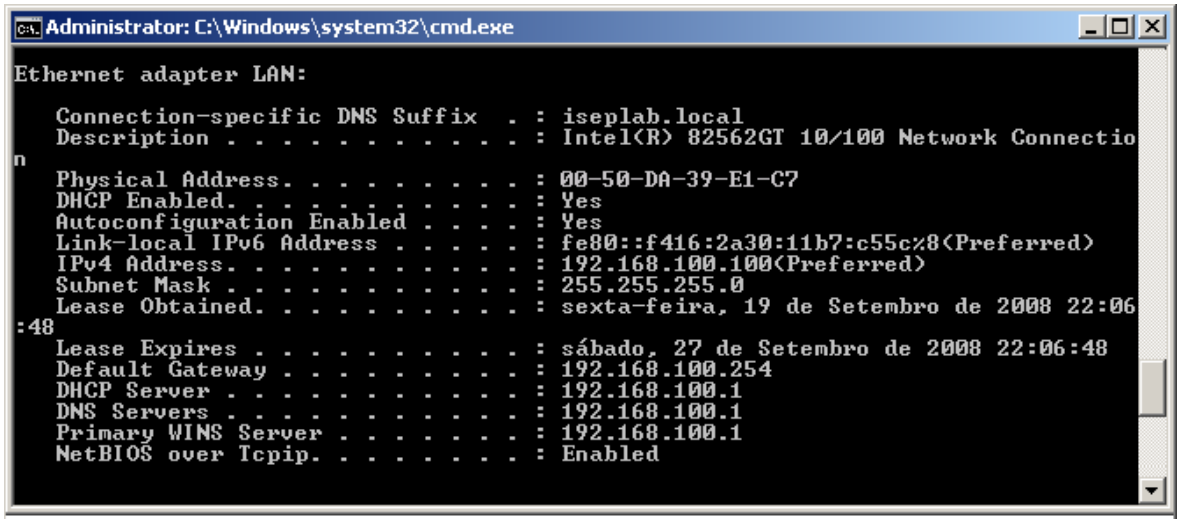


Figura 21 – Configurações da rede local

5.3.4. ACESSO À REDE WIRELESS

Devido ao elevado número de aplicações disponibilizadas através da Internet, torna-se possível demonstrar como o mecanismo de segurança a "atacar" (neste caso o WEP), é vulnerável e limitado no que respeita a uma protecção efectiva.

Para isso, serão utilizados os seguintes elementos:

- Portátil HP Compaq 6720s (com Wi-Fi Intel Pro Wireless embutido);
- Router Dlink DSLG624T com Wi-Fi;
- Aplicação OmniPeek Personal 4.1 (para efectuar a captura de tráfego);
- Aplicação WinAirCrack 2.6 (com AirCrack 2.3) (para decifrar a chave a partir do tráfego gerado).

Com estes 4 elementos, será possível mostrar como se pode decifrar a chave de uma rede WEP, através do tráfego enviado.

O primeiro passo para isto, passa por correr a aplicação OmniPeek Personal. Com esta aplicação, será possível instalar drivers compatíveis com a placa de rede sem fios (neste caso embutida no portátil), para que esta possa monitorizar o tráfego enviado de outros dispositivos.

Estando os drivers instalados, o passo seguinte passa por seleccionar o tipo de tráfego que se quer monitorizar e capturar. Como é visível na imagem seguinte, o router é identificado, pelo que se deverá seleccionar o endereço MAC do mesmo como filtro de tráfego.

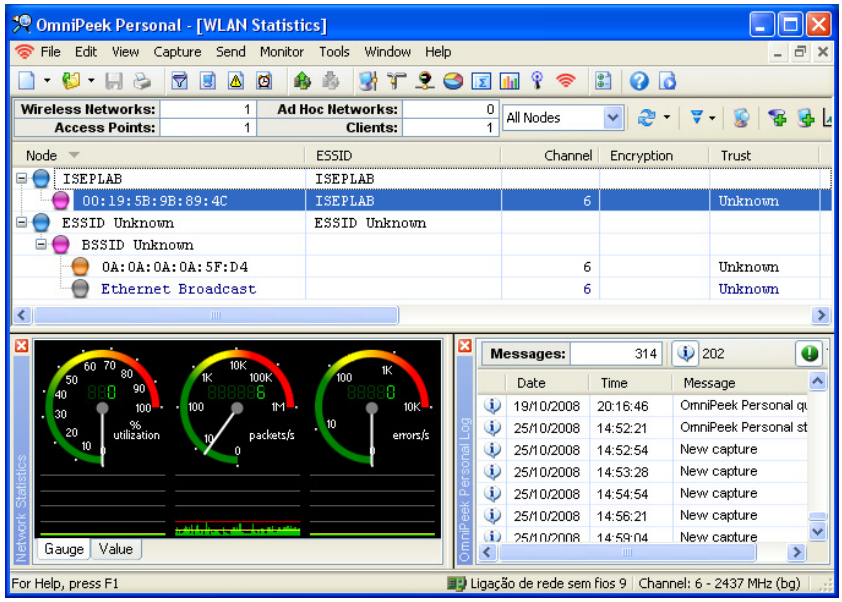


Figura 22 – Selecção do Router para filtragem de tráfego

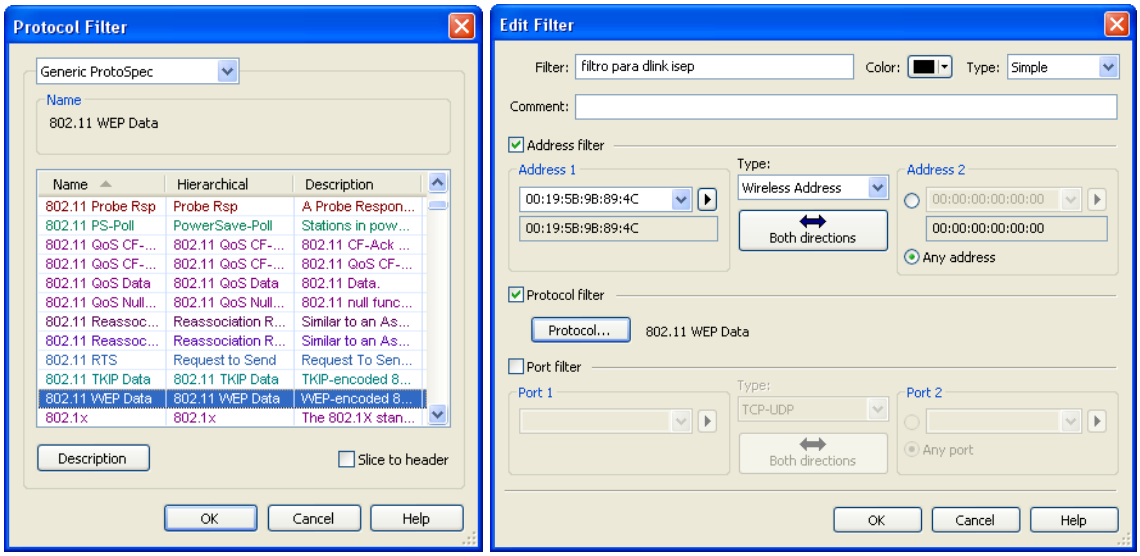


Figura 23 – Selecção do filtro, canal, e MAC, na captura do tráfego

Após a criação deste filtro, o próximo passo consiste em capturar o tráfego enviado pelo router. Inicia-se a função de captura do OmniPeek Personal, e selecciona-se o canal Wi-Fi que se pretende analisar (neste caso o 6) e inicia-se a captura.

Visto que para que seja possível realizar a decifragem, serão necessários cerca de 200.000 IV (vectores de inicialização), será necessário capturar o mesmo número de pacotes, aproximadamente (isto porque se utilizou uma chave de 64 bits apenas). [15]

Como a placa de rede Wi-Fi embutida no portátil não permite a injecção de pacotes na rede Wi-Fi que se pretende "atacar" (o que iria diminuir incrivelmente o tempo necessário para

capturar os pacotes necessários), o processo demora um período de tempo maior (na casa das horas, em vez dos minutos com equipamento que permitisse injecção de pacotes).

Desta forma, foram feitas várias capturas de tráfego para contabilizar o número de pacotes necessário, após o qual utilizamos a aplicação WinAirCrack. Esta aplicação irá recolher o tráfego analisado e a partir dele, irá verificar os IV para determinar a chave da rede.

Depois da quantidade de tráfego estar capturada, é necessário guardar esse mesmo tráfego como ficheiros .dmp, tipo usado no WinAirCrack. Assim, com a aplicação WinAirCrack aberta, selecciona-se o tipo de encriptação a decifrar como por exemplo o WEP e introduzem-se os ficheiros .dmp capturados.

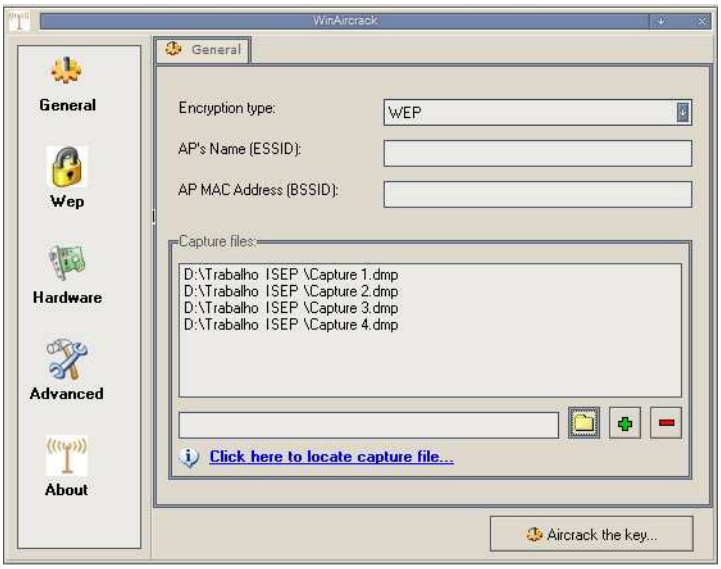


Figura 24 – Configurações gerais do WinAirCrack

Relativamente ao WEP e ao tipo de chave utilizada, escolhem-se as opções automáticas, de forma a acelerar o processo de decifragem. Seria também possível efectuar filtragem, como do endereço MAC, mas visto que o mesmo já foi efectuado no OmniPeek Personal, não é necessário utilizá-lo aqui.

Além disto, selecciona-se na parte relativa ao Hardware a placa de rede sem fios disponibilizada e indica-se o número de processadores a utilizar para processamento como 2 (o portátil tem um processador Core 2 Duo, tendo dois núcleos internos, sendo considerado pelo Windows como 2 processadores independentes).

Figura 25 – Configurações de computação do WinAirCrack

Após estas configurações no WinAirCrack, procede-se então à decifragem da chave. O WinAirCrack apresenta uma janela de comandos com as redes Wi-Fi que estavam disponíveis nos ficheiros .dmp, tendo o utilizador que escolher qual quererá analisar.

Figura 26 – Ecrã de escolha da rede Wi-Fi

Depois de escolhida a rede, o WinAirCrack irá computar o tráfego de rede, analisado os IV recolhidos e devolvendo a chave utilizada pela rede WEP. Este processo poderá demorar alguns minutos ou algumas horas, dependendo da complexidade da chave.

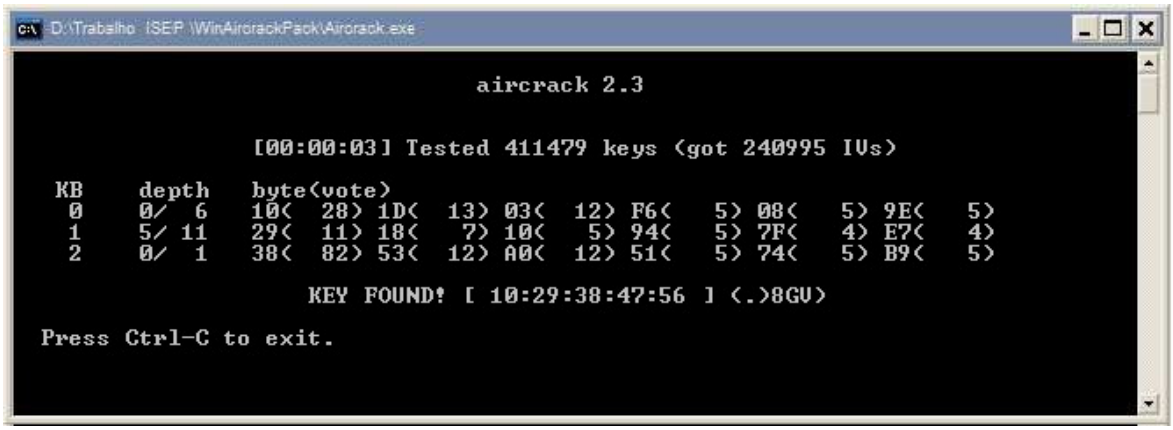


Figura 27 – Descoberta da chave de rede (WinAirCrack)

A chave recolhida poderá ser utilizada depois no acesso à rede, processo onde é normalmente requisitado essa chave. Após inserida a chave, poderá verificar-se que o acesso à rede foi efectuado com sucesso, mostrando que o mecanismo de segurança WEP é facilmente quebrável, com aplicações disponíveis na Internet e ao alcance de cada um.

5.3.5. SERVIÇOS E APLICAÇÕES

A nível de vulnerabilidades de segurança de serviços e aplicações foram verificadas as seguintes vulnerabilidades de segurança:

- Não existe qualquer firewall (o shorewall neste caso apresenta o log como passagem de todo o tráfego como é visível na figura 28),

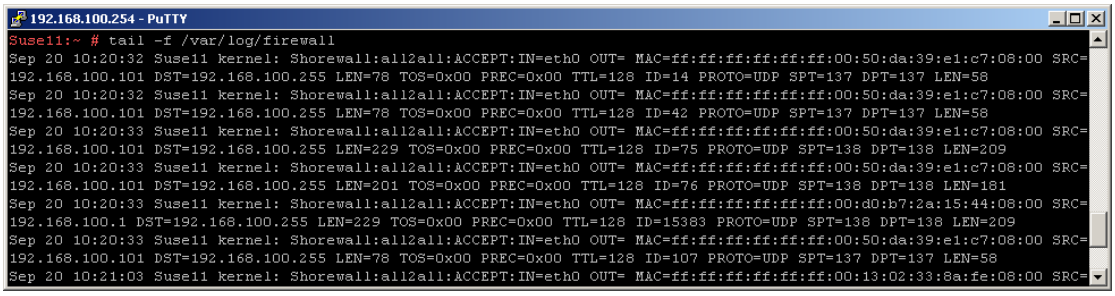


Figura 28 – Consulta dos registos de firewall

- Não existe qualquer software de gestão de actualizações e/ou correcções dos sistemas operativos, a não existência de anti-vírus, como se verifica com a ferramenta de teste MBSA, deixam os sistemas de tal forma vulneráveis, que, devido a um vírus, foi necessária a reinstalação do pc de teste, devido ao famoso "blaster" e ecrã azul, como podemos verificar nas figuras 29 e 30.

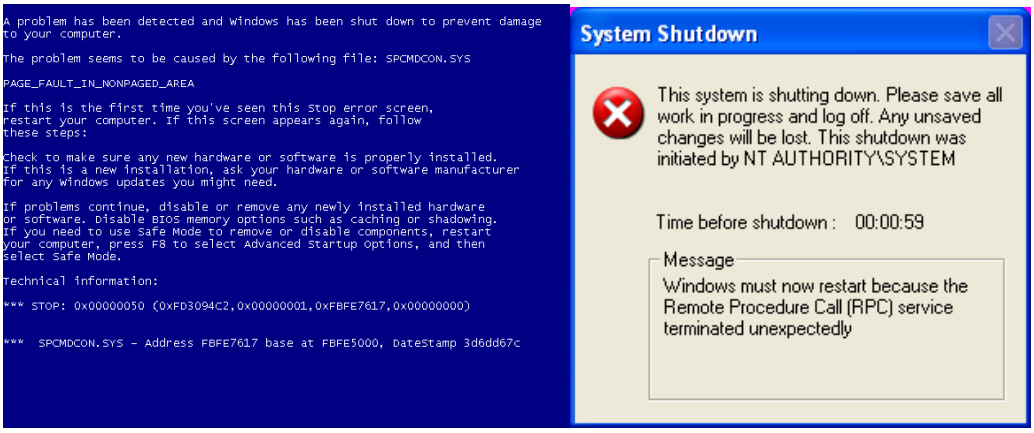


Figura 29 – Ecrãs de erro e falha não esperada

Security Update Scan Results

Score	Issue	Result
	Windows Security Updates	41 security updates are missing. 6 service packs or update rollups are missing. What was scanned Result details How to correct this

Figura 30 – MBSA para as actualizações

5.3.6. ACESSO A RECURSOS INTERNOS OU EXTERNOS

Qualquer utilizador de dentro da organização tem acesso à infra-estrutura sem controlo, sendo estes internos ou temporários à organização. A política de palavras-passe é insuficiente, podendo qualquer intruso através de técnicas como dedução ou ataque de dicionário pode facilmente obter acesso à infraestrutura. Na figura seguinte apresenta-se o ecrã de relativo às configurações de acesso à conta, a nível da criação de *passwords*.

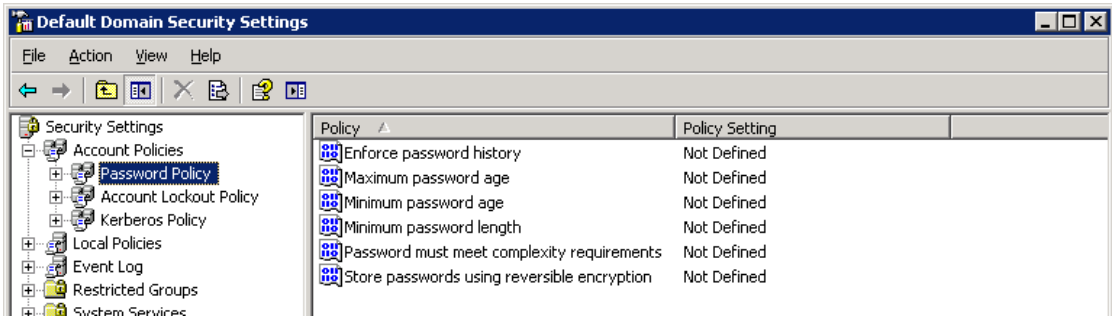


Figura 31 – Consulta de configurações de acesso

A não utilização de firewalls internas ou diferenciação de redes permitem a qualquer intruso ter acesso a qualquer sistema depois estar ligado à rede e, posteriormente, procurar o que necessita. No caso de um intruso procurar um servidor de e-mail para enviar e-mails falsos ou injuriosos, por exemplo, basta com o *nmap* procurá-lo e depois concretizar os seus objectivos como se verifica na figura seguinte.

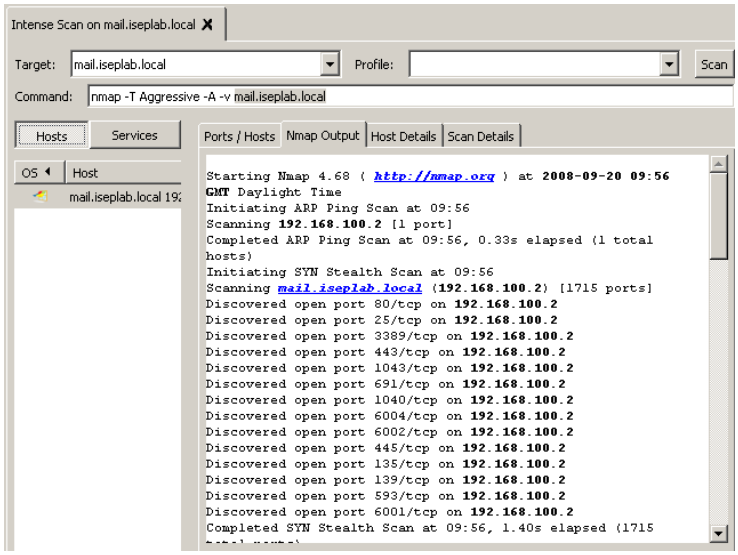


Figura 32 – Pesquisa de serviços

Serviços disponibilizados quer para o interior quer para o exterior, como o serviço de *webmail ou FTP* são inseguros uma vez que é possivel obter informação confidencial. Através de técnicas como *sniffing* de rede ou MITM é possível obter acesso a estes servidos obtendo-se por exemplo contas de acesso que posteriormente são usadas para obter acesso aos como se demonstra nas figuras seguintes usando ferramentas como o *wireshark*, conseguiu-se obter as contas de acesso ao site *FTP e Webmail*. Estes serviços devem ser colocados numa DMZ para que, caso algum intruso tenha acesso a estes sistemas não consigam acesso à rede interna.

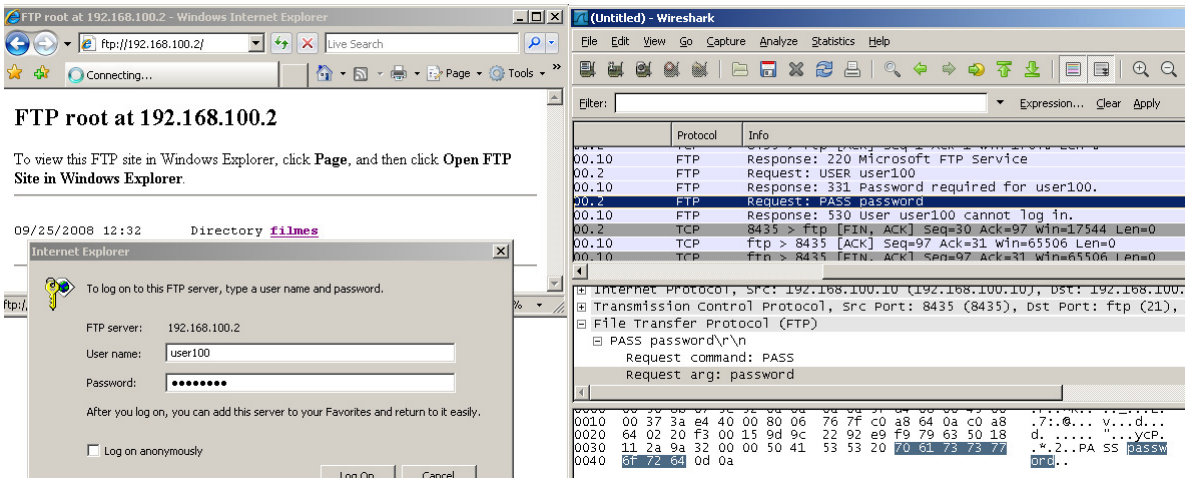


Figura 33 – Obtenção da conta de acesso FTP

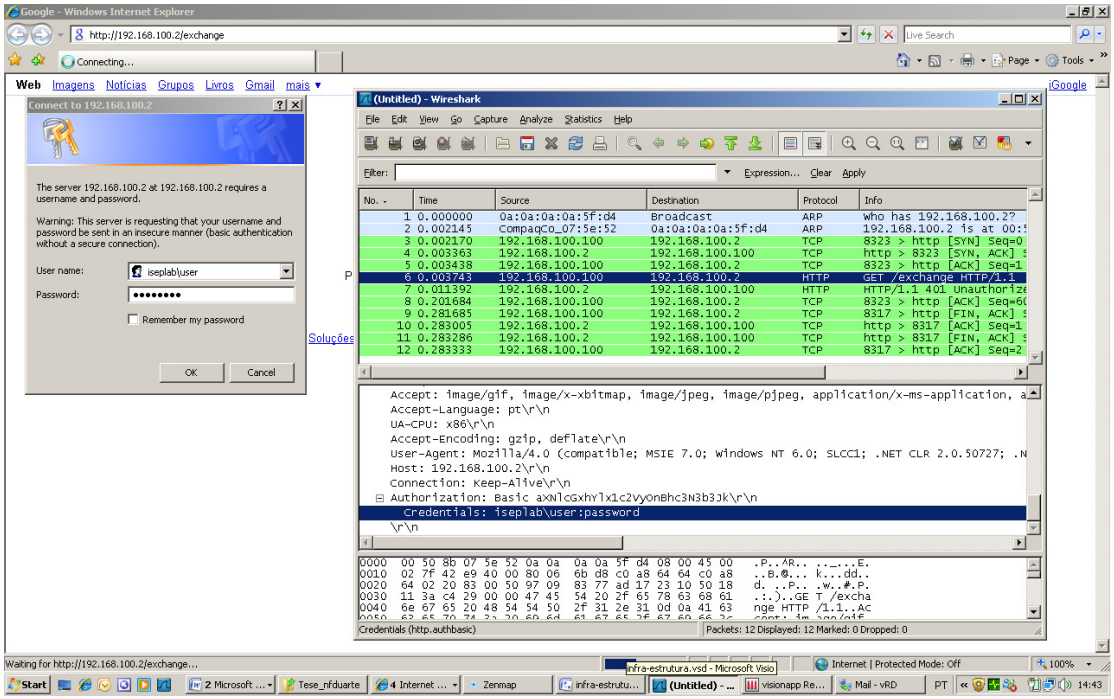


Figura 34 – Obtenção da Conta de Acesso Webmail

5.3.7. VULNERABILIDADES DO SERVIDOR DE *E-MAIL*

O facto de não existir qualquer servidor de *mail relay* com *antispam* e *anti-vírus*, como se verifica na figura seguinte, faz com que entrem cerca de 2/3 de *e-mails* indesejáveis na organização. Este facto tem por consequência um aumento significativo do espaço da base de dados do Exchange, e consequente aumento do espaço em disco que poderá levar ao bloqueio do servidor, uma vez que os utilizadores não têm limites nas suas caixas de correio. Por outro lado, como se verifica na figura seguinte, o facto do servidor de e-mail visto do exterior ser, o servidor interno, faz com que este fique mais vulnerável a ataques.

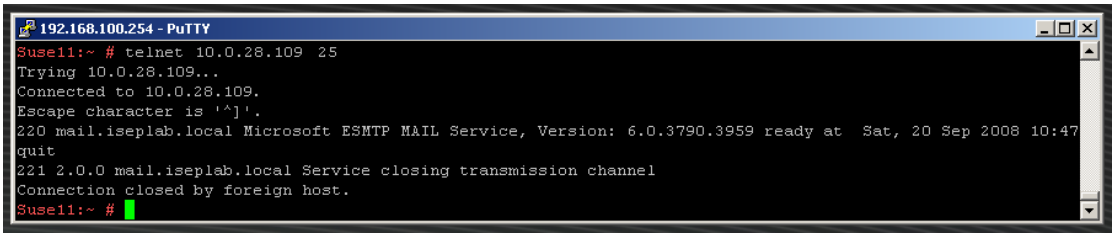


Figura 35 – Vulnerabilidade de acesso ao servidor de correio interno

Outra consequência é o despoletar de vírus, reencaminhamento de spam, ficando mais cedo ou mais tarde a organização com o endereço de *e-mail* em listas negras de endereços que enviam *spam* (como é o caso da *spamhaus*). A consequência desta situação é a impossibilidade de ser possível o envio de e-mails para outras organizações. Na figura seguinte é apresentado o teste de um endereço de e-mail que está listado, no *spamhaus*.

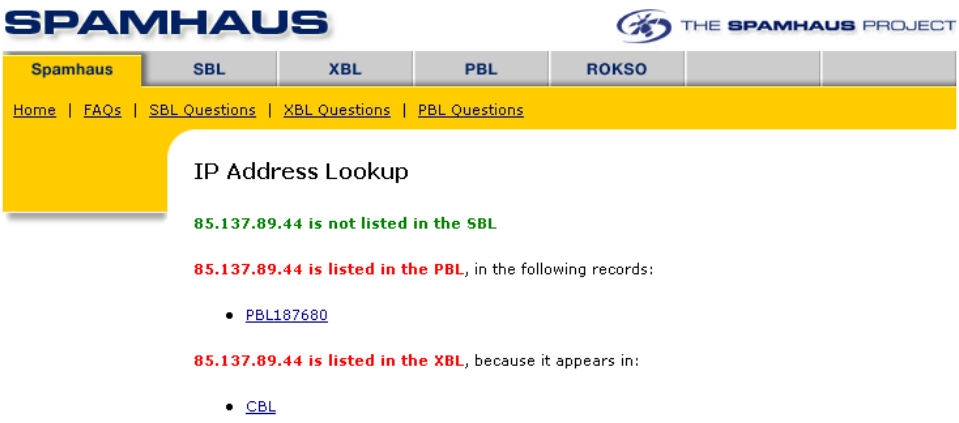


Figura 36 – Configurações do Spamhaus

De referir, também que neste caso, o facto de que, os utilizadores que não recebem e-mails do exterior, por não possuírem o endereço *smtp* externo @caramelo.com conseguem enviar e-mails para o exterior @iseplab.local. Isto deve-se ao facto de não existir qualquer controlo no envio de e-mails para o exterior.

No ficheiro log apresentado de seguida, de um servidor de *e-mail* relay, mostra-se que em apenas em 1 minuto, 4 e-mails de *spam,* foram encaminhados para os utilizadores sem serem bloqueados ou limpos. Daqui comprova-se o aumento que a base de dados do servidor de e-mail terá, e por consequência o espaço em disco do servidor, se não existir controlo a este nível.

```
Sep 20 00:56:46 suse11 postfix/smtpd[26428]: NOQUEUE: reject: RCPT from
5acea84d.bb.sky.com[90.206.168.77]: 554 Service unavailable; Client host
[90.206.168.77] blocked using bl.spamcop.net; Blocked - see
http://www.spamcop.net/bl.shtml?90.206.168.77;
from=<atsesaks1990@absolutflooring.com> to=<qualidade@caramelo.com>
proto=ESMTP helo=<5acea84d.bb.sky.com>
Sep 20 00:56:47 suse11 postfix/smtpd[26428]: NOQUEUE: reject: RCPT from
5acea84d.bb.sky.com[90.206.168.77]: 554 Service unavailable; Client host
[90.206.168.77] blocked using bl.spamcop.net; Blocked - see
http://www.spamcop.net/bl.shtml?90.206.168.77;
from=<automitr_2004@absolutflooring.com> to=<qualidadedd@caramelo.com>
proto=ESMTP helo=<5acea84d.bb.sky.com>
Sep 20 00:56:47 suse11 postfix/smtpd[26428]: NOQUEUE: reject: RCPT from
5acea84d.bb.sky.com[90.206.168.77]: 554 Service unavailable; Client host
[90.206.168.77] blocked using bl.spamcop.net; Blocked - see
http://www.spamcop.net/bl.shtml?90.206.168.77;
from=<ausenlos@absolutflooring.com> to=<qualidadek@caramelo.com>
proto=ESMTP helo=<5acea84d.bb.sky.com>
Sep 20 00:56:47 suse11 postfix/smtpd[26428]: NOQUEUE: reject: RCPT from
5acea84d.bb.sky.com[90.206.168.77]: 554 Service unavailable; Client host
[90.206.168.77] blocked using bl.spamcop.net; Blocked - see
http://www.spamcop.net/bl.shtml?90.206.168.77; from=<rejean-
ausley@absolutflooring.com> to=<qualidaded@caramelo.com> proto=ESMTP
helo=<5acea84d.bb.sky.com>
```

5.3.8. ABUSO DE RECURSOS

Os acessos à internet não são controlados, sendo possível a qualquer utilizador aceder a qualquer site da internet, seja ele fidedigno ou não, e, configurar contas de correio pessoais, (pop3) sem controlo de anti-vírus ou limitação de tráfego.

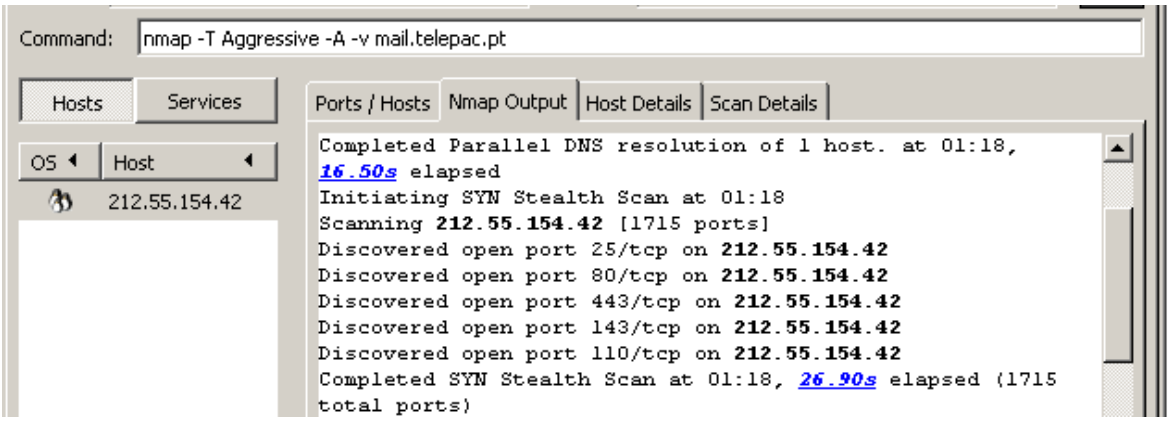


Figura 37 – Validação de abuso de recursos de utilizadores para o exterios

Por outro lado, aplicações como *eMule* ou *Kazaa* fazem com que a vulnerabilidade para *worms* seja mais elevada e a performance do acesso à internet seja de baixa qualidade. Esta situação vai-se reflectir nos acessos externos ao *e-mail e webmail*, uma vez que a linha de acesso à internet serve todos os serviços. Como se pode verificar na imagem seguinte, a não existência, de controlo, para uma linha de 512k, por exemplo, faz com que esta esteja sempre no limite da sua capacidade, para não falar no processamento que os equipamentos estão sujeitos. Nesta figura verifica-se pelo *Total rates,* tráfego total a passar no interface, que está próximo dos 500k.

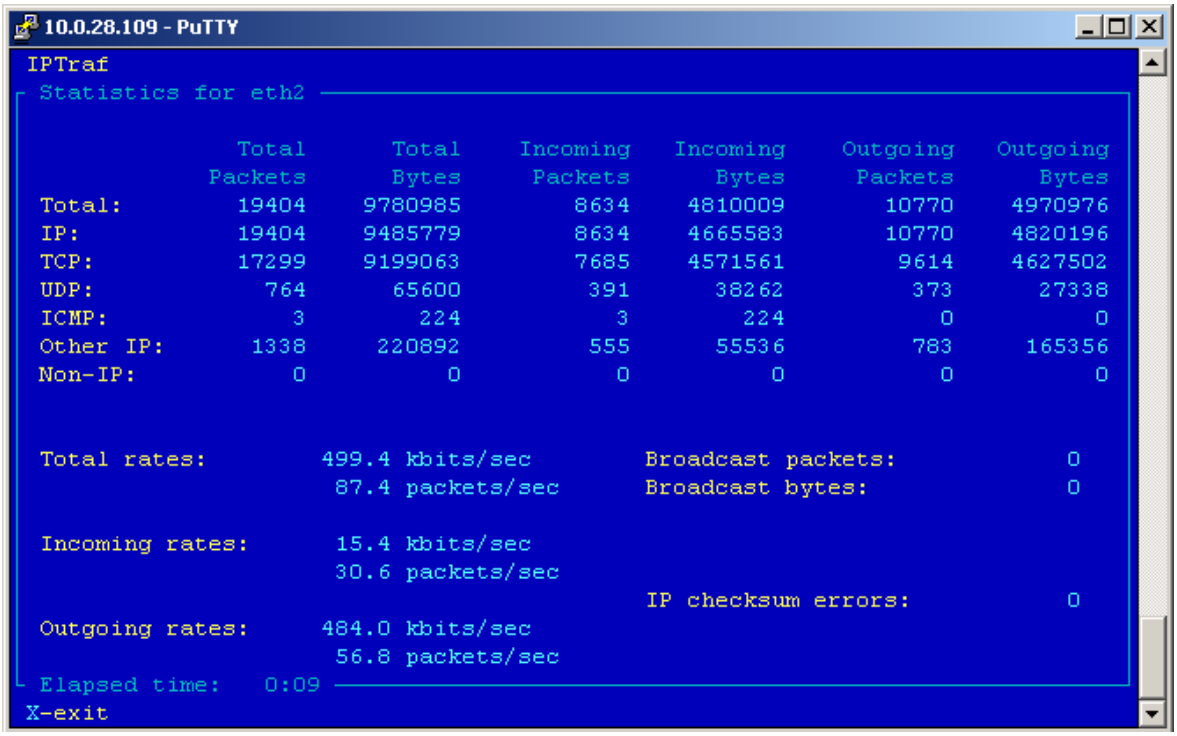


Figura 38 – Monitorização de tráfego na linha para o exterior

5.3.9. ACESSOS REMOTOS

A nível de acessos remotos ou serviços externos da organização só é possível por *webmail*, ou, directamente via *ssh* e *remote desktop* directo aos servidores vistos não existir qualquer acesso VPN. Isto é uma falha de segurança grave visto que o acesso via RDP é considerado um protocolo não seguro sendo possível a detecção das contas de acesso aos servidores. Por outro lado com uma solução de VPN, os utilizadores para além de terem segurança teriam acesso a mais recursos como acesso a ficheiros ou outros sistemas.

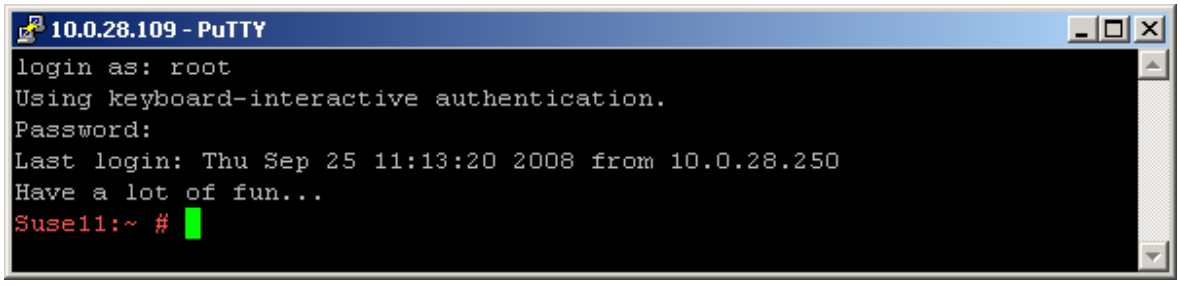


Figura 39 – Vulnerabilidade de acesso ao Suse 11 via ssh

5.4. RESUMO

Neste capítulo relativo à descrição do caso prático em estudo, foi feita uma definição pormenorizada da arquitectura da rede, e de toda a sua estrutura, nomeadamentem a nível de atribuições de endereços de rede internos e externos. Foram definidas as configurações de servidores e protocolos, como o *domain controller* e e-*mail server*, e o *WEP* no caso das redes *wi-fi*. É de salientar a enumeração dos equipamentos utilizados e referência às marcas, modelos e configurações necessárias, toda a organização da rede e estruturação a nível de cablagem, servidores, activos de rede e postos de trabalho. Configurações e realizados testes de segurança básica, são descritos neste capítulo, de modo a mostrar o mais objectivamente possível, as características e motivações deste projecto. Após os testes de vulnerabilidade, foram referidas formas de acesso à rede através da quebra de palavra-passe WEP pelo AirCrack; ataques por clonagem de endereço MAC, exploração de vulnerabilidades do sistema operativo. Para finalizar foram descritos os problemas de abuso de recursos, e-mail não endereçado (*spam*), que passam pelos servidores sem serem detectados ou terminados, e as vulnerabilidades dos acessos remotos à organização.

6. APLICAÇÃO DE SEGURANÇA À REDE DE ESTUDO

6.1. INTRODUÇÃO

O objectivo deste projecto consiste na constução de um prótotipo de uma rede, com interligação de sistemas e protocolos de sugurança, e implementação de serviços web, *webmail, firewall*, entre outros. Um dos aspectos com maior relevo é a monitorização de eventos, nos quais se poderá ter uma noção do tipo e quantidade de tráfego que circula na rede. Desta forma deve definir-se as acções necessárias para manter a segurança e melhor gerir esse tráfego. Sem suprimir a privacidade e criatividade inerentes às necessidades dos utilizadores da rede, consegue-se gerir e definir políticas para utilizadores, serviços e máquinas físicas. Este é o capítulo que mais contribui para a tese, na medida em que permite evidenciar as vulnerabilidades dos sistemas de rede, e mais importante ainda, permite definir as acções/soluções para corrigir essas mesmas vulnerabilidades.

6.2. ARQUITECTURA DA REDE

Nesta fase é mantida toda a estrutura física da rede definida no capítulo anterior, sendo apenas adicionado um novo sistema CentOS, como servidor de autenticação de utilizadores Linux, integrando modos de compatibilidade com o sistema operativo Windows. Uma vez que esta tese é de uma rede empresarial, fica salvaguardada a eventualidade de e existência de uma directoria *openldap* Linux, em detrimento do controlador de domínio Microsoft.O serviço de FTP foi colocado na DMZ, protegendo deste modo a rede interna.

O objectivo principal desta nova rede prende-se com a implementação de segurança. Conceitos como a confidencialidade, disponibilidade e integridade são requisitos obrigatórios. Um dos passos fulcrais passa pela integração dos serviços externos do sistema numa zona desmilitarizada ou DMZ, de modo a proteger a rede interna, colocando uma separação lógica entre os dois componentes, e originando numa barreira adicional de segurança. Além disto, pretende-se desabilitar todos os protocolos não seguros, e implementar soluções com segurança acrescida, como por exemplo, o http e o ftp. A interligação física de todos os equipamentos mantém-se através do switch HP e do ponto de acesso wireless como no cenário do capítulo anterior. Outras características serão também referidas neste capítulo como integração de anti-vírus e anti-spam, firewall, VPNs, entre outros.

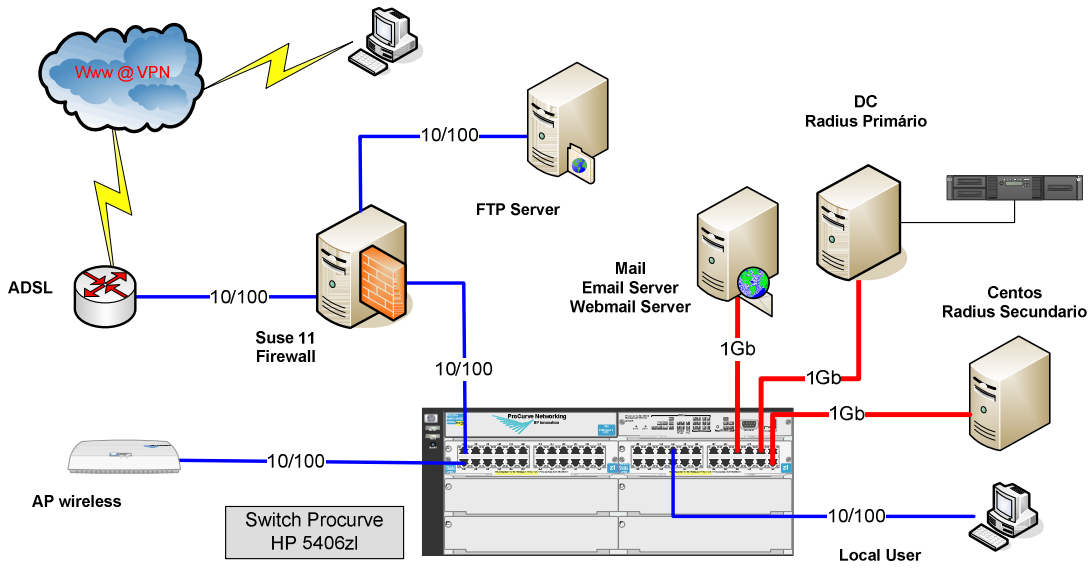


Figura 40 – Infra-estrutura física

Todos os restentes sistemas apresentados no capítulo anterior apenas foram reconfigurados e/ou adicionados ferramentas para a gestão e protecção da rede em estudo.

Desta forma pretende-se implementar uma infra-estrutura com segurança, e para isto, definiram-se, os equipamentos necessários, critérios de configurações, funções e serviços de cada um.

De forma a minimizar as vulnerabilidades do cenário do capítulo anterior, foram então definidos os sequintes critérios, de forma a que, a infraestrutura lógica, teve que ser alterada como se pode verificar na figura 41:

- Correcção das falhas na instalação dos sistemas, sendo definidas políticas de segurança, quer a nível de computadores quer a nível de utilizadores, implementação de anti-virus e sistemas de actualizações automáticos.

- Elaborar protecções contra a obtenção de informação por reconhecimento externo, acesso a serviços e aplicações, nomeadamente com a implementação de firewalls e segmentação da infra-estrutura (VLANs com ACLs).

- Garantir que só os utilizadores autorizados têm acesso à infra-estrutura da organização, sendo a atribuição de IP por *DHCP* (por endereços MAC ou não), feita depois de validados os utilizadores via *EAP / 802.1x* e sendo encaminhados automaticamente, para as respectivas *VLANs.* Esta situação terá de ser válida para rede Ethernet ou Wireless. Este ponto permite evitar que haja ataques do tipo clonagem de endereços.

- Passar todos os serviços de acesso do exterior, se possível para uma zona desmitilarizada DMZ, nomeadamente o serviço FTP.

- Proteger a organização e os sistemas contra abuso de recursos, sejam eles externos (com utilização do servidor de email para fins não fidedignos), que a nível interno (como acesso indevido da internet, e-mail e outros recursos de rede).

- Garantir o acesso remoto dos utilizadores de forma segura e controlada.

- Garantir um controlo e gestão da infra-estrutura, sendo esta o mais funcional possível para os utilizadores, de forma a causar o menor impacto possível.

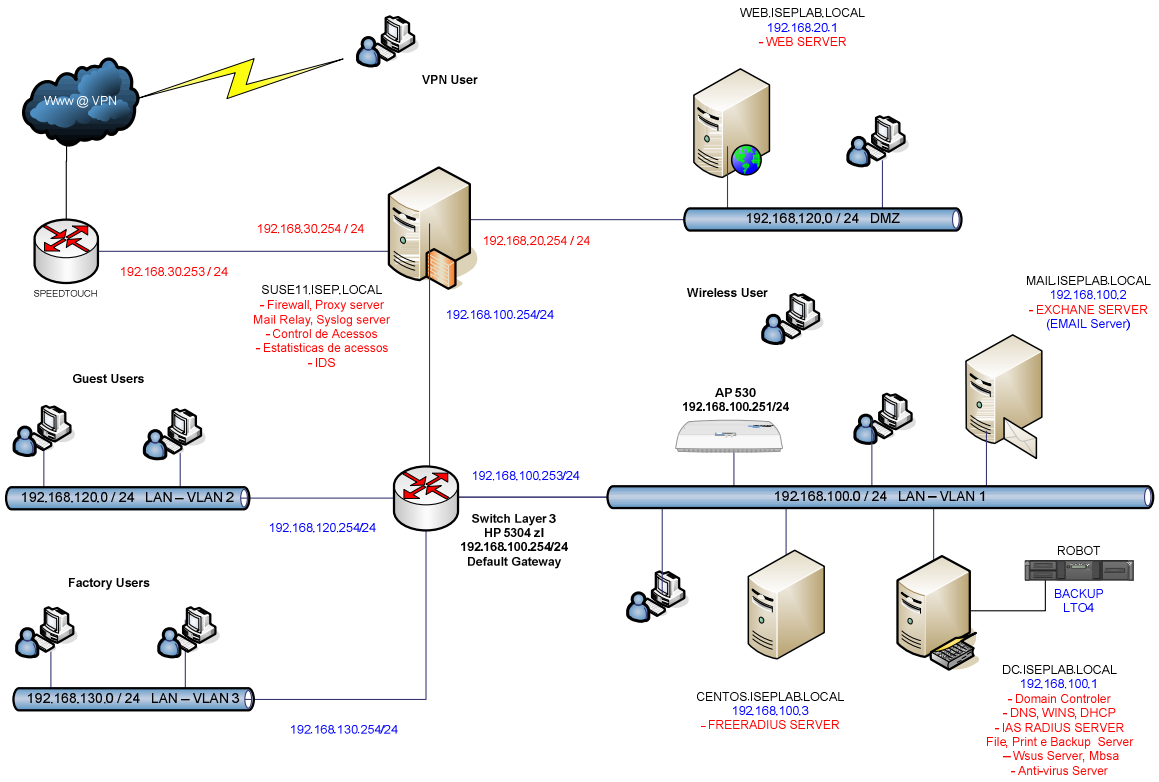


Figura 41 – Infra-estrutura lógica

Depois de implementada a infraestrutura, o objectivo neste capítulo é efectuar uma análise das soluções implementadas com a realização de demonstrações, com vista a validação destas, na remoção das falhas ou vulnerabilidades da infra-estrutura.

6.2.1. EQUIPAMENTOS

Neste projecto foram usados os seguintes equipamentos com as seguintes funções:

- Um swich HP Procurve 5406 zl, layer 3 como core switch da infra-estrutura,
    - Será o Default Gateway das Diferentes Redes
    - Autenticação 802.1x via Ethernet para os utilizadores
    - Port security para o Ponto de Acesso Wireless
    - O switch está configurado com as 3 VLAN´s
        - Rede Interna, (192.168.100.253/24 – user)

        - Rede para utilizadores convidados (192.168.120.254/24 – user120 Guest)
        - Rede do departamento financeiro (192.168.130.254/24 – user130)

- 3 Pc´s que serão os nossos servidores de teste e estarão na rede local.
    - Controlador de Domínio / servidor de Autenticação (dc.iseplab.local)
        - W2k3 Standard, Wsus, Anti-vírus, MBSA, IAS
        - Servidor de autenticação Radius Primário
        - IP – 192.168.100.1/24
    - Servidor de correio e servidor de *webmail* seguro (mail.iseplab.local)
        - W2k3 standard, Exchange 2k3 standard
        - IP – 192.168.100.2/24
    - Suse 11 – Será apenas default Gateway do switch HP Procurve
        - IP – 192.168.100.254 / 24
        - Servidor de Firewall, Proxy c/ controlo de acessos e conteúdos
        - Servidor de Log, gestão e estatísticas
    - ContOS – Será o Servidor de autenticação Radius Secundário
        - Integração com Directoria Activa da Microsoft
        - IP – 192.168.100.3 / 24
- 1 Pc que será o utilizador localizado rede interna.
- 1 Portátil que será o utilizador externo ou remoto quando fora da empresa.
- Como gateway teremos um router adsl, simulado com o acesso à internet cedido pelo ISEP.
- 1 Router / AP wireless que será o nosso equipamento de restes para os acessos wireless dos utilizadores à rede via 802.1x.

- Definição de 3 utilizadores: user, user120 e user130.
- Os utilizadores temporários, caso do "user120", só deverão ter acesso à internet
- Atribuição de IP por *DHCP* (por endereços MAC ou não) só deve ser feita depois de validados os utilizadores via *EAP / 802.1x*, sendo encaminhados automaticamente para as respectivas *VLANs.* Situação válida para rede Ethernet ou Wireless. Este ponto permite evitar que haja ataques do tipo clonagem de endereços.
- Todos utilizadores da organização têm que ter correio interno e só alguns devem ter correio externo. O "user130" deverá ter acesso apenas ao *e-mail* interno e o "user" ao e-mail interno e externo. O endereço externo é @caramelo.com.
- Todo o e-mail de entra ou sai da organização deve ser filtrado eliminando-se todo o tipo e e-mail duvidoso sujeito a provocar danos na organização.
- Os utilizadores que têm correio externo devem conseguir aceder ao correio remotamente do exterior de forma segura.

6.2.2. SERVIDORES E POSTOS DE TRABALHO

O DC acumulará a parte de autenticação como servidor de *Radius* primário para os utilizadores, computadores e equipamentos activos da rede, autenticação dos acessos à internet, servidor de anti-vírus e *software* de actualizações e correcções da infra-estrutura.

Uma das vulnerabilidades dos sistemas é a tolerância a falhas, e, com a implementação de autenticação radius, é importante a redundância dos servidores. Para isso será instalado / configurado um servidor com *CentOS* com *freeradius*, integrado com a Directoria Activa. Este, funcionará como servidor de *radius* secundário da infra-estrutura para autenticação, sendo demonstrado desta forma também, a compatibilidade e integração entre os diferentes sistemas.

O servidor Linux Suse 11, neste cenário, já terá as funções de router *Firewall*, Mail Relay c/ *antispam* e anti-vírus, *proxy* com controlo de acessos e conteúdos, servidor de *VPN* e servidor de estatísticas e monitorização.

1. DC.ISEPLAB.LOCAL

A nível do DC foram redefinidas as partições de instalação para 20 Gb para o sistema operativo e políticas de segurança, quer a nível de acessos, quer a nível de comunicações, sendo instalado o *software* de actualizações ou correcções e gestão destas (Microsoft Wsus), assim como software de anti-vírus, o Etrust CA. Todo o *software* é gerido por consola no próprio servidor.

- **Definição das Políticas de Segurança**

  - Criada uma conta Admin copiada da conta Administrator com palavra-chave – !QAZ2wsx (Esta é uma *password* segura que irá ser usada em todos os equipamentos, de modo a facilitar o desenvolvimento do sistema)

  - Desactivada a conta Administrator do Domínio

  - Definição da Política de palavra-chave para os utilizadores

Na figura seguinte é demonstrada a política de segurança de *passwords* de utilizador, aplicada aos utilizadores e computadores do domínio Microsoft nomeadamente:

- Mínimo de 6 caracteres

- Válida de 30 a 60 dias

- Encriptação de *passwords*

- Obrigatoriedade de respeitar o grau de complexidade (número e tipo de caracteres mínimo)

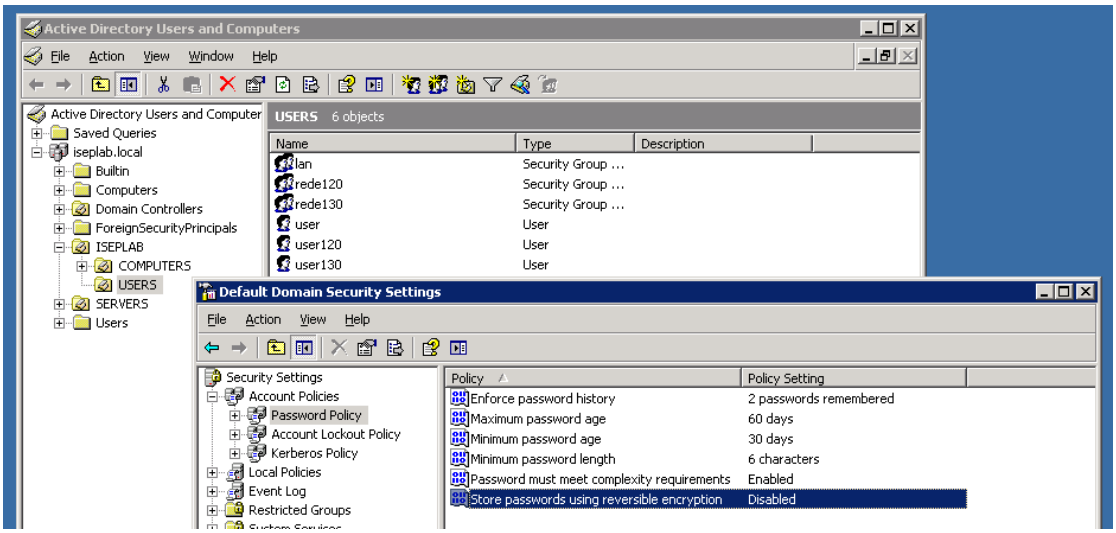


Figura 42 – Configuração de políticas de segurança (palavras-chave)

- **ANTI-VÍRUS**

Como anti-vírus da infra-estrutura foi usado o ETrust CA, sendo instalada a consola de gestão no servidor dc.iseplab.pt. A partir desta consola, consegue-se instalar e gerir o anti-vírus dos postos, gerir as actualizações, efectuar pesquisas periódicas aos postos, enviar relatórios e definir alertas (por *e-mail* por exemplo ao administrador de sistemas). Na figura seguinte é apresentada a consola central de gestão do ETrust, com a configuração da política de actualização quer do próprio servidor, quer dos postos, para validar actualizações às 14h30 da tarde.

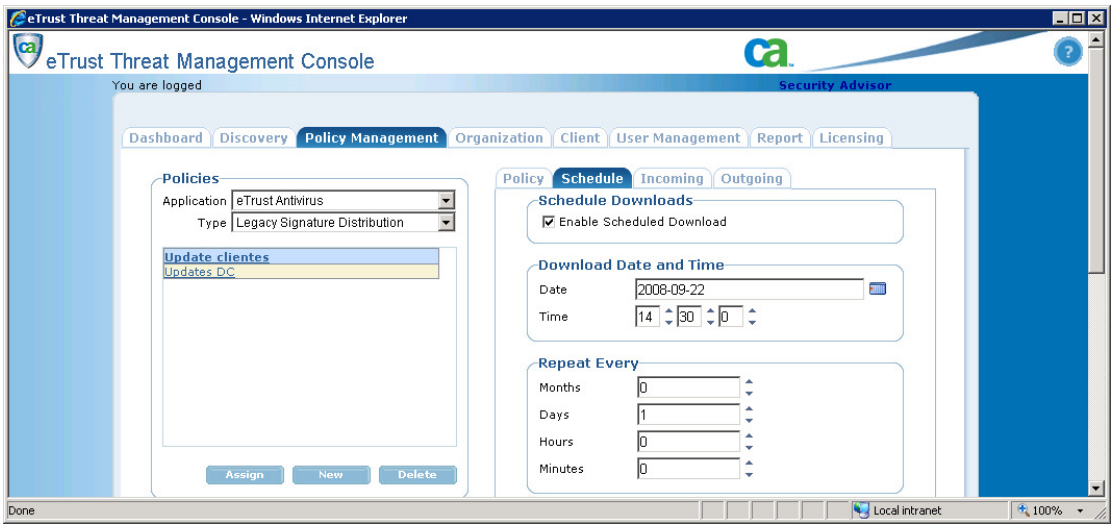


Figura 43 – Consola do Etrust

A nível de políticas de actualizações, foram definidas as actualização da internet para o servidor de gestão pelas 01h00 da manhã, diáriamente, para não influenciar o acesso à internet durante o dia laboral, e as actualizações aos postos por volta das 14h30, hora em que os utilizadores têm os PC's ligados, no início da tarde.

A instalação dos anti-vírus nos postos é simples na medida em que pode ser feita remotamente, do servidor de anti-vírus, integrado com a directoria activa da Microsoft, bastando selecionar o posto para a instalação.

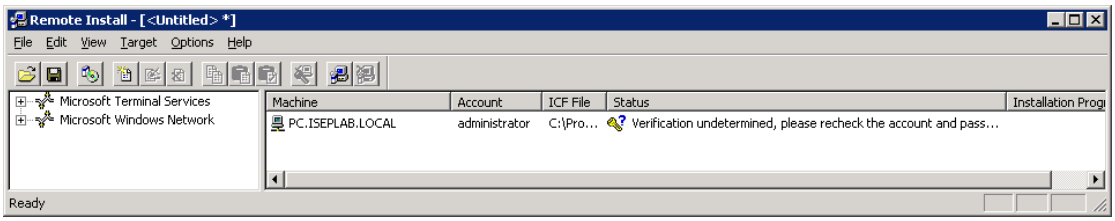


Figura 44 – Instalação remota do Anti-vírus

De referir também que caso algum posto não tenha anti-vírus instalado (em particular o Etrust) através de um script de netlogon é enviado um *e-mail* ao administrador de sistemas a informar, sendo este utilizador desligado da rede.

```
echo off
if not exist "C:\Program Files\CA\eTrust Antivirus" goto NoAntiVirus
goto fim
:NoAntiVirus
HOSTNAME > c:\TEMP.TXT
rem TYPE c:\TEMP.TXT
\\dc\NETLOGON\mailsend      -smtp      mail      -d      iseplab      -t
administrator@caramelo.com -f NoAV_detectected@iseplab.pt -c none -b none
-sub No_AV_Dectected -m c:\temp.txt
pause
rem shutdown -l
goto fim
:fim
```

- **WSUS – Windows Update Services**

O Wsus é uma aplicação de gestão e actualização de todos os sistemas Microsoft instalados (Windows, Office, entre outros).

Para instalar o Wsus foram necessários os seguintes pacotes de Software:

- Microsoft Internet Information Services (IIS) 6.0.
- Microsoft .NET Framework Version 2.0 Redistributable Package, disponivel em http://go.microsoft.com/fwlink/?LinkId=68935.
- Microsoft Management Console 3.0 for Windows Server 2003 (KB907265), disponivel em http://go.microsoft.com/fwlink/?LinkId=70412.
- Microsoft Report Viewer Redistributable 2005, disponivel em http://go.microsoft.com/fwlink/?LinkId=70410 .

Depois de efectuar a instalação dos pacotes acima descritos foi configurada uma GPO (Group Policy Object) para obrigar todos os postos da organização a efectuarem as actualizações pelo servidor de actualizações dc.iseplab.local. Nesta política define-se a que horas as actualização são aplicadas, de onde são descarregadas e se existem permissões para reiniciar os postos ou não.

Depois de se adicionar um PC ao domínio, este é deslocado para a unidade organizacional (grupo de utilizadores) da directoria activa, pois caso contrário a política não é aplicada. Na figura abaixo apresenta-se a política aplicada neste cenário.

Os servidores não devem ser considerados na política. Devem ter as actualizações definidas no painel de controlo para o modo de "Notify me but don't automatically download or install updates" (ver figura 45), uma vez que devido à sua criticidade as actualizações ou correcções devem ser feitas primeiro em servidores de teste. Este facto deve-se a que determinadas actualizações alterem o funcionamento global do sistema, podendo implicar modificações a nível do *kernel* ou núcleo do sistema, que quando incompatíveis com outras aplicações podem comprometer o bom funcionamento do servidor.

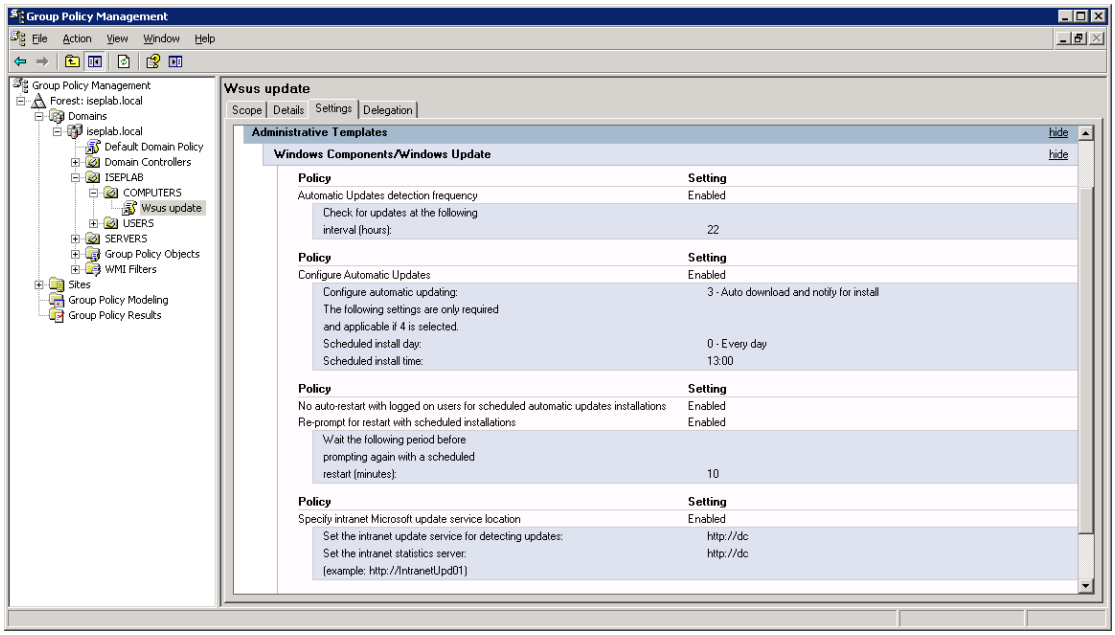


Figura 45 – Definição da Política de Actualização dos Postos

A nível de configuração do WSUS, deve-se configurar o *Proxy Server,* com o endereço do servidor para acesso à internet, quais os productos da Microsoft a actualizar automaticamente e definir uma hora de sicronização do servidor. Este faz com que o *download* das actualizações só se faça, diariamente (durante a noite para o servidor de Wsus), apenas uma vez da internet, para descongestionamento de recursos.

Como polílica associada a nível de Wsus, (Figura 46) foi configurado um grupo de computadores onde adicionamos todos os PC's da rede, ou aqueles que se entenda que devem efectuar as actualizações automaticamente. Desta forma, como todos os PC's ficam associados à GPO, é possível colocar alguns em *standy by*, visto que algumas aplicações existentes são incompatíveis com as actualizações, e assim sendo, é preferível efectuar as actualizações manualmente ou num momento posterior.

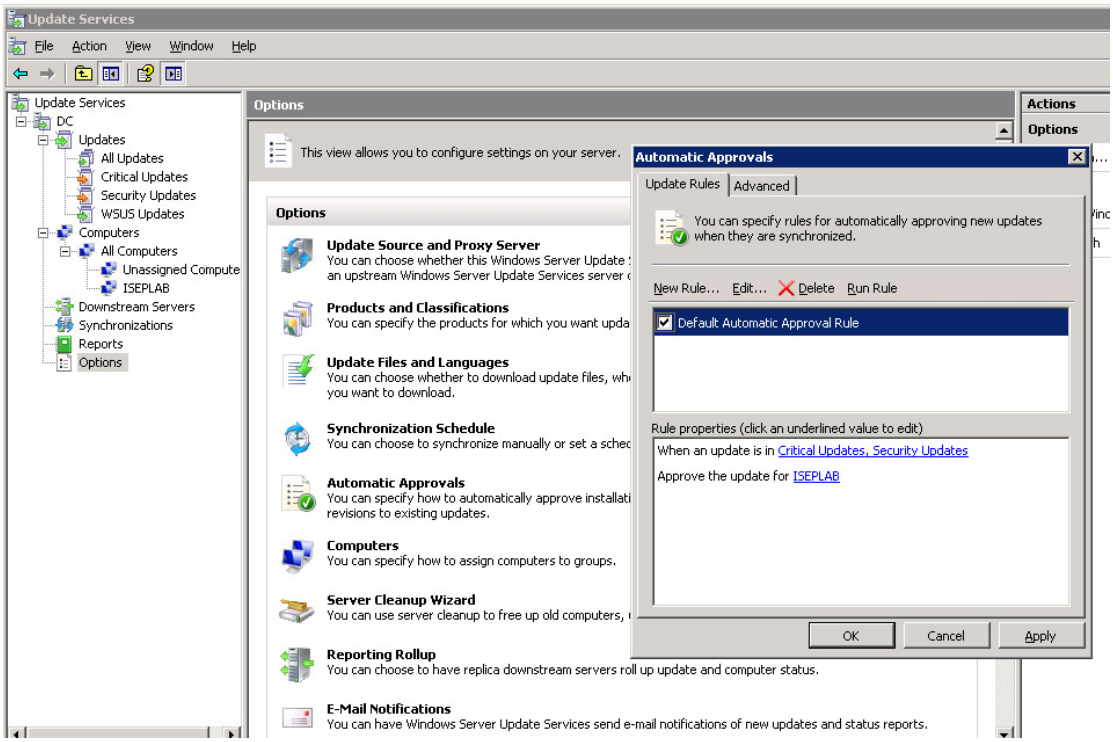


Figura 46 – Windows Update Services

- **DHCP**

A nível de DHCP foram adicionados os grupos de endereços para as novas VLAN´s (possibilitando a atribuição automática de endereços IP para as novas redes segmentadas) como se pode verificar na figura seguinte. Desta forma, de cada vez que os utilizadores de cada VLAN acederem à rede, é lhes atribuído um endereço IP via DHCP, da VLAN correspondente, automaticamente. Esta funcionalidade, para funcionar sem problemas, é complementada com o "ip helper" do switch de rede, que será abordada nos activos de rede.

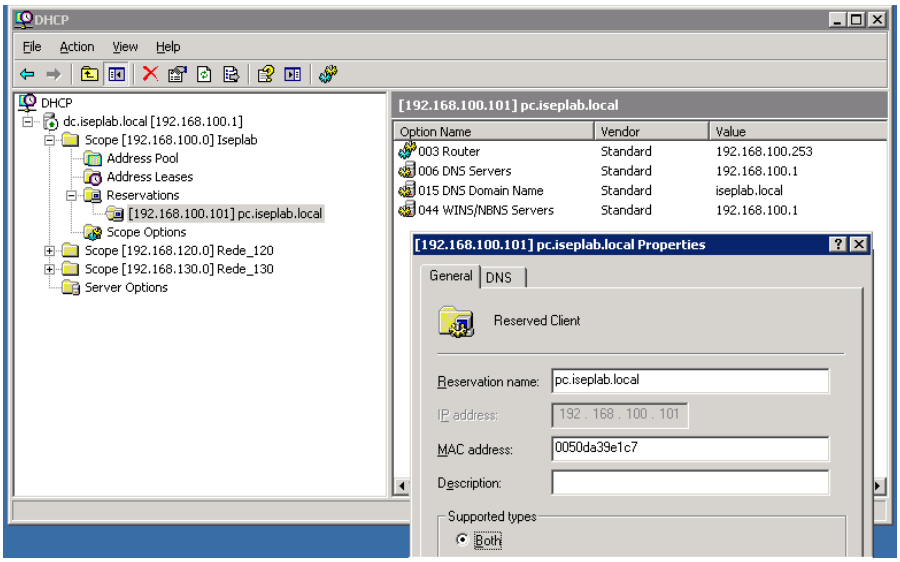


Figura 47 – Configuração DHCP para múltiplas Vlan´s

- **CERTIFICATION AUTHORITY**

O Certification authority permite, com a ajuda do *IIS selfssl*, gerar o certificado digital de acesso para o IIS, quer do acesso ao webmail quer para a autenticação 802.1x.

Para isto, do servidor controlador de domínio invoca-se os selfssl e cria-se 2 certificados, um para o dc.iseplab.local e outro para o mail.iseplab.local, com validade de 5 anos.

```
selfssl /n:cn=mail.iseplab.local /v:1325
selfssl /n:cn=dc.iseplab.local /v:1325
```

Depois de gerados os certificados é só adiciona-los ao IIS de cada servidor e configurar os serviços para se usar ssl.

- **IAS – Internet Autentication Service**

A nível de serviços, foi adicionado aos já existentes, o IAS (Internet Autentication Service), componente integrada no Windows 2003 *server*. Depois de instalado, no IAS têm que se definir os equipamentos que vão ter autorização para validação, neste caso o Switch HP e o AP Dlink, e definir a palavra-chave de *Radius* que é !QAZ2wsx.

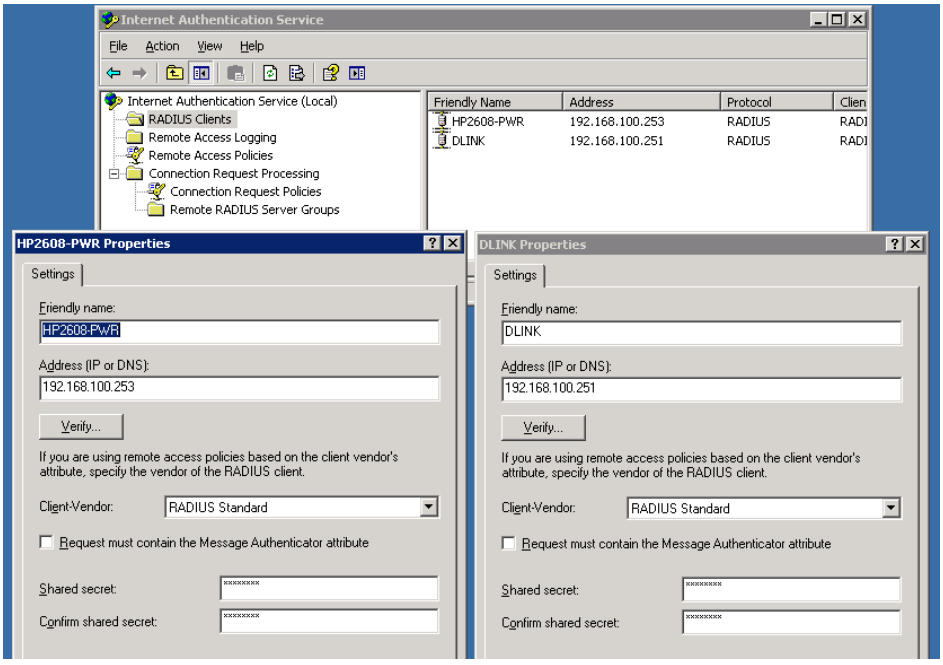


Figura 48 – Configuração Radius dos Clientes switch e AP

As imagens acima, correspondem à configuração do switch e do access point, ambos definidos com *password* segura *Radius*, e com os IPs 192.168.100.253 (switch) e 192.168.100.251 (access point).

De seguida, é necessário configurar as políticas de atribuição automática de VLAN's, baseadas nos grupos da directoria activa definidos anteriormente. Na figura abaixo é visível o grupo associado à política Rede 120 por exemplo, em que é definido que os utilizadores da Rede 120, podem ligar-se à rede por Ethernet ou Wireless, sendo-lhes atribuída automaticamente a VLAN 2, com o endereço IP desta.

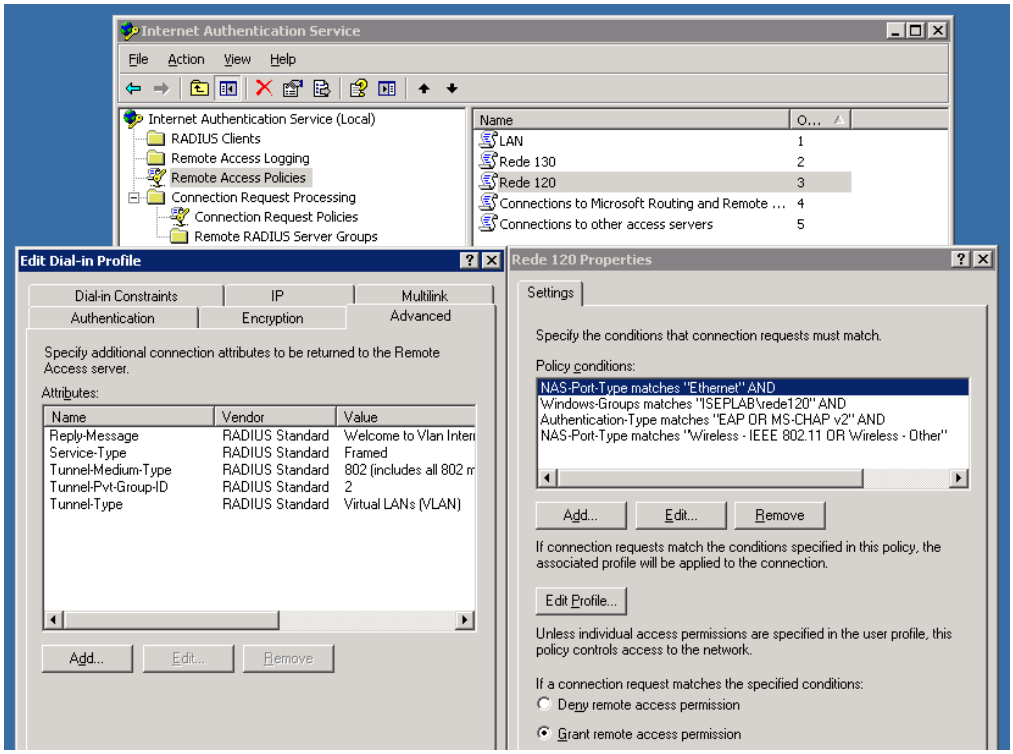


Figura 49 – Configuração da autenyicação Radius para os utilizadores

Nesta figura podemos verificar do lado direito, em "Privacy conditions", como a Rede 120 está configurada para aceitar pedidos por porta *Wireless* e *Ethernet*, bem como o protocolo de autenticação (EAP ou MS-CHAP v2). No lado direito é apresentado no "dial up" a atribuição automática da vlan, que neste case é a 2, para a rede 120.

2. SUSE11.ISEPLAB.LOCAL

No que diz respeito ao servidor Suse Linux, foram mantidas todas as configurações de rede apenas sendo feita uma alteração a nível do /etc/resolv.conf, uma vez que vamos ter interligação à directoria activa da Microsoft.

```
Vi /etc/hosts
192.168.100.254 suse11.iseplab.local suse11
192.168.100.1   dc.iseplab.local dc
192.168.100.2   mail.iseplab.local mail
192.168.100.3   centos.iseplab.local contos
```

```
192.168.20.254  dmz.iseplab.local dmz
10.0.28.109     wan.iseplab.local wan
```

```
vi /etc/resolv.conf
#domain iseplab.local
nameserver 192.168.100.1
nameserver 193.136.60.10
nameserver 193.136.60.2
```

- **Políticas de segurança**

Em seguida foram definidas palavras-passe segundo os requisitos sugeridos na secção 3.3.1, ficando a política de segurança defnida seguinte forma:

- Criada uma conta de utilizador "Admin" com palavra-chave !QAZ2wsx
- Foi definida a palavra-chave de root (*Super User*) para !QAZ2wsx
- Foi desactivado o acesso SSHv2 à conta root sendo necessário correr o comando "su", para ter privilégios *root,* como ve verifica na figura 50.

```
vi /etc/ssh/sshd_config
#LoginGraceTime 2m
#PermitRootLogin yes
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 3
```

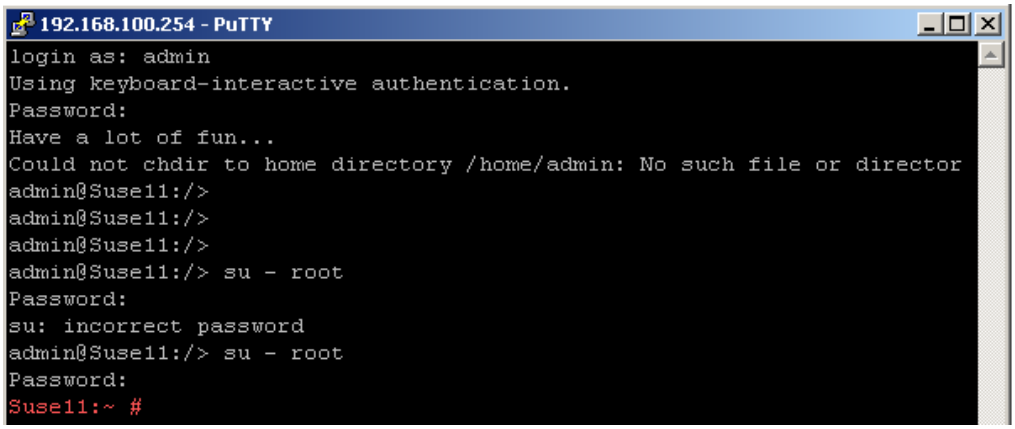


Figura 50 – Configuração do administrador com palavra-chave segurança

- **Firewall de perímetro**

Para este cenário, a firewall (Shorewall) foi reconfigurada para permitir apenas a passagem dos protocolos essenciais para acesso quer do exterior quer do interior da firewall. As alterações mais significativas à parametrização do cenário anterior foram as seguintes (extracto do Anexo 1):

```
Vi /etc/shorewall/interfaces
#ZONE INTERFACE   BROADCAST   OPTIONS
lan     eth0    detect
dmz     eth1    detect
wan     eth2    detect
vpn     tun0    detect
vpn     tun1    detect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE

Vi /etc/shorewall/masq
#INTERFACE              SOURCE          ADDRESS          PROTO   PORT(S)
IPSEC   MARK
eth2    eth0
eth2    eth1
tun0  tun1
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE

Vi /etc/shorewall/policy
#SOURCE        DEST          POLICY         LOG LEVEL   LIMIT:BURST
lan            vpn            ACCEPT           info
vpn            lan            ACCEPT           info
fw             vpn            ACCEPT           info
vpn             fw            ACCEPT           info
dmz            all             DROP            info
lan            all             DROP            info
wan            all             DROP            info     10/sec:20
all            all             DROP            info
#all           all             ACCEPT          info
#LAST LINE -- DO NOT REMOVE
```

Os pedidos externos de *e-mail* (porta 25) são encaminhados para o *Postfix Mail Relay* enquanto que o *webmail* (neste cenário já porta 443) é encaminhado directamente para o servidor interno, que neste caso é o mail.iseplab.local. De referir que a *firewall* já está definida para o acesso VPN da OPENVPN. Outra referência é a protecção contra ataques DoS com a definição do "`LIMIT:BURST`" para 10/sec:20

```
Vi /etc/shorewall/rules
#ACTION  SOURCE   DEST        PROTO DEST    SOURCE       ORIGINAL
#                                          PORT    PORT(S)    DEST
## Acessos para SMTP e Webmail
ACCEPT     wan            fw                       tcp     53      -
ACCEPT     wan            fw                       tcp     25      -
ACCEPT     wan            fw                       tcp     http,https    -
DNAT       wan            lan:192.168.100.2        tcp     443     -
## Acessos para o OPENVPN
ACCEPT      net           fw      udp     1194
ACCEPT      fw            net     udp     1194
ACCEPT      net           fw      udp     1196
ACCEPT      fw            net     udp     1196
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

- **Samba / winbind**

Para ser possivel a integração dos sistemas Linux com a directoria activa da Microsoft, foi necessário a instalação dos pacotes *samba / winbind,* respectivamente *samba-client-3.2.0-22.1, samba-winbind-3.2.0-22.1.* Esta integração é necessária, para que seja possivel, a autenticação por utilizador a nível do proxy squid, e a nível de autenticação do servidor *freeradius*, na directoria activa do domínio Microsoft. Os ficheiros smb.conf e krb5.conf, são os responsáveis por establecer a ponte entre o sistema Linux e o sistema Miceosoft. Esta configuração está preparada para o Linux Suse11, mas para o CentOs, basta alterar em "Realms" o nome do servidor.

De seguida são apresentadas as configurações dos serviços *samba/winbind* e *kerberos*, necessários à validação em Linux, de utilizadores do domínio Microsoft. Podemos encontrar configurações a nível do domínio, gama de endereços IP, *logs* e portas.

Configuração do Samba e Kerberos (NTLM_AUTH)

/etc/samba/smb.conf

```
[global]
workgroup = iseplab
netbios name = iseplab
realm = iseplab.local
security = ads
encrypt passwords = yes
password server = 192.168.100.1
wins server = 192.168.100.1
load printers = no
winbind separator = /
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes
template homedir = /dev/null
template shell = /dev/bash
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
preferred master = false
local master = no
domain master = false
dns proxy = no
```

Configuração do Kerberos

/etc/krb5.conf

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
```

```
[libdefaults]
 default_realm = ISEPLAB.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 ISEPLAB.LOCAL = {
  kdc = suse11.iseplab.local:88
  admin_server = suse11.iseplab.local:749
  default_domain = iseplab.local
 }

[domain_realm]
 .iseplab.local = ISEPLAB.LOCAL
 iseplab.local = ISEPLAB.LOCAL

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

- **Proxy c/ autenticação por utilizador**

Para configurar o proxy com autenticação foi instalado o pacote associado, squid-*2.6.STABLE20-12*. Esta autenticação poderá ter duas vertentes: por LDAP e por NTLM. Nesta última, é necessário o pacote adicional *samba-winbind-3.2.0-22.1*.

Cada um destes dois tipos de autenticação baseia-se na validação da existência de utilizadores, que deverão estar associados a um grupo da directoria activa do domínio Microsoft, chamado "utilizadores Internet". Neste caso, se o utilizador pertencer ao grupo, é-lhe concedido o acesso. Caso contrário, ser-lhe-á vedado o acesso à Internet.

No caso da autenticação LDAP, é feita apenas através de parametrizações definidas no ficheiro squid.conf, funcionando como uma pergunta à directoria activa, sempre que algum utilizador tentar aceder à internet. No entanto, na óptica do utilizador, sempre que seja aberta uma janela do *browser*, é-lhe exigida a colocação do *username* e *password*.

- No caso da autenticação LDAP a parametrização do /etc/squid/squid.conf é a seguinte:

```
http_port 3128
```

```
dns_nameservers 192.168.100.1 193.136.60.10 193.136.60.2

auth_param basic program /usr/sbin/squid_ldap_auth -b
"dc=iseplab,dc=local" -h 192.168.100.1 -p 3268 -D
"cn=squidiseplab,ou=Users,dc=iseplab,dc=local" -w "isepsquid" -f
(&(sAMAccountName=%s)(objectClass=Person))

auth_param basic children 5
auth_param basic realm do ISEP
auth_param basic credentialsttl 2 hours

external_acl_type gruposquid %LOGIN /usr/sbin/squid_ldap_group -h
192.168.100.1 -p 3268 -b "dc=iseplab,dc=local" -f "(&(cn=%g)(member=%u))"
-F "sAMAccountName=%s" -D "cn=squidisep" -w "isepsquid" -d 1

acl squid-user-ad proxy_auth REQUIRED
acl squid-grupo-ad external gruposquid internet

#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl hp src 192.168.100.103/255.255.255.255
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
acl our_networks src 192.168.100.0/24
acl our_networks2 src 192.168.120.0/24
acl our_networks4 src 192.168.130.0/24
http_access allow java_jvm
http_access allow updates
http_access allow password
http_access allow our_networks
http_access allow our_networks2
http_access allow our_networks4
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow rede_vouga
http_access allow localhost
http_access deny all
```

Se optar-se pela autenticação NTLM, esta requere a configuração do *samba/winbind* e *kerberos*, mas o acesso à Internet, na óptica do utilizador, é transparente. Isto significa que a validação do acesso à Internet é feita quando o utilizador faz *login* no domínio, ou seja, não é necessário colocar o *login* sempre que é aberta uma janela nova do *browser*. Daqui a

necesssidade no ponto anterior de ser necessário a instalação / configuração dos pacotes *samba / winbind*.

- No caso da autenticação NTLM a configuração do squid.conf é a seguinte:

```
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-
ntlmssp --require-membership-of=iseplab+internet
auth_param ntlm children 30
auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-
basic --require-membership-of=iseplab+internet
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
acl password proxy_auth REQUIRED
```

- **Controlo de conteúdos de acesso à Internet**

O *Dansguardian* é uma aplicação que permite a gestão de conteúdos *Web*. Isto significa que poderão ser limitados os acessos a sites, domínios e outras localizações Web, através do bloqueio baseado em conteúdos dos próprios sites. Exemplos são "sex", "fcporto" etc. Depois de instalado o pacote *dansguardian-2.9.9.5-5.2*, é necessário adaptar a gestão das portas de acesso do proxy (squid) a nível de configuração, através do ficheiro /etc/dansguardian/dansguardian.conf da seguinte forma:

```
# the port that DansGuardian listens to.
filterport = 8080
# the ip of the proxy (default is the loopback - i.e. this server)
proxyip = 127.0.0.1
# the port DansGuardian connects to proxy on
proxyport = 3128
```

Relativamente à gestão de conteúdos, isso pode ser feito através dos ficheiros existentes no directório /etc/dansguardian/lists/ onde, apesar de já existirem bloqueios ou autorizações por omissão, estas podem ser alteradas. Estes ficheiros estão apresentados no Anexo 3.

- **Controlo de acesso à Internet**

O controlo de acesso à Internet feito pelos utilizadores autorizados, é validado com o SARG. Esta ferramenta permite saber quais os sites acedidos por determinado utilizador, a que horas e quanto tempo e que largura de banda utilizou. O pacote a instalar é o *sarg-2.2.5-19*, no servidor Suse Linux 11. Depois de configurar o servidor Web como se vai ver no próximo item, os dados dos acessos podem ser consultados via Web em "Lista de

websites consultador por utilizador".

A nível de configuração apenas temos que alterar o seguinte em vi /etc/sarg/sarg.conf:

```
access_log /var/log/squid/access.log
output_dir /srv/www/htdocs/squid-reports/sarg/
resolve_ip yes
date_format e
```

Os relatórios são actualizados segundo scripts que actualizam as estatísticas, diariamente, semanalmente e mensalmente, como se pode verificar no crontab abaixo, descrito no Anexo 2.

```
# SARG REPORTS
00 00 * * *             /usr/sbin/sarg-reports daily >/dev/null 2>&1
00 01 * * 1             /usr/sbin/sarg-reports weekly >/dev/null 2>&1
30 02 1 * *             /usr/sbin/sarg-reports monthly >/dev/null 2>&1
```

- **Serviço Web APACHE**

De forma a obter e gerar as estatísticas de acesso e controlo de utilizadores, usou-se um servidor Web [22], com uma intranet. Este servidor pode ser consultado de qualquer local da rede interna, ou só de algumas máquinas previamente selecionadas, se for o caso. Os pacotes instalados foram o *apache2-2.2.8-28.1*, servidor web e o *apache2-mod_php5-5.2.5-66.1* para o suporte das estatísticas do servidor de relay de *e-mail*, entre outros. Como se vai verificar na parametrização, o servidor Web trabalha sobre a porta 81, e com controlo de acesso, devendo-se ao facto de estar menos sujeito a ataques internos. A página principal pode ser visualizada por qualquer pessoa mas para aceder a qualquer um dos itens tem que efectuar um *login* por utilizador e palavra-passe.

```
vi /etc/apache2/listen.conf
Listen 81

vi /etc/apache2/httpd.conf
<Files "sarg">
AuthUserFile "/var/wwwpasswd/.htpasswd"
AuthName "Area Restrita -"
AuthType Basic
require valid-user
</Files>
```

Com vista a uma gestão centralizada das estatísticas foi desenvolvido o interface Web para emglobar todas as restantes ferramentas de estatísticas, Como verificar na figura seguinte.

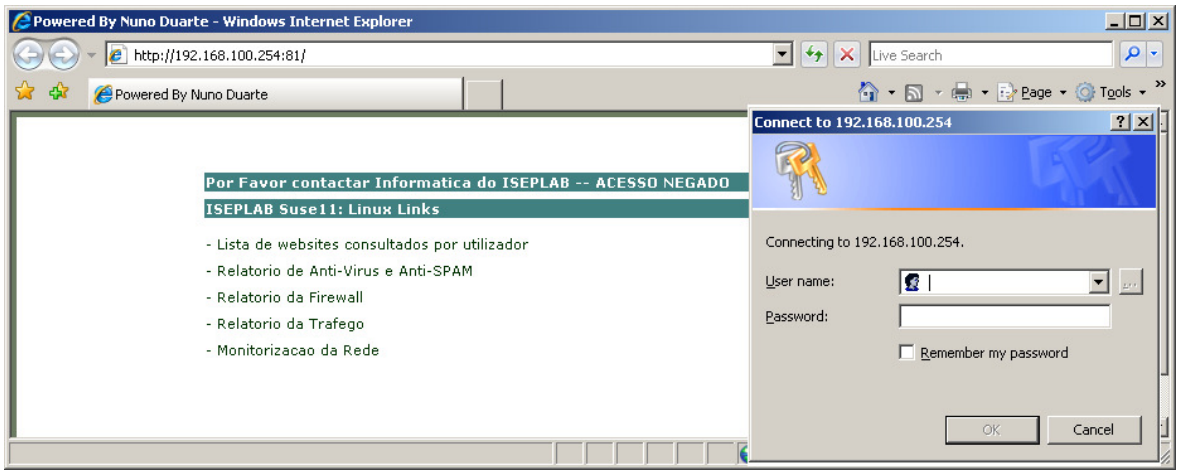


Figura 51 – Interface Web para Acesso Ferramentas de gestão

- **Mail relay com anti-spam e anti-vírus**

Para implementar a protecção de envio e recepção de *e-mail*, foi implementada uma solução híbrida com 4 sistemas que se integram entre si: *postfix, amavis, spamassassin e clamd*. Posteriormente, será associado o amavis-stats, pacote que vai permitir gerar as estatísticas que vão apresentar a relação e-mail, vírus, spam, entre outros.

Os pacotes necessários a esta protecção foram:

```
postfix-2.5.1-28.1
spamassassin-3.2.4-29.1
clamav-0.93-19.1
amavisd-new-2.5.1-102.1
amavis-stats-0.1.13-1
```

1) **Postfix**

No ficheiro main.cf definem-se as políticas de autorização, como quais os domínios autorizados a efectuar relay, (neste caso são o iseplab.local e caramelo.com), requisitos para a recepção de *e-mail, (helo required)* quais as listas de spam a consultar sempre que se recebe *e-mail, (spamcop e spamhaus)* etc. Como domínio de relay autorizado (`relay_domains`) está definido apenas o caramelo.com para que os utilizadores que é requisito não terem *e-mail* externo não conseguirem enviar ou receber e-mail do exterior. Apenas por curiosidade, o facto de este servidor responder a pedidos smtp em nome de um relay *Lotus Notes*, já por si é uma medida de segurança na medida em que pode desviar os ataques para vulnerabilidades de um sistema que não é o real.

```
vi /etc/postfix/main.cf
smtpd_banner = Relay ESMTP Lotus Notes
myhostname = suse11.iseplab.local
mydomain = iseplab.local
mydestination=$myhostname,$myhostname.$mydomain,.caramelo.com
relay_domains = $mydestination, hash:/etc/postfix/transport
smtpd_sender_restrictions =
        hash:/etc/postfix/access,
        permit_mynetworks,
        reject_non_fqdn_sender,
        reject_unknown_sender_domain,
        permit
smtpd_helo_required = yes
smtpd_recipient_restrictions =
        permit_mynetworks,
        reject_unauth_pipelining,
        reject_non_fqdn_recipient,
        reject_unknown_recipient_domain,
        reject_unauth_destination,
        reject_rbl_client bl.spamcop.net,
        reject_rbl_client zen.spamhaus.org,
        permit
message_size_limit = 10240000
content_filter = smtp-amavis:[127.0.0.1]:10024
```

Neste ficheiro define-se o transporte para os domínios autorizados, isto é, para que servidores se enviam os e-mails com determinado domínio. Neste caso todos os e-mails para o domínio caramelo.com são encaminhados para o Servidor de Exchange interno. Como o domínio iseplab.local está comentado, este servidor apenas recebe e-mails para o domínio caramelo.com.

```
vi /etc/postfix/transport
# Domain            TRANSPORT(5)
caramelo.com     smtp:[192.168.100.2]
#iseplab.local   smtp:[192.168.100.2]
```

2) Amavis / Clamav

Após configuração, quando o servidor smtp (postfix) receber um *e-mail,* envia-o para o sistema de filtragem (amavisd-new) que invoca os diversos filtros e altera os cabeçalhos conforme os resultados e devolve o e-mail ao servidor *smtp*. Isto é configurado no postfix no ficheiro *main.cf.*

```
message_size_limit = 10240000
content_filter = smtp-amavis:[127.0.0.1]:10024
```

Em seguida é necessário parametrizar o domínio que vai passar pelo relay (caramelo.com vai ser autorizado a passar pelo servidor), os endereços para o envio dos alertas e relatórios (spamdb@caramelo.com) e qual o anti-vírus se vai utilizar, que neste caso é o clamav como se pode visualizar no ficheiro seguinte.

```
Vi /etc/amavis.conf
# a convenient default for other settings
$mydomain = 'caramelo.com';
# Endereco de e-mail para enviar o spam
$spam_quarantine_to = "spamdb\@$mydomain";
# Endereco de e-mail para enviar o spam
$bad_header_quarantine_to = "spamdb\@$mydomain";
# ### http://www.clamav.net/
 ['ClamAV-clamd',
   \&ask_daemon, ["CONTSCAN {}\n", "127.0.0.1:3310"],
   qr/\bOK$/, qr/\bFOUND$/,
   qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

3) Spamassassin

A configuração consiste em activar o filtro anti-spam no ficheiro */etc/amavis.conf*:

```
# Default SPAM checking mode
# Uncomment the two lines below to enable it back
#
@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl,
\$bypass_spam_checks_re);
# [...]
```

Na configuração por omissão, os e-mails considerado spam são colocados em quarentena e nenhuma informação chega ao destinatário. Nesta configuração os e-mails indicam apenas as probabilidades de serem spam, deixando ao administrador a escolha das acções a realizar como se verifica a seguir.

```
use strict;
# earlier files.
# See /usr/share/doc/amavisd-new/ for documentation and examples of
# the directives you can use in this file

$sa_spam_subject_tag = '***SPAM*** ';
$sa_tag_level_deflt  = undef;  # add spam info headers if at, or above
that level
```

```
$sa_tag2_level_deflt = 6.31;    # add 'spam detected' headers at that
level
$sa_kill_level_deflt = 9999;    # triggers spam evasive actions
```

A "sensibilidade" do filtro anti-spam pode ser refinada alterando o valor de *$sa_tag2_level_deflt*: Com um valor mais baixo, serão necessários menos indicadores para que a mensagem seja considerada *spam*. No entanto, este valor não deve ser inferior a 5, ou corremos o risco de todas as mensagens, mesmo as mais legítimas, começarem a ser classificadas como *spam*. As actualizações dos filtros estão definidas para que sejam actualizados diariamente, via crontab.

```
# SPAMASSASSIN UPDATES
00 02 * * 1             /usr/bin/sa-update >/dev/null 2>&1
```

4) Ficheiros Log

A nível de ficheiros log o /var/log/mail e /var/log/mail.info apresentam toda a informação do envio/recepção de e-mails, assim como o estado das mensagens que foram bloqueadas com vírus, spam, e afins.

```
Tail -f /var/log/mail.info
Sep 20 11:46:20 suse11.iseplab.local/usr/sbin/amavisd[21833]: (21833-03)
Passed CLEAN, [192.1.1.5] <> -> <administrator@sensormatic.com>, Message-
ID: <Cd1yuD56s0000004a@mail.iseplab.local>, mail_id: Ajwqz85gHi11, Hits:
1.088, 1333 ms
Sep 21 00:45:02 suse11.iseplab.local/usr/sbin/amavisd[22385]: (22385-06)
Blocked SPAM, [192.53.123.73] <administrator@teste.com> ->
<user130@caramelo.com>, quarantine: spam-e7SKlQGKXYAo.gz, Message-ID:
<020301c7305d$462db1c0$973b4b42@kcwkvfy>, mail_id: e7SKlQGKXYAo, Hits:
15.265, 1358 ms
```

Como a maior parte das vezes os administradores não têm tempo para se ligarem aos servidores para ver o estado ou evolução do servidor de relay, foi implementado um módulo para gestão e estatística dos e-mails do servidor de Mail Relay. Como se pode verificar na figura seguinte, acedendo através do interface Web, ao relatório de anti-vírus e anti-spam o administrador tem acesso às estatísticas diárias, semanais, mensais e anuais de todos os *e-mails* processados.

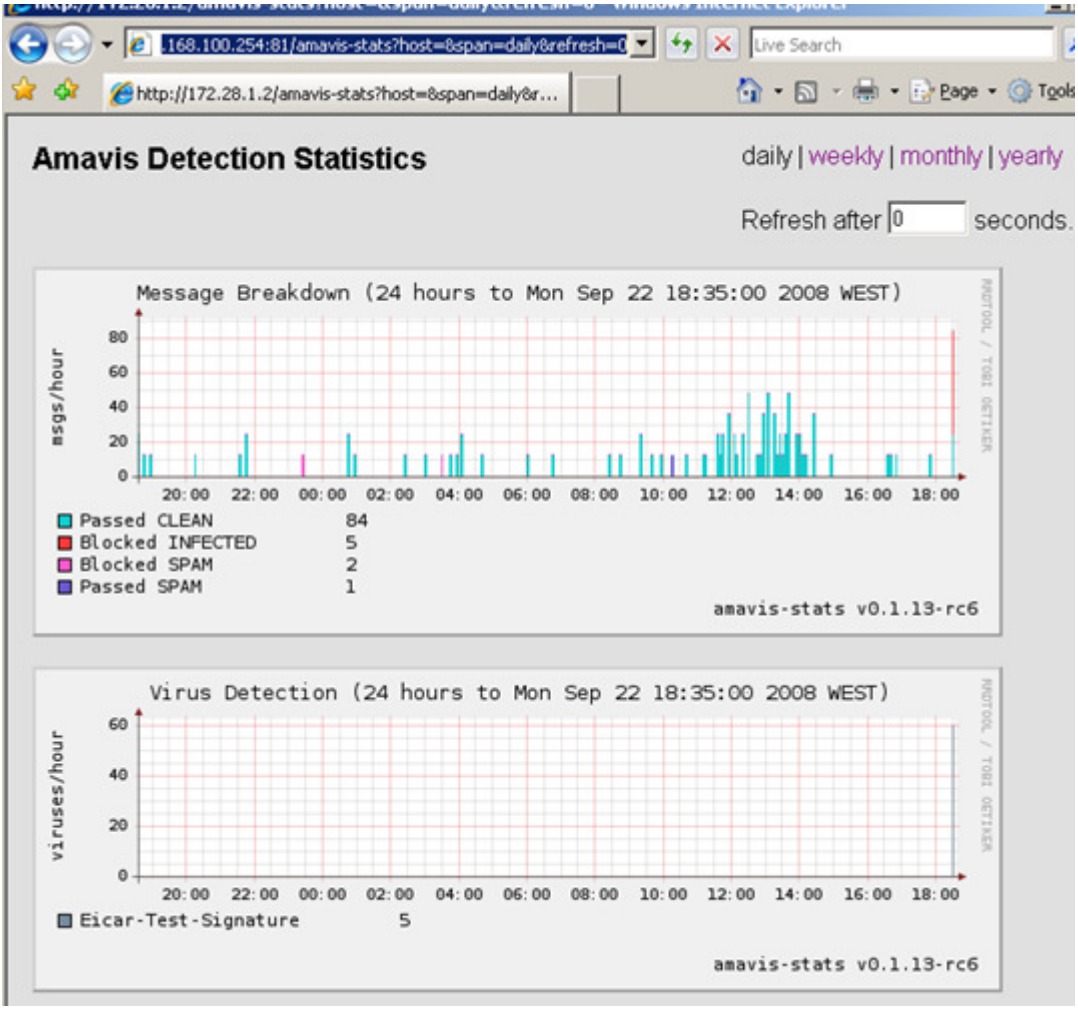


Figura 52 – Relatório de E-mail para o Anti-vírus e Anti-spam

- **MONITORIZAÇÃO DE REDE**

Para manter uma monitorização constante da rede foram instaladas algumas ferramentas que interligadas com o servidor Web permitem monitorizar o tráfego, eventuais problemas com activos de rede e estatísticas, relatórios e alertas.

1) Nagios

O Nagios é uma popular aplicação de monitorização de rede do tipo código aberto e licenciado pelo sistema GPL – *General Public License*. Pode monitorar tanto *hosts,* serviços, tendo a possibilidade de enviar alertas ao administrador quando ocorrem problemas e/ou também quando os problemas são resolvidos. Neste caso o Nagios foi instalado para enviar alertas do estado dos equipamentos activos e servidores caso surja

algum problema, como a quebra de alguns serviços, como o servidor Web, ou até falha ou roubo de equipamentos.

O pacote instalado no Suse 11 foi o nagios-3.0.1-19.1, foi criada uma conta de serviço nagios com palavra passe !QAZ2wsx sendo definidos os equipamentos a gerir, o switch (HP), o ponto de acesso wireless (Dlink) e o Suse11 Linux. No ficheiro seguinte ilustra-se um extracto da configuração que pode ser consultado no Anexo 5.

```
vi /etc/nagios/objects/switch.cfg

define host{
      use          generic-switch
      host_name    hp-5406-pwr
      alias        hp-5406-pwr Switch
      address      192.168.100.253
      hostgroups   switches
      }

define host{
        use             generic-switch
        host_name       dlink-g624t
        alias           dlink-g624t
        address         192.168.100.251
        hostgroups      switches
        }
define hostgroup{
      hostgroup_name    switches
      alias       Network Switches
      }
```

Sempre que existirem problemas com os equipamentos acima referidos é enviado um relatório por e-mail para o endereço abaixo indicado nos contactos.

```
vi /etc/nagios/objects/contacts.cfg

define contact{
        contact_name                    nagiosadmin
        use                           generic-contact
        alias                           Nagios Admin
        e-mail                           nagios@caramelo.com
        }
```

2) NTOP

O ntop é uma aplicação que analisa o tráfego de uma rede e a utilização da mesma. O Ntop é baseado em *libpcap* e foi escrita numa forma portátil para que trabalhe em qualquer plataforma, tanto Unix como Windows.

Os Administradores podem usar um web browser (e.g. netscape) para navegar pelo ntop e extrair informação sobre o tráfego e o estado da rede. O uso de um interface de internet, a

configuração e administração limitada via internet, a utilização de poucos recursos e de pouca memória torna o ntop fundamental para a monitorização de vários tipos de rede.

O pacote instalado foi o ntop-3.3-94.1, tendo-se definido a conta admin como conta de serviço, foi configurado o acesso Web, podendo-se ter acesso pelo link "Relatório de tráfego". Os interfaces configurados para análise de tráfego, foram o externo e interno, para como podemos ver na tabela seguinte e/ou o Anexo 6, e, depois de activos é só consultar e gerar os relatórios que se desejar.

Tabela 1 – Configuração dos Interfaces no Ntop

Command line	
Started as....	/usr/bin/ntop -P /var/lib/ntop -i eth0,eth2 -u root -w 192.168.100.254:82
Resolved to....	/usr/bin/ntop -P /var/lib/ntop -i eth0,eth2 -u root -w 192.168.100.254

3) IPTRAF

O Iptraf é uma ferramenta que permite a monitorização de trafego num deterninado segmento de rede no que respeita à quantidade, tipo, origem e destino, de mesma forma que o NTOP, mas apresentando duas características que se distinguem. Por um lado, pelo facto de monitorizar e enumerar os portos e interfaces utilizados em tempo real, e por outro, a possibilidade de se executar esta ferramenta via shell, ou seja com uma ligação remota via ssh a um servidor. O pacote instalado foi o iptraf-3.0.0-114.1.

4) ANALOG / FWANALOG

Uma vez conseguidas as análises do tráfego e acesso aos recursos de internet, foi necessário ter uma ferramenta que apresentasse estatísticamente e com interface Web tudo o que se passava na firewall, como acessos, ataques, etc. Para isso usou-se a conjugação analog (monitorização de acessos) com firewall analog (monitorização de acessos sobre *firewalls*).

O *analog* é uma ferramenta que analisa e processa estatísticamente ficheiros log para posteriormente gerar relatórios de acesso a servidores.

O *fwanalog* que é uma ferramenta em shell script, que gera relatórios (utilizando o analog) através de ficheiros log das firewalls, nomeadamente ipchains e iptables no caso de sistemas Linux e ficheiros log de pix (sistema integrado de *hardware* e *software* de

firewall) no caso da Cisco.

É necessário configurar o *fwanalog* para apresentar o caminho onde vai estar a página do interface Web. Será preciso também indicar o tipo de *log* que, no caso do shorewall (Linux) é o *iptables*. Por fim, é ainda necessário referia o caminho do *log* que é var/log/firewall.

```
vi /usr/local/fwanalog-0.6.9/fwanalog.opts
outdir="/srv/www/htdocs/fwanalog"
logformat="iptables"
# The name of your logfiles, with a wildcard if you want
inputfiles_mask="firewall*"
# The directory where your logfiles are in,
inputfiles_dir="/var/log"
analog="analog"
```

Para que estes relatórios sejam actualizados constantemente foi definido um período de actualização de 30 minutos como se pode ver na linha do *crontab*.

```
# FWANALOG
30 * * * *              /usr/local/fwanalog-0.6.9/fwanalog.sh
```

Para se ter acesso ao interface Web do fwanalog, é necessário seleccionar "Relatório da Firewall" do site de acesso às estatísticas e relatórios, no servidor Web, definido na figura 51.

- **VPN – OPENVPN**

As principais razões que levaram à opção do OpenVPN foram a portabilidade através das muitas plataformas Linux, a sua excelente estabilidade, a facilidade de instalação e o suporte a IP dinâmico e NAT.

No Windows, o OpenVPN pode ler certificados e chaves privadas de leitores de cartões sendo o interface para o utilizador amigável.

Para a instalação foi usado o pacote openvpn-2.0.9-96.1, para a VPN e os pacotes openssl-0.9.8g-47.1 e openssl-certs-0.9.8g-47.1 para a emissão dos certificados, sendo a configuração do servidor a seguinte:

```
port 1196
float
proto udp
dev tun
tun-mtu 1500
tls-server
tls-auth /etc/openvpn/easy-rsa/keys/tls.key 0
```

```
dh /etc/openvpn/easy-rsa/keys/dh1024.pem
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/server_ssl_key.crt
key /etc/openvpn/easy-rsa/keys/server_ssl_key.key
ifconfig-pool-persist /etc/openvpn/ipp.txt
# Reserved IPs for VPN clients
server 10.0.1.0 255.255.255.0
#
# Routes and DNS
push "route 192.168.100.0 255.255.255.0"
push "dhcp-option DNS 192.168.100.1"
push "dhcp-option WINS 192.168.100.1"
push "dhcp-option DOMAIN iseplab.local"
push "dhcp-option NTP 192.168.100.1"
push "redirect-gateway"
client-to-client
keepalive 10 120
comp-lzo
user nobody
group nobody
persist-key
persist-tun
daemon
verb 5
mute 5
log /var/log/openvpn_dynamic.log
status /var/log/openvpn_status.log
;duplicate-cn
```

A configuração do cliente é a seguinte:

```
remote 10.0.28.109 1196
dev tun
proto udp
float
resolv-retry infinite
nobind
persist-key
persist-tun
comp-lzo
;verb 5
mute 5
ca ca.crt
cert client_ssl_key.crt
key client_ssl_key.key
tls-client
tls-auth tls.key 1
cipher BF-CBC
# Wireless networks often produce a lot of duplicate packets.  Set this
flag
# to silence duplicate packet warnings.
;mute-replay-warnings
# These settings are shared by all clients
client
ns-cert-type server
;user nobody
;group nobody
```

3. CENTOS.ISEPLAB.LOCAL

No servidor Suse CentOS, foi feita uma instalação mímina do sistema operativo, sendo adicionados os pacotes de samba e winbind da mesma forma que o Suse 11 (pagina 116). Foram feitas idênticas configurações de rede, apenas sendo feita uma alteração a nível do ficheiro /etc/hosts e /etc/resolv.conf, uma vez que vamos ter interligação à directoria activa da Microsoft. Este servidor apenas foi implementado com o intuito de num cenário em que não exista uma directoria activa de Microsoft, mas uma directoria Linux ou Unix de openLDAP. Por outro lado com a implementação de um sistema de AAA passa a ser requesito a redundância e compatibilidade entre sistemas. De seguida são apresentadas as configurações de rede associadas.

```
Vi /etc/hosts
192.168.100.254 suse11.iseplab.local suse11
192.168.100.1   dc.iseplab.local dc
192.168.100.2   mail.iseplab.local mail
192.168.100.3   centos.iseplab.local contos
192.168.20.254  dmz.iseplab.local dmz
10.0.28.109     wan.iseplab.local wan
```

```
vi /etc/resolv.conf
#domain iseplab.local
nameserver 192.168.100.1
nameserver 193.136.60.10
nameserver 193.136.60.2
```

Os pacotes necessários, para além dos de samba e winbind são os seguintes, para ser suportado o funcionamento como servidor de radius com interligação ldap.

```
freeradius-1.1.3-1.2.el5
samba-3.0.23c-2.el5.2.0.2
krb5-libs-1.5-26
krb5-devel-1.5-26
krb5-workstation-1.5-26
pam_krb5-2.2.11-1
```

Da mesma forma que foram configurado o serviço de IAS para suportar os clientes (switch e AP) foi necessário colocar estes equipamentos, como clientes autorizados, a efectuar a autenticação radius no ficheiro seguinte:

/etc/raddb/clients.conf

```
client 192.168.100.253  {
      secret = !QAZ2wsx
      shortname = localhost
```

```
}
client 192.168.100.251 {
      secret = !QAZ2wsx
      shortname = 192.168.100.251
```

Do ponto de vista de configuração, para a suportabilidade de aplicação automática da vlan correspondente ao utilizador validado na rede, esta foi feita pelo ficheiro seguinte, onde se apresentam os grupos associados a cada vlan. Por exemplo para grupo "lan" é aplicada a vlan 1.

/etc/raddb/users

```
DEFAULT NAS-Port-Type == "Wireless-802.11", Ldap-Group == "lan"
      Service-Type = "Framed",
      Tunnel-Type = 13,
      Tunnel-Medium-Type = 6,
      Tunnel-Private-Group-Id = 1,
      Reply-Message = "%u WIFI Auth OK - VLAN 1"
DEFAULT NAS-Port-Type == "Ethernet", Ldap-Group == "lan"
      Service-Type = "Framed",
      Tunnel-Type = 13,
      Tunnel-Medium-Type = 6,
      Tunnel-Private-Group-Id = 1,
DEFAULT NAS-Port-Type == "Ethernet", Ldap-Group == "Rede120"
      Service-Type = "Framed",
      Tunnel-Type = 13,
      Tunnel-Medium-Type = 6,
      Tunnel-Private-Group-Id = 2,
DEFAULT NAS-Port-Type == "Ethernet", Ldap-Group == "Rede130"
      Service-Type = "Framed",
      Tunnel-Type = 13,
      Tunnel-Medium-Type = 6,
      Tunnel-Private-Group-Id = 3,
```

Relativamente à restante configuração e parametrização, por esta ser demasiada extensa e está descrita em anexo no Anexo 4.

4. MAIL.ISEPLAB.LOCAL

A nível do servidor de correio/Web, foi mantida a estrutura do cenário anterior, no entanto, a nível de encaminhamento do envío de *e-mail,* este é feito agora redirecionando todo o e mail para o servidor de *Mail Relay*. Esta configuração pode ser verificada na figura seguinte.

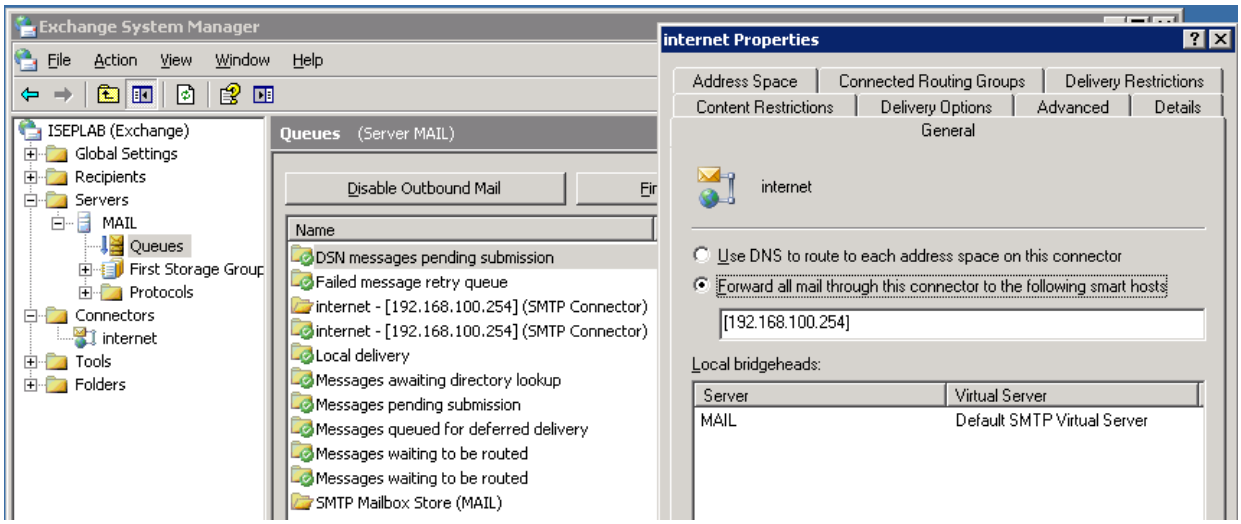


Figura 53 – Reconfiguração do Exchange por ecaminhamento para o Mail Relay

5. POSTOS DE TRABALHO

Neste cenário os postos de trabalhos obtêm endereços atribuídos por DHCP com ou sem atribuição de IP via endereço MAC. O único ponto a validar para este cenário foi se as placas de redes dos postos de teste suportavam a autenticação via 802.1x, o que se verificou, e a instalação e actualização do anti-vírus como se vê na figura seguinte.

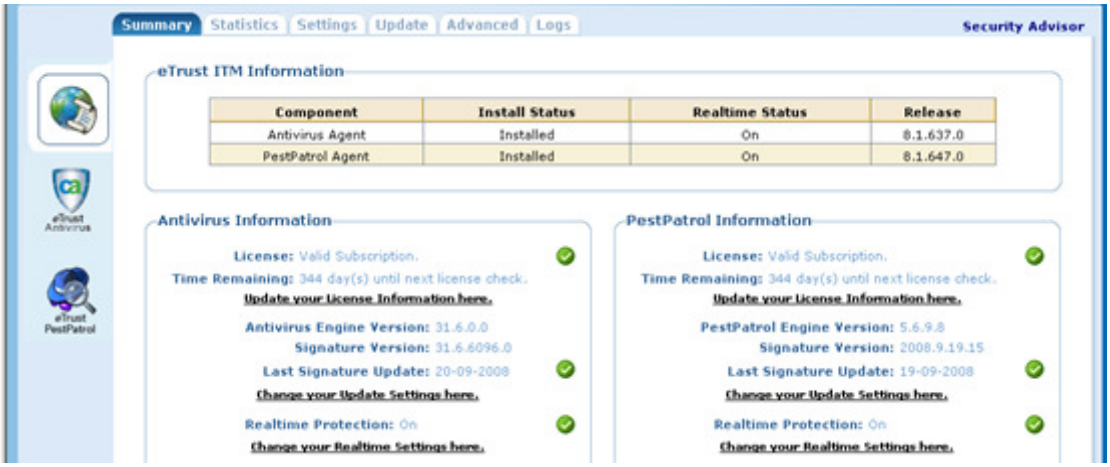


Figura 54 – Anti-vírus do posto de trabalho

6.2.3. ACTIVOS DE REDE

- **SWITCH DE REDE HP PROCURVE**

O switch implementado neste cenário funciona, como core switch da rede, como se pode verificar na configuração apresentada. Sendo o router para as vlan´s criadas e como exemplo, firewall para a vlan 120 que só terá acesso à internet e serviços de atribuição de IP `(ip access-list extended "vlan_120”)`.

Para ser aplicada a política de segurança foi definida uma conta Admin para leitura e escrita com palavra-chave !QAZ2wsx (usada a mesma para simplificar a implementação e estudo da rede) e as comunidades SNMP para leitura isepro e escrita iseprw. Para este switch foram definidas as 3 vlan, segundo o cenário de teste, sendo as portas sem autenticação as portas 6 e 8, e as de autenticação eap/802.1x as portas 5 e 7. Por consequência, estas duas portas ficam impossibilitadas, de serem usadas para acgregação de tráfego (*lacp*[1]).

```
hostname "ISEP CORE"
snmp-server contact "nuno duarte"
snmp-server location "datacenter"
max-vlans 50
web-management management-url ""
time daylight-time-rule Middle-Europe-and-Portugal

ip access-list extended "vlan_120"
10 permit tcp 192.168.120.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 53
20 permit udp 192.168.120.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 53
30 permit tcp 192.168.120.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 8080
40 permit tcp 192.168.120.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 66
50 permit tcp 192.168.120.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 67
60 permit tcp 192.168.120.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 21
70 permit tcp 192.168.120.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 443
80 deny   ip any  any

interface 5
   no lacp [1]
exit
interface 7
   no lacp
exit
ip default-gateway 192.168.100.254
sntp server 192.168.100.1
ip routing
timesync sntp
sntp unicast
snmp-server community "isepro" Unrestricted

vlan 1
   name "rede_100"
   untagged 1-4,9
```

```
   ip address 192.168.100.253 255.255.255.0
   no untagged 5-8
   exit
vlan 2
   name "rede_120"
   untagged 5-6
   ip address 192.168.120.254 255.255.255.0
   ip helper-address 192.168.100.1
      ip access-group "internet" in
   exit
vlan 3
   name "rede_130"
   untagged 7-8
   ip address 192.168.130.254 255.255.255.0
   ip helper-address 192.168.100.1
   exit
port-security  9  learn-mode  static  action  send-disable  mac-address
0050da39e1c7
aaa authentication port-access eap-radius
radius-server dead-time 1440
radius-server timeout 15
radius-server retransmit 5
radius-server key !QAZ2wsx
radius-server host 192.168.100.1
radius-server host 192.168.100.3
aaa port-access authenticator 5,7,9
aaa port-access authenticator active
aaa port-access 5,7
spanning-tree
ProCurve Switch HP#
```

[1] Lacp – *Link Aggregation Control Protocol* – protocolo usado para agregar várias portas, com o objectivo de obter um desempenho superior, e que por omissão está desactivado.

Para configurar a segurança à porta do ponto de acesso wireless, em caso de manuseamentos não autorizados do equipamento, usou-se para este switch o protocolo "port-security" para a porta 9 com segurança via endereço MAC. Este cenário prevê que aquando de um abuso ou modificação de dados na porta usada, esta seja automaticamente desabilitada, e em simultâneo seja enviado um aviso ao administrador do sistema.

```
ProCurve Switch HP(config)# port-security ethernet 9 ?
Action      Define device's action in case of an intrusion detection.
Address-limit     Define number of authorized addresses on the port(s).
Clear-intrusion-flag    Clear intrusion indicator for the port(s)
Learn-mode  Define the mode of acquiring authorized MAC address(es).
Mac-address Configure the address(es) authorized on the port(s).

ProCurve Switch HP(config)# show port-security
  Port Learn Mode           | Action
  ---- -------------------- + ------------------------
  8    Continuous           | None
  9    Static               | Send Alarm, Disable Port
```

- **Ponto de acesso wireless dlink**

A nível do ponto de acesso wireless, as configurações de rede mantêm-se as do cenário anterior apenas sendo alteradas a default gateway para 192.168.100.253 e as configurações wireless que passam para 802.1x, como mostra a figura seguinte.

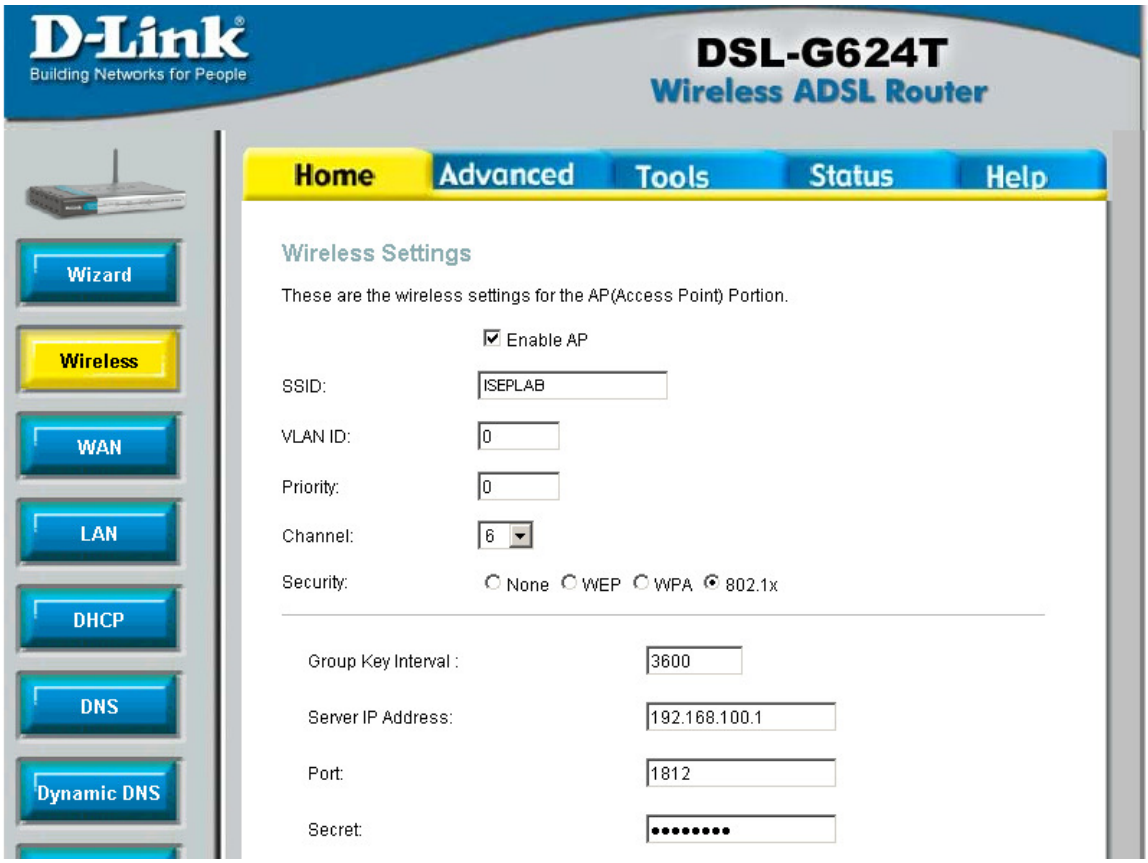


Figura 55 – Configuração do Access Point com segurança 802.1x

6.3. TESTES E ANÁLISE DE RESULTADOS

6.3.1. INSTALAÇÃO DOS SISTEMAS

Na instalação dos sistemas foram definidas partições separadas, nomeadamente 3 para os sistemas Microsoft, sendo a sua organização a seguinte

1. Instalação do sistema operativo conhecido como c:\ com no mínimo 30Gb
2. Localização das bases de dados da directoria activa, no caso do DC e bases de dados do Exchange no caso do servidor de e-mail
3. Paginação de memória no disco *(page file ou swap)*
4. Suporte de redundância para discos em caso de falha.

Nos sistemas Linux foram feitas as instalações por omissão, com a excepção do directório /var/log que foi colocado numa partição diferente.

Com estas configurações estão salvaguardadas situações de vulnerabilidades, com problemas de sistemas operativos, e, consequente perca de dados caso seja necessária a sua reinstalação.

6.3.2. RECONHECIMENTO EXTERNO

No caso da pesquisa pelo nmap, ao interface externo do router verificou-se que com a implementação da firewall as portas disponíveis diminuíram consideravelmente. Como se verifica, apenas o acesso FTP é o acesso dito inseguro, daí o facto, como se vai ver mais à frente, deste serviço ter sido passado para a DMZ. De referir que, com a alteração à resposta de smtp do postfix, não é possível o nmap reconhecer o servidor de *e-mail*.

- **nmap** (pesquisa de portas disponíveis no router / firewall)

```
nmap -PE  -v -PA21,22,23,80,3389 -sU -T4 -A 10.0.28.109

Scanning 10.0.28.109 [1000 ports]
Discovered open port 443/tcp on 10.0.28.109
Discovered open port 21/tcp on 10.0.28.109
Discovered open port 25/tcp on 10.0.28.109
PORT     STATE SERVICE       VERSION
21/tcp   open   ftp      Microsoft ftpd
25/tcp   open   smtp
53/tcp   closed domain
80/tcp   closed http
443/tcp  open   ssl/http Microsoft IIS webserver 6.0
```

As portas que estão disponíveis para o exterior são associadas aos serviços disponibilizados, sendo eles o acesso ao *webmail (443), e-mail (25) e ftp (21).*

6.3.3. ACESSO À REDE DE COBRE

- **Utilizadores Autorizados**

Foi utilizado um PC de teste, ligado à porta 4 do switch core, que está configurado sem autenticação EAP/802.1X. Verificou-se a situação do cenário da rede desprotegida, ou seja, qualquer utilizador consegue obter endereço IP, e consegue ligar-se à infra-estrutura.

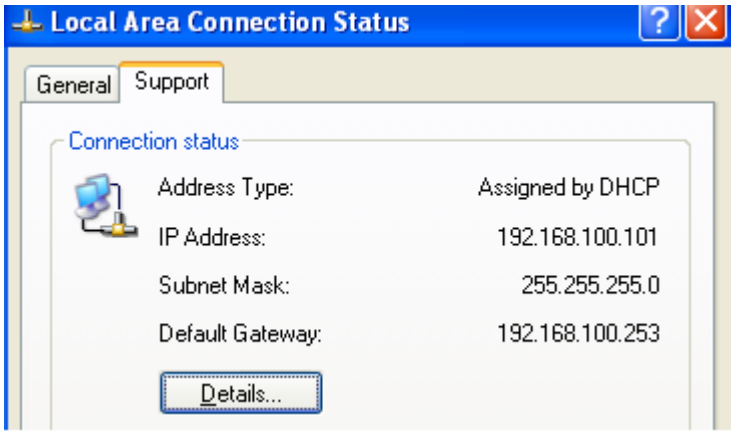


Figura 56 – Ligação sem autenticação

De seguida, mudou-se o cabo de rede do PC de teste da porta 4 para a porta 5, sendo verificado que a obtenção de endereço IP deixou de ser automatica, e uma vez que se desactivou nas propriedades da placa de rede o "user windows login" passando a ser exigido um login e palavra-chave para o acesso à infraestrutura de rede, como podemos ver na figura 60.

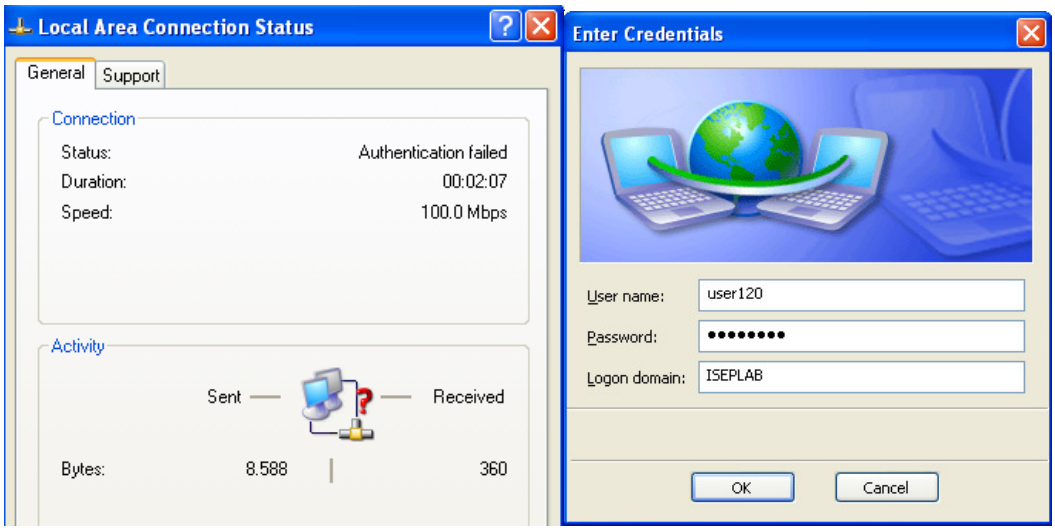


Figura 57 – Ligação com autenticação

Como foi definido na directoria activa, associada ao IAS, efectuou-se login com o user120, uma vez que tinha permissões de acesso à rede pela vlan 2, foi-lhe atribuído endereço IP da rede 120 como se pode verificar a seguir.

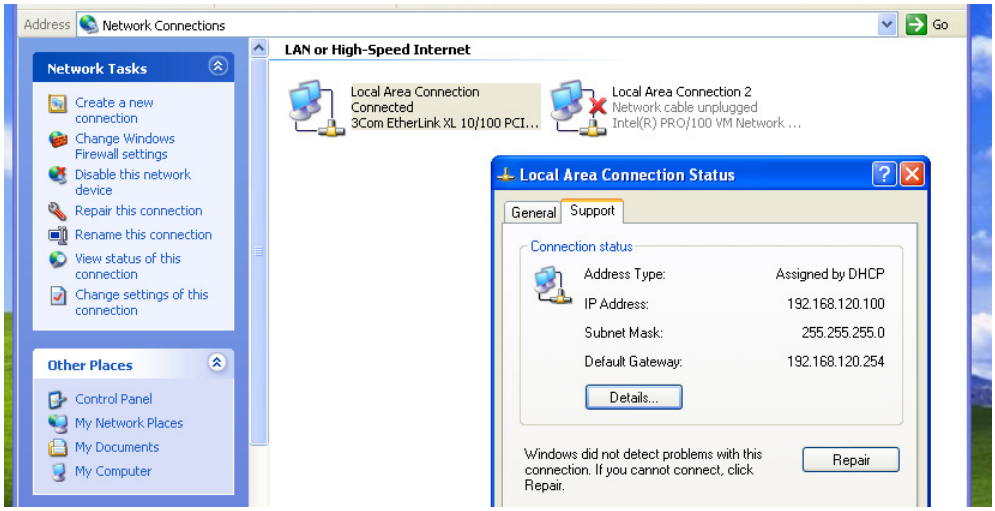


Figura 58 – Ligação à Vlan 2, rede 120

Relativamente ao IAS sempre que um utilizador é validado e atribuído um endereço IP é sempre registado esse facto no registo de eventos (*eventviewer*) do Windows, e, como se pode verificar de seguida quando o utilizador "user120" efectuou login, no IAS foram validadas todas as permissões.

```
Fully-Qualified-User-Name = iseplab.local/ISEPLAB/USERS/user120
NAS-IP-Address = 192.168.100.253
NAS-Identifier = ProCurve Switch HP
Client-Friendly-Name = HP2608-PWR
Client-IP-Address = 192.168.100.253
Calling-Station-Identifier = 00-50-da-39-e1-c7
NAS-Port-Type = Ethernet
NAS-Port = 5
Proxy-Policy-Name = switch connection
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = Rede 120
Authentication-Type = PEAP

EAP-Type = Secured password (EAP-MSCHAP v2)
```

Feito o teste com o user120, terminou-se a sessão com este utilizador e iniciou-se a sessão com o user130, mantendo-se a ligação ao switch na mesma porta, independentemente de esta estar associada à vlan 2 no switch ou seja, rede 120. Quando surgiu o ecrã de para colocar o utilizador e palavra-chave, foi colocado o user130 com a respectiva palavra-chave, e verificou-se que, apesar da porta estar associada à vlan 2, automaticamente foi atribuído um endereço ip da rede 130 ou seja da vlan 3. Isto deve-se ao facto ao ser independentemente às vlan´s associadas as portas do switch, a autenticação Eap/802.1x, tem "perioridade" em relação à vlans locais ao switch pré-configuradas. Nas figuras

seguintes, são apresentados os ecrãs de login, obtenção de ip e validação no IAS, do utilizador associado à rede 130.

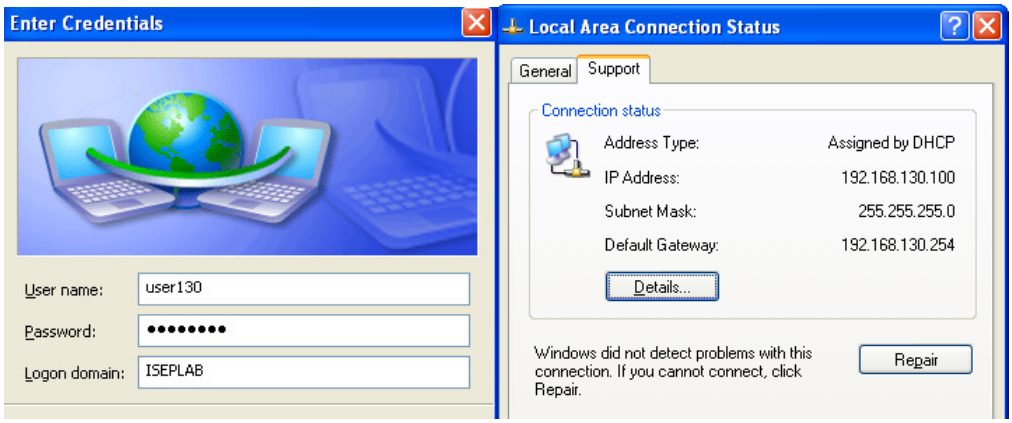


Figura 59 – Conecção à Vlan 3, rede 130

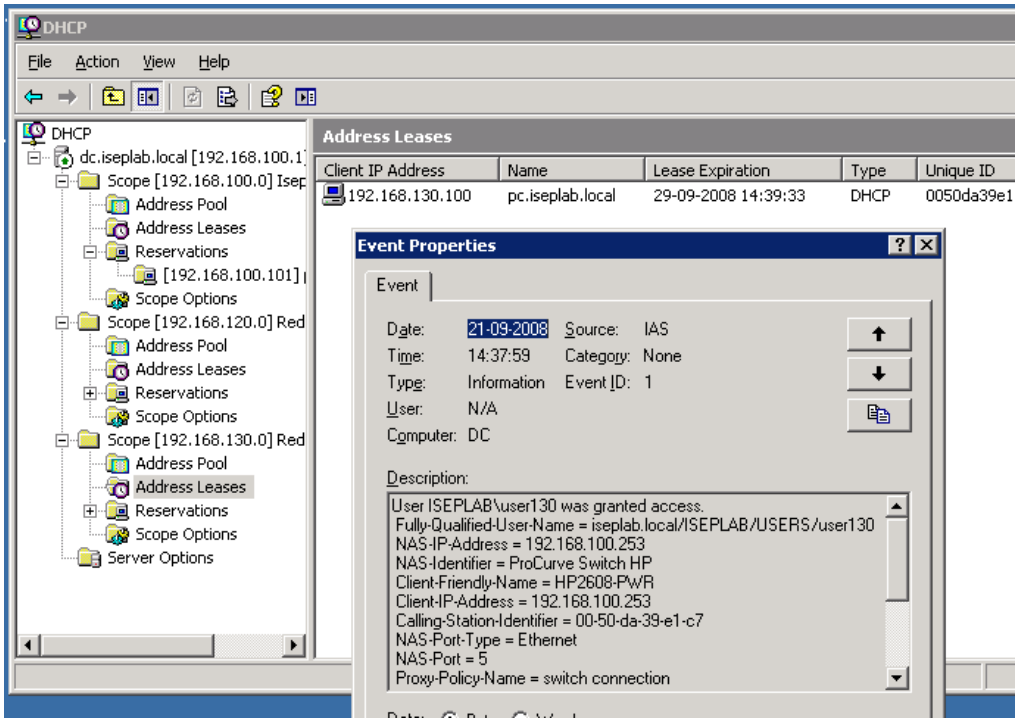


Figura 60 – Validação no IAS e atribuição de IP à Vlan 3

- **Utilizadores Não Autorizados**

Um segundo teste realizado com o sistema Eap/802.1x foi a utilização de utilizadores falsos, como se de um intruso se tratasse, ou utilização de IP fixo no acesso à rede.

No primeiro caso, ao colocar o utilizador “hacker”, este ao ser validado no IAS, como nem sequer existia na directoria activa, o acesso foi negado. No segundo caso, não foi feita

qualquer validação no IAS, mas como a porta do switch está com a autenticação activa o utilizador não tem acesso à rede sem primeiro se autenticar, como se verifica a seguir.

```
User ISEPLAB\hacker was denied access.
 Fully-Qualified-User-Name = ISEPLAB\hacker
 NAS-IP-Address = 192.168.100.253
 NAS-Identifier = ProCurve Switch HP
 Called-Station-Identifier = 00-1c-2e-b9-2c-40
 Calling-Station-Identifier = 00-50-da-39-e1-c7
 Client-Friendly-Name = HP2608-PWR
 Client-IP-Address = 192.168.100.253
 NAS-Port-Type = Ethernet
 NAS-Port = 5
 Proxy-Policy-Name = switch connection
 Authentication-Provider = Windows
 Authentication-Server = <undetermined>
 Policy-Name = <undetermined>
 Authentication-Type = EAP
 EAP-Type = <undetermined>
 Reason-Code = 8

 Reason = The specified user account does not exist.
```

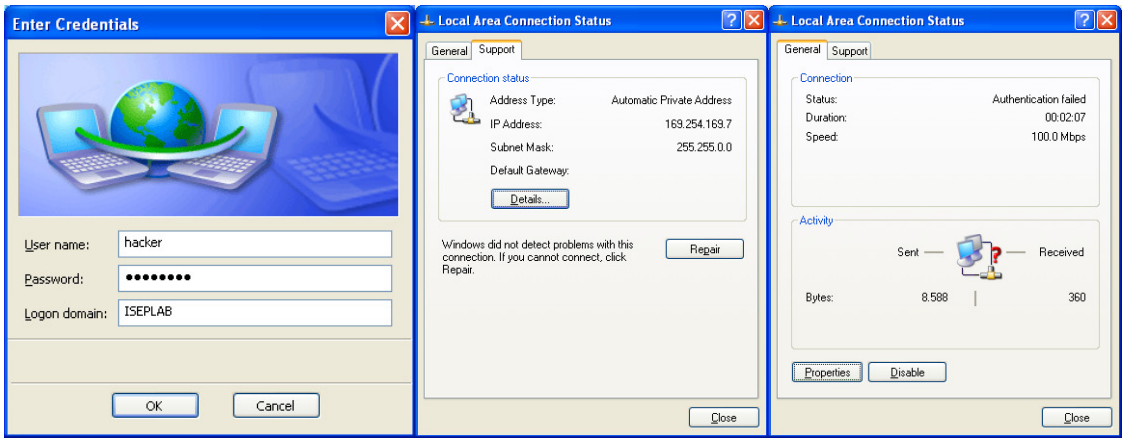


Figura 61 – Autenticação com um utilizador falso

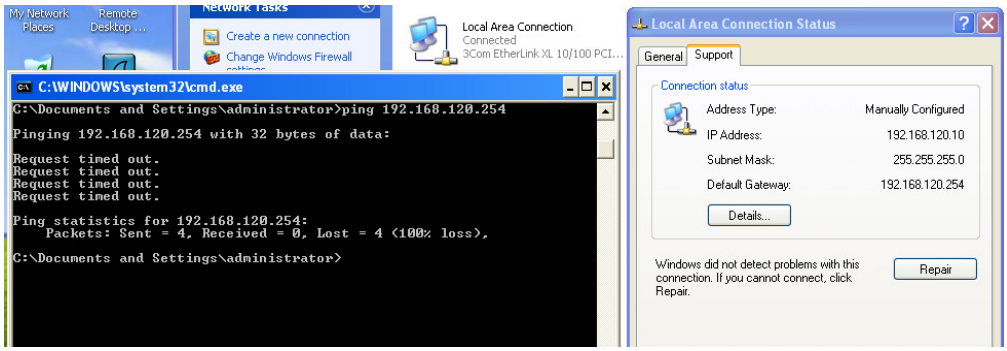


Figura 62 – Tentativa de acesso por ip fixo

De referir que foi feita uma tentativa de com o wireshark obter eventuais utilizadores ou palavras-passe dos acessos Eap/802.1x apenas sendo obtido o utilizador, porque se executou o wireshark no posto de teste como se vê na figura seguinte.

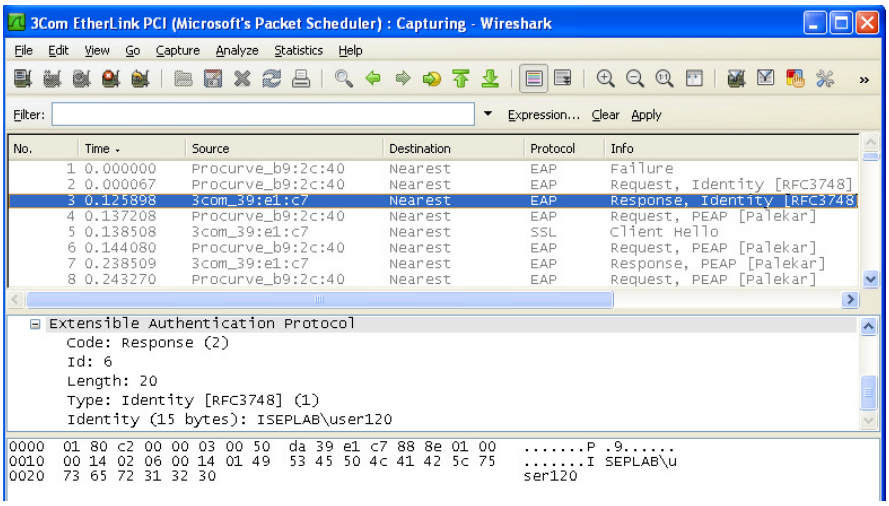


Figura 63 – Obtenção do utilizador de EAP

6.3.4. ACESSO À REDE WIRELESS

Os acessos wireless via Eap/802.1x funcionam da mesma forma que os acessos via cabo Ethernet, apenas o meio físico é diferente. Para este cenário não se conseguiu obter acesso à rede pelos métodos do capítulo anterior.

De referir apenas que para o caso do ponto de acesso wireless ser furtado, a configuração de segurança no switch bloqueia a porta como se mostra no teste seguinte.

Neste caso, a porta 9 foi configurada para ficar activa e activou-se a função de segurança que em caso de troca de equipamento, a porta bloqueia.

```
ProCurve Switch HP# show port-security 9
 Port Security
  Port : 9
  Learn Mode [Continuous] : Static              Address Limit [1] : 1
  Action [None] : Send Alarm, Disable Port
  Authorized Addresses
  --------------------
  0050da-39e1c7
ProCurve Switch HP# show interfaces brief
 Status and Counters - Port Status
                  | Intrusion                              MDI    Flow
  Port Type       | Alert     Enabled Status Mode          Mode   Ctrl
  ---- ---------- + --------- ------- ------ ----------- ------ -----
  8    10/100TX   | No        Yes     Down   10FDx       MDIX   off
  9    100/1000T  | Yes       Yes     Up     100FDx      MDIX   off
ProCurve Switch HP#
```

Neste momento foi retirado o ponto de acesso e colocado outro equipamento com um endereço MAC diferente o que causou o bloqueio da porta.

```
ProCurve Switch HP# show port-security intrusion-log
 Status and Counters - Intrusion Log
  Port MAC Address    Date / Time
  ---- -------------- -------------------------
```

```
   9    0002a5-108768 027/08/08 10:17:12
ProCurve Switch HP#
ProCurve Switch HP# show interfaces brief
 Status and Counters - Port Status
                  | Intrusion                                  MDI    Flow
  Port Type       | Alert     Enabled Status Mode       Mode   Ctrl
  ---- ---------- + --------- ------- ------ ---------- ------ -----
  8    10/100TX   | No        Yes     Down   10FDx      MDIX   off
  9    100/1000T  | Yes       No      Down   1000FDx    MDIX   off
```

Neste momento se o ponto de acesso for retirado e colocado de novo, este passa a funcionar de novo, esta situação é para salvaguardar uma possível falha de alimentação. Nesta situação o *nagios* envia um alerta ao administrador a reportar a situação. Nas figuras seguintes são apresentados o interface Web do nagios para os equipamentos e o *e-mail* de alerta ao administrador, com o aviso da falha.

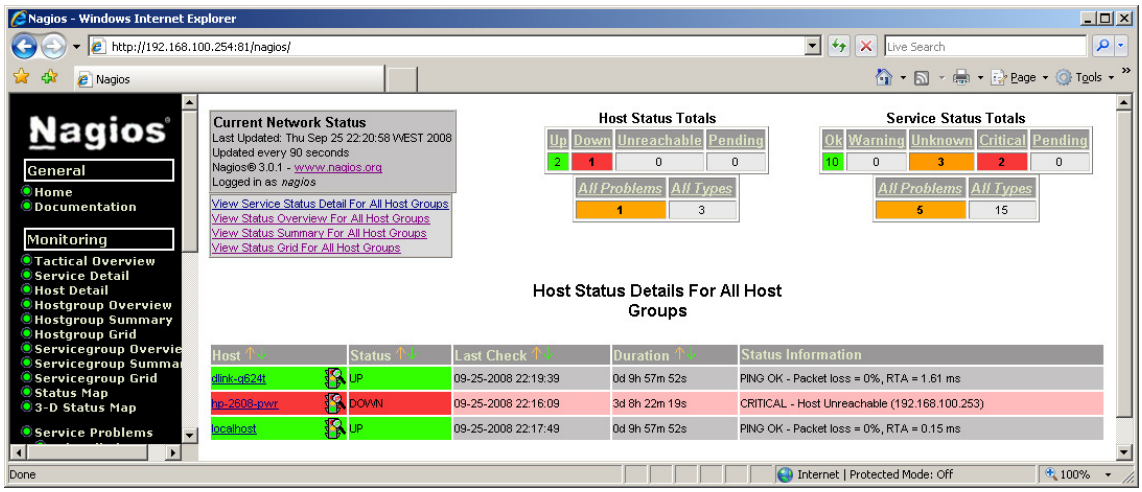


Figura 64 – Interface de monitorização do Nagios

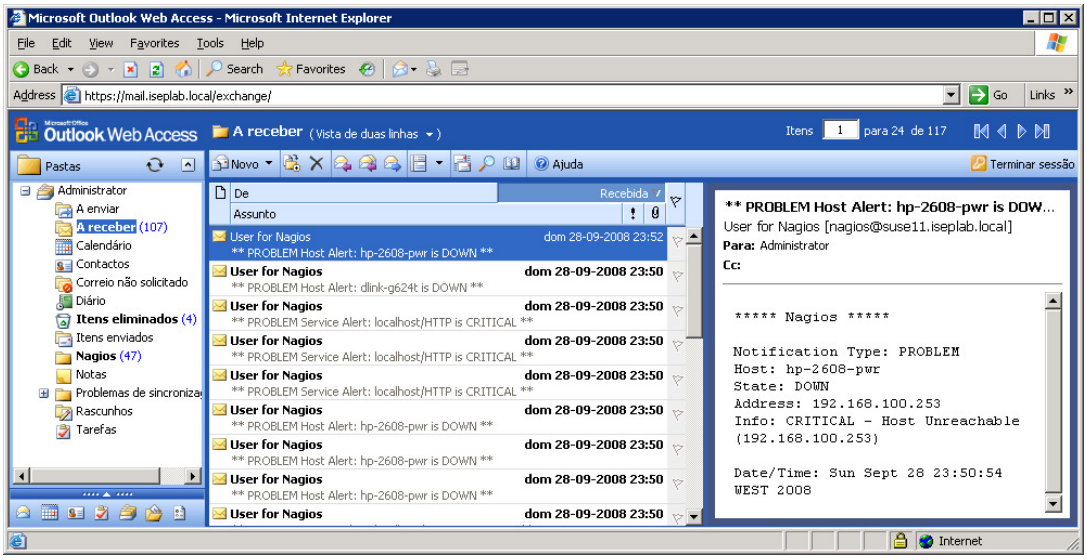


Figura 65 – Alerta do nagios ao administrador

6.3.5. SERVIÇOS E APLICAÇÕES

Relativamente às vulnerabilidades de segurança de serviços e aplicações apresentadas no cenário anterior, depois de aplicadas as correcções, verificou-se o seguinte:

- Com a instalação de uma firewall (neste caso o *Shorewall*) verificou-se que as portas/serviços disponíveis para o exterior diminuíram de forma considerável, uma vez que todo o tráfego por omissão está bloqueado.

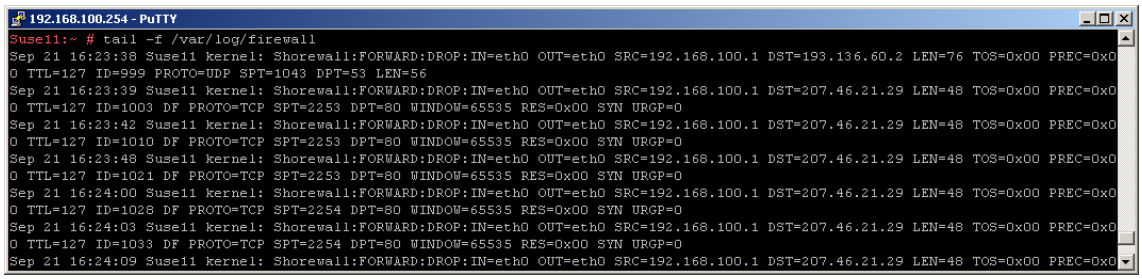


Figura 66 – Consulta dos registos de firewall

De referir que como no ficheiro */etc/shorewall/policy* o Limit:Brust, está definido para o interface externo, isto faz com que o sistema esteja protegido contra ataques de DoS, uma vez que o *Limit* define o número máximo de ligações por segundo, e o *Brust* é o número máximo de ligações tolerado.

- Para que o admnistrador não seja obrigado a ligar-se ao servidor de firewall, sempre que necessite de consultar os ficheiros log, pode consultar um interface Web que faz a gestão estatística destes ficheiros log. O acesso por este interface é em "Relatório de firewall" como se pode verificar na figura 67 a listagem e numero de pacotes bloqueados e na figura 68 o relatório gráfico.

Listing blocked packets, sorted by the number of blocked packets.

#blocks	%blocks	Mbytes	last time	blocked packet
19556	36.86%	1.46	Jun/25/08 00:07	192.168.30.255
19556	*36.86%*	*1.46*	*Jun/25/08 00:07*	*192.168.30.255/udp*
19533	*36.82%*	*1.45*	*Jun/25/08 00:07*	*192.168.30.255:netbios-ns (137)/udp*
23	*0.04%*	*0.01*	*Jun/23/08 19:58*	*192.168.30.255:netbios-dgm (138)/udp*
13649	25.73%	1.08	Sep/18/08 15:29	192.168.100.255
13649	*25.73%*	*1.08*	*Sep/18/08 15:29*	*192.168.100.255/udp*
13195	*24.87%*	*0.99*	*Sep/18/08 15:29*	*192.168.100.255:netbios-ns (137)/udp*
454	*0.86%*	*0.10*	*Sep/18/08 15:29*	*192.168.100.255:netbios-dgm (138)/udp*
7466	14.07%	0.40	Sep/18/08 09:42	192.168.100.254
4114	*7.75%*	*0.25*	*Sep/18/08 09:42*	*192.168.100.254/udp*
4112	*7.75%*	*0.25*	*Sep/18/08 09:42*	*192.168.100.254:domain (53)/udp*
1		*0.00*	*Sep/17/08 23:48*	*192.168.100.254:39000/udp*

Figura 67 – Interface Web de análise da firewall

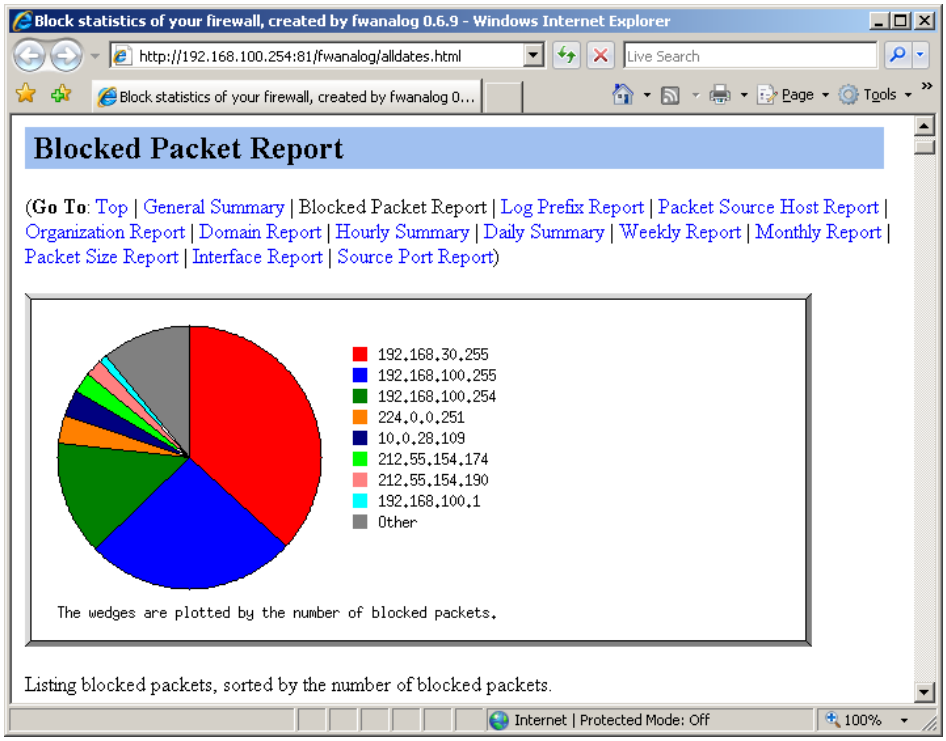


Figura 68 – Interface Web de análise da firewall

- Software de gestão de actualizações e/ou correcções dos sistemas operativos da Microsoft (wsus), associado a GPO's tornando os sistemas menos vulneráveis, mais fiáveis e seguros, garantindo que todos os utilizadores são abrangidos, como se verifica na figura seguinte retirada do MBSA para a política de actualizações.

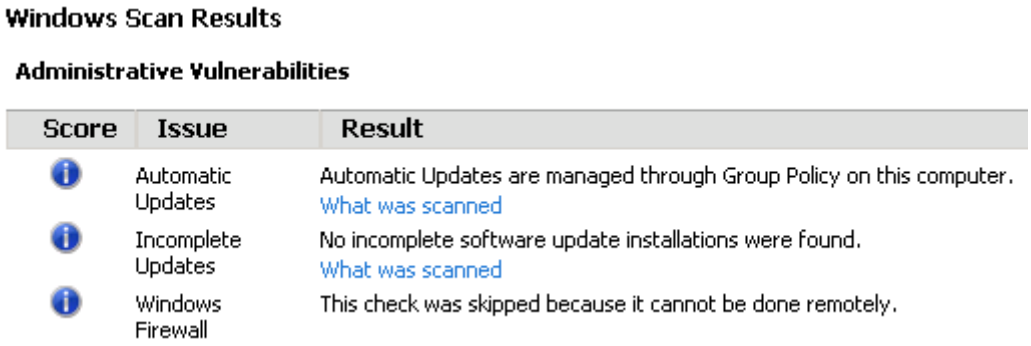


Figura 69 – MBSA para as políticas de actualizações

- De referir que apesar de o MBSA não apresentar qualquer erro, ou situação crítica, avisa para o facto de ser necessário efectuar aprovações no Wsus. Neste caso existiem já algumas aprovações pendentes, como é o caso de uma para o Office e 89 para segurança.

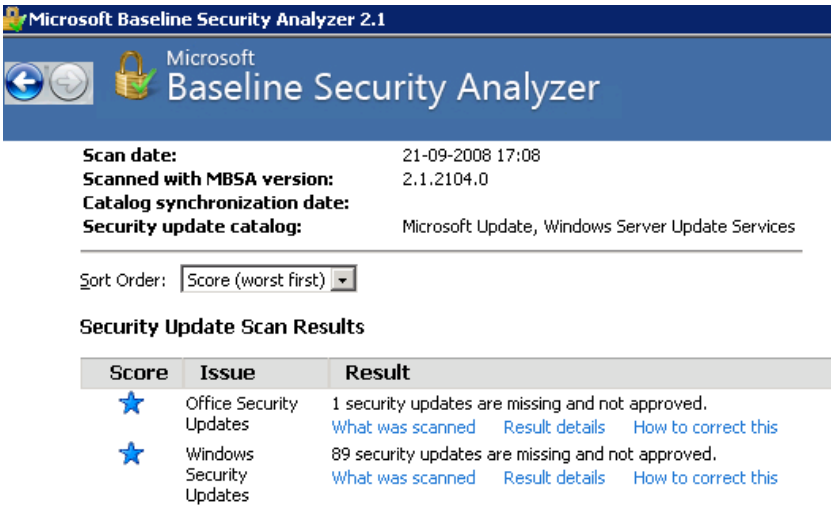


Figura 70 – MBSA para as actualizações

- Software de gestão anti-vírus. Uma vez implementado um anti-vírus foram detectados uma série de vírus e worms nos equipamentos, como se pode verificar no relatório da consola central depois de efectuar uma pesquisa por vírus, worms, etc, aos servidores e postos. Pelo figura seguinte pode-se verificar a lista dos virus mais encontrados e o número de virus encontrado por máquina.

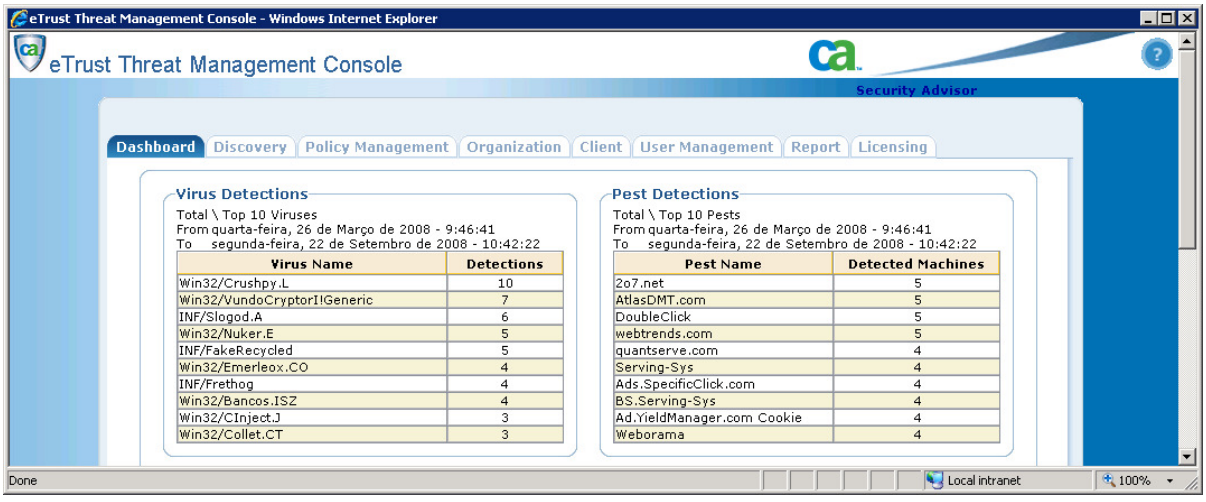


Figura 71 – Relatório da consola do servidor de Anti-vírus

Além da consola central, pode-se validar ao "nível do utilizador", ou a nível dos postos de trabalho, como se verifica na figura seguinte, estatísticas do anti-vírus. Neste caso o utilizador estaria informado também, da detecção e relatório dos nove vírus encontrados.

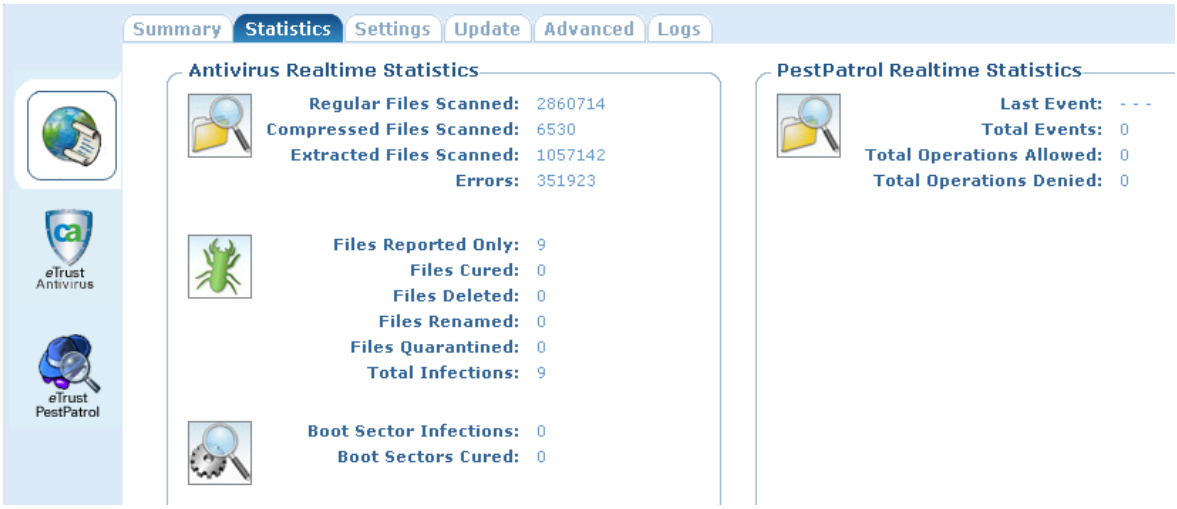


Figura 72 – Relatório da consola do Anti-vírus do posto de trabalho

6.3.6. VULNERABILIDADES DO SERVIDOR DE CORREIO.

Neste novo cenário serão verificadas e corrigidas as vulnerabilidades relativas ao servidor de correio electrónico, encontradas anteriormente. A inclusão de filtros *anti-spam* e de anti-vírus (e respectivas configurações) são as medidas mais relevantes. No entanto, de referir também que nem sempre o que se recebe como spam, é realmente spam ou seja pode ser um *e-mail* fidedigno importante, e a pensar nisso, a quarentena, permite o administrador recuperar, esse ou esses emails.

Como primeiro teste foi analisado o ficheiro *log* relativo ao *e-mail* de entrada, sendo verificado que todos os endereços listados, nas listas de referência para este trabalho (spamcop e spamhaus), são rejeitados como se pode verificar de seguida. Esta primeira acção leva a que os emails não cheguem ao Exchange e/ou utilizadores, o que, além de proteger a rede, não preenche a capacidade das bases de dados com lixo.

Log do Postfix Linux (cat /var/log/mail.info)

```
Sep 20 00:54:12 suse11 postfix/smtpd[26428]: NOQUEUE: reject: RCPT from
85.137.89.44.dyn.user.ono.com[85.137.89.44]: 554 Service unavailable;
Client host [85.137.89.44] blocked using bl.spamcop.net; Blocked - see
http://www.spamcop.net/bl.shtml?85.137.89.44;
from=<1namoey@BLUWORLDUSA.COM> to=<paisdesenho-02@caramelo.com>
proto=ESMTP helo=<85.137.89.44.dyn.user.ono.com>
Sep 20 00:54:14 suse11 postfix/smtpd[26427]: NOQUEUE: reject: RCPT from
64-195-93-61.mod.clearwire-dns.net[64.195.93.61]: 554 Service
unavailable; Client host [64.195.93.61] blocked using zen.spamhaus.org;
http://www.spamhaus.org/query/bl?ip=64.195.93.61;
```

Na segunda fase efectuou-se o teste de e-mail relay, em que o objectivo era tentar usar o servidor de relay, como servidor de reenvio de emails para outros endereços não fidedignos. Outro teste, foi assegurar também que os utilizadores internos, que não têm *email* externo, não conseguem enviar ou receber email de e para o exterior. Para realizar estes testes, tentou-se enviar um e-mail para 1980937@isep.ipp.pt a partir do utilizador user120@iseplab.local, sendo obtido o resultado de *Relay access denied*.

```
C:\> ping suse11.iseplab.local
Pinging suse11.iseplab.local [10.0.28.250] with 32 bytes of data:
Reply from 10.0.28.250: bytes=32 time=4ms TTL=128
Reply from 10.0.28.250: bytes=32 time=2ms TTL=128
Reply from 10.0.28.250: bytes=32 time=2ms TTL=128
Reply from 10.0.28.250: bytes=32 time=3ms TTL=128
Ping statistics for 10.0.28.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms
C:\>telnet suse11.iseplab.local 25
220 Relay ESMTP Lotus Notes
helo ok.pt
250 suse11.iseplab.local
mail from:user120@iseplab.local
250 Ok
rcpt to:1980937@isep.ipp.pt
554 <1980937@isep.ipp.pt>: Relay access denied
quit
C:\>

cat /var/log/mail.info | grep isep
Sep 28 18:53:25 suse11 postfix/smtpd[11184]: NOQUEUE: reject: RCPT from
bl9-149-88.dsl.telepac.pt[82.154.213.245]: 554 <1980937@isep.ipp.pt>:
Relay access denied; from=<user120@iseplab.local>
to=<1980937@isep.ipp.pt> proto=SMTP helo=<ok.pt>
```

Uma vez efectuado o bloqueio por listas anti-spam e fechado o relay, o teste final é validar se os emails que passam por estas duas protecções sendo spam ou emails com vírus, chegam ou não aos utilizadores da organização. Para efectuar estes testes, foram utilizadas e/ou modificados ficheiros de teste, para simular o envio de emails não fidedignos [23-A]. Para estes ficheiros, os quais se destacam os da figura 73, pode-se consultar, algum código associado com mais detalhe, no anexo 7, no entanto adianta-se as principais caracteristicas:

```
Suse11:~/emails-test # ll
-rw-r--r-- 1 root root 57838 Sep 28 23:59 sample-mail-bomb.txt
-rw-r--r-- 1 root root  1234 Sep 28 23:59 sample-badh.txt
-rw-r--r-- 1 root root  4295 Sep 28 23:59 sample-executable.txt
-rw-r--r-- 1 root root  6494 Sep 28 23:59 sample-nonspam.txt
-rw-r--r-- 1 root root  4656 Sep 28 23:59 sample-spam.txt
-rw-r--r-- 1 root root   799 Aug 25  2003 sample-spam-GTUBE-junk.txt
-rw-r--r-- 1 root root  4530 Sep 28 23:59 sample-virus-executable.txt
-rw-r--r-- 1 root root   178 Sep 28 23:59 sample-virus-simple.txt
Suse11:~/emails-test #
```

Figura 73 – Amostras para simulação de e-mails não fidedignos

a) *Sample-mail-bomb.txt* – Consiste no envio em massa de e-mails ou do mesmo email para o mesmo servidor. Geralmente usado em ataques de DoS, com o intuito de bloqueio do serviço ou apenas para enviar spam para outros endereços.
b) *Sample-badh.txt* – Consiste no envio de um e-mail com um cabeçalho não fidedigno.
c) *Sample-executable.txt* – Consiste no envio de um e-mail com anexo executavel.
d) *Sample-nonspam.txt* – Consiste no envio de um e-mail fidedigno, com ou sem anexos.
e) *Sample-spam.txt* – Consiste no envio de um e-mail como *spam* normal.
f) *Sample-spam-GTUBE-junk.txt* – Consiste no envio de e-mail como *spam Generic Test for Unsolicited Bulk Email* [23-A]
g) *Sample-virus-executable.txt, sample-virus-simple.txt* – Consiste no envio de e-mails com anexos, executáveis ou não, como se fossem vírus.

Apesar de se realizarem testes com todos os ficheiros de simulação acima referidos, sendo os testes realizados com sucesso, apenas serão apresentados 3 testes modelo.

- Como primeiro teste foi enviado para o e-mail do administrador com virus simulado.

```
Suse11:~/emails-test # sendmail -i administrator@caramelo.com < sample-
virus-executable.txt
```

Pelo ficheiro log, verifica-se que o e-mail foi bloqueado no anti-vírus sendo o e-mail reencaminhado para o e-mail de alertas que é o spamdb@caramelo.com.

```
Tail -f /var/log/mail

Sep 29 00:09:07 Suse11 postfix/qmgr[5594]: 70B13ABB68:
from=<virusalert@caramelo.com>, size=2081, nrcpt=1 (queue active)
Sep 29 00:09:07 Suse11 postfix/smtp[6433]: 0A4ECABB6C:
to=<administrator@caramelo.com>, relay=127.0.0.1[127.0.0.1]:10024,
delay=0.63, delays=0.18/0/0.01/0.44, dsn=2.7.0, status=sent (250 2.7.0
Ok, discarded, id=05227-03 - VIRUS: Eicar-Test-Signature)
Sep 29 00:09:07 Suse11 postfix/qmgr[5594]: 0A4ECABB6C: removed

Sep 29 00:09:07 suse11.iseplab.local /usr/sbin/amavisd[5227]: (05227-03)
Blocked INFECTED (Eicar-Test-Signature), <root@suse11.iseplab.local> ->
<administrator@caramelo.com>, quarantine: virus-xN4A+B-srr3f, Message-ID:
<98228.1081981676@example.com>, mail_id: xN4A+B-srr3f, Hits: -, size:
4791, 436 ms

Sep 29 00:09:07 Suse11 postfix/smtp[6446]: 70B13ABB68:
to=<spamdb@caramelo.com>, relay=192.168.100.2[192.168.100.2]:25,
delay=0.22, delays=0.12/0/0/0.09, dsn=2.6.0, status=sent (250 2.6.0
<VAxN4A+B-srr3f@suse11.iseplab.local> Queued mail for delivery)
Sep 29 00:09:07 Suse11 postfix/qmgr[5594]: 70B13ABB68: removed
```

- Como segundo teste foi enviado um e-mail ao administrador com spam.

```
Suse11:~/emails-test # sendmail -i administrator@caramelo.com < sample-
spam-GTUBE-junk.txt
```

Pela análise do ficheiro log, também se verifica que o e-mail é bloqueado, sendo reencaminhado posteriormente para o e-mail de alertas pré-definido.

```
Tail -f /var/log/mail
Sep 29 00:28:44 Suse11 postfix/qmgr[5594]: C2BD1ABB6C:
from=<root@suse11.iseplab.local>, size=941, nrcpt=1 (queue active)
Sep 29 00:28:45 Suse11 postfix/smtpd[6848]: connect from
localhost[127.0.0.1]
Sep 29 00:28:45 Suse11 postfix/smtpd[6848]: 2D977ABB68:
client=localhost[127.0.0.1]
Sep 29 00:28:45 Suse11 postfix/cleanup[6835]: 2D977ABB68: message-
id=<GTUBE1.1010101@example.net>
Sep 29 00:28:45 Suse11 postfix/qmgr[5594]: 2D977ABB68: from=<>,
size=1731, nrcpt=1 (queue active)
Sep 29 00:28:45 Suse11 postfix/smtpd[6848]: disconnect from
localhost[127.0.0.1]
Sep 29 00:28:45 Suse11 postfix/smtp[6843]: C2BD1ABB6C:
to=<administrator@caramelo.com>, relay=127.0.0.1[127.0.0.1]:10024,
delay=0.68, delays=0.25/0.06/0.01/0.36, dsn=2.5.0, status=sent (250 2.5.0
Ok, id=05224-05, DISCARD(bounce.suppressed))
Sep 29 00:28:45 Suse11 postfix/qmgr[5594]: C2BD1ABB6C: removed

Sep 29 00:28:45 suse11.iseplab.local /usr/sbin/amavisd[5224]: (05224-05)
Blocked SPAM, <root@suse11.iseplab.local> ->
<administrator@caramelo.com>, Message-ID: <GTUBE1.1010101@example.net>,
mail_id: NlGosRj5Tjw4, Hits: 1003.022, size: 941, 354 ms

Sep 29 00:28:45 Suse11 postfix/smtp[6852]: 2D977ABB68:
to=<spamdb@caramelo.com>, relay=192.168.100.2[192.168.100.2]:25,
delay=0.27, delays=0.08/0.1/0/0.09, dsn=2.6.0, status=sent (250 2.6.0
<GTUBE1.1010101@example.net> Queued mail for delivery)
Sep 29 00:28:45 Suse11 postfix/qmgr[5594]: 2D977ABB68: removed
```

- Como segundo teste foi enviado um e-mail limpo ao administrador, sem problemas.

```
Suse11:~/emails-test # sendmail -i administrator@caramelo.com < sample-
nonspam.txt
```

Do ficheiro log verifica-se que o e-mail foi enviado para o administrador, passou pelos filtros como e-mail limpo, e foi entregue sem problemas.

```
Tail -f /var/log/mail
Sep 29 00:35:24 Suse11 postfix/qmgr[5594]: CC522ABB68:
from=<root@suse11.iseplab.local>, size=7176, nrcpt=1 (queue active)
Sep 29 00:35:25 Suse11 postfix/smtp[7002]: 939EFABB6C:
to=<administrator@caramelo.com>, relay=127.0.0.1[127.0.0.1]:10024,
delay=15, delays=0.25/0.06/0.01/14, dsn=2.0.0, status=sent (250 2.0.0 Ok:
queued as CC522ABB68)
Sep 29 00:35:25 Suse11 postfix/qmgr[5594]: 939EFABB6C: removed
```

```
Sep 29 00:35:24 suse11.iseplab.local /usr/sbin/amavisd[5227]: (05227-05)
Passed CLEAN, [208.192.102.199] <root@suse11.iseplab.local> ->
<administrator@caramelo.com>, Message-ID:
<v0421010eb70653b14e06@[208.192.102.193]>, mail_id: l-99mqGJpYxu, Hits:
0.704, size: 6713, queued_as: CC522ABB68, 14197 ms

Sep 29 00:35:25 Suse11 postfix/smtp[7028]: CC522ABB68:
to=<administrator@caramelo.com>, relay=192.168.100.2[192.168.100.2]:25,
delay=0.33, delays=0.14/0.08/0.01/0.1, dsn=2.6.0, status=sent (250 2.6.0
<v0421010eb70653b14e06@[208.192.102.193]> Queued mail for delivery)
Sep 29 00:35:25 Suse11 postfix/qmgr[5594]: CC522ABB68: removed
```

Como análise final dos resultados obtidos nos testes realizados, apenas a salientar como se pode verificar nas figuras 73 e 74, que a caixa de correio do utilizador "administrator" e a caixa de correio do utilizador "spamdb" para os testes realizados. Nestas figuras comprova-se que o administrator apenas recebeu o e-mail dito limpo, enquanto que o spamdb recebeu todos os outros emails.

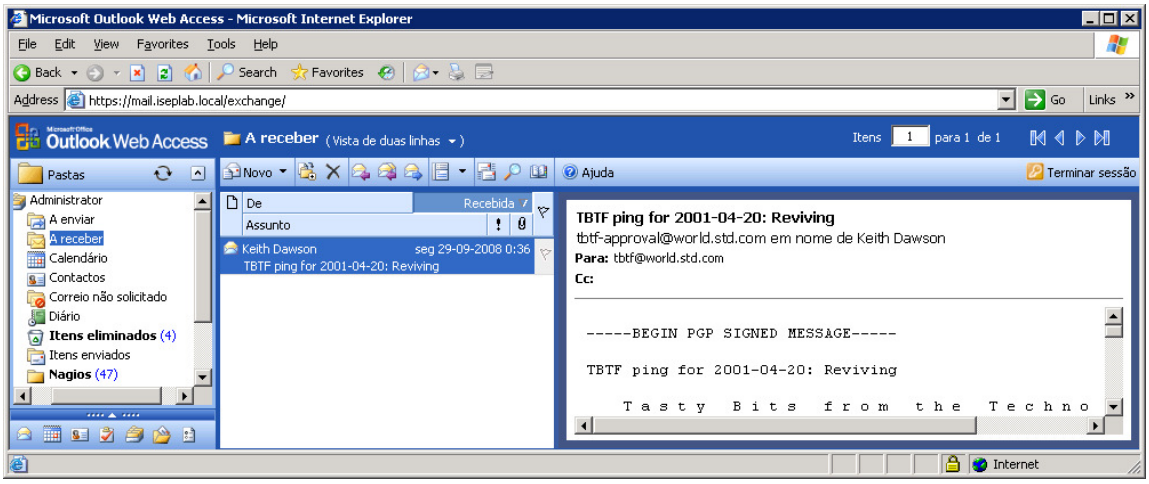


Figura 74 – Caixa de correio do Administrator

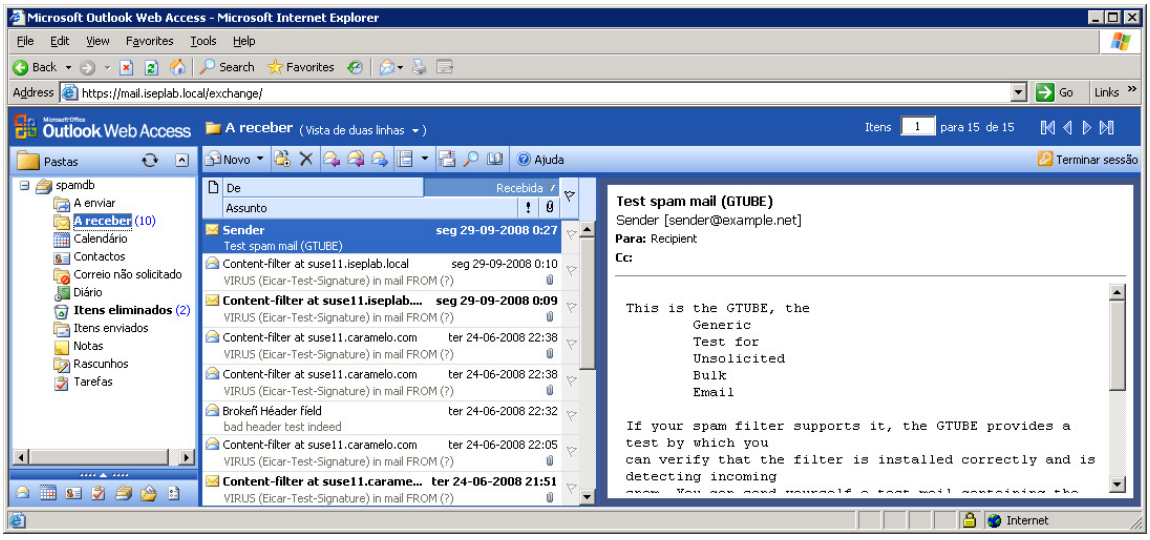


Figura 75 – Caixa de correio do Spamdb

Finalizando, foi verificado o endereço público, quanto à possibilidade de este fazer parte de alguma lista de endereços propícios, a enviar *spam.* Como se verifica na figura 77 esta ocorrencia não se verifica.

Figura 76 – Configurações do Spamcop

6.3.7. ACESSOS A RECURSOS

- **Internos**

Uma vez activa a autenticação no acesso à infraestrutura, quer por cabo Ethernet ou fibra, quer por wireless, significa que os utilizadores que têm acesso à infraestrutura são utilizadores autorizados pela organização.

Pela análise no nmap à firewall verificou-se que os recursos a que os utilizadores têm acesso são o acesso ao proxy (8080) para a internet e as portas 81 e 82, para acesso às estatísticas. Para além disto, tanto os utilizadores da Rede100 como os da Rede130, têm acesso aos recursos que tinham no cenário anterior.

```
nmap -PE  -v -PA21,22,23,80,3389 -sU -T4 -A 192.168.100.254

Scanning 192.168.100.254 [1000 ports]
Discovered open port 8080/tcp on 192.168.100.254
Discovered open port 82/tcp on 192.168.100.254
Discovered open port 81/tcp on 192.168.100.254
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.0 (protocol 2.0)
81/tcp   open   http       Apache httpd 2.2.8 ((Linux/SUSE))
82/tcp   open   ntop-http  Ntop web interface 3.3
113/tcp  closed auth
8080/tcp open   http-proxy DansGuardian HTTP proxy
```

Do ponto de vista da rede o grupo de utilizadores a testar os acessos aos recursos limitados que foram atribuídos é o grupo de utilizadores da Rede120. Estes não têm acesso ao servidor de Exchange, por exemplo, e só têm acessos às portas necessárias no DC, para acesso a DNS e DHCP. Como se pode verificar na leitura seguinte do nmap, apenas aparece como disponível o acesso ao DNS.

```
nmap -PE -v -PA21,22,23,80,3389 -A -T4 dc.iseplab.local
Scanning dc.iseplab.local (192.168.100.1) [1000 ports]
Discovered open port 53/tcp on 192.168.100.1
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS
53/udp    open  domain?
```

- **Externos**

Pode-se também verificar que os acessos a serviços disponibilizados para o exterior são seguros, não sendo possível obter informação confidencial no acesso serviço de *webmail*, como acontecia no cenário 1. Neste novo cenário, foi incluída a protecção por SSL sendo que o acesso ao e-mail está por https. Neste caso, as tentativas para detectar a palavra-passe não tiveram qualquer sucesso.

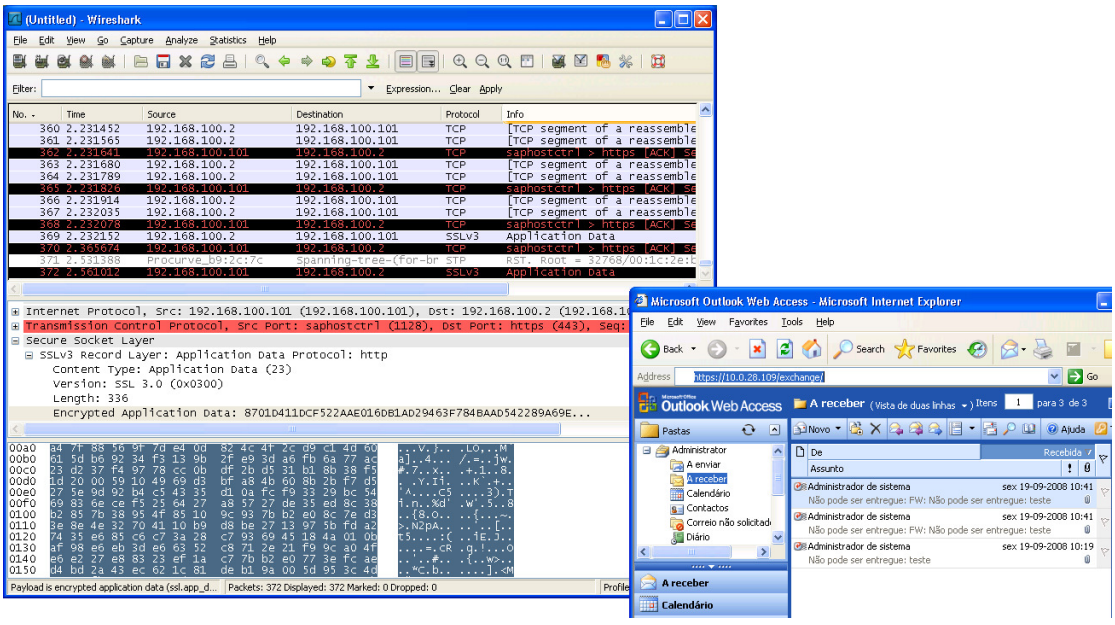


Figura 77 – Obtenção da Conta de Acesso Webmail (Encriptada)

No que se refere ao acesso ao *e-mail*, o servidor de Exchange já não está vulnerável na medida em que, quem responde agora aos pedidos externos é o Suse11 com o Postfix, possuindo este, já as devidas protecções, mas esse ponto será abordado posteriormente. Na figura seguinte, pode-se verificar o teste de acesso via smtp ao endereço externo, obtendo-

se como resposta, o postfix com "banner" de *Lotus Notes*. Este descrição falsa do servidor de e-mail, deve-se ao facto de que em determinadas situções, é suficiente para desviar a base dos ataques, para o sistema que não é o existente.

Figura 78 – Acesso ao servidor de e-mail

Em relação ao serviço de FTP, como é um serviço disponibilizado para utilizadores externos à organização, manteve-se o acesso ao serviço, do modo dito como inseguro, mas deslocado para a DMZ, estando disponível apenas do exterior. Esta movimentação leva a garantir a integridade da segurança da rede interna.

- **Abuso de Recursos**

Uma das vulnerabilidades do cenário anterior era o abuso de recursos por parte dos utilizadores, nomeadamente o acesso à internet. Com a implementação das várias soluções, firewall, vlan's, só falta efectuar os testes de acesso aos recursos de internet via proxy (192.168.100:8080).

Pelos testes efectuados, foi verificado que só os utilizadores com permissões de acesso à internet, são os que realmente conseguem aceder, caso contrário o acesso é negado. Com a utilização de um utilizador sem premissões de acesso, como se verifica na figura seguinte, o acesso foi negado.

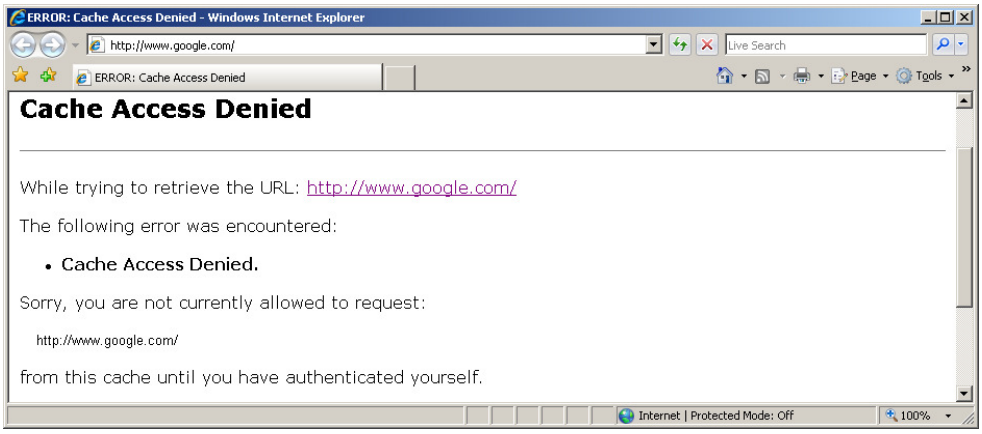


Figura 79 – Acesso negado à internet

No entanto os utilizadores privilegiados ainda têm que passar pelo controlo de conteúdos, e para isso, fez-se uma pesquisa em www.google.com pela paravra “sex” ou “sexo” obtendo-se o seguinte resultado como mostra a figura 81. O verificado foi que o conteúdo foi bloqueado, sendo essa informação reportada ao utilizador.

Figura 80 – Acesso autorizado à internet

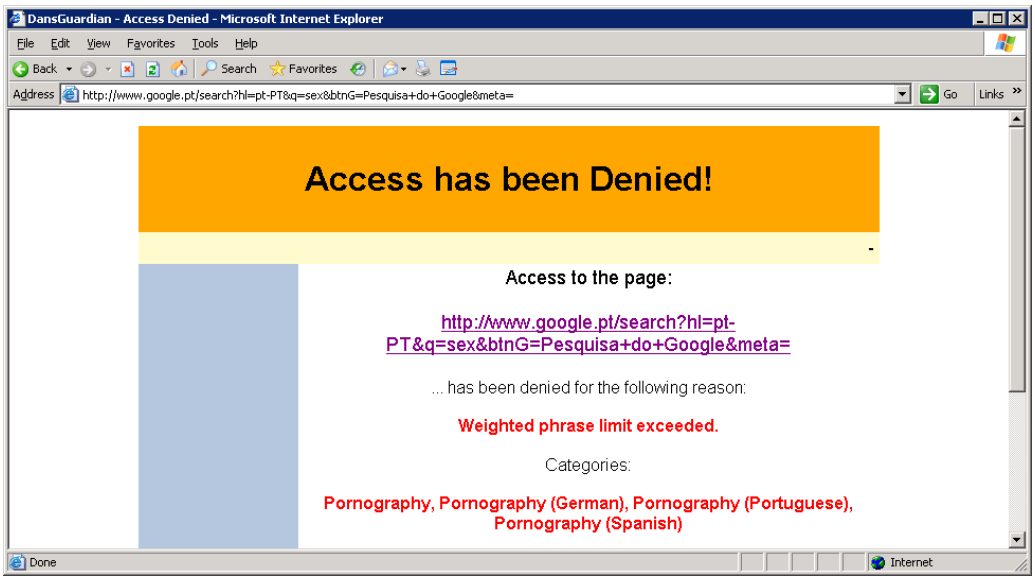


Figura 81 – Bloqueio de Conteúdos

A filtragem de conteúdos tem que estar actualizada, uma vez que todos os dias vão aparecendo novas páginas de conteúdos dúvidosos. Para actualizar esta filtragem, os administradores conseguem, através do controlo de acessos através do interface Web, analisar quais os sites mais acedidos, quais as estatísticas de acesso, de forma a bloquear eventuais sites, que estejam a passar despercebidos da políticas de bloqueio de conteúdos.

Um exemplo de acesso às estatísticas de controlo de acessos pode ser verificado na figura seguinte.

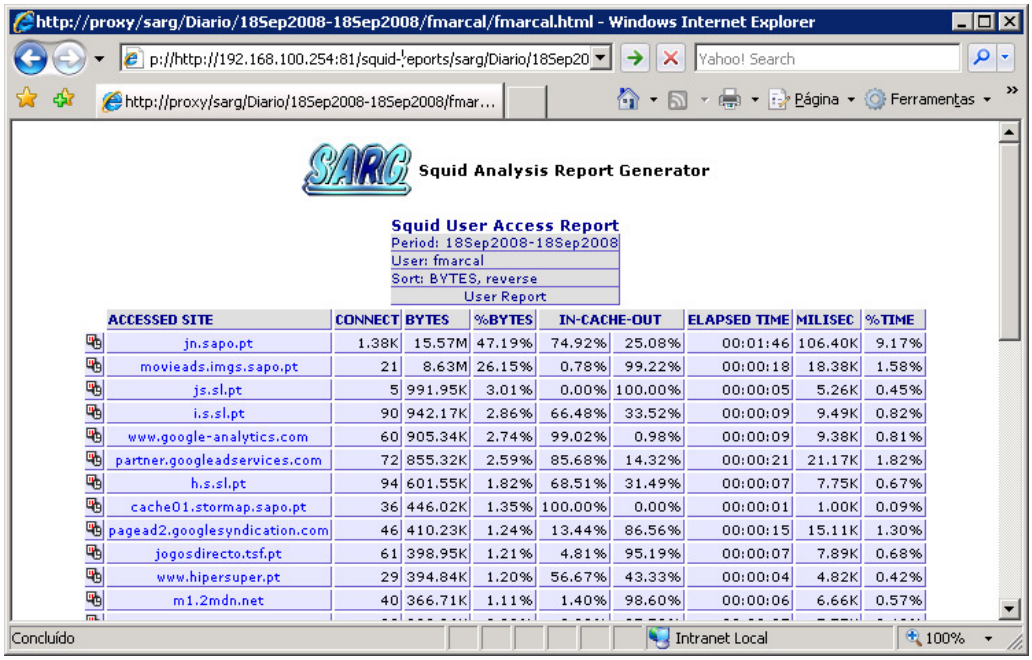


Figura 82 – Estatísticas de controlo de acessos.

Finalmente, com o controlo e filtragem de *e-mail* e com implementação do controlo de acessos e conteúdos implementados foi verificado que a largura de faixa utilizada no acesso à internet, diminuiu consideravelmente. Isto fez com que a qualidade de serviço, para o exterior, e do exterior melhore consideravelmente, sem serem necessários investimentos, em novas linhas de comunicações ou aumento da largura de faixa das existentes, como se verifica com nova análise com o *iptraf*.

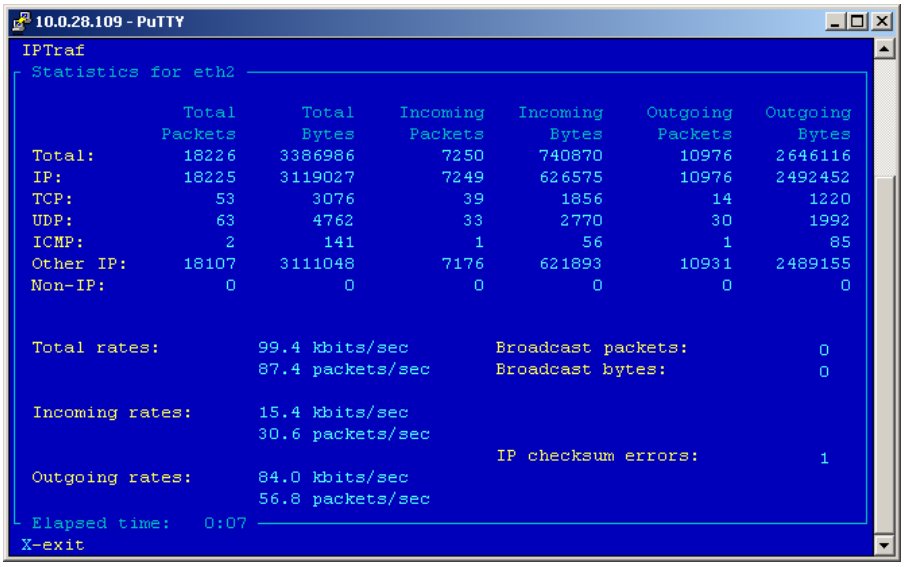


Figura 83 – Estatísticas de análise de tráfego.

No entanto, o acesso ao *iptraf* requer uma ligação ao servidor via ssh, e para administradores terem acesso a um leque de informação mais detalhada, foi desenvolvido um interface Web, podendo ser gerados relatórios de tráfego mais pormenorizados. O acesso a este interface é pelo "Relatório de tráfego".

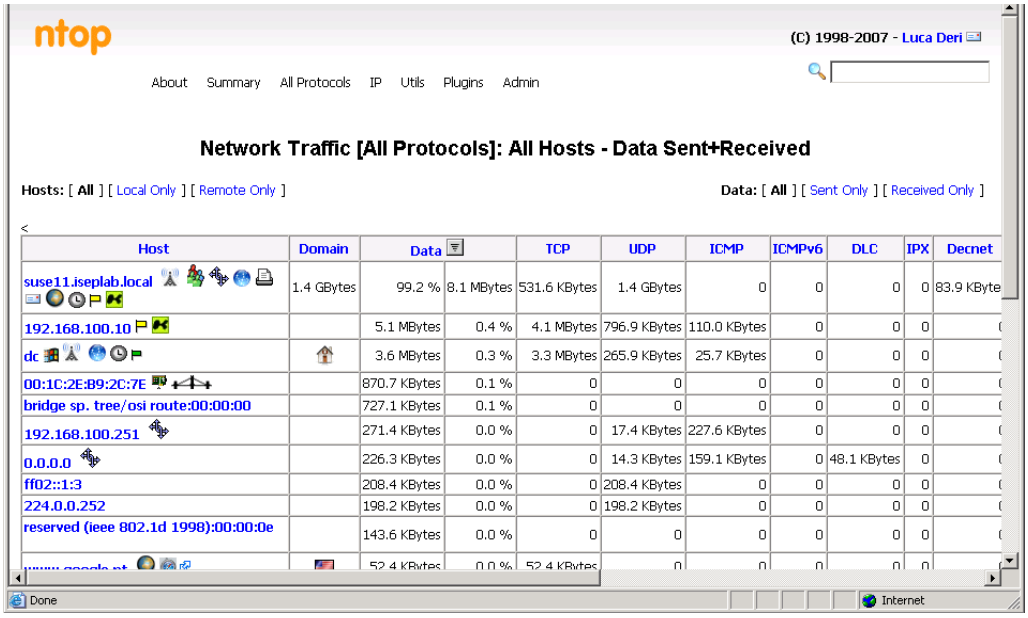


Figura 84 – relatório de análise de tráfego.

6.3.8. ACESSOS REMOTOS.

Uma vez que alguns utilizadores e/ou administradores, utilizavam o acesso RDP e ssh do exterior para aceder aos equipamentos no interior, verificou-se que agora estes serviços neste capítulo foram encapsulados numa VPN. Deste modo mantendo a mesma metodologia no acesso, garante-se confidencialidade e segurança na transferência dos dados.

Para realizar os testes, foi utilizado um posto modelo, instalado o openvpngui, copiado o certificado e ficheiro de configuração cliente, como se verifica na figura 85.

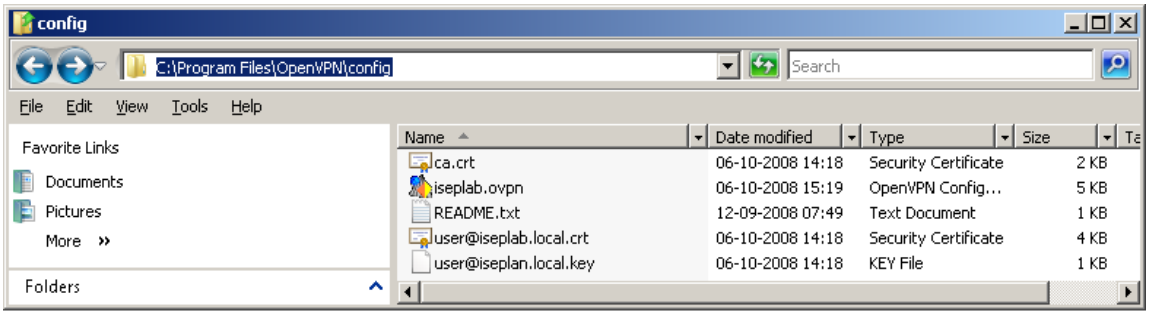


Figura 85 – Configuração do cliente openvpn.

Depois de configurado o acesso aliente, verifica-se o acesso à infraestrutura com sucesso, de modo seguro, como podemos verificar na figura 86.

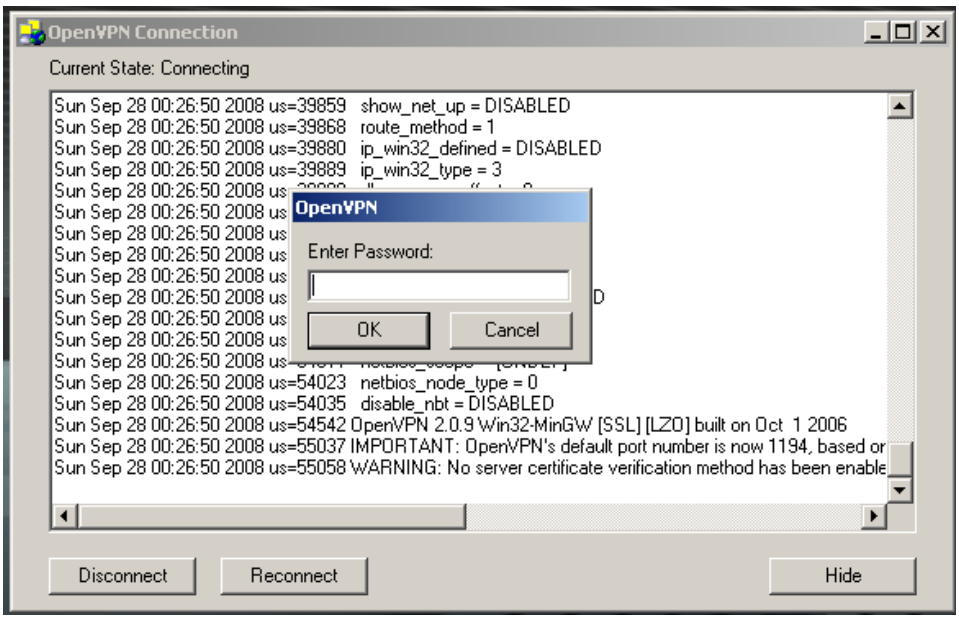


Figura 86 – Ligação por openvpn.

6.4. RESUMO

Este capítulo é de certa forma o culminar de toda uma investigação que incluiu dezenas de testes efectuados ao sistema, com o objectivo final de garantir – com o maior grau de confiança possível – uma elevada segurança para o sistema, para a informação que nele circula, e para os seus utilizadores.

Neste capítulo é possível verificar a fundo todo o *software* utilizado no caso de estudo e comprovar através de testes efectuados à rede (simulações de ataques), o estado da segurança, e as melhorias encontradas (optimização de configurações e correcção de vulnerabilidades) face a um sistema que não recorra às medidas de segurança aqui definidas. Todos os passos de implementação e configuração da rede foram enunciados de modo a que seja possível perceber o funcionamento, as regras e métodos actuais para a implementação correcta de segurança num sistema informático em rede. Em concreto, foram descritas as comfigurações óptimas para servidores, postos de trabalho e referenciadas políticas e protocolos de segurança. Foi verificada a protecção acrescida das redes *ethernet* e *wi-fi*, através de proteções 802.1x, e ainda a estruturação de permissões, chaves de acesso, e filtragem de e-mail (*spamhaus*), anti-vírus (*e-Trust*), *firewall* (*shorewall*) e VPN *(openvpn),* para uma protecção máxima de todo sistema.

7. CONCLUSÕES

A segurança é um dos conceitos mais debatidos na actualidade. No caso da informática e electrónica é um problema em constante mutação, mas também é um problema da sociedade, e é fácil criar relações de semelhança entre a vida e os computadores. Muitos dos algoritmos de segurança implementados por reconhecidos programadores, surgem de ideias que partem desde os métodos de combate romanos, até aos métodos de ataque de grupos de crime organizado. A crescente interligação de pessoas e sistemas cria novos factores de risco, mas em muitos casos, as soluções já foram inventadas, bastando agora adaptá-las a esta realidade virtual.

Num meio ideal, teriamos um computador numa casa blindada, com protecção contra terramotos, incêncios, cheias, roubos e furacões. E ainda assim a informação estaria completamente insegura, bastando para isso conectar um cabo, com uma extremidade na placa de rede, e a outra num meio de acesso à internet.

Esta realidade é bem conhecida. O ser humano não pode saír de casa sem se colocar automaticamente em risco, tal são os perigos (queda de aviões, acidentes de automóvel,

roubos, etc.). No entanto, tudo isto surge como um mal menor, tal é a necessidade que temos de "viver".

A partir do momento que temos uma organização, temos necessidade de a publicitar, e automaticamente temos proveitos e riscos inerentes. E infelizmente, quando tudo isto envolve o campo da segurança informática, nenhum sistema é 100% fiável.

Alguns dos pontos fulcrais de segurança, verificados durante este projecto, são enunciados de seguida.

Administração de Sistemas de Redes:

- Definir palavra-chave de administrador no Sistema Operativo;

- Definir expiração de palavras-chave para contas de utilizador;

- Activar filtros *spam* e filtros de conteúdos para web e webmail;

- Activar e actualizar anti-vírus e firewall em servidores e clientes;

- Executar periodicamente software de actualização de sistema e anti-vírus para manter as máquinas seguras a novas ameaças;

- Manter e consultar diariamente registos (*logs*) dos eventos do sistema e definir políticas de segurança e de pró-actividade no sistema;

- Definir listas de acesso, bloqueando e/ou desactivando serviços e portas não usados;

- Procurar definir áreas desmilitarizadas, separando a rede global (internet) da rede interna, através de canais de protecção extra;

- Formar utilizadores na perspectiva dos perigos da execução indiscrimidada de software e execução de arquivos recebidos via e-mail, ou pedidos exteriores de palavras-passe ou quaisquer tipos de códigos especiais (ataques engenharia social);

- Implementar soluções seguras na disponibilização de serviços, protegendo com protocolos, canais de comunicação seguros, e encriptando a informação.

Palavras-chave seguras (utilizadores e/ou administradores):

- Não usar chaves visíveis, que se possam encontrar físicamente (marca do pc, etc.);

- Não usar contextos pessoais, como nomes de pessoas, datas importantes (aniversários, etc.), nomes de animais de estimação, entre outros.

- Não usar informação pessoal conhecida por outros;

- Não divulgar a terceiros ou escrever em papel ou formato digital (usar palavra que seja fácil de lembrar, para não levar a que se escreva);

- Procurar usar simultâneamente, letras, números e caracteres especiais ("@", "_", "$"), e acima de um total de 5 caracteres.

Segurança em redes Wifi:

Qualquer tipo de segurança é melhor do que nenhuma. No entanto dever-se-à usar a que mais se adequa à rede em questão, tendo as seguintes noções:

- Protocolos por ordem de decrescente de nível de protecção: 802.1x, WPA2, WPA, WEP;

- Tentar limitar o nível de sinal aos trâmites físicos do espaço empresarial;

- Usar chaves complexas e alterá-las periodicamente;

7.1. OBJECTIVOS REALIZADOS

Este projecto foi em simultâneo uma aposta nas componentes teórica e prática da segurança informática da actualidade. Tentou-se relatar, nos Capítulos 1 e 2, a situação actual dos sistemas em rede, e dos perigos a que estão sujeitos, bem como de possíveis soluções.

Nos Capítulos 3, 4 e 5 é feito um levantamento de soluções baseadas em regras, métodos e aplicações que permitem orientar o sistema e os seus intervenientes a obter o maior nível de segurança possível, colocando por vezes em contraponto, o elevado controlo (excesso de zelo) com a desmedida "liberdade" do utilizador.

O Capítulo 6 é bastante importante tendo em conta o âmbito deste trabalho. A situação de um Administrador de Sistemas é ao mesmo tempo, previligiada, e de grande responsabilidade, e independentemente das aplicações usadas serem *open source* ou proprietárias, ou se os utilizadores têm formação informática elevada ou não, a realidade é que a segurança do sistema depende do administrador do mesmo, e uma má configuração ou a despreocupação com o que acontece na rede pode ter consequências terríveis.

Os Capítulos 7 e 8 estão relacionados com a implementação de um caso prático de um sistema informático em rede, com diversos dispositivos e meios de interligação, bem como aplicações oriundas de fabricantes diferentes. Esta heterogeneização do sistema permite encontrar um número de potenciais falhas e/ou perigos relativamente maior, e em simultâneo, leva a uma clara comparação das diversas ferramentas de administração de redes disponíveis no mercado. No Capítulo 7 em particular, é feita uma caracterização de todo o sistema, e da sua interligação física (ao nível da cablagem e posição geográfica) e lógica (configurações da rede, meios de acesso, redes virtuais, entre outros). Ainda neste capítulo irão verificar-se situações de falha de segurança, mediante testes efectuados à rede, através uso de ferramentas comuns, ora para garantir a segurança (*updates*, anti-vírus, anti-spam), ora para verificar a falta desta (decifragem de chaves Wi-Fi, detecção de *login's* de utilizador, captura de tráfego, etc.). Todas as falhas reportadas neste capítulo (e outras por acréscimo) serão corrigidas numa implementação segura desta rede, definida no Capítulo 8.

7.2. LIMITAÇÕES & TRABALHO FUTURO

Este trabalho foi pautado com algumas limitações nomeadamente na área de simulação do ISP (operador de internet).

De referir também que o facto de, alguns equipamentos serem consignados, levou a alguma demora no desenvolvimento de testes de segurança interna da infraestrutura. Por outro lado, alguns testes tiverem que ser repetidos, com novos equipamentos, já que alguns destes equipamentos consignados, tiveram que ser devolvidos ou substituídos.

Finalisando a nível de limitações existentes, foram o facto de algumas aplicações terem sido utilizadas como versões demonstrativas, sendo necessária a sua reinstalação passado algum tempo.

Como trabalho futuro, numa primeira fase, ficou a análise estatística dos resultados obtidos e implementação do acesso seguro ao servidor web *apache* usando SSL ou implementação de envio / recepção de e-mail via SSL com o exterior.

7.3. APRECIAÇÃO FINAL

O trabalho desenvolvido durante a execução desta tese teve um pouco de gosto pessoal associado, dada área em que o tema se enquadra. Isto por si só, permitiu trabalhar com afinco e vontade de produzir uma solução completa e pormenorizada de um assunto actual, e de uma preocupação para o futuro. Infelizmente, a variável "tempo" não esteve propriamente a favor, na medida em que determinados assuntos ainda ficaram por referir, como:

- A utilização do *ProCurve Manager Plus* para a gestão e monitorização dos equipamentos da rede, em sistemas Microsoft, em detrimento do *nagios*;
- Implementação de uma solição de e-mail seguro *(smtps)*

Bibliografia

[1] Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, “Network Security Bible”, Wiley, 2005.

[2] Internet Security Lectures by Prabhaker Mateti http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/Top/index.html

[3] DNS and BIND, Fifth Edition By Paul Albitz, Cricket Liu May 2006

[4] CISCO CCSP SECUR, Greg Bastien, Christian Abera Degu Copyright© 2004 Cisco Systems, Inc.

[5] Eric Vyncke and Christopher Paggen, CCIE No. 2659, “LAN Switch Security: What Hackers Know About Your Switches”.

[6] http://technet.microsoft.com/en-us/wsus/default.aspx

[7] *Building Internet Firewalls, 2nd Edition*. Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman. O’Reilly & Associates, 2000.

[8] Chris McNab, “Network Security Assessment”, O’Reilly, Março 2004.

[9] Chris Hare, Karanjit Siyan, “Internet Firewalls And Network Security”, E-Book.

[10] Madjid Nakhjiri, Mahsa Nakhjiri, “AAA and Network Security for Mobile Access”.

[11] Mike De Leo, Cisco Networkers, “Securing 802.11 Wireless Networks”.

[12] Mike D. Schiffman, “Building Open Source Network Security Tools: Components and Techniques”.

[13] Morgan Kaufmann, “Information.Assurance”, Novembro 2007.

[14] Cisco, “Network Security Policy: Best Practices White Paper”, 2003.

[15] Andrew Lockhart, “Network Security Hacks”, O’Reilly, Abril 2004.

[16] Pravir Chandra, Matt Messier, John Viega, “Network Security with OpenSSL”, O’Reilly, Junho 2002.

[17] Jaime Dias, http://paginas.fe.up.pt/~jaime/0506/SSR/SSR.htm
Jaime Dias, http://paginas.fe.up.pt/~jaime/

[18] Shorewall Firewall, http://www.shorewall.net/
Fwanalog, http://tud.at/programm/fwanalog/

[19] Squid, http://www.squid-cache.org/

[20] Dansguardian, http://dansguardian.org/

[21] Sarg, http://sarg.sourceforge.net/

[22] Apache, http://www.apache.org/

[23] Postfix, http://www.postfix.org/, Amavis, http://www.amavis.org/
Spamassassin, http://spamassassin.apache.org/, Clamav, http://www.clamav.net/

[23-A] http://spamassassin.apache.org/gtube/, http://www.ijs.si/software/amavisd/

[24] Nagios, http://www.nagios.org/

[25] Ntop, http://www.ntop.org/
Iptraf, http://iptraf.seul.org/

[26] Ca anti-virus, http://www.ca.com/us/products/product.aspx?id=156

[27] MBSA, http://technet.microsoft.com/en-us/security/cc184924.aspx

[28] OpenVpn, http://openvpn.net/

[29] Outlook Express Security Update: VCard Buffer Overflow
http://www.microsoft.com/downloadS/details.aspx?familyid=7B1BC6BB-AA2E-48F5-BBBF-0F5F53FA2205&displaylang=en

[30] NIST, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, Sheila Frankel Bernard Eydt Les Owens Karen Scarfone

[31] Prentice Hall, “Intrusion Detection With Snort”, O’Reilly, 2006.

Anexo 1 SHOREWALL

1. Foi efectuado o download dos pacotes em http://www.shorewall.net/download.htm, sendo posteriormente instalados.

```
Suse11:~# rpm -ivh shorewall-common-4.0.11-0base.noarch.rpm
Preparing...                ########################################### 
[100%]
package shorewall-common-4.0.11-0base.noarch.rpm installed

Suse11:~# rpm -ivh shorewall-shell-4.0.11-0base.noarch.rpm
Preparing...                ########################################### 
[100%]
package shorewall-shell-4.0.11-0base.noarch.rpm installed
```

2. Configuração dos interfaces

```
Vi /etc/shorewall/interfaces  // Configuração dos interfaces
#############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
lan     eth0    detect
dmz     eth1    detect
wan     eth2    detect
lan     ppp+    -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

3. Configuração das políticas de segurança por defeito

```
Vi /etc/shorewall/policy
#############################################################################
#SOURCE                 DEST                        POLICY                  LOG
LIMIT:BURST
#                                                   LEVEL
#dmz            all             DROP            info
#lan            all             DROP            info
#wan            all             DROP            info       10/sec:10
#all            all             DROP            info
all             all             ACCEPT          info
#LAST LINE -- DO NOT REMOVE
```

4. Arranque dos serviços

```
Vi /etc/shorewall/shorewall.conf
#                       S T A R T U P   E N A B L E D
#############################################################################
STARTUP_ENABLED=yes
#############################################################################
```

```
#                                 L O G G I N G
###############################################################################
LOGFILE=/var/log/firewall
LOGFORMAT="Shorewall:%s:%s:"
LOGTAGONLY=No
```

5. Definição das zonas de firewall

```
Vi /etc/shorewall/zones
###############################################################################
#ZONE   TYPE          OPTIONS        IN                    OUT
#                                       OPTIONS
fw      firewall
lan     ipv4
wan     ipv4
dmz     ipv4
vpn     ipv4
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

6. A nível de pedidos externos de *e-mail* (porta 25) *e webmail* (porta 80) são encaminhados directamente para o servidor interno, que neste caso é o mail.iseplab.local, no ficheiro rules para o primeiro cenário.

```
Vi /etc/shorewall/rules
#############################################################################
#ACTION  SOURCE   DEST        PROTO DEST    SOURCE       ORIGINAL
#                                      PORT    PORT(S)    DEST
## Acessos para SMTP e Webmail
DNAT     wan            lan:192.168.100.2       tcp     25      -
DNAT     wan            lan:192.168.100.2       tcp     http      -

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para o Segundo cenário temos o seguinte ficheiro rules

```
#ACTION   SOURCE            DEST                  PROTO    DEST      SOURCE
ORIGINAL
#                                                 PORT    PORT(S)    DEST
# REGRAS DE DNS
ACCEPT  lan:192.168.100.1               wan             udp     53      -
ACCEPT  fw              lan:192.168.100.1               udp     53      -
ACCEPT  fw              wan                             udp     53      -
ACCEPT  wan             dmz:192.168.20.1                tcp     53      -
ACCEPT  dmz:192.168.20.1                wan             tcp     53      -
ACCEPT  dmz             lan:192.168.100.1               udp     53      -
## SMTP - EMAIL
ACCEPT          wan                     fw              tcp     25      -
ACCEPT          fw                      wan             tcp     25      -
ACCEPT         fw                     lan:192.168.100.2  tcp     25      -
ACCEPT          lan:192.168.100.2       fw              tcp     25      -
# OWA - EXCHANGE
DNAT    wan             lan:192.168.100.2        tcp    https   -
# Acesso FTP
DNAT    wan             dmz:192.168.20.1        tcp    ftp     -
ACCEPT  wan             fw                      tcp     ftp     -
ACCEPT  fw              wan                     tcp     ftp     -
ACCEPT  fw              dmz                     tcp     ftp     -
ACCEPT  dmz             wan                     tcp     ftp     -
```

```
# ACCESSOS http,https,squid,ftp
#REDIRECT lan           8080                    tcp     www     -
ACCEPT  lan             fw                      tcp     81      -
ACCEPT  lan             fw                      tcp     82      -
ACCEPT  lan             fw                      tcp     8080    -
ACCEPT  lan:192.168.100.1       fw                      tcp     3128    -
ACCEPT  lan:192.168.100.2       fw                      tcp     3128    -
ACCEPT  fw              wan                     tcp   http,https,ftp    -
ACCEPT  wan             fw                      tcp   http,https,ftp   -
# ACCESSOS da ldap
ACCEPT  fw              lan:192.168.100.1       tcp     3268    -
# TIME SERVER
ACCEPT  lan:192.168.100.1       wan     tcp     13
# ICMP - PINGS
ACCEPT  lan             lan             icmp    -
ACCEPT  lan             fw              icmp    -
ACCEPT  fw              lan             icmp    -
ACCEPT  fw              dmz             icmp    -
ACCEPT  fw              wan             icmp    -
ACCEPT  lan             wan             icmp    -
ACCEPT  wan             lan             icmp    -
ACCEPT  wan             fw              icmp    -
```

7. Serviços Start / Stop / Restart

```
Suse11:~# /etc/rc.d/shorewall stop
Suse11:~# /etc/rc.d/shorewall start
Suse11:~# /etc/rc.d/shorewall restart
Suse11:~# /etc/rc.d/shorewall status
```

8. Logs

```
Suse11:~# tail –f /var/log/firewall
```

Anexo 2 SARG

Código para gerar os relactorios para o SARG,

```
Vi /usr/sbin/sarg-reports
# TEMP Files
TMPFILE=/tmp/sarg-reports.$RANDOM
 ERRORS="${TMPFILE}.errors"

# Date Calc
MANUALDATE=$2
case "$(uname)" in
"FreeBSD")
         TODAY=$(date +%d/%m/%Y)
     YESTERDAY=$(date -v-1d +%d/%m/%Y)
       WEEKAGO=$(date -v-1w +%d/%m/%Y)
      MONTHAGO=$(date -v-1m +01/%m/%Y)-$(date -v-1m +31/%m/%Y)
   ;;
"OpenBSD")
         TODAY=$(date +%d/%m/%Y)
     YESTERDAY=$(date -r $((`date +%s` - 86400 )) +%d/%m/%Y)
       WEEKAGO=$(date -r $((`date +%s` - 604800)) +%d/%m/%Y)
      MONTHAGO=$(perl -e '@t=localtime(time); $y=$t[4]==0?$t[5]+1899:$t[5]+1900;
$m=$t[4]==0?12:$t[4]; print "1/$m/$y-
",$m==2?$y%4>0?28:29:$m==4||$m==6||$m==9||$m==11?30:31 ,"/$m/$y\n";')
   ;;
*)
         TODAY=$(date --date "today" +%d/%m/%Y)
     YESTERDAY=$(date --date "1 day ago" +%d/%m/%Y)
       WEEKAGO=$(date --date "1 week ago" +%d/%m/%Y)
      MONTHAGO=$(date --date "1 month ago" +01/%m/%Y)-$(date --date "1 month ago"
+31/%m/%Y)
   ;;
esac

export LC_ALL=C

# Main index.html creation
create_index_html ()
{
  echo -e "\
  <html>\n\
  <head>\n\
  <title>$PAGETITLE</title>\n\
  </head>\n\
  <body>\n\
  <div align=center>\n\
    <a href=$LOGOLINK><img border=0 src=$LOGOIMG></a>\n\
    <table border=0 cellspacing=6 cellpadding=7>\n\
      <tr>\n\
        <th align=center nowrap><b><font face=Arial size=4
color=green>$PAGETITLE</font></b></th>\n\
      </tr>\n\
      <tr>\n\
        <td align=center bgcolor=beige><font face=Arial size=3><a
href=$DAILY>$DAILY</a></font></td>\n\
      </tr>\n\
      <tr>\n\
```

```
        <td align=center bgcolor=beige><font face=Arial size=3><a
href=$WEEKLY>$WEEKLY</a></font></td>\n\
      </tr>\n\
      <tr>\n\
        <td align=center bgcolor=beige><font face=Arial size=3><a
href=$MONTHLY>$MONTHLY</a></font></td>\n\
      </tr>\n\
    </table>\n\
  </div>\n\
  </body>\n\
  </html>" > $HTMLOUT/index.html
}

# Functions
exclude_from_log ()
{
  cat $ERRORS | grep -v "$EXCLUDELOG1" | grep -v "$EXCLUDELOG2"
  rm -f $TMPFILE*
}

manual ()
{
  DAILYOUT=$HTMLOUT/$DAILY
  mkdir -p $DAILYOUT
  create_index_html
  if [ -z "$MANUALDATE" ]
    then
      echo "No date given, please specify a valid date (DD/MM/YYYY)"
    else
      $SARG -f $CONFIG -d $MANUALDATE -o $DAILYOUT
  fi
}

today ()
{
  DAILYOUT=$HTMLOUT/$DAILY
  mkdir -p $DAILYOUT
  create_index_html
  $SARG -f $CONFIG -d $TODAY -o $DAILYOUT >$ERRORS 2>&1
  exclude_from_log
}

daily ()
{
  DAILYOUT=$HTMLOUT/$DAILY
  mkdir -p $DAILYOUT
  create_index_html
  $SARG -f $CONFIG -d $YESTERDAY -o $DAILYOUT >$ERRORS 2>&1
  exclude_from_log
}

weekly ()
{
  WEEKLYOUT=$HTMLOUT/$WEEKLY
  mkdir -p $WEEKLYOUT
  create_index_html
  $SARG -f $CONFIG -d $WEEKAGO-$YESTERDAY -o $WEEKLYOUT >$ERRORS 2>&1
  exclude_from_log
}

monthly ()
{
  MONTHLYOUT=$HTMLOUT/$MONTHLY
  mkdir -p $MONTHLYOUT
  create_index_html
  $SARG -f $CONFIG -d $MONTHAGO -o $MONTHLYOUT >$ERRORS 2>&1
  exclude_from_log
}
```

```
case $1 in
    manual)
        manual
        ;;
    today)
        today
        ;;
    daily)
        daily
        ;;
    weekly)
        weekly
        ;;
    monthly)
        monthly
        ;;
   esac
```

Anexo 3 DANSGUARDIAN

```
vi /etc/dansguardian/lists/bannedextensionlist
#Banned extension list
# File extensions with executable code
# The following file extensions can contain executable code.
# This means they can potentially carry a virus to infect your computer.
.ade  # Microsoft Access project extension
.adp  # Microsoft Access project
.asx  # Windows Media Audio / Video
.bas  # Microsoft Visual Basic class module
.bat  # Batch file
.cab  # Windows setup file
.chm  # Compiled HTML Help file
.cmd  # Microsoft Windows NT Command script
.com  # Microsoft MS-DOS program
.cpl  # Control Panel extension
.crt  # Security certificate
.dll  # Windows system file
.exe  # Program
.hlp  # Help file
.ini  # Windows system file
.hta  # HTML program
.inf  # Setup Information
.ins  # Internet Naming Service
.isp  # Internet Communication settings
```

Anexo 4 FREERADIUS

Neste anexo apresenta-se as configurações do Freeradius para que seja possível a autenticação dos utilizadores associados a cada VLAN com integração com a directoria activa da Microsoft pelo controlador do domínio.

/etc/raddb/clients.conf

```
client 127.0.0.1 {
      secret = !QAZ2wsx
      shortname = localhost
}
client 192.168.100.251 {
      secret = !QAZ2wsx
      shortname = 192.168.100.251
}
client 192.168.100.253 {
      secret = !QAZ2wsx
      shortname = 192.168.100.253
}
```

/etc/raddb/eap.conf

```
eap {
        default_eap_type = peap
        timer_expire = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = yes
        tls {
                private_key_password = whatever
                private_key_file = ${raddbdir}/certs/cert-srv.pem
                certificate_file = ${raddbdir}/certs/cert-srv.pem
                CA_file = ${raddbdir}/certs/demoCA/cacert.pem
                dh_file = /dev/null
                random_file = /dev/urandom
                fragment_size = 1024
```

```
                include_length = yes
        }
        peap {
                default_eap_type = mschapv2
        }
        mschapv2 {
        }
}
```

/etc/raddb/users

```
DEFAULT NAS-Port-Type == "Wireless-802.11", Ldap-Group == "lan"
      Service-Type = "Framed",
      Tunnel-Type = 13,
      Tunnel-Medium-Type = 6,
      Tunnel-Private-Group-Id = 1,
      Reply-Message = "%u WIFI Auth OK - VLAN 1"
DEFAULT NAS-Port-Type == "Ethernet", Ldap-Group == "lan"
      Service-Type = "Framed",
      Tunnel-Type = 13,
      Tunnel-Medium-Type = 6,
      Tunnel-Private-Group-Id = 1,
DEFAULT NAS-Port-Type == "Ethernet", Ldap-Group == "Rede120"
      Service-Type = "Framed",
      Tunnel-Type = 13,
      Tunnel-Medium-Type = 6,
      Tunnel-Private-Group-Id = 2,
DEFAULT NAS-Port-Type == "Ethernet", Ldap-Group == "Rede130"
      Service-Type = "Framed",
      Tunnel-Type = 13,
      Tunnel-Medium-Type = 6,
      Tunnel-Private-Group-Id = 3,
```

/etc/raddb/radiusd.conf

```
prefix = /usr
exec_prefix = ${prefix}
sysconfdir = /etc
localstatedir = /var
sbindir = ${exec_prefix}/sbin
logdir = ${localstatedir}/log/radius
```

```
raddbdir = ${sysconfdir}/raddb
radacctdir = ${logdir}/radacct
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/radiusd
log_file = ${logdir}/radius.log
libdir = /usr/lib/freeradius
pidfile = ${run_dir}/radiusd.pid
user = radiusd
group = radiusd
max_request_time = 30
delete_blocked_requests = no
cleanup_delay = 5
max_requests = 1024
bind_address = 10.13.10.253
port = 0
hostname_lookups = no
allow_core_dumps = no
regular_expressions     = yes
extended_expressions    = yes
log_stripped_names = no
log_auth = yes
log_auth_badpass = no
log_auth_goodpass = no
usercollide = no
lower_user = no
lower_pass = no
nospace_user = no
nospace_pass = no
checkrad = ${sbindir}/checkrad
security {
      max_attributes = 200
      reject_delay = 1
      status_server = no
}
proxy_requests  = yes
$INCLUDE  ${confdir}/proxy.conf
$INCLUDE  ${confdir}/clients.conf
snmp = no
$INCLUDE  ${confdir}/snmp.conf
thread pool {
```

```
        start_servers = 5
        max_servers = 32
        min_spare_servers = 3
        max_spare_servers = 10
        max_requests_per_server = 0
}
modules {
        $INCLUDE ${confdir}/eap.conf
        mschap {
                authtype = MS-CHAP
                with_ntdomain_hack = yes
        }
        checkval {
                item-name = Calling-Station-Id
                check-name = Calling-Station-Id
                data-type = string
        }
        preprocess {
                huntgroups = ${confdir}/huntgroups
                hints = ${confdir}/hints
                with_ascend_hack = yes
                ascend_channels_per_line = 23
                with_ntdomain_hack = no
                with_specialix_jetstream_hack = no
                with_cisco_vsa_hack = no
        }
        files {
                usersfile = ${confdir}/users
                acctusersfile = ${confdir}/acct_users
                preproxy_usersfile = ${confdir}/preproxy_users
                compat = no
        }
        detail {
                detailfile   =   ${radacctdir}/%{Client-IP-Address}/detail-
%Y%m%d
                detailperm = 0600
        }
        acct_unique {
                key = "User-Name, Acct-Session-Id, NAS-IP-Address, Client-
IP-Address, NAS-Port"
        }
```

```
radutmp {
      filename = ${logdir}/radutmp
      username = %{User-Name}
      case_sensitive = yes
      check_with_nas = yes
      perm = 0600
      callerid = "yes"
}
radutmp sradutmp {
      filename = ${logdir}/sradutmp
      perm = 0644
      callerid = "no"
}
attr_filter {
      attrsfile = ${confdir}/attrs
}
counter daily {
      filename = ${raddbdir}/db.daily
      key = User-Name
      count-attribute = Acct-Session-Time
      reset = daily
      counter-name = Daily-Session-Time
      check-name = Max-Daily-Session
      allowed-servicetype = Framed-User
      cache-size = 5000
}
always fail {
      rcode = fail
}
always reject {
      rcode = reject
}
always ok {
      rcode = ok
      simulcount = 0
      mpp = no
}
expr {
}
digest {
```

```
        }
        exec {
                wait = no
                input_pairs = request
        }
        exec echo {
                wait = yes
                program = "/bin/echo %{User-Name}"
                input_pairs = request
                output_pairs = reply
        }
}
instantiate {
        exec
        expr
}
authorize {
        preprocess
        mschap
        eap
        ldap
        files
}
authenticate {
        Auth-Type MS-CHAP {
                mschap
        }
        eap
}
preacct {
        preprocess
        acct_unique
        ntdomain
}
accounting {
}
session {
}
post-auth {
}
```

```
pre-proxy {
}
post-proxy {
      eap
}
```

Anexo 5 NAGIOS

/etc/nagios/objects/switch.cfg

```
##############################################################################
######
# SWITCH.CFG - SAMPLE CONFIG FILE FOR MONITORING A SWITCH
#
# Last Modified: 10-03-2007
#
# NOTES: This config file assumes that you are using the sample
configuration
#      files that get installed with the Nagios quickstart guide.
#
##############################################################################
###
###
#
# HOST DEFINITIONS
#
##############################################################################
###

# Define the switch that we'll be monitoring

define host{
      use         generic-switch
      host_name   hp-2608-pwr
      alias       hp-2608-pwr Switch
      address           192.168.100.253
      hostgroups  switches
      }

define host{
        use             generic-switch
        host_name       dlink-g624t
        alias           dlink-g624t
        address         192.168.100.251
        hostgroups      switches
        }

##############################################################################
######
#
# HOST GROUP DEFINITIONS
#
##############################################################################
###

# Create a new hostgroup for switches
```

```
define hostgroup{
      hostgroup_name    switches
      alias       Network Switches
      }

##############################################################################
######
#
# SERVICE DEFINITIONS
#
##############################################################################
###

# Create a service to PING to switch

define service{
      use               generic-service
      host_name         hp-2608-pwr
      service_description     PING
      check_command           check_ping!200.0,20%!600.0,60%
      normal_check_interval   5
      retry_check_interval    1
      }
define service{
        use                     generic-service
        host_name               dlink-g624t
        service_description     PING            ;
        check_command           check_ping!200.0,20%!600.0,60%
        normal_check_interval   5
        retry_check_interval    1
        }
# Monitor uptime via SNMP

define service{
      use               generic-service   ;
      host_name         hp-2608-pwr
      service_description     Uptime
      check_command           check_snmp!-C public -o sysUpTime.0
      }
define service{
        use                     generic-service
        host_name               dlink-g624t
        service_description     Uptime
        check_command           check_snmp!-C public -o sysUpTime.0
        }
# Monitor Port 1 status via SNMP
define service{
      use               generic-service
      host_name         hp-2608-pwr
      service_description     Port 1 Link Status
      check_command           check_snmp!-C public -o ifOperStatus.1 -r 1
-m RFC1213-MIB
      }
define service{
        use                     generic-service
        host_name               dlink-g624t
        service_description     Port 1 Link Status
        check_command           check_snmp!-C public -o ifOperStatus.1 -r
1 -m RFC1213-MIB
        }
# Monitor bandwidth via MRTG logs
```

```
define service{
      use                 generic-service   ; Inherit values from a
template
      host_name           hp-2608-pwr
      service_description     Port 1 Bandwidth Usage
      check_command
      check_local_mrtgtraf!/usr/bin/mrtg/192.168.100.253_1.log!AVG!100000
0,1000000!5000000,5000000!10
      }
```

/etc/nagios/objects/contacts.cfg

```
define contact{
     contact_name              nagiosadmin
     use                       generic-contact
     alias                     Nagios Admin
     e-mail                     nagios@caramelo.com
        }
```

Anexo 6 CONFIGURAÇÃO *NTOP*

```
Suse11:~ # vi /etc/sysconfig/ntop
# Specifies the network interface used by ntop
NTOPD_IFACE="eth0,eth2"

# Please note that an HTTP server is NOT needed  in
# order to use the program in interactive mode.
#
NTOPD_PORT="192.168.100.254:82"

# define SSL port. Please note, that you have to generate
# a certificate to run run ntop with this option.
# This may be done with the commands:
# openssl req -new -x509 -sha1 -extensions v3_ca -nodes -days 365 -out
cert.pem
# cat privkey.pem cert.pem > /etc/ntop/ntop-cert.pem
# /bin/rm -f privkey.pem cert.pem
#
# NTOPD_SSL_PORT="3001"
#
NTOPD_SSL_PORT=""
## Type:        string
## Default:     "wwwrun"
#
# define the user to run ntop. This should not be root!
#
NTOP_USER="admin"
## Type: string
## Default: ""
## ServiceRestart: ntop
#
# Additional arguments when starting ntop with the init script
# /etc/init.d/ntop or rcntop.
#
```

Anexo 7 FICHEIROS DE SIMULAÇÃO DE E-MAIL NÃO FIDEDIGNO

```
Vi sample-mail-bomb.txt
From: virus-tester
To: undisclosed-recipients:;
Subject: amavisd test - 100.zip mail bomb
Message-ID: <77115.1055868666@example.com>
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="-"
This is a MIME encoded message.  Decode it with "munpack"
or any other MIME reading software.
---
Content-Type: application/octet-stream; name="100.zip"
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="100.zip"
Content-MD5: X+muYik0Ez+BojtKyHyvLA==
```

```
Vi sample-badh.txt
Date: Mon, 22 Oct 2008 12:36:25 +0000
Message-ID: <N1msdrbJXNPfV4@example.com>
Subject: teste de bad header
 indeed
From: "BrokeÃ± HÃ©ader fÃeld" <test@localhost>
X-Mailer:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx123456789
 yyyyyyyyyy
 zzzzzzzzzz
To: undisclosed-recipients: ;
testing, 1, 2, 3...
```

```
vi sample-spam-GTUBE-junk.txt
Subject: Test spam mail (GTUBE)
Message-ID: <GTUBE1.1010101@example.net>
Date: Wed, 23 Jul 2003 23:30:00 +0200
From: Sender <sender@example.net>
To: Recipient <recipient@example.net>
Precedence: junk
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
This is the GTUBE, the
        Generic
        Test for
        Unsolicited
        Bulk
        Email
If your spam filter supports it, the GTUBE provides a test by which you
can verify that the filter is installed correctly and is detecting
incoming
spam. You can send yourself a test mail containing the following string
of characters (in upper case and with no white spaces and line breaks):
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
You should send this test mail from an account outside of your network.
```

```
vi sample-virus-simple.txt
From: virus-tester
To: undisclosed-recipients:;
Subject: amavisd test - simple - virus scanner test pattern

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
~
```