Universidade de Aveiro Departamento de Eletrónica, Telecomunicações e Informática
2013

Malique Seidi

Segurança da Rede de Comunicações numa Instituição de Ensino Superior

Universidade de Aveiro
2013
Departamento de Eletrónica, Telecomunicações e Informática

Malique Seidi

Segurança na Rede de Comunicações numa Instituição de Ensino Superior

Tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Eletrónica e Telecomunicações, realizada sob a orientação científica do Doutor António Manuel Duarte Nogueira (orientador) e do Doutor Paulo Jorge Salvador Serra Ferreira (co-orientador), ambos Professores Auxiliares do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro.

o júri

presidente

Prof. Doutor André Ventura da Cruz Marnoto Zúquete
Professor Auxiliar, Universidade de Aveiro

Doutor Eduardo Rinn Estanqueiro Rocha
Investigador Associado, Leipzig University Of Applied Science

Prof. Doutor António Manuel Duarte Nogueira
Professor Auxiliar, Universidade de Aveiro

agradecimentos

Antes de mais, agradeço a Deus, pela vida e saúde e presença constante nos momentos em que mais preciso, aos meus Pais a quem devo todo o meu Eu, e a minha querida filha.

O meu mais profundo obrigado aos Professores António Nogueira e Paulo Salvador, meu orientador e co-orientador, respetivamente, que desde o início mostraram total disponibilidade para me orientar neste mestrado. Com eles aprendi muito, não só como investigador mas também como pessoa, pelo carinho que manifestam aos seus alunos.

Não esquecendo, a equipa de centro de informática de IPT na pessoa do Engº Joaquim Pombo, pelo apoio prestado no desenvolvimento deste trabalho.

E finalmente, não por ser menos importante, aos meus caros AMIGOS que podem ser aqueles que aceitam um convite para a festa, mas sobretudo aqueles que aparecem nas horas difíceis sem ser convidados.

palavras-chave

Segurança à rede. Sistema de deteção e prevenção de intrusões, Ameaças, Ataques.

resumo

A segurança no ambiente de redes de computadores é um elemento essencial para a proteção dos recursos da rede, dos sistemas e da informação. Os mecanismos de segurança normalmente utilizados são criptografia de dados, firewalls, mecanismos de controlo de acesso e sistemas de deteção de intrusões. Os sistemas de deteção de intrusões têm sido alvo de muita investigação já que constituem um mecanismo muito importante para a monitorização e deteção de eventos suspeitos em redes de computadores. A investigação nesta área visa adequar os mecanismos de deteção por forma a aumentar a sua eficiência.

Ameaças na Internet tornaram-se cada vez mais sofisticados e são capazes de contornar as soluções básicas de segurança, como firewalls e antivírus. É portanto necessária uma proteção adicional para aumentar a segurança global da rede. Uma possível solução para melhorar a segurança é adicionar um sistema de deteção de intrusões (IDS) como uma camada adicional nas soluções de segurança.

A deteção de intrusões aparece muitas vezes associada à prevenção de intrusões, que pode ser definida como o processo de detetar e impedir as intrusões, no sentido de evitar as possíveis consequências nefastas. Os Sistemas de Deteção e Prevenção de Intrusões (IDPS) estão focados em identificar possíveis incidentes, evitar o acesso a informação de login e reportar todos os resultados ao administrador de segurança.

Além disso, as organizações utilizam IDPS para outros fins, tais como a identificação de problemas com as políticas de segurança, documentar ameaças existentes e identificar quem tenta violar as políticas de segurança. Os IDPS tornaram-se assim num complemento necessário para a infraestrutura de segurança de quase todas as organizações.

Esta dissertação pretende analisar a rede de comunicações do Instituto Politécnico de Tomar, identificando as suas principais deficiências de segurança e propondo soluções capazes de atenuar os problemas identificados.

keywords

Network Security, Intrusion Detection and Prevention System, Threat, Security Attack.

abstract

Security in the computer network environment is an essential element for the protection of the network resources, systems and information. The security mechanisms that are usually applied include data cryptography, firewalls, access control mechanisms and intrusion detection systems. Intrusion detection systems have been largely investigated in recent years because they are an important mechanism for monitoring and detecting suspicious events in computer network environments. Research in this area aims to improve the efficiency of the detection mechanisms.

Security threats are becoming more and more sophisticated and able to bypass basic security solutions, such as firewalls and antivirus scanners. Therefore, additional protection is needed to enhance the network overall security. One possible solution is the deployment of an intrusion detection system (IDS) as an additional security layer.

Intrusion detection is the process of monitoring events occurring in a computer system or network, analyzing them and look for signs of possible incidents, which can be violations or imminent threats of violation of computer security policies. Intrusion prevention is the process of performing intrusion detection and attempting to avoid detected incidents. Intrusion detection and prevention systems (IDPS) are mainly focused on identifying possible incidents, logging information about them, try to stop those incidents and report them to security administrators.

Organizations also use IDPSs for other purposes, such as identify problems on security policies, document security threats and avoid individuals from violating security policies. So, IDPSs became a necessary addition to the security infrastructure of every organization.

This thesis aims to analyze the communications network of the Polytechnical Institute of Tomar, identifying their major security deficiencies and proposing solutions that can mitigate those problems.

ÍNDICE

Índice de Figuras

Índice de Tabelas

Lista de Siglas e Acrónimos

DAC: Discretionary access control

DdoS: Distributed Denial of Service Attack

DNS: Domain Name System

DHCP: Dynamic Host Configuration Protocol

DoS: Denial of Service

EAP: Extensible Authentication Protocol

FTP: File Transfer Protocol

HIDS: Host Intrusion Detection System

HIPS: Host Intrusion Prevention System

HTML Hyper Text Markup Language

HTTP: Hypertext Transfer Protocol

IANA: Internet Assigned Numbers Authority

ICMP: Internet Control Message Protocol

ICV : Integrity Check Value

IDS: Sistema de Detecção de Intrusão

IGMP: Internet Group Management Protocol

IP: Internet Protocol

IPS: Sistema de Prevenção de Intrusão

IPS: Internet Protocol Suite

IPSec: Internet Protocol Security

IPT; Instituto Politécnico de Tomar

LAN: Local Area Network

MAC: Mandatory Access Control

MIC: Message Integrity Check

MSK: Master Session Key

MTU: Maximum Transmit Unit

NFS: Network File System

NIDS: Network Intrusion Detection System

NIPS: Network Intrusion Prevention System

NTFS: New Technology File System

OSI: Open Systems Interconnection

OSPF: Open Shortest Path First

PMK: Primary Master Key

PSK: Pre Shared Key

PTK; Pariwise Transient Key

RBAC: Role Based Access Control

RPC: Remote Procedure Calls

SMTP: Simple Mail Transfer Protocol

SO: Sistema Operativo

SQL: Structured Query Language

SSH: Secure Shell Client

PPTP*:* Point-to-Point Tunneling Protocol

DES*:* Data Encryption Standard

AES*:* Advanced Encryption Standard

L2TP*:* Layer 2 Tunneling Protocol

NAT*:* Network Address Translation

TCP: Transmission Control Protocol

TEK: Temporal Encryption Key

TI: Tecnologia da Informação

TMK: Temporal MIC Key

UDP: User Datagram Protocol

WAN: Wide Area Network

WEP: Wired Equivalent Privacy

WPA: Wi-fi Protect Access

VPN: virtual private network

VOIP: Voice over Internet Protocol

1. INTRODUÇÃO

As redes de computadores surgiram da necessidade de trocar informação entre utilizadores. No princípio as redes eram restritas às universidades, centros de pesquisas e departamentos governamentais, que possuíam mais recursos e possibilidades de implementação. Dessa forma, o acesso estava restrito a um pequeno grupo de pessoas que possuía vínculo com essas instituições.

Atualmente, com a queda dos custos de implementação de rede, é impossível pensar num ambiente de trabalho onde os computadores não estejam interligados, a fazer partilha de recursos ou acesso à *internet*. Com toda essa disponibilidade, garantir a segurança dos dados passou a ser uma grande preocupação, pois tendo acesso à *internet* possibilita-se que a rede privada seja atingida pelo mundo exterior. Então, se métodos de segurança não forem implementados, todo o sistema informático corre o risco de ser explorado, a partir de várias fontes e de várias formas, podendo causar perda de conectividade ou divulgação de dados confidenciais.

Segundo [23], segurança da informação pode ser definida como proteção contra ataques ou divulgação não intencional dos dados que estão armazenados ou que transitam através de uma rede de computadores. Uma forma de facilitar a compreensão do que é segurança da informação é diferenciar segurança de privacidade: privacidade é a necessidade de restringir o acesso aos dados e informações, enquanto que segurança é garantir esta privacidade.

Com a crescente quantidade de incidentes de segurança, o tratamento manual de cada incidente torna-se uma atividade inviável para o administrador de segurança. Desta forma, sistemas de deteção de intrusões na rede (*Network Intrusion Detection System - NIDS*) e sistemas de prevenção de intrusões (*Intrusion Prevention System - IPS*) tornam-se extremamente relevantes.

Um IPS ideal é aquele que, mesmo na ocorrência de falhas no seu *hardware*, consegue detetar tráfego malicioso em toda a rede e bloqueá-lo o mais próximo da sua origem, sem afetar o bom funcionamento da rede.

É comum um IPS atuar no modo ativo (*inline*), ou seja, no meio físico capturando, analisando e devolvendo o tráfego à rede. Neste modo, o IPS é normalmente instalado na periferia da rede, precedendo uma *firewall* ou mesmo um *router* que dá acesso a uma rede externa. Desta forma, a captura e a análise restringem-se ao tráfego que passa pelo IPS. Consequentemente, um tráfego malicioso num segmento interno da rede não é capturado e não pode ser bloqueado (como por exemplo, a disseminação de um *worm*).

Um IPS também pode atuar capturando tráfego espelhado por um *switch* (modo passivo). Porém, neste caso, o IPS só consegue bloquear tráfego se possuir alguma integração com os demais equipamentos da rede. Como geralmente o parque de ativos da rede é bastante heterogéneo, dificilmente este cenário é encontrado na prática.

As redes de computadores estão cada vez mais interligadas, pelo que a estabilidade e a segurança se tornam imprescindíveis, já que o mundo dos negócios está fortemente apoiado na Tecnologia da Informação (TI), podendo, em caso de falha, todo o negócio ser prejudicado.

A referência [35] apresenta os três princípios de segurança, ilustrados na Figura 1:

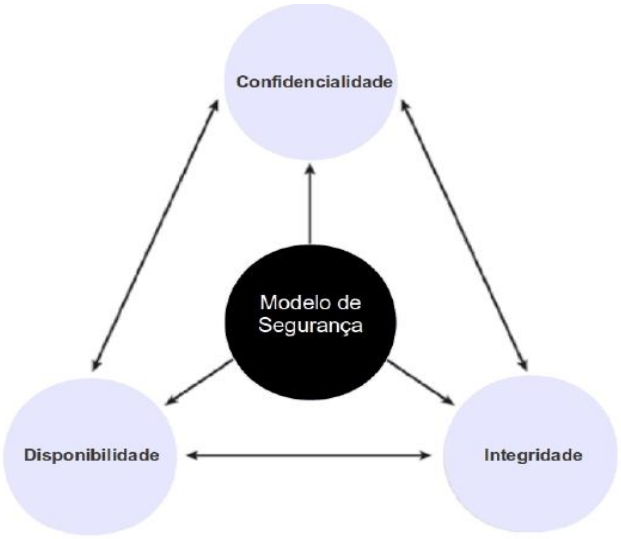


Figura 1 - Princípios de segurança
Fonte: Do autor com base em [35]

- confidencialidade: impede a divulgação de informações confidenciais a pessoas não autorizadas;
- integridade: impede a modificação não autorizada de dados, sistemas e informações, proporcionando a garantia de dados íntegros;

- disponibilidade: é a prevenção contra perda de acesso a recursos e informações, garantindo dessa forma que a informação está disponível para uso quando necessário.

Para [33], um administrador de rede tem que pensar como um atacante, pois só assim pode determinar a melhor forma de proteger os seus recursos, fazendo uma análise da rede para avaliar o nível de proteção de que realmente necessita.

A crescente sofisticação das ferramentas capazes de efetuar ataques de segurança, as novas ameaças de segurança que surgem diariamente, o fácil acesso à *internet* e o aumento exponencial no número de utilizadores da Internet, tornam cada vez mais complexa a tarefa de manter uma rede segura. O fator segurança está cada vez mais presente no nosso quotidiano, e manter a segurança das redes tem-se tornado uma tarefa árdua e desafiadora. Nesse sentido, os utilizadores das redes de computadores são constantemente incentivados a utilizar software antivírus, ferramentas de deteção e prevenção de intrusões (IDS/IPS), instalar *firewalls*, entre outras ferramentas que podem auxiliar na proteção da rede.

Na tentativa de minimizar as deficiências existentes nos sistemas de deteção atuais, foram propostas algumas soluções no sentido de detetar ataques em canais cifrados ao nível das camadas de transporte e aplicação da pilha protocolar TCP/IP, sem haver necessidade do conhecimento da chave privada. Os trabalhos baseiam-se essencialmente na deteção de anomalias com base em perfis de tráfego [2] e [6].

Uma solução de defesa para ataques direcionados à camada de aplicação é apresentada por [8], em que os autores propõem uma solução baseada no acoplamento de um monitor que observa as mensagens de controlo do protocolo que são transmitidas entre cliente e servidor, tornando possível detetar ataques baseados em comportamentos anómalos do protocolo. Este trabalho continua os estudos inicialmente apresentados em [6] e [35], acrescentando a funcionalidade de redução da efetividade dos ataques a nível da aplicação por meio da inserção de intervalos entre o processamento dos pedidos.

Por outro lado, a contenção de ataques por meio da gestão dos recursos do servidor é também uma prática plausível de ser utilizada: técnicas de qualidade de serviço são utilizadas para diminuir a quantidade de largura de banda disponível para o endereço IP ofensivo, principalmente para ataques do tipo DoS (*Denial of Service*).

A referência [7] apresenta um sistema de deteção de intrusões baseado num agente (*proxy*) criptográfico EPIDS (*Encrypted Proxy Intrusion Detection System*), no qual todas as ligações provenientes de um cliente SSH são intercetadas por um *proxy* transparente capaz de extrair a informação do pacote cifrado, analisar e validar a existência de conteúdo malicioso, enquanto reencaminha os pedidos ao serviço. A técnica adotada utiliza o mesmo princípio do ataque *Man-in-the-middle* [32], o qual possibilita a intercetação e manipulação de pacotes criptográficos por meio da intercetação e troca da chave pública original do servidor por uma chave pública falsa.

1.1 Objetivos

Este trabalho tem por objetivo identificar e propor soluções de segurança para a rede de dados do campus do Instituto Politécnico de Tomar (IPT), tendo por base a análise qualitativa e quantitativa dos dados recolhidos pela ferramenta de IDS/IPS (Sistema de Deteção e Prevenção de Intrusões) instalada na infraestrutura de comunicações desta instituição.

A manutenção da segurança de uma rede de dados é dificultada quando esse ambiente é híbrido e heterogéneo. O ambiente da grande maioria das instituições de ensino tem precisamente estas características. Para ajudar a manter a segurança da rede de dados do IPT irá ser estudado um sistema automático capaz de monitorizar, detetar e prevenir tentativas de intrusão através da análise dos dados recolhidos sobre os protocolos e pacotes, fazendo uso de metodologias de deteção multidimensional por meio da análise de assinaturas de ataques, anomalias protocolares e comportamento do tráfego.

1.2 Estrutura da Dissertação

O presente trabalho está dividido em seis capítulos. Os dois primeiros fazem uma introdução aos conceitos básicos das redes de computadores, enquanto os outros três se dedicam à área da segurança e sua aplicação.

O Capítulo 2 descreve os modelos OSI e TCP/IP, incluindo as funções de cada uma das suas camadas. A finalizar é feita uma correlação entre os dois modelos, mostrando a não compatibilidade das suas camadas.

O Capítulo 3 aborda os principais problemas de segurança das redes de dados e os principais tipos de ataques de segurança. Além disso, aborda as principais dificuldades para conter ameaças e as boas práticas para minimizar os problemas relativos à segurança. Ainda neste capítulo são apresentados mecanismos de defesa, controlo de acesso, entre outros, que têm por função garantir e aumentar o nível de segurança lógica da rede.

O Capítulo 4 aborda o sistema de detecção e prevenção de intrusões, o tema principal do trabalho proposto. Descreve os conceitos, tipos de implementação e formas de funcionamento. A contextualização deste capítulo serve como base para a estrutura do sistema a ser descrito no capítulo seguinte.

O Capítulo 5 começa por efetuar a análise de um ambiente base, identificação do problema, apresentação física e lógica de um ambiente ideal e descrição das ferramentas utilizadas na implementação do IDS/IPS.

No Capítulo 6, é feita uma análise qualitativa dos dados obtidos pela ferramenta de análise, o *FortiAnalizer*. Finalmente, são apresentadas as considerações finais do autor quanto aos propósitos e resultados obtidos com o estudo do processo de identificação de ameaças na rede de dados analisada.

2. ARQUITETURAS PROTOCOLARES EM CAMADAS

Neste capítulo são apresentados os modelos protocolares OSI e TCP/IP, sendo ainda efetuada uma comparação entre eles. Estes modelos são essenciais para se compreender o tema da segurança nas redes de computadores, e ainda pelo facto de as ferramentas de segurança do tipo IDS/IPS interagirem directamente nas suas diferentes camadas.

2.1. Redes de computadores

Segundo [11], uma rede consiste em diversos dispositivos interligados, tais como computadores e servidores, e comunicando entre si, partilhando recursos físicos e lógicos. Esses recursos incluem hardware e software, como meio de armazenamento dos dados.

As redes de computadores surgiram para viabilizar a troca e a partilha de informações e dispositivos periféricos, preservando a independência das várias estações de processamento e permitindo a integração em ambientes de trabalho cooperativos [41].

As redes locais estão circunscritas a áreas geográficas de dimensões relativamente reduzidas, como é o caso de universidades e empresas. A Figura 2 ilustra o conceito de rede local, vista como uma infraestrutura que permite a partilha de recursos.

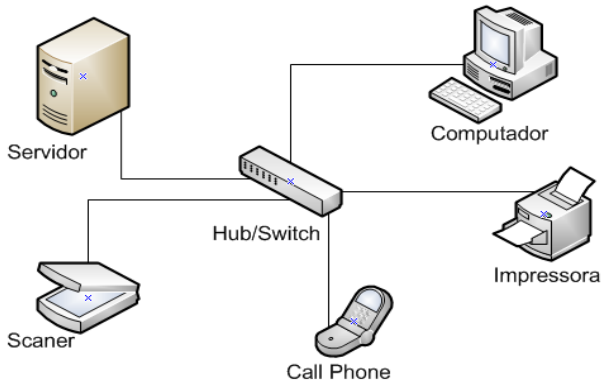


Figura 2 - Rede de computadores local

As redes podem apresentar diferentes topologias ou formas de interligação dos dispositivos. As duas topologias mais comuns são em anel, em que um dispositivo se liga a outro até se fechar o anel, e estrela, em que cada dispositivo é ligado a um "distribuidor" ou nó central. As redes utilizam diferentes protocolos, ou seja, normas de envio e recepção

de pacotes. Os dispositivos são interligados através de algum meio físico, tal como fio de cobre, fibra óptica ou *wireless*, cada um apresentado as suas características específicas.

2.1.1 Modelo OSI (Open Systems Interconnection)

Atendendo à complexidade de estabelecer regras de cooperação entre todas as entidades da rede, o problema foi dividido num conjunto de sub-problemas. De facto, num mesmo nó existem diferentes entidades que desempenham funções distintas; por outro lado, em diferentes nós existem entidades semelhantes que desempenham funções idênticas. Nesse sentido, as entidades dos diferentes nós foram agrupadas em camadas funcionais e foram estabelecidas regras de cooperação entre as entidades da mesma camada funcional localizadas em diferentes nós, tendo ainda sido definidas interfaces entre as diferentes camadas funcionais localizadas no mesmo nó.

Obtiveram-se deste modo arquitecturas protocolares organizadas em camadas, que permitem definir um conjunto global de regras de cooperação entre as diferentes entidades. Uma das principais vantagens das arquitecturas protocolares em camadas é a possibilidade de substituição de camadas, sem afectar as camadas adjacentes, desde que seja garantido o mesmo tipo de serviço e mantidas as mesmas interfaces entre as camadas.

A Organização Internacional para a Normalização, ISO (*International Organization for Standardization*), foi uma das primeiras organizações a definir formalmente uma arquitectura padrão com o objectivo de facilitar o processo de interligação entre máquinas de diferentes fabricantes. O padrão OSI (*Open Systems Interconnection*) foi lançado em 1984.

O Modelo OSI permite comunicação entre máquinas heterogéneas e define directivas genéricas para a construção de redes de computadores (sejam elas de curta, média ou longa distância) independentemente da tecnologia utilizada.

Esta arquitectura é um modelo que divide as funcionalidades das redes de computadores em 7 camadas de abstracção. Cada protocolo implementa uma funcionalidade associada a uma determinada camada, como é possível observar na Figura 3.

Figura 3 - Modelo OSI (Fonte: [5])

Camada 1 - Física

Faz o interface com a camada de dados e com o meio físico. É responsável pela definição das interfaces com o meio físico e pela transmissão e recepção do sinal entre nós adjacentes.

Camada 2 - Dados

Faz o interface com a camada física e com a camada de rede e é responsável pela formação das tramas, multiplexagem e desmultiplexagem dos dados enviados sobre a camada física. Pode ainda incluir funções de controlo de erros e de controlo do acesso ao meio físico.

Camada 3 - Rede

Faz o interface com a camada de dados e com a camada de transporte e é responsável pelo encaminhamento da informação de nó para nó.

Camada 4 - Transporte

Faz o interface com a camada de rede e com a camada de sessão e é responsável pelo controlo da ligação entre os pontos extremos. A camada de transporte pode fornecer diferentes classes de serviço com diferentes qualidades de serviço.

Camada 5 – sessão

Faz a interface com a camada de transporte e com a camada de apresentação e é responsável pela gestão de múltiplas ligações entre sistemas.

Camada 6 – Apresentação

Faz a interface com a camada de transporte e com a camada de aplicação e é responsável por assegurar a compatibilidade da representação da informação entre diferentes sistemas.

Camada 7 – Aplicação

Faz o interface com a fonte de informação e com a camada de apresentação. A camada de aplicação faculta à fonte de informação os meios para esta aceder ao sistema de comunicações.

Cada uma das camadas desempenha um subconjunto das funções necessárias ao processo de comunicação entre duas entidades distintas e distantes. As camadas superiores acedem aos serviços das camadas inferiores através de SAPs (*Service Access Points).* Alterações na implementação de uma dada camada não implicam alterações nas camadas adjacentes, desde que o tipo de serviço e as interfaces sejam mantidos inalterados. As funcionalidades implementadas numa dada camada dependem das funcionalidades requeridas pelas camadas superiores, o que significa que existem diferentes protocolos para uma mesma camada, tal como se ilustra na figura 4.

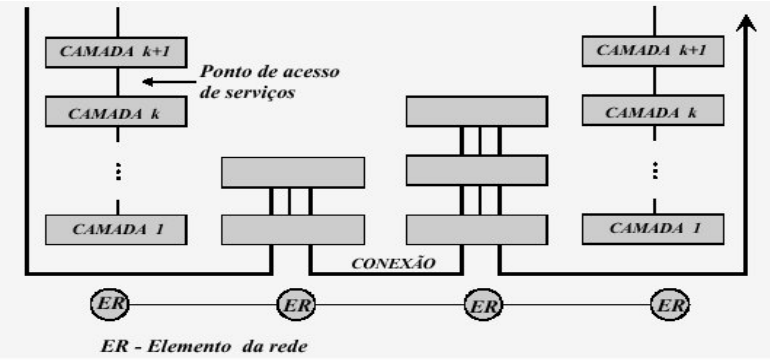


Figura 4 - Pontos de acesso de serviços (Fonte: [5])

As várias camadas funcionais desempenham um conjunto de funções de acordo com protocolos pré-estabelecidos. De forma a implementar os vários protocolos, as várias camadas no nó emissor vão adicionando informação sob a forma de cabeçalhos ou terminações à informação que lhes é passada pelas camadas superiores.

No nó receptor esta informação vai sendo retirada à medida que a informação circula das camadas inferiores para as camadas superiores. Neste processo os cabeçalhos são

inicialmente retirados e depois inseridos novamente, com nova informação [5]; tal como se ilustra na figura 5:

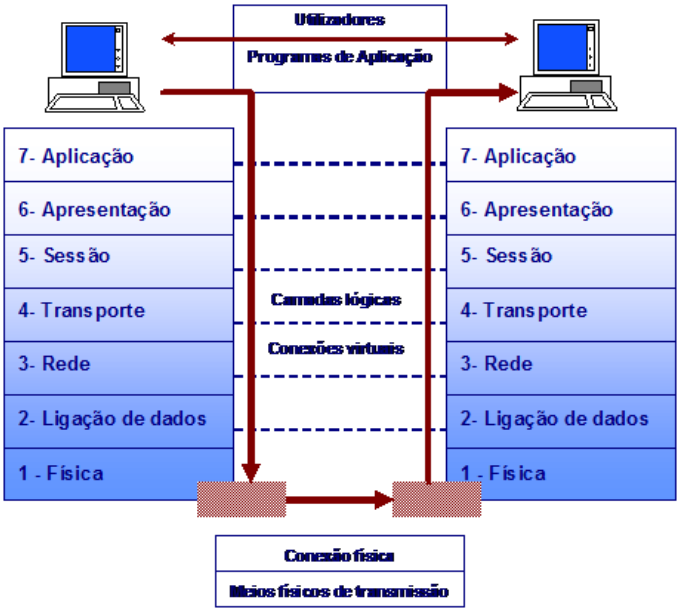


Figura 5 - Comunicação entre camadas (Fonte: [5])

2.1.2 Modelo TCP/IP

A arquitetura protocolar TCP/IP foi desenvolvida em 1974 especificamente para a Internet, mas devido ao sucesso desta acaba por ser utilizada em muitos sistemas que suportam serviços não diretamente relacionados com a Internet. É comum dividir o modelo TCP/IP em quatro camadas funcionais, como é possível observar na figura 6.

Figura 6 - Modelo TCP/IP (Fonte: [5])

Camada 1 – Acesso à rede

Engloba as funções da camada de dados do modelo OSI e é responsável pela comunicação entre elementos diretamente ligados à mesma rede.

Camada 2 – Internet (Rede)

É responsável pelas funções de encaminhamento da informação pelos diferentes nós e fornece serviços de segmentação e reagrupamento da informação.

Camada 3 - Transporte

Engloba as funções da camada de transporte do modelo OSI, permitindo ainda endereçar a informação a um processo específico dentro de uma máquina.

Camada 4 – Aplicação

Engloba as camadas de Aplicação, Apresentação e Sessão do modelo OSI, tendo a função de controlar o tráfego, representar e codificar os dados.

De forma a entregar a informação a um processo específico, os protocolos de nível 4 do protocolo TCP/IP utilizam um "endereço" designado por porta. A Tabela 1 exemplifica alguns protocolos da camada de aplicação:

Tabela 1 - Protocolos da camada de aplicação

Protocolo	Função
Telnet	*Login* remoto
File Transfer Protocol (*FTP*)	Transferência de ficheiros
Simple Mail Transfer Protocol (*SMTP*)	Entrega de correio eletrônico
Hypertext Transfer Protocol (*HTTP*)	Acesso a *web sites*
Domain Name System (*DNS*)	Resolução de nomes de domínios
Open Shortest Path First (*OSPF*)	Protocolo de encaminhamento
Network File System (*NFS*)	Partilha de diretórios

O *TCP* é orientado à ligação, ou seja, cria um circuito virtual, *full duplex* (tem a capacidade de enviar e receber dados simultaneamente) entre duas aplicações, sendo todos os *bytes* numerados para que seja possível a retransmissão em caso de falhas.

Na Figura 7 é possível observar, de maneira ilustrativa, o túnel virtual criado pelo protocolo TCP, com características ponto a ponto e *full duplex.*

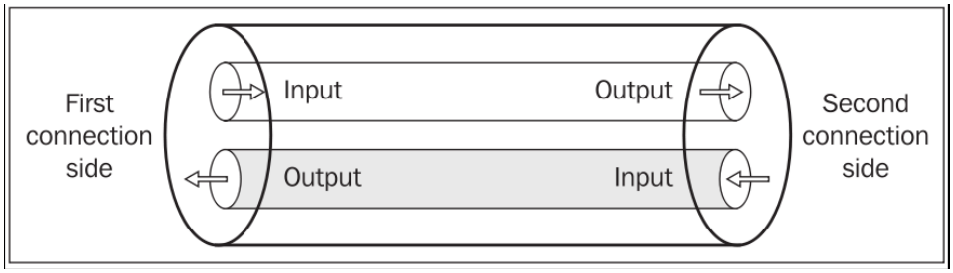


Figura 7 - - Ligação ponto a ponto bidirectional (Fonte: [5])

O detalhe da estrutura de um segmento *TCP* pode ser observado na Figura 8, na qual se identificam alguns campos: porta de origem e de destino, usadas para identificar as portas no emissor e no recetor, respectivamente; o número de sequência, utilizado para controlo uma vez que os pacotes devem ser enviados e recebidos por ordem; *checksum*, utilizado para verificar a integridade dos dados.

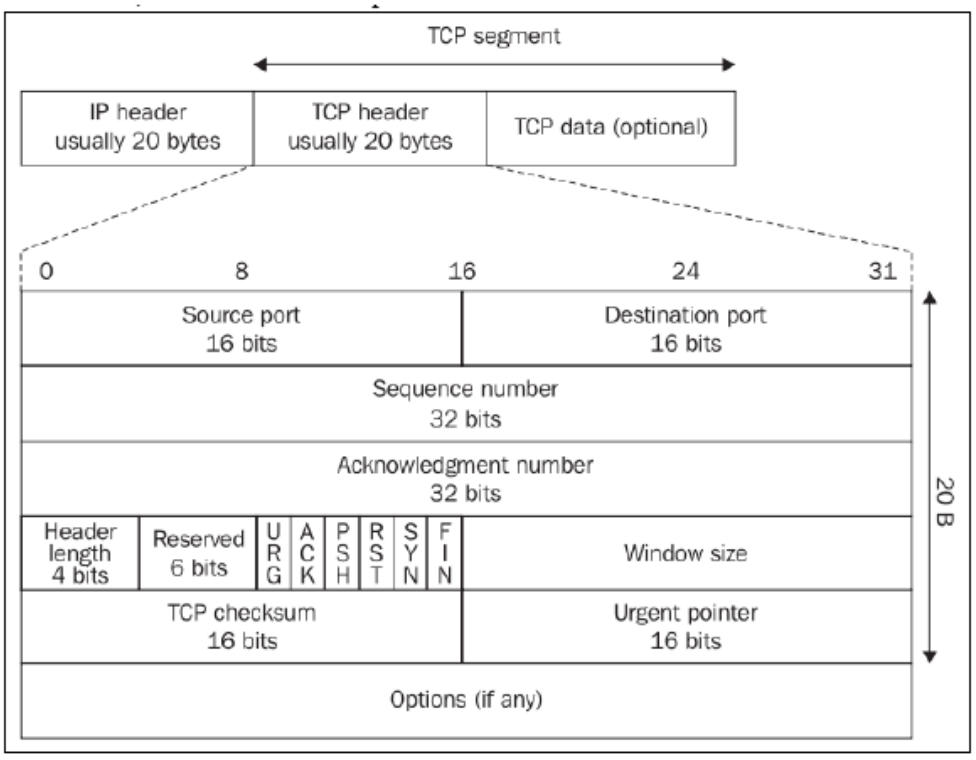


Figura 8 - Segmento TCP (Fonte: [27]).

O protocolo IP transmite dados entre dispositivos, enquanto que o protocolo TCP transfere dados entre as aplicações nestes dispositivos, utilizando para isso a porta na qual o serviço está a ser executado.

Todas as aplicações que utilizam o protocolo *TCP* têm a garantia de que os dados serão entregues. Porém, a proteção garantida pelo *TCP* não oferece proteção contra ataques a rede de dados [27]. A garantia do protocolo limita-se à entrega dos dados. Os pontos de origem e destino na ligação são identificados por um número de porta que, no caso do protocolo *TCP*, pode variar de 0 a 65535. No caso da *internet*, a aplicação de destino é endereçada por meio de um endereço *IP*, um número de porta e o protocolo.

As portas de 0 até 1.024 são conhecidas e reservadas, com regulação feita pela *Internet Assigned Numbers Authority* (*IANA*). A Tabela 2 relaciona alguns serviços e portas [3].

Tabela 2 - Algumas portas atribuídas

Nº Porto	Protocolo	Função
21	*FTP*	Transferência de ficheiros
23	*TELNET*	*Login* remoto
25	*SMTP*	Entrega de correio eletrônico
69	*TFTP*	Transferência de ficheiros
79	*FINGER*	Verificação de informações de utilizadores
80	*HTTP*	Acesso a *web sites*
110	*POP3*	Acesso remoto a e-mails
119	*NNTP*	Notícias

2.1.3 Modelo OSI vs TCP/IP

Uma questão que normalmente se levanta é a da correlação entre as normas ISO dos modelos OSI e TCP/IP. As principais semelhanças entre os dois modelos podem ser resumidas da seguinte forma:

- ambos são estruturados em camadas;
- ambos têm camadas de aplicação, embora incluam serviços diferentes;
- ambos têm camadas de transporte e de rede comparáveis;
- a tecnologia de comutação de pacotes é presumida por ambos.

Quanto ás diferenças, podemos enumerar as seguintes:

- o TCP/IP combina os aspetos das camadas de apresentação e de sessão do modelo OSI dentro da sua camada de aplicação;
- o TCP/IP combina as camadas física e de ligação do modelo OSI numa única camada;

- o TCP/IP parece ser mais simples por ter menos camadas;
- ao contrário do modelo OSI, onde os protocolos são agrupados por camadas tendo em conta a sua funcionalidade, no TCP/IP é usual agrupar os protocolos tendo em conta os serviços que necessitam. Ou seja, um protocolo que necessite apenas dos serviços da camada 3 é colocado na camada 4, independentemente da sua funcionalidade, o que faz com que se tenha na mesma camada TCP/IP protocolos com funcionalidades muito distintas e diferentes daquelas que o nome da camada levaria a supor.

A Figura 9 ilustra a comparação entre os dois modelos:

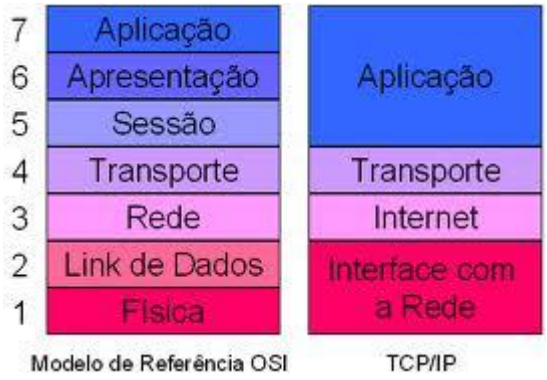


Figura 9 - Comparação entre os modelos OSI e TCP/IP (Fonte: [5])

3. MECANISMOS DE SEGURANÇA EM REDES

Segundo [23], segurança de redes é um termo muito amplo que abrange a proteção dos dados armazenados e dos que transitam na rede de computadores contra a divulgação não autorizada, modificação acidental ou intencional. Neste capítulo será apresentada a definição de risco e ameaça de segurança, bem como identificadas as principais vulnerabilidades e os tipos de ataques que geralmente ocorrem numa rede de computadores.

3.1 Riscos e ameaças nas redes

Os autores da referência [9] definem risco em segurança da informação como a probabilidade de um agente explorar uma vulnerabilidade, comprometendo a confidencialidade, integridade e disponibilidade (CIA, *confidentiality, integrity, availability*) dos dados. No momento que uma rede de dados passa a ser parte importante de uma organização, existem algumas considerações que devem ser feitas quanto aos riscos existentes.

- as informações que transitam pela rede estão sujeitas a ser capturadas;
- os *e-mails* podem ser capturados, lidos, modificados e/ou falsificados;
- a *internet* deve ser considerada um ambiente hostil e portanto, não confiável;
- novas tecnologias significam novas vulnerabilidades;
- a interação entre diferentes ambientes resulta na multiplicação dos pontos vulneráveis;
- a segurança é complexa.

De acordo com [42], é essencial que se execute uma análise de riscos durante a fase inicial de um projeto de rede, pois é quando se identificam os bens que se pretende proteger contra as mais diversas ameaças, que podem envolver desastres naturais, ataques de *hackers*, erros acidentais de configuração, falhas na política de segurança, *spam*, negligência, entre outros. A Figura 10 ilustra alguns exemplos que caracterizam fatores de risco.

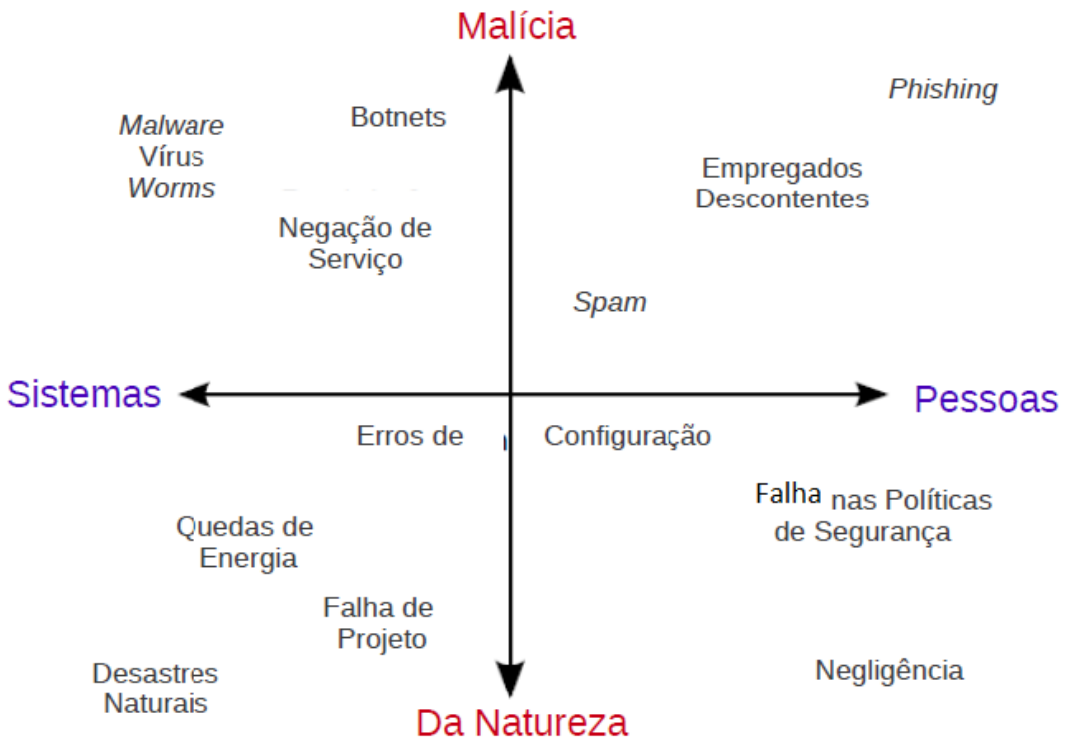


Figura 10 - Factores de risco: natureza versus malícia e sistemas versus indivíduos (Fonte: [42])

A identificação das ameaças numa rede de computadores é extremamente importante, pois elas fazem uso das vulnerabilidades para atingir o sistema de segurança. As ameaças e os riscos de segurança estão fortemente interligados: identificando-se os riscos, podem-se identificar as ameaças.

Utilizadores de sistemas computacionais geralmente não possuem conhecimento dos impactos e consequências das suas ações sobre a segurança da rede de dados. Muitas vezes as falhas de segurança não partem de uma ação mal intencionada, mas são antes causadas por ignorância ou erro humano.

As ameaças incluem geralmente incidentes envolvendo vandalismo, roubo de equipamento ou dados, intrusão, entre outras situações, variando de uma organização para outra [43]. Inúmeras vezes a principal ameaça à segurança da rede de computadores parte de dentro da própria empresa, tem origem nos próprios utilizadores que promovem possíveis vulnerabilidades que podem ser exploradas por atacantes [34].

3.1.1 Instabilidades e Ataques

A *internet* traz grandes benefícios para as empresas mas constitui também um problema. De facto, empregados e clientes passam a ter acesso remoto à organização, mas esse novo acesso pode acarretar enormes problemas causados por indivíduos que tentam burlar a segurança da rede ilegalmente, através de vulnerabilidades, ou seja, pontos fracos no projeto da rede que podem ser explorados com más intenções.

As vulnerabilidades envolvem a presença de falhas ou *bugs* nos mais variados sistemas, tais como sistemas operativos, aplicações desatualizadas, correções contra vírus e *spywares*, utilização de senhas que podem ser quebradas facilmente, entre outros [42].

Segundo [44], as principais falhas de segurança são causadas pela complexidade nas aplicações, já que o avanço computacional fez com que os códigos, alguns deles executados em dispositivos de rede, fossem cada vez mais amplos e complexos, podendo conter desde centenas a milhares de linhas.

Para um utilizador normal, manter uma rede segura parece ser simples, supondo que para isso basta criar senhas complexas e ter um antivírus. Mas não existe uma solução simples para proteger uma rede de computadores. Tal facto percebe-se devido a diferentes tipos de ataques sofridos pelos utilizadores no seu quotidiano. São gastos anualmente milhões de euros em segurança de informação, não diminuindo a taxa de sucesso de ataques.

Segundo [42], ataque pode ser definido como uma ou mais tentativas de comprometer a confidencialidade, integridade e disponibilidade da rede de dados no sentido de obter um controlo parcial ou total de dispositivos que se comunicam em rede. A maioria dos ataques não são casuais. O invasor acredita que há algo a ganhar em atacar a segurança do sistema. Esses ataques podem ser oriundos de fontes internas ou externas, por algum utilizador desatento, ou mal-intencionado, por um ex-funcionário insatisfeito com a demissão ou por algum atacante desconhecido [34].

Algumas invasões são efetuadas simplesmente para que seja percebido que um determinado *site* ou *host* foi atacado, desconfigurando o *site* com textos ou imagens. Outros são mais maliciosos, procurando extrair informações importantes. Noutros casos, pode acontecer quebra de senhas ou até mesmo se efetuada a clonagem de um *site* inteiro, fazendo com que os utilizadores sejam direcionados para um local desconhecido [29].

Os ataques à rede podem ser classificados como ativos ou passivos [45]:

- os ataques ativos incluem injeção de ficheiros maliciosos, alterações de dados ou congestionamento da rede, tendo a intenção de causar prejuízos à vítima. Este tipo de ataque só pode ser identificado através dos rastos deixados pelo invasor;
- os ataques passivos, na maioria das vezes, não têm intenção de prejudicar o funcionamento da rede, mas sim obter informações ou dados sigilosos, tornando-se deste modo difíceis de detetar.

3.1.2 Tipos de Ataques

Em seguida, são descritos os principais tipos de ataques sofridos nas redes de computadores, suas definições, as principais dificuldades para conseguir contê-los e a caraterização dos atacantes. Por fim, são apresentadas algumas defesas que uma rede deve apresentar para se tornar mais segura.

3.1.2.1 Malware

A referência [23] resume o termo *malware* como sendo equivalente a software malicioso, tal como vírus, *worms* e cavalos de troia. Os códigos maliciosos são injetados, segundo [43], com a finalidade de infiltrar-se no computador do utilizador, sem que este conheça ou permita. As três principais categorias de *malware* são: programas que não visam ganhos comerciais; programas que têm por objetivo ocultar a identidade dos invasores e softwares que visam o roubo de dados e consequente ganho comercial.

A palavra *malware* vem do termo mal, de maldade. Na definição de [44], muitos programadores desenvolvem este tipo de aplicação com o intuito de brincadeira, outros como forma de vandalismo, de protesto ou mesmo de roubo. Observam os autores ainda que *malware* deve ser visto como um software que faz com que intencionalmente o sistema passe a não se comportar de maneira correta.

3.1.2.2 Força bruta

Este tipo de ataque caracteriza-se por simples tentativas de acertar a senha testando todas as possibilidades de forma exaustiva, ou seja, o atacante não tenta invadir o sistema ou parar o serviço, apenas acredita que tentando todas as possibilidades terá sucesso [34] Levando em consideração que serão testadas todas as possibilidades, nenhum algoritmo de criptografia é imune a este ataque. O atacante esta ciente do tempo necessário para quebrar

a criptografia, já que dependendo da senha utilizada, o tempo para que um ataque de força bruta tenha sucesso pode ser de dias, semanas, anos ou até mesmo ser considerado computacionalmente incalculável.

Tendo em vista a relação entre o tamanho da senha e o tempo necessário para obter êxito na sua descoberta, [34] calcularam o número de possibilidades para diversos tamanhos da chave e diversos algoritmos criptográficos, tal como se apresenta na Tabela 3. É possível observar que, com o aumento do tamanho da chave, o número de combinações possíveis aumenta de maneira exponencial e, consequentemente, o tempo e os recursos computacionais exigidos para decifrar a senha são cada vez maiores.

Tabela 3 - Métodos de criptografia

Criptografia	bits na chave	Número de possibilidades
Netscape	*40*	1.1×10^{6}
Data Encryption Standard DES)	*56*	72.1×10^{6}
Triple DES (2 keys)	*112*	5.2×10^{33}
International Data Encryption Algorithm (IDEA)	*128*	3.4×10^{38}
Rivest Cipher (RC4)	*128*	3.4×10^{38}
Triple DES (3 keys)	*168*	3.7×10^{30}
Blowfish	*UP to 448*	
Advanced Encryption Standard (AES)	128, 192, 256	$3.4x10^{38}$

Segundo [23], geralmente os ataques são feitos utilizando um nome de utilizador conhecido. Esses ataques são mais facilmente percebidos pelos administradores, já que as tentativas de *login* são registradas.

3.1.2.3 Ataques Denial of Service (DoS)

Segundo [46], um ataque *DoS* é caracterizado como uma tentativa explícita de impedir que os utilizadores que devem ter acesso a determinado serviço não o consigam fazer. As técnicas mais utilizadas para alcançar os objetivos são: tentativas de inundar a rede e impedir o tráfego legítimo, tentativas de bloquear um servidor pelo envio de inúmeros pedidos até que ele não consiga responder a todos, envio de pacotes mal formados para servidores ou serviços; e tentativas de interromper um serviço como um todo ou para determinado utilizador.

Normalmente, os ataques de *DoS* não são capazes de causar falhas em todos os serviços da rede, já que são ataques direcionados a serviços, como o *Domain Name System* (*DNS*), para que os clientes não o consigam utilizar [43]. Nesse sentido, os ataques de *DoS* podem resultar num consumo exagerado de recursos da rede ou de um servidor, em modificação

ou alteração de configuração em dispositivos ou falhas em serviços como bases de dados ou servidores *web*.

A referência [23] explica que ataques de *DoS* não podem ser evitados, sendo apenas possível detetar este tipo de ataque quando ele já estiver em curso, tomando então as medidas apropriadas para que os ataques não surtam efeito.

Uma variação dos ataques *DoS* são os ataques do tipo *Distributed Denial of Service* (*DDoS*), em que vários atacantes despoletam ataques contra o mesmo alvo, normalmente um serviço válido, com a tentativa de executar mais pedidos do que pode ser atendido [46]. Os atacantes são máquinas *zombie*, máquinas cujos utilizadores não têm conhecimento de que o seu *host* está a participar no ataque. Na Figura 11 ilustra-se os agentes de um ataque *DDoS*.

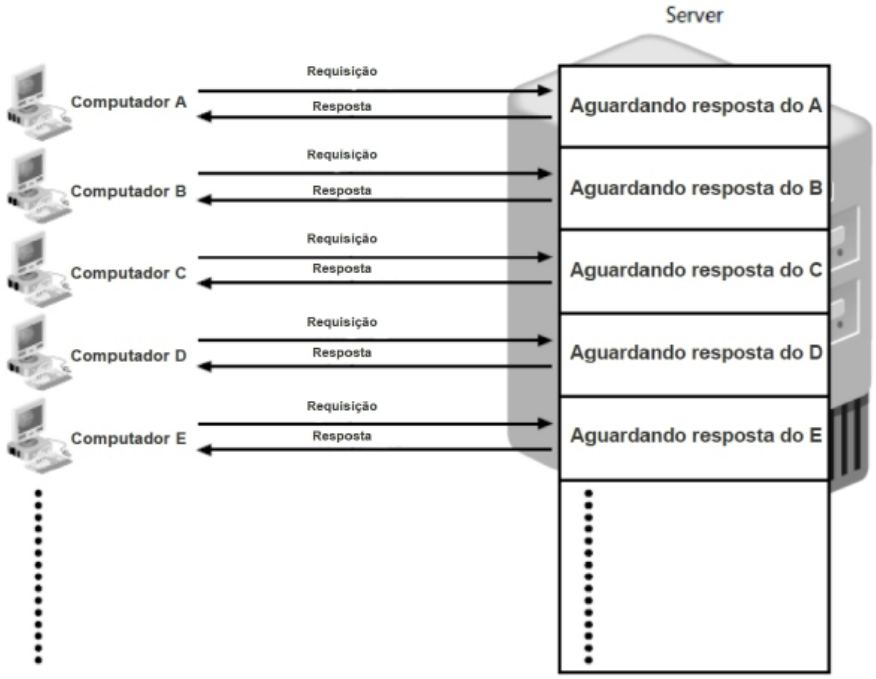


Figura 11 - Formato de um ataque DdoS (Fonte: [46])

3.1.2.4 Spoofing

Segundo [29], o termo *spoofing* significa representar ou fazer-se passar por alguém, ou seja, o atacante fingir ser alguém ou outra coisa, apresentando informações falsas. Para [23], um ataque *spoofing* envolve a falsificação do endereço de origem. É o ato de usar uma máquina para representar o papel de outra. A maioria das aplicações e ferramentas no *Unix* baseiam-se na autenticação do IP de origem.

Há uma variedade de ataques diferentes que usam *spoofing*:

- como a maioria dos sistemas de rede mantêm registos de atividade do utilizador, um invasor pode falsificar o seu endereço para que as suas ações sejam atribuídas a um utilizador válido;
- um invasor pode falsificar o seu endereço de rede utilizando um endereço confiável e conhecido, a fim de enganar o computador de destino;
- pode-se mostrar uma janela de *login* fictícia a pedir o nome e senha, permitindo que o invasor capture as credenciais válidas de um utilizador.

3.1.2.5 Engenharia social

A engenharia social é o processo de obtenção de informações sobre algo ou alguém baseado na sua confiança, ou seja, o atacante procura por diversos meios obter informações sigilosas de pessoas que conhece. Este ataque também envolve uma interação entre o atacante e o atacado, seja por meio de telefone, um anexo de *e-mail* pedindo informações ou *sites* nos quais a vítima, confiando no atacante, lhe concede informações [43].

O ataque de engenharia social, segundo [43] e [44], é o mais difícil de ser bloqueado, sendo a sensibilização dos utilizadores sobre a importância de manter os dados e as informações seguras o único meio de mitigá-lo. Esta técnica é uma das mais antigas, existindo casos de atacantes que acionam serviços de suporte fazendo-se passar por utilizadores legítimos.

3.1.2.6 Buffer Overflow

Um ataque do tipo *Buffer Overflow* tira partido de um erro de programação num programa, aplicação ou sistema. O *hacker* pode inserir o seu próprio código num programa e a partir daí assumir o controlo de um sistema. Por ser resultado de um erro de programação, é quase impossível para um técnico de rede detetar condições de *Buffer Overflow*. Estes ataques são normalmente detetados por *hackers* ou pelo fabricante do software [23].

De acordo com [43], *Buffer Overflow* é uma condição no sistema que causa uma falha na sua segurança ou a utilização indevida de memória que provoca uma falha no sistema. Um atacante pode lançar esse tipo de ataque escrevendo código malicioso especificamente destinado a usar toda a memória do sistema alvo.

Quando um programador escreve uma aplicação, cria *pools* de memória para aceitar entrada de utilizadores ou de outras aplicações. Por exemplo, uma aplicação de *login* deve alocar espaço de memória para permitir que o utilizador insira um nome de *login* e uma senha. Para alocar espaço de memória para esta informação, o programador deve fazer uma previsão sobre o tamanho dos dados que serão recebidos para cada variável. *Buffer Overflow* ocorre quando são recebidos mais dados por um processo do que o esperado e não existe contingência para quando o processo tem de lidar com uma quantidade excessiva de dados [34].

Segundo [13], estes são os ataques mais difundidos na *internet*, representando quase metade de todas as vulnerabilidades encontradas. A Figura 12, ilustra um ataque do tipo *Buffer Overflow*.

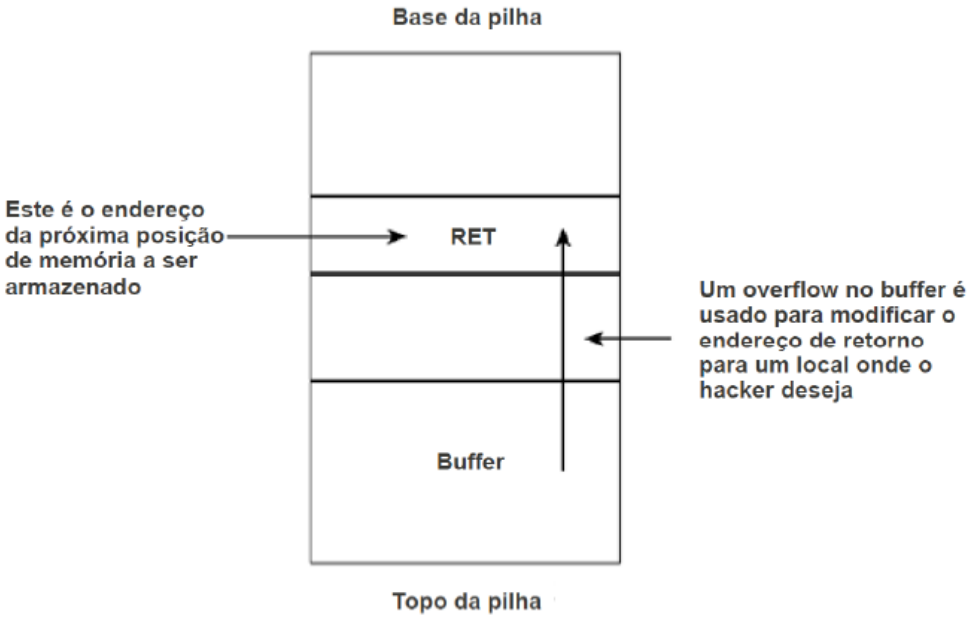


Figura 12 - Exemplo de um ataque do tipo Buffer Overflow (Fonte: [13])

3.1.2.7 Repetição

De acordo com [29], um ataque de repetição é semelhante a um ataque passivo do tipo *man-in-the-middle*. Considerando que um ataque passivo envia imediatamente a informação a transmitir, um ataque de repetição faz uma cópia da informação antes de a enviar para o destinatário. Uma repetição simples *man-in-the-middle* implica a captura das credenciais de login entre o computador cliente e o servidor. Quando a sessão termina, o ataque do tipo *man-in-the-middle* tenta repetidamente as credenciais capturadas. Um ataque mais sofisticado aproveita as comunicações entre um dispositivo de rede e um

servidor, uma vez que são frequentemente enviadas entre os dispositivos de rede e o servidor mensagens de administração que contêm pedidos específicos. Quando o servidor recebe a mensagem, responde com outra mensagem administrativa para o remetente. Para evitar este tipo de ataques, cada uma das transmissões deve ser criptografada, impedindo que o atacante possa ver o seu conteúdo, e deve incluir um código que indica se a mensagem foi alterada. O servidor lê o código e, se reconhecer que a mensagem foi alterada, não responde [47].

Usando um ataque de repetição, um atacante pode capturar uma mensagem transmitida a partir do dispositivo de rede para o servidor. Mais tarde, poderá enviar a mensagem original para o servidor, que poderia responder pensando ter sido encaminhada pelo dispositivo válido. Neste momento, é estabelecida uma relação de confiança entre o atacante e o servidor, o atacante sabe que vai receber uma resposta do servidor cada vez que envia uma mensagem. Sendo assim, pode usar esse conhecimento como uma ferramenta valiosa para alterar o conteúdo da mensagem captada. Dessa forma, consegue finalmente fazer a modificação e o servidor irá responder informando o atacante que ele teve sucesso na transferência da mensagem [48].

3.1.3 Dificuldades para evitar ataques

Segundo [29], existem várias dificuldades para conter um ataque à segurança de uma rede:

- **velocidade nos ataque**s: com várias ferramentas disponíveis, os atacantes podem rapidamente encontrar pontos fracos ou falhas no sistema pelos quais podem lançar ataques rápidos e sem precedentes;
- **ataques mais sofisticados**: a constante sofisticação dos ataques torna-os cada vez mais complicados de intercetar;
- **ataques distribuídos**: os invasores podem fazer uso de várias fontes, o que torna impossível evitar o ataque por meio da identificação de um único *host;*
- **confundir o utilizador**: nos ataques atuais existe pouca ou nenhuma informação para corrigir o problema, tornando assim complicado tomar uma decisão;
- **simplicidade nas ferramentas de ataques**: antigamente o atacante necessitava de um bom conhecimento técnico sobre a ferramenta que iria utilizar para efetuar o ataque. Hoje em dia, essas ferramentas estão disponíveis na *internet* e não requerem nenhum conhecimento técnico para serem executadas.

Na Figura 13 apresenta-se uma comparação entre a sofisticação dos ataques e a dificuldade de intrusão nos últimos anos .

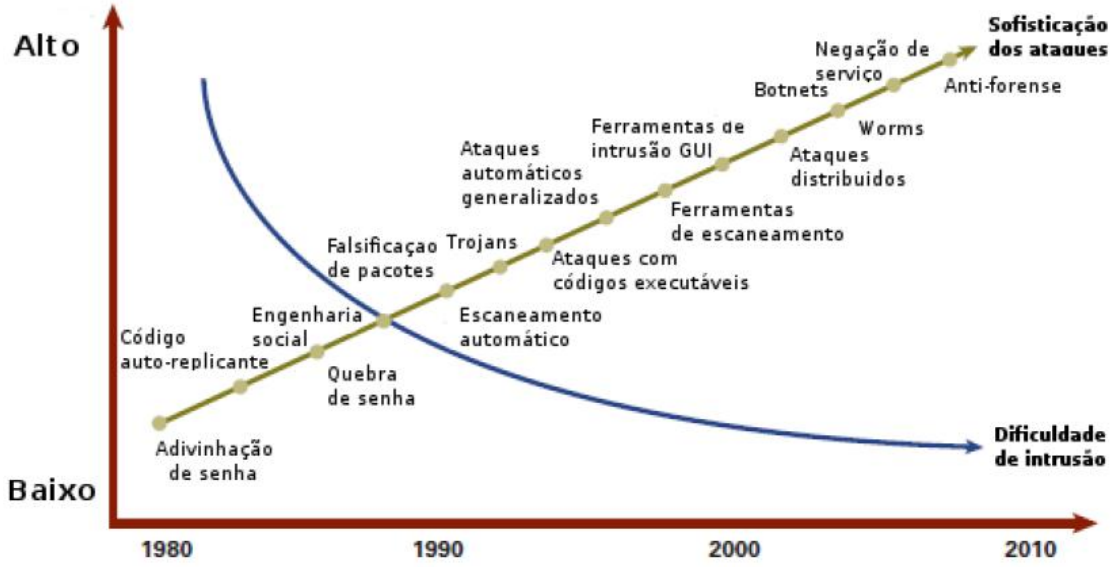


Figura 13 - Sofisticação nas ferramentas de ataques (Fonte: [45])

3.1.4 Agentes que fazem ataques

Com a crescente disponibilização de serviços via *internet*, as empresas ganharam em agilidade mas abriram portas para acessos indevidos, que podem ser exploradas por diversos grupos de atacantes [23].

Existem vários tipos de pessoas por detrás dos ataques, que podem ser separadas em diferentes grupos: *hackers, crackers, script kiddies,* espiões, funcionários, criminosos e ciberterroristas, entre outros [29].

3.1.4.1 Hackers e Crackers

Embora exista dificuldade em diferenciar os dois termos que são utilizados para definir pessoas que invadem sistemas, o termo *hacker* considera pessoas que são bons programadores, que conhecem os sistemas, estudam-nos com a finalidade de aumentar o conhecimento e domínio da tecnologia, enquanto os *crackers* são pessoas que causam problemas de segurança recorrendo a atividades ilegais. O que mais desafia e motiva esses atacantes são declarações, normalmente proferidas por departamentos comerciais, de que os seus sistemas são 100% seguros [23] .

A referência [29] salienta que, por lei, todos os ataques são considerados ilegais, mas alguns *hackers* consideram que é ético invadir um *host* desde que não se afete sua integridade, sem cometer roubo, vandalismo, ou qualquer quebra de confidencialidade. Esses *hackers* afirmam que a sua motivação é melhorar a segurança procurando falhas no sistema para que estas possam ser posteriormente corrigidas.

3.1.4.2 White Hat Hackers

Este grupo considera-se bem intencionado, invadindo sistemas não para benefício pessoal mas com a intenção de encontrar algum problema, seja uma rede vulnerável, um sistema mal configurado, um *bug* de software ou qualquer aspeto que possa prejudicar a segurança. Caso sejam encontradas falhas, os hackers relatam o ocorrido para o administrador de rede ou para o responsável pelo software ou hardware [29].

Os *White Hat Hackers* também são contratados por empresas para testar as defesas da rede. A principal característica deste grupo é estar bem informado sobre vulnerabilidades, assim como ter alta capacidade de programação. Normalmente escrevem as suas próprias ferramentas de *cracking* [34].

3.1.4.3 Espiões

Os espiões são indivíduos contratados para atacar um computador ou um sistema específico com o intuito de obter informações importantes para quem os contrata. Ao contrário dos *hackers* e dos *script kiddies*, os espiões procuram não deixar rastos e não chamar a atenção para as suas ações [23] .

3.1.4.4 Empregados

Uma das maiores ameaças para as empresas, quando o assunto é segurança da informação, reside numa fonte muito improvável, os seus próprios funcionários, já que eles conhecem mais da rede, dos sistemas e da segurança do que quaisquer outras pessoas. Funcionários descontentes podem ter a intenção de retaliar contra a empresa. Em alguns casos, podem ser motivados por dinheiro, no sentido de fornecer informações a terceiros [23]. As principais ameaças vindas dos empregados são:

- empregados utilizando técnicas *hacker* para aumentar o seu nível de acesso, permitindo o acesso e divulgação de segredos comerciais, roubar dinheiro, entre outros;

- empregados que divulgam os dados a que legitimamente têm acesso com o intuito de obter ganhos financeiros;
- familiares que, em momentos de visita, ganham acesso aos computadores e sistemas da empresa;
- pessoal que consegue acesso físico ao *datacenter* e tem a possibilidade de causar algum dano;
- antigos funcionários que podem vingar-se em ataques físicos ou por meio de técnicas *hacking*.

Além das ameaças intencionais, [23] cita algumas ameaças sem intenção que podem ser causadas pelos empregados:

- ser vítima de um ataque de engenharia social, ajudando um atacante a ganhar acesso não autorizado à rede ou aos sistemas;
- involuntariamente revelar dados confidenciais;
- fisicamente danificar ou causar falhas em equipamentos que resultem em perda de dados ou indisponibilidade de acesso;
- introduzir ou modificar dados com valores inconsistentes ou errados, ou, acidentalmente, apagar dados.

Essas ameaças somente podem ser tratadas e evitadas dando mais formação aos utilizadores, já que muitos escrevem senhas em monitores e cadernos, permitem o acesso ao computador das empresas, entre outras falhas graves.

3.1.4.5 Ciberterroristas

Os ciberterroristas são *hackers* motivados por crenças políticas, religiosas ou filosóficas, que atacam posições opostas ás suas ideologias. São considerados os atacantes mais temidos, pois é quase impossível prever quando ou onde podem despoletar um ataque. Os seus objetivos podem incluir um pequeno grupo de computadores ou redes que podem afetar um elevado número de utilizadores (podemos por exemplo pensar nos computadores que controlam uma rede de energia elétrica, provocando um colapso geral; neste caso, um ataque isolado pode causar um apagão que afeta dezenas de milhões de pessoas).

3.1.4.6 Black Hat Hackers

É considerado o grupo mais perigoso, já que são pessoas preparadas para agir, motivadas pela ganância ou por grande vontade de causar danos a terceiros. Criam as suas próprias ferramentas e são muito cuidadosas para não deixar rastos [34].

3.1.5 Fases de um ataque

Atualmente existem vários tipos de ataques, que são compostos por cinco etapas [29]:

- **procura de informações**: é a primeira etapa de um ataque e consiste em sondar informações que possam ser usadas nos próximos ataques, tais como o tipo de hardware utilizado, versão de software ou *firmware* e até mesmo informações pessoais sobre os utilizadores;
- **invasão de qualquer defesa**: após a identificação de portas e a recolha de informação, o passo seguinte é intensificar o ataque com a finalidade de quebrar a defesa, o que pode ser este de várias formas, como, por exemplo, quebra de senhas;
- **modificação das informações de segurança**: logo após invadir um sistema, o próximo passo é modificar as informações de segurança, permitindo assim que o acesso seguinte seja feito com maior facilidade;
- **apropriação de outros *hosts* ou sistemas**: assim que um *host* tenha sido comprometido, é utilizado para atacar outros computadores na rede;
- **congelamento das redes e dispositivos**: se o invasor quiser, pode trabalhar de forma maligna, infetando o computador, danificando dados, roubando ficheiros valiosos ou realizando ataques de negação de serviço.

Na figura 14 são ilustradas as várias etapas de um ataque.

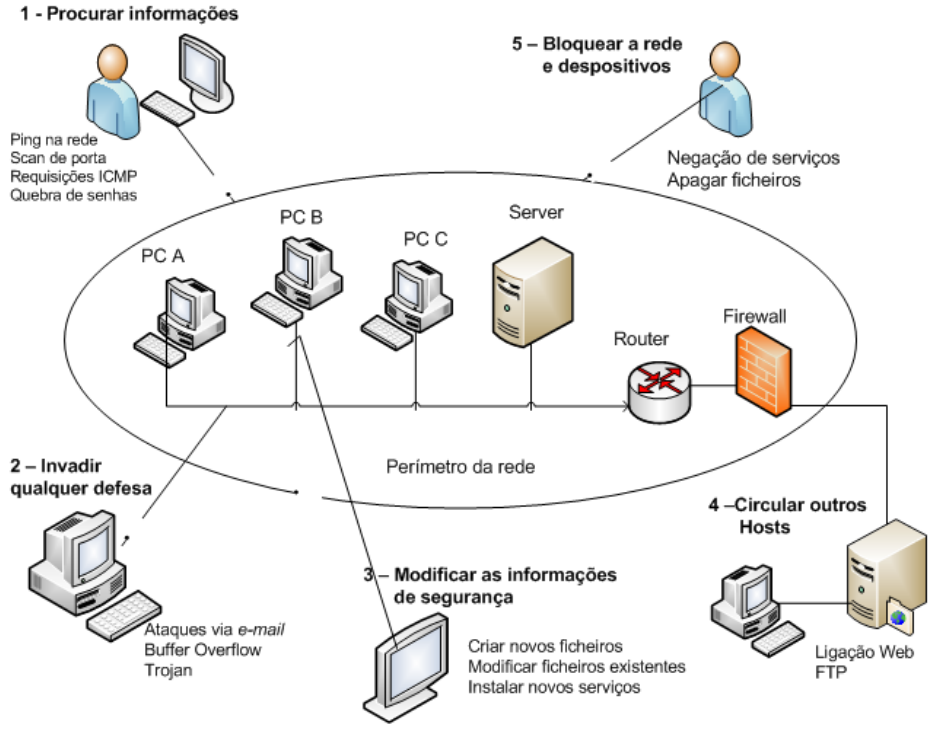


Figura 14 - Etapas de um ataque (Fonte: [29]).

3.1.6 Estratégias de defesa contra ataques

Num contexto ideal, qualquer indivíduo que utiliza um sistema de rede devia estar ciente das questões de segurança e ter a capacidade de tomar medidas defensivas. No entanto, na prática, a tarefa de proteger redes e sistemas recai sobre os administradores dos sistemas. Estes muitas vezes não são apenas responsáveis pela configuração e acompanhamento das redes contra ataques, mas também por ter um papel ativo na execução das políticas de segurança formais e informais e sensibilizar os utilizadores sobre possíveis vulnerabilidades [42].

Um dos principais problemas relacionados com a segurança da rede é a falta de investimento que, em parte, decorre da dificuldade de quantificar o valor associado à segurança. No entanto, esse impasse está a mudar e as grandes organizações começaram a perceber a importância da segurança da rede de dados depois de elas se terem tornado numa parte importante do negócio. Consequentemente, tem surgido um grande número de empresas de segurança que atuam na prestação de serviços de segurança, tanto para os indivíduos como para as organizações. A utilização de *firewalls*, atualização de sistemas operativos, implementação de programas antivírus tornaram-se comuns. Embora tenha

aumentado a preocupação com a defesa da rede e o número de serviços prestados nesta área, as defesas devem ser baseadas em cinco princípios fundamentais de segurança: **proteção por camadas**, **limitação**, **diversidade**, **simplicidade** e **obscuridade**.

3.1.6.1 Proteção por camadas

A abordagem em camadas tem a vantagem de criar uma barreira de defesas múltiplas que possam ser coordenadas para prevenir uma variedade de ataques. A segurança da informação também deve ser criada em camadas, pois um mecanismo de defesa simples pode ser relativamente fácil de ser atacado. Num sistema de segurança protegido por camadas torna improvável que um invasor tenha as ferramentas e habilidades necessárias para romper todas as camadas de defesas. Sendo assim, a abordagem em camadas pode ser útil para resistir a uma variedade de ataques, fornecendo uma proteção mais abrangente.

3.1.6.2 Limitação

Quando se limita o acesso à informação reduzem-se as potenciais ameaças. Limitar é garantir que somente pessoas autorizadas têm acesso aos dados importantes. Além disso, a quantidade de acesso concedido a alguém deve ser limitada ao que a pessoa precisa de saber [29].

Algumas maneiras de limitar o acesso são baseadas em tecnologias como a atribuição de permissões de leitura e não de modificação de ficheiros, enquanto outros são processuais e proíbem um funcionário de remover um documento necessário ao funcionamento do sistema.

3.1.6.3 Diversidade

A diversidade está relacionada com a proteção organizada por camadas. Assim como é importante proteger os dados utilizando estratégias baseadas em camadas, a diversidade de camadas deve ser tal que os atacantes, ao penetrarem numa camada, não possam usar as mesmas ferramentas para atingir as camadas seguintes. Assim, ao ser violada uma camada, não se compromete todo o sistema [29].

3.1.6.4 Simplicidade

Os ataques podem vir de várias fontes e de diversas maneiras. Os sistemas complexos são difíceis de compreender e permitem muitas oportunidades para que algo não funcione.

Manter um sistema simples para o administrador e complexo para o atacante pode ser difícil mas, uma vez conseguido, gera um grande benefício para a segurança da rede [29].

3.1.6.5 Obscuridade

Um exemplo de obscuridade seria não revelar o tipo do computador, sistema operativo, software e ligação de rede utilizados por um *host.* Com essas informações ocultas fica muito mais difícil a um atacante descobrir os pontos fracos do sistema. Inclusive, em muitos casos quando um atacante não consegue essas informações, parte para outro computador no qual a informação é facilmente encontrada [29].

3.2. Política de segurança

Uma política de segurança é um conjunto de regras, práticas e procedimentos que ditam como as informações sensíveis serão geridas, protegidas e distribuídas. Na esfera de segurança de rede, as políticas são geralmente pontos específicos que abrangem uma única área. Uma política de segurança é um documento que expressa exatamente o que deve ser feito para estabelecer os níveis de segurança, quais são os objetivos a ser alcançados pelos mecanismos que controlam a segurança da rede de dados. Este documento é escrito pela gestão de segurança e destina-se a descrever os "porquê" e os "como" de segurança da informação, descrevendo procedimentos padrão, referências e diretrizes na implementação da política [35].

De acordo com [23], é necessária uma quantidade significativa de esforço para preparar e manter uma política de segurança útil. Tal como um documento de requisitos de sistema, ela precisa de ser revista em intervalos de tempo regulares para determinar a necessidade de atualização.

A confiança é um dos principais temas em muitas políticas. Algumas organizações confiam demais nos seus empregados e acreditam que todos vão fazer o que está certo. Mas isso nem sempre acontece. Sabe-se que a maioria das organizações precisa de políticas para assegurar que todos estão em conformidade, seguindo o mesmo conjunto de regras [35]. As políticas tendem a elevar a apreensão das pessoas, já que elas não querem se comprometer com regras e regulamentos. A política deve definir o nível de controlo de utilizadores, observar e conciliar com as metas de produtividade. Uma política de rigor excessivo será difícil de implementar porque o cumprimento pode ser minimizado ou

ignorado. Pelo contrário, uma política definida vagamente pode ser evadida e não garantir a responsabilização. Uma boa política tem que ter o equilíbrio certo.

De seguida são apresentados os principais itens que compõem uma política de segurança.

3.2.1. Objetivos da política de segurança

A referência [47] explica que os objetivos fundamentais da política de segurança são permitir acesso ininterrupto a recursos da rede para utilizadores autenticados e negar o acesso aos não autenticados. É claro que isso é sempre um ato de equilíbrio entre as necessidades dos utilizadores e a natureza evolutiva da tecnologia da informação. Os utilizadores preferem abrir acessos, enquanto o administrador da rede insiste em acesso restrito e controlado. Assim que o *hacker* descobre uma possível falha de segurança por meio de acesso não autorizado, torna-se o árbitro da política de segurança. Assim, o projeto de segurança de redes e sua implementação representa a derradeira batalha das mentes entre o chefe de segurança e o *hacker*. As funções essenciais de uma boa política de segurança são:

- nomear um administrador de segurança familiarizado com as necessidades dos utilizadores;
- configurar uma política de segurança hierárquica para refletir na estrutura corporativa;
- definir os recursos de acesso éticos à *Internet*;
- evoluir a política de acesso remoto;
- fornecer um conjunto de procedimentos de tratamento de incidentes.

3.2.2. A importância da política de segurança

A política de segurança é a base para todas as questões relacionadas com a proteção da informação. A necessidade de estabelecer uma política de segurança é um fato realçado unanimemente em recomendações provenientes tanto do meio militar como do meio técnico e, mais recentemente, do meio empresarial [9].

É por meio dessa política que todos os aspetos envolvidos na proteção de recursos existentes são definidos e, portanto, grande parte do trabalho é dedicado à sua elaboração e planeamento [35].

Segundo [23], uma política de segurança é um documento que define a filosofia e a estrutura de segurança da organização. Serve para vários propósitos:

- tornar mais fácil para a equipa de TI justificar gastos com a segurança;
- identificar o uso aceitável de recursos de computação numa organização;
- identificar quem tem acesso a quê;
- funcionar como um contrato de segurança com os empregados.

Além do seu papel primordial nas questões relacionadas com a segurança, a política de segurança, uma vez fazendo parte da cultura da empresa, tem a importante função de facilitar e simplificar a gestão de todos os recursos. A gestão de segurança é a arte de criar e administrar a política de segurança, pois não é possível gerir o que não pode ser definido [9].

3.2.3 O planeamento da política de segurança

Na fase inicial do planeamento da política de segurança, existe a necessidade de compreender todos os riscos que podem ser encontrados. Uma abordagem reativa pode trazer problemas futuros para a organização. Sendo assim, a proatividade é essencial e depende de uma política de segurança bem definida, com definições de responsabilidades individuais claras de modo que facilite a gestão da segurança da rede [9].

O planeamento de uma política de segurança envolve a definição do que é uma política de segurança, entender o seu ciclo e conhecer as etapas do seu desenvolvimento. Existem vários termos para se definir uma política de segurança, mas um conjunto de requisitos específicos tem que ser seguido e cumprido.

Uma visão geral do planeamento pode ser observada na Figura 15, cuja pirâmide mostra que a política fica no topo, acima das normas e dos procedimentos.

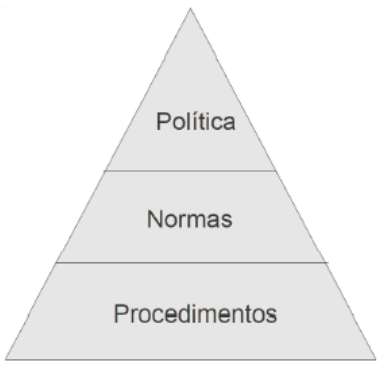


Figura 15 - planeamento da política de segurança (Fonte: [9])

A **política** é o elemento que orienta as ações e as implementações futuras, de uma maneira global, enquanto que as **normas** abordam os detalhes, como os passos da implementação, os conceitos e os projetos de sistemas e controlos. Os **procedimentos** são utilizados para que os utilizadores possam cumprir aquilo que foi definido na política e os administradores de sistemas possam configurar os sistemas de acordo com as necessidades da organização [9].

3.3. Mecanismos de Defesa das Redes

Neste capítulo são descritos os principais mecanismos de defesa de redes, como *firewall*, controlo de acesso, antivírus, criptografia, entre outros.

3.3.1. Firewall

A necessidade de utilização cada vez maior da *internet* pelas organizações e a constituição de ambientes corporativos levam a uma crescente preocupação com a segurança. Como consequência, verificou-se uma rápida evolução nesta área, principalmente em relação à *firewall*, que é um dos principais componentes do sistema de segurança. Um *firewall* é um ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, pelo qual passa todo tráfego, permitindo o controlo, a autenticação e os registo de toda a informação trocada.

Em [34], os autores definem *firewall* como uma barreira de proteção que controla o tráfego de dados entre um computador e a *internet*. Ao contrário de um simples router, que apenas direciona o tráfego de rede, o *firewall* é um sistema que reforça uma política de controlo de acesso. Depois de determinar os níveis de acesso que se pretendem fornecer, o *firewall* garante que nenhum acesso além do determinado será permitido. Cabe ao *firewall* garantir que a política de controlo de acesso seja seguida por todos os utilizadores.

Segundo [29], um *firewall* é normalmente usado para filtragem de pacotes, projetado para impedir a entrada de dados maliciosos ou não permitidos. Pode ser baseado em *software*, mais adequado para o uso doméstico, podendo ser executado localmente na máquina do utilizador, ou *hardware*, localizado num ponto específico para proteger uma rede inteira. Os *firewalls* de *hardware* estão normalmente localizados fora do perímetro da rede, atuando como a primeira linha de defesa.

Um exemplo de localização de *firewalls* é mostrado na Figura 16.

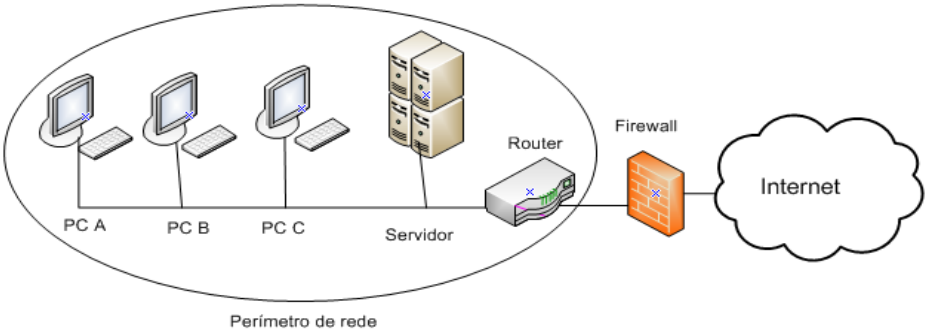


Figura 16 - Firewall como primeira linha de defesa

Como uma primeira linha de defesa, o *firewall* tem como objetivo bloquear todos os tipos de acesso indevidos, que não estão de acordo com a política de segurança. Isto acaba por contribuír para uma falsa expectativa relativamente à segurança total da organização. É importante ter em mente que o *firewall* é apenas uma parte de um conjunto de componentes de um sistema de segurança necessário para a proteção das organizações. Para uma proteção ideal é necessário fazer uso de outras ferramentas, como IDS/IPS, antivírus, controlo de acesso, entre outras, que serão abordadas mais tarde neste capítulo.

3.3.2. Controlo de acesso

O controlo de acesso refere-se ao método de conceder ou negar acesso a recursos de rede por meio de políticas de segurança. Na sua forma mais simples, controlo de acesso é aplicado em ficheiros e pastas, ou em outros recursos de rede partilhados por meio de atribuição de permissões [43]. A seguir descrevem-se as principais categorias que envolvem o controlo de acesso.

3.3.2.1 Mandatory Access Control (MAC)

Mecanismo, normalmente codificado num sistema operativo, que tem a função de proteger computadores, dados e dispositivos do sistema de um uso/acesso não autorizado [43].

3.3.2.2 Role Based Access Control (RBAC)

Usado para implementar mecanismos de segurança com base nas funções executadas por um utilizador ou grupo de utilizadores, o RBAC é altamente flexível e configurável, fornecendo administração centralizada [43].

3.3.2.3 Discretionary Access Control (DAC)

Geralmente implementado no sistema operativo sob a forma de permissões e direitos de utilizador. Um exemplo de DAC são as permissões NTFS *(New Technology File System)* usadas nos computadores baseados no sistema operativo Windows [43].

Um antivírus é uma solução de segurança amplamente adotada. Utilizado em empresas de pequeno a grande porte, identifica e remove do computador vários tipos de *malware*. É uma das aplicações mais antigas em termos de segurança. Este software pode analisar infeções no sistema operativo, bem como monitorizar a atividade do computador verificando novos documentos, para detetar algum vírus. Uma das desvantagens é que o software deve ser atualizado constantemente para reconhecer novos vírus [29].

3.3.3 Criptografia

A criptografia é uma ciência fundamental para a segurança da informação, ao servir de base para diversas tecnologias e protocolos, tais como a infraestrutura de chaves públicas, o IP*Security* (IPSec) e o *Wired Equivalent Privacy* (WEP). As suas prioridades incluem sigilo, integridade, autenticação e o não repúdio, e garantem o armazenamento, as comunicações e as transações seguras essenciais no mundo atual [9].

A cifragem *(encryption)* compreende o processo de disfarçar a mensagem original de modo que o seu conteúdo seja escondido numa mensagem com texto cifrado, enquanto a decifragem consiste no processo de transformar o texto cifrado novamente no texto claro original [48].

Os processos de cifragem e decifragem são realizados pelo uso de algoritmos com funções matemáticas que transformam os textos claros em textos cifrados e vice-versa [9].

3.4. Segurança da informação na rede wireless

Atualmente, as redes sem fio estão cada vez mais difundidas devido à sua flexibilidade e desempenho. De facto, nos últimos anos verificou-se um grande aumento no número de redes locais sem fio, WLAN (Wireless Local Area Network), utilizadas por utilizadores domésticos, instituições, universidades e empresas. Esta crescente utilização trouxe consigo não só maior mobilidade e flexibilidade para os seus utilizadores, mas também uma maior preocupação com a segurança. É exatamente essa preocupação que faz com que novos protocolos de segurança sejam criados, desenvolvidos e atualizados.

A primeira barreira de segurança adotada foi o WEP (Wired Equivalent Privacy), o primeiro protocolo de segurança, que conferia uma certa segurança para as redes sem fio com base na camada de ligação do modelo OSI.

Após vários testes realizados com este protocolo foram detetadas algumas vulnerabilidades e falhas que fizeram com que o WEP perdesse credibilidade. No WEP a mesma chave é usada por todos os utilizadores da rede, gerando uma repetição altamente indesejável da sequência do algoritmo RC4, o que dá margem para ataques bem-sucedidos e para a descoberta de pacotes por parte de eventuais intrusos.

Para melhorar as falhas e limitações do WEP surgiu o WPA (Wi-Fi Protected Access). Este mecanismo corrigiu vários erros do WEP, mas apresenta ainda algumas falhas, para além do facto de o seu desempenho ter uma queda significativa em termos de estabilidade. Assim, surgiu o WPA2 como a promessa de constituir a solução definitiva de segurança e estabilidade para as redes sem-fio do padrão Wi-Fi.

3.4.1. WEP

O protocolo WEP (*Wired Equivalent Privacy*) foi projetado para assegurar às redes sem fio 802.11 um nível de segurança equivalente ao de uma rede de cabo. Utiliza o conceito de chaves partilhadas ou *Shared Key* e processa os dados utilizando chaves idênticas em ambos os dispositivos de ligação.

Quando a segurança no 802.11 é ativada, cada estação tem uma chave secreta partilhada com a estação base. O padrão não especifica como as chaves são distribuídas. Uma vez estabelecidas, essas chaves permanecem estáticas por meses ou anos [3].

A privacidade fornecida pelo WEP baseia-se em chaves criptográficas simétricas de 40 bits e um vetor de inicialização público de 24 bits (IV – *Initialization Vector*). Para se estabelecer ligação à essa rede a estação deve conhecer a chave actual, dessa forma um utilizador indesejado somente poderá aceder os seus dados se conseguir quebrar a criptografia do protocolo [10].

O WEP pode ser utilizado entre o Ponto de Acesso (AP – *Access Point*) e os clientes da rede (modo infra-estrutura), ou na comunicação direta entre clientes (modo *ad-hoc*).

3.4.1.1 O algoritmo RC4 e a criptografia no WEP

O protocolo WEP utiliza o algoritmo de criptografia RC4, que possui duas funcionalidades básicas: uma para gerar um “código” que será usado para encriptar e desencriptar (KSA -

Key Scheduler Algorithm) e outra para realizar a criptografia propriamente dita da mensagem com o uso deste código (PRGA).

A função KSA é responsável por gerar uma permutação pseudo-aleatória do conteúdo de uma chave secreta. O fato de ela ser pseudo-aleatória deve-se à invariância do valor devolvido com o tempo, dependendo apenas do valor de entrada. Portanto, é necessária a execução desta função apenas uma vez para a obtenção da permutação que será usada.

A função PRGA é responsável pela encriptação da mensagem a partir do valor devolvido pelo KSA. Ela consiste basicamente em operações de Ou-Exclusivo entre a permutação da chave secreta e a mensagem de entrada, devolvendo uma mensagem cifrada. Pela lógica de Boole, sabe-se que operações deste tipo são simétricas e, portanto, a aplicação do PRGA na mensagem cifrada gera a mensagem original caso a permutação utilizada seja a mesma do processo de encriptação. [3].

O RC4 é considerado um algoritmo de chave simétrica de cifra de fluxo ("*stream cypher*") pelo fato de o processo de encriptação e decriptação serem independentes do tamanho da mensagem de entrada. Como cada bit de saída é função apenas do bit de entrada, a segurança não é muito elevada.

O funcionamento do WEP pode ser dividido em duas partes: autenticação e encriptação/decriptação de mensagens. Como foi dito, o mecanismo de encriptação/decriptação baseia-se no algoritmo RC4. Para garantir maior segurança no processo, a permutação oriunda do KSA deve ser diferente para cada mensagem enviada. Para isto, existe um vetor de inicialização pseudo-aleatório que é recalculado a cada iteração do algoritmo e é acrescentado à chave secreta. Como quem recebe a mensagem não possui este valor, o mesmo deve ser incluído no texto cifrado que será enviado. Por fim, existe ainda um mecanismo que provê integridade ao conteúdo do texto cifrado que é recebido, tendo em vista que o meio de propagação da mensagem é muito suscetível a erros.

O lado esquerdo da Figura 17 demonstra o processo de encriptação da mensagem. A entidade responsável pelo envio calcula o próximo valor da sequência do vetor de inicialização, concatena-o com a chave secreta que ele compartilha com a entidade que receberá a mensagem e calcula o valor da permutação a partir do KSA. Após este processo, divide a mensagem original de forma a que esta possa caber em num pacote WEP e calcula o valor do *hash* (a partir da função CRC-32). Em seguida, é aplicado o algoritmo PRGA

sobre o pedaço da mensagem e o respectivo valor de hash. O resultado deste processo é depois concatenado com o valor atual do vetor de inicialização e finalmente enviado.

No lado direito da Figura 17 ilustra-se o processo inverso, que é realizado pela entidade que recebe o texto cifrado. Primeiramente, ocorre a separação do vetor de inicialização e da mensagem cifrada. O primeiro é concatenado com a chave secreta que é compartilhada com a entidade que realizou o envio e passa novamente pelo KSA. Com isto, obtém-se a mensagem original acrescida do *hash* no PRGA. Assim, o resultado desta função divide-se em mensagem original e *hash*. Por fim, é aplicada a mesma função resumo que fora usada pela entidade que enviou a mensagem e ocorre a comparação com o que recebeu. Caso haja alguma discrepância dos resultados, é solicitado o reenvio do pacote; caso contrário, é enviada uma mensagem de confirmação de recebimento correto.

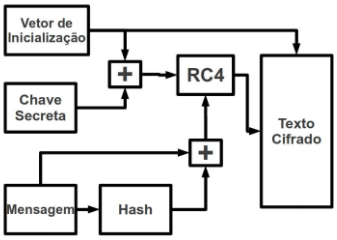


Figura 17 - O protocolo WEP

3.4.1.2 Service set identification (SSID)

O SSID, *Service Set Identifier*, é o nome designado para uma rede de área local sem fio específica. A norma 802.11 sempre forneceu alguns mecanismos de segurança básicos para impedir que a sua flexibilidade seja uma possível ameaça. Para isso, os pontos de acesso podem ser configurados com um identificador do conjunto de serviços (SSID). A placa NIC (Network Interface Card) também deve conhecer este SSID para o associar ao AP e assim passar para a transmissão e recepção de dados na rede.

A segurança proporcionada por este mecanismo é fraca pelas seguintes razões:

- Todas as placas NIC e todos os AP conhecem perfeitamente o SSID;
- O SSID é enviado por wireless de maneira transparente (sinalizado pelo AP);
- A placa NIC pode controlar localmente caso a associação de SSID desconhecido seja permitida.

3.4.1.3 Autenticação *Open System*

A autenticação *Open System*, também chamada de autenticação nula, é a forma de autenticação mais simples nas redes IEEE 802.11. As estações que requerem autenticação com esse mecanismo serão sempre autenticadas, exceto no caso de uma estação se recusar a autenticar alguma estação em particular. O mecanismo envolve dois passos:

- A estação requerente declara sua identidade e requer autenticação.
- A estação solicitada fornece o resultado da autenticação.

3.4.1.4 Autenticação *Shared-Key*

A autenticação *Shared-Key* envolve estações que partilhem uma chave secreta. Não há necessidade de transmitir a chave de forma aberta, mas o mecanismo de privacidade WEP é necessário. A chave secreta deve ser entregue às estações participantes através de um canal seguro independente do IEEE 802.11. No modo *Shared Key*, a estação que inicia a autenticação é chamada *requester* e a outra é o *responder* [3].

Esta forma de autenticação envolve quatro passos:

- *Requester* envia uma mensagem {*authentication request*} ao *responder* (AP) solicitando autenticação por *shared-key*.
- *Responder* responde com uma mensagem {*authentication response*} contendo um desafio (*challenge*).
- *Requester* cifra o desafio com a sua chave WEP e devolve-o numa nova mensagem {*authentication request*}.
- Se o *responder* decifrar o *authentication request* e obter o desafio original, ele responde com um *authentication response* concedendo acesso ao *requester*.

3.4.1.5 Vulnerabilidades do WEP

- Troca de chaves deve ser feita manualmente

  A chave deve ser partilhada por todos na rede, tanto um lado como o outro da comunicação precisa de conhecer a chave para o processo de cifragem e decifragem. Isto, num ambiente muito amplo e com muita mobilidade é um problema, por mais segura que seja a metodologia de distribuição da chave.

  Uma vez que a chave é a mesma para todos os utilizadores, cada pacote deve ter um vetor de inicialização diferente para evitar a repetição de uma mesma sequência

RC4, pois o RC4 é composto pela chave secreta e pelo vetor de inicialização de 24 bits.

- Vetor de inicialização relativamente pequeno
  Como o vetor possui o tamanho de apenas 24 bits, o período de troca fica limitado ao número de pacotes que são enviados e recebidos na transmissão. É possível que um invasor realize operações de análise estatística dos pacotes cifrados com a mesma chave durante o período de repetição.
- Colisão de pacotes, devido à reinicialização do contador do Vetor de inicialização

3.4.2 WPA

Devido a todos os problemas detetados no protocolo WEP, um grupo de investigadores da Wi-Fi Alliance e do IEEE desenvolveram um novo protocolo que resolvesse algumas das vulnerabilidades encontradas. Surgiu então no ano de 2002 a primeira versão do WPA (*Wi-Fi Protected Access*), que também foi designado por WEP2 ou TKIP (*Temporal Key Integrity Protocol*) [49].

De acordo com [50], o protocolo WPA trouxe algumas modificações na autenticação de utilizadores, usando as normas 802.1x e EAP (*Extensible Authentication Protocol*). Pode também ser utilizado com chaves partilhadas, comportando-se dessa forma exatamente como o WEP. Oferece segurança para diferentes tipos de redes, desde pequenas redes domésticas até grandes corporações. Pode ainda ser configurado em redes do tipo infra-estrutura utilizando um servidor RADIUS (*Remote Authentication Dial-In User Server*) para efetuar a autenticação dos utilizadores.

Além do valor do ICV (*Integrity Check Value*), já utilizado pelo WEP, a integridade no WPA é assegurada por mais um valor que é adicionado ao pacote, uma mensagem de verificação de integridade denominada MIC (*Message Integrity Check*).

3.4.2.1 Chaves do WPA

No WEP a chave é estática e tem a dupla função de autenticar o utilizador e criptografar a mensagem. O WPA apresenta dois grupos de chaves:

- **Pairwise Key**: É utilizada para que haja comunicação direta entre duas estações ou entre um *Acess Point* e uma estação. Neste tipo de comunicação unicast deve existir uma chave conhecida apenas pelas duas partes da comunicação.

- **Group Key**: Utilizado quando uma estação deseja comunicar-se com todas as outras estações da rede, comunicação broadcast. Neste caso, é utilizada uma chave que é conhecida por todas as estações. O *Group Key* também é utilizado para comunicações do tipo multicast, onde uma estação deseja comunicar com um grupo específico de estações.

O WPA, como foi referido anteriormente, é destinado a ambientes residenciais e corporativos. Em ambientes residenciais, utiliza-se o *WPA-PSK*, em que a chave PMK (*Primary Master Key*) é derivada da *PSK* (*Pre-Shared Key*) ou seja, a chave primária é originada pela própria chave secreta configurada no *Access Point*.

Para ambientes corporativos a chave PMK será originada a partir da MSK (*Master Session Key*), que é uma chave que foi partilhada durante o processo de autenticação 802.1x/EAP. A PMK nunca é usada para encriptação ou integridade. Ela é usada para gerar chaves temporárias (*Pairwise Transient Key - PTK*). A PTK é um conjunto de chaves, incluindo entre elas a chave de criptografia de dados (*Temporal Encryption Key – TEK* ou *TK*) e a chave de integridade de dados (*Temporal MIC Key* - TMK). Terminado o *4-Way-Hadshake* garante-se que tanto o cliente como *Access Point* têm a mesma PTK e estão prontos para a troca de dados.

3.4.2.2 Temporal Key Integrity Protocol (TKIP)

O TKIP é um protocolo de chave temporária criado em 2002 e faz parte do padrão WPA. Foi a primeira tentativa de corrigir as anomalias apresentados pelo WEP, tanto que ainda guarda algumas características do WEP como a utilização do algoritmo modificado RC4.

O TKIP usa uma chave chamada *Temporal Key*, resultante da combinação entre a chave partilhada do *Access Point* e do cliente e o endereço MAC da placa de rede wireless do cliente. O TKIP implementa um número de sequência para evitar ataques de repetição e inserção. Relativamente à integridade dos dados, é utilizado o algoritmo MIC - *Message Integrity Checksum* (Michael).

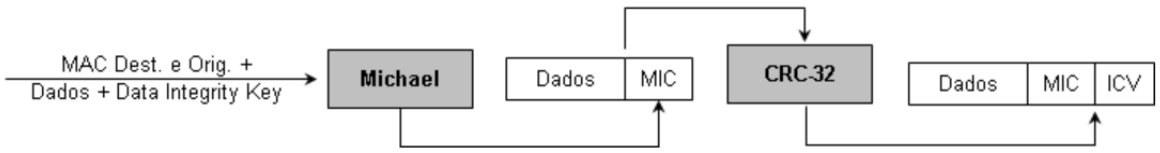


Figura 18 - Integridade WPA (http://www.infosegura.eti.br/artigos/80211.php)

3.4.2.3 Message Integrity Chec (MIC)

O MIC fornece um campo adicional de 8 bytes que protege tanto os dados do *payload* como o cabeçalho do pacote, impedindo um atacante de capturar e alterar pacotes de dados. O algoritmo que implementa o MIC é conhecido como Michael Shamir [49]. Tanto o receptor como o emissor executam e comparam os valores do MIC. Se o resultado não for semelhante, é porque houve alteração dos dados.

3.4.2.4 Extensible Authentication Protocol (EAP)

O WPA utiliza o EAP (Extensible Authentication Protocol), um protocolo de autenticação genérico, que através de um servidor central de autenticação, autentica cada utilizador antes que este tenha acesso à rede. Possibilita inúmeras formas de autenticação, inclusive certificação digital, e a sua definição foi feita na RFC 2284.

Segundo [1], o funcionamento do EAP é composto por três elementos: o cliente, um ponto de acesso à rede que deverá ser responsável pela autenticação, e um servidor de autenticação, contendo uma base de dados onde são guardadas as informações de autenticação do cliente. Essas autenticações podem ser uma simples validação de nome de utilizador e senha ou um sistema de controlo que verifica a autenticidade de uma assinatura digital, por exemplo.

O protocolo EAP, na sua definição, permite a utilização de uma grande variedade de mecanismos de autenticação, como *smart cards*, Kerberos, *public key*, *one-time passwords*. Como a maioria destes métodos só permitem a autenticação do cliente no servidor, em vários casos é preciso o suporte à autenticação mútua e a utilização de um mecanismo de estabelecimento de chaves de sessão. Isso levou à criação do protocolo EAP-TLS: este mecanismo permite a autenticação mútua e negociação do algoritmo de criptografia e chaves criptográficas antes do protocolo de aplicação transmitir ou receber dados, fornecendo privacidade e integridade na comunicação.

3.4.2.5 Vulnerabilidades do WPA

- Negação de Serviço (*Denial of service*)

  O MIC tem um mecanismo de proteção para evitar ataques de força bruta, mas esse mecanismo acarreta um ataque de negação de serviço (DoS). Quando dois erros de MIC são detectados em menos de um minuto, o AP cancela a ligação por 60

segundos e altera a chave de integridade. Portanto, com uma simples injeção de pacotes mal formados é possível fazer um ataque de negação de serviço.

- O Algoritmo de combinação de chaves é fraco
- Ataques de dicionário

  Neste tipo de ataque, o atacante testa senhas em sequência ou palavras comuns. Senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque: alguns fabricantes usam senhas pequenas (de 8 a 10 caracteres), pensando que o administrador irá modificá-las.

3.4.3 WPA2

Embora o WPA tivesse corrigido vários erros do WEP, ainda manteve algumas vulnerabilidades. Além disso, o seu desempenho teve uma queda significativa em termos de estabilidade. Houve, por isso, necessidade de criar um outro protocolo que fosse mais seguro do que o WPA e tivesse um melhor desempenho. Em setembro de 2004, a Wi-Fi Alliance apresentou o WPA2, a segunda geração de segurança do WPA, com a promessa de ser a solução definitiva de segurança e estabilidade para as redes sem-fio do padrão Wi-Fi.

O WPA2 está baseado no IEEE 802.11i, emenda da norma 802.11 ratificada em junho de 2004. Segundo muitos analistas, esta norma 802.11i era exatamente o que faltava para estimular implementações seguras de redes wireless nas empresas [49].

A principal mudança entre o WPA2 e o WPA é o método criptográfico utilizado. Enquanto o WPA utiliza o TKIP com o RC4, o WPA2 utiliza o *Advanced Encyptation Standard* (AES) em conjunto com o TKIP com chave de 256 *bits*. Tal como o WPA, o WPA2 usa tecnologia de autenticação IEEE 802.1X/EAP ou tecnologia de PSK, mas trabalha com um mecanismo novo de encriptação avançado e mais robusto que o TKIP que usa o Counter-Mode/*Cipher Block Chaining Message Authentication Code* (CBC-MAC), chamado de AES [49].

Na sua especificação, a norma 802.11i garante que os dados enviados são criptografados e não são violados por nenhum tipo de interseção.

3.4.3.1 Advanced Encryption Standard (AES)

AES é um tipo de codificação de chave simétrica que usa grupos de bits de comprimento fixo chamados blocos. Com o AES, os bits são codificados em blocos de texto que é

calculado independentemente. Trabalha com blocos de 128 bits, com tamanhos de chave possíveis de 128, 192 e 256 bits. A utilização do AES inclui quatro etapas, que são repetidas 10, 12 ou 14 vezes dependendo do tamanho da chave. Para a implementação de WPA2/802.11i de AES, cada círculo é repetido 10 vezes [49].

3.4.3.2 Vulnerabilidades WPA2

Segundo o [51], especialistas em segurança da AirTight Networks descobriram uma falha de segurança no protocolo WPA2 que denominaram "Hole 196". Este nome surgiu como referência à página 196 do manual de normas do IEEE, onde se tratam as chaves usadas pelo WPA2: a PTK (Pairwise Transient Key), que é única para cada cliente e usada para tráfego unidirecional, e a GTK (Group Temporal Key), que é usada para broadcast.

A PTK consegue detectar quando dados e endereços MAC estão ser forjados. Já a GTK não consegue detectar essa falsificação. De acordo com a referência [51], essa é a questão central, já que pode deixar um cliente gerar pacotes arbitrários de broadcast para que outros clientes respondam com informação sobre as suas PTKs secretas, que podem ser descodificadas pelos atacantes.

A AirTight disse que bastam 10 linhas extras de código, disponível na web para o driver *open source* Madwifi, para fazer um PC com uma placa de rede comum simular o endereço MAC de um *Acess Point* e passar a ser um gateway para o envio de tráfego [51].

Segundo a [49], o atacante pode utilizar uma técnica chamada *ARP Spoofing*, uma vulnerabilidade que existe em redes sem fio mas também em redes de cabo. *ARP Spoofing* não recupera chaves para redes sem fio usando criptografia WPA2-AES ou WPA-TKIP, ou seja, para que o "Hole 196" possa ser explorado é necessário que o *hacker* tenha acesso à chave WPA2 e esteja autenticado na rede, o que é um pouco menos provável.

3.4.4 Comparação WEP, WPA e WPA2

O WPA procura corrigir as vulnerabilidades conhecidas do WEP: enquanto o WEP não possui qualquer meio de autenticação de utilizador, o WPA fornece esquema de autenticação mútuo que usa a norma IEEE 802.1X/EAP. Como já foi referido, o WPA2 também inclui um novo mecanismo de criptografia avançado (AES) que usa o Conter-Mode/CBC-MAC Protocol (CCMP).

Existem dois modos de trabalhar com WPA e WPA2: *Enterprise* e *Personal*. Em ambos os casos os dois protocolos têm autenticação e criptografia.

No modo *enterprise*, cada utilizador possui uma chave única para aceder à WLAN, fornecendo assim um nível alto de privacidade individual. O WPA utiliza o TKIP que utiliza um padrão de criptografia que calcula e emite chaves de criptografia para cada pacote de dados comunicado em cada sessão de cada utilizador, tornando extremamente difícil quebrar essa barreira. No WPA2, o padrão de criptografia usado é o AES, que é mais forte que o TKIP, fornecendo então uma proteção adicional de rede [49].

O modo Personal foi projetado para uso doméstico, ou seja, utilizadores que não têm servidores de autenticação disponível. Utiliza uma chave pré-partilhada (PSK) para autenticação, em vez do mecanismo IEEE 802.1X.

Quanto à proteção contra ataques à WLAN, o WPA e o WPA2 protegem a rede de uma variedade de ameaças. O WPA evita as limitações de segurança do WEP original, resultantes de uma criptografia imperfeita e da falta de autenticação. Usando TKIP, traz um algoritmo de criptografia maior e com autenticação IEEE 802.1X/EAP. Juntos, TKIP e autenticação mútua protegem a rede Wi-Fi de uma variedade de ameaças quando o modo WPA-Enterprise é usado.

O WPA2 oferece proteção avançada através da utilização do AES e autenticação IEEE 802.1X/EAP, baseado num padrão de autenticação mútua mais forte e criptografia avançada para proteger a rede sem fios de uma variedade de ameaças e ataques. Apesar de ter sido descoberta a ameaça “Hole 196”, conforme apresentado anteriormente, para que essa vulnerabilidade possa ser explorada é necessário que o invasor tenha acesso à chave WPA2 e seja um utilizador autenticado na rede.

4. SISTEMA DE DETECÇÃO E PREVENÇÃO DE INTRUSÃO

Os conceitos de prevenção e deteção de intrusões são antigos e vêm do âmbito da proteção à propriedade física, mas têm sido recentemente utilizados em relação ao valor das informações e dos dados armazenados em sistemas computacionais. Embora complementares, os temas deteção e prevenção serão tratados separadamente.

4.1. Sistema de deteção de intrusão

Intrusion Detection System (IDS) refere-se, de acordo com [40] ao sistema capaz de detetar ataques e atividades maliciosas em rede de dados ou sistemas computacionais. Na definição de [15], um IDS é software, hardware ou a combinação de ambos para detetar intrusões. Para [28], o sistema deve ser capaz de detetar ameaças antes de os danos serem infligidos ao sistema computacional que necessita de proteção. No mesmo sentido, [15] afirma que o IDS consiste na utilização de técnicas e métodos que procuram identificar, com base em assinaturas de tráfego ou deteção de anomalias, atividades anormais ou consideradas suspeitas tanto na rede como no *host*.

A deteção baseada em assinaturas funciona da seguinte forma: todos os dados que transitam na rede são compostos, entre outras informações, por campos que os identificam e que podem ser detetados com a utilização de software específico. Então, o sistema de deteção verifica todo o tráfego em busca de pacotes com assinaturas conhecidas. Detetar atividades suspeitas fundamentadas em anomalias tende a ser um processo mais simples, visto que se baseia em dados presentes no cabeçalho dos pacotes e utiliza os dados históricos para identificar comportamento considerado anormal.

Não existe consenso entre autores, mas, de acordo com [40], os sistemas podem ser divididos em duas grandes categorias: *Network Intrusion Detection System* (NIDS) e *Host Intrusion Detection System (*HIDS), detalhados na próxima seção.

4.1.1 Network Intrusion Detection System (NIDS)

Os autores da referência [52] definem NIDS como uma derivação de IDS cujo funcionamento se basea na monitorização de toda a rede a partir da perspectiva do local da sua localização, normalmente um segmento de rede.

Os sensores de um sistema de NIDS são geralmente placas de rede que funcionam em modo promíscuo, ou seja, com a capacidade de capturar todo o tráfego de rede que passa

pelo segmento em questão. Essa técnica pode ser implementada utilizando equipamentos do tipo *HUB* ou pela utilização de espelhamento de portas em *switches*.

A Figura 19 mostra uma rede com três NIDS posicionados para proteger os servidores que possuem uma vista para a rede externa e também as estações de trabalho ligadas ao segmento da rede interna. Segundo [52], a utilização de múltiplos NIDS dentro de uma mesma rede é exemplo do que se chama de arquitetura de defesa em profundidade.

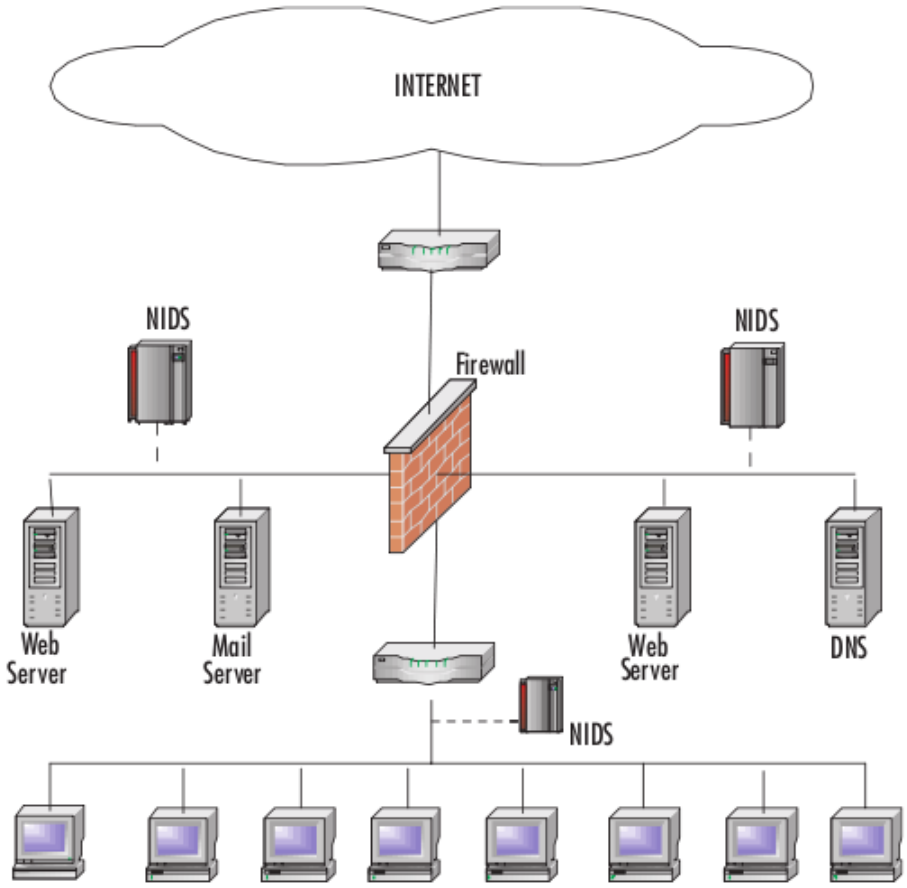


Figura 19 - Posicionamento do NIDS na rede (Fonte: [52])

Uma das vantagens da implementação de um NIDS é o fato de ele não ter qualquer impacto sobre a rede ou sistemas que esteja a monitorizar, já que não adiciona carga aos *hosts* da rede. Outra vantagem é que o sistema é totalmente transparente aos atacantes.

Como desvantagem pode mencionar o fato de que segmentos de rede com muito tráfego podem ocasionar a saturação da capacidade dos servidores de rede, necessitando de um estudo específico com vista à segmentação do tráfego em sistemas NIDS complementares.

4.1.2 Host Intrusion Detection System (HIDS)

De acordo com [40], um HIDS é um IDS que monitoriza somente o sistema na qual está instalado, monitorizando o tráfego de rede do *host*, os registos de eventos, e a integridade dos ficheiros do sistema. [52] salientam que um HIDS, por estar em execução num *host*, conhece melhor as informações de segurança locais, como chamadas e registo de sistemas.

Uma vantagem dos HIDS é o fato de as regras serem específicas, ou seja, apenas são verificados os serviços do sistema operativo do *host* e os serviços que realmente estão em execução, sem necessidade de verificações genéricas sobre como os NIDS devem operar.

Segundo o conceito de segurança em profundidade, defendido por [52], o HIDS pode ser a última instância de segurança após o ataque ter obtido êxito ao passar pelos sistemas de *firewall* e NIDS existentes na rede.

Há algumas desvantagens quanto à utilização de HIDS, tendo em conta que ele deve ser específico para o sistema operativo em questão: isto pode ser um fator complicado para redes heterogéneas, já que fornecedores podem não disponibilizar o seu software ou hardware para os mais diversos sistemas operativos existentes no mercado. Outra questão importante é a carga que o HIDS agrega ao *host* no qual está em execução. Outro fator de cuidado é a compreensão quanto ao funcionamento do HIDS, tendo em conta que algumas regras podem entar em conflito com aplicações instaladas.

A manutenção de rede com um grande número de HIDS é apontada como uma desvantagem e um desafio, pois se o sistema HIDS não tiver uma gestão centralizada o trabalho para administrar sistemas individuais pode inviabilizar a adoção de tais ferramentas, uma vez que a quantidade de alertas gerados pode ser intensa e necessitar de um tempo muito grande para a sua análise.

A Figura 20 representa uma rede em que alguns *hosts* implementam um sistema de HIDS. Como é possível observar, nem todos os *hosts* possuem a ferramenta e deve-se supor que em cada um deles estejam configuradas regras específicas.

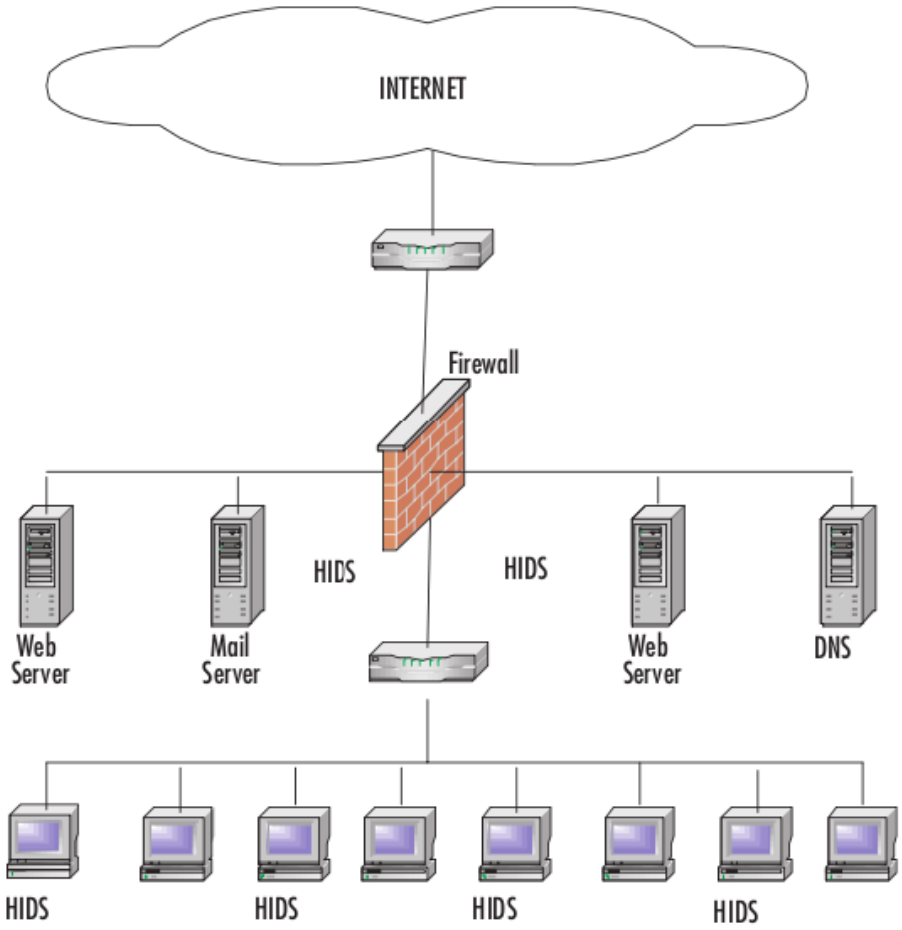


Figura 20 - HIDS em hosts específicos (Fonte: [52]).

4.2. Sistema de prevenção de intrusões

A prevenção de intrusões é uma tecnologia promissora na área de segurança de redes. Os sistemas de prevenção de intrusões surgiram como uma evolução dos IDS e combinam a capacidade de inspeção de pacotes com características de filtragem naturais dos *firewalls*, embora de forma mais transparente [53].

O conceito de IPS é semelhante ao de IDS, já que ambos requerem assinaturas de ataques conhecidos para detetar ameaças na rede de dados. Enquanto um IDS normalmente deteta tentativas de intrusão e envia alertas para o administrador da rede, o IPS inclui outras medidas para deter a intrusão em tempo real. Desenvolvido como medida de prevenção, atua bloqueando automaticamente possíveis ataques antes que eles tenham sucesso. Sendo assim, o IPS é um dispositivo que irá bloquear um ataque antes que ele chegue ao seu alvo. Embora pareça que esta tecnologia possa substituir um *firewall*, é necessário ter em mente que ela oferece uma camada a mais de proteção e, por ser uma

evolução do IDS, considera-se uma das primeiras linhas de defesa da segurança da informação. Assim, o IDS é como se fosse um alarme de um carro que soa somente quando alguém abre a porta, enquanto que o IPS dispara o alarme e trava as portas com o intuito de que o invasor não leve o carro [45].

Um sistema de IPS pode tomar várias ações: bloqueios de portas em *switch*, interação com políticas de *firewall* externos, regras dos routers, ou, ainda geração de tráfego na camada de transporte [54].

Segundo [25], um IPS tipicamente consiste em quatro componentes principais ilustrados na Figura 21:

- **normalizador de tráfego**: irá interpretar o tráfego de rede e fazer análise, reestruturar os pacotes e executar as funções básicas de bloqueio, além de fornecer alimentação para o *scanner* de serviço e para a máquina de deteção;
- ***scanner* de serviço**: cria uma tabela de referência, que classifica as informações e ajuda o modelador de tráfego a administrar o fluxo das informações;
- **máquina de deteção**: realiza uma comparação entre a tabela de referência e determina a resposta adequada;
- **modelador de tráfego**: controla o fluxo das informações.

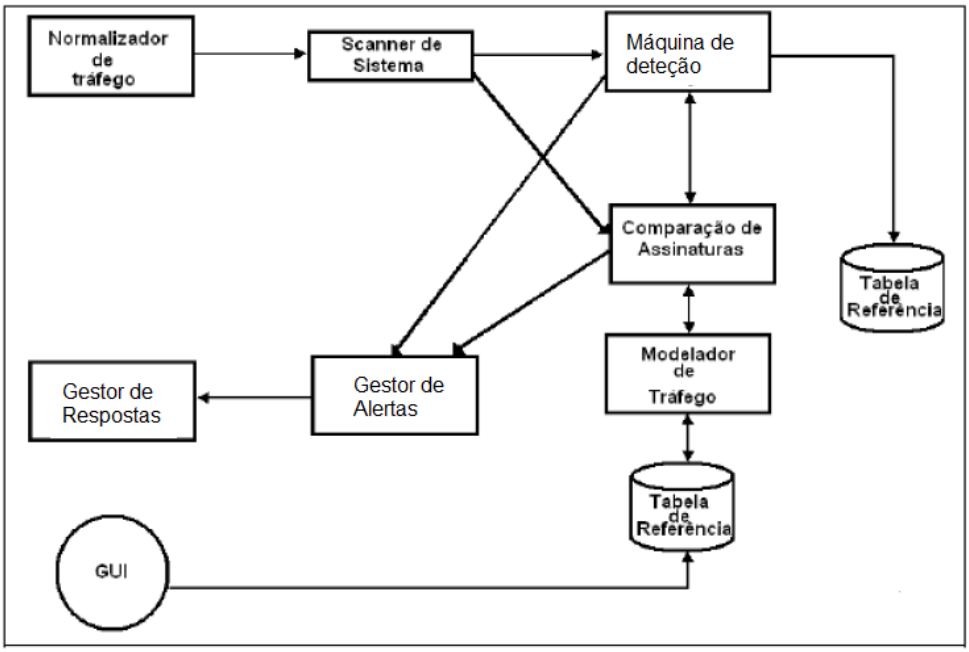


Figura 21 - Padrão do sistema IPS (Fonte: [25])

Existem dois tipos de sistema de prevenção de intrusão: IPS baseado em rede (NIPS) e IPS baseado em *host* (HIPS), os quais são descritos nas seções a seguir.

4.2.1. Network Intrusion Prevention System (NIPS)

Uma rede baseada em IDS é projetada para monitorizar o tráfego de forma passiva e gerar alarmes quando tráfego suspeito for detetado, enquanto um sistema baseado em NIPS é projetado para ir um passo além e tentar impedir o ataque [47].

Um IPS baseado em rede é um sistema de prevenção de intrusão instalado no *gateway*, de forma que o tráfego passe por ele como se fosse mais um elemento. É assim um elemento *inline*, posicionado para que possa evitar tentativas de ataques maliciosos como cavalos de Tróia, *backdoors*, *rootkits*, vírus, *worms*, entre outras ameaças. Na Figura 22 é ilustrada o NIPS numa estrutura de rede.

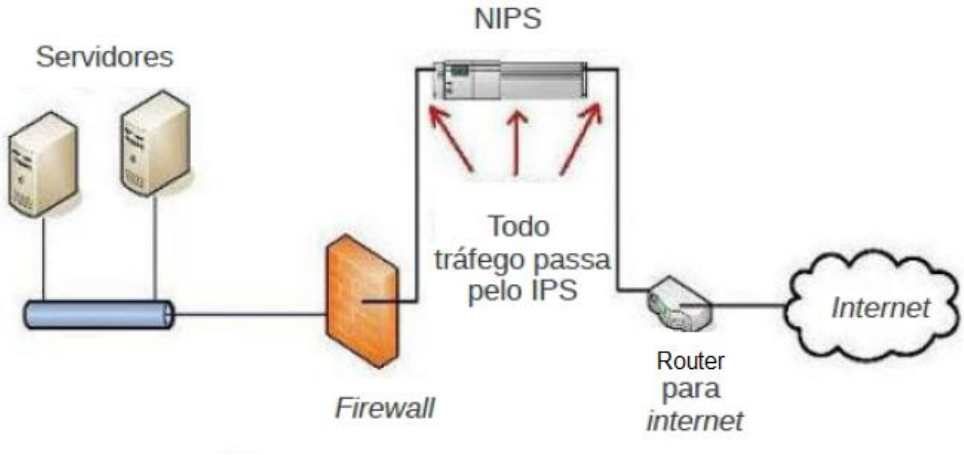


Figura 22 - Localização do NIPS numa rede de computadores (Fonte: [26]).

Tecnicamente, um NIPS realiza dois tipos de funções: filtragem de pacotes e deteção de intrusão, podendo fornecer medidas nas seguintes camadas:

- **dados**: *shutdown* administrativo *d*a porta do *switch* que está sofrer o ataque; tal atitude só é praticável para ataques que são gerados de um sistema local;
- **rede**: interage com o *firewall* externo ou router para adicionar uma regra geral para bloquear todas as comunicações de endereço de IP individual ou de uma rede inteira;
- **transporte**: gera pacotes TCP-RST *(reset)* para quebrar ligações TCP maliciosas ou emitir algum pacote de erro pretencente ao protocolo ICMP *(internet control message protocol)* no sentido de responder a tráfego UDP *(user datagram protocol)* malicioso;

- **aplicação**: alertas de dados maliciosos na camada de aplicação não podem causar danos antes de alcançar o sistema alvo. Isto requer que o IPS esteja *inline* no caminho da comunicação.

4.2.2. Host Intrusion Prevention System (HIPS)

Um IPS baseado em *host* também atua como a última linha de defesa. O software é instalado em cada máquina que precisa de ser protegida. Um HIPS consiste num servidor de gestão e um agente que está em execução entre a aplicação e o *kernel* do sistema operativo. É incorporado a um módulo carregável do *kernel* se o *host* for *Unix*, ou a um *driver* de sistema se o *host* for *Windows*. Dessa forma, o agente pode intercetar chamadas do sistema para o *kernel*, compará-las às listas de controlo de acesso ou regras de comportamento definidas no HIPS e decidir permitir ou bloquear o acesso a recursos específicos, tais como pedidos de leitura e escrita em disco, pedidos de ligação de rede, modificações de registo, ou escrever para a memória [53].

Segundo [47], uma das vantagens do HIPS é que o tráfego de rede criptografado pode ser analisado após o processo de descriptografia que ocorre no sistema protegido, proporcionando assim uma oportunidade para detetar um ataque que teria sido escondido num NIPS ou NIDS. O próximo capítulo apresenta a arquitetura de IDS/IPS numa rede de computadores.

4.3 Formas de Deteção de Intrusão

A deteção de intrusões torna-se possível a partir da recolha de dados da entidade a ser protegida. Esses dados podem ser recolhidos da rede ou em estruturas de controlo do sistema como *logs*, tabelas de processos e outros. As técnicas aplicadas na identificação de uma invasão analisam as informações recolhidas na busca de desvios de comportamento ou por padrões de ataques conhecidos.

Na classificação por modelo de análise das informações, os sistemas são classificados em:

- Deteção por assinatura: baseia-se na identificação de um padrão de ataque já conhecido e chamado de assinatura;
- Deteção por anomalia: baseia-se no desvio de comportamento de um sistema de uma rede.

Os sistemas baseados em assinatura têm como vantagem a detenção do "conhecimento" sobre o comportamento normal ou suspeito, podendo ser identificada de uma forma mais simples a ocorrência de um ataque e também diminuir o número de falsos ataques.

A desvantagem deste tipo de sistema é que a especificação das assinaturas tem de ser altamente qualificada para a identificação correta dos ataques em diferentes situações. Outra desvantagem é a falta de automatismo no reconhecimento de novos ataques, pois estes precisam de ser previamente especificados no sistema.

O sistema baseado na identificação de anomalias normalmente possui uma base de conhecimento e mecanismos que ajudam a identificar se o evento é efetivamente um ataque, se é uma variação de um ataque conhecido, ou se é apenas uma situação suspeita. Esse tipo de deteção é modelado para ser flexível, permitindo a identificação de situações que fogem ao padrão de comportamento da rede.

A desvantagem de sistemas baseados em anomalias é que eles aprende sobre comportamentos não usuais, que não são necessariamente ilícitos. E assim, poderá gerar alarmes falsos. Se o sistema aprende a aceitar comportamentos perigosos como normal, poderá não sinalizar um ataque real quando ele ocorrer.

Segundo [55], existem outras classificações de sistemas de deteção de intrusão referentes ao processamento das informações e características gerais do sistema, e que são:

- Tempo de deteção: as técnicas são agrupadas pela sua eficiência em detetar a intrusão, dividindo-se em *real-time*, *near real-time* e *non real-time*;
- Processamento de dados: os dados podem ser processados de forma distribuída ou centralizada;
- Recolha de dados: os dados recolhidos podem ser de uma fonte centralizada ou de fontes distribuídas;
- Segurança: habilidade para contornar intrusões ao próprio sistema de deteção, contornando ataques de evasão e inserção;
- Grau de interoperabilidade: indica o quanto um determinado sistema é capaz de operar em conjunto com outras ferramentas de segurança da rede;
- Grau de resposta a intrusões: um IDS pode responder a um ataque de forma passiva ou ativa. A maioria dos IDS oferece apenas mecanismos para geração de alertas aos responsáveis pelas redes e/ou sistemas sobre os possíveis ataques. No entanto,

poderiam responder aos ataques de forma ativa, por exemplo, finalizando sessões de utilizadores, ligações de rede, configurando firewalls, entre outras.

As características acima apontadas não são exclusivas de um sistema de deteção de intrusões. E de entre elas uma característica muito importante é a segurança do sistema de deteção, pois a segurança do ambiente depende do grau de correção e integridade da informação por ele fornecida.

4.3.1. Deteção por Assinatura

O método de deteção por assinatura consiste em representar um ataque conhecido através de um padrão ou assinatura para que os ataques descritos e variações do mesmo possam ser identificados [55]. Exemplos de intrusões reconhecidas através da utilização deste método são tentativas de ligação com um endereço IP reservado; pacotes TCP com combinações de *flags* ilegais; tentativas de saturar a pilha do buffer de DNS (*Domain Name System*); DoS (*Denial of Service*) num servidor POP3 (*Post Office Protocol*); ataques de acesso a ficheiros num servidor FTP; e-mails que tenham vírus; ataques de SYN Flooding; entre outros.

A maior dificuldade encontrada no desenvolvimento deste tipo de IDS é definir uma assinatura que engloba as variações de um ataque, mas não englobe as atividades normais. Outra dificuldade é a definição de uma referência sobre o protocolo a ser utilizada para definição das regras de comportamento e possíveis violações. As fontes utilizadas são a RFC (*Request for Comments*) do protocolo e a análise do comportamento do mesmo, pois nem sempre através da RFC é possível prever a ocorrência de falhas decorrentes da implementação do protocolo, evitando assim a ocorrência de alarmes falso negativos ou falso positivos.

Além destes fatores, observa-se que este tipo de abordagem exige a atualização dos padrões de ataque para que o sistema não fique obsoleto.

4.3.2. Deteção por anomalia

A deteção por anomalia, conforme [55], baseia-se em caracterizar o comportamento de programas, protocolos e utilizadores através da construção de um modelo (perfil), utilizando métricas tais como número de chamadas de sistema, tempo de utilização do CPU, número de ligações de rede num determinado período de tempo, tamanho dos

pacotes, etc. Este perfil pode também ser pré-determinado, por exemplo, tipo de utilizadores, tipo de rede, embora isto reduza as hipóteses do IDS se adaptar aos diferentes estados do sistema.

A ideia utilizada para investigar anomalias é executar a comparação do estado do sistema ou de pacotes capturados com os dados do perfil estabelecido. Quando ocorrem variações significativas entre estes dados, considera-se que ocorre uma tentativa de intrusão.

Os problemas encontrados no desenvolvimento de sistemas de deteção por anomalias, de acordo com [56], são:

- A descrição do comportamento de um sistema de maneira efetiva e eficiente, por motivos tais como o reconhecimento do comportamento do utilizador final;
- A definição dos limites aceitáveis de variação entre o dado analisado e o perfil estabelecido, pois, na dependência destes, atividades normais podem ser interpretadas como intrusões, gerando alarmes falso-positivos; ou em situações piores, as intrusões não são detetadas, gerando alarmes falso-negativos.

Várias técnicas estão a ser estudadas para poderem ser aplicadas à deteção de anomalias, envolvendo diversas métricas para elaboração de perfis de comportamento [57]. Algumas das técnicas utilizadas são descritas a seguir:

- Métodos baseados em sequências: para cada uma das chamadas de sistema ocorridas durante a execução normal de um programa, gera-se uma lista contendo as chamadas que a precedem com uma separação de até *n* chamadas;
- Métodos baseados em frequências: modelam a distribuição de frequência de sequências de chamadas de sistemas. As sequências que durante a monitorização ocorrerem em frequências distantes em relação ao modelo serão consideradas intrusões;
- Data Mining: estes métodos são utilizados para extrair as informações mais relevantes de grandes volumes de dados. A intenção é obter uma caracterização mais compacta de um comportamento normal, generalizando-o de forma a incluir padrões que não puderam ser observados durante a fase de preparação;
- Máquina de Estados Finita: baseia-se na ideia de que uma chamada de sistema possui estados anteriores e posteriores à sua execução. Através da análise dos

dados, determina-se a frequência com que cada estado ocorre. Os caminhos na execução do programa que não correspondem a estados e transições previstas, ou ocorram em frequências diferentes da observada, são considerados intrusões;

- Redes Neurais: a rede é treinada de forma a prever a próxima ação do utilizador com base nos seus *n* comandos anteriores. Conforme o desvio em relação a esta previção, é possível identificar um ataque.

O problema destes métodos é que eles podem ser treinados pelos invasores, fazendo com que intrusões sejam consideradas estados normais do sistema ou da rede. Com isto, a facilidade de atualização de um sistema de deteção através da utilização destas técnicas é prejudicada, pois torna-se necessário garantir que o comportamento do sistema ou da rede seja normal durante o período de recolha de dados. Deve-se, com isso, utilizar métodos auxiliares para a redução e normalização dos dados, fazendo com que apenas comportamentos considerados normais e relevantes estejam presentes no perfil.

Outra grande dificuldade é conseguir generalizar o comportamento anterior de forma a prever ações futuras. Embora esta dificuldade também exista na fase de definição das assinaturas, é mais acentuada na deteção por anomalia, uma vez que o comportamento futuro pode não ser idêntico ao comportamento passado.

4.3.3. Método Estatísticos para Sistema de Deteção de Anomalias

Os métodos estatísticos são utilizados nos sistemas de deteção de intrusões, principalmente baseados na deteção de anomalias, para determinar a ocorrência de intrusões ou para o pré-processamento dos dados que serão utilizados por outros métodos como, por exemplo, redes neuronais.

Os primeiros trabalhos relevantes nesta área foram apresentados por [19] e [22]. A vantagem destes métodos é a sua capacidade de tratar e representar explicitamente as variações e ruídos envolvidos nas atividades dos sistemas computacionais. Além disso, eles apresentam um bom desempenho computacional, bons índices de reconhecimento e escalabilidade, minimizando o tempo de resposta dos sistemas de deteção, aumentando a confiança no resultado do sistema e reduzindo falhas de processamento.

Mas ainda assim, continua a persistir um dos principais problemas dos sistemas de deteção de anomalias que é a construção dos perfis de comportamento que são utilizados para a comparação com as ações atuais, na tentativa de deteção de desvios do

comportamento considerado normal. A manutenção dos perfis é igualmente importante nestes sistemas, porque elas devem refletir a alteração de comportamento dos sistemas observado como forma de aprender as mudanças que ocorrem e não invalidar o processo por utilizar dados que não refletem corretamente o comportamento real.

4.3.4. Trabalhos relacionados com métodos estatísticos para deteção de anomalias

Uma grande quantidade de trabalhos tem utilizado a probabilidade condicional, mais especificamente o Teorema de Bayes, tanto em sistemas de segurança quanto em sistemas de gestão de falhas [4]. De forma a obter melhores índices de reconhecimento de eventos verdadeiros e um bom desempenho, os investigadores têm utilizado alguma destas técnicas combinadas com sistemas especialistas, redes neurais, lógica fuzzy, entre outros [14].

Os sistemas de deteção de intrusão baseados em métodos estatísticos, puros ou combinados com outros métodos, têm sido aplicados com objetivos variados como: deteção de intrusão em sistemas, através da verificação das sequências de comandos utilizadas por um utilizador; deteção da legitimidade do utilizador através da monitorização das ações, tanto no *host* como na rede; deteção de intrusões em sistemas de comunicação móvel; deteção de intrusões em serviços específicos, etc. Esses sistemas têm em comum o objetivo de detetar um evento ou uma sequência de eventos que se desviam do comportamento considerado normal e, portanto, caracterizam uma intrusão.

Em [19], é apresentado um sistema baseado em métodos estatísticos que observa o comportamento de sistema computacional e aprende de forma adaptativa o que é um comportamento normal para um utilizador ou para um grupo de utilizadores, bem como identifica situações potenciais de ocorrência de intrusões. Este sistema utiliza uma base de conhecimento que consiste em perfis de comportamento. Os perfis armazenam informações sobre distribuições de frequência, médias e covariâncias em vez de armazenar todos os dados de forma bruta, para minimizar os requisitos de memória. A manutenção dos perfis é realizada diariamente, de forma a refletir nos perfis as alterações naturais de comportamento dos utilizadores. Os dados armazenados anteriormente também são processados de forma que as informações mais novas tenham maior peso nas decisões do que as informações antigas. O método estatístico aplicado é bastante complexo, porque utiliza vários métodos para verificar as informações até concluir se o evento caracteriza uma intrusão.

É importante ressalvar algumas considerações feitas pelo autor. Em primeiro lugar, ele define níveis de alarmes de acordo com o nível de suspeita em relação à atividade, e os limiares e ações a serem realizadas são configuradas dinamicamente, de acordo com a política de cada sistema. Em segundo lugar, o autor identifica que a análise das variáveis deve ser feita de forma contínua no tempo, para que se possa determinar a variação das medidas e suas tendências. Desta forma, pode-se determinar se o comportamento tende a desviar-se do comportamento considerado normal, se permanece como normal ou anormal, e, caso seja anormal, verificar se retorna a um nível de normalidade.

Em [3], o autor utiliza uma abordagem estatística para detetar *network scans* em tempo real. O mecanismo é baseado em dois fatores: o quanto incomum é um sistema de origem ter acesso a um destino ou porta deste destino; e a quantos destinos e portas um sistema de origem teve acesso. Segundo o autor, este método é capaz de detetar intrusões em tempo real e, além disso, combina uma forma eficiente de indexar os acessos com uma abordagem probabilística para detetar os acessos que caracterizam os *network scans*. No entanto, este método não é capaz de *network scans* coordenados e realizadas a partir de origens distribuídas.

Em [12], o autor apresenta um sistema de deteção de anomalias dedicado à deteção de intrusões em *hosts*. O trabalho baseia-se na premissa de que utilizadores legítimos podem ser classificados em categorias, de acordo com a percentagem de comandos que usam num período específico. Isto é, um utilizador legítimo, durante o tempo de permanência no sistema, irá gerar uma quantidade de informação suficiente para definir o seu perfil. Logo, quando o comportamento do utilizador se afastar do perfil, o sistema poderá considerar que pode estar a ocorrer utilização indevida das credenciais do utilizador. Os principais pontos para o autor são a seleção das informações que compõem o perfil, de forma a eliminar um conjunto potencial de comandos com erro de introdução, e também os casos que não correspondem a uma situação normal de uso. A seleção dos dados permite também minimizar os requisitos de memória e processador, melhorando o desempenho do sistema. O autor apresenta um método que utiliza lógica *fuzzy*, medidas como média e desvio padrão e algoritmos genéticos para o tratamento dos dados do perfil, de forma a selecionar as informações relevantes. Os dados resultantes são submetidos a uma rede neural que determina a ocorrência de uma intrusão. O algoritmo utilizado neste passo é uma variação do algoritmo LVQ (*Learning Vector Quantization*) [17].

Em [33], o autor apresenta um sistema para deteção de intrusões em serviços Internet. O autor propõe a utilização de medidas como média e desvio padrão para obter informações sobre os eventos recolhidos no sentido de determinar o grau de anormalidade dos eventos da aplicação. Nesta solução, a inteligência do sistema é obtida pela utilização de medidas como média e desvio padrão e probabilidade condicional.

5. ANÁLISE DO SISTEMA DE DETECÇÃO E PREVENÇÃO DE INTRUSOS

A ferramenta de IDS/IPS descrita neste capítulo tem como base o estudo feito até ao momento sobre o funcionamento básico desse tipo de ferramenta, mostrando como o IDS/IPS deve ser disposto na rede de computadores e como as anomalias serão detetadas. O objetivo principal da utilização das ferramentas de IDS/IPS é a identificação e bloqueio de ameaças, podendo ainda fazer a análise qualitativa dos bloqueios ocorridos.

Este capítulo inicia-se com a apresentação do modelo base encontrado no terreno. Seguidamente, é efetuada a identificação dos pontos passíveis de falhas no sistema de IDS/IPS. Finalmente, é apresentado o modelo ideal e feita a descrição do funcionamento da ferramenta existente.

5.1 Modelo de ambiente base encontrado

Esta seção visa apresentar o ambiente de rede básico inicial em que se baseia o estudo, nomeadamente a estrutura física e lógica na qual há a necessidade de incluir meios que aumentem a segurança da rede.

As Figuras 23 e 24 ilustram o nível físico e lógico da infraestrutura de rede, a rede de dados do Instituto Politécnico de Tomar (IPT). Esta rede dispõe de uma grande variedade de equipamentos e caracteriza-se por uma vasta heterogeneidade de perfis dos utilizadores que diariamente a utilizam.

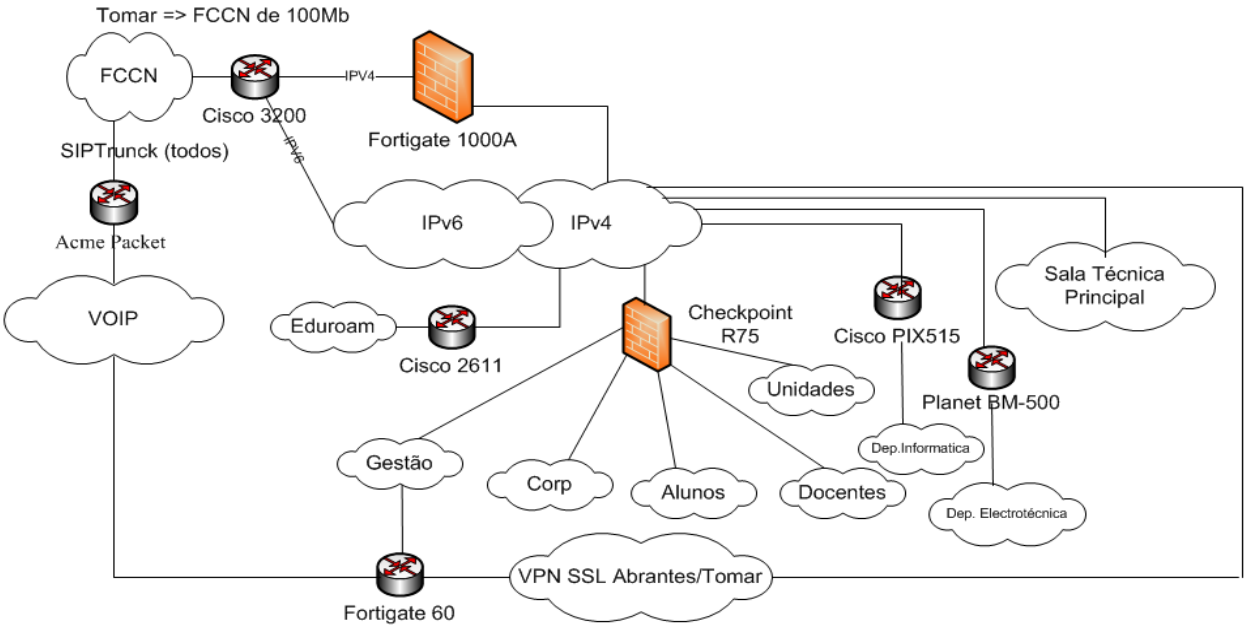


Figura 23 - Modelo físico do ambiente encontrado (Fonte: Centro informático do IPT)

A estrutura da rede é caracterizada por aplicações do tipo cliente/servidor, em que o servidor constitui a peça fundamental do modelo porque é ele que disponibiliza os serviços requeridos pelos clientes.

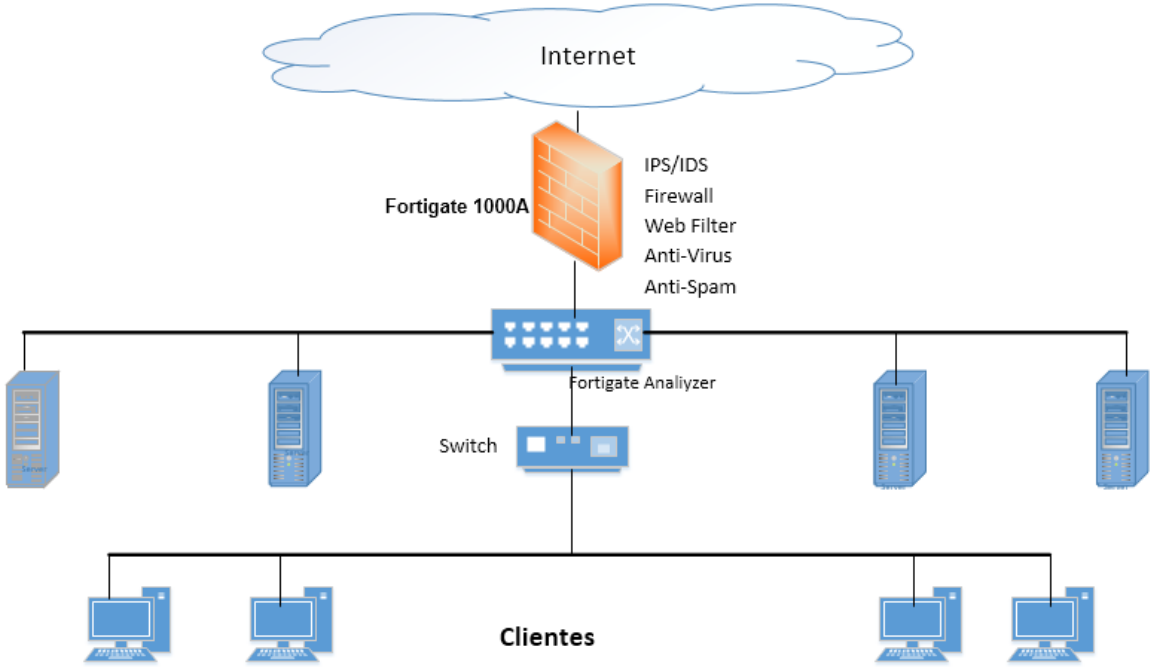


Figura 24 - Modelo lógico do ambiente encontrado

Além do *firewall* e do filtro *web*, é possível perceber que a atual rede apresenta ferramentas anti-virus, anti-spam e um serviço IPS/IDS que monitoriza e analisa o tráfego em tempo real.

Neste ambiente base podem-se identificar alguns pontos de vulnerabilidade, os quais são abordados na próxima seção.

5.2 Determinação do problema

Conforme descrito na seção anterior, a rede de dados em que se efetuou o estudo é utilizada por diferentes níveis de utilizadores, desde os que têm conhecimento avançado na área de informática até aos que pouco conhecem de um sistema de rede. Sendo assim, todos os utilizadores correm o risco de ser infetados na rede por vírus, *malwares* e *spywares*, os quais podem interferir na segurança da rede local ou divulgar informações sigilosas e não autorizadas para o mundo exterior. A ameaça pode mesmo vir dos próprios utilizadores da rede local. A Figura 25 ilustra algumas das vulnerabilidades (pontos de falha de segurança) mais críticas encontradas neste ambiente.

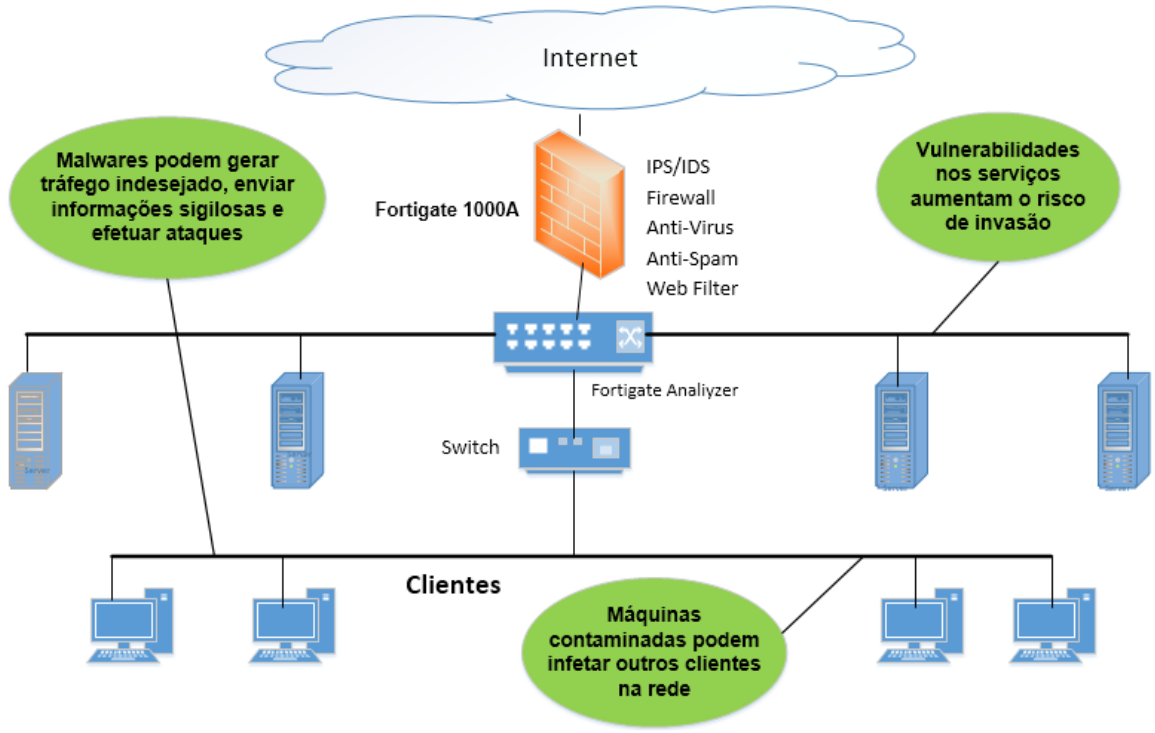


Figura 25 - Pontos de falha encontrados no modelo do ambiente

Os pontos de falha de segurança são originados nas redes internas ou na rede externa. O modelo descrito, no qual se baseia este estudo, é típico de uma rede de grande dimensão, como é a rede de dados do IPT, que é utilizada por professores, alunos e visitantes. Por se tratar de uma rede com amplos acessos, abrangendo um público de inúmeras características, ela sofre constantes ameaças, para além de não ser possível efetuar um controlo específico do *software* que cada utilizador está executar na rede, porque estes utilizam os seus computadores pessoais com permissões administrativas próprias no sistema operativo, podendo instalar e executar qualquer programa que esteja ao seu alcance.

Os principais pontos considerados críticos na estrutura apresentada são os seguintes:

- erro de configuração no *firewall*: atacantes podem fazer uso de uma má configuração do *firewall* que protege a rede;
- vulnerabilidades: *bugs* em sistemas operativos ou *softwares* utilizados em servidores, podem gerar vulnerabilidades;
- máquinas internas contaminadas: máquinas contaminadas podem disseminar vírus por toda a rede, contaminando outros computadores;

- *malwares*: podem gerar tráfego indesejado, enviar informações sigilosas a atacantes e até mesmo gerar ataques externos. Estes *malware* são normalmente obtidos a partir de ataques de engenharia social ou através do acesso a *sites* infetados.

Para tentar minimizar os problemas apresentados, a seção seguinte apresenta o que seria um ambiente ideal de utilização, corrigindo os diversos pontos de falhas observados.

5.3 Pontos ideais para aplicação da ferramenta

Como é possível observar, a segurança da rede de dados pode ser afetada de diversas formas. No entanto, há uma forma automática de detetar uma ameaça ou intrusão na rede, assim como medir a quantidade de ameaças sofridas. A solução passa por implementar um sistema de IDS/IPS, que incorpora as funcionalidades mencionadas até ao momento e traz como resultado um aumento no nível de segurança da rede de dados através do bloqueio de inúmeras ameaças. Para tal, após analisar o ambiente base encontrado, deve-se verificar se a estrutura da rede local apresenta os requisitos necessários para a utilização da ferramenta, assim como definir os pontos vulneráveis a ataques. Da análise do ambiente, é possível extrair informações que ajudam a definir os pontos ideais da aplicação da ferramenta IDS/IPS. A Figura 26 ilustra o modelo da solução proposta e que responde aos requisitos de segurança de redes elencados anteriormente neste trabalho.

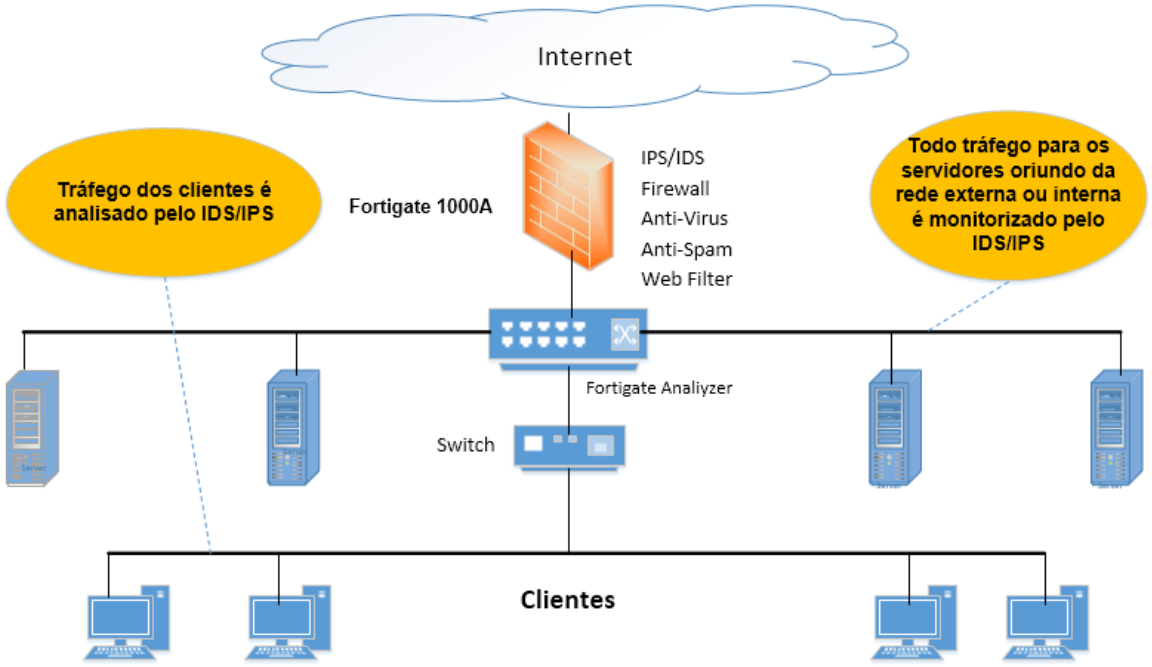


Figura 26 - IDS/IPS proposto para a rede de dados

Os pontos de aplicação do IDS/IPS foram estrategicamente escolhidos por serem os mais propícios ás vulnerabilidade na rede de dados, e nesse sentido requerem uma análise minuciosa de todo o tráfego gerado pelos *hosts*.

A funcionalidade primordial da estrutura de IDS/IPS é analisar o tráfego da rede de dados, identificar e homologar possíveis ameaças ou ataques. Confirmado um desses casos, o sistema atuará de forma automática, bloqueando a origem do problema.

5.4 Arquitetura da ferramenta IPS/IDS

Nesta seção será apresentada a arquitetura da ferramenta de IPS/IDS existente. A subseção seguinte descreve o seu modo de funcionamento.

5.4.1. O FortiGate 1000A

O Fortigate-1000A é uma aplicação da marca Fortinet que implementa todas as funções de segurança de *gateway* em tempo real sem comprometer o desempenho das redes e oferecendo todos os níveis de proteção para combater as ameaças mais sofisticadas. O Fortigate detecta e elimina as ameaças mais perigosas do tráfego Web ou e-mail como vírus, worms, intrusos, conteúdo Web não permitido e outros, inspecionando todo o tráfego, inclusive o criptografado como o HTTPS. Além da proteção ao nível de aplicação, o Fortigate implementa firewall, VPN, IDS/IPS, *traffic shaping*, DLP, otimização WAN,

encaminhamento das camadas 2 e 3, controlos de aplicação, suporte para VOIP (H. 323. e SCCP) e proteção anti-spam, tudo através de plataformas de fácil gestão. O produto oferece tecnologia com funções únicas em UTM como DLP, aceleração de rede e segurança em protocolos HTTPS, POPS e IMAPS.

As principais vantagens do Fortigate podem ser resumidas da seguinte forma:

- a aceleração ASIC permite uma qualidade de segurança superior com a tecnologia multi-ameaças. No fundo, proporciona várias tecnologias de segurança num único equipamento, o que facilita a manutenção;
- permite a elaboração de relatórios e solução de problemas;
- possui oito portas switch internas que eliminam a necessidade de um hub adicional, reduzindo investimentos em equipamentos e encargos de gestão;
- apresenta facilidades de gestão e implementação. Constitui uma solução integrado, *all-in-one*, que fornece diversas combinações de funções de segurança permitindo apoio aos sistemas existentes e a adição de novas funcionalidades.
- está disponível para integração com *FortiManager* e *FortiAnalyzer,* simplificando a gestão de segurança, relatórios e análise, reduzindo despesas operacionais.
- Os serviços de subscrição *FortiGuard* entregam de forma automática e em tempo real proteções atualizadas contra ameaças de segurança.

A Tabela 4 apresenta os serviços proporcionados pela ferramenta Fortigate 1000A.

Tabela 4 - Serviços de segurança do Fortigate 1000A

FIREWALL	**WEB FILTERING**	**LOGGING/MONITORING**
ICSA Labs Certified (Enterprise Firewall) NAT, PAT, Transparent (Bridge) Routing Mode (RIP v1 & v2, OSPF, BGP, & Multicast) Policy-Based NAT Virtual Domains (NAT/Transparent mode) VLAN Tagging (802.1q) User Group-Based Authentication SIP/H.323 NAT Traversal WINS Support Customized Protection Profiles	URL/Keyword/Phrase Block URL Exempt List Content Profiles Blocks Java Applet, Cookies, Active X FortiGuard Web Filtering Support **ANTISPAM** Real-Time Blacklist/Open Relay Database Server MIME Header Check Keyword/Phrase Filtering IP Address Blacklist/Exempt List Automatic Real-Time Updates From FortiGuard Network	Internal Logging Log to Remote Syslog/WELF server Graphical Real-Time and Historical Monitoring SNMP Email Notification of Viruses And Attacks VPN Tunnel Monitor Optional FortiAnalyzer Logging

VIRTUAL PRIVATE NETWORK (VPN)

ICSA Labs Certified (IPSec & SSL)
PPTP, IPSec, and SSL
Dedicated Tunnels
DES, 3DES, and AES Encryption Support
SHA-1/MD5 Authentication
PPTP, L2TP, VPN Client Pass Through
Hub and Spoke VPN Support
IKE Certificate Authentication
IPSec NAT Traversal
Dead Peer Detection
RSA SecurID Support

INTRUSION PREVENTION SYSTEM (IPS)

ICSA Labs Certified (NIPS)
Protection From Over 3000 Threats
Protocol Anomaly Support
Custom Signature Support
Automatic Attack Database Update

TRAFFIC SHAPING

Policy-based Traffic Shaping
Differentiated Services (DiffServ) Support
Guarantee/Max/Priority Bandwidth

NETWORKING/ROUTING

Multiple WAN Link Support
PPPoE Support
DHCP Client/Server
Policy-Based Routing
Dynamic Routing (RIP v1 & v2, OSPF, BGP, & Multicast)
Multi-Zone Support with Routing Between Zones

ANTIVIRUS

ICSA Labs Certified (Gateway Antivirus)
Includes AntiSpyware and Worm Prevention
HTTP/SMTP/POP3/IMAP/FTP/IM and Encrypted VPN Tunnels
Automatic "Push" Virus Database Update
File quarantine Support
Block by File Size or Type

HIGH AVAILABILITY (HA)

Active-Active, Active-Passive
Stateful Failover (FW and VPN)
Device Failure Detection and Notification
Link Status Monitor
Link failover

USER AUTHENTICATION

Local Database
Windows Active Directory (AD) Integration
External RADIUS/LDAP Integration
IP/MAC Address Binding
Xauth over RADIUS for IPSEC VPN
RSA SecurID Support

VIRTUAL DOMAINS (VDOMs)

Separate Firewall/Routing domains

Separate Administrative domains
Separate VLAN interfaces
10 VDOMs (standard)
Up to 250 VDOMs (optional license -
models 3000 and higher)

A seguir são descritos alguns dos serviços da ferramenta Fortigate que constam da Tabela 4.

O serviço Virtual Domains (VDOMs) permite que uma unidade Fortigate funcione como várias unidades independentes, o firewall que controla todo o tráfego das interfaces, zonas e VLANs que passam pelo Fortigate.

O VPN permite implementar modos de acesso mais seguros utilizando protocolos de segurança IPSEC, PPTP e SSL.

A ferramenta contém ainda um sistema antivírus avançado, anti-spam contra correio não solicitado e filtragem web para bloquear alguns sites com base nas categorias de conteúdo que considerar não aconselháveis.

O sistema de prevenção de intrusão (IPS) do Fortigate combina a deteção e prevenção de intrusão por assinatura e anomalia com baixa latência, apresentando uma excelente confiabilidade.

6. DESCRIÇÃO DOS DADOS

Os dados aqui analisados dizem respeito ao ano de 2012. Ao longo destes período, o sistema de IDS/IPS efetuou a monitorização em tempo real de todo o tráfego da rede de dados do campus do Instituto Politécnico de Tomar, identificou e impediu fraudes na rede de forma automática. Durante este período o número de utilizadores que fez uso da rede da instituição foi significativo, gerando milhares de alertas. Estes dados foram obtidos através da ferramenta *FortiAnalyzer* que centraliza os *logs* enviados por equipamentos Fortinet na rede facilitando a gestão de eventos e operações de auditoria de segurança.

A descrição é separada por subseções, apresentando cada uma delas as ameaças e a interação exercida pela ferramenta de segurança.

6.1 Ameaças oriundas da rede externa

Ao permitir que os utilizadores tenham acesso ao mundo exterior, várias portas são abertas e passam a poder ser atingidas por inúmeros *hosts* localizados em qualquer parte do mundo. O administrador de rede pode estar convencido que o *firewall* é a sua proteção máxima e que com ele nada poderá afetar a integridade dos dados. No entanto, o *firewall* mesmo sendo uma ferramenta de segurança trabalha de forma que determinadas portas sejam abertas para possibilitar o acesso a um determinado serviço. Com isso, o ambiente está sempre sujeito a riscos de segurança. A seguir são descritos dois casos de ameaça à segurança da rede de dados que somente o sistema de detecção e prevenção de intrusõess é capaz de identificar.

- **Ataque do tipo DoS**

O *Slowloris* é uma ferramenta de ataque HTTP DoS. Ela cria *sockets* e envia requisições HTTPs válidas para o alvo continuamente em intervalos de tempo regulares. Dessa forma, tenta iludir o *web server* evitando que essas ligações sejam fechadas. O *Slowloris* aguarda a ligação bem sucedida de todos os *sockets* para iniciar o ataque. Essa técnica permite indisponibilizar o alvo, dificultando a detecção do ataque. A ferramenta concorre com os acessos válidos, normalmente ganhando essa concorrência, fazendo com que o serviço *web* fique indisponível para quem a ele queira ter acesso.

- ***Scan* de portas**

Fazer o *scanning* de portas é uma forma alternativa de detectar serviços abertos numa máquina, mesmo que todas as portas TCP estejam fechadas no *firewall*. Com a técnica de *scanning* de portas, podem-se obter várias informações dos serviços disponíveis num determinado servidor, ou até mesmo numa máquina interna da rede. Muitos atacantes utilizam essa técnica para recolher informações quanto a um *host*, pois com o *scanning* podem determinar que serviços podem ser inspecionados e possivelmente atingidos. Existem diversas ferramentas para efetuar o *scanning* de portas, sendo a ferramenta mais utilizada para testes o *Nmap.*

O *Nmap* é um software livre que realiza *port scanning.* É muito utilizado para avaliar a segurança dos computadores e para descobrir serviços ou servidores numa rede de computadores. Na Figura 27 são apresentados alguns alertas gerados pelo IPS/IDS quando este se encontrava a efetuar deteção de anomalias na rede de dados do IPT.

#	Last Activity	Type	Level	Source	Destination	Attack ID	Severity	Status	Message	Packet Log	Protocol
1	07/11/2012 14:07	ips	alert	93.144.48.82	193.137.132.75	285212775	critical	dropped	anomaly: udp_dst_sessi		17
2	07/11/2012 14:07	ips	alert	193.137.132.75	97.77.234.150	285212773	critical	dropped	anomaly: udp_src_sessi		17
3	07/11/2012 14:07	ips	alert	93.108.178.53	193.137.5.142	101646345	critical	drop_session	operating_system: LPRr		6
4	07/11/2012 14:07	ips	alert	93.108.178.53	193.137.5.142	101974394	high	detected	misc: Hummingbird.Inetl		6
5	07/11/2012 14:06	ips	alert	193.137.132.75	213 152 248 197	103350334	high	detected	operating_system: IRIX		6
6	07/11/2012 14:06	ips	alert	93.108.178.53	193.137.5.142	101646345	critical	drop_session	operating_system: LPRr		6
7	07/11/2012 14:06	ips	alert	93.108.178.53	193.137.5.142	101974394	high	detected	misc: Hummingbird.Inetl		6
8	07/11/2012 14:06	ips	alert	188.67.226.181	193.137.132.75	285212775	critical	dropped	anomaly: udp_dst_sessi		17
9	07/11/2012 14:06	ips	alert	193.137.132.75	92.28.75.214	285212773	critical	dropped	anomaly: udp_src_sessi		17
10	07/11/2012 14:06	ips	alert	93.108.178.53	193.137.5.142	101646345	critical	drop_session	operating_system: LPRr		6

Figura 27 - Alertas gerados pelo IPS/IDS

Com base nesta informação, é possível observar o que aconteceu, quando aconteceu, quem originou o sucedido e para quem foi feita a tentativa de ataque.

6.2 Ameaças oriundas da rede interna

Num rede de computadores, as ameaças podem ser originadas tanto externa como internamente, e muitas vezes o perigo pode estar dentro da própria instituição. No caso da rede do IPT a situação não é diferente, pois diariamente vários utilizadores fazem uso da rede para troca de *e-mails*, acessos a ficheiros e navegação na *web.* Muitas vezes sem saber, esses utilizadores podem gerar ameaças e interferir no funcionamento de todo o sistema. Por estar ligada em diversos pontos da rede de dados, a ferramenta IPS/IDS monitoriza *hosts* internos, garantindo assim a segurança quando forem detetadas anomalias.

Um utilizador interno pode ter o seu computador infectado sem saber. Para garantir que isso não ocorra, é necessário que o IDS/IPS consiga identificar a máquina infectada e a bloqueie para que não infecte os demais clientes da rede. Neste caso, foram detetados durante o período de recolha de dados, máquinas infetadas com alguns dos vírus mais frequentes, e que estão descritos na Tabela 5.

Tabela 5 - Virus mais detetados

Nome	Eventos	% de Total
JS/PackRedir.A!tr.dldr	515	89,10
HTML/Iframe.TJL!exploit	46	7,96
PossibleThreat	9	1,56
W32/Slupim.B!tr	4	0,69
JS/Iframe.ZO!exploit	2	0,35
W32/Agent2.KPV!tr	1	0,17
PHP/C99Shell.I!tr.bdr	1	0,17
Total	**578**	**100,00**

A Figura mostra a distribuição percentual dos vírus detetados.

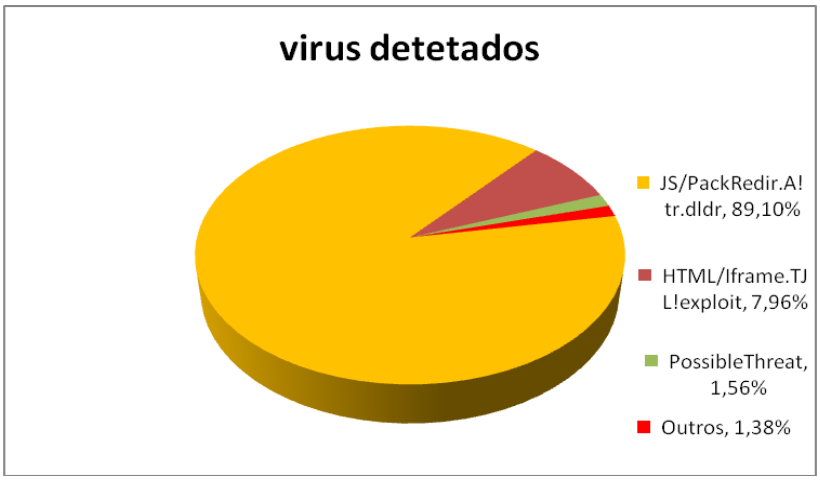


Figura 28 - Percentagem de vírus detetados

6.3 Análise qualitativa dos bloqueios executados

Com o intuito de medir a quantidade de alertas gerados durante o período de estudo, constatou-se que a rede *wireless* do Centro Politécnico IPT é acedida por um número significativo de utilizadores (fonte dos dados, Centro de Informática do IPT) sendo que são gerados alguns alertas que são gravados em bases de dados e que envolvem desde ameaças graves até eventos de tráfego considerado normal numa rede de computadores. Na Figura 29 estão identificados alguns alertas recolhidos.

Type	Level	Source	Destination	Attack ID	Severity	Status	Protocol
ips	alert	93.108.178.53	193.137.5.142	101974394	high	detected	6
ips	alert	210.164.41.179	193.137.132.75	285212775	critical	dropped	17
ips	alert	193.137.132.75	178.80.105.223	285212773	critical	dropped	17
ips	alert	70.191.229.79	193.137.132.75	285212775	critical	dropped	17
ips	alert	193.137.132.75	79.9.254.131	285212773	critical	dropped	17

Figura 29 - Lista de eventos ocorridos durante o estudo

Foi efetuada uma análise qualitativa de todos os bloqueios efetuados durante o período de estudo, pois ela estabelece padrões de comportamento facilmente verificáveis através dos factos observados. É possível quantificar os bloqueios por meio das informações recebidas pela ferramenta *FortiAnalyzer*.

Na Tabela 6, apresentam-se os dados estatísticos de utilização do Hotspot e-U durante os quatro meses de 2012 considerados para este estudo.

Tabela 6 - Dados estatísticos mensais obtidos acerca do Hotspot e-U

Periodo	Julho	Agosto	Setembro	Outubro
Sessões locais ipt.pt	15.146	1.648	10.967	23.084
Users locais ipt.pt	743	87	763	1.109
Sessões Remotas de *users* locais ipt.pt	12.436	871	6.601	14.523
Users locais em roming ipt.pt	184	32	142	214

Na Figura 30 é apresentado o gráfico de cada um dos quatro meses respeitantes ao período considerado, e que relaciona a percentagem de acessos com o fato de serem efetuados por utilizadores locais, remotos ou em roaming.

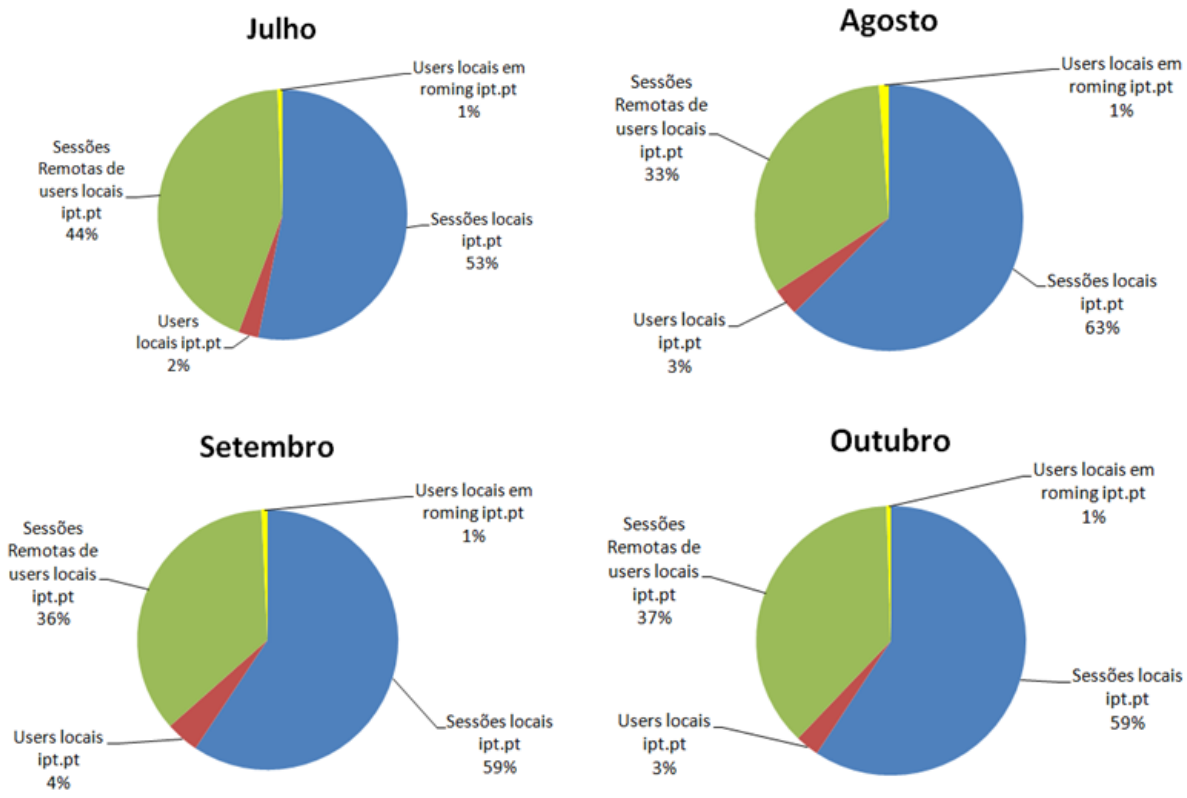


Figura 30 - Percentagens em função de perfil de utilizador

O gráfico da Figura 30 mostra que a percentagem de sessões locais é substancialmente superior em todos os meses quando comparada com a percentagem de utilizadores remotos ou em roaming.

Tabela 7 - Dados mensais de acessos, alertas e bloqueios obtidos

Período	Julho	Agosto	Setembro	Outubro
Acessos	14.740	10.992	12.560	14.208
Alertas	104.668	59.952	47.912	77.912
Bloqueios	5.944	1.912	1.456	2.252

Os dados obtidos são separados por meses para uma melhor visualização, sendo efetuado o somatório dos dias correspondentes a cada mês. Os dados apresentados na Tabela 7, correspondentes ao número de acessos, alertas e de bloqueios, foram obtidos através da

ferramenta *FortiAnalzer* administrada pela equipa do Centro de Informática do Instituto Politécnico de Tomar.

A Tabela 8 apresenta o somatório do número de utilizadores que fizeram uso da rede, da quantidade de alertas e bloqueios gerados pelo *FortiAnalizer*.

Tabela 8 - Somatório dos dados obtidos no período de homologação

Somatório dos dados	
Acessos	52.500
Alertas	290.444
Bloqueios	11.564

O valor 52.500 corresponde ao número de acessos: este valor foi obtido a partir do somatório de *logins* diários não repetitivos. São descartados todos os acessos repetidos diariamente, obtendo-se assim somente logins únicos que utilizaram a rede, podendo-se distinguir o utilizador que fez *login* somente uma vez daqueles que efetuaram vários *logins* durante o dia.

Quanto aos valores dos alertas e bloqueios, foi feito um somatório dos dados obtidos durante os quatro meses do estudo. Com os dados obtidos, foi possível efetuar uma análise de quão eficaz foram os bloqueios gerados pela ferramenta. A fim de efetuar uma análise mais clara, os resultados são apresentados no gráfico da Figura 31.

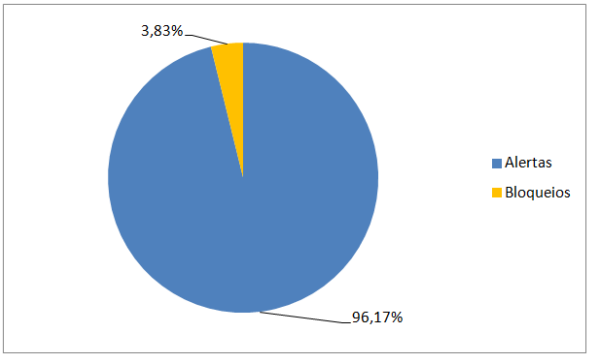


Figura 31 . Percentagem de alertas versus bloqueios

Conforme pode ser observado, foi realizado o cruzamento dos valores obtidos na Tabela 8 de modo a medir a percentagem de bloqueios efetuados durante o período de homologação. Dos 290.444 alertas gerados, foram identificados 11.564 como assinaturas de tráfego indesejado, correspondendo a 3,83% do total. Num ambiente onde não existe esta ação de

prevenção automática, seria humanamente impossível ao administrador da rede conseguir identificar e bloquear todos os *hosts* aqui detectados, isto porque não se consegue identificar ou medir quantas ameaças poderiam surgir após o primeiro incidente, ou seja, uma ameaça não detectada pode vir a gerar muitas outras.

Na Tabela 9 é apresentado o número de bloqueios por assinatura referente ao mês de setembro de 2012.

Tabela 9 - Quantidade de bloqueios por assinaturas

Assinaturas	Spywares	Conficker	TeamViewer	Logmein	Tunel SSH	Slowloris	UltraSurf	Total
Bloqueios por assinatura	738	218	1.865	28	35	7	7	2.898

Durante o período em que foi feita a recolha dos dados constantes da Tabela 9, foram atingidos 2.898 *hosts* bloqueados. É de salientar que muitas outras assinaturas poderiam ser identificadas e bloqueadas pela ferramenta, mas nenhum tráfego correspondente a elas foi gerado pelos utilizadores durante esse período. O gráfico da Figura 32 apresenta a percentagem de cada assinatura no total de bloqueios gerados.

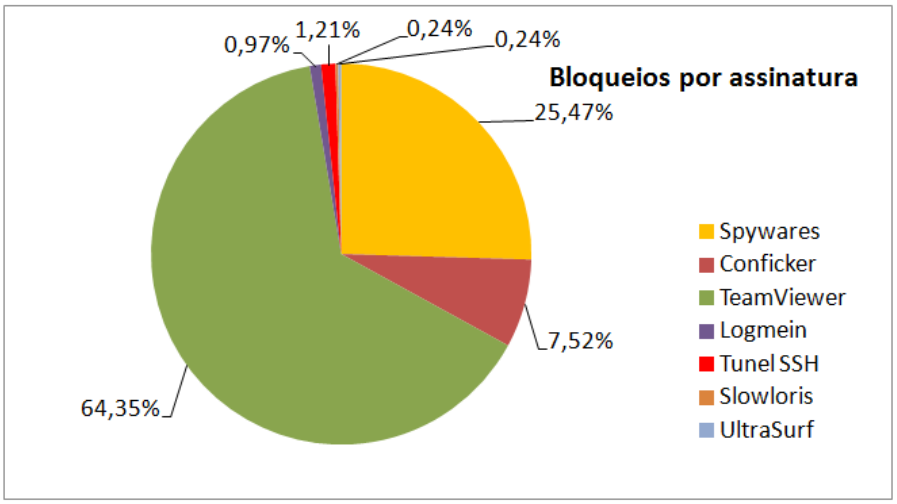


Figura 32 - Percentagem por assinatura bloqueada

Conforme se pode observar, houve maior incidência do uso de ferramenta de acesso remoto pela *internet*. Com o software *TeamViewer*, o utilizador pode aceder a qualquer outro *host* ligado à rede e fazer uso dos acessos por ele disponibilizados. O segundo maior incidente, correspondendo a 25,47% dos bloqueios, foram os *spywares*, *que* consistem num

programa automático de computador que recolhe informações sobre o utilizador e transmite essa informação a uma entidade externa, sem o conhecimento nem o consentimento do utilizador. A assinatura desenvolvida para identificar acesso por túnel SSH corresponde a 1,21% dos bloqueios, tornando-se mais atuante do que assinaturas como *UltraSurf, Logmein* e *Slowloris.*

Analisado os dados obtidos, pode-se concluir que a rede está bem protegida contra ataques sobretudo quando vindos de fora, porque o tráfego passa necessariamente pelo sistema IDS/IPS. Contudo, existem alguns pontos vulneráveis como está indicado na Figura 25: máquinas internas contaminadas podem difundir vírus por toda a rede, contaminando outros computadores; a ameaça pode advir de uma má configuração do *firewall* e como a ferramenta se localiza na interface entre as redes interna e externa, somente passa por ela o tráfego gerado de e para fora, o que faz com que a rede possa ser ameaçada a partir de dentro.

A solução podia ser fazer passar todo o tráfego interno pelo IPS, o que por outro lado iria causar congestionamento na rede. Neste caso, o mais aconselhável é colocar mais uma proteção, conforme se indica na Figura 26, de modo a que todo o tráfego oriundo da rede interna para os servidores seja analisado por esse agente.

6.4 Considerações de segurança da rede

De acordo com o que foi descrito nas secções anteriores, constata-se que os problemas de segurança estão relacionados com a diversidade de comportamentos, dispositivos e sistemas que compõem a rede de dados. A disseminação da Web trouxe consigo a necessidade de colocar todos os serviços "sobre Web". O que aconteceu foi a natural migração das estruturas de segurança para a camada de aplicação, utilizando os mecanismos de troca de mensagens cifradas disponíveis nos protocolos de segurança embutidos nos *browsers* de qualquer utilizador. Essa mudança vem acompanhada de uma pressão crescente dos utilizadores pela utilização indiscriminada de computadores pessoais para acesso à Internet.

Outro aspecto importante da segurança da rede de dados está relacionada com a disponibilidade lógica da infra-estrutura. A rede pode ficar indisponível ou ter o seu desempenho reduzido devido à má configuração das interfaces dos *switches* e *routers*, por exemplo, quando ligações TCP operam em *half-duplex* por diferença de velocidade nas

portas, ou devido a *loops* de encaminhamento. Este tipo de problema é acidental, ou seja não é provocado, e pode ser resolvido ajustando a configuração.

O desempenho da rede pode ser também prejudicado pelo excesso de tráfego, que prejudica em particular algumas aplicações em detrimento de outras. Por exemplo, aplicações VoIP ou acessos por VPN, muito utilizadas na comunicação com as escolas superiores do IPT, embora não consumam muita largura de banda individualmente, podem representar uma parte significativa da largura de banda disponível quando se considera todo o tráfego de voz agregado. Essas aplicações são sensíveis a variações de atraso e, havendo tráfego concorrente, principalmente de natureza orientada à ligação (TCP), verão o seu desempenho prejudicado. O conhecimento do perfil de tráfego pode ajudar a dimensionar *links* de comunicação, em momentos críticos, prever e gerir a sua expansão.

A mesma problemática ocorre na rede sem fios, que opera sobre meio partilhado. Os padrões actuais de rede wireless fornecem uma banda nominal razoável (IEEE 802.11a) mas que é decrescente em função do número de utilizadores que acedem em simultâneo.

É necessário melhorar alguns detalhes da segurança da rede do IPT, sobretudo nos processos relacionados com o uso das tecnologias de informação. As normas devem ser claras e compreendidas por todos. Deve, por isso, ser empreendidos esforços para disseminar o conhecimento relacionado com a segurança. Existem assimetrias na estrutura de recursos humanos e dos departamentos que são naturais num Politécnico da dimensão do IPT; contudo, com formação adequada dos profissionais existentes é possível elevar o conhecimento relacionado com segurança, sem grandes investimentos novos.

Os equipamentos existente é aceitável e pode melhorar com pouco investimento, aumentando essencialmente o controlo sobre o que já existe. Isto pode ser conseguido com formação dos profissionais diretamente envolvidos na administração diária da rede. É interessante constar que, em grande parte, estas conclusões estão de acordo com o descrito na referencia [58].

Um outro aspecto que merece atenção é o de se garantir a segurança das aplicações e sistemas de gestão centralizada. Nesta categoria inclui-se o sistema de correio electrónico do domínio ipt**.**pt e os sistemas administrativos. Deve ser considerada a necessidade de construir uma estrutura de armazenamento de dados resistente e que permita manobras sem descontinuidades no fornecimento de serviços. Trata-se de construir um sistema com replicação síncrona de dados, em locais geograficamente distintos, e com grande

capacidade de armazenamento, permitindo a agregação de novos serviços. O armazenamento e o processamento de dados cruciais ao funcionamento do Politécnico poderá ser conduzido via sistema primário ou replicado, com vantagens:

- em situações de greves, ocupações e eventos inesperados;
- as manutenções podem ser programadas apenas a partir do cronograma da equipa técnica, sem envolver acordo com todos os dependentes da infra-estrutura;
- sistemas dependentes de armazenamento podem ser agregados no sistema proposto, podendo dispor de *backup* automático.
- o acesso aos dados poderá ser feito pela rede de armazenamento exclusiva ou pela rede Ethernet.

7. CONCLUSÃO

A informação é um dos bens mais valiosos para muitos, sejam empresas ou pessoas. Foi com esta ampla visão que surgiu a ideia de fazer o estudo do sistema de IDS/IPS utilizado na rede de dados do IPT e que tem como objetivo propocionar a maior proteção possível à infraestrutura de comunicações desta instituição.

O *FortiGate* 1000A é utilizado para proporcionar a maior proteção possível na rede do IPT. Trata-se de uma ferramenta de instalação simples, sendo que a sua configuração foi feita tendo em vista a proteção de diversos servidores. A invisibilidade do *FortiGate* pode ser considerada boa pelo fato de fazer o bloqueio de um ataque, o atacante saber que não obteve sucesso no ataque embora não saiba porquê, já que o *FortiGate* irá simplesmente fazer a negação do pacote sem mandar nenhuma mensagem de retorno.

Com a utilização do *FortiGate* 1000A no IPT foram obtidos resultados satisfatórios, principalmente contra tentativas geradas a partir de *scripts*, que às vezes podem chegar a congestionar a rede dependendo da quantidade de ataques que forem projetados.

Os resultados obtidos durante o período de avaliação demonstraram que 3,83% do total de alertas gerados foram devidamente bloqueados, equivalendo a um montante de 11.564 *hosts*, o que seria humanamente impossível de ser atingido sem o auxílio de uma ferramenta de gestão automática. Caso tal tráfego não fosse contido, a disseminação das ameaças poderia gerar um número de incidentes significativamente maior, já que o objetivo principal da maioria dos *malwares* é a sua auto replicação. Com a integração do IDS/IPS com outras ferramentas de segurança, foi possível obter um relacionamento mais seguro com os utilizadores.

A aplicação do IDS/IPS pode ser feita em qualquer rede de dados, desde que obedecidos os padrões de funcionamento da ferramenta. O ponto chave de sua utilização é o conhecimento do tráfego da rede e a aplicação das assinaturas já existentes.

A arquitetura de software da ferramenta possibilita que a investigação criteriosa das suas aplicações possa resultar num ganho ainda maior, principalmente para os agentes de detecção e bloqueio.

Relativamente à segurança das redes sem fios, estudaram-se os diversos protocolos utilizados atualmente. Embora o protocolo WPA tenha sido proposto para substituir o

WEP, corrigindo as suas vulnerabilidades, também já apresentou algumas falhas. Já o protocolo WPA2 tem cumprido bem o papel para que foi proposto, proporcionando segurança e estabilidade. É o protocolo mais utilizado atualmente.

Apesar de ter sido descoberta uma vulnerabilidade (“Hole 196”), para que ela possa ser explorada é necessário que o invasor tenha acesso à chave WPA2 e seja um utilizador autenticado na rede. Se isso acontecer, por mais seguro que qualquer protocolo possa ser, fica difícil evitar qualquer falha de segurança. Além disso, qualquer tecnologia só irá funcionar bem se for configurada devidamente, caso contrário, a má configuração dos pontos de acesso e dos clientes fará com que as invasões continuem a acontecer.

Dois meios primários de atribuir segurança a uma rede sem fios são criptografia e autenticação; o ideal é que esses métodos trabalhem juntos e se complementem. Muitas vezes somente protocolos não são suficientes para garantir o nível de segurança desejado. Nestes casos, torna-se necessário configurar outros métodos de segurança para reforçar o bloqueio, como por exemplo, a utilização de filtros baseados em MAC ou a desativação do broadcasting do SSID.

REFERENCIAS

[1] FLEISHMAN, G; ENGST A. “Kit do Iniciante em Redes Sem Fio”, 2ª Edição, Editora Makron Books, 2005.

[2] YASINSAC A., “An Environment for Security Protocol Intrusion Detection,” *Journal of Computer Security*, vol. 10, p. 177-188, 2002.

[3] TANENBAUM Andrew S. “Redes de computadores”. 4ª Edição. Rio de Janeiro, 1997.

[4] R. STERRIT, A. MARSHALL, C. SHAPCOTT, S. McCLEAN, “Exploring Dynamic Bayesian Belief Networks for Intelligent Fault Managemet Systems. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics”, vol. 5, p. 3646-3652, 2000.

[5] William Stallings, “Data and Computer Communications”, Prentice Hall International, 8ª Edição, 2006.

[6] SEKAR R., GUPTA A., FRULLO J., SHANBHAG T., TIWARI A., YANG H., ZHOU S., “Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions,” *Proceedings of the 9th ACM Conference on Computer and Communications Security,* p. 265-274, 2002.

[7] PLAGGEMEIER, M: TOLLE, J., “Secure Shell Proxy Intrusion Detection,” *Proceedings of R.T.O. Information Systems Technology Panel Symposium on Real Time Intrusion Detection,* Maio, 2002.

[8] NOONAN, Wes., DUBRAWSKY Ido., “Firewall fundamentals”,Indianapolis: Cisco Press,, 2006.

[9] NAKAMURA, Emílio Tissato; GEUS Paulo Lício de. “Segurança de redes em ambientes cooperativos”, 1ª Edição. São Paulo. Novatec, 2007.

[10] D-LINK, “D-Support for wireless LAN, D-PR; D-Linker Professional Resellers for Wireless”, 2002

[11] MCQUERRY Steve., “Interconnecting cisco network devices, Part 1 (ICND1)”, Cisco Press, 2008.

[12] J. MARIN, D. RAGSDALE, J. SURDU, “A Hybrid Approach to the Profile Creation and Intrusion Detection”. In Proceedings of the IEEE DARPA Information Survivability Conference and Exposition,” vol. 1, p. 69-76, 2001.

[13] MALIK, Saadat., “Network security principles and practice”, Indianapolis: Cisco Press, 2002.

[14] J. LUO, S. BRIDGE, M. VAUGHN, “Fuzzy Frequent Episodes for Real-Time Intrusion Detection”, In Proceedings of the 10th IEEE International Conference on Fuzzy Systems,” vol. 1, p. 368-371, 2001.

[15] REHMAN, Rafeeq. “Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID”, 1ª edição. New Jersey: Prentice Hall, 2003.

[16] T. LECKIE, A. YASINSAC, “Metadata for Anomaly Based Security Protocol Attack,” *IEEE Transactions on Knowledge and Data Engineering,* vol. 16 N. 10, Outubro 2004.

[17] T. KOHONEN, “Learning Vector Quantization for Pattern Recognition. Technical Report, TKK-F-A601. University of Technology, Helsinki,” 1986. [Online]. Disponível em: www.cis.hut.fi/~mikkok/dt.ps.gz. [Acedido em 03 2013].

[18] S. JOGLEKAR, S. TATE, “ProtoMon: Embedded Monitors for Cryptographic Protocol Intrusion Detection and Prevention,” *IEEE International Conference on Information Technology: Coding and Computing,* vol. 1, p. 81-88, Abril 2004.

[19] JAVITZ, Harold S. VALDES, Alfonso., "The SRI IDES Anomaly Detector". In: Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy," p. 316 –326, 1991.

[20] C. HUNT, "TCP/IP network administration", 3ª Edição, O'Reilly, 2002.

[21] G. HELMER, J. WONG, V. HONAVAR, L. MILLER, "Automated Discovery of Concise Predictive Rules for Intrusion Detection," 2000. [Online]. Disponível em: http://www.researchindex.com. [Acedido em Agosto 2013].

[22] P.HELMAN, "Statistical Foundations of Audit Trail Analysis for the Detection of Computer Misuse", IEEE Transactions on Software Engineering," vol. 19, p. 886-901, Setembro 1993.

[23] HARRINGTON Jan. "Network security: a practical approach", San Francisco: Elsevier Inc. 2005.

[24] E. HALL, "Internet core protocols: The Definitive Guide", O'Reilly, 2000.

[25] ENDORF, Carl; SCHULTZ, Eugene;, MELLANDER, Jim. "Intrusion Detection and Prevention". 1ª edição. Chicago: McGraw-Hill Osborne Media, 2004.

[26] CARTER Earl; HOGUE, Jonathan. "Intrusion prevention fundamentals". Indianapolis: Cisco Press, 2006.

[27] DOSTÁLEK Libor, KABELOVÁ, Alena. "Understanding TCP/IP: a clear and comprehensive guide to TCP/IP protocols", Packt Publishing Ltd, 2006.

[28] COX, Kerry J; GERG, Christopher. "Managing security with Snort and IDS tolls". Sebastopol: O'Reilly, 2004.

[29] CIAMPA, Mark. "Security + Guide to network security fundamentals",3ª Edição. Boston. Course Technology, 2009.

[30] B. CARNE, "A professional's guide to data communication in a TCP/IP world", Artech House Inc, 2004.

[31] C. LECKIE, R. KOTAGIRI, "A Probabilistic Approach to Detecting Network Scans", In Proceedings of the IEEE/IFIP Network Operation and Management Symposium," p. 359-372, 2002.

[32] BURKHOLDER, P., "SSL Man-in-the-Middle Attacks," SANS Reading Room, 2002. [Online]. Disponível em: <http://www.sans.org/rr/whitepapers/threats/480.php>. [Acedido em Fevereiro 2013].

[33] BRONSTEIN A., "Self-Aware Services: Using Bayesian Networks for Detecting Anomalies in Internet-based Services", In IEEE/IFIP INTEGRATED NETWORK MANAGEMENT PROCEEDINGS , p. 623-638, 2001.

[34] BRENTON, Chris; HUNT Cameron. "Active defense: A comprehensive guide to network", Alameda:: SYBEX Inc, 2001.

[35] BHAIJI Yusuf, "CCIE professional development series network security technologies and solutions", 1ª Edição; Cisco Press, 2008.

[36] "McAfee Labs, "McAfee Threats Report: Third Quarter 2010", [Online]. Disponível em: http://www.mcafee.com/us/threat_center/white_paper.html . [Acedido em Outubro 2012].

[37] "Fortinet FortiGate FortiGate-1000 Administration," [Online]. Disponível em: http://www.manualslib.com/manual/239810/Fortinet-Fortigate-Fortigate-1000.html . [Acedido em Outubro 2012].

[38] "Cisco-1, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2009-2014,. [Cited 2010-12-15].," [Online]. Disponível em: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html. [Acedido em Agosto 2013].

[39] CERT Coordination Center, “Vulnerability Discovery: Bridging the Gap Between Analysis and Engineering”, [Online]. Disponível em: http://www.cert.org/archive/pdf/CERTCC_Vulnerability_Discovery.pdf. [Acedido em Maio 2013].

[40] SCOTT Charlie; WOLFE, Paul; HAYES, Bert. “Snort for Dummies. Hoboken: Publishing Inc., 2004

[41] SOARES, Luiz Fernando Gomes. LEMOS, Guido; COLCHER Sergio, “Redes de computadores: das LANs, MANs e WANs as Redes ATM”, Rio de Janeiro, 1995.

[42] ALPCAN, Tansu, BASAR Tamer, “Network security: decision and game theoretic approach”, 1ª Edição, Illinois: Cambridge University Press, 2010.

[43] BHARDWAJ, Pawan K., “A+, Network+, Security+ Exams”, 1ª Edição, O’Reilly, 2007.

[44] SMITH, Sean; MARCHESINI John., “The craft of system security”, vol. 1ª Edição. Boston: Addison-Wesley Professional, 2008.

[45] DOHERTY, Jin; ANDERSON, Neil; MAGGIORA Paul Delta., “Cisco neworking simplified”, 2ª Edição. Indianapolis: Cisco Press, 2007.

[46] VYNCKE, Eric, C. PAGGEN, “LAN switch security: What hackers know about your switches”, Indianapolis: Cisco Press, 2007.

[47] VACCA, John R., “Network and system security”, 1ª Edição. Burlington: Syngress, 2010.

[48] TODOROV, Dobromir., “Mechanics of user identification and authentication: fundamentals of identity management”. New York: Auerbach Publications, 2007

[49] WI-FI ALLIANCE, “Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise”, Março, 2005. Disponível em: http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf (Acedido em Outubro, 2013)

[50] RUFINO, N. M. “Segurança em redes sem fio – Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth”. São Paulo. Novatec, 2005

[51] IDG NOW!, “Descoberta falha no protocolo de segurança Wi-Fi WPA2”, Disponível em: http://computerworld.uol.com.br/seguranca/2010/07/26/descoberta-falha-no-protocolo-de-seguranca-wi-fi-wpa2 (Acedido em Novembro, 2013)

[52] CASWELL, Brian; BEALE, Jay; BAKER, Andrew; “Snort IDS and IPS Toolkit”, Jay Beale's Open Source Security, Syngress, 2007.

[53] TIPTON, Harold F; KRAUSE, Micki. “Information security management handbook”, 6ª edição. Boca Raton: Auerbach Publications, 2007.

[54] MAIA, Igor da Silva Neiva; REHEM, Sandro Herman Pereira. “Sistemas de prevenção de intrusão baseado em software livre: debian e snort”, Projeto final para obtenção do grau de especialista em Rede de Computadores, Brasília, 2005. Disponível em: http://www.scribd.com/doc/13224983/Sistemas-de-Prevencao-de-Intrusao-baseado-em-Software-Livre-Igor-Neiva-e-Sandro-Herman-UCB (Acedido em Novembro, 2012)

[55] AXELSSON, Stefan. Research in Intrusion-Detection Systems: A Survey. 1998. Technical Report, Department of Computer Engineering, Chalmers University of Technology Göteborg, Sweden, Disponível em: http://www.researchindex.com/

[56] COOLEN, R; LUIJF, H. N. M. “Intrusion Detection: Generics and Stat-of-the-Art”, 2002, Technical Report, North Atlantic Treaty Organization, Disponível em: <http://www.dtic.mil/dtic/tr/fulltext/u2/a418712.pdf> (Acedido em Janeiro, 2013)

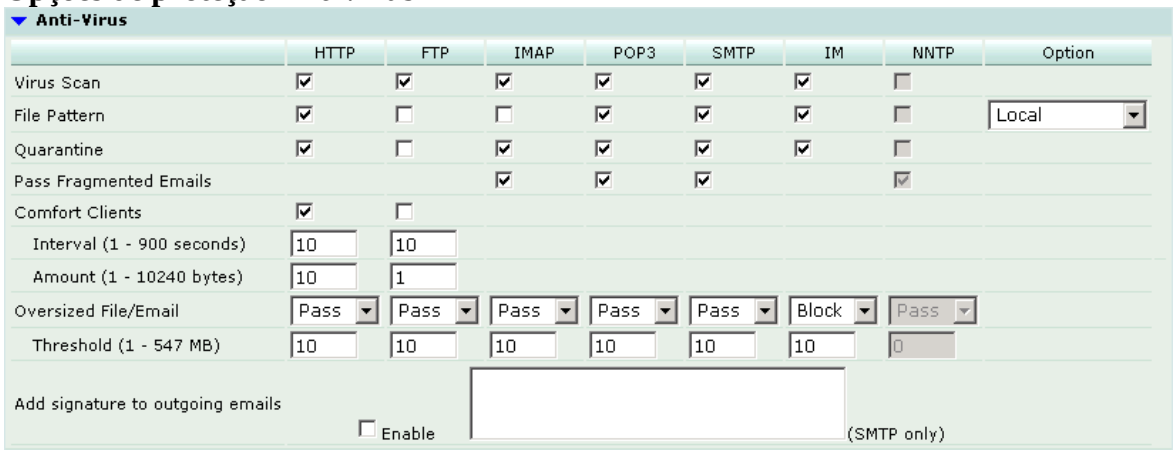
[57] WARRENDER, Christina: FORREST, Stephanie: PEARLMUTTER, Barak. “Detecting Intrusions Using System Calls: Alternative Data Models”. In Proceedings of the IEEE Symposium on Security and Privacy”, p. 133 –145, 1999.

[58] B. Schneier, “University Networks and Data Security”, IEEE Security and Privacy , Volume 4 , Issue 5 (Setembro 2006), p. 88. ISSN:1540-7993

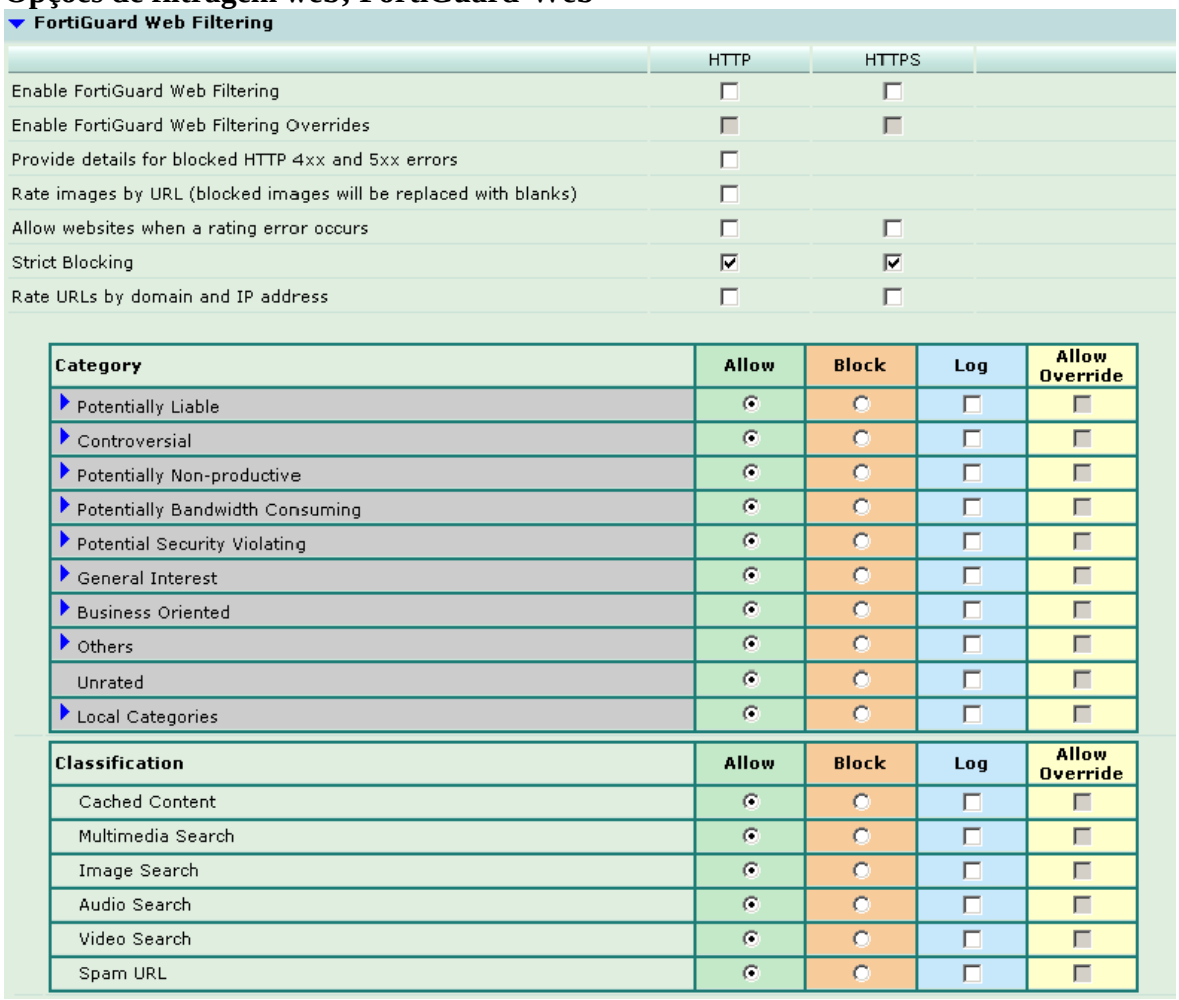
ANEXOS

Neste anexo são apresentadas algumas das opções de configuração do FortiGate 1000A.

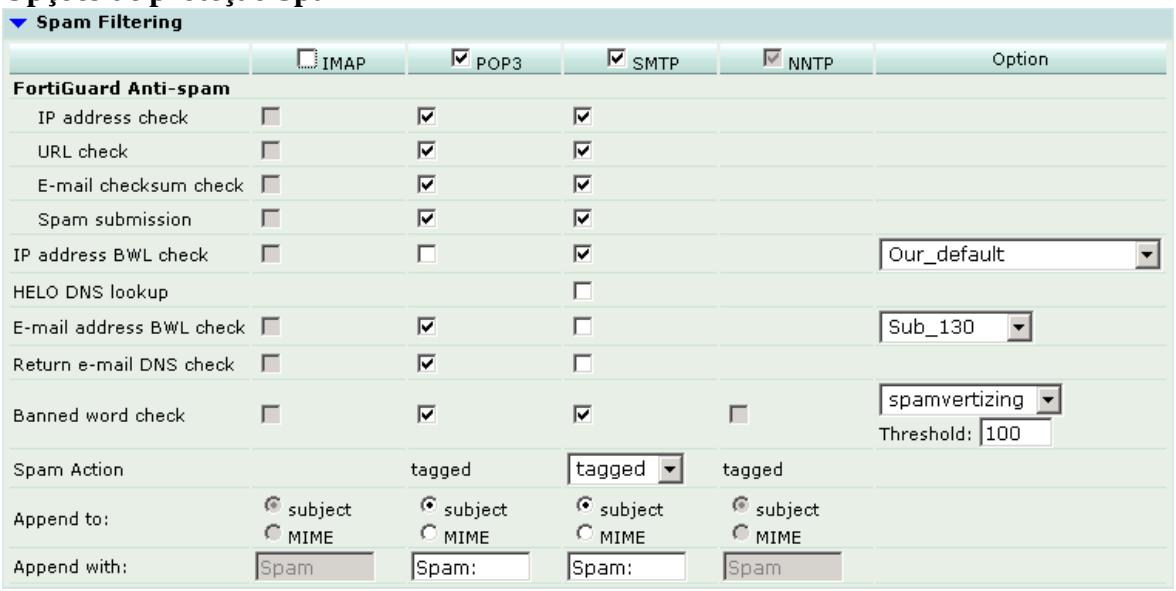
Opções de proteção AntiVirus



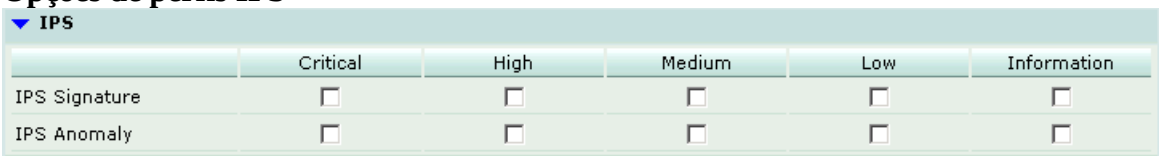
Opções de filtragem web; FortiGuard-Web



Opções de proteção Spam



Opções de perfis IPS



Opções de perfis de conteúdo do ficheiro FortiAnalizer

Estão disponíveis as opções seguintes para IM e P2P através do perfil de proteção