Instituto Politécnico de Leiria

Departamento de Engenharia Informática

Dissertação de Mestrado em Engenharia Informática

Computação Móvel

Deep Packet Inspection em Redes Wireless de Âmbito Alargado

Paulo Alexandre Nogueira Jorge

Leiria, Setembro de 2013

Agradecimentos

Esta tese não poderia estar concluída sem prestar um especial agradecimento a todos os que me ajudaram a concretizá-la.

Em primeiro lugar, gostaria de agradecer ao meu orientador: ao Professor Doutor António Manuel de Jesus Pereira, por toda a orientação, simpatia e disponibilidade demonstrada ao longo de todo este ano letivo e ao longo dos vários anos em que tive o prazer de receber todos os seus ensinamentos nesta grande Instituição.

Ao Instituto Politécnico de Leiria, e em especial, ao Departamento de Engenharia Informática (DEI) da Escola Superior de Tecnologia e Gestão (ESTG) por todas as condições de trabalho disponibilizadas.

A todos os meus colegas de curso - em especial ao Daniel Fuentes, Cláudio Freire, Luís Correia e Rui Sábio - que me acompanharam ao longo desta dura jornada e com os quais tive uma cooperação excelente.

Aos meus familiares e amigos, um enorme obrigado pela presença e apoio no decorrer deste meu percurso académico.

Os agradecimentos finais vão para os meus pais pelo apoio constante e incentivo ao longo da realização deste projeto e de todo o curso. Sem o seu esforço, nada disto teria sido possível.

A todos os que foram referidos, um muito obrigado!

Resumo

No mundo das Redes de Computadores existem os mais distintos problemas, mas os dois que persistem em continuar a dar maiores dores de cabeça aos administradores de sistemas deste tipo de infraestruturas são a segurança e o exponencial aumento das aplicações consumidoras de largura de banda. Para além disso, ainda existem várias zonas no país, especialmente nos meios rurais, que não dispõem de qualquer infraestrutura que permita aos seus habitantes estabelecerem qualquer tipo de contacto com a rede tecnológica global - a Internet.

O DEI, em parceria com o CIIC e o INOV, encetou um projeto inovador que permitiu colmatar este problema de infoexclusão numa freguesia dos arredores do distrito de Leiria - freguesia da Memória. Este projeto consistiu na implementação de uma infraestrutura de acesso à Internet baseada em comunicações sem fios. O sucesso foi de tal ordem que gerou uma enorme aceitação por parte de todos os habitantes das distintas localidades pertencentes à freguesia - o que levou a um enorme crescimento no consumo da baixíssima largura de banda disponível.

Esta dissertação pretende apresentar uma solução para suprir o problema da caracterização do tráfego que circula nesta tipologia de redes. Essa caracterização deve permitir realizar a distinção entre o tráfego de trabalho do lúdico. Para isso, a mesma é baseada no tema das *firewalls* de nova geração, mais especificamente recorrendo à tecnologia *Deep Packet Inspection* de forma a analisar todo o tráfego que circula pela infraestrutura de rede e, dessa análise, proceder à caracterização do mesmo. Essa informação será um recurso muito importante que pode ser utilizado pelos administradores de sistemas para otimizar a largura de banda existente de forma a distribuí-la equitativamente por todos os utilizadores.

Os resultados alcançados, nos testes elaborados à solução implementada, revelaram o potencial que um mecanismo de *Deep Packet Inspection* bem configurado, numa rede sem fios de âmbito alargado, pode trazer aos administradores de sistemas da mesma pelo detalhe que é apresentado quanto à caracterização do tráfego.

Abstract

We have the most distinct kind of problems in the networking computer world, but the two of them that continue to persist to give big headaches to the system administrators are security and the increase of bandwidth by applications. There are still several regions in the country, especially in rural areas, which have no infrastructure that allows its inhabitants to establish any kind of contact with the Internet.

DEI, in partnership with the CIIC and INOV, undertook an innovative project to implement a wireless infrastructure for Internet access in the parish of Memória – located near the city of Leiria. The project was such a success that generated a huge acceptance by all the residents from the distinct localities. That led to an enormous growth in the consumption of the very low bandwidth available for everyone.

This dissertation aims to present a solution to overcome the problem of characterizing the traffic that flows in this type of networks. This characterization should perform a differentiation between the working and entertaining traffic. To perform that, it is based on the theme of the next-generation firewalls, specifically using Deep Packet Inspection technology in order to analyze the entire packets that are flowing through the network infrastructure. This information will be a very important resource that can be used by systems administrators to optimize the network and to find methods to distribute the bandwidth equitably by all users.

The results achieved, after testing the implemented solution, revealed the potential that a good mechanism of Deep Packet Inspection can bring to this kind of infrastructures.

Índice

Índice de Figuras

Índice de Tabelas

Listagem de acrónimos

Sigla	Significado
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
ASP	Active Server Pages
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CBQ	Class Based Queuing
CBR	Constant Bit Rate
CGI	Common Gateway Interface
CIIC	Centro de Investigação em Informática e Comunicações
CLI	Command Line Interface
CSS	Cascading Style Sheets
CSV	Comma-separated values
DEI	Departamento de Engenharia Informática
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
DSCP	Differentiated Services
DSL	Digital Subscriber Line
EEPROM	Electrically-Erasable Programmable Read Only Memory
EPROM	Erasable Programmable Read Only Memory
ESTG	Escola Superior de Tecnologia e Gestão
ETSI	European Telecommunications Standards Institute
FIFO	First In, First Out
FTP	File Transfer Protocol
GNU	GNU's Not Unix

GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPL	Instituto Politécnico de Leiria
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPTV	Internet Protocol Television
IR	Infrared
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
Kbps	Kilobits Per Second
KBps	KiloBytes Per Second
LDAP	Lightweight Directory Access Protocol
LED	Light-emitting diode
Mbps	Megabits Per Second
MIMO	Multiple-Input Multiple-Output
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
P2P	Peer-to-peer
PHP	PHP: Hypertext Preprocessor
PoE	Power over Ethernet
PROM	Programmable Read Only Memory
QoS	Quality of Service
RED	Random Early Detection
RF	Radio Frequency
ROM	Read Only Memory
RSVP	Resource Reservation Protocol
SDK	Software Development Kit

SFQ	Stochastic Fair Queuing
SMTP	Simple Mail Transfer Protocol
SO	Sistema Operativo
SONET	Synchronous Optical Networking
SSH	Secure Shell
SSL	Secure Sockets Layer
TBF	Token Bucket Filter
TC	Traffic Control
TOS	Type of Service
TPC	Transmission Control Protocol
URL	Uniform Resource Locator
VBR	Variable Bit Rate
VLAN	Virtual Local Area Network
VoIP	Voice Over IP
VPN	Virtual Private Network
WBL	Wireless de Banda Larga
WEP	Wired Equivalent Privacy
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WRAN	Wireless Regional Area Network

Capítulo 1

1 Introdução

O exponencial aumento do consumo da largura de banda é, e sempre foi, um problema crítico na área das redes de computadores. Mesmo com o aumento das velocidades de acesso, o problema continua em subsistir, pois os utilizadores estão cada vez mais sedentos de informação, especialmente desde o *boom* dos *smartphones/tablets* associados às redes móveis e ao acentuado consumo de tráfego multimédia, necessidade de informação em qualquer lado e a qualquer hora.

Apesar do aumento do consumo de largura de banda por parte dos utilizadores ser um tema crítico em quase todo o género de topologias de rede, quem sofre mais são as redes sem fios, especialmente as redes *wireless* de âmbito alargado. Isso acontece, pois na maioria das vezes essas redes são implementadas em locais onde o acesso à Internet é inexistente ou caso exista, é de baixo débito. Para além disso, e tal como o próprio nome indica (âmbito alargado) essas redes fornecem não só o típico acesso à Internet, mas outros tipos de serviços existentes na própria infraestrutura – *streaming* de vídeo,

repositório de dados ou *backups*, acesso a serviços através de *cloud computing*, entre muitos outros.

Desse cenário coloca-se a seguinte questão: de que forma é que se consegue diferenciar cada tipo de serviço e obter estatísticas do que circula na rede? Para isso, existe uma forma de analisar o payload de cada pacote que circula na rede recorrendo ao *Deep Packet Inspection* (DPI).

O *Deep Packet Inspection* é muito útil para analisar cada pacote à procura de deformidades a nível de protocolos, *vírus*, *spam*, intrusões e aplicações para decidir se esse mesmo pacote pode, ou não, seguir o seu caminho ou se o mesmo precisa de ser encaminhado/classificado/bloqueado. O DPI também é usado para efeito de recolha de informação estatística do que se passa na rede.

Recorrendo ao *Deep Packet Inspection* podemos analisar de uma forma mais aprofundada o que realmente se passa nas redes *wireless* de âmbito alargado e, tentar assim, otimizar os recursos existentes para que os mesmos sejam distribuídos de uma forma mais justa por todos os utilizadores de acordo com o tipo de aplicação.

1.1 Objetivos

O principal objetivo desta dissertação é o de delinear um protótipo que permita realizar a análise e, dessa mesma análise, proceder à caracterização de todo o tráfego que circula numa infraestrutura de rede, permitindo assim, otimizar os recursos a nível de largura de banda, em especial em redes *wireless* de âmbito alargado.

Para tal, o modelo baseou-se na infraestrutura já existente, e em funcionamento há vários anos, na freguesia da Memória que se encontra dividida em três classes distintas:

- Servidores: responsáveis pelo fornecimento de todos os serviços disponíveis para os habitantes (monitorização da rede, partilha de ficheiros, *streaming*, entre outros);
- *Routers*: estes dispositivos são essenciais ao encaminhamento e tratamento de todo o tráfego que circula na rede e à interligação das diferentes localidades dispersas pela freguesia;

- Clientes: usufruem dos serviços que lhes chegam por intermédio do equipamento que possuem em casa e que capta o sinal que é enviado através das antenas distribuídas ao longo de toda a infraestrutura.

Os seguintes objetivos enumerados pretendem colmatar alguns dos problemas presentes em cada uma das diferentes classes expostas anteriormente, sendo eles:

- Implementação de um *gateway* que realize a ponte entre a rede interna e a rede externa;
- Implementação de um servidor que utilize um mecanismo de *Deep Packet Inspection* para proceder à análise de todo o tráfego gerado pelos utilizadores da rede;
- Implementação de um portal, *web-based*, que da análise dos pacotes realizados pelo servidor descrito no ponto anterior, disponibilize a informação de forma amigável ao administrador da rede e que caracterize o tráfego o mais detalhadamente possível;
- A solução final deverá ser capaz de se encaixar com ferramentas de análise de rede tais como: Nagios, Cacti, Observium entre outros.

Este projeto pretende otimizar o funcionamento das redes de âmbito alargado, mais especificamente aquelas que tenham um esquema muito similar ao existente na Memória, contribuindo assim, para uma experiência mais equitativa por todos os utilizadores no acesso a todos os serviços disponíveis.

Procura-se ainda demonstrar que é possível implementar uma moderna solução que permita analisar e caracterizar todo tráfego que circule numa rede, recorrendo a um moderno mecanismo de *Deep Packet Inspection*, associado à ideologia de *firewalls* de nova geração, apenas e só recorrendo à utilização de *software* de código aberto.

1.2 Estrutura do Documento

O presente documento encontra-se organizado de forma a permitir que o leitor compreenda progressivamente as várias fases de desenvolvimento de todo este trabalho. Estas vão desde a fase de investigação até à apresentação da solução desenvolvida, testes e considerações finais do projeto.

O segundo capítulo apresenta os principais protocolos, aborda o funcionamento dos canais e frequências para além de descrever os diferentes tipos de redes sem fios existentes.

No terceiro capítulo são abordados os diferentes mecanismos existentes para a realização da qualidade de serviço nas telecomunicações e de que forma este podem, ou não, influenciar as aplicações de rede. A descrição dos três modelos de QoS mais utilizados é efetuada no término desse capítulo.

O capítulo quatro pretende demonstrar a importância do tema da segurança quando se debate o tema das redes informáticas.

O capítulo seguinte, o quinto, transporta o leitor para a evolução das *firewalls* ao longo dos anos e permite entender a enorme mudança que as mesmas sofreram.

O sexto capítulo descreve um dos temas que muito se tem ouvido falar nestes últimos tempos nesta área - o conceito de *Deep Packet Inspection*. Explica-se o que é, para que serve e os enormes ganhos que podem advir da utilização desta tecnologia.

No sétimo capítulo, arquitetura, é realizado um levantamento das necessidades existentes na infraestrutura de uma rede rural sem fios de âmbito alargado. Ao realizar esse levantamento os problemas identificados foram divididos em várias partes sendo que cada uma delas se foca em problemas específicos.

O oitavo capítulo apresenta, de uma forma muito genérica, todos os passos que foram necessários para implementar a solução final que tem como principal propósito minimizar grande parte das deficiências identificadas no capítulo anterior. Para além disso, também são descritas as principais ferramentas utilizadas no decorrer de todo este processo.

De forma a verificar a eficiência e o bom funcionamento de toda a solução implementada é apresentado, no capítulo nove, um conjunto de testes cujo objetivo é o de validar as funcionalidades mais importantes. Como se pode imaginar, é de todo impossível conseguir incluir todos os testes efetuados neste documento.

A conclusão deste relatório situa-se no décimo, e último capítulo, onde são expostas algumas reflexões finais, para além de deixar em aberto algumas ideias para trabalho futuro.

Capítulo 2

2 Redes Wireless

As redes de banda larga de comunicações Wireless têm tido, nestes últimos anos, um crescimento exponencial no meio tecnológico. Este tipo de comunicações está amplamente implementado em todas as áreas de negócio, especialmente em zonas rurais que se encontram, normalmente, mais isoladas. Em algumas regiões rurais do território nacional esse isolamento leva a um fraco investimento por parte das operadoras de telecomunicações em infraestruturas cabladas, visto não existir o número de habitantes necessários para obterem um retorno financeiro fiável e sustentado. A solução para esses casos é a implementação de redes WBL (Wireless de Banda Larga).

Neste capítulo são abordados alguns conceitos relativamente às redes sem fios, tais como: normas IEEE 802.11, frequências e alguns tipos de redes Wireless.

2.1 IEEE 802.11

Em 1990 o IEEE definiu uma comissão científica com o principal objetivo de investigar um padrão fiável para a comunicação sem fios. Ao fim de sete anos de investigação e desenvolvimento, essa comissão, em 1997, aprovou o padrão IEEE 802.11 que trabalha com taxas de transmissão na ordem dos 1 e 2 Mbps e opera no intervalo de frequências entre 2,4 GHz e 2,4835 GHz [Selada, 2008].

Nos tópicos seguintes são descritas algumas das normas mais utilizadas em redes WBL que derivaram deste padrão.

2.1.1 IEEE 802.11a

Este padrão Wi-Fi foi definido em 1999 para a frequência dos 5GHz. Tem uma capacidade de transmissão máxima de até 54 Mbps, apesar de alguns fabricantes não padronizados terem conseguido velocidades entre 72 e 108 Mbps. Inicialmente, suportava um máximo de 64 utilizadores ligados num único AP (*Access Point*), tendo como principal desvantagem a utilização uma frequência não licenciada - não acessível a todos. O alcance geográfico máximo na sua transmissão é de aproximadamente 50 metros.

Apesar da data da sua criação ter sido em 1999, apenas em 2001 se começaram a comercializar os primeiros equipamentos que funcionavam com esta norma. O atraso na comercialização permitiu que a norma IEEE 802.11b a suplantasse. Para além disso, a incompatibilidade entre estas duas normas teve um enorme impacto na predominância no mercado global. Como se pode imaginar, e apesar da vantagem da velocidade de transmissão para um curto alcance, a primeira perdeu em relação à sua grande concorrente não só pelo atraso na comercialização de equipamentos, mas também pelo elevado custo dos equipamentos [Frazão, 2011].

2.1.2 IEEE 802.11b

No final de 1999 foi lançada uma atualização do padrão 802.11, designado de 802.11b. A grande diferença em relação ao padrão predecessor é a possibilidade de conseguir estabelecer comunicações nas seguintes velocidades de transmissão: 1 Mbps, 2 Mbps, 5.5 Mbps e 11 Mbps. Opera no mesmo intervalo de frequência que o seu antecessor, ou seja, entre os 2,4 GHz e 2,4835 GHz. Caso não existam interferências que impeçam a

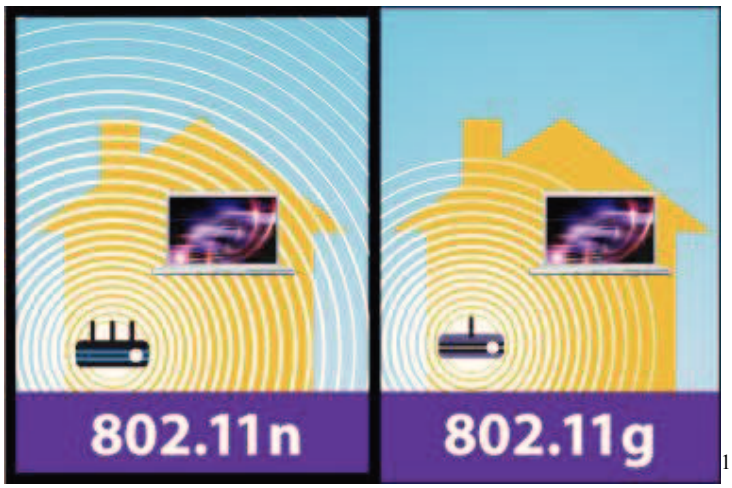
propagação da transmissão, a área de cobertura, teórica, é de 140 metros em espaços abertos e de 38 metros em lugares fechados (escritórios, residências, escolas). O padrão 802.11b foi o grande responsável pela popularização, em vasta escala, das redes Wi-Fi [Salvador, 2008].

2.1.3 IEEE 802.11g

Este padrão foi definido em 2003, sendo o sucessor da versão 802.11b. Os dois modelos são compatíveis, ou seja, um dispositivo de rede que esteja a trabalhar no modo 802.11g pode comunicar sem qualquer problema com outro a operar em 802.11b. É necessário ter em conta que a transmissão dos dados fica restringida, pois a velocidade de transmissão na norma mais antiga é menor. A grande vantagem é a de operar com taxas de transmissão de até 54 Mbps, ou seja, velocidade semelhante ao padrão 802.11a. A diferença entre os dois é que o 802.11g funciona na frequência dos 2,4 GHz, ao contrário da norma 802.11a que opera nos 5 GHz o que possibilita que o primeiro tenha uma área de cobertura mais vasta (semelhante à do seu antecessor - IEEE 802.11b) [Salvador, 2008].

2.1.4 IEEE 802.11n

O padrão IEEE 802.11n começou a ser desenvolvido em 2004 e entrou em funcionamento em 2009 com o intuito de suceder ao 802.11g. A grande diferença em relação aos seus antecessores foi a de adicionar uma nova funcionalidade, o *Multiple-Input Multiple-Ouput* (MIMO), que permite aumentar a taxa de transferência de dados combinando vários meios de transmissão, ou seja, podem ser utilizadas múltiplas antenas para transmissão e receção. Este novo mecanismo permitiu aumentar de forma drástica a transmissão de dados até um valor máximo de 600 Mbps. Permite operar numa das duas frequências: 2,4 GHz ou 5 GHz, o que lhe permite ser completamente compatível com todos os padrões criados anteriormente. O espaço de cobertura em relação aos seus antecessores é quase do dobro, sendo que, teoricamente, em espaços fechados é de 70 metros, enquanto em lugares abertos é de 250 metros [Fuentes et all, 2011].



[1]

Figura 1 - Comparação de sinal - 802.11n vs 802.11g

2.1.5 IEEE 802.11e

Esta norma, definida em 2005, foi reconhecida por conseguir agregar QoS nas redes sem fios. É particularmente interessante para aplicações sensíveis a interferências, tendo como exemplo as comunicações *Voice Over IP* (VoIP) e *Internet Protocol Television* (IPTV). Resumindo, veio possibilitar diferenciar o tráfego que circula pela rede através de classes [Fuentes et all, 2011].

2.1.6 IEEE 802.11h

A especificação IEEE 802.11h foi definida para o correto funcionamento dos padrões: 802.11a e 802.11n, que operam nos 5 GHz, na Europa. O principal objetivo é o de incrementar os *standards* em questão com funções que permitam diminuir ou mesmo eliminar possíveis interposições. Para tal, o padrão 802.11h utiliza dois mecanismos para otimizar as transmissões via rádio:

- TPC: permite que o rádio ajuste a potência do sinal consoante a distância do recetor;
- DFS: escolhe um canal, automaticamente, de forma a minimizar a interferência noutros sistemas que operem na mesma frequência [Fuentes et all, 2011].

[1] Fonte: http://www.sonnettech.com/product/images/side_ariaextremen_1010.jpg

2.1.7 IEEE 802.11i

O desenvolvimento desta norma teve como principal objetivo otimizar a segurança - especialmente desde que foram detetadas vulnerabilidades no algoritmo *Wired Equivalent Privacy* (WEP) - nas comunicações sem fios bem como os mecanismos de autenticação existentes.

Devido a tudo isso, e com o objetivo de combater essas vulnerabilidades, em 2003 foi criado o *Wi-Fi Protected Access* (WPA). Foram realizadas modificações quanto ao tipo de cifragem utilizada – passou-se a usar uma chave de 128 bits e um *Initialization Vector* (IV) de 48 bits [Fuentes et all, 2011].

2.2 Canais e Frequências

Como vimos no tópico anterior (2.1), o IEEE 802.11, mais conhecido por WLAN/Wi-Fi, permite definir os atributos para os diferentes canais utilizados. Estes atributos permitem que se realize a comunicação entre os diferentes módulos Wi-Fi criando assim uma WLAN. Para garantir que as soluções WLAN operem de uma forma satisfatória, os parâmetros, tais como: as frequências de sinal RF (rádio frequência), os números dos canais e as larguras de banda, devem ser corretamente definidos.

As normas 802.11b, 802.11g e 802.11n operam nos 2,4 GHz, ou seja, no espectro de licença gratuita para utilizadores individuais, não sendo assim necessária requisitar uma licença de utilização.

2.2.1 Noção básica de canal

No padrão 802.11 existe um total de catorze canais definidos para serem utilizados na frequência dos 2,4 GHz. Nem todos os canais são permitidos em todo o mundo. A Anatel autoriza 11 que são usados na América do norte, enquanto na Europa são permitidos o uso de 13 canais definidos pelo ETSI. Os canais têm um espaçamento de 5 MHz de distância, com exceção dos dois últimos que têm um espaçamento de 12 MHz. O padrão 802.11 especifica uma largura de banda de 22 MHz e 25 MHz na separação dos canais, embora os valores nominais mais comummente utilizados sejam de 20 MHz. O espaçamento da largura de banda em 20/22 MHz e a separação dos canais em 5 MHz significa que os canais adjacentes se sobrepõem provocando assim, interferências nos canais adjacentes.

Os 22 MHz de largura de banda por canal são válidos para todas as normas, apesar de o padrão 802.11b poder funcionar nas seguintes velocidades: 1, 2, 5.5 ou 11 Mbps, enquanto a norma 802.11g pode funcionar até uma velocidade máxima de 54 Mbps. As diferenças surgem no esquema de modulação RF utilizado, apesar dos canais WLAN serem idênticos em todas as normas 802.11 aplicáveis.

Ao utilizar o Wi-Fi como forma de fornecer serviços em WLANs para escritórios, escolas, *Hotspots*, entre outros locais, é fundamental assegurar que os parâmetros dos canais estejam corretamente definidos, de forma a garantir o desempenho pretendido.

A tabela abaixo demonstra as frequências dos catorze canais Wi-Fi disponíveis em todo o mundo.

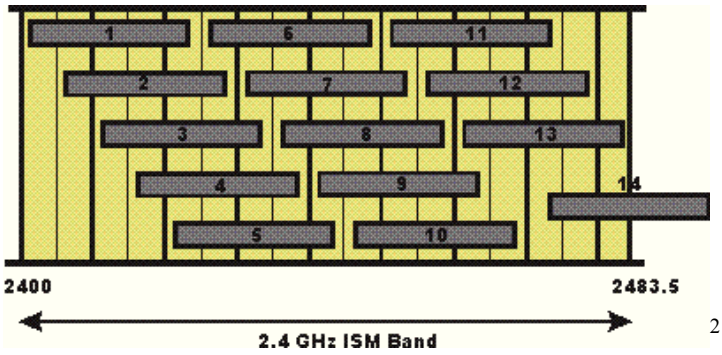
Número do canal	Frequência menor (em MHz)	Frequência intermédia (em MHz)	Frequência maior (em MHz)
1	2401	2412	2423
2	2404	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2451	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

Tabela 1 - Listagem de frequências dos 14 canais na gama dos 2,4 GHz

De notar que nem todos os canais estão acessíveis em todos os países.

2.2.2 Sobreposição e seleção

Os canais utilizados no padrão IEEE 802.11 estão separados em intervalos de 5 MHz e cada um tem uma largura de banda de 22 MHz. Como se pode observar na imagem abaixo (Figura 2 - Sobreposição de canais Wi-Fi), há cinco combinações possíveis para a ocorrência de sobreposição de canais:



[2]

Figura 2 - Sobreposição de canais Wi-Fi

1. 1, 6 e 11;
2. 2, 7 e 12;
3. 3, 8 e 13;
4. 4, 9 e 14 se esta última permitir;
5. 5, 10 e 14 se a última ocorrer.

Normalmente, os *routers* estão definidos, por defeito, para utilizar o canal 6, ou seja, a sobreposição mais provável de acontecer é a primeira.

Devem-se utilizar, preferencialmente e de forma a reduzir ao máximo as interferências, os canais mais separados entre si, pois a energia tende a alastrar-se acima da largura de banda nominal [Fuentes et all, 2011].

2.3 Tipos de redes wireless

As redes WLAN, também conhecidas por Wi-Fi ou redes sem fios, são recorrentemente utilizadas. As constantes melhorias dos protocolos e padrões existentes, para além da criação de muitos outros, permitem que as mesmas tenham velocidades de transferência muito elevadas e com um cada vez menor tempo de latência.

[2] Fonte: http://www.radio-electronics.com/

No mundo das redes sem fios existem vários tipos de redes. Nos tópicos seguintes são descritos os mais conhecidos e as suas principais características [Salvador, 2008].

2.3.1 WPANs - Redes Pessoais

Os tipos de redes *Wireless Personal Area Network* (WPAN) caracterizam-se por serem de curto alcance, ou seja, correspondem, aproximadamente, à área de trabalho de uma pessoa (10 metros). Interligam todos os dispositivos utilizados por um utilizador: computadores, portáteis, impressoras, *smarthphones*, entre outros tipos de dispositivos.

Figura 3 - Exemplo de uma rede WPAN

Existem distintas tecnologias associadas às WPANs. Aquela que deve ser a mais conhecida, pelo simples facto de vir na maior parte dos dispositivos móveis que são vendidos hoje em dia, é o *Bluetooth* (também conhecido por IEEE por 802.15.1[3]) que foi lançado pela Ericsson no ano de 1994. Permite um *throughput* máximo na ordem de 1 Mbps num alcance de até 30 metros. Uma das suas reconhecidas mais-valias vem da sua eficiente utilização de energia o que faz uma tecnologia apetecível de implementar em pequenos dispositivos móveis.

Outras das tecnologias associadas a este tipo de redes *wireless* são os infravermelhos (IR - infrared) que têm vindo a cair em desuso, pois apesar de permitirem velocidades de alguns megabits por segundo, necessitam que haja linha de vista entre os dispositivos envolvidos na troca de informação. Foi lançada em 1995 e conta com mais de 150 membros.

[3] http://www.ieee802.org/15/pub/TG1.html

O ZigBee – também designado de IEEE 802.15.4[4] – é recorrentemente utilizado para interligar dispositivos *wireless*. Tem um custo muito reduzido associado a uma eficiência energética muito interessante para que seja utilizado em pequenos dispositivos eletrónicos. Funciona no espectro dos 2.4 GHz recorrendo a 16 canais o que permite velocidades de transferência na ordem dos 250 kbps num alcance de até 100 metros.

As redes WPAN são oficialmente designadas pela norma IEEE 802.15 [Fuentes et all, 2011].

2.3.2 WLAN - Redes Locais

As redes *Wireless Regional Area Network* (WLAN), mais conhecidas por Wi-Fi, estão bastante em voga. Como o próprio título indica, são utilizadas em redes locais: escritórios, prédios ou *campus*. São utilizadas para substituir ou expandir redes cabladas.

Figura 4 - Exemplo de redes WLAN

Este tipo de redes oferecem distintas funcionalidades que permitem melhorar o dia-a-dia dos seus utilizadores, pois são bastante flexíveis para além de poderem ser configuradas em múltiplas topologias – dependendo claro está do contexto em que as mesmas são aplicadas.

[4] http://www.sensor-networks.org/index.php?page=0823123150

São uma excelente alternativa para aqueles casos em que as redes LAN são difíceis ou mesmo impossíveis de implementar – como é o caso prático da implementação deste tipo de topologia, com fantásticos resultados, na freguesia da Memória (parte da implementação encontra-se representada na Figura 4 – Exemplo de redes WLAN).

Tecnicamente são designadas por IEEE 802.11[5] [Fuentes et all, 2011].

2.3.3 WMAN - Redes Metropolitanas

O termo *Wireless Metropolitan Area Networks* (WMAN) foi definido pelo IEEE na norma 802.16[6]. Semelhante ao WLAN (802.11), contudo com melhor desempenho, foi a base para a criação da tecnologia WiMAX. O WiMAX opera no intervalo de frequências entre os 2 GHz e os 11 GHz, com um alcance máximo de 50 km para velocidades máximas de 70 Mbps. Suporta voz e vídeo, para além de ter qualidade de serviço já incorporado.

As redes WMAN são comummente utilizadas como uma alternativa wireless para ligações de Internet de banda larga e serviços integrados: vídeo, voz e dados (DSL, fibra ótica, entre muitos outros).

2.3.4 WRAN

O padrão IEEE 802.22[7], mais conhecido por *Wireless Regional Area Network* (WRAN), utiliza as frequências que não são utilizadas no espectro reservado às transmissões televisivas. A utilização dessas frequências permitem levar o acesso de banda larga até às zonas com fraca densidade populacional, tipicamente ambientes rurais, tendo por isso um enorme potencial de aplicabilidade [Salvador, 2008].

2.4 Síntese

Neste capítulo foram identificados e definidos os mais importantes termos e tecnologias utilizadas na área das redes sem-fios. Resumiram-se algumas das variantes da norma IEEE 802.11 facultando assim uma melhor perceção do método de funcionamento das mesmas.

[5] http://ieee802.org/11/
[6] http://grouper.ieee.org/groups/802/16
[7] http://www.ieee802.org/22

Também foram descritos a noção de canal e frequência, dois termos absolutamente fulcrais quando debatemos qualquer tema na área das redes *wireless*. Identificou-se por que razão a utilização de dois canais muito próximos pode ser prejudicial ao bom funcionamento de uma rede sem fios.

Finaliza-se este capítulo com a identificação e principais características existentes nas arquiteturas de redes sem-fios mais conhecidas, para além de associar a cada uma delas a norma padrão IEEE 802.1x utilizada.

Capítulo 3

3 Quality of Service (QoS)

O acrónimo QoS – *Quality of Service* – refere-se à capacidade de prestar um melhor serviço no tráfego de rede sobre várias tecnologias subjacentes, tais como: Frame Relay, Aysnchronous Transfer Mode (ATM), redes Ethernet e 802.1, *Synchronous Optical Networking* (SONET) entre outras. O QoS é um conjunto de tecnologias que permitem às aplicações solicitar e receber os níveis de serviço previstos em termos de capacidade de processamento de dados (largura de banda), variações de latência (*jitter*) e atrasos.

Através de uma correta configuração de QoS numa rede podemos obter os seguintes benefícios:

- Controlo sobre os recursos: onde temos o controlo sobre os recursos que estão a ser utilizados (largura de banda, equipamentos, entre muitos outros). Como exemplo, podemos limitar, ou mesmo impossibilitar, a utilização de largura de

banda para programas que utilizem o protocolo *Peer-to-Peer* (P2P) ou aumentar o nível de prioridade para serviços críticos;

- Maior grau de eficiência nos recursos utilizados na rede: recorrendo a equipamentos ou *software* para proceder à gestão e monitorização de toda a infraestrutura, podemos saber com que intuito a nossa rede está a ser utilizada;

- Personalização de serviços: o nível de controlo e visibilidade fornecidos pela utilização de mecanismos de QoS permitem que a entidade que esteja a fornecer um serviço de acesso à Internet possa facultar aos clientes distintos graus de serviços diferenciados;

- Coexistência de aplicações críticas: os mecanismos de QoS permitem que uma rede possa ser utilizada, de forma o mais eficiente possível, garantido que as aplicações mais críticas - com maior nível de importância para um negócio ou interesse aos consumidores finais - tenham a largura de banda necessária e com o menor atraso possível. De salientar que as restantes aplicações não passam a estar inacessíveis, mas sim a utilizar a menor largura de banda possível de forma a não interromper o bom funcionamento das que são mais relevantes (recorrendo para isso a determinadas regras ou métricas que permitem um nível de equidade o mais justo possível);

- Rede estruturada para o futuro: a implementação dos corretos mecanismos de QoS numa rede informática é essencial para que a mesma esteja precavida para um futuro próximo, permitindo assim, a integração dos mais variados e distintos tipos de serviços que existem e aparecem diariamente no universo tecnológico;

- A utilização de qualidade de serviço permite fornecer maior garantia e segurança nas aplicações para a Internet, uma vez que o tráfego de aplicações mais críticas (voz sobre IP, videoconferência) passam a ter maior prioridade, enquanto os utilizadores de aplicações mais comuns continuam a utilizar um método de *best-effort* (melhor esforço).

Actualmente existem dois mecanismos para implementar QoS na Internet: serviços integrados (IntServ) e serviços diferenciados (DiffServ). O IntServ é um modelo baseado em reserva de recursos, enquanto os serviços diferenciados são uma proposta onde os pacotes são marcados consoante classes pré-definidas.

Nos tópicos seguintes será apresentada uma ideia geral do conceito, os mecanismos e os modelos de QoS existentes [Pereira, 2006].

3.1 Tipos de aplicações de rede

Existem dois tipos de aplicações distintas, as aplicações multimédia e as aplicações elásticas [Meddeb, 2010].

As aplicações multimédia são, tradicionalmente, muito sensíveis ao atraso ponto-a-ponto e à variação desse mesmo atraso, para além disso toleram uma perda ocasional de pacotes.

As aplicações multimédia são, tradicionalmente, muito sensíveis ao atraso ponto-a-ponto e à variação desse mesmo atraso, para além disso toleram uma perda ocasional de pacotes.

As aplicações elásticas podem aceitar grandes atrasos, apesar de indesejáveis, sem que haja um impedimento no sucesso das comunicações. Neste tipo de aplicações (Web, e-mail, FTP, telnet, entre outras) a integridade da informação é fundamental, visto que caso existam perdas tem de se garantir o reenvio da informação.

3.1.1 Componentes que influenciam as comunicações multimédia

As comunicações multimédia são influenciadas por diversos componentes:

- Um desses componentes, os *buffers*, permitem armazenar, temporariamente, os pacotes que circulam pela rede. Têm uma capacidade máxima que caso seja excedida, origina perda de pacotes;
- Outro componente, a distância, refere-se à distância que tem que ser percorrida pelos pacotes entre dois pontos (emissor -> recetor). Quanto maior a distância, maior o tempo necessário para que o pacote chegue ao seu destino;
- O processamento é utilizado de forma a processar os dados na origem e apresentar a informação no destino. Existe processamento nos equipamentos de rede (routers, *switchs*, *firewalls proxies*, entre outros dispositivos) de forma a processar os pacotes;

- As perdas ocorrem quando os dados enviados não chegam ao destino. Caso existam muitas perdas, torna-se impossível reproduzir qualquer tipo de informação;
- O atraso depende da distância entre a origem e o destino, do tempo que os pacotes perdem nos *buffers*, do tempo que os equipamentos necessitam para processar os pacotes e do tempo que os equipamentos terminais precisam de forma a apresentar a informação;
- O *jitter* é a variação do atraso, ou seja, os pacotes quando são enviados do terminal origem, partem com um determinado espaço entre cada pacote apesar de chegarem ao terminal destino com um espaçamento diferente;
- Os *bottlenecks* são pontos de congestionamento que ocorrem ao longo do *link* que interliga o emissor e o recetor. Esse congestionamento pode ocorrer na rede de acesso, no *backbone*, na rede terminal ou nos servidores, apesar de o *bottleneck* se deslocar para o *backbone* à medida que a capacidade da rede de acesso aumenta;
- O *throughput* define a taxa de transmissão entre o terminal origem e o terminal de destino. É sempre inferior à velocidade permitida pelas interfaces de rede, para além de algumas aplicações gerarem uma taxa constante de bits (CBR), enquanto outras geram taxas variáveis (VBR) [Meddeb, 2010].

3.2 Mecanismos de QoS

Os principais mecanismos utilizados pelo QoS são:

- Classificação: permite organizar o tráfego, ou seja, os pacotes que circulam pela rede em diferentes categorias;
- Marcação: permite definir ou modificar os atributos pertencentes a uma determinada classe. Comummente utilizado em conjugação com o mecanismo de classificação;
- Gestão de Congestão: permite controlar o congestionamento determinando a ordem pela qual os pacotes são enviados, baseando-se nas prioridades atribuídas a esses pacotes. Implica a criação de filas que são realizadas segundo a classificação década pacote, e o agendamento de cada um numa fila de transmissão;

- Controlo de Congestão: permite realizar a monitorização do tráfego de rede com o principal intuito de evitar o congestionamento através do descarte de pacotes;
- *Policing* e *Shaping*: estes dois mecanismos são utilizados para limitar o débito que circula na rede. Quando esse limite é atingido, o tráfego em excesso é: descartado, marcado ou atrasado. O *policing* realiza o descarte ou marcação de pacotes, enquanto o mecanismo de *shaping* faz um *queuing* aos pacotes quando estes atingem um limite pré-definido;
- Sinalização: desempenha um papel fundamental na configuração global *end-to-end* de serviços de QoS na rede. É uma forma de comunicação que permite que um nó de rede possa comunicar, ou sinalizar, com os nós vizinhos de forma a solicitar o tratamento de um determinado tipo de tráfego;
- Eficiência da ligação: foi estruturado para reduzir a latência e o jitter que ocorrem no tráfego de rede. Funciona através de vários mecanismos que realizam: queuing, compressão e fragmentação, de modo a melhorar a eficiência e a previsibilidade dos níveis dos serviços da camada de aplicação [Meddeb, 2010].

3.3 Modelos para Qualidade de Serviço

Nos subtópicos seguintes descrevem-se as diferenças dos três principais modelos de qualidade de serviço.

3.3.1 Best-Effort

Este tipo de modelo não oferece qualquer garantia quanto à entrega de dados ao utilizador final. Pode-se fazer uma analogia com os correios em que apesar de ser depositada a carta na caixa do correio, nada nos garante que a mesma chegue ao seu destino. O carteiro fará o maior esforço (*best-effort*) para entregar essa mensagem, apesar do remetente nunca saber se a mesma chegou ao seu destino [ESTG, 2009].

3.3.2 Serviços integrados (*IntServ*)

O modelo de qualidade de serviços integrados caracteriza-se pela sua reserva de recursos. Antes de estabelecer uma comunicação, o emissor requisita ao destinatário a alocação de recursos necessários de forma a obter a melhor qualidade na transmissão de

dados. Essa alocação de recursos é realizada através do protocolo *Resource Reservation Protocol* (RSVP) que troca mensagens de controlo. A troca dessas mensagens permite reservar os recursos necessários, sendo eles: a largura de banda e o tempo que a ligação será mantida.

O *IntServ* caracteriza-se pela alocação de recursos para dois novos tipos de serviços: o serviço garantido para aplicações que precisam de atraso, e serviços de carga controlada para aplicações que necessitam de segurança e que têm como principal destaque o serviço *best-effort*.

Pegando na analogia do tópico anterior, podemos comparar o serviço *IntServ* a um jacto privado, em que o cliente sabe que parte de um determinado local, a uma determinada hora, e chega ao destino sem qualquer atraso, visto ter a garantia do serviço [ESTG, 2009].

3.3.3 Serviços diferenciados (*DiffServ*)

O modelo de qualidade de serviços diferenciados funciona na base de definição de serviços. Para tal, utiliza um campo existente no cabeçalho IP, o *Type of Service* (TOS), que representa o tipo de serviço associado a um pacote IP. Apesar de o campo TOS já estar definido no pacote IP, só passou a ser utilizado quando começaram a ser criadas classes, de forma a diferenciar os pacotes que circulam pela rede. Esse novo *layout* do TOS designa-se por DS Field (*Differentiated Service Field*).

Com a introdução do modelo de serviços diferenciados, apareceram dois novos tipos de serviços: os serviços *premium* e os serviços assegurados. Os serviços *premium* foram criados pensando em aplicações que precisam de uma baixo *jitter* e um baixo atraso, enquanto os serviços assegurados são utilizados para garantir que os clientes tenham acesso aos serviços mínimos mesmo que haja congestionamento na rede.

O *DiffServ* tem sido o modelo mais utilizado na implementação do QoS, pois é o que exige menos a nível de processamento por parte dos *routers* [ESTG, 2009].

3.3.4 Resumo dos diferentes modelos de QoS

A tabela seguinte (**Erro! A origem da referência não foi encontrada.**) resume as principais diferenças existentes entre os três modelos de qualidade de serviço descritos anteriormente.

	IntServ	DiffServ	Best-Effort
Filtragem do Qos	Por fluxo	Por classe	Tratamento igual e justo para todos
Serviços	Guaranteed (quantitativo) Controlled Load (qualitativo)	Expedited forwarding e Assured Forwarding	"Best-Effort"
Alocação de recursos	Dinâmica	Estática ou Dinâmica	Nenhuma
Sinalização	RSVP (host/router)	RSVP (host) Nenhuma no router de core	Nenhuma
Classificação	Multi-campo no host/router	Multi-campo na edge e DiffServ no core	Nenhuma
Controlo	No host/router	Marcação na edge e fila de espera no core	Apenas FIFO
Complexidade	Alta	Média	Baixa

Tabela 2 - Diferenças entre os modelos de QoS

3.4 Síntese

Neste capítulo foi analisada a importância da realização de qualidade de serviço nas telecomunicações. Realizou-se a distinção entre os dois principais tipos de aplicações existentes para além de descrever que componentes as influenciam.

Finaliza-se este capítulo com a explicação dos principais mecanismos utilizados em qualidade de serviço, seguido da descrição dos três principais modelos utilizados: *best-effort*, *IntServ* e *DiffServ*.

Capítulo 4

4 Segurança

Este termo é recorrentemente utilizado nas mais diversas áreas. Tal como em todas elas também no âmbito da computação o mesmo é utilizado e é um ponto essencial no bom funcionamento de um sistema informático, ou para este caso de estudo, numa infraestrutura de rede.

A inexistência de mecanismos de segurança ou a incorreta implementação dos mesmos pode prejudicar, de uma forma muitas vezes gravosa, os utilizadores finais. Nos tópicos seguintes estão descritos alguns pontos essenciais quanto a esta matéria – mais orientados, claro está, para área das redes informáticas. A finalizar o capítulo explica-se de que forma os mecanismos de DPI podem ser úteis na proteção/prevenção, de ataques informáticos.

4.1 Segurança numa rede informática

Respondendo à questão mais genérica: "Para quê a segurança numa rede informática?", o responsável, ou responsáveis, por toda a infraestrutura de rede deverão reconhecer que esta questão se refere a todas e quaisquer questões com o âmbito de proteger a mesma. Mais especificamente pensando sempre nos tópicos seguintes:

- Usabilidade;
- Confiabilidade;
- Integridade;
- Segurança de toda a rede e respetivos dados que por lá circulam.

Um plano eficaz de segurança permite identificar as mais diversas ameaças, evitando assim, que as mesmas se propaguem pela nossa infraestrutura de rede.

Os administradores deverão ter sempre em conta os perigos envolventes (Figura 5). Para isso, será uma boa ideia categorizar os possíveis agentes invasores:

- *Virus*, *worms* e *trojans*; Spyware e adware;
- Ataques de *Denial of Service* (DoS);
- Roubo/interceção de dados que circulam na rede;
- Roubo de identidade.

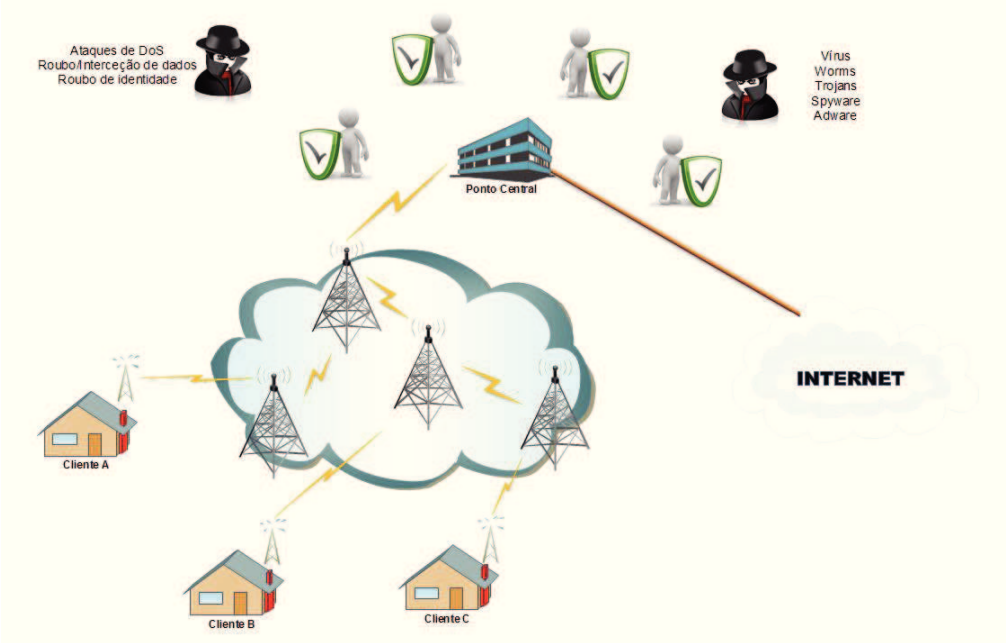


Figura 5 - Camadas de segurança

O plano delineado nunca se deve focar numa só solução de proteção, pois as ameaças podem surgir de todos os lados. Assim sendo, devemos delinear todo o nosso plano, seguindo a "ideologia da cebola", ou seja, implementar o máximo de camadas de segurança possível para que, caso uma delas falhe, o agente invasor tenha pela frente o máximo número de barreiras possível.

A segurança de uma rede passa pela instalação e configuração do binómio *hardware*/*software*. O *software* utilizado deve ser constantemente atualizado e monitorizado - de salientar que os administradores de uma rede deverão testar sempre qualquer nova atualização, recorrendo para tal a um ambiente de testes o mais aproximado possível da solução real, de forma a estudar o impacto que essas modificações podem ter no bom funcionamento da infraestrutura. Um bom nível de segurança passa, normalmente, pela utilização de um vasto número de componentes - que funcionam, comummente, em conjunto. Esses componentes podem ser:

- *Firewalls* - permitem bloquear os acessos não autorizados à rede;
- Anti-virus e anti-spyware;
- *Virtual Private Networks* (VPNs) - permitem realizar acessos remotos de forma segura.

4.2 Ameaças

A grande maioria das redes internas a nível global é de pequena dimensão (não têm mais do que 10 dispositivos com um endereço associado), pois atualmente a grande maioria dos habitantes dispõem de uma rede pessoal em suas casas. Normalmente, os atacantes focam o seu tempo e conhecimento não tanto a este tipo de redes mais pequenas, mas sim para redes com maior dimensão de forma a obterem proveitos financeiros (através do roubo informação ou chantagem) ou para terem algum reconhecimento a nível mundial (atacando empresas ou instituições de renome).

Essas ameaças ocorrem na maioria das vezes de problemas identificados há muito tempo na área das tecnologias da informação como é o caso dos perigos que podem advir dos endereços públicos. Apesar da implementação do NAT (*Network Address Translation*) ter resolvido em grande parte esta situação, assim que o atacante tem acesso à rede interna, o mesmo sabe que recorrentemente a mesma se encontra dividida por departamentos (ex.: contabilidade, marketing) ou regiões (pegando o exemplo das redes Wireless de Âmbito Alargado onde normalmente se atribui uma gama de endereços por localidade) para além de saber que grande parte dos administradores de redes/sistemas têm o mau vício de utilizar os primeiros e últimos endereços associados ao *gateway* e servidores. Felizmente uma das funcionalidades que o IPv6 utiliza, a autoconfiguração de endereços, pode ajudar a colmatar este género de ameaças, mas infelizmente a maioria das empresas ainda se encontra reticente em implementar estes sistemas, quer pelos custos associados da aquisição de novos equipamentos, quer pela falta de formação dos seus técnicos quanto a esta matéria.

A utilização de servidores, ou máquinas virtuais, para cada tipo de serviços numa infraestrutura de rede, apesar de facilitar a vida de todos, pode-se tornar num enorme problema. Por exemplo, se um atacante obtém acesso a um servidor Samba onde se encontram guardadas todas as informações quanto às senhas de acesso a sistemas, *emails*, dados pessoais, entre outros, pode fazer com o intuito original do ataque se torne numa situação realmente dramática quer para entidade atacada, quer para os que dela usufruam [SANS, 2001].

Finalizando, gostaria de deixar os principais tópicos que constituem grandes desafios ao nível de segurança nos próximos tempos:

- Espionagem e sabotagem de equipamentos por entidades governamentais - como forma de controlar o que o cidadão comum faz ou mesmo restringirem a liberdade de expressão destes;
- Ataques de DDoS em escalas cada vez maiores;
- Perda de confiança na *Cloud* - visto os ataques serem cada vez mais direcionados ao serviços aí existentes;
- O eterno problema das senhas - tendo uma repercussão cada vez maior principalmente pelos últimos ataques efetuados a gigantes tecnológicos como a Sony, LinkedIn, Yahoo, entre muito outros;

A ameaça interna - o eterno problema de segurança que advém da falta de formação ou instinto de vingança de alguns utilizadores de redes informáticas.

4.3 Síntese

Este capítulo pretende apenas reforçar a importância da mesma no mundo das comunicações para além de demonstrar que este tópico foi seriamente tido em conta ao longo de todo o processo de elaboração desta dissertação. A utilização de mecanismos de *Deep Packet Inspection* em redes sem fios de âmbito alargado podem ser úteis para descobrir algumas das vulnerabilidades em termos de segurança que possam existir neste género de infraestruturas. Através da análise do *payload* de cada pacote que circula na rede é possível identificar o tipo de ameaça que se pode encontrar a circular na rede (*vírus*, *spyware*, entre outros). Para além disso, os mecanismos de DPI podem facilmente ajudar os administradores de sistemas a identificarem a proveniência de ataques do género DoS através do rastreamento dos endereços de origem.

Capítulo 5

5 *Firewalls* de nova geração

O rápido e contínuo crescimento da Internet faz com que as tradicionais *firewalls* sejam cada vez menos eficazes em termos de protecção de redes informáticas, especialmente em infraestruturas empresariais em que a segurança se torna um dos pontos críticos pelos direitos intelectuais envolvidos.

A rápida evolução das aplicações, das quais resultam sempre novas ameaças, juntamente com uma relativa estagnação das tecnologias de segurança mais tradicionais, resultaram numa perda de visibilidade e de controlo para as organizações de tecnologias de informação que tentam manter as suas empresas os mais seguras possível.

Apesar do contínuo esforço para restaurar a visibilidade e o controlo das aplicações de forma a recuperar a vantagem em proteger as suas redes e o seu activo mais importante, a informação, a maioria das organizações permanecem frustradas. Na falta de uma solução que seja realmente inovadora, as mesmas focam-se em *appliances* de segurança

especializadas que infelizmente não conseguem resolver completamente os desafios com que nos deparamos hoje em dia no campo da segurança. Devido ao clima económico em que nos encontramos, as organizações devem fazer mais com menos - tanto em termos financeiros como ao nível de equipas especializadas nas área das tecnologias de informação. Correcções de carácter muito complexo e dispendioso são muitas vezes inaceitáveis.
Ao invés disso, é necessária uma abordagem realmente nova e inovadora no ramo da segurança de redes informáticas - é hora de reinventar a *firewall*!

5.1 Cenários de aplicação e ameaça

As designadas aplicações empresariais 2.0 estão a ser cada vez mais utilizadas pelos mais variados tipos de utilizadores. A facilidade com que as mesmas podem ser acedidas, combinado com o fato com que os utilizadores com mais conhecimentos estão acostumados a utilizá-las, aponta para uma contínua tendência na sua utilização. Aquilo que começou por ser uma mão cheia de aplicações que eram essencialmente focadas em pesquisa, *linking* e *tagging*, rapidamente se transformou numa massificação de aplicações que permitem criar, *networking* e partilha.

Exemplos de aplicações de primeira geração empresarial:

- Wikis (ex.: Socialtext[8]);
- Blogging (ex.: Blogger[9]);
- Ferramentas de RSS *feeds* (ex.: NewsGator[10]);
- Ferramentas de mensagens instantâneas (ex.: AIM[11] – AOL Instant Messenger).

Exemplos de aplicações de segunda geração empresarial:

- Ferramentas de gestão de conteúdos (ex.: SharePoint[12]);

[8] http://www.socialtext.com/
[9] http://www.blogger.com
[10] http://www.newsgator.com/
[11] http://www.aim.com/
[12] http://office.microsoft.com/en-us/microsoft-sharepoint-collaboration-software-FX103479517.aspx

- Ferramentas de partilha de ficheiros (ex.: MegaUpload.com);

- Redes sociais complexas (ex.: Facebook[13] e Twitter[14]);

- Ferramentas de divulgação/publicação de conteúdos (ex.: Youtube[15]);

- Ferramentas avançadas que unificam diversos canais de comunicação (ex.: Skype[16]).

O grande desafio não vem só do exponencial crescimento e diversidade de aplicações, mas de como as devemos classificar: "boas" ou "más"? Apesar de muitas delas poderem ser consideradas facilmente de "boas" (bem comportadas) pelo seu reduzido risco e grande proveito de utilização, existem outras que podem ser claramente classificadas como más – elevado risco e que não trazem qualquer tipo de proveito. Mas e aquelas, que são muitas (e cada vez mais), que se situam *in media rés*[17]?

Apesar de parecer fácil realizar a distinção de uma aplicação da outra, em termos práticos, isto realmente não acontece por uma variedade de razões. De forma a maximizar a sua acessibilidade e utilização, muitas aplicações são projetadas desde o início da sua conceção para contornar as designadas *firewalls* tradicionais, permitindo assim, ajustar dinamicamente a forma como as mesmas comunicam. Isto torna-se um pesadelo para os administradores de sistemas, mas os utilizadores finais agradecem visto significar que podem utilizar a aplicação em qualquer lugar, a qualquer hora. As táticas mais comuns implementadas pelos desenvolvedores de novas aplicações, de modo a contornarem os mecanismos de proteção das *firewalls*, incluem:

- *Port hopping*: técnica que permite que os portos ou protocolos utilizados na aplicação mudem de forma aleatória ao longo de uma sessão;
- Utilização de portos não-padrão: como executar a aplicação AOL Instant Messenger sobre o protocolo TCP no porto 80 (HTTP) em vez de utilizar o mesmo recorrendo ao *standard* - TCP no porto reservado ao AOL Instant Messenger (5190[18]);

[13] https://www.facebook.com/
[14] https://twitter.com/
[15] http://www.youtube.com/
[16] http://www.skype.com/en/
[17] http://www.infopedia.pt/$in-medias-res
[18] http://kb.netgear.com/app/answers/detail/a_id/1166/~/port-numbers-for-port-forwarding

- Utilização de túneis dentro de serviços comumente utilizados: por exemplo, utilizar o cliente uTorrent[19] para realizar transferência de ficheiros por P2P (*peer-to-peer*) executando o mesmo através de HTTP (porto 80);
- Escondendo-se recorrendo a criptografia SSL: permite mascarar o tráfego de aplicações, por exemplo, recorrendo ao porto TCP 443 (HTTPS).

Como podemos ler no interessante artigo lançado pela Palo Alto Networks - "The Application Usage and Risk Report – An Analysis of End User Application Trends in the Enterprise" - esta enorme e conceituada empresa da indústria de Segurança em Redes descobriu através de um estudo que das 741 aplicações analisadas, 65 porcento foram criadas utilizando as táticas descritas nos quatro pontos anteriores [Palo Alto, 2010].

Outro assunto muito interessante, e que foi enfatizado no mesmo artigo, foi o fato de muitas aplicações não serem o que realmente parecem ser. As aplicações mais comummente encontradas que realizam *port hopping* são uma combinação de aplicações empresariais e de uso pessoal.

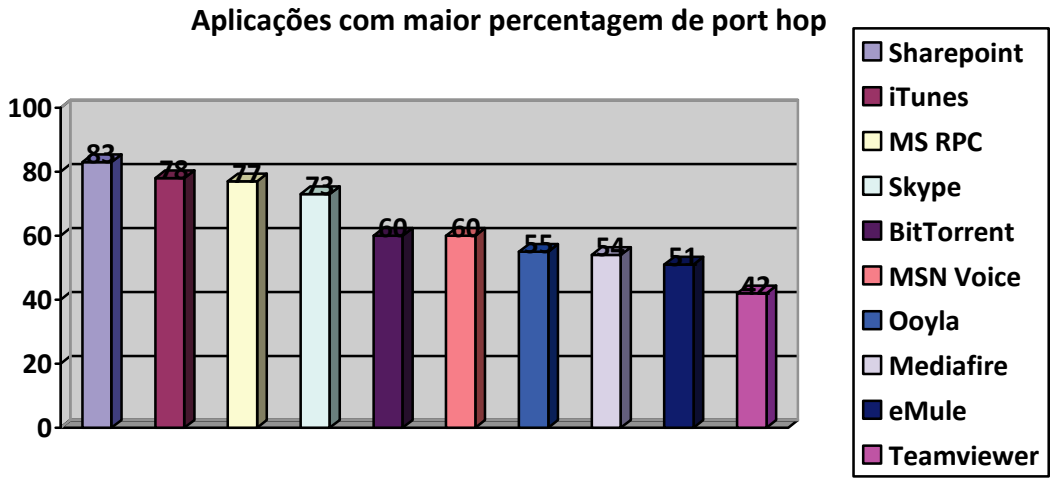


Figura 6 – Aplicações com maior percentagem de *port hop* [Palo Alto, 2010]

Estima-se que o tráfego HTTP e HTTPS que circula numa rede empresarial rondem os 66 porcento. Isto não é um problema, mas pode transformar-se num ponto crítico do ponto de vista da segurança tradicional de uma infraestrutura. A gigantesca variedade de aplicações que funcionam sobre HTTP e HTTPS são praticamente indistinguíveis em equipamentos de segurança de rede mais antigos. O impacto negativo das organizações

[19] http://www.utorrent.com/

perderem ainda mais o controlo sobre as suas comunicações só revela o facto que o paradigma de planeamento e implementação de aplicações tem evoluído de uma forma dramática [Palo Alto, 2010].

5.2 *Firewalls*?

Hoje em dia já não se fala tanto, nem se demonstra o mesmo interesse que se verificava há uns anos, quando se falava de *firewalls*. Estas eram o elemento mais importante de uma infraestrutura de rede. Afinal, o que é que aconteceu?

A resposta, que já não é novidade para ninguém e que é frequentemente ouvida no mundo tecnológico, é que a Internet veio mudar tudo! No passado milénio, as *firewalls* efetuavam de fato um trabalho muito satisfatório quanto ao controlo de tráfego que circulava numa rede. Isto acontecia pois as aplicações eram tipicamente "bem comportadas". Os pacotes associados ao *email* fluíam, tipicamente, pelo porto 25 (SMTP), os de FTP no porto 20 e tudo o que fosse associado a uma "normal" navegação pela *Web* circulava no porto 80. Tudo seguia um determinado conjunto de regras que se pode resumir pela seguinte fórmula: "portos + protocolos = aplicações". Essas normas padrão permitiam que as *firewalls* tivessem tudo sobre controlo - bloquear um porto significava pura e simplesmente bloquear a aplicação associado ao mesmo.

Atualmente, uma grande percentagem do tráfego circula pela rede recorrendo a SSL no porto 443 (HTTPS). Pior ainda, é que existem cada vez mais aplicações que definem as suas próprias regras, ou seja, utilizam outros protocolos, circulam por portos que não lhes pertencem e escondem-se recorrendo a túneis SSL. Resumindo, estas não jogam um jogo limpo - são "mal comportadas".

Isto acarreta uma grande probabilidade de risco e um novo conjunto de vulnerabilidades numa rede, visto estas aplicações conseguirem furar uma *firewall* sem serem detetadas. Este "suposto" fiável equipamento de segurança funciona normalmente, como se nada de errado estivesse a acontecer, simplesmente porque se continua a reger por regras que já não existem.

5.3 *Firewalls* de nova geração

De forma a restaurar a *firewall* como sendo a pedra angular a nível de segurança de uma rede, as designadas *firewalls* de nova geração vieram tentar resolver o problema descrito no tópico anterior. Partindo do zero, e limpando de certa forma a antiga ideologia, uma *firewall* de nova geração começa por classificar o tráfego logo no topo da pilha protocolar, ou seja, logo na raiz do problema, na camada de aplicação.

Os requisitos funcionais necessários para um bom funcionamento deste novo género de equipamentos incluem a capacidade de:

- Identificar as aplicações independentemente do porto, protocolo, técnicas evasivas, ou cifragem SSL antes que seja feita qualquer coisa;
- Proporcionar uma visibilidade e controlo granular baseado em políticas sobre as aplicações, incluindo regras de forma individual;
- Identificar, com a maior precisão possível, os utilizadores e utilizar posteriormente essa informação como um atributo para políticas de controlo;
- Fornecer proteção em tempo-real contra uma vasta gama de ameaças, incluindo aquelas que operam na camada de aplicação;
- Integrar, e não apenas combinar, a ideologia de *firewall* tradicional para além de ter a capacidade prevenir qualquer intrusão de rede.

[20]

Figura 7 – Requisitos para *firewalls* de nova geração

O segredo para a implementação de *firewalls* de nova geração, tal como a Figura 7 – Requisitos para firewall de nova geração representa, é a capacidade de fazer tudo o que uma tradicional firewall faz com capacidade avançadas que combinam tecnologias inovadoras de identificação, alto desempenho para além das características fundamentais adicionais que permitem a produção de uma solução eficaz de segurança.

5.3.1 Níveis de Identificação

As *firewalls* de nova geração contemplam três níveis distintos de identificação:

- Identificação por aplicação: estabelecer o binómio "porto + protocolo" é um primeiro passo bastante importante na identificação de uma aplicação, mas, por si só, é insuficiente. Uma robusta identificação e inspeção da aplicação permite um controlo granular do fluxo de sessões. Exige uma abordagem de múltiplos fatores de forma a determinar a identidade das aplicações na rede, independentemente do porto, protocolo, cifragem ou táticas evasivas. Algumas dessas técnicas incluem:
    - Deteção de protocolos e decifrar aplicações: determina o protocolo da aplicação (por exemplo, HTTP) e, se a mesma estiver a utilizar SSL, decifra o tráfego de modo a que possa continuar a ser analisada. O

[20] Fonte: http://www.computrad.co.uk/application-aware-firewalling-service.php

tráfego é cifrado novamente assim que todas as tecnologias de identificação envolvidas tiveram a oportunidade de operar;

- Aplicação de protocolo de descodificação: determina se o protocolo utilizado na respetiva aplicação é o "real", ou se ele está a ser utilizado em modo túnel de forma a esconder a real aplicação (por exemplo, podemos utilizar o cliente uTorrent P2P de forma a operar sobre HTTP);

- Assinaturas de aplicação: forma de observar propriedades e características únicas de forma a identificar corretamente a aplicação em questão, independente do porto e protocolo utilizado. Isso inclui a capacidade de detetar funções muito específicas dentro das aplicações (por exemplo, transferências de arquivos embutidos em sessões de mensagens instantâneas);

- Heurística: para o tipo de tráfego que ilude a identificação por análise de assinaturas, análises heurísticas são aplicadas permitindo a identificação de aplicações problemáticas - como são o caso do P2P ou de ferramentas de VoIP que utilizam recorrentemente formas de cifragem proprietária.

- Identificação por utilizador: recorrendo à tecnologia de identificação por utilizador, podemos realizar o mapeamento de endereços IP por utilizador, permitindo assim uma visibilidade e controlo da atividade dos mesmos na rede. Estes dados tornam-se assim disponíveis para:

  - Identificar especificamente quem é responsável pela aplicação, conteúdo e ameaças que possam perturbar o bom funcionamento da rede;

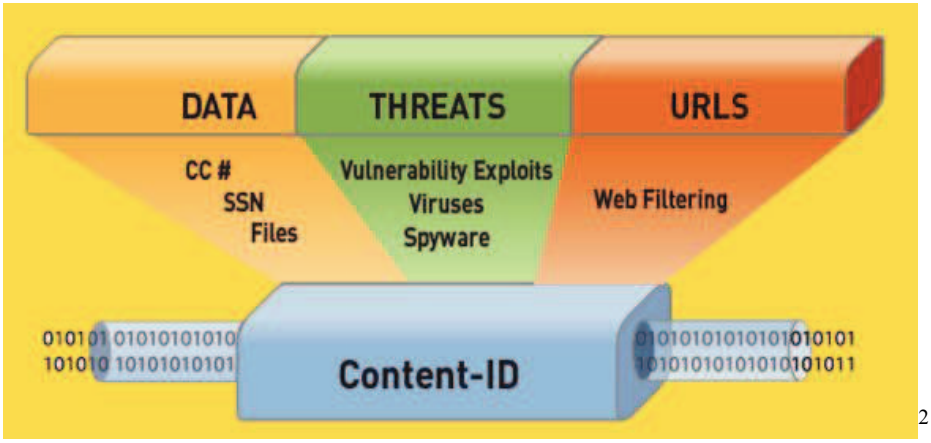
  - Permitir a utilização da identidade como uma variável a ser incluída nas políticas de controlo de acesso;

  - Facilitar o *troubleshooting* e resposta a incidentes e realização de relatórios.

  Recorrendo à identificação por utilizador, os departamentos de informática ganham um poderoso aliado com a principal funcionalidade de auxiliar no controlo das aplicações de uma forma bastante inteligente. Por exemplo, podem permitir uma aplicação de redes sociais para apenas um conjunto de pessoas que

necessitam da mesma para uma utilização legítima (por exemplo, permitir a utilização da mesma ao departamento de recursos humanos de uma organização).

- Identificação por conteúdo: permite à nova geração de *firewalls* capacidades totalmente inéditas, tais como a prevenção em tempo real de ameaças que circulam em tráfego supostamente confiável, controlar hábitos de navegação na *Web* para além da filtragem de dados e/ou ficheiros [Keil, 2009].



[21]

Figura 8 – Filtragem por conteúdo [Keil, 2009]

5.4 Critérios essenciais

Nos pontos seguintes, e como se encontra representado na figura 9, são descritos alguns dos critérios fundamentais que são usualmente associados às *firewalls* de nova geração [Pathan, 2013].

[21] Fonte: http://www.networkworld.com/community/node/45409

Figura 9 – Critérios essenciais associados a uma *firewall* de nova geração

5.4.1 Identificar aplicações, não portos

Esta nova geração de equipamentos de segurança deve conseguir identificar uma aplicação assim que estes a "vejam", independentemente do porto que estejam a utilizar, protocolo, cifragem SSL, ou qualquer outro género de técnica evasiva de modo a providenciar o máximo controlo a nível de políticas de segurança definidas.

Também é bastante importante que este género de dispositivos possua uma listagem extensa a nível de assinaturas de aplicações instaladas no próprio sistema de forma a evitar quaisquer problemas de latência a nível de leitura das mesmas em locais remotos (por exemplo, baseados na *cloud*). Essa biblioteca de dados deve ser regularmente atualizada com novas assinaturas que vão aparecendo (devido ao desenvolvimento desenfreado de nova aplicações) pelo próprio fornecedor ou recorrendo a qualquer outro tipo de serviço que permita a atualização das mesmas.

5.4.2 Identificação dos utilizadores, não endereços IP

Uma total integração com serviços de diretório como: *Active Directory*, LDAP e *eDirectory*[22] permite aos administradores de sistemas identificar a atividade da rede a

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

um conjunto de utilizadores/grupos, e não apenas a endereços IP. Quando associado a tecnologias de identificação de aplicações e conteúdo, o departamento de IT pode usufruir desses dados para criar políticas de segurança, investigar e criar relatórios sobra determinada aplicação, identificar ameaças e hábitos de navegação na Web para além de conseguir saber a atividade de transferência de dados.

A identificação por utilizador permite ajudar a combater o grande desafio de utilizar apenas e somente endereços IP como forma de monitorizar e controlar o conteúdo que circula pela infraestrutura de rede, há alguns anos essa metodologia, identificação por IP, era bem-vinda e funcionava perfeitamente, mas foi-se tornando cada vez mais traiçoeira assim que se mudou para um modelo centralizado da Internet.

Para agravar ainda mais o problema, a utilização de dispositivos móveis explodiu nos últimos anos o que permite com que os utilizadores possam aceder à rede em praticamente qualquer parte do globo. As redes sem-fios que realizam uma redistribuição de endereços IP assim que se mude de zona tornam também as coisas mais complicadas. O resultado é que infelizmente a identificação por endereço IP é um mecanismo cada vez mais ineficiente para realizar a monitorização e controlo da atividade dos utilizadores numa rede.

Atualmente ainda se recorrem a algumas técnicas eficazes de forma a proceder ao controlo recorrendo ao binómio utilizador <-> IP tais como: monitorização por *login* ou recorrendo a portais captativos.

5.4.3 Identificação de conteúdo

Com utilizadores a utilizar qualquer aplicação e a navegar na Internet com impunidade, é normal que os responsáveis pela infraestrutura lutem de forma a se precaverem de qualquer género de ameaça. Uns dos passos iniciais é o de controlar as aplicações de modo a reduzir a atividade de qualquer agente indesejado. De seguida, podem ser implementadas políticas que permitam o controlo do conteúdo.

As *firewalls* de nova geração contemplam, usualmente, os seguintes recursos em termos de identificação de conteúdo:

- Prevenção de ameaças: investigar novos meios que previnam vulnerabilidades existentes em aplicações, *spyware* e vírus para que os mesmos não penetrem de

forma danosa na rede. Um desses meios passa por recolher um conjunto de dados e inspecionar o seu conteúdo recorrendo a mecanismos de descodificação - após a devida análise os mesmos voltam a ser codificados. Esta técnica permite identificar assinaturas com um reconhecido rasto de carácter malicioso;

- Análise de vírus baseadas em *stream*: esta técnica passa por realizar a análise assim que um pacote entra na rede, em oposição ao que usualmente acontece, esperar que todo o ficheiro seja enviado, e só então proceder ao seu rastreamento;

- Proteção contra vulnerabilidades: ativa a prevenção de vulnerabilidades em aplicações recorrendo a um conjunto de sistemas IPS (*Intrusion Prevention System*) para bloquear redes conhecidas/desconhecidas, vulnerabilidade devidamente exploradas da camada de aplicação, *buffer overflows*[23], ataques de DoS (*Denial of Service*) e análise de portos que possam comprometer ou danificar informação;

- Filtragem por URL: possibilidade de criar distintas categorias de URL personalizadas de forma a criar políticas e atribuí-las a grupos ou utilizadores específicos de modo a permitir/bloquear o seu acesso a determinadas páginas *Web*;

- Filtragem de ficheiros e dados: permite aos administradores de sistemas implementar políticas que reduzam os riscos associados à transferência de arquivos não autorizados.

5.4.4 Visibilidade

As *firewalls* de nova geração são muito úteis aos administradores de sistemas pois fornecem-lhes informação de uma forma muito eficaz. A capacidade de estes conseguirem visualizar rápida, facilmente e detalhadamente uma aplicação, utilizadores e a informação que circula na rede é de um valor incalculável ao seu trabalho diário.

[23] http://en.wikipedia.org/wiki/Buffer_overflow

5.4.5 Controlo

Uma solução robusta de *firewalls* de nova-geração deve contemplar o controlo de aplicações seguindo uma metodologia granular como:

1. Permitir/negar;
2. Permitir apenas algumas funcionalidades associadas a uma determinada aplicação e aplicar *traffic shaping*;
3. Analisar;
4. Permitir a utilização a um determinado conjunto de utilizadores ou grupos;
5. Decifrar e inspecionar.

5.4.6 Performance

Esta nova geração de dispositivos de rede deve permite executar funções de segurança avançadas que são computacionalmente intensivas. Isto deve-se às análises que são efetuadas em tempo real associado a tempos com muito baixa latência. Uma *firewall* de nova geração tem de conseguir ser capaz de lidar com fluxos de tráfego de alta velocidade, *multi-gigabit*, recorrendo para tal a processadores específicos.

5.4.7 Flexibilidade

A flexibilidade numa rede permite garantir a compatibilidade com praticamente qualquer género de ambiente computacional. Permitir uma contínua implementação sem a necessidade de reformulação, ou mesmo reconfiguração, depende de uma variedade gama de recursos tais como: VLANs (802.1q), *port trunking*[24], funcionamento em modo transparente[25], utilização de protocolos de roteamento dinâmico (por exemplo, OSPF e BGP), suporte a IPv6, IPSec e SSL VPN.

5.4.8 Escalabilidade

A escalabilidade é um tópico essencial apesar de depender essencialmente da existência de recursos sólidos de gestão, isto inclui um dispositivo centralizado e de gestão de políticas, para além da necessidade de sincronização entre dispositivos distintos - e de

24 http://www.hp.com/rnd/device_help/help/hpwnd/webhelp/HPJ4121A/port_trunking.htm

25 http://www.draytek.co.za/content/tinymce/plugins/openfile/uploads/files/vigorpro_6.pdf

hardware de alta performance e fiabilidade. A escalabilidade também pode ser facilitada recorrendo a sistemas virtuais onde com apenas uma *firewall* física, e após uma correta configuração da mesma, esta possa agir como várias.

5.4.9 Confiabilidade

A confiabilidade ajuda a garantir um funcionamento contínuo. Implica recursos tais como:

- *Failover* ativo-passivo e/ou ativo-ativo[26];
- Sincronização da configuração e do estado do dispositivo;
- Utilização de componentes redundantes (por exemplo, fontes de alimentação duplas).

5.5 Síntese

Este capítulo descreveu a evolução das *firewalls* ao longo dos últimos anos e de que forma tiveram que recorrer a conceitos cada vez mais avançados como meio de se atualizarem e encaixarem num meio em que as vulnerabilidades crescem a um ritmo exponencial.

26 http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.ase_15.0.ha_avail/html/ha_avail/ha_avail3.htm

Capítulo 6

6 Deep Packet Inspection

Este capítulo pretende descrever o principal tema desta dissertação - o *Deep Packet Inspection* (DPI) e alguma da tecnologia que permitiu a criação desta - pela necessidade de uma cada vez maior segurança e do sempre presente instinto evolutivo presente na mente humana. Nos próximos parágrafos é explicado com algum detalhe o que é, como pode ser utilizado na segurança de infraestruturas de rede e de sistemas informáticos. Também é focado, de uma forma geral, a controvérsia existente em torno deste mecanismo de análise de pacotes que circulam numa rede para além de perceber se de facto o mesmo é, ou não, eficaz.

6.1 A era pré DPI - Firewalls

As primeiras *firewalls* eram basicamente divididas em dois tipos: baseadas em *proxies* ou pela configuração de uma tabela com um determinado conjunto de regras.

As *proxy firewalls* funcionam segundo a intervenção destas e o protocolo de uma aplicação. Dessa intervenção são aplicados controlos de segurança, quando apropriados, aos comandos e/ou dados da aplicação. Um *proxy* é essencialmente a implementação de uma referência orientada à segurança do protocolo de uma aplicação, em algumas situações, omitindo totalmente operações perigosas ou o fornecimento de controlos adicionais em determinados comandos de segurança crítica. Os *proxies* sempre foram considerados um projeto de segurança conservador pois reduzem a probabilidade de *backdoors* (tentativa de usurpar qualquer tipo de informação enquanto o atacante continua em anonimato) visto estar efetivamente a analisar as características de segurança do protocolo aplicacional ao invés de estar realmente a aplicá-las. As primeiras *firewalls* baseadas em filtragem de pacotes implementaram uma tabela de políticas de pesquisa muito simples baseadas nos seguintes parâmetros: *'{ source-ip, destination-ip, source-port, destination-port, SYN-seen yes/no } permit or deny*'. A grande vantagem na utilização da filtragem de pacotes é o de ser um mecanismo extremamente rápido, uma vez que utiliza muito pouco poder computacional. Para além disso, é relativamente fácil de implementar, uma vez que não requer praticamente experiência nenhuma na área de segurança de sistemas. Desde o início que as *proxies firewalls* foram reconhecidas por serem mais seguras, pois realizam de uma forma muito eficaz a validação sobre os protocolos aplicacionais de acesso à rede. Esta ainda continua a ser uma propriedade muito importante das *firewalls* baseadas em *proxies*.

O baixo requisito computacional requerido na filtragem por pacotes, e o facto de requerer pouca experiência em segurança, permitiu que esta metodologia fosse fácil de implementar em componentes baseados em silício, tornando-se assim umas das funcionalidades padrão em praticamente todo e qualquer equipamento utilizado para encaminhar pacotes pela rede - routers.

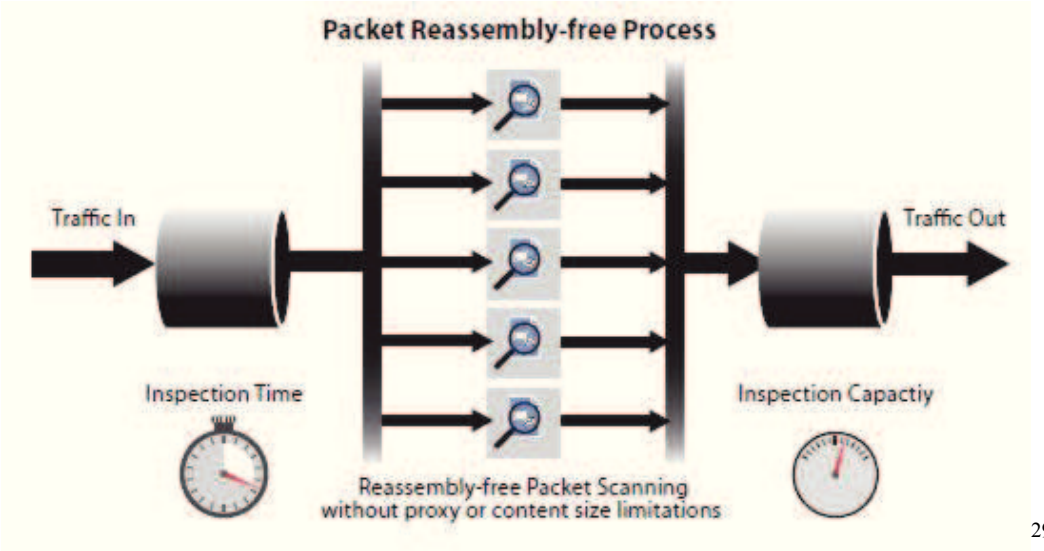
Por volta de 1993, começaram a aparecer no mercado as designadas *stateful firewalls*. Implementavam uma tabela que permitia controlar se a ligação tinha origem por detrás da *firewall* permitindo o envio de pacotes. Assim, conseguiu-se, realizando a análise dos comandos do protocolo FTP, utilizar aplicações (*layer* 7) de forma transparente através da *firewall*. Versões posteriores das *stateful firewalls* adicionaram a interpretação dos números de sequenciamento TCP e começaram a analisar também pedidos de consulta/resposta de DNS para garantir que só os pacotes de retorno eram autorizados em resposta a consultas que tinham origem do interior da rede. De salientar que este tipo

de *firewalls* introduziu estas funcionalidades para superar as vulnerabilidades aquando da sua conceção - ataques do género TCP RST *flood*[27] e DNS *cache poisoning*[28]. As *proxies firewalls* nunca sofreram deste género de vulnerabilidades. As *stateful firewalls*, como recorrentemente acontece no meio tecnológico, continuaram a evoluir, muitas das vezes em resposta aos novos tipos de técnicas de *hacking* que se iam descobrindo, e que abriam novas brechas de segurança nas infraestruturas de rede. Já as *proxies firewalls* evoluíram principalmente devido às cada vez maiores exigências em termos de desempenho e transparência [Dubrawsky, 2010].

6.2 Conceito de *Deep Packet Inspection*

O *Deep Packet Inspection* é uma forma de analisar todo o *payload* de um pacote (figura 10) que circula na rede em busca de deformidades de protocolos, *vírus*, *spam*, intrusões e aplicações de forma a decidir se o pacote pode seguir o seu caminho, ou se o mesmo, precisa de ser: encaminhado/classificado/bloqueado (caso necessite pode rever estes conceitos no subcapítulo 3.2).

Para além disso, o DPI também é recorrentemente utilizado para efeito de recolha de dados estatísticos.



[29]

Figura 10 - Análise de pacotes com DPI

[27] http://www.networkcomputing.com/unixworld/security/004/004.txt.html
[28] http://searchsecurity.techtarget.com/definition/cache-poisoning
[29] Fonte: http://www.online-edge.co.uk/images/rfdpi2.jpg

6.3 A segurança e o mecanismo DPI

Nos primórdios da Internet a segurança era um pouco colocada de parte visto a parca prevalência de utilizadores na área das IT e, em especial, da rede global designada Internet. O nível de segurança passava por basicamente bloquear os "maus" e permitir o acesso apenas aos "bons" do mundo exterior tecnológico - recorrendo a *firewalls*. Elas é que decidiam, através da utilização de um conjunto de regras relativamente fáceis de implementar, que ponto de destino (como por exemplo um determinado conjunto de servidores) é que tinha a capacidade de comunicar com o mundo exterior. Ao longo do tempo a Internet evoluiu de tal forma, que a mesma se tornou, e torna, cada vez mais complexa. As vulnerabilidades já não se podem perspetivar do mesmo modo, pois atualmente existem nas diversas camadas da rede (sendo estas assim invisíveis caso os administradores de sistemas utilizem apenas os métodos de proteção descritos no tópico anterior 6.1 - A era pré DPI - Firewalls). Resumindo, o conceito de perímetro de segurança é cada vez mais ambíguo.

O DPI permite avançadíssimas funções de segurança tal como a pesquisa completa de uma *string*[30] existente num pacote de forma a permitir que os administradores de sistemas sejam capazes de identificar/bloquear ataques de *Layer* 7 (camada de aplicação do Modelo OSI[31]) tais como: *vírus*, *worms*, *spam*, entre muitos outros, com baixíssimas taxas de falsos positivos. Realizando uma analogia genérica, podemos imaginar os administradores de sistemas como carteiros que abrem as cartas enviadas, conseguindo assim, visualizar o seu conteúdo e, caso sejam mal-intencionados, podem até modificar informação.

Muitas agências nacionais de segurança estão a utilizar o DPI para intercetar conteúdo ilegal em redes *core* IP.

[30] http://searchitchannel.techtarget.com/feature/Searching-for-multiple-strings-in-packet-payloads
[31] http://www.linktionary.com/o/osi.html

6.4 Relação com as infraestruturas de rede

O DPI está a ser utilizado por empresas, operadoras de telecomunicações e mesmo agências governamentais na área de *data mining*[32] na Internet e controlo de tráfego. Permite que façam um melhor controlo de aplicações indesejadas (P2P, *streaming* de vídeo entre outros) que consomem muita largura de banda e não geram qualquer tipo de receitas.

Permite que os administradores identifiquem os utilizadores que estão a utilizar aplicações que possam estar a ser restringidas em empresas para além de os auxiliar a identificar, de uma forma mais amigável, os pontos fracos da rede – que podem levar a *bottlenecks*[33] – permitindo assim, uma melhor gestão e planeamento da mesma.

6.5 Áreas de aplicação

O DPI pode ser utilizado em várias áreas no universo das redes:

- QoS: bloqueando aplicações que exigem muita largura de banda e/ou permitem a partilha de ficheiros muitas das vezes ilegais pois infringem as leis de direitos de autor - como é o caso do P2P. Recorrendo ao DPI os operadores de serviços de Internet podem otimizar a largura de banda disponível, atribuindo a mesma de uma forma equitativa por todos os utilizadores, minimizando assim probabilidade de congestão da rede;

- Publicidade direcionada: através da análise do tráfego que circula por toda a infraestrutura, os provedores de serviços digitais conseguem, recorrendo a avançadíssimas técnicas de *data mining*, descobrir os interesses dos seus utilizadores. Esta informação pode ser utilizada posteriormente como forma de ganhar algum dinheiro vendendo essa informação a empresas especializadas de publicidade. Isto pode ser visto como uma forma bastante interessante de cobrir os custos de infraestruturas de carácter gratuito (como o são, normalmente, as Redes Wireless de Âmbito Alargado);

32 http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm

33 http://www.techopedia.com/definition/24819/network-bottleneck

- Diferenciação de serviços: os ISPs podem recorrer a esta tecnologia para realizar a distinção dos mais diversificados serviços vendidos aos seus clientes (como exemplo, diferenciação de planos de dados ilimitados dos que têm limites mensais). Para isso, são criados distintos grupos e os clientes são adicionados num deles. Caso o utilizador final pretenda realizar uma mudança de tarifário/plano basta simplesmente modificar o grupo a que este pertence – facilitando assim o trabalho do prestador de serviços;

- Monitorização de tráfego: recorrendo aos dados estatísticos adquiridos consegue-se ter uma boa perceção dos padrões comportamentais de cada utilizador ou aplicação. Essencial aos administradores da rede de forma a realizarem uma gestão e planeamento contínuo de toda a infraestrutura de forma mais otimizada possível.

6.6 Porque há tanta controvérsia quando se fala de DPI?

O *Deep Packet Inspection* é uma tecnologia que gere um grande debate na área da Engenharia e Comunicações. Há quem afirme que pode mudar a neutralidade da rede e existem mesmo rumores que a mesma poderá estar a ser utilizada como um dos principais meios de censura na Internet. Utilizando como exemplo um dos países onde existe maior censura na Internet, na China, eles dão-se ao luxo de bloquear algumas páginas *web* e em alguns casos modificar conteúdo informativo, recorrendo ao DPI, para modificar *strings* de texto. Assim, as entidades governamentais conseguem controlar todo e qualquer tipo de informação que chegue aos utilizadores finais sem que os mesmos se apercebam das modificações. Infelizmente, isto vai contra os princípios originais da criação da Internet, em que foi desenvolvida para ser um serviço totalmente gratuito e liberal, ou seja, sem que houvesse a discriminação de pacotes [Wagner, 2009].

6.7 Síntese

Após avaliar algumas tecnologias DPI, há uma enormidade de benefícios que os administradores podem obter recorrendo a esta tecnologia. Há limitações, mas no geral, esta tecnologia funciona realmente (como se pode comprovar mais à frente aquando da

utilização desta tecnologia e da análise dos resultados em que a mesma foi utilizada num cenário de Rede Wireless de Âmbito Alargado).

O DPI veio revolucionar o mundo das redes. Até à sua chegada tudo era feito a pensar apenas na conectividade, ou seja, transportar um pacote do ponto A para o ponto B (um conceito a nível de *hardware*). Equipamentos como *switches* e *routers* são construídos com relativamente pouco *software*. O grande paradigma de mudança introduzido com o DPI foi o conceito a nível de utilização intensiva de *software* numa área focada essencialmente na utilização de *hardware*. O desafio pela implementação desta tecnologia passa por integrar a mesma num universo já existente, ou seja, sem provocar o abrandamento de troca de informação a que os utilizadores se encontram habituados, aumentando assim, com recurso a *software*, o nível de segurança e controlo de uma infraestrutura de comunicação.

Capítulo 7

7 Arquitetura

Neste capítulo é definida a arquitetura de projeto para a implementação de uma solução que permita a utilização da tecnologia Deep Packet Inspection numa rede rural sem fios ou, como se tem vindo a designar ao longo de toda esta dissertação, Rede Wireless de Âmbito Alargado.

Inicialmente é realizada uma descrição muito breve da visão geral da solução proposta, para além de contextualizar alguns dos benefícios que podem ser incrementados neste tipo de intraestrutura de rede. Também são apresentados os distintos módulos definidos e que fazem parte integrante das ideias estruturadas para a implementação de toda a solução. Finalizando este capítulo, procede-se à análise da estrutura da arquitetura.

7.1 Visão geral da solução

Apesar da elevada disseminação da Internet de banda larga ainda existem, infelizmente, muitas zonas rurais por este nosso belo país onde esta tecnologia não é acessível. Isto acontece pelas mais variadas razões. Quer seja pela acidentada localização geográfica que não permite/dificulta a implementação de soluções viáveis ou, na maior parte das vezes, pela inexistência de investimento em infraestruturas por parte dos ISPs que após uma cuidada análise, chegam à conclusão que tal investimento não lhes vai proporcionar o retorno financeiro pretendido.

Mesmo atravessando uma grave crise financeira, felizmente ainda se aplicam, e bem, fundos para o proveito das populações mais isoladas através da implementação de Redes Wireless de Âmbito Alargado. Estas são normalmente constituídas por equipamentos de rede que permitem a transmissão de dados recorrendo a ondas de rádio.

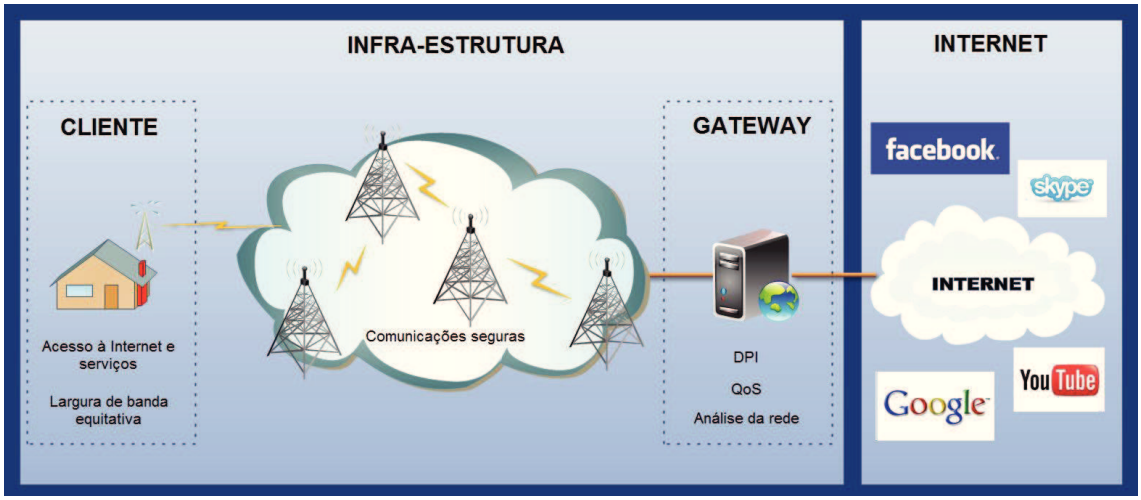


Figura 11 - Arquitetura global

A arquitetura que é mais comummente utilizada (e que representada na figura 11) é constituída pelos seguintes três agentes:

- *Gateway*: considerado o ponto central deste tipo de redes, visto ser aqui que se estabelece a ponte entre a rede interna (comunicação e serviços fornecidos para os utilizadores que usufruem deste género de infraestrutura) e a rede externa (ligação usualmente contratada a uma entidade de telecomunicações que permite que haja pelo menos uma ligação à rede global - Internet);

- Cliente: está normalmente numa das extremidades da rede. Representa todas as entidades que usufruem dos serviços fornecidos (exemplos: Internet, VoIP, videovigilância, IPTV, alojamento pessoal de dados na *cloud* interna, entre muitos outros tipos de serviços que podem ser implementados para o bem destas populações). Normalmente, os utilizadores necessitam de ter equipamentos adequados que permitam a captação do sinal de rádio difundido pelas antenas que se encontram estrategicamente colocadas ao longo de toda a infraestrutura;

- Infraestrutura: é a espinha dorsal deste género de soluções. Representa todo o esqueleto da rede de âmbito alargado onde se englobam os dois pontos anteriormente descritos.

Uma das possíveis soluções para realizar a caracterização de todo o tráfego que circula neste tipo de redes passa por implementar, no *core* da mesma, um servidor que permita realizar a monitorização de toda a infraestrutura e, através da análise desse dados, aplicar regras de QoS, recorrendo para tal a *firewalls* de nova geração com mecanismos de *Deep Packet Inspection*. Isto pode ser uma alternativa viável que permita não só otimizar toda a infraestrutura de rede, mas principalmente fornecer, de uma forma equitativa, por todos os utilizadores, os parcos recursos de largura de banda existentes.

7.2 Módulo do *Gateway*

Pode-se considerar que dos três agentes envolvidos em toda a solução, este é o mais importante, pois é aqui que se estabelece a ponte entre o que vem do mundo exterior (Internet) e o que circula na rede interna. De modo a construir uma solução eficiente e barata - não nos esqueçamos que estamos a falar de Redes Wireless de Âmbito Alargado que têm como principal intuito levar a Internet, muitas vezes de forma gratuita, onde a mesma não existe, recorrendo para tal, e na grande maioria das vezes, a orçamentos financeiros muito reduzidos, uma das ideias passa pela implementação de um agente servidor que englobe funcionalidades como: disponibilizar em *real time* o estado do mesmo, da rede, criar relatórios com dados estatísticos essenciais e úteis ao(s) administrador(es) da infraestrutura entre muitas outras funções.

Um dos maiores problemas neste género de redes é a existência de políticas de QoS estáticas. Isto é uma enorme barreira visto essas regras básicas não permitirem a distribuição da largura de banda existente de uma forma equitativa por todos os

utilizadores. Essa injustiça ocorre, pois é muito difícil caracterizar o tráfego que circula ao longo de toda a infraestrutura de rede. A maioria das ferramentas de análise existentes ainda se baseiam na ideologia que o tráfego é "bem comportado", ou seja, tudo o que seja navegação *web* apenas utiliza o porto 80, as aplicações apenas utilizam os portos padrão que lhes são comummente conhecidas e atribuídas, esquecendo assim que as mesmas são atualmente construídas a pensar nessa grande vulnerabilidade podendo assim essas "saltar" de porto em porto (5 - *Firewalls* de nova geração). De forma a evitar que isso aconteça uma alternativa a esse sistema passa por instalar neste agente um mecanismo baseado em *Deep Packet Inspection* que tenha como grande objetivo realizar uma análise minuciosa de tudo o que circula pela rede. Para garantir resultados satisfatórios, este mecanismo terá que se basear numa metodologia de análise mais moderna, baseando-se para tal nos três seguintes essenciais paradigmas que quebram os métodos de análise da "velha guarda":

- Identificar aplicações, não portos;
- Identificar conteúdo, não pacotes;
- Identificar utilizadores, não endereços IP.

Figura 12 - Módulo do *Gateway*

Após realizar essa análise, este agente servidor terá de conseguir utilizar as estatísticas e disponibilizá-las numa plataforma *web* amigável para que o administrador da rede possa ter acesso a essa informação onde quer que esteja de forma a implementar regras de QoS que se enquadrem ao que se passa realmente na rede ao invés do que acontece usualmente. Configurar um determinado conjunto de regras baseado somente ao que "normalmente acontece" resulta numa má gestão da largura de banda existente, levando

assim, a uma distribuição de recursos injusta por todos os beneficiários deste serviço de cariz comunitário.

7.3 Módulo de infraestrutura

Como já foi descrito neste documento, a velocidade contratada para Redes Wireless de Âmbito Alargado é por vezes bastante limitada. Isto acontece pois estas localizam-se, normalmente, em meios geográficos por vezes muito acidentados e em áreas rurais onde o acesso ao mundo virtual é muitas vezes inexistente. Daí a necessidade da criação deste género de projetos que permitem combater a exclusão tecnológica.

Recorrentemente, neste género de soluções, o tráfego que circula pela rede é classificado e marcado apenas pelos *routers* existentes. Isto leva a uma elevada sobrecarga por parte dos mesmos, visto terem que lidar com todo o fluxo de tráfego gerado pelas dezenas de clientes que usufruem deste serviço. Para isso, e de forma a otimizar os recursos existentes, uma das possíveis soluções passa por integrar no agente servidor (7.2 - Módulo do *Gateway*) um mecanismo que fizesse o mesmo que é feito por estes dispositivos. Isto pode facilmente ser feito recorrendo a sistemas baseados em Linux onde o seu *kernel* integra por defeito um poderosíssimo mecanismo de classificação e marcação de pacotes designado de *Traffic Control*[34] (TC). Esta alternativa pode ser realmente útil como forma de reduzir a carga de processamento dos *routers* que estão estrategicamente colocados por toda a infraestrutura, permitindo assim que os mesmos possam utilizar esse processamento extra em outras tarefas (ex. reencaminhamento de tráfego *multicast* ou processar qualquer outro tipo de pacotes relativos a outros serviços que existem ou poderão vir a existir na rede - partilha de ficheiros, serviço interno de *cloud*, sistemas de videovigilância de casas ou mesmo de área florestal, entre muitos outros que podem beneficiar os utilizadores que usufruam deste género de solução).

7.4 Módulo do cliente

Visto as Redes Wireless de Âmbito alargado serem soluções desenvolvidas para o benefício dum aglomerado de pessoas, daqui provém todo o tipo de problemas que podem gerar vulnerabilidades ou reduzir o bom funcionamento deste género de

[34] http://www.lartc.org/

infraestruturas de rede. É neste agente cliente (figura 13) que todo o tráfego que circula pela infraestrutura é gerado. Podemos mesmo afirmar que é por causa dele que temos que estar constantemente a investigar novos meios de análise de tráfego de pacotes de forma a otimizar ao máximo os parcos recursos existentes. A postura de cada utilizador é o que vai permitir ditar que regras de QoS deverão ser utilizadas. Este agente tem criado ao longo dos já vários anos de existência da Internet uma enorme dor de cabeça aos administradores de sistemas pela contínua necessidade de mais e sempre mais largura de banda, o que requere cada vez mais atenção, análise e um cuidado planeamento das infraestruturas que estes técnicos especializados administram.

Figura 13 - Módulo do Cliente

7.5 Síntese

Este capítulo descreve, de forma genérica, uma arquitetura em que se possa encaixar uma solução que utilize um mecanismo de *Deep Packet Inspection* em Redes Wireless de Âmbito Alargado. Começou-se por apresentar uma visão geral da solução, ou seja, um sistema que se enquadre nas características da infraestrutura e que proceda a uma análise cuidada de todo o tráfego que circula pela rede de forma a caracterizá-lo da melhor forma possível. Para isso a ideia passa por esquecer as velhas ideologias de análise de tráfego, em que se generalizava que uma aplicação apenas utilizava o porto que lhe era atribuído, passando a utilizar mecanismos mais modernos passeados na ideologia de *firewalls* de nova geração.

Foram também debatidas algumas ideias de forma a proceder à utilização de mecanismos de *Deep Packet Inspection* e de que forma utilizar a informação fornecida por esse mecanismo de modo a utilizá-la e atualizar as regras de qualidade de serviço consoante o que realmente circula pela rede (e não o que usualmente acontece).

Neste capítulo também se propôs uma solução para reduzir a carga de trabalho dos *routers* que se encontram distribuídos por toda a infraestrutura, utilizando assim, essa capacidade de processamento extra para redirecionar tráfego gerado por serviços, ao invés de utilizar grande parte da mesma para proceder à marcação e classificação de pacotes. Finaliza-se com uma nota da responsabilidade e impacto do agente cliente numa infraestrutura do género da que está a ser analisada nesta dissertação.

Capítulo 8

8 Implementação da solução

Este capítulo descreve todo o processo de criação do serviço implementado que recorre a um sistema baseado na tecnologia *Deep Packet Inspection*. Começa-se por enquadrar a arquitetura descrita no capítulo anterior com um cenário real. De seguida, descrevem-se todas as ferramentas utilizadas e o funcionamento de cada um dos agentes envolvidos. De modo a fechar este capítulo é apresentado um tópico que esquematiza, de uma forma simples, todo o funcionamento da solução criada seguindo-se uma síntese de todo o trabalho realizado.

8.1 Enquadramento da solução com a arquitectura definida

De forma a criar toda uma solução que se enquadre com a arquitetura definida no capítulo anterior, mais concretamente numa rede rural sem fios de âmbito alargado, esta

dissertação baseia-se num cenário e caso de estudo real com características bastante semelhantes, o da freguesia da Memória, que se passa a descrever.

Na freguesia da Memória foi implementado, há alguns anos, uma rede sem fios, resultante de um projeto final de curso da Escola Superior de Tecnologia e Gestão de Leiria (ESTG Leiria), com o objetivo de facultar aos habitantes dessa região um acesso à Internet de forma gratuita. Esta situação levou à implementação desta infraestrutura nesta pequena freguesia dos arredores de Leiria que tem sido um caso de enorme sucesso.

A rede da Memória é composta por duas ligações ADSL de 8Mbits/s (o débito real anda à volta dos 6Mbits por cada ligação) de *downstream* e 640kbits/s de *upstream* situada na junta de freguesia. Dessa localização, essas duas ligações são injetadas em toda a infraestrutura de forma a chegar aos habitantes que tenham acesso ao serviço. Para tal, cada utilizador tem em suas casas um equipamento que recebe o sinal *wireless* que é enviado através de antenas omnidirecionais localizadas em várias zonas da freguesia. Como se pode deduzir, a velocidade da ligação partilhada por todos os habitantes desta região é muito reduzida, pelo que se exige que exista um controlo bastante rigoroso relativamente à qualidade de serviço. Daí a enorme necessidade de implementar uma solução que permita uma análise minuciosa, e em tempo-real, de todo o tráfego que circula pela rede de modo a caracterizá-lo corretamente para, após analisar toda a informação recolhida, implementar regras de QoS da forma, o mais correta, possível. Na ilustração abaixo está representado um esquema genérico da estrutura existente na Memória.

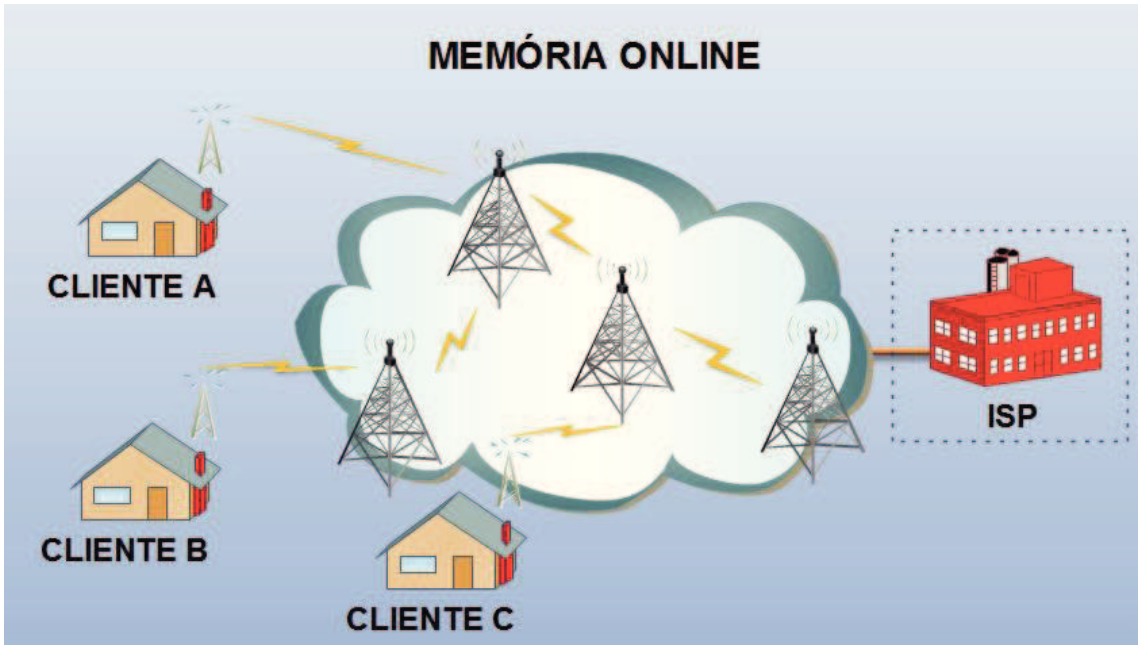


Figura 14 - Esquema genérico da Memória Online

8.2 Ferramentas Utilizadas

Nos subtópicos seguintes serão descritas, pelo seu grau de importância, as ferramentas utilizadas na implementação e desenvolvimento da solução.

8.2.1 Ubuntu

É um sistema operativo baseado na conhecida distribuição GNU/Linux Debian que é distribuído segundo a licença de código aberto. Atualmente é um dos SO's mais utilizados no mundo, é patrocinado pela empresa britânica Canonical Ltd., tendo como grande responsável Mark Shuttleworth, um empresário sul-africano. Apesar do sistema operativo ser completamente gratuito, a Canonical gera receitas através da venda de suporte técnico e de outros tipos de serviços que estão vinculados ao Ubuntu. Nos últimos anos esta distribuição Linux tem ganho terreno face a outras bastante conhecidas sendo atualmente a mais usada em servidores[35].

[35] http://redhatlinux4u.wordpress.com/2012/05/21/the-top-10-linux-server-distributions/

8.2.2 ClearOS

É uma distribuição Linux que é baseada em CentOS[36]. O CentOS, por sinal, é baseado numa outra gigante distribuição Linux que é muito utilizada em ambiente profissional - o Red Hat[37]. Continuando a descrição, o ClearOS foi projetado de raiz para ser utilizado em pequenas e médias empresas como um *gateway* e servidor de rede, recorrendo para isso, a um amigável painel de controlo de administração que pode ser acedido utilizando um simples *browser*. Este pacote de *software* é desenvolvido pela ClearFoundation e permite a aquisição de alguns módulos pagos que podem ser adquiridos através do ClearCenter.

Esta distribuição contém um conjunto enorme de funcionalidades, tais como:

- Segurança e *networking*;
- *Firewalling* do tipo *stateful*[38];
- VPN's;
- Filtragem de conteúdo;
- Web *proxy*;
- Antivírus;
- Serviço de *email*;
- Serviço de partilha de ficheiros e impressoras (Samba e CUPS respetivamente);
- Permite implementar um sistema de tolerância a falhas através da ideologia MultiWAN (agregação de distintas ligações para caso uma delas falhe, continuemos a ter acesso à Internet através de outra ligação que pode ser, por exemplo, fornecida por um diferente provedor de Internet – bastante útil para o caso de estudo da Memória visto aí existirem dois *links* de acesso ao exterior).

8.2.3 ntop

A ferramenta ntop[39] permite analisar e disponibilizar estatísticas muito concretas do que se passa numa rede: Pode-se comparar este serviço a outro que vem por defeito no

[36] http://www.centos.org/
[37] http://www.redhat.com/
[38] http://www.slideshare.net/Sandra4211/stateful-firewalls
[39] http://www.ntop.org

kernel dos sistemas baseados em Unix, 'top'[40], que faz a mesma coisa, mas disponibilizando dados em tempo real de todos os serviços que se encontram a ser executados num Sistema Operativo.

Em modo interativo, este disponibiliza o *status* da rede num terminal[41]. Caso queiramos, esta ferramenta também pode agir como um servidor *Web* criando ficheiros HTML que nos permitam visualizar a mesma informação de forma mais amigável.

Para além disso, e se utilizarmos os binários (e os compilarmos de forma correta) que contenham um projeto distinto, mas criado pela mesma equipa de desenvolvimento, designado de nDPI, este permite estender a biblioteca original do ntop, adicionando a este, novos protocolos e/ou aplicações com assinaturas, por norma, muito difíceis de monitorizar (exemplo: permite a deteção de protocolos conhecidos que estejam a funcionar em portos que não sejam os padrão, ou ainda, como por exemplo, detetar tráfego Skype que esteja a circular no porto 80). Esta extensão é baseada num projeto já extinto, e que desapareceu de forma misteriosa, designado de OpenDPI. A lista atualizada de todos os protocolos suportados pelo nDPI encontra-se disponível na página do projeto ntop, mais concretamente em: http://www.ntop.org/products/ndpi/. O nDPI é uma das melhores soluções de DPI para caraterização de tráfego como ficou demonstrado num recente estudo: [Bujlow et all, 2013].

Este é talvez o componente de *software* mais importante de toda esta solução, pois é ele que permite monitorizar a rede em tempo real utilizando um mecanismo proprietário de *Deep Packet Inspection*. Se bem configurado, e associado a um servidor baseado em Linux, conjuntamente com a poderosa ferramenta que este último contém por defeito no seu *kernel*, o *traffic control*, pode ser uma ferramenta muito poderosa para que os dados disponibilizados sejam utilizados da melhor forma possível pelos administradores de sistemas de modo a desenvolver ferramentas, ou *scripts*, que configurem dinamicamente regras de QoS que se enquadrem realmente àquilo que se passa na rede. Esta magnífica ferramenta é de fato uma mais-valia para utilizar em infraestruturas de rede com baixa largura de banda, pois ajuda a caracterizar todo o tráfego de modo a depois otimizar a rede, conseguindo assim, distribuir a largura de banda existente, de forma, o mais justa possível, por todos os utilizadores.

[40] http://linux.about.com/od/commands/l/blcmdl1_top.htm
[41] http://www.codewalkers.com/c/a/Miscellaneous/The-Terminal-in-UNIX/

8.2.4 Perl

O Perl é uma linguagem de programação reconhecida por ser bastante estável e multiplataforma. É utilizada em aplicações de teor crítico nos mais variados sectores, apesar de ser especialmente usada no desenvolvimento Web. O Perl é uma das linguagens preferidas pelos administradores de sistemas pela sua versatilidade no processamento de *strings*, manipulação de texto e na utilização de expressões regulares (*pattern matching*).

Esta linguagem foi criada por Larry Wall em Dezembro de 1987. Tem as suas origens no shell scripting, AWK e linguagem C, estando disponível na grande maioria dos sistemas operativos existentes, embora seja utilizado mais comummente em sistemas UNIX.

Foi utilizada maioritariamente para a criação de alguns *scripts* que realizam um *parse* dos dados estatísticos fornecidos pela ferramenta de análise da rede descrita no subtópico anterior, que recorre a um mecanismos de Deep Packet Inspection, de forma a aplicar as regras de QoS recorrendo ao TC do servidor Linux.

8.2.5 PHP

O PHP - acrónimo de *PHP: HyperText Preprocessor* - é uma linguagem de programação poderosa que é utilizada, preferencialmente, na criação de conteúdos dinâmicos e interativos para a Internet. As suas grandes características são:

- Velocidade;
- Robustez;
- Estruturado e orientado a objetos;
- Grande portabilidade, independentemente da plataforma (basta escrever uma vez e está pronto a utilizar em qualquer lugar);
- Sintaxe muito similar às do C/C++ e Perl.

É uma alternativa amplamente utilizada por ser de cariz livre e muito eficiente, comparativamente ao seu grande concorrente pago, o ASP da Microsoft. Apesar de existirem linguagens de programação mais modernas e avançadas para a criação de

conteúdos para a *Web*, como é o caso do Ruby[42], decidiu-se por utilizar esta de forma a integrar mais facilmente com projetos já desenvolvidos.

8.3 Implementação da arquitetura proposta

Antes de explicar neste subcapítulo a implementação de toda a solução, de salientar que para a caracterização do tráfego recorrendo ao mecanismo de *Deep Packet Inpection* foram gastas muitas horas a estudar, instalar, otimizar e testar algumas soluções que acabaram por não ser utilizadas na solução final apresentada. Todas elas são/eram, baseadas num modelo de desenvolvimento *open source*. As ferramentas analisadas foram:

- OpenDPI[43]: considerada a primeira ferramenta *open source* que recorre ao mecanismo de DPI. Infelizmente este projeto desapareceu, sem se perceber muito bem o porquê, apesar de ainda ser possível de encontrar, com algum esforço, os binários associados a este projeto. Pela sua descontinuidade, esta ferramenta foi obviamente descartada;

- TrafficSqueezer[44]: esta solução, também ela um projeto *open source*, revelou-se de facto muito interessante. A mesma pode-se considerar uma solução que combina as principais funcionalidades das ferramentas descritas anteriormente: ClearOS + ntop. Infelizmente demonstrou ser muito pouco consistente pelos sucessivos *bugs* e resultados díspares. Os problemas podem ter sido da minha parte, pois basta uma incorreta configuração na compilação do *kernel* ou qualquer outro dos parâmetros de configuração para que os resultados não sejam os desejados. Aquando da escrita de todo este documento, tinha saído uma nova versão que infelizmente não me foi possível de testar, mas que promete corrigir grande parte dos problemas que foram encontrados em versões anteriores. Para além de deixar a página deste projeto (ver nota de rodapé) também aqui deixo o *link* onde o leitor pode realizar o download deste interessante projeto de forma totalmente gratuita em: http://sourceforge.net/projects/trafficsqueezer/.

[42] http://www.ruby-lang.org/en/
[43] Domínio ainda ativo, mas sem conteúdo: http://www.opendpi.org/
[44] http://www.trafficsqueezer.org/

Para além de todas as ferramentas *open source* já aqui descritas com o propósito de realizar a caracterização do tráfego de uma rede informática, também me foi possível falar com alguns dos responsáveis pela implementação de algumas soluções proprietárias disponibilizadas por gigantes da área do *networking* e segurança, tais como: Fortinet e Palo Alto Networks, Inc. na última Info Security Europe 2013 que decorreu na cidade de Londres. Essa experiência revelou-se de facto muito elucidativa e só veio demonstrar a enorme diferença que ainda existe neste ramo entre soluções gratuitas e soluções pagas que apenas estão ao alcance de grandes e poderosas empresas/instituições pela enormidade dos custos necessários para as adquirir.

De modo a produzir uma solução que se enquadre na arquitetura proposta no capítulo 7, a escolha acabou por recair na utilização do binómio ClearOS + ntop (que como já vimos integra um módulo que contém um mecanismo de DPI, nDPI, que foi baseado no código fonte do extinto OpenDPI).

Para proceder à implementação da solução, começou-se por proceder à criação e configuração de uma máquina virtual baseada em ClearOS. A essa máquina virtual foram adicionadas duas placas de redes virtuais, uma configurada em modo *bridge* (eth0) e a outra em modo *host* (eth1). À primeira foi configurado um IP fixo de rede para além do óbvio *gateway* (que permite a ligação à rede externa - Internet). Na segunda placa de rede virtual foi associado um endereço, também ele estático, para a rede local - será este endereço que representará na solução final o *gateway* aos quais os equipamentos localizados em casa dos utilizadores se irão ligar.

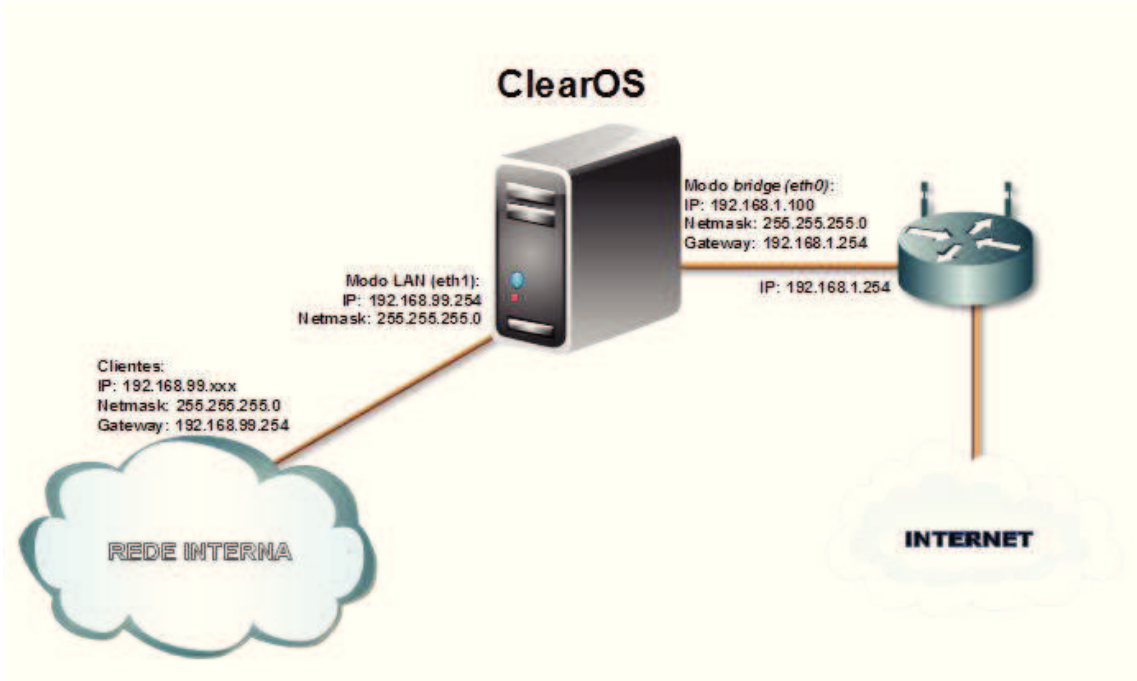


Figura 15 - Esquema de implementação do *gateway*

Após a configuração do *gateway* (figura 15), foi criada uma nova máquina virtual (figura 16) que tem como principal objetivo analisar todo o tráfego que circula pela rede interna. Dessa análise, que recorre à ideologia já apresentada neste documento de *firewalls* de nova geração e a um mecanismo de *Deep Packet Inspection*, resultará a caracterização detalhada de todo o tráfego. O sistema operativo escolhido foi o Ubuntu associado à compilação e integração do projeto ntop no código fonte da distribuição Linux utilizada. Aquando da configuração desta máquina virtual, visto essa se comportar como um vulgar agente cliente da rede, apenas foi necessário adicionar uma placa de rede. É através desta interface de rede que o processo nDPI (8.2.3 ntop) estará constantemente a correr em *background* de forma a analisar todos os pacotes que circulem pela rede com recurso a um poderoso mecanismo de DPI de código aberto. Essa informação é fulcral para analisar o que se está a passar em tempo real na rede para, posteriormente, e da análise dessa informação, criar regras de qualidade de serviço que sejam implementadas no *gateway*. Na implementação da solução, essas regras foram configuradas de duas formas: via a *dashboard* de configuração (w*eb-base*d) existente no ClearOS e, com resultados mais fiáveis, recorrendo a *scripts* que implementem IPtables (esses scripts realizam um *parse* da informação disponibilizada pelo ntop e aplicam as regras de uma forma automática. Isto é muito útil, pois recorrendo ao serviço *cron*, que vem por defeito em praticamente todas as versões do

kernel Linux, qualquer administrador de sistemas pode configurar de quanto em quanto tempo quer que esses *scripts* sejam executados).

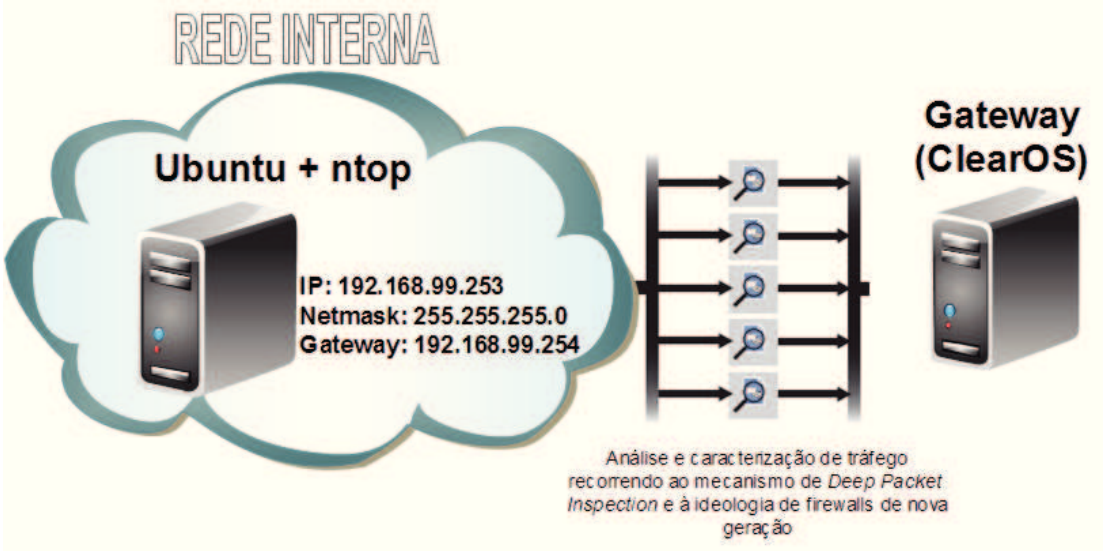


Figura 16 - Partilha de informação entre servidor DPI e o *gateway*

Como se pode observar na ilustração anterior (figura 16) o servidor com o mecanismo de DPI analisa todo o tráfego que passa pelo *gateway* e procede à análise do mesmo. Após essa análise todos os dados são enviados para o *gateway*. Isso acontece, pois apesar de a máquina que realiza a caracterização de todo o tráfego guardar essa informação, a mesma apenas é guardada localmente em ficheiros do tipo *comma-separated values* (CSV). Para isso, criou-se uma base de dados MySQL localizada no *gateway*. Toda essa informação é posteriormente utilizada nos *scripts* desenvolvidos que realizam *firewalling* com recurso a IPtables. Decidiu-se criar essa base de dados, e de os manter numa máquina diferente, para caso o servidor que contém o serviço de DPI falhe, o administrador tenha, noutro local, toda a caracterização do tráfego realizada até então salvaguardada. Para além disso, essa base de dados pode revelar-se muito útil para integrar toda essa análise em outras ferramentas de análise tais como: Nagios, Observium, entre outras.

A atualização dessa base de dados é realizada da seguinte forma: o *gateway* tem um serviço configurado que copia, de quinze em quinze minutos através de um canal cifrado, a caracterização do tráfego guardada em formato CSV realizada pelo servidor DPI para o *gateway*. Aí, e recorrendo a um *script* realizado em Perl, esses dados em formato CSV são tratados e importados para a base de dados MySQL.

8.4 Solução final

A Figura 17 - Explicação da solução implementada, representa, de uma forma simples, como todos os agentes envolvidos comunicam entre si através da solução implementada.

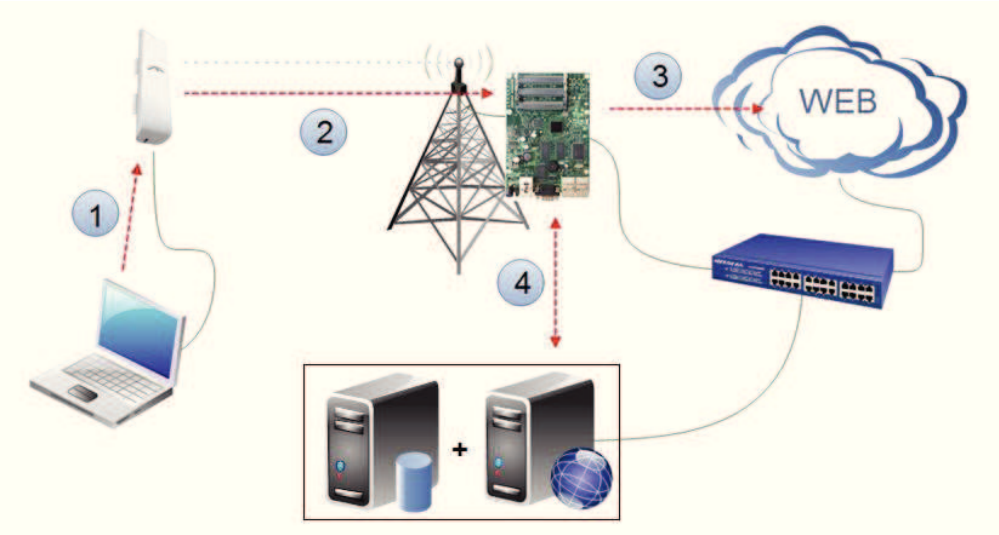


Figura 17 - Explicação da solução implementada

1. O agente Cliente procede a uma normal navegação pelo mundo virtual;
2. O *router*, instalado na casa do cliente, recebe todos os pacotes gerados e envia-os para o equipamento no *core* da rede;
3. Os equipamentos existentes ao longo de toda a infraestrutura recebem e reencaminham todo o tráfego para a Web;
4. O binómio constituído pelas máquinas virtuais: ClearOS + ntop procedem à análise de todos os pacotes gerados pelo utilizador e realizam uma caracterização detalhada recorrendo ao mecanismo de *Deep Packet Inspection*. A informação contida em formato CSV no servidor DPI (ntop) é copiada e importada, de quinze em quinze minutos, para a base de dados MySQL existente no servidor *gateway* (ClearOS).

A figura 18 representa o algoritmo de comunicação entre os dois servidores (explicada anteriormente, no ponto 4) para a criação da base de dados MySQL através da caracterização do tráfego efetuada no servidor DPI, guardada em formato CSV.

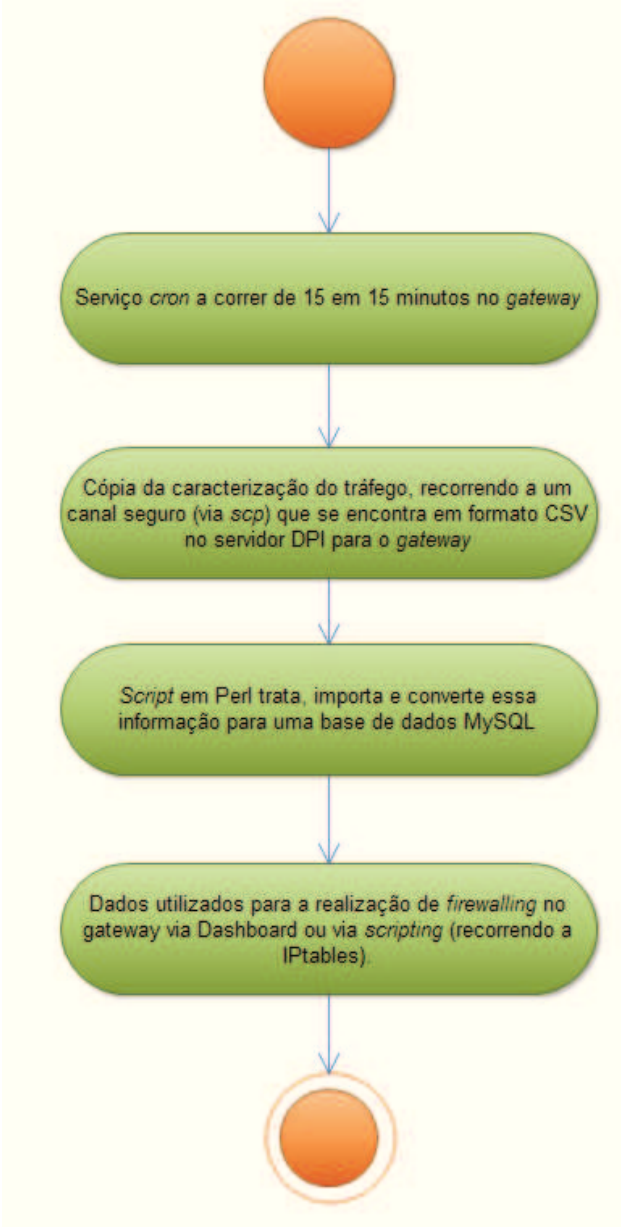


Figura 18 – Algoritmo de comunicação entre os servidores para a criação da base de dados

8.5 Síntese

Este capítulo pretendeu demonstrar todos os passos necessários para a implementação de uma solução fiável que permitisse resolver o problema apresentado no capítulo anterior (7 - Arquitetura).

Foram também descritas as principais ferramentas utilizadas para além dos passos utilizados para a implementação da solução. Para fechar, é explicado esquematicamente a forma de funcionamento da solução.

Capítulo 9

9 Testes

Neste capítulo são apresentados alguns dos testes efetuados de forma a verificar a funcionalidade e resultados de todo o trabalho realizado. O cenário de testes descreve todo o material disponível e utilizado para garantir a integridade da solução desenvolvida. Todos estes testes são essenciais para simular, da forma o mais realista possível, a reação da solução aquando de uma possível integração da mesma na infraestrutura da Memória. Os dados são apresentados por intermédio de imagens e gráficos associados de uma breve descrição.

9.1 Cenário de Testes

De forma a realizar a validação da solução implementada, foi utilizado um cenário de testes que pretende demonstrar, da forma mais real possível, o funcionamento do

sistema através de uma pequena simulação do cenário encontrado na Memória. Para isso, foram utilizadas três máquinas virtuais:

- Uma com o ClearOS instalado e que pretende simular o *gateway*. Esta máquina virtual, como já vimos anteriormente, terá duas placas de rede:
    - Uma que recebe uma ligação à Internet de forma a simular um dos dois *links* existentes no cenário da Memória que são utilizados para injetar e partilhar esse acesso a todos os utilizadores da rede interna ao mundo virtual;
    - A outra placa será utilizada como sendo a ponte/*gateway* de todas as máquinas existentes na rede interna e que permitirá a partilha da ligação fornecida pelo provedor de Internet.
- A outra máquina virtual utilizada para estes testes foi configurada com Ubuntu e tem também compilado o projeto ntop que permite analisar e caracterizar todo o tráfego gerado pelos clientes. Para os testes, e devido a limitações de *hardware*, esta máquina virtual também foi configurada de forma a funcionar como um agente cliente;
- Por último, a terceira máquina virtual utilizada funciona somente como sendo um agente cliente e contém instalada uma distribuição Ubuntu Desktop 12.04. Será maioritariamente utilizada ao longo dos testes para testar algumas aplicações que são muito difíceis de caracterizar por causa do *port hopping* que realizam (ex.: Skype, Bittorrent, Dropbox, entre outras).

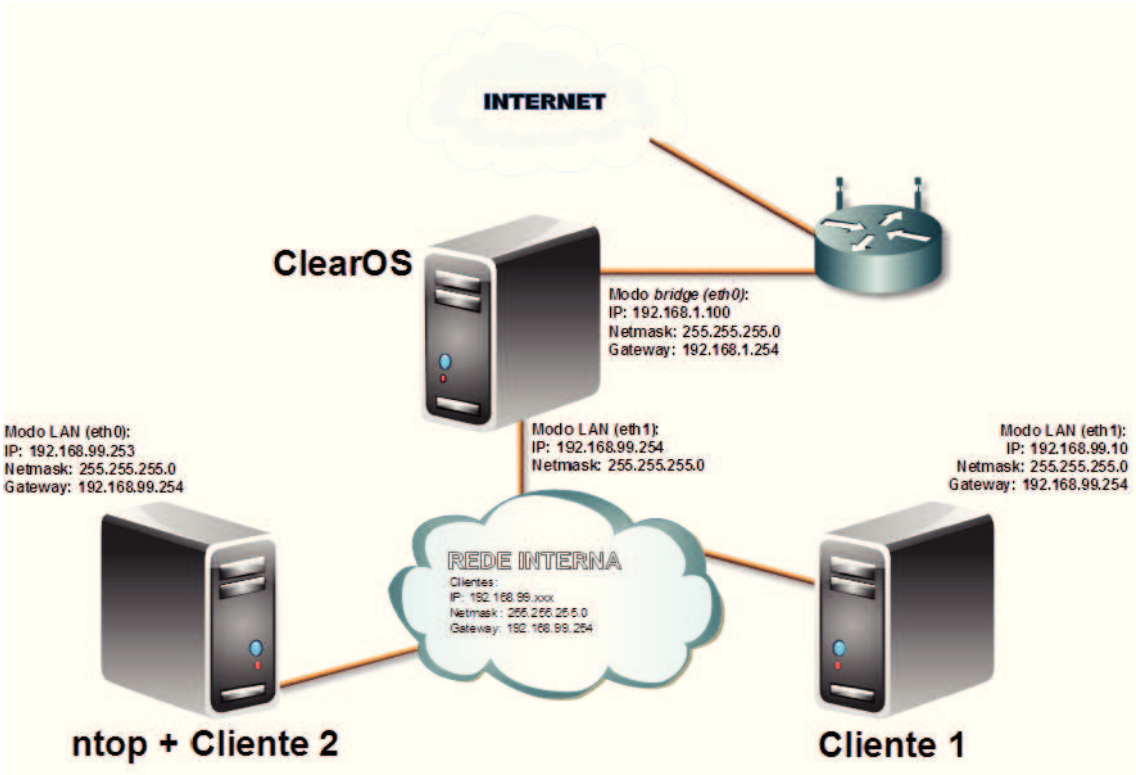


Figura 19 - Cenário de testes

Na ilustração acima encontra-se a esquematização do cenário de testes utilizado. Após a instalação do mesmo, o primeiro passo foi o de iniciar o *gateway* (ClearOS). De seguida, iniciaram-se as duas restantes máquinas virtuais para que comunicassem corretamente com o *gateway*, para além de receberem do mesmo o acesso à Internet. De referir que no caso do Cliente 2 (o que também contém o mecanismo de *Deep Packet Inspection* compilado no *kernel*) também foi necessário proceder ao início do *daemon* de análise da rede associado à interface adequada - neste caso eth0. Este processo estará continuamente a correr em *background* ao longo de todos os testes efetuados, pois é ele que permite realizar e caraterizar todo o tráfego que circula na rede.

9.2 Testes às configurações e conectividade

O grande objetivo deste grupo de testes é o de se verificar se todas máquinas virtuais se encontram a comunicar entre elas, e ao mundo virtual, para além de comprovar se as interfaces associadas a cada uma delas se encontram corretamente configuradas.

9.2.1 ClearOS

Nas figuras seguintes podemos confirmar que os endereços foram configurados segundo o que foi definido para o cenário de testes. Também se pode comprovar que esta máquina virtual se encontra a funcionar em modo *gateway*, para além, de os servidores de DNS configurados e utilizados serem os públicos do Google.

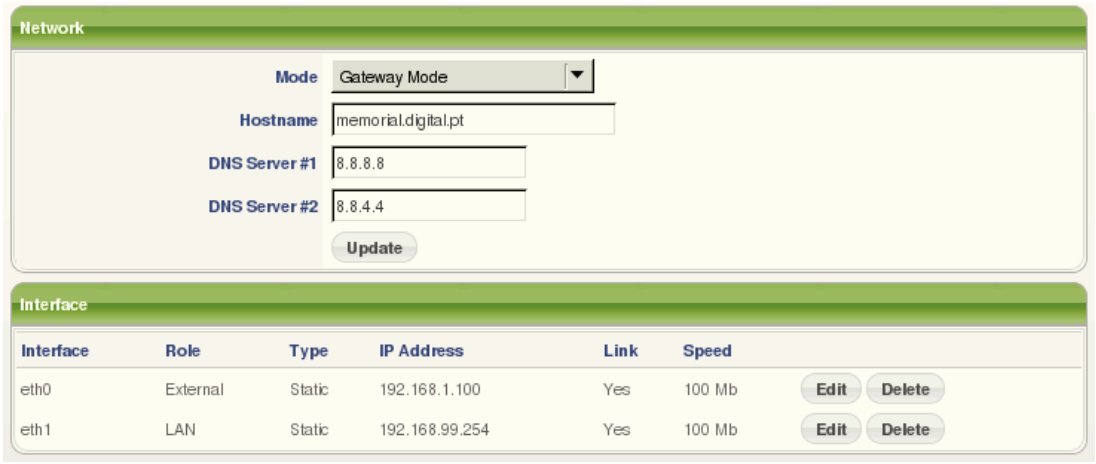


Figura 20 – Configuração do ClearOS - modo gráfico

```
[root@memorial ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:6C:8E:AB
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6c:8eab/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:221377 errors:3 dropped:0 overruns:0 frame:0
          TX packets:20279 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:122221131 (116.5 MiB)  TX bytes:1530183 (1.4 MiB)
          Interrupt:10 Base address:0xd020

[root@memorial ~]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:56:FE:1F
          inet addr:192.168.99.254  Bcast:192.168.99.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe56:fe1f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16205 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1533179 (1.4 MiB)  TX bytes:16472214 (15.7 MiB)
          Interrupt:9 Base address:0xd240
```

Figura 21 - Interfaces ClearOS - modo CLI

9.2.2 Cliente 1

A figura seguinte demonstra a configuração para o Cliente 1.

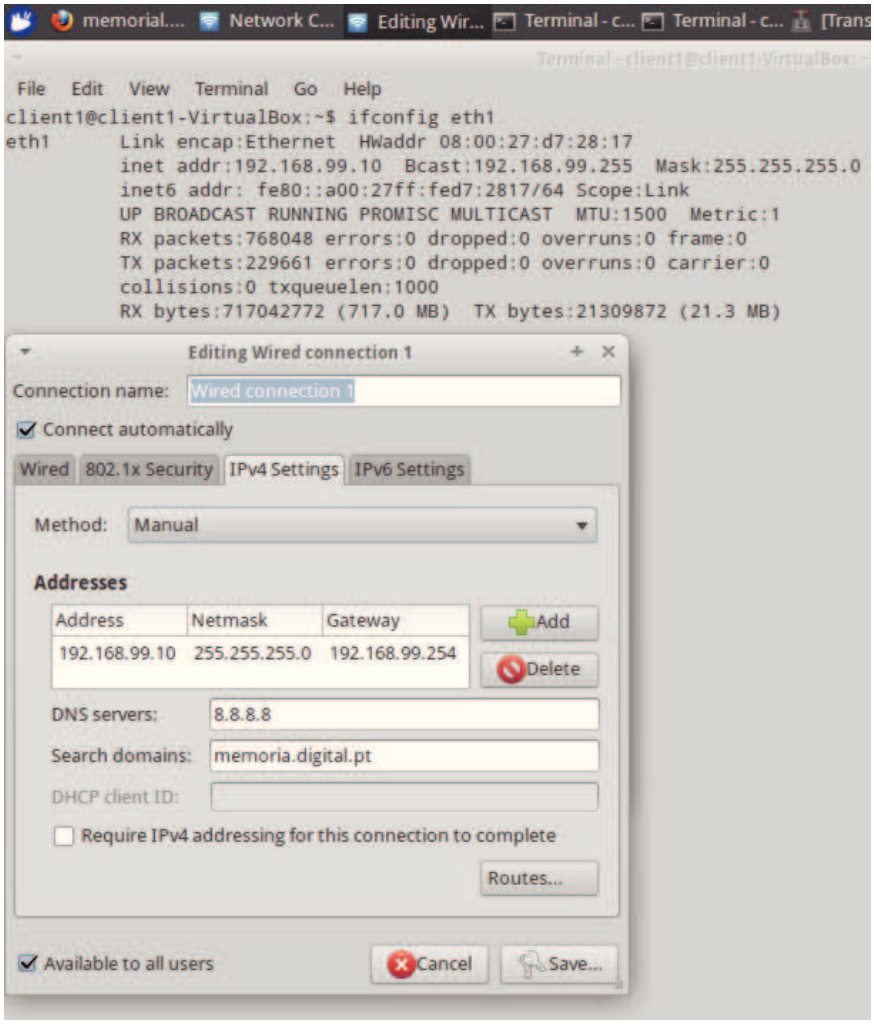


Figura 22 - Interface de rede - Cliente 1

Após comprovar a correta configuração da interface, testou-se a comunicação entre o Cliente 1 e o servidor, para além de testar a comunicação entre esta máquina virtual e a Internet.

```
client1@client1-VirtualBox:~$ ping -c5 192.168.99.254
PING 192.168.99.254 (192.168.99.254) 56(84) bytes of data.
64 bytes from 192.168.99.254: icmp_req=1 ttl=64 time=1.48 ms
64 bytes from 192.168.99.254: icmp_req=2 ttl=64 time=0.574 ms
64 bytes from 192.168.99.254: icmp_req=3 ttl=64 time=0.626 ms
64 bytes from 192.168.99.254: icmp_req=4 ttl=64 time=0.947 ms
64 bytes from 192.168.99.254: icmp_req=5 ttl=64 time=0.774 ms

--- 192.168.99.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.574/0.880/1.482/0.329 ms
client1@client1-VirtualBox:~$ ping -c5 sapo.pt
PING sapo.pt (213.13.146.140) 56(84) bytes of data.
64 bytes from sapo.pt (213.13.146.140): icmp_req=1 ttl=120 time=36.0 ms
64 bytes from sapo.pt (213.13.146.140): icmp_req=2 ttl=120 time=33.0 ms
64 bytes from sapo.pt (213.13.146.140): icmp_req=3 ttl=120 time=32.5 ms
64 bytes from sapo.pt (213.13.146.140): icmp_req=4 ttl=120 time=33.1 ms
64 bytes from sapo.pt (213.13.146.140): icmp_req=5 ttl=120 time=32.4 ms

--- sapo.pt ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 32.439/33.438/36.042/1.345 ms
client1@client1-VirtualBox:~$
```

Figura 23 - Cliente 1: teste às comunicações

9.2.3 Cliente 2

De seguida são demonstrados os resultados aquando da realização dos testes efetuados para o Cliente 2.

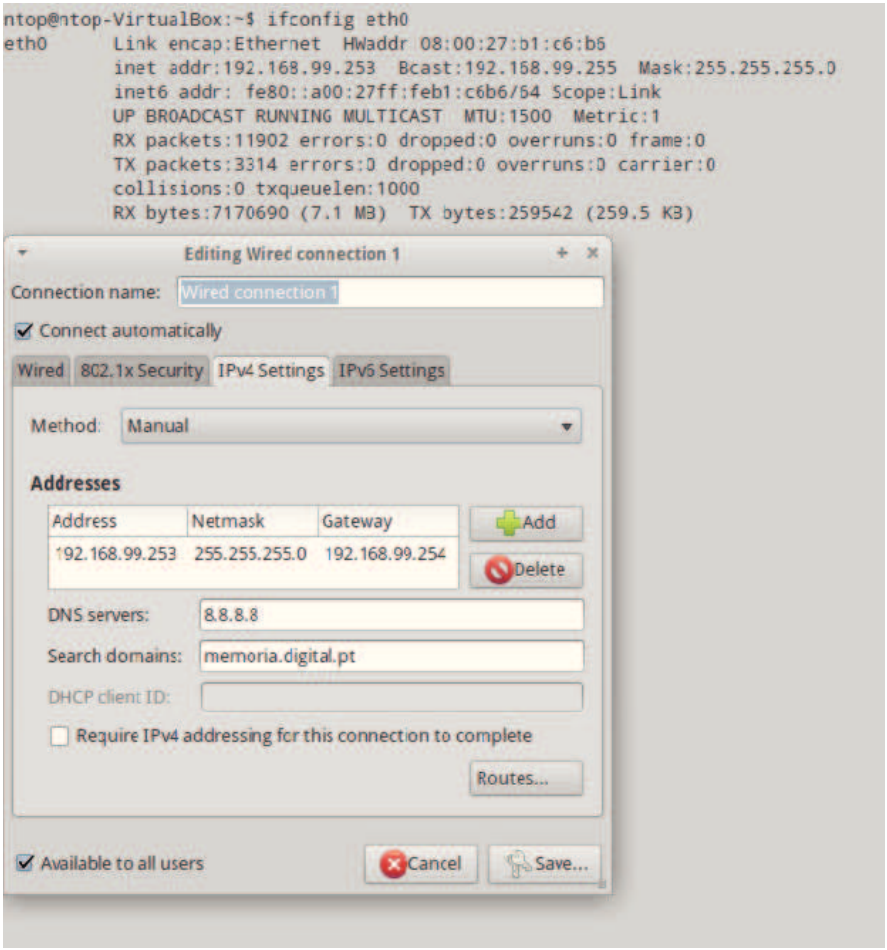


Figura 24 - Interface de rede - Cliente 2

Como podemos ver pela figura 25, a comunicação entre esta máquina virtual e o *gateway* e Internet foi realizada com sucesso.

```
ntop@ntop-VirtualBox:~$ ping -c5 192.168.99.254
PING 192.168.99.254 (192.168.99.254) 56(84) bytes of data.
64 bytes from 192.168.99.254: icmp_req=1 ttl=64 time=2.09 ms
64 bytes from 192.168.99.254: icmp_req=2 ttl=64 time=0.662 ms
64 bytes from 192.168.99.254: icmp_req=3 ttl=64 time=0.549 ms
64 bytes from 192.168.99.254: icmp_req=4 ttl=64 time=0.679 ms
64 bytes from 192.168.99.254: icmp_req=5 ttl=64 time=0.526 ms

--- 192.168.99.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.526/0.902/2.095/0.599 ms
ntop@ntop-VirtualBox:~$ ping -c5 sapo.pt
PING sapo.pt (213.13.146.140) 56(84) bytes of data.
64 bytes from sapo.pt (213.13.146.140): icmp_req=1 ttl=120 time=38.0 ms
64 bytes from sapo.pt (213.13.146.140): icmp_req=2 ttl=120 time=33.6 ms
64 bytes from sapo.pt (213.13.146.140): icmp_req=3 ttl=120 time=33.3 ms
64 bytes from sapo.pt (213.13.146.140): icmp_req=4 ttl=120 time=32.8 ms
64 bytes from sapo.pt (213.13.146.140): icmp_req=5 ttl=120 time=33.4 ms

--- sapo.pt ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 32.847/34.268/38.079/1.926 ms
```

Figura 25 - Cliente 2: teste às comunicações

9.3 Teste à execução do *daemon* de DPI

Este teste teve como principal objetivo verificar se o processo que é necessário estar a correr constantemente em *background* executava e reconhecia corretamente a interface de rede que pretendemos utilizar (eth0) de forma a capturar, analisar e caraterizar todos os pacotes que circulem pelo cenário de testes.

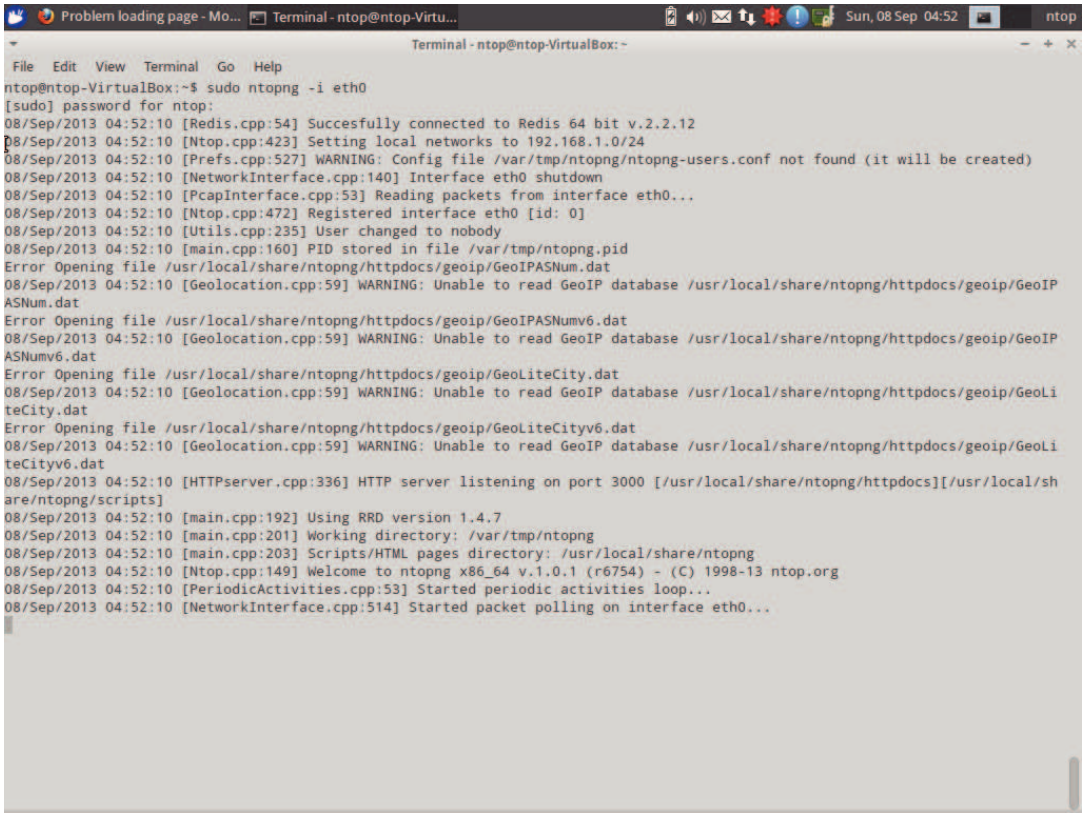


Figura 26 - ntopng *daemon*

Como se pode verificar na ilustração anterior (figura 26), o processo foi executado com sucesso, logo os binários deste projeto de código livre foram executados e configurados com sucesso para utilizar neste cenário de testes. Este processo continuará a executar em *background* até que se proceda ao seu término.

Na figura podemos verificar que existem alguns *warnings*. Esses avisos estão a ocorrer pois aquando da compilação de todo o *software* optou-se por não incluir alguns módulos de forma a otimizar os recursos existentes – neste caso, o aviso refere-se à inexistência da compilação do *plugin* que permite realizar a localização geográfica dos dispositivos da rede.

9.4 Acesso à *dashboard* do ntop

O teste seguinte foi o de aceder à plataforma de monitorização gráfica da ferramenta ntop. O principal intuito foi o de testar o utilizador e *password* definida (utilizador: *admin* | *password*: *root*). Para isso foi necessário utilizar um *browser* e redirecionar o pedido para o endereço (192.168.99.253) + porto (por defeito é o porto 3000 para

ligação por HTTP ou 3001 para HTTPS) da máquina virtual em que o ntop se encontra compilado.

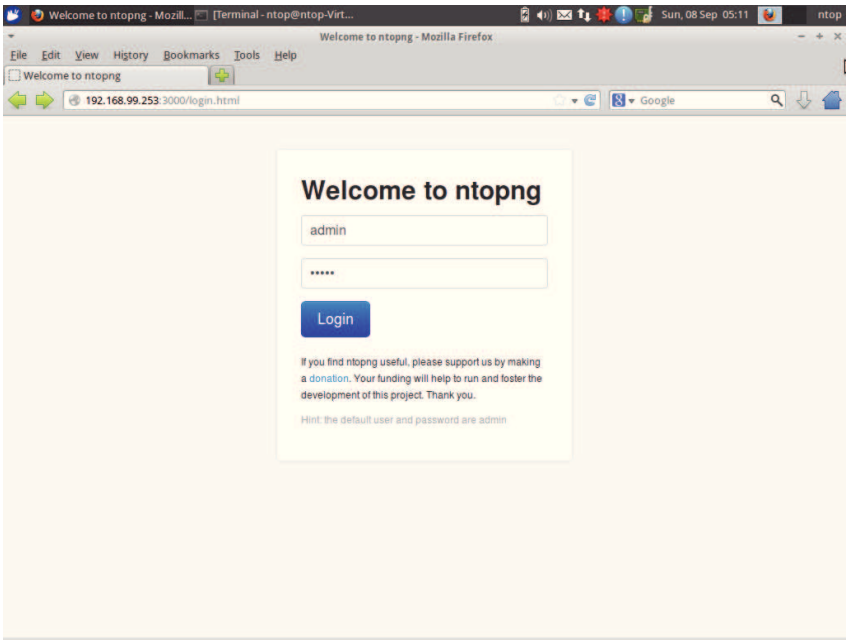


Figura 27 - ntop - *dashboard login*

Após a realização do *login* com sucesso o utilizador é redirecionado para a *dashboard* desta ferramenta. Como podemos ver na figura seguinte, e após proceder à escolha dos protocolos mais utilizados no momento, a ferramenta lista a aplicação Spotify[45] (apesar de ser relativamente recente esta aplicação já permite caracterizar o tráfego proveniente deste cliente de música que se encontra listado por me encontrar a utilizar o mesmo aquando dos testes), ICMP (na altura dos testes estava a *pingar* em cada uma das máquinas virtuais a página do Google) e DNS (*queries* comummente realizadas para a resolução de nomes).

[45] https://www.spotify.com

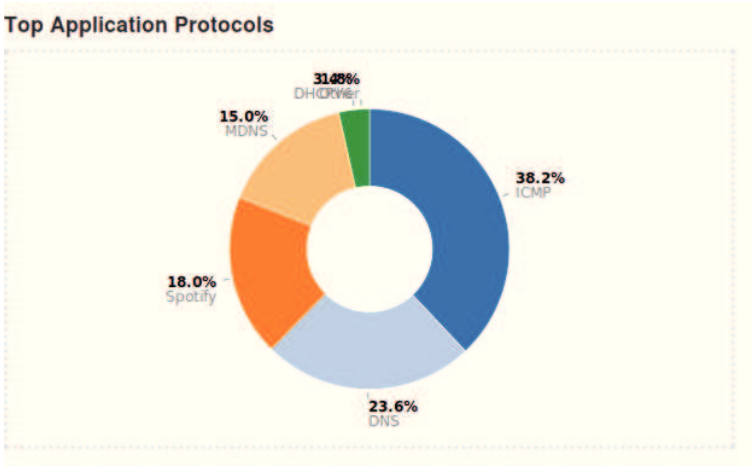


Figura 28 - ntop – protocolos/aplicações mais utilizadas

9.5 Caraterização de tráfego "mal comportado"

Pode-se considerar este o subcapítulo mais importante quanto à bateria de testes efetuadas na solução implementada, visto ser aqui que são demonstrados parte dos resultados adquiridos após a realização de testes a algumas das aplicações que mais dores de cabeça dão atualmente aos administradores de sistemas, visto estas terem a capacidade de mudar de porto ou utilizar protocolos que não lhes pertençam por defeito.

9.5.1 Tráfego P2P

Para testar as capacidades do ntop, ferramenta que recorre à ideologia das *firewalls* de nova geração e a um poderoso mecanismo de DPI, decidiu-se começar por testar a sua eficácia quanto à capacidade de analisar tráfego P2P. Para isso, decidiu-se proceder à descarga de dois *torrents* que permitissem efetuar o *download* das seguintes distribuições Linux: Ubuntu Server 12.04 e CentOS 6.4.

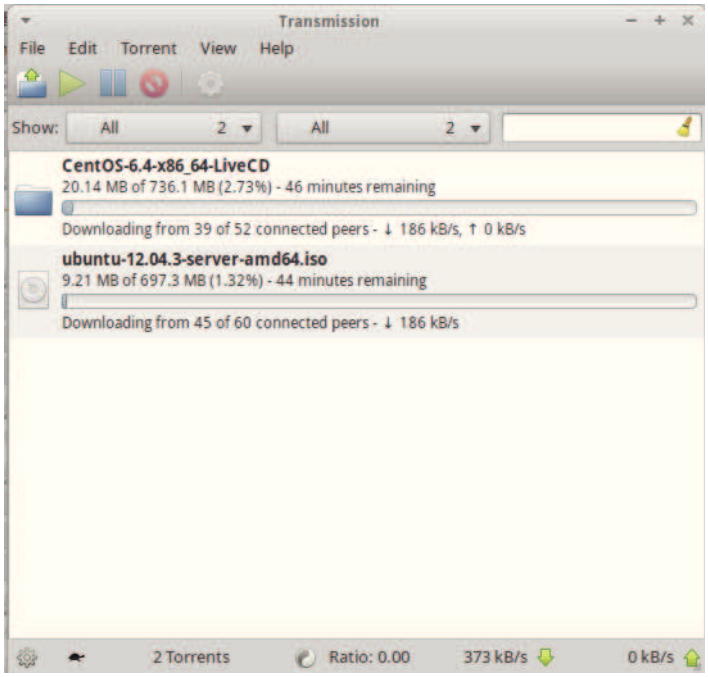


Figura 29 - Transmission - *download* de tráfego P2P

O cliente de *BitTorrent* escolhido para realizar tal tarefa foi o Transmission[46] que vem por omissão no sistema operativo instalado na máquina virtual de testes do Cliente 1. Primeiramente testou-se a opção por defeito em que o cliente escolhe dinamicamente os portos que vai utilizar, e também foi testado para utilizar somente o protocolo HTTPS (utilizando assim *BitTorrent* cifrado com os protocolos HTTP + SSL).

Na figura 30 podemos observar a capacidade que o ntop tem de identificar todos os canais de comunicação / *peers* que estão a ser utilizados para que o Cliente 1 possa proceder ao *download* dos dois *torrents*.

[46] http://www.transmissionbt.com/

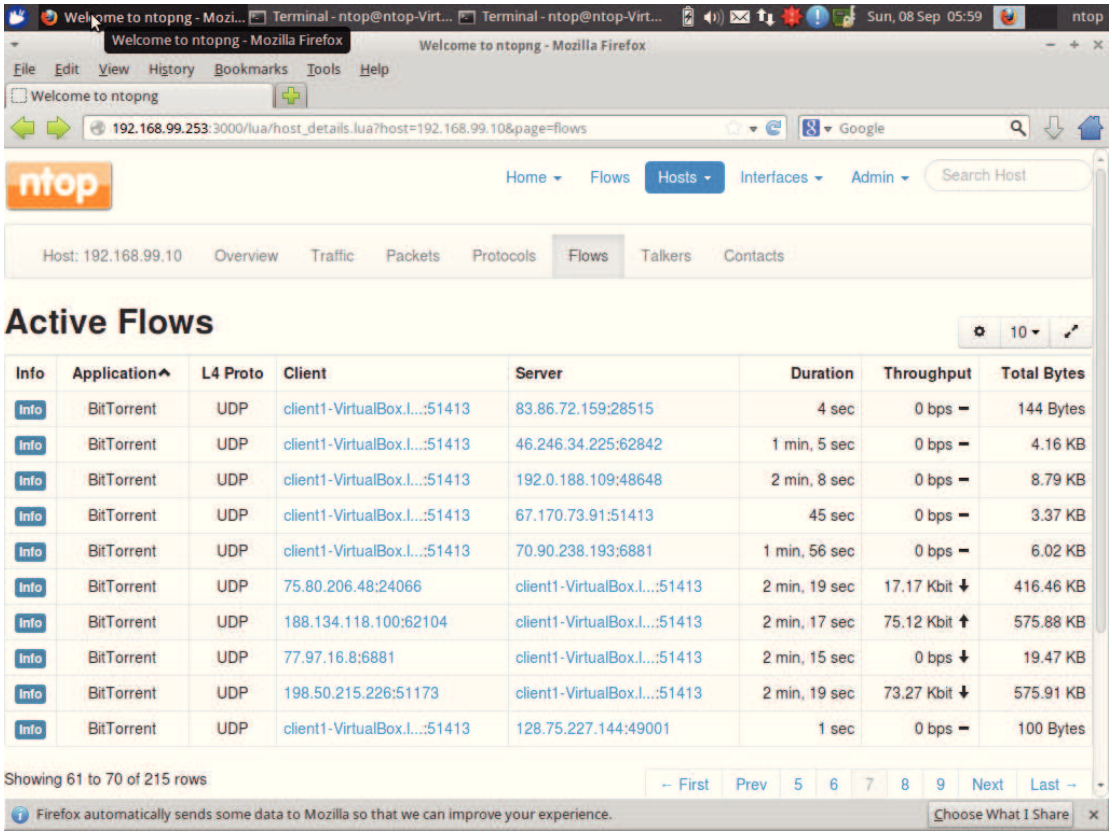


Figura 30 - ntop - identificação de todos os *peers* para aplicação BitTorrent

Realizando a listagem de todos os *hosts* existentes na rede (aqui o ntop tem a capacidade de listar não só os clientes internos, mas também os externos à rede, neste caso lista todos os *peers* envolvidos aquando do download dos *torrents*, o que como se pode imaginar foram centenas de computadores a partilhar informação, podemos filtrar para visualizar apenas e só os clientes da rede interna) podemos visualizar na figura seguinte que o grande responsável pelo enorme consumo de recursos na rede, com uma enorme diferença, foi o Cliente 1. Essa informação pode ser facilmente acedida, caso se escolha para organizar a informação por *'Traffic'*.

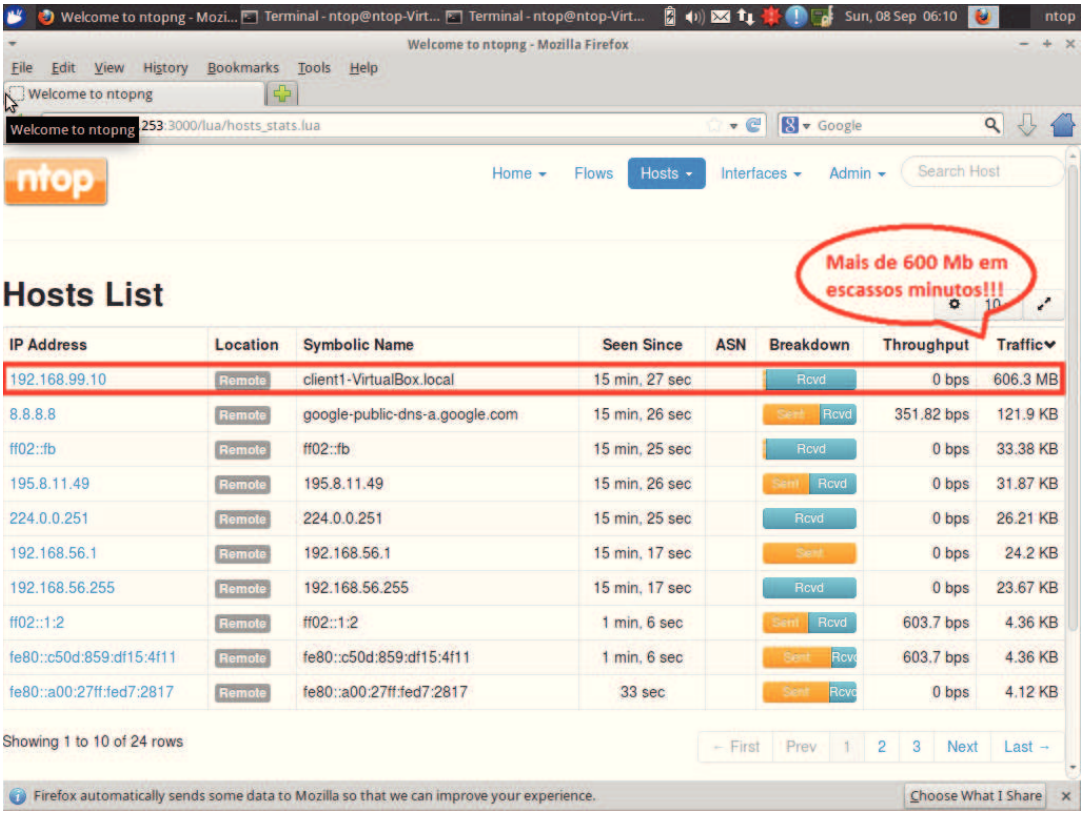


Figura 31 - ntop - Listagem de *hosts* por maior percentagem de tráfego

9.5.2 Skype

A realização deste teste teve como principal objetivo verificar o quão bem implementado está o padrão de reconhecimento da assinatura da aplicação Skype no ntop quanto à análise e caracterização dos pacotes que circulam na rede.

Antes de proceder à instalação e configuração do cliente Skype, mas agora no Cliente 2, realizou-se um *screenshot* para visualizar a influência que o Cliente 1 teve no tráfego gerado na rede no teste anterior. Como se pode confirmar na imagem seguinte (figura 32) o tráfego *BitTorrent* teve um enorme impacto.

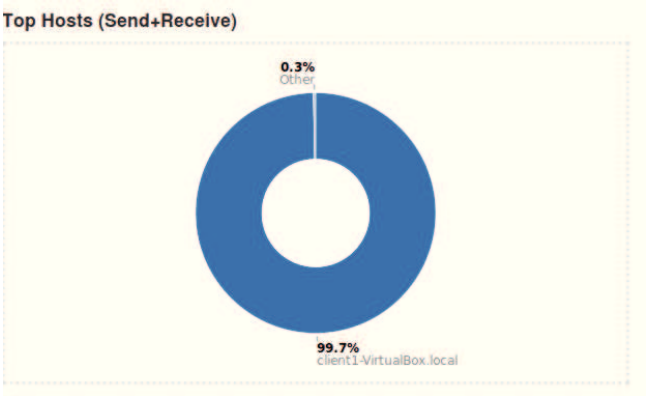


Figura 32 - Impacto to Cliente 1 na performance da rede

Continuando na parte dos testes com a aplicação Skype, após proceder à instalação da mesma, ao mesmo tempo que se realizava uma comum navegação na Internet, realizou-se uma pequena chamada recorrendo a esta aplicação de voz sobre IP. A deteção da aplicação foi em tempo-real e a deteção dos protocolos associados ao Cliente 2 estão representados na figura 33.

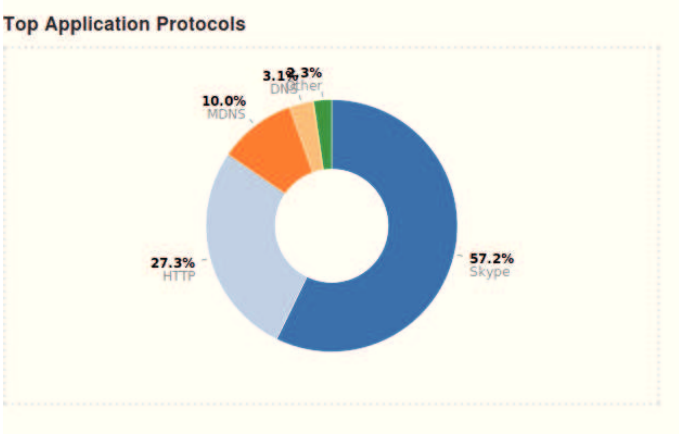


Figura 33 - Caracterização do tráfego após realizar uma chamada Skype

Aquando deste teste teve-se uma perceção muito interessante da capacidade desta aplicação em realizar um *port hopping* muito agressivo de forma a utilizar os portos existentes no Cliente 2, não se focando assim apenas a um conjunto de portos restritos.

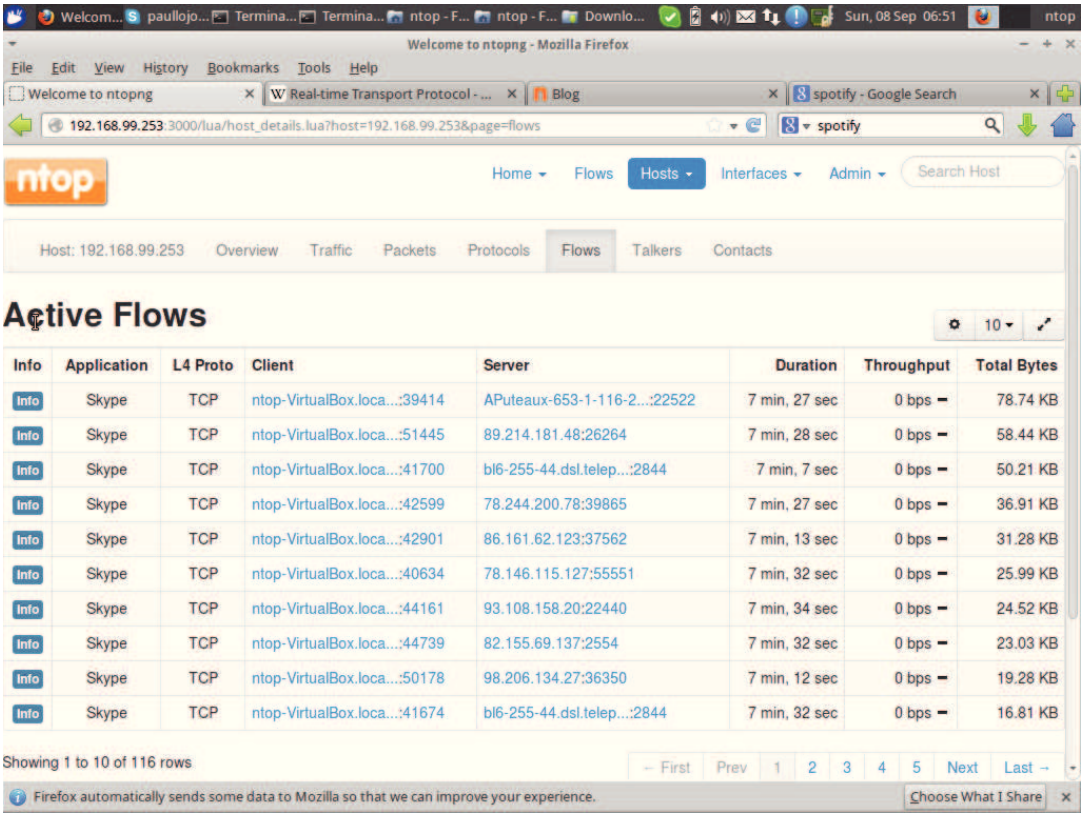


Figura 34 - Capacidade do Skype em realizar *port hopping*

9.5.3 DropBox

O teste seguinte focou-se na utilização de uma aplicação que exige bastante de uma infraestrutura de rede - o DropBox. Isto acontece, pois este tipo de serviços disponibiliza cada vez mais espaço gratuito aos utilizadores para além de estar constantemente a verificar se existe algum documento atualizado. Para este teste não se instalou a aplicação cliente no sistema operativo. Optou-se apenas por aceder a este serviço pela *web* de forma a verificar se o ntop também procede à análise dos pacotes, que são acedidos via HTTPS, e consegue também caracterizar esta aplicação corretamente.

Este teste foi realizado no Cliente 1, onde previamente se realizou o *download* de dois *torrents*, e consistiu em proceder ao download de um ficheiro que está nos servidores Cloud deste serviço.

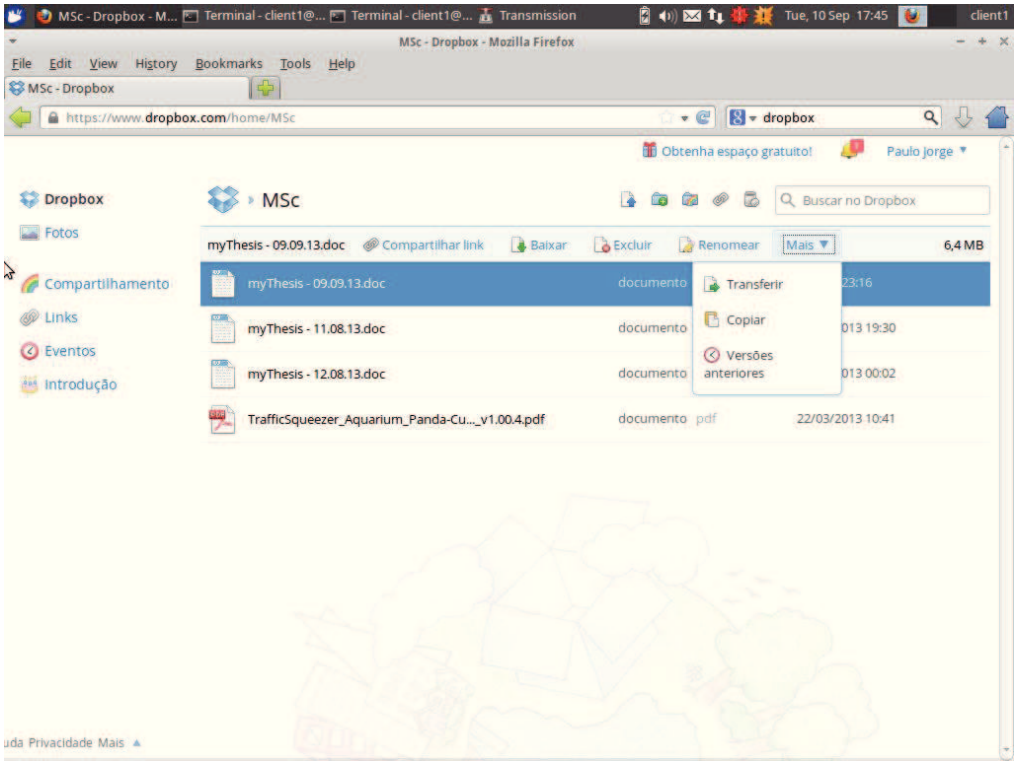


Figura 35 - Download de um ficheiro via HTTPS - DropBox

Como se pode confirmar na imagem anterior, o acesso foi feito recorrendo ao protocolo HTTPS e procedeu-se ao *download* de um ficheiro com aproximadamente 6,4 MB.

Ao aceder à *dashboard* do ntop, os resultados foram de fato muito interessantes. Esta ferramenta conseguiu proceder à caracterização do tráfego mesmo apesar de termos acedido via *web* (recorrendo ao protocolo HTTPS: HTTP + SSL) e conseguiu realizar a caracterização e apresentar os resultados pelo nome da aplicação, e não pelos protocolos utilizados, como podemos ver na figura 36 (também se pode verificar o total de MB's gastos que está certamente a contar o tamanho do ficheiro que foi descarregado localmente acrescentando algum tráfego que foi gasto para proceder ao *login*, navegar pelo diretório do serviço e abertura de alguns ficheiros).

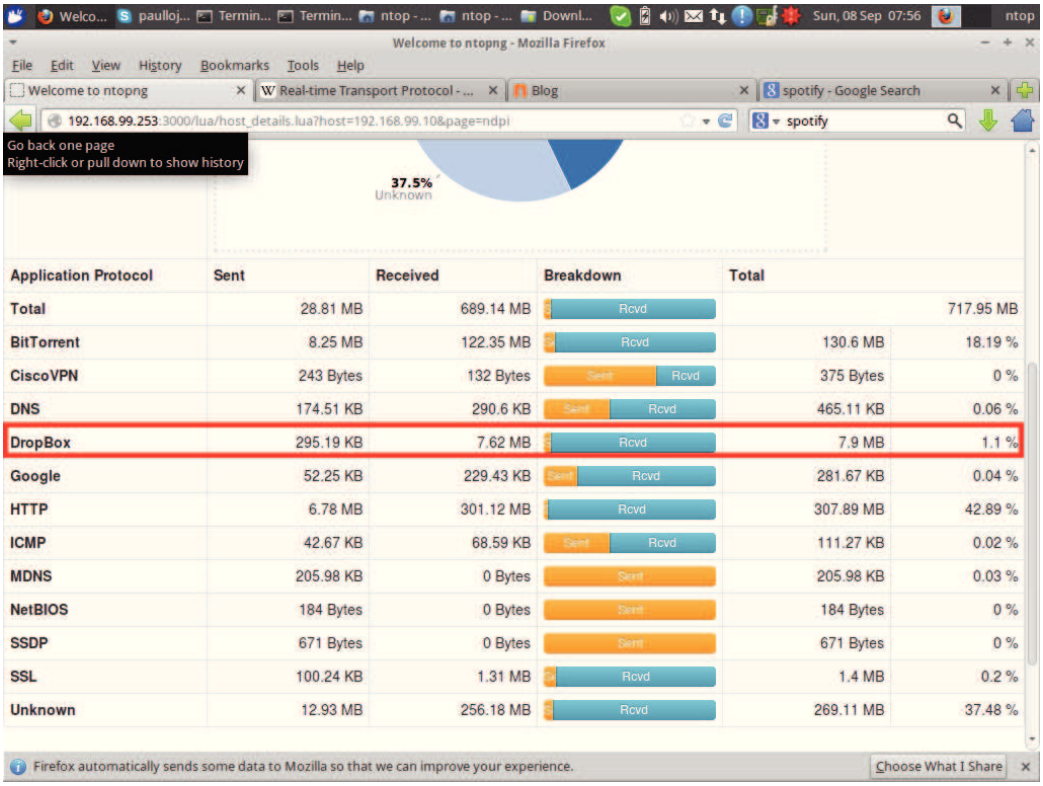


Figura 36 - Caraterização do tráfego associado ao serviço DropBox

9.5.4 YouTube

Como se pode imaginar, e como já vimos neste documento, este género de redes *wireless* comunitárias de âmbito alargado possuem um *link* que provém do ISP de débito muito reduzido. A visualização de vídeo pode ter um impacto muito grande no bom funcionamento e distribuição dos recursos existentes por toda a população. Daí, a necessidade da ferramenta de monitorização implementada conseguir identificar onde é que se está a gastar uma maior percentagem dos recursos. Para além de esse impacto na performance ocorrer, na maior parte das vezes pela realização de *downloads*, quer seja por P2P ou qualquer outra forma, uma tarefas mais críticas passa pela visualização de conteúdo digital.

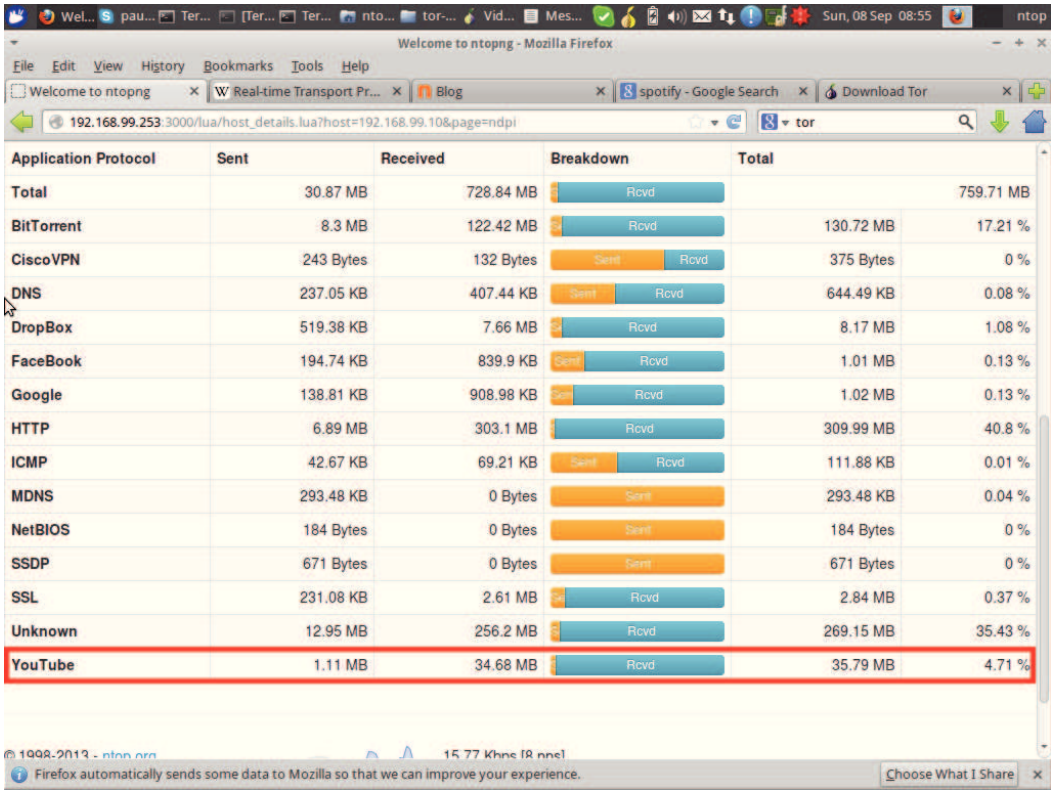


Figura 37 - Caraterização do tráfego associado ao serviço YouTube

Como se pode visualizar da ilustração anterior, associado ao tráfego BitTorrent já gerado, o Cliente 1 encontra-se mais uma vez a consumir grande parte dos recursos da rede através da visualização de conteúdo multimédia recorrendo para tal, e mais especificamente, ao serviço YouTube.

9.5.5 Tor

O Tor[47] é um projeto, de código aberto, bastante interessante que permite a utilização de *proxies* para navegar pela Internet de forma anónima. É muito utilizado por pessoas que tenham um conhecimento acima da média na área das tecnologias da informação para aceder a conteúdos que se encontram bloqueados no país onde residem (exemplo: na China e Irão realizam uma enorme filtragem do que os cidadãos podem visualizar na Internet ou mesmo países em que se pensa que a liberdade é um dado adquirido, como no Reino Unido, em que bloqueiam alguma páginas tais como: Pirate Bay ou muitas outras por causa da proteção da propriedade intelectual digital).

[47] https://www.torproject.org/

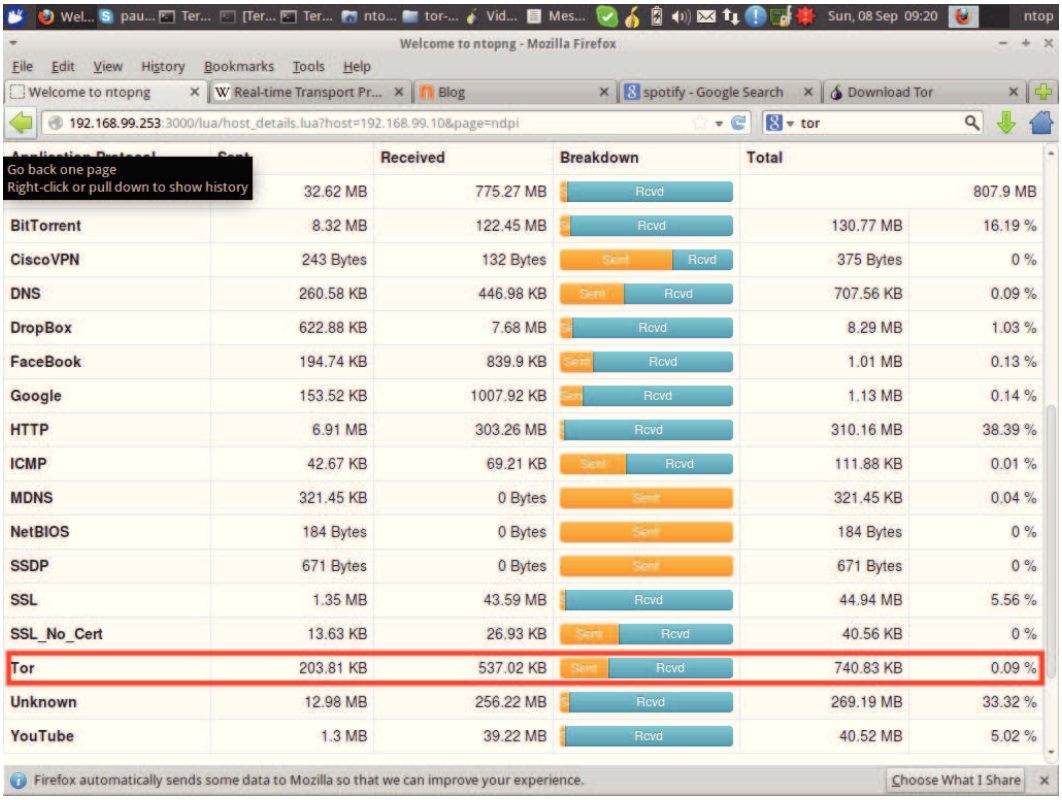


Figura 38 - Caraterização do tráfego associado ao projeto Tor

Um dos testes consistiu em verificar se a máquina virtual responsável por caracterizar o tráfego do cenário de testes conseguia ou não identificar qualquer utilizador que recorra a este projeto.

9.5.6 Facebook

Outro dos protocolos de aplicação também testados foi o do Facebook. Apesar de não ser muito importante proceder à caracterização deste serviço numa rede comunitária, decidiu-se proceder a este teste de forma a demonstrar que esta solução também pode ser utilizada num ambiente profissional. Todos nós temos conhecimento de muitos funcionários perderem grande parte das suas horas de trabalho em redes sociais o que leva à falta de produtividade. O ntop permite realizar a análise e caraterização de acessos às principais redes sociais tais como: Facebook, Twitter, MSN, entre muitas outras.

Para este teste foi mais uma vez utilizado o Cliente 1 e acedeu-se à página do Facebook. Tal como acontece com o DropBox, e os principais serviços *online*, estes obrigam a que

o acesso seja feito por HTTPS, mas como podemos ver (figura 39), mais uma vez, o ntop consegue identificar esse acesso sem quaisquer problemas.

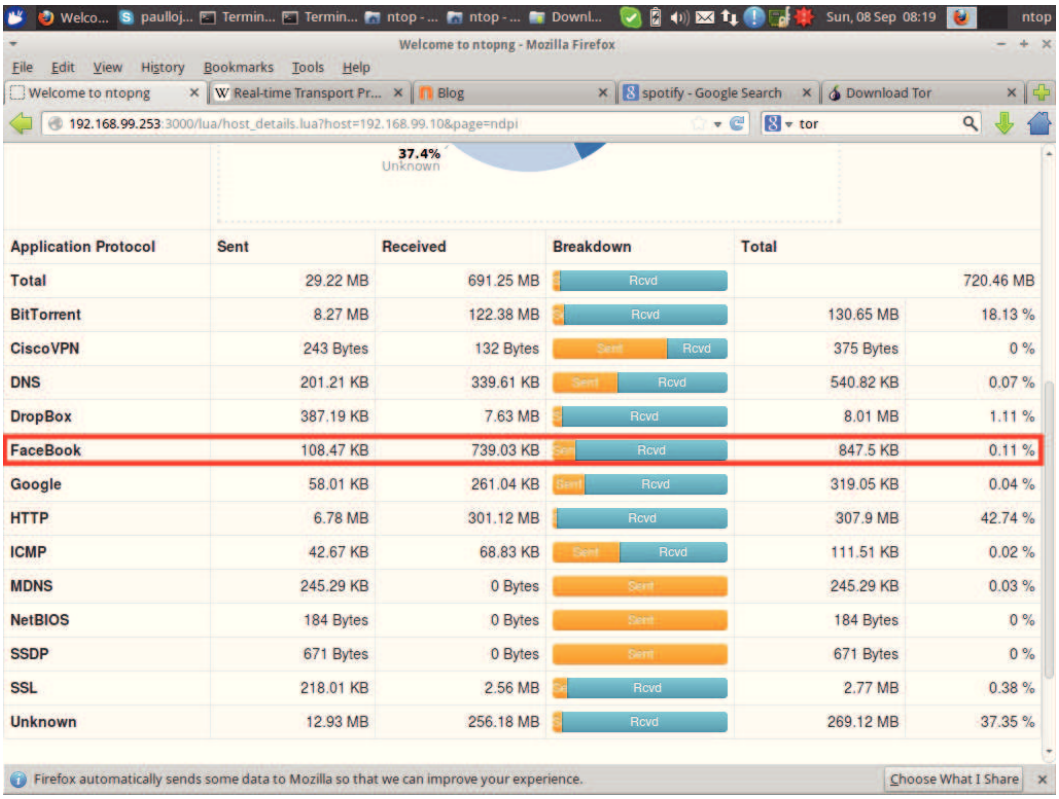


Figura 39 - Caraterização do tráfego associado ao serviço Facebook

Para além disso, é possível realizar um rastreio do tempo a que o utilizador ficou ligado àquela página, quantas vezes acedeu ao longo da última hora/dia recorrendo a uma análise dos *logs* disponibilizados.

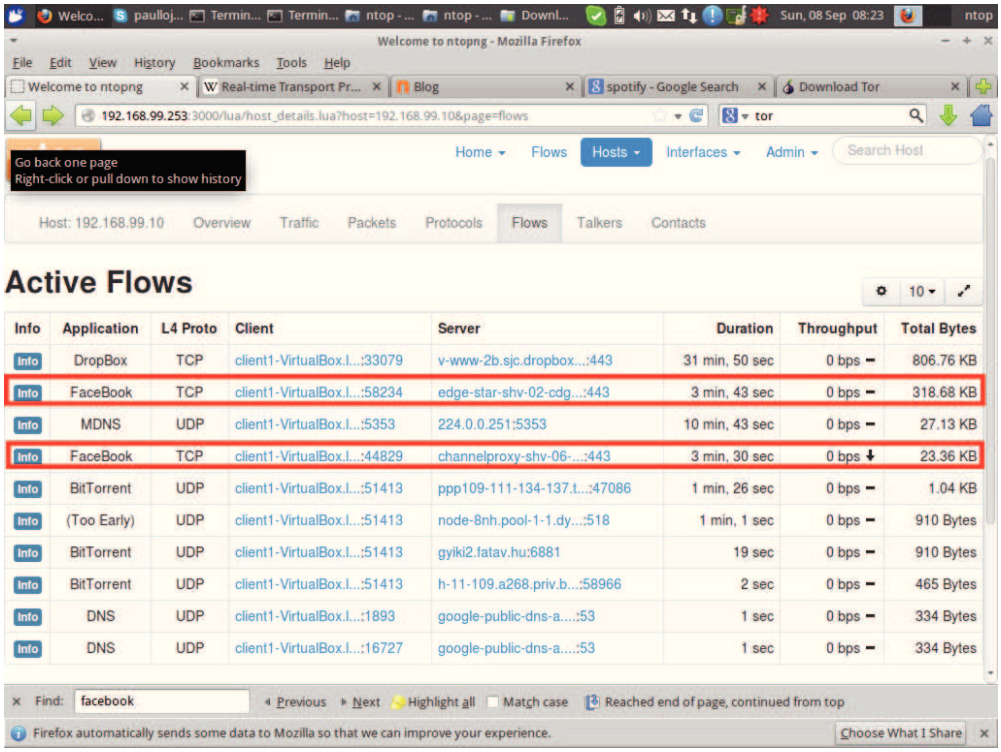


Figura 40 - Número de acessos ao Facebook

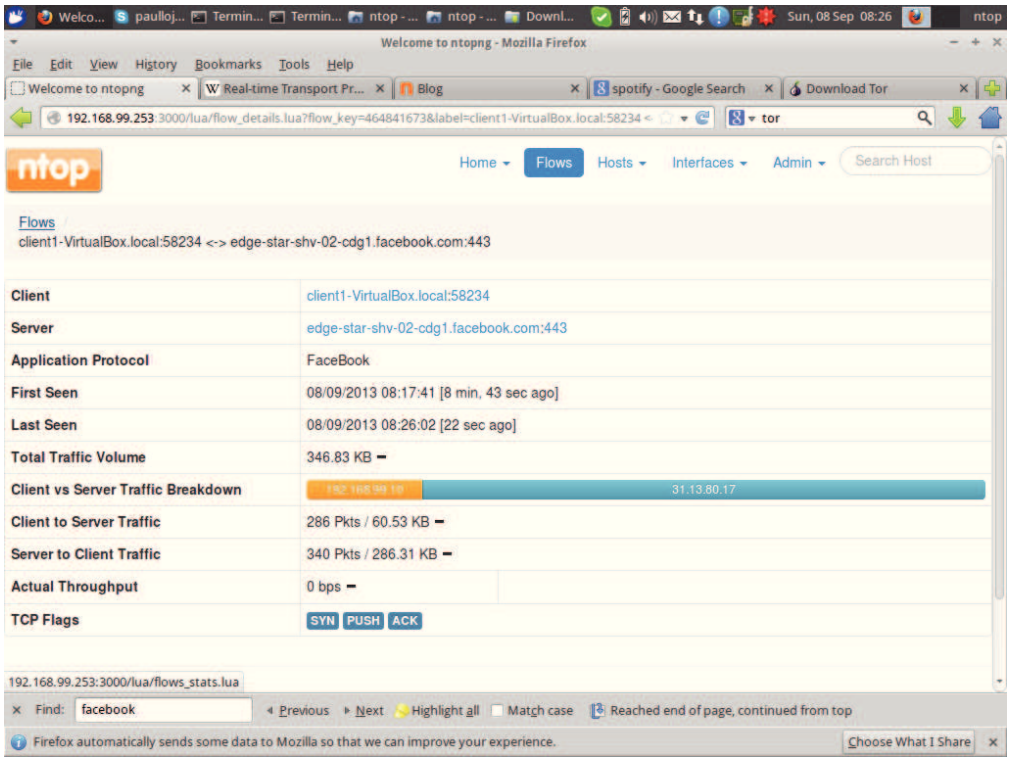


Figura 41 - Informação detalhada do primeiro acesso

9.6 Síntese

Neste capítulo foi apresentado um cenário de testes que teve como objetivo validar toda a solução implementada e proposta. Como seria de esperar, não foi de todo possível testar todas as funcionalidades existentes nas ferramentas utilizadas para a criação de um *gateway* associado ao avançado sistema implementado que permite caracterizar todo o tráfego que circula pela rede. Apesar disso, e após o conjunto de testes efetuados, os resultados revelaram-se de fato muito interessantes e só vieram demonstrar os benefícios que um mecanismo de *Deep Packet Inspection* bem configurado numa rede *wireless* de âmbito alargado pode trazer aos administradores de sistemas da mesma.

A solução proposta revelou-se de fato muito prometedora, visto estarmos a falar de um conjunto de ferramentas utilizadas de código aberto, ou seja, sem qualquer tipo de custos, excetuando no tempo necessário à implementação e afinação das mesmas por parte dos técnicos especializados.

Capítulo 10

10 Conclusões

O objetivo inicial desta Dissertação era o definir e apresentar uma solução que permitisse realizar a análise e proceder a uma detalhada caracterização do tráfego que circula numa rede *wireless* de âmbito alargado, ou seja, numa infraestrutura baseada em comunicações sem fios, recorrendo a um mecanismo de *Deep Packet Inspection*. Para a realização deste trabalho foi tido em conta a forma de funcionamento de uma rede do género que já se encontra em funcionamento há alguns anos e que tem sido um enorme caso de sucesso, para além de ser um excelente ecossistema de investigação, na freguesia da Memória.

Para conseguir cumprir os objetivos propostos, foi necessário realizar uma grande pesquisa de forma a perceber melhor o método de funcionamento das redes sem fios, os protocolos utilizados e as frequências/canais utilizados.

De seguida, realizou-se um estudo relativamente aos mecanismos de QoS orientados às telecomunicações para entender de que forma as aplicações são influenciadas. Também foram analisados os três principais modelos de QoS utilizados.

Os três capítulos seguintes permitiram perceber a importância do tema da segurança na área das telecomunicações, para além de descrever o enorme impacto que a evolução das *firewalls* teve ao longo dos anos. O sexto capítulo debruça-se num tema muito atual, e que é o principal tema desta dissertação - a tecnologia de *Deep Packet Inspection*.

Como foi explicado no capítulo 7, a arquitetura permitiu debater algumas das deficiências existentes quanto à análise e posterior caracterização do tráfego que circula numa rede sem fios de âmbito alargado. Daí debruçou-se sobre uma possível solução que pudesse minimizar essas deficiências.

Da arquitetura, e consequente análise dos problemas encontrados, resultou o planeamento e implementação de uma solução baseada em mecanismos de *Deep Packet Inspection* e na ideologia das *firewalls* de nova geração. Para isso, foram descritas as várias ferramentas utilizadas e a forma de implementação de cada um dos agentes envolvidos.

De forma a proceder à validação da solução implementada executaram-se alguns testes, apresentados no nono capítulo, que foram bastante importantes, pois aí constatou-se que a solução apresentada e implementada se encontrava realmente funcional. A caracterização do tráfego apresentada foi de tal forma detalhada que os administradores deste tipo de infraestruturas podem utilizar toda essa informação para criarem regras de QoS adaptadas a cada caso. Usualmente isso não acontece, pois normalmente é utilizado um determinado conjunto de regras que diferencia especificamente algum tipo de tráfego recorrendo a um escasso número de classes, o que se revela muito ineficaz, pela capacidade das aplicações mais modernas, que são desenvolvidas de raiz a pensar nessa situação, em recorrer a avançadíssimos mecanismos de *port hopping*.

Como se pode comprovar, e após a finalização de todo este trabalho, a solução apresentada revelou de fato que pode ser uma mais-valia para cenários deste género, visto permitir analisar e caraterizar de forma muito detalhada todo o tráfego que por lá circula. Para além disso, também a criação de uma base de dados com toda esta informação, e localizada num diferente local, no *gateway*, pode ser mais um

componente de fácil integração em ferramentas de monitorização, ou mesmo, como repositório de informação atualizada para aplicação de regras de qualidade de serviço dinâmicas. Toda essa informação pode ser muito valiosa para otimizar a reduzida largura de banda usualmente existente nestes casos de estudo, recorrendo à criação de regras de QoS específicas para cada caso, e não como acontece, onde são criadas recorrendo ao que se perspetiva que por lá circule.

10.1 Trabalho futuro

Quanto ao trabalho futuro gostaria de apresentar alguns pontos onde a solução idealizada pode ser melhorada ou mesmo integrada com o que já existe:

- Implementar todo o trabalho aqui descrito num cenário real, preferencialmente naquele que foi aqui tido em conta, ou seja, na rede sem fios de âmbito alargado da freguesia da Memória de forma a entender a eficiência do mesmo aquando da análise e caracterização de tráfego num ambiente constituído por dezenas de utilizadores;

- Integrar este projeto com o que já existe feito nessa rede comunitária a nível de QoS e monitorização da rede - integração com o Nagios. Para isso terá que ser estudado de que forma é que se podem manter a classes já existentes e qual a melhor maneira de integrar novas classes direcionadas para os utilizadores que tenham hábitos de utilização do serviço que prejudiquem os restantes;

- Analisar a possibilidade de criar uma solução completa que consista num ecossistema que fosse capaz de proceder à análise e caracterização de tráfego, aplicar regras em tempo-real de QoS, utilizando os dados analisados, e enviar relatórios do estado deste género de infraestruturas de rede em *real time*. Seria interessante utilizar apenas ideologias modernas, com recurso a mecanismos de *Deep Packet Inspection* e *firewalls* de nova geração, descartando assim os velhos hábitos que todo o tráfego é "bem comportado" esquecendo assim que atualmente se utilizam avançadíssimos algoritmos aquando do desenvolvimento de aplicações para contornar todo e qualquer género de restrição numa rede.

Bibliografia

[Aboul-Magd, 2011] – Aboul-Magd, O., "Wireless Local Area Networks Quality of Service: An Engineering Perspective", John Wiley & Sons, 2011.

[Blum et all, 2011] – Blum, R., & Bresnahan, C., "Linux Command Line and Shell Scripting Bible", John Wiley & Sons, 2011.

[Bujlow et all, 2013] – Bujlow, T., & Carela-Español, V., & Barlet-Ros, P., "Comparison of Deep Packet Inspection (DPI) Tools for Traffic Classification", 2013.

[Cisco, 2001] – Cisco Press, "Internet Quality of Service", 2001.

[Cisco, 2004] – Cisco Press, "End-to-End QoS Network Design: Quality of Service in LANs, WANs and VPNs", 2004.

[Cisco, 2007] – Cisco Systems, Inc., "Link Efficiency Mechanisms Overview", 2007.

[Cisco, 2011] – Cisco Systems, Inc. (s.d.). *Quality of Service (QoS)*, "Internetworking Technology Handbook": http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.html, 2011.

[Cisco,2011] – Cisco Systems, Inc. (s.d.). *Quality of Service Overview.*, "Cisco IOS Quality of Service Solutions Configuration Guide": http://www.europe.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_overview_ps6350_TSD_Products_Configuration_Guide_Chapter.html, 2010.

[Cordeiro et all,2006] – Cordeiro, C., Challapali, K., & Birru, D., "IEEE 802.22. Journal of Communications", 2006.

[Costa et all, 2009] – Costa, A., & Nobre, T.,"*Redes Wireless de Banda Larga",* Instituto Politécnico de Leiria, 2009.

[Dubrawsky, 2010] – Dubrawsky, I., "Firewall Evolution - Deep Packet Inspection", Symantec, 2010.

[ESTG, 2009] – ESTG, Instituto Politécnico de Leiria, "Modelos e Mecanismos de QoS. *Serviços Multimédia"*, Instituto Politécnico de Leiria, 2009.

[Frazão, 2011] – Frazão, L., "Gestão de Redes Wireless de Banda Larga em Ambientes Rurais", – Instituto Politécnico de Leiria, 2011.

[Fuentes et all, 2010] – Fuentes, D., & Jorge, P., "Albergaria Digital", projeto de planeamento de redes informáticas – Instituto Politécnico de Leiria, 2010.

[Fuentes et all, 2011] – Fuentes, D., & Jorge, P., "Redes Wireless do Futuro – Monitorização e Gestão Automática da Rede", projeto informático – Instituto Politécnico de Leiria, 2011.

[Guelich et all, 2000] – Guelich, S., & Gundavaram, S., & Birznieks, G., "CGI Programming with Perl", O'Reilly, 2000.

[IEEE, 2005] – IEEE - Institute of Electrical and Electronics Engineers,"*IEEE 802.15 Working Group for Wireless Personal Area Networks"*, http://www.ieee802.org/15/about.html, 2005.

[IEEE, 2010] – IEEE - Institute of Electrical and Electronics Engineers,"*The IEEE 802.16 Working Group on Broadband Wireless Access Standards"*, http://www.ieee802.org/16/, 2010.

[IEEE, 2011] – IEEE - Institute of Electrical and Electronics Engineers, "*IEEE 802.11 WIRELESS LOCAL AREA NETWORKS",* http://www.ieee802.org/11/, 2011.

[Keil, 2009] – Keil, M., "What's the biggest firewall issue for enterpresises?", Palo Alto Networks, 2009.

[Lash, 2001] – Lash, D., "The Web Wizard's Guide to PERL and CGI", Prentice Hall, 2001.

[Marcelino, 2008] – Marcelino, I., "Estruturação de um sistema de monitorização remota e de prevenção de infoexclusão de idosos no seu domicílio", Tese de Mestrado – Universidade de Trás-os-Montes e Alto Douro, 2008.

[Meddeb, 2010] – Meddeb, A., "Internet QoS: Pieces of the Puzzle", IEEE Commun. Mag., vol. 48, no. 2, pp. 86-94 2010.

[Palo Alto, 2010] – Palo Alto Networks, "The Application Usage and Risk Report – An Analysis of End User Application Trends in the Enterprise", Spring, 2010.

[Pathan, 2013] – Pathan, A., & Monowar, M., "Building Next-Generation Converged Networks: Theory and Practice", CRC Press, 2013.

[Patwardhan et all, 2002] – Patwardhan, N., & Siever, E., & Spainhour, S., "Perl in a Nutshell", O'Reilly, 2002.

[Pereira, 2006] – Pereira, A., "Mapeamento entre Arquiteturas de Serviços Integrados e de Serviços Diferenciados para suporte de Qualidade de Serviço na Internet", Tese de Doutoramento – Universidade de Coimbra, 2006.

[Rankin et all, 2010] – Rankin, K.,& Hill, B., "The Official Ubuntu Server Book", Prentice Hall, 2010.

[Salvador, 2008] – Salvador, N., "*Modelo de Gestão para Redes Wireless Banda Larga",* Tese de Mestrado – Universidade de Trás-os-Montes e Alto Douro, 2008.

[SANS, 2001] – SANS Institute InfoSec Reading Room, "Network Security Concepts and Essentials: A University Overview", SANS, 2001.

[Schmitt, 2001] – Schmitt, J., "Heterogeneous Network Quality of Service Systems", 2001.

[Selada, 2008] – Selada, R., *"Redes Wireless Banda Larga"*, 2008.

[Vugt, 2008] – Vugt, S.,"Pro Ubuntu Server Administration", APRESS, 2008.

[Wagner, 2009] – Wagner, B., "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'", 2009.

[Wikipédia,2011] – Wikipedia.org, *http://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg*, 2011.

[Xiao et all, 1999] – Xiao, X., & Ni, M. N., "Internet QoS: A Big Picture", IEEE Network, 1999.