

Junho de 2018

Relatório Final

Projeto Temático em Redes de Computadores

LICENCIATURA EM TECNOLOGIAS DA INFORMAÇÃO

RELATÓRIO FINAL NO ÂMBITO DA UNIDADE
CURRICULAR PROJETO TEMÁTICO EM REDES DE
COMPUTADORES

Autores:

Carlos Girão (82007)

Cláudio Cardoso Cruz (81607)

Pedro Moreno (87989)

Ricardo Balreira (88078)

Rodrigo Tavares (81544)

Junho de 2018

Relatório Final
Projeto Temático em Redes de Computadores

Relatório Final no âmbito da unidade curricular
Projeto Temático em Redes de Computadores da
Licenciatura em Tecnologias da Informação,
realizado no ano letivo 2017/2018 em Águeda, sob
orientação dos Professores Joaquim Ferreira e
Ricardo Marau, docentes da unidade curricular.

Autores:

Carlos Girão (82007)

Cláudio Cardoso Cruz (81607)

David Andrade Duarte (81572)

Pedro Moreno (87989)

Ricardo Balreira (88078)

Rodrigo Tavares (5144)

“O teu trabalho vai ocupar grande parte da tua vida,
e a única maneira de ficar verdadeiramente satisfeito
é fazer o que tu acreditas ser um bom trabalho. E a
única maneira de fazer um bom trabalho é amar o
que
fazes. Se ainda não o encontraste, continua a
procurar.
Não te acomodes. Tal como todas as outras
questões
do coração, tu saberás quando o encontrares.”

Steve Jobs

Grupo 2:

Carlos Girão 82007

Cláudio Cruz 81607

Pedro Moreno 87989

Ricardo Balreira 88078

Rodrigo Tavares 81544

Resumo

Serve o presente relatório de suporte inicial ao orientador do projeto e que visa reunir e tratar de todas as etapas que nos foram solicitadas, de modo a tornar possível alcançar os objetivos propostos ao nosso grupo de trabalho. Este documento destina-se a orientar o docente pelas várias fases deste projeto, bem como elucidá-lo em relação a tudo o que foi planeado e, posteriormente, realizado.

A proposta para este projeto foi a instalação de um protótipo de rede empresarial. De modo a emular esta mesma rede com a maior eficácia foi utilizado o software GNS3, sendo este um emulador de software para redes que permite a combinação de dispositivos virtuais e reais para simular redes complexas, baseando-se numa combinação de software de emulação Dynamips para hospedar imagens do Cisco IOS e Virtual PC Simulator para simular hosts de rede, integrando-se, também, com máquinas virtuais QEMU e VirtualBox.

Relativamente à rede da empresa, esta deveria incluir componentes específicas, tais como: suporte de encaminhamento (OSPF), tradução de endereços de rede (NAT), servidores DHCP e DNS, firewall e proxy, não esquecendo as normas de segurança que uma rede empresarial deve conter. Assim sendo, foi conveniente atribuir a cada departamento uma única identificação através de um endereço, respeitando os critérios envolventes nos serviços de segurança e configuração da rede. Definiu-se, também, um endereço do protocolo IP em volta dos edifícios de forma a abranger todas as redes IP existentes nos mesmos.

Neste documento está presente a estrutura do trabalho onde inclui a planificação do mesmo, bem como o levantamento dos requisitos (funcionais e não funcionais), o orçamento da solução da rede e as diversas etapas da configuração da rede de uma forma bem explícita, com o objetivo de esclarecer ao leitor, de forma clarividente, como foi efetuada cada tarefa.

Índice

1. INTRODUÇÃO	1
2. PLANIFICAÇÃO DO TRABALHO.....	3
2.1 Requisitos.....	3
2.2 Infraestrutura de Rede	4
3. ORÇAMENTO DA SOLUÇÃO.....	5
4. DESCRIÇÃO DAS ATIVIDADES DESENVOLVIDAS	7
4.1 OSPF	7
4.1.1 Configuração OSPF.....	9
4.2 NAT	13
4.2.1 Configuração NAT	13
4.3 DHCP	19
4.3.1 Configuração DHCP	20
4.4 DNS.....	25
4.4.1 Configuração DNS	25
4.5 FIREWALL	29
4.5.1 Configuração da Firewall	29
4.6 PROXY	37
4.6.1 Instalação e configuração do programa Squid	37
4.7 TFTP	41
4.7.1 Configuração	42
4.8 SNMP	45
4.9 VPN.....	47
4.10 WEB SERVER.....	49
4.10.1 Implementação do Web Server.....	50
5. BIBLIOGRAFIA.....	52

Índice de figuras

Figura 1 - OSPF packet header	8
Figura 2 - Esquema de rede	9
Figura 3 - Configuração do OSPF (ISP).....	10
Figura 4 - Configuração do OSPF (Eng_Com).....	11
Figura 5 - Configuração do OSPF (Datacenter)	11
Figura 6 - Configuração do OSPF (Gestão)	11
Figura 7 - Definição das redes interna e externa.....	14
Figura 8 - ACLs padrão para tradução das redes dos Departamentos.....	15
Figura 9 - Associação das lista criada à interface externa do router ISP	15
Figura 10 - Atribuição do name server	16
Figura 11 - Comando IP domain-lookup.....	16
Figura 12 - Teste do envio de pedidos por ping	16
Figura 13 - Lista das traduções por parte do NAT	17
Figura 14 - Criação das pools por DHCP	21
Figura 15 - Configuração do DHCP Relay Agent	22
Figura 16 - Atribuição de IP dinâmico ao PC	23
Figura 17 - Processo de aluguer quatro fases	23
Figura 18 - Lista específica dos clientes (PCs) e routers vizinhos	24
Figura 19 - Configuração de exclusão de endereços IP	24
Figura 20 - Ativação do servidor DNS e DNS primary.....	26
Figura 21 - Nomeação dos hostnames e configuração do Name server e NS-Record	26
Figura 22 - Domain-lookup.....	26
Figura 23 - Servidor DNS como Name server	26
Figura 24 - Resolução de nomes por parte do router ISP	27
Figura 25 - Ping para o DNS do Facebook no PC1	27
Figura 26 - Resolução dos nomes por parte de um router de um Departamento	27
Figura 27 - Exemplo de ACL	30
Figura 28 - ACL estendida	31
Figura 29 - ACL padrão	31
Figura 30 - Parâmetros da ACL estendida	32
Figura 31 - Parâmetros da ACL padrão	32
Figura 32 - ACLs criadas para a firewall	34
Figura 33 - Aplicação da lista na interface do router ISP.....	34
Figura 34 - Visualização do comando no show running config.....	35

Figura 35 - Teste se a firewall está funcional	35
Figura 36 - Instalação Squid	37
Figura 37 - Hostname Proxy	38
Figura 38 - Lista de redes afetadas pelo proxy	39
Figura 39 – Ficheiro tftp-hpa de base	42
Figura 40 - Ficheiro tftp-hpa alterado	42
Figura 41 – Index default do servidor apache	50
Figura 42 – Código HTML do servidor Apache	51
Figura 43 – Index final do servidor Apache	51

1. Introdução

No âmbito do Projeto Temático em Redes de Computadores, foi proposto o desenvolvimento de uma rede informática que fosse de encontro aos requisitos descritos numa folha de atividade entregue ao presente grupo. Como tal, e tendo em vista parte da sua implementação, esta primeira foi feita através de um simulador de redes (GNS3) e a restante parte foi implementada fisicamente com o auxílio a hardware existente e disponibilizado pela ESTGA. Foi encarregue aos professores Joaquim Ferreira e Ricardo Marau, responsáveis pela orientação dos grupos, toda a supervisão e direção durante o desenvolvimento deste projeto. De modo a garantir um bom desenvolvimento, coordenado, profissional e bem estruturado, utilizaram-se ferramentas de apoio ao projeto, tais como o mapa de Gantt para controlar e ilustrar o desenvolvimento e tempos das diferentes etapas do mesmo. Utilizou-se também o Git como repositório centralizado do trabalho, permitindo assim um acesso mais facilitado por parte de todos os elementos integrantes do grupo à versão mais atualizada do projeto.

Em suma o trabalho consistiu na realização e implementação de um protótipo de rede empresarial instituindo quatro departamentos em três edifícios respeitando os serviços de segurança, atribuindo a cada departamento uma única identificação através de um endereço, respeitando os critérios envolventes nos serviços de segurança e configuração da rede. Também se definiu um endereço do protocolo IP em volta dos edifícios de forma a abranger todas as redes IP existentes nos mesmos.

Nesta terceira versão do relatório serão debatidos os seguintes aspetos: os requisitos funcionais e não funcionais que fundamentam a estrutura do projeto; a infraestrutura da rede que fundamenta a estrutura do projeto; esquematização, configuração e disposição da rede básica simulada no GNS3, bem como outros novos complementos – proxy, firewall e serviços TFTP, VPN, SNMP e Web server; levantamento de um novo orçamento tendo em conta os equipamentos necessários para implementar uma rede física; planificação e a forma como foram distribuídas as tarefas por todos os elementos do grupo.

2. Planificação do trabalho

2.1 Requisitos

Com a plenitude de descrever de forma explícita e concreta o funcionamento que se prevê na implementação de um protótipo de rede empresarial, foram estabelecidos os requisitos funcionais e não funcionais mediante o contexto do problema.

No que respeita aos requisitos funcionais, estes encontram-se abaixo discriminados:

- Atribuição dos endereços IP para cada departamento (Datacenter, Dep. Engenharia, Dep. Gestão e Dep. Comercial), bem como em cada edifício;
- Segmentação da intranet pelas várias redes IP;
- Encaminhamento dinâmico na intranet;
- Implementação dos serviços SNMP, TFTP, proxy, DNS, DHCP e NAT na rede;
- Fornecimento de endereços IP dinâmicos a todas as máquinas cliente;
- Utilização de encaminhamento dinâmico na intranet;
- Atribuição de um endereço IP predefinido ao ISP;
- Proteção de toda a rede empresarial por firewall não excluindo o funcionamento estrito dos serviços de rede;

Contextualizando os requisitos não funcionais, estão definidos no texto seguinte:

- Suporte de 20, 10, 40 e 100 máquinas para o Datacenter, Dep. Gestão, Dep. Comercial e Dep. Engenharia, respetivamente;
- Implementação da tecnologia cablada Ethernet em todas as redes IP e rede wireless nos departamentos Comercial e de Engenharia;
- Interligação da intranet com um fornecedor de acesso à internet (ISP) no edifício 1;
- Conectividade entre todos os edifícios e departamentos;
- Acessibilidade à sua rede interna apenas por parte dos departamentos Comercial e de Engenharia;
- Suporte de endereços IP classe C em toda a rede;
- Identificação de cada edifício e departamento por um endereço IP de forma a ser o seu único domínio (identificador);
- Acesso à intranet exterior por parte das máquinas nos departamentos;

- Enumeração das máquinas e routers num ficheiro de configuração para possível consulta;
- Armazenamento dos backups num diretório para cada router;
- Implementação do daemon que irá estar encarregue de ser executado em segundo plano.

2.2 Infraestrutura de Rede

Em relação à realização das tarefas, estas estiveram em torno de simular a rede descrita anteriormente no programa GNS3, configurando a rede básica. As tarefas desempenhadas envolveram-se no seguinte: configurar o encaminhamento dinâmico (OSPF, de forma a cada router conhecer as redes que o interliga), o protocolo DHCP (responsável por atribuir endereços IP dinâmicos às máquinas), o protocolo NAT (traduz os endereços IP privados das máquinas de uma rede em endereços IP públicos de forma a terem acesso à rede exterior (Internet)) e o protocolo DNS (desempenha o papel de resolução de nomes e permite que uma máquina seja nomeado por um nome ao critério da pessoa). Acrescentou-se ainda um servidor proxy (funciona como suporte entre a máquina e o servidor de forma a assegurar o acesso da máquina à Internet) e uma firewall (permite controlar todos os pedidos e pacotes que chegam ao servidor com firewall).

3. Orçamento da Solução

(Enviado em anexo)

4. Descrição das Atividades Desenvolvidas

4.1 OSPF

O OSPF, sigla usada como abreviatura para “Open Shortest Path First” é um protocolo utilizado para traçar rotas de redes. Este foi desenvolvido devido à necessidade de se implementar um IGP (Internal Gateway Protocol) para a comunidade da internet. O protocolo OSPF tem por base a tecnologia link-state, em que cada nó da rede constrói um mapa da sua conectividade com a mesma, o que permite que seja construído e calculado o caminho mais curto para qualquer destino conhecido.

No protocolo OSPF as atualizações das bases de dados dos routers são menos frequentes e são instantâneas, ao contrário das atualizações numa rede RIP que demora muito mais tempo uma vez que as bases de dados só vão sendo atualizadas quando informações antigas expiram. A desvantagem dos primeiros algoritmos para calcular os caminhos mais curtos, é que estes exigiam muitos ciclos de memória e CPU.

Assim, a terminologia do algoritmo OSPF é discutida entre as vantagens e desvantagens do protocolo para um projeto de redes de grande dimensão.

O OSPF é um protocolo link-state. Deste modo podemos considerar que um link é uma interface do router e o estado do link é uma descrição dessa mesma interface e do seu relacionamento para com os routers vizinhos. A descrição das interfaces devem de incluir, por exemplo, o endereço IP da interface, a máscara, o tipo de rede ao qual ela está conectada, os routers ligados à rede, etc. Todos estes link-states são posteriormente armazenados e guardados numa base de dados para cada um dos routers da rede.

Este introduziu novos conceitos para a comunidade, como a autenticação de atualizações de roteamento, as Variable Length Subnet Masks (VLSM), o resumo de rotas.

Version	Type	Packet Length
Router ID		
Area ID		
Checksum		Authentication Type
Authentication Data		

Figura 1 - OSPF packet header

O OSPF usa um algoritmo chamado Dijkstra para determinar o caminho mais curto, este calcula o caminho mais curto para cada destino com base nos custos cumulativos exigidos para alcançar esse destino. De uma maneira superficial o algoritmo funciona da seguinte forma:

Inicialmente o router gera um anúncio *link-state*, este representa o conjunto de todos os *link-states* que o router tem. De seguida cada router que receber uma atualização para um determinado *link-state* deve de armazenar uma cópia na sua base de dados e, em seguida, deve de transmitir essa atualização aos outros routers. Após isso o router usa o algoritmo Dijkstra de modo a determinar a ramificação de caminho mais curto.

Os destinos, os custos associados e o salto do nó seguinte dão origem à tabela de roteamento de IP. Se não existirem alterações para a rede OSPF, como por exemplo a alteração do custo de um link, o OSPF não irá fazer nada até que haja uma alteração. Assim todas as mudanças que ocorrerem são comunicadas por meio de pacotes *link-state*, e o algoritmo Dijkstra é recalculado para localizar o novo caminho mais curto.

4.1.1 Configuração OSPF

De modo a realizar o encaminhamento dinâmico para este esquema de rede apresentado na figura abaixo começou-se por abrir o terminal de todos os routers Datacenter, ISP, Eng_Com e Gestão.

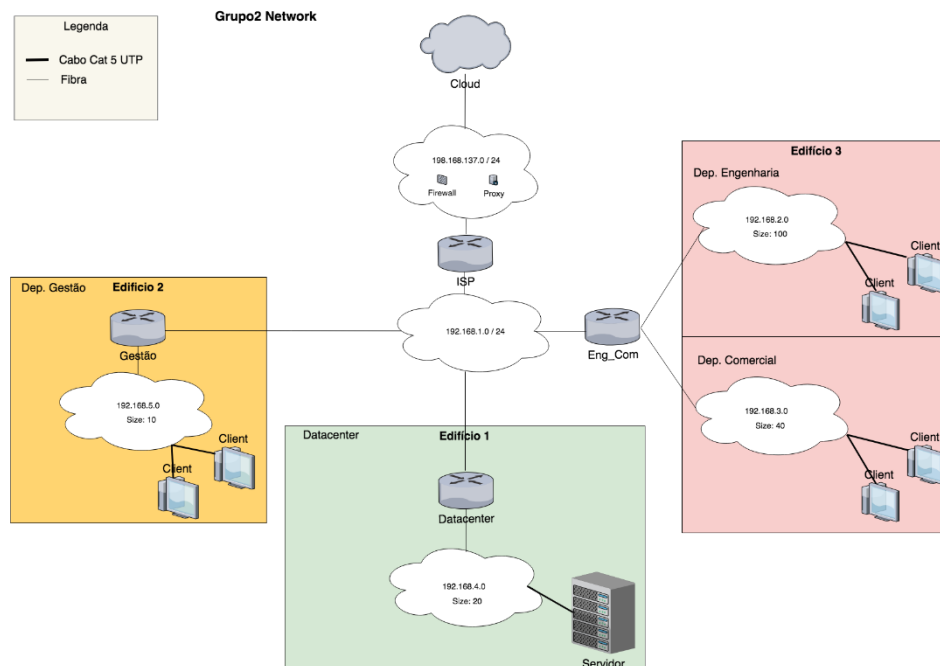


Figura 2 - Esquema de rede

Após a abertura dos quatro terminais foram escritos os mesmos 5 comandos de configuração para todos os routers à exceção do router ISP que necessitou de mais um comando extra.

Para cada um dos quatro routers começou-se por digitar o comando “router ospf 1”. Este comando cria um processo de *routing* OSPF onde o utilizador entra em modo de configuração do OSPF para aquele router. De um modo geral o process_id é apenas um identificador interno utilizado para o processo de *routing*.

Neste caso o valor atribuído foi 1, no entanto poderia ser qualquer outro inteiro positivo, uma vez que este ID não se faz corresponder em mais nenhum dispositivo da rede (Figura 2).

```
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 192.168.1.0 0.0.0.255 area 0
network 192.168.229.0 0.0.0.255 area 0
default-information originate
```

Figura 3 - Configuração do OSPF (ISP)

De seguida foi executado o comando router-id que após entrarmos em modo de configuração do router OSPF, é utilizado para se configurar um determinado ID para cada um dos routers, assim, foram atribuídos os seguintes IDs a cada um dos routers da rede (Figura 3).

- ISP: 1.1.1.1 (Figura 2)
- Eng_Com: 2.2.2.2 (Figura 3)
- Datacenter: 3.3.3.3 (Figura 4)
- Gestao: 4.4.4.4 (Figura 5)

Após a execução deste comando o terminal responde com a mensagem “log-adjacency-changes” que notifica alterações de alto nível no estado do relacionamento (Figura 3).

```
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
```

Figura 4 - Configuração do OSPF (Eng_Com)

Prontamente foi implementado o comando network que define os endereços IP nos quais o OSPF é executado bem como o ID da área para essa interface. Ou seja, neste comando são especificadas todas as redes vizinhas que o router atual vai conhecer.

```
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
network 192.168.1.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
```

Figura 5 - Configuração do OSPF (Datacenter)

```
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
network 192.168.1.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
```

Figura 6 - Configuração do OSPF (Gestão)

Por fim, foi executado o comando “default-information originate” no entanto este último é apenas para o router ISP, este permite que os restantes routers que estão ligados ao router ISP possam conhecer a rota até à interface externa, sem que seja preciso criar uma rota estática para cada router. Assim, com esse comando todos os routers ficam automaticamente a conhecer a interface exterior do router ISP (Figura 2).

4.2 NAT

O NAT (*Network Address Translation*), permite que uma máquina com um endereço IP privado seja traduzido para um endereço IP público de forma a ter acesso à rede externa (Internet). Caso contrário, uma máquina com endereço IP privado nunca irá conseguir aceder à Internet pois esta mesma rede é constituída por endereços IP públicos.

Consiste, noutras palavras, num protocolo que atribui a uma máquina ou grupo de máquinas um endereço IP permitindo, assim, que naveguem e comuniquem com outras máquinas numa rede, não existindo limitações no endereçamento. Tal como o próprio nome indica, baseia-se na tradução dos endereços IP e portas TCP de uma dada rede local para a internet. Uma porta é um número inteiro que identifica determinado serviço ou aplicação, pelo que também pode ser utilizado no protocolo NAT para ser um meio de distinção de um conjunto de máquinas quando estas contêm o mesmo IP público.

4.2.1 Configuração NAT

Dando jus à configuração do NAT é necessário, em primeiro lugar, definir qual vai ser a rede interna e a rede externa (rede onde estará, eventualmente, a Internet). A rede interna é composta pela rede onde estão situadas todas as máquinas que se pretende traduzir para que possam ter acesso à rede externa, e a rede externa é, simplesmente, a Internet. Portanto, para cada interface do router ISP, router este que está ligado diretamente ao ISP (serviço que fornece Internet), é necessário definir a rede interna (*ip nat inside*) e a rede externa (*ip nat outside*), tal como mostra a figura. Basta aceder ao modo de configuração da consola (*configure terminal*) e inserir os comandos descritos anteriormente.

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet0/1
ip address dhcp
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
```

Figura 7 - Definição das redes interna e externa

Após a configuração da divisão das interfaces por redes interna e externa, deve-se criar as ACLs. Uma ACL tem como objetivo controlar todo o tráfego que passa pelo router com as ACLs criadas, de forma a permitir ou descartar determinados pacotes. Para o caso utilizaram-se ACLs padrão (<1-99>), que permitem ou descartam os pacotes para determinado endereço de origem com a máscara inversa (wild card). Na configuração abaixo, é possível ver que se criaram cinco ACLs padrão para que seja permitido que os pacotes vindos das redes de cada Departamento possam ser traduzidos pelo protocolo NAT e tenha acesso à Internet. Cada endereço de rede corresponde aos Departamentos, pois todas as redes, neste caso, continham máquinas com endereço IP privado (Figura 7). Havia outras maneiras de fazer, como por exemplo: criar apenas uma ACL que permitisse a passagem dos pacotes para qualquer rede (substituindo o endereço de rede pelo parâmetro *any*); ou então criar uma ACL estendida. Uma ACL estendida (<100-199>) já engloba a especificação do protocolo, endereço de origem e endereço de destino, serviço. Desta forma, outra alternativa seria criar uma ACL estendida que permitisse a passagem dos pacotes de qualquer rede (endereço de origem) para o endereço de destino do router ISP pelo protocolo IP (Internet Protocol) ou especificar cada rede dos Departamentos no endereço de origem, evitando assim o risco de ter o descontrolo total dos pacotes que são recebidos de endereços desconhecidos.


```
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
access-list 1 permit 192.168.5.0 0.0.0.255
access-list 1 permit 192.168.1.0 0.0.0.255
```

Figura 8 - ACLs padrão para tradução das redes dos Departamentos

Dando por terminada esta fase é necessário agora definir a lista ACL criada para a interface exterior do router ISP. Antes de tudo, é importante referir que há três maneiras de criar o protocolo NAT: NAT estático, NAT dinâmico e NAT *overload* (*Port Forwarding*).

No NAT estático, define-se um único IP estático a uma máquina. Por exemplo, existem 100 computadores; com o IP estático seria necessário definir um IP estático para cada PC, o que seria bastante trabalhoso.

O NAT dinâmico funciona por configuração de pools (conjunto de endereços IP endereçáveis para determinada rede), com o propósito de atribuir um IP dinâmico da pool a cada máquina. Tendo vários PCs, uma alternativa seria optar pelo NAT dinâmico criando uma pool com endereços IP públicos e atribuir dinamicamente a esse conjunto de PCs.

O NAT *overload* (PAT), tal como fora utilizado no projeto, permite que, utilizando o endereço IP da interface exterior do router com o protocolo NAT atribua a um conjunto de PCs. Estes PCs vão ser distinguidos pelo porto que lhes é atribuído, sendo o método mais utilizado nas topologias de rede.

Para a tradução dos PCs da rede interna, configurou-se o NAT *overload* para que cada PC possa ser diferenciado pelo porto, que é único, tal como se pode ver na figura 9.

```
ip nat inside source list 1 interface FastEthernet0/1 overload
```

Figura 9 - Associação das lista criada à interface externa do router ISP

Tendo em vista o comando acima, o NAT vai ser aplicado na rede interna (origem - source) com as ACLs definidas anteriormente com a caracterização do número um, pelo que vão ser traduzidas utilizando o IP da interface fastethernet 0/1 do router ISP por overload. Após a configuração do NAT, é necessário criar um name server (Figura 9) para um endereço IP externo e o “domain-lookup” para que o router conheça o servidor e ative o sistema de procura pelo domain-name (Figura 10).

```
ip name-server 8.8.8.8
```

Figura 10 - Atribuição do name server

```
(config)#ip domain-lookup  
(config)#
```

Figura 11 - Comando IP domain-lookup

Estando o NAT configurado, é altura de testar se a configuração foi feita corretamente.

Existe um comando que lista todas as traduções feitas quando há um PC que “pinga” para um endereço IP da rede externa, designado por “show ip nat translations” (Figura 12).

```
PC-1> ping 8.8.8.8  
64 bytes from 8.8.8.8 icmp_seq=1 ttl=43 time=180.624 ms  
64 bytes from 8.8.8.8 icmp_seq=2 ttl=43 time=88.079 ms  
64 bytes from 8.8.8.8 icmp_seq=3 ttl=43 time=108.568 ms  
64 bytes from 8.8.8.8 icmp_seq=4 ttl=43 time=77.034 ms  
64 bytes from 8.8.8.8 icmp_seq=5 ttl=43 time=88.059 ms  
  
PC-1> ping google.com  
google.com resolved to 172.217.17.14  
64 bytes from 172.217.17.14 icmp_seq=1 ttl=54 time=144.131 ms  
64 bytes from 172.217.17.14 icmp_seq=2 ttl=54 time=76.569 ms  
64 bytes from 172.217.17.14 icmp_seq=3 ttl=54 time=87.044 ms  
64 bytes from 172.217.17.14 icmp_seq=4 ttl=54 time=80.041 ms  
64 bytes from 172.217.17.14 icmp_seq=5 ttl=54 time=70.024 ms  
  
PC-1>
```

Figura 12 - Teste do envio de pedidos por ping

A figura acima confirma que o PC1 conseguiu encontrar o endereço IP do Google, incluindo o DNS (Figura 11).

```
ISP#sh ip nat translations
```

Proto	Inside global	Inside local	Outside local	Outside global
icmp	192.168.137.133:19597	192.168.5.2:19597	8.8.8.8:19597	8.8.8.8:19597
icmp	192.168.137.133:19853	192.168.5.2:19853	8.8.8.8:19853	8.8.8.8:19853
icmp	192.168.137.133:20109	192.168.5.2:20109	8.8.8.8:20109	8.8.8.8:20109
icmp	192.168.137.133:20365	192.168.5.2:20365	8.8.8.8:20365	8.8.8.8:20365
icmp	192.168.137.133:20621	192.168.5.2:20621	8.8.8.8:20621	8.8.8.8:20621
icmp	192.168.137.133:24461	192.168.5.2:24461	172.217.17.14:24461	172.217.17.14:24461
icmp	192.168.137.133:24717	192.168.5.2:24717	172.217.17.14:24717	172.217.17.14:24717
icmp	192.168.137.133:24973	192.168.5.2:24973	172.217.17.14:24973	172.217.17.14:24973
icmp	192.168.137.133:25229	192.168.5.2:25229	172.217.17.14:25229	172.217.17.14:25229
icmp	192.168.137.133:25485	192.168.5.2:25485	172.217.17.14:25485	172.217.17.14:25485

```
ISP#
```

Figura 13 - Lista das traduções por parte do NAT

Pela figura 12, pode-se ver que em ambos os pedidos (ping 8.8.8.8 e ping google.com) o PC foi traduzido com o IP da interface fastethernet 0/1 do router ISP, sendo o endereço 192.168.5.2 do próprio PC cujo pedido foi feito ao endereço externo 8.8.8.8. Em cada tradução, o número do porto varia pois são feitos novos pedidos, no entanto, é por este procedimento que as máquinas são distinguidas fora da rede interna. Para o caso do DNS do Google, o ocorrido é idêntico.

4.3 DHCP

O DHCP (Dynamic Host Configuration Protocol), um modelo cliente-servidor, consiste num protocolo de gestão centralizada dos endereços IP que são usados na rede permitindo assim fazer uma configuração automática e dinâmica de cada máquina que esteja ligada a uma rede TCP/IP.

Numa rede onde este protocolo esteja implementado, o cliente DHCP, um dispositivo de rede que possua a capacidade de adquirir as configurações TCP/IP de um servidor DHCP, tenta encontrar um ou mais servidores que ofereçam os padrões desejados a fim de possibilitar que a sua máquina possa ser configurada de uma forma autónoma. Graças ao DHCP, os dispositivos da rede recebem as configurações do servidor, e por sua vez, o utilizador não necessita de configurar manualmente os endereços IP.

De uma forma muito generalizada, o DHCP opera da seguinte forma:

- Quando uma máquina se liga a uma rede, o cliente DHCP envia um pacote UDP em *broadcast*, destinado a todas as máquinas da rede, com uma requisição DHCP;
- Qualquer servidor DHCP na rede poderá responder a essa requisição e manter a gestão dos endereços IP usados na rede e as informações sobre os parâmetros de configuração dos clientes, como o *gateway* padrão, nome do domínio, servidor de nomes e servidor de horário;
- O servidor DHCP que acolha este pacote responderá ao cliente, que efetuou o pedido, com um pacote com configurações onde constará, pelo menos, um endereço IP e uma máscara de rede, além de dados opcionais, como o *gateway*, servidores de DNS, etc.

4.3.1 Configuração DHCP

Para a configuração do protocolo DHCP, com os respetivos clientes e servidor, foi tomado como base o seguinte esquema de rede apresentado na figura x acima.

Inicialmente a configuração do DHCP começou no router ISP, definindo-o como o DHCP server. De seguida, entrou-se no modo de configuração do terminal, através do comando “configure terminal”, a fim de se estabelecer as pools de forma a atribuir IPs dinâmicos às máquinas, mediante a rede. As pools são definidas como um conjunto de IPs endereçáveis. Configurou-se então quatro pools para cada rede que representa cada departamento, ou seja, cada cliente DHCP. Inseriu-se então o comando “ip dhcp pool cliente”, sendo o parâmetro cliente o nome da pool de endereços do servidor, ao critério da pessoa (Figura 13).

Posto isto, introduziu-se o comando “network 192.168.1.0 /24”, de modo a especificar o número da sub-rede e a máscara do pool de endereços DHCP, e, posteriormente, o endereço IP do DNS server através do comando “dns-server 192.168.x.x”. O comando “default-router 192.168.x.x” explicita o endereço IP da interface do router na rede a que diz respeito a pool que está a ser configurada.

Por exemplo, está a ser definida a pool para o departamento de Gestão, a “network” vai ser o endereço de rede 192.168.5.0 /24 e o “default-router” o IP 192.168.5.1. De referir que este mesmo processo foi efetuado para cada router dos departamentos, devido ao facto de ser necessário efetuá-lo para cada cliente DHCP da rede.

Configurou-se também, sendo um comando facultativo, a duração do lease (“lease” significa renda, aluguer), que é o tempo em que o IP se encontra válido. Estabeleceu-se então 7 dias para cada pool criada.

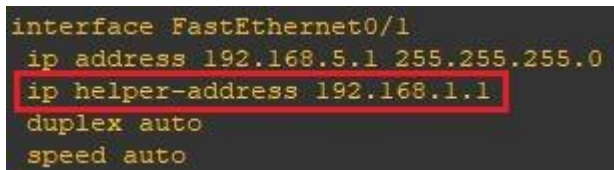
Posto isto, para se ter acesso à configuração do router, basta inserir o comando “do show running”, caso o utilizador esteja dentro do modo de configuração de modo a apresentar toda a configuração efectuada anteriormente. Caso contrário, é apenas “show running”.

```
ip dhcp pool Gestao
  network 192.168.5.0 255.255.255.0
  default-router 192.168.5.1
  dns-server 192.168.1.1
  domain-name grupo2.local
  lease 7 2 30
!
ip dhcp pool Datacenter
  network 192.168.4.0 255.255.255.0
  default-router 192.168.4.1
  dns-server 192.168.1.1
  domain-name grupo2.local
  lease 7 2 30
!
ip dhcp pool Engenharia
  network 192.168.2.0 255.255.255.0
  default-router 192.168.2.1
  dns-server 192.168.1.1
  domain-name grupo2.local
  lease 7 2 30
!
ip dhcp pool Comercial
  network 192.168.3.0 255.255.255.0
  default-router 192.168.3.1
  dns-server 192.168.1.1
  domain-name grupo2.local
  lease 7 2 30
```

Figura 14 - Criação das pools por DHCP

A comunicação inicial com o servidor DHCP é feita mediante o uso de *broadcasts*. Mas como a maior parte dos routers rejeitam o facto de deixar passar os *broadcasts*, seria necessário instalar um servidor DHCP em cada segmento da rede. No entanto, para uma rede real, em termos financeiros, iria ser muito mais dispendioso. Para resolver este problema existem três opções: configurar os routers de forma a deixarem passar os *broadcasts*; instalar um servidor DHCP em cada segmento; instalar o serviço DHCP *Relay Agent* numa máquina do segmento onde estão os clientes dinâmicos. A forma mais simples e económica seria instalar um serviço DHCP *Relay Agent* em cada router, para que o *broadcast* saia da rede local (LAN). O DHCP *Relay* funciona da seguinte forma: uma máquina envia pedido para atribuição de IP. Como ele não tem qualquer conhecimento da LAN, envia um broadcast, e como o papel do router é descartar o tráfego broadcast, o pedido nunca chega ao servidor DHCP. O DHCP *Relay* permite que o tráfego broadcast passe através do router até ao router. Desta forma, a configuração do DHCP *Relay Agent* nos restantes routers: **Gestão**, **Datacenter** e **Eng_Com**. Para isso, acede-se a cada interface dos routers que estejam com máquinas na rede para receberem IP dinâmico e insere-se o comando “ip helper-address 192.168.x.x”.

Todas as redes que contiverem PCs, deve-se aceder à respetiva interface do router que está ligada diretamente e executar o comando anterior. Por exemplo, para o router Gestão faz-se o seguinte: acede-se à interface *fastethernet* 0/1, pois tem PCs conectados nessa mesma rede e procede-se à execução do comando “ip helper-address 192.168.1.1”, cujo endereço IP representa a interface *fastethernet* 0/0 do router ISP (servidor DHCP) (Figura 14). O procedimento é igual para os restantes routers clientes.



```
interface FastEthernet0/1
ip address 192.168.5.1 255.255.255.0
ip helper-address 192.168.1.1
duplex auto
speed auto
```

Figura 15 - Configuração do DHCP Relay Agent

O DHCP *Relay*, noutras palavras, funciona como um agente de retransmissão DHCP encaminhando os pedidos DHCP entre clientes, quando eles não pertencem à mesma rede, permitindo assim que o tráfego de transmissão passe pelo router (cliente).

Concluída a configuração, é altura de testar se o DHCP funciona corretamente. Como tal, basta abrir o terminal de um PC cliente e inserir o “ip dhcp”, tal como mostra a figura 15. Pela figura é possível ver toda a informação de atribuição de IP na máquina, tal como fora feito anteriormente nas *pools* no router ISP. O elemento “DDORA” que se obtém na resposta ao “ip dhcp” valida o processo de aluguer. O processo de aluguer é constituído por quatro fases (*Discover*, *Offer*, *Request*, *Acknowledgement*), tal como se pode ver na figura. A imagem 16 especifica o caminho que é percorrido após o envio de um pedido ao servidor DHCP.


```
PC-2> ip dhcp
DDORA IP 192.168.4.2/24 GW 192.168.4.1

PC-2> sh ip

NAME       : PC-2[1]
IP/MASK    : 192.168.4.2/24
GATEWAY    : 192.168.4.1
DNS        : 192.168.1.1
DHCP SERVER : 192.168.1.1
DHCP LEASE : 613798, 613800/306900/537075
DOMAIN NAME : grupo2.local
MAC        : 00:50:79:66:68:01
LPORT      : 10048
RHOST:PORT : 127.0.0.1:10049
MTU        : 1500

PC-2>
```

Figura 16 - Atribuição de IP dinâmico ao PC

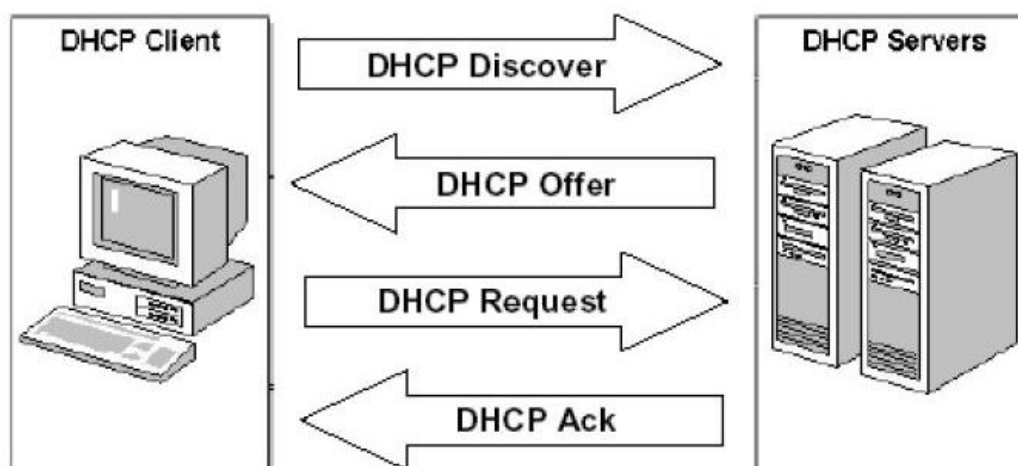


Figura 17 - Processo de aluguer quatro fases

Estando o DHCP a funcionar corretamente nos PCs da rede, ainda é possível ver as ligações vinculadas em cada PC pelo servidor DHCP (ISP). Tal como mostra a figura, uma lista é exibida com todas as ligações criadas no servidor DHCP com os PCs, através do comando “show ip dhcp binding”, e também todas as entradas vizinhas, ou seja, todos os clientes, pelo comando “show cdp neighbors” (Figura 17).

```
ISP#
ISP#
ISP#
ISP#
ISP#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration    Type
                Hardware address/
                User name
192.168.2.2      0100.5079.6668.04    Mar 02 2002 12:21 AM    Automatic
192.168.2.3      0100.5079.6668.05    Mar 02 2002 12:21 AM    Automatic
192.168.3.1      0100.5079.6668.02    Mar 01 2002 12:27 AM    Automatic
192.168.3.2      0100.5079.6668.03    Mar 02 2002 12:22 AM    Automatic
192.168.4.2      0100.5079.6668.01    Mar 02 2002 12:20 AM    Automatic
192.168.5.1      0100.5079.6668.00    Mar 01 2002 12:26 AM    Automatic
ISP#sh cdp nei
ISP#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID      Local Intfcae    Holdtime    Capability    Platform    Port ID
Gestao         Fas 0/0          162         R S I         3725        Fas 0/0
Datacenter     Fas 0/0          161         R S I         3725        Fas 0/0
Eng.Com        Fas 0/0          161         R S I         3725        Fas 0/0
ISP#
```

Figura 18 - Lista específica dos clientes (PCs) e routers vizinhos

Para evitar que as máquinas obtenham endereço IP igual à “default-gateway” (endereço da interface do router a que a máquina está ligada) que estejam interligados, fez-se uma exclusão de todos os endereços IP estáticos das interfaces dos routers ligadas às redes com PCs. Esse comando consiste em definir de forma explícita o endereço IP que se pretende excluir quando há a atribuição de IP dinâmico. Por exemplo, para a rede ligada ao router Comercial insere-se o comando “ip dhcp excluded-address 192.168.3.2” para excluir o endereço IP da interface fastethernet 0/1. Tal como mostra a figura 18, fez-se a exclusão para os restantes routers.

```
ip dhcp excluded-address 192.168.5.1
ip dhcp excluded-address 192.168.4.1
ip dhcp excluded-address 192.168.3.1
ip dhcp excluded-address 192.168.2.1
```

Figura 19 - Configuração de exclusão de endereços IP

4.4 DNS

O DNS (*Domain Name System*) é um sistema de tradução de nomes que permite que um utilizador tenha acesso à Internet por endereço Web próximo da linguagem humana. Trata-se de uma base de dados distribuída para mapear nomes de máquinas (hostnames) em endereços IP e vice-versa. Caso se pretenda aceder à página do Google, inserimos o endereço da página Web, ao invés do próprio endereço IP. Todas as páginas Web têm um DNS, ou seja, um nome que o denomina, e é por esse nome que as pessoas utilizam. Seria ridículo usar os endereços IP para entrar numa página. Desta forma, o DNS funciona de maneira transparente no sistema; ele converte o endereço introduzido num endereço IP que seja legível para a máquina. Sem o DNS, a Internet que se conhece hoje não existiria. É a forma mais adaptada e fácil dos humanos conseguirem referir máquinas é de associar um nome ao endereço.

4.4.1 Configuração DNS

Com efeito, a configuração do DNS consistirá então em definir o servidor DNS de forma a ser capaz de resolver os nomes, atribuir um nome a cada router para que seja mais simples na sua utilização, definir o “domain name” e o SOA (*Start Of Authority*) record, o router *master (primary)*, “nameservers” e ainda os “hostnames” (associar um nome a cada máquina).

No router ISP começa-se por disponibilizar o servidor DNS pelo comando “ip dns server” e, em seguida, o DNS *primary (master)*. O DNS *server primary* é responsável por ler todos os dados da “domain zone” e também desempenha o papel de comunicar com o “secondary” server (servidor secundário). A sintaxe do dns *primary* consiste então em nomear o domain name ao critério do utilizador, tendo em conta os sufixos (Ex: x.local, x.com, x.pt, x.us...) e então é que se passa a estabelecer a gravação do SOA. O SOA (*Start of Authority*) permite gravar muitos parâmetros, como por exemplo: o nome que identifica o “record”, *email*, TTL (número de segundos que a gravação será armazenada em cache por outros servidores), entre outros... Para o caso, fez-se apenas um SOA para o nome do servidor primário e *mailbox*. Tal como se pode ver na figura, todos os parâmetros descritos envolvem-se então no nome do domínio e fazer um record para o nome do servidor primário e *mailbox*. O nome do domínio e do servidor primário vão ser “grupo2.local” e “isp.grupo2.local”, respetivamente, incluindo a mailbox (“mail.grupo2.local”) (Figura 19).

```
ip dns server
ip dns primary grupo2.local soa isp.grupo2.local mail.grupo2.local 21600 900 7776000 86400
```

Figura 20 - Ativação do servidor DNS e DNS primary

Sucedese então para o registo dos nomes para cada *host* (máquina). Para o primeiro caso foi preciso indicar um NS-Record (*Authorative name server*) para o endereço do router ISP de modo a que seja definido o local onde deve estar gravado o *domain name*. O NS-Record identifica o DNS server responsável pela zona (*zone*). Uma zona deve conter um NS-Record para cada um dos seus DNS servers (primários e secundários). Caso não se indique o NS-Record, o próprio router nunca irá conseguir resolver o nome isp pelo “ping”. Para as restantes situações, atribuiu-se um nome aos restantes routers especificando o endereço IP respetivo. No último comando é demonstrado o *Name server* para um IP externo para que o router ISP possa ter acesso à rede externa. Para isso, também é necessário ativar o “domain-lookup” para que o router ISP consiga traduzir o *name server* com o sistema de *domain-name*, tal como fora explicado na configuração do protocolo NAT (Figura 20).

```
ip host grupo2.local ns 192.168.1.1
ip host isp 192.168.1.1
ip host gestao 192.168.1.4
ip host datacenter 192.168.1.3
ip host eng_com 192.168.1.2
ip name-server 8.8.8.8
```

Figura 21 - Nomeação dos hostnames e configuração do Name server e NS-Record

Feito isto, o router ISP já é capaz de fazer a resolução de nomes para a rede externa, para si próprio e também para os restantes routers. No entanto, os restantes routers ainda desconhecem o nome do servidor DNS, pelo que é necessário aceder à consola de cada router e atribuir o comando “ip name-server 192.168.1.1” (Figura 22), incluindo o “ip domain-lookup” (Figura 21) de forma a ativar a tradução para o endereço IP do router ISP. Para cada router, o procedimento é o mesmo.

```
(config)#ip domain-lookup
(config)#
```

Figura 22 - Domain-lookup

```
ip name-server 192.168.1.1
```

Figura 23 - Servidor DNS como Name server

Posto isto, todos os routers já são capazes de resolver os nomes, quer de forma inversa quer de forma direta. As imagens (figuras 23, 24 e 25) seguintes confirmam que as máquinas conseguem “pingar” para qualquer hostname ou DNS de uma página Web.

```
ISP#ping gestao
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 124/151/192 ms
ISP#ping google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 216.58.211.206, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/39/76 ms
```

Figura 24 - Resolução de nomes por parte do router ISP

```
PC-1> ping facebook.com
facebook.com resolved to 157.240.1.35
84 bytes from 157.240.1.35 icmp_seq=1 ttl=47 time=315.786 ms
84 bytes from 157.240.1.35 icmp_seq=2 ttl=47 time=114.104 ms
84 bytes from 157.240.1.35 icmp_seq=3 ttl=47 time=81.073 ms
84 bytes from 157.240.1.35 icmp_seq=4 ttl=47 time=117.606 ms
84 bytes from 157.240.1.35 icmp_seq=5 ttl=47 time=91.583 ms
```

Figura 25 - Ping para o DNS do Facebook no PC1

```
Gestao#ping isp
Translating "isp"...domain server (192.168.1.1) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/19/24 ms
Gestao#ping eng_com
Translating "eng_com"...domain server (192.168.1.1) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/17/32 ms
Gestao#ping google.com
Translating "google.com"...domain server (192.168.1.1) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 216.58.211.206, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/102/144 ms
Gestao#
```

Figura 26 - Resolução dos nomes por parte de um router de um Departamento

4.5 Firewall

Todos os computadores e servidores têm uma *firewall* configurada, que tanto pode ser no *software*, hardware ou ambos. A *firewall* consiste, portanto, num equipamento de segurança da rede que permite monitorar ou controlar todo o tráfego vindo do interior ou do exterior. Tem como principal função permitir ou rejeitar determinada informação ou pacotes provenientes do emissor baseado no conjunto de regras definidas nessa mesma *firewall*. Imaginemos que um computador pretende aceder a uma página Web que não consta nas regras de permissão de endereços externos (Internet). A *firewall* deteta de imediato que se trata de conteúdo maligno e que pode danificar o sistema da máquina. A configuração deste programa ou dispositivo de *hardware* baseia-se na filtragem de todos os pacotes que são encaminhados da rede externa ou interna, e se um pacote que é recebido não pertencer a esse filtro, não passa pela firewall. Sem uma *firewall* configurada, qualquer um pode ter acesso à máquina com ligação à rede de Internet, tendo conhecimento do que a pessoa do outro lado está a fazer. Tem liberdade absoluta, podendo fazer conexões por *telnet* (protocolo que permite que um PC se consiga conectar remotamente a outra máquina) e por FTP (*File Transfer Protocol*), por exemplo.

4.5.1 Configuração da Firewall

De forma a adaptar a definição da firewall consoante o objetivo do trabalho, era pedido que se configurasse a firewall criando filtros que permitissem a passagem dos diversos serviços pelo router ISP. Com efeito, na rede simulada no GNS3, a implementação da firewall fez-se no router que está diretamente ligado à rede externa (Internet). Para equipamentos da Cisco, existem três maneiras de configurar a firewall: por máquina virtual (interligar um sistema operativo da Virtual Box à rede do GNS, atribuir um IP dinâmico proveniente do DHCP server com todos os requisitos definidos na pool do DHCP e configurar a firewall na própria máquina no modo kernel); utilizando o modelo Zone-Based Policy Firewall (consiste em estabelecer as redes interna (inside zone) e externa (outside zone) nas interfaces do router. Depois de definidas as redes, por defeito, estas não permitem qualquer passagem de informação para qualquer serviço entre o router com firewall. Posteriormente, segue-se para a filtragem dos serviços); ou por Access-Lists. Entre os três tipos de configuração, a Zone-Based Policy é a mais simples de implementar, no entanto, a imagem IOS utilizada nos routers não contempla esse modelo. Utilizou-se então as Access-lists por ter sido a única configuração abordada nas aulas de Tecnologias de Redes de Computadores e pela razão descrita anteriormente.

As Access-lists foram então definidas no router (ISP) que está ligado diretamente à cloud de forma a ser mais fácil controlar o tráfego. Esta forma de integrar a firewall tem como objetivo filtrar os pacotes do protocolo IP. O router examina o pacote vindo interna ou externamente, analisa e compara com a lista de permissões e rejeições e, a partir daí, ou permite a continuidade do envio do pacote ou descarta-o. Os parâmetros das ACLs envolvem-se no seguinte: número da lista criada, tipo de protocolo (TCP, UDP, ICMP, OSPF...), endereço de origem, endereço de destino e tipo de serviço/aplicação (FTP, Telnet, SNMP, SMTP, DNS, DHCP...).

A imagem seguinte demonstra um exemplo de uma Access-list criada no âmbito de controlar o tráfego de pacotes:

```
access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 102 deny ip any any
```

Figura 27 - Exemplo de ACL

Na figura acima é possível observar que foi criada uma access-list com o propósito de permitir o tráfego do protocolo IP (Internet Protocol). A regra na primeira access-list da figura dita que o router permite que o tráfego vindo do endereço de origem (10.1.1.0) com a wild card (máscara inversa) respetiva - 0.0.0.255 - se aloque ou passe pelo endereço de destino, que neste caso vai ser o endereço 172.16.1.0 /24. Ou seja, basicamente todo o tráfego que seja encaminhado pelo ip 10.1.1.0 /24 até ao endereço de destino 172.16.1.0 /24 nunca vai ser descartado. Na segunda access-list, a regra estabelecida tem como designação de "Implicit Deny All". No fim de definir todas as access-lists, deve-se identificar este comando de forma a bloquear ou a permitir todo o tráfego restante. No caso da figura acima, após a regra de permissão é necessário criar uma access-list que descarte todo o tráfego que não siga os requisitos da primeira access-list ("access-list 102 deny ip any any"). O último comando executa então o seguinte: para qualquer endereço de origem e destino, descarta tudo que não esteja mediante o exigido na "permit" acima. No que respeita ao número da lista, há diversos tipos de gamas que estão em torno de objetivos diferentes, contudo apenas duas foram utilizadas no projeto. As duas gamas utilizadas na configuração da rede têm como designação de ACLs padrão (standard) e ACLs estendidas (extended). As ACLs padrão (<1-99>) classificam pacotes de acordo com o endereço origem, enquanto que as ACLs estendidas (<100-199>) classificam pacotes de acordo com o endereço de origem, endereço de destino, protocolo nível 4 e o número do porto (número inteiro que identifica determinado serviço ou aplicação) ou nome do serviço.

A figura representa uma ACL padrão cuja regra permite que os pacotes enviados pelo endereço de rede 192.168.146.0 sejam aceites pela própria máquina com a ACL criada. O segundo IP corresponde à wild card do endereço de rede. A figura simboliza uma ACL estendida cujas regras definidas já envolvem protocolos e serviços. No exemplo da figura, criou-se uma ACL com o protocolo TCP de forma a permitir a receção da informação por parte do serviço telnet do IP 10.1.1.2 até ao endereço de destino 172.16.1.1.

As imagens 27 e 28 são exemplos feitos no terminal do router ISP no GNS3, realçando os parâmetros necessários para criar uma access-list padrão e estendida. Na figura 29 é possível ver que o terminal contém todas as categorias quando se pretende executar determinada instrução, ordenando alfabeticamente os comandos disponíveis a serem aplicados com uma breve descrição. Nos terminais do GNS3, quando haja alguma dúvida na função ou significado de algum parâmetro, basta executar o comando "?". A figura 30 representa os mesmos aspetos para as ACLs estendidas.

```
access-list 10 permit 192.168.146.0 0.0.1.255
```

Figura 28 - ACL estendida

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

Figura 29 - ACL padrão

```
ISP(config)#access-list ?
<1-99>      IP standard access list
<100-199>   IP extended access list
<1000-1099> IPX SAP access list
<1100-1199> Extended 48-bit MAC address access list
<1200-1299> IPX summary address access list
<1300-1999> IP standard access list (expanded range)
<200-299>   Protocol type-code access list
<2000-2699> IP extended access list (expanded range)
<300-399>   DECnet access list
<600-699>   Appletalk access list
<700-799>   48-bit MAC address access list
<800-899>   IPX standard access list
<900-999>   IPX extended access list
dynamic-extended Extend the dynamic ACL absolute timer
rate-limit    Simple rate-limit specific access list

ISP(config)#access-list 1 ?
deny          Specify packets to reject
permit       Specify packets to forward
remark       Access list entry comment

ISP(config)#access-list 1 permit ?
Hostname or A.B.C.D Address to match
any            Any source host
host          A single host address

ISP(config)#access-list 1 permit 192.168.1.1 ?
A.B.C.D Wildcard bits
log        Log matches against this entry
<cr>

ISP(config)#access-list 1 permit 192.168.1.1 0.0.0.255
```

Figura 31 - Parâmetros da ACL padrão

```
ISP(config)#access-list 100 permit tcp 192.168.1.1 0.0.0.255 host isp ?
ack      Match on the ACK bit
dscp     Match packets with given dscp value
eq       Match only packets on a given port number
established Match established connections
fin      Match on the FIN bit
fragments Check non-initial fragments
gt       Match only packets with a greater port number
log      Log matches against this entry
log-input Log matches against this entry, including input interface
lt       Match only packets with a lower port number
neq      Match only packets not on a given port number
option   Match packets with given IP Options value
precedence Match packets with given precedence value
psh      Match on the PSH bit
range    Match only packets in the range of port numbers
rst      Match on the RST bit
syn      Match on the SYN bit
time-range Specify a time-range
tos      Match packets with given TOS value
urg      Match on the URG bit
<cr>

ISP(config)#access-list 100 permit tcp 192.168.1.1 0.0.0.255 host isp eq ?
<0-65535> Port number
bgp       Border Gateway Protocol (179)
chargen   Character generator (19)
cmd       Remote commands (rcmd, 514)
daytime   Daytime (13)
discard   Discard (9)
domain    Domain Name Service (53)
drip      Dynamic Routing Information Protocol (3949)
echo      Echo (7)
exec      Exec (rsh, 512)
finger    Finger (79)
ftp       File Transfer Protocol (21)
ftp-data  FTP data connections (20)
gopher    Gopher (70)
hostname  NIC hostname server (101)
ident     Ident Protocol (113)
irc       Internet Relay Chat (194)
klogin    Kerberos login (543)
kshell    Kerberos shell (544)
```

Figura 30 - Parâmetros da ACL estendida

Para o projeto em questão, foi necessário implementar a firewall criando access-lists estendidas, pois era pedido que se mantivessem abertos todos os portos necessários ao funcionamento dos serviços de rede (OSPF, DHCP, DNS, TFTP, FTP, SNMP, WWW...). Portanto, a figura abaixo é uma porção da configuração da firewall no router ISP, sendo necessário ter em atenção à ordem dos filtros criados. Isto é, como o GNS processa sequencialmente a lista de access-lists, é pouco recomendável que se defina as access-lists por ordem aleatória.

Por exemplo: pretende-se que o serviço WWW esteja funcional para as máquinas internas na rede, ou seja, que tenham acesso à Internet quando enviam um pedido para um IP ou o DNS de uma página Web. Para que tal aconteça, terá que existir, primeiramente, o seguinte: um filtro que permita o suporte de encaminhamento dinâmico (OSPF), para que as máquinas internas possam enviar pacotes para o ISP; pedido de atribuição de IP dinâmico por parte do DHCP server; e ainda a disponibilidade da resolução de nomes (DNS). Definidos estes serviços, é possível então criar um filtro para o serviço WWW. Muitos dos serviços dependem de outros, o que é importante ter em atenção a este aspeto, pois um computador não consegue ter conectividade com um router se não existir encaminhamento dinâmico ou estático ou um PC não consegue ter acesso à Internet se o router ISP não estiver com o domain-lookup e o name server bem configurados.

Na figura 31 repara-se que na configuração das ACLs se começou por permitir o protocolo OSPF para que todos os routers conheçam todas as redes envolventes. Seguidamente, criou-se mais um conjunto de ACLs que permitissem que qualquer endereço, pelo protocolo IP, pudesse ter acesso ao router ISP. Definiu-se também pelo protocolo UDP o serviço de DHCP em cada rede dos Departamentos da rede interna para que estes possam receber a atribuição de IP por parte do router ISP. De forma a testar se a firewall está configurada corretamente, criou-se uma ACL para descartar qualquer pacote enviado para o IP externo (1.1.1.1). Este endereço pertence a um DNS da Internet. Outro pormenor que é visto na imagem é o parâmetro “remark”, que consiste em atribuir um nome ao critério do administrador antes de criar a ACL permit ou deny, de forma a distinguir melhor a configuração que foi feita. De relembrar que a configuração abaixo é apenas uma pequena parte da filtragem criada.

```
access-list 100 remark Allow Distribuicao OSPF access to ISP
access-list 100 permit ospf 192.168.1.0 0.0.0.255 host 192.168.1.1
access-list 100 remark Allow Engenharia OSPF access to ISP
access-list 100 permit ospf 192.168.2.0 0.0.0.255 host 192.168.1.1
access-list 100 remark Allow Comercial OSPF access to ISP
access-list 100 permit ospf 192.168.3.0 0.0.0.255 host 192.168.1.1
access-list 100 remark Allow Datacenter OSPF access to ISP
access-list 100 permit ospf 192.168.4.0 0.0.0.255 host 192.168.1.1
access-list 100 remark Allow Gestao OSPF access to ISP
access-list 100 permit ospf 192.168.5.0 0.0.0.255 host 192.168.1.1
access-list 100 remark Allow access to ISP
access-list 100 permit ip any host 192.168.1.1
access-list 100 remark Deny access to ISP
access-list 100 deny ip any host 1.1.1.1
access-list 100 remark Allow Engenharia DHCP access to ISP
access-list 100 permit udp 192.168.2.0 0.0.0.255 eq bootpc host 192.168.1.1 eq bootps
access-list 100 remark Allow Comercial DHCP access to ISP
access-list 100 permit udp 192.168.3.0 0.0.0.255 eq bootpc host 192.168.1.1 eq bootps
access-list 100 remark Allow Datacenter DHCP access to ISP
access-list 100 permit udp 192.168.4.0 0.0.0.255 eq bootpc host 192.168.1.1 eq bootps
access-list 100 remark Allow Gestao DHCP access to ISP
access-list 100 permit udp 192.168.5.0 0.0.0.255 eq bootpc host 192.168.1.1 eq bootps
access-list 100 remark Allow ICMP access to ISP
access-list 100 permit icmp any any
```

Figura 32 - ACLs criadas para a firewall

Para executar a firewall criada é necessário aplicar as ACLs à entrada da interface do router. Caso se prefira que o controlo dos pacotes seja feito na interface de entrada do router, utiliza-se o “inbound packets”. Isto permitirá que os pacotes sejam descartados ou permitidos de imediato sem que acedam ao interior do router. Se for preferível que seja na interface de saída do router, utiliza-se o “outbound packets”. Nesta situação, a informação acede ao interior do router e só depois é revisto na interface de saída (Figura 33).

```
ISP(config-if)#ip access-group 100 ?
  in    inbound packets
  out   outbound packets
```

Figura 33 - Aplicação da lista na interface do router ISP

A imagem abaixo (Figura 33) corresponde ao comando executado na interface de entrada no router ISP (fastethernet 0/0)

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip access-group 100 in
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet0/1
ip address dhcp
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
```

Figura 34 - Visualização do comando no show running config

Para testar se a firewall está a funcionar corretamente, executa-se o comando “ping” nos PCs para o DNS de uma página Web, um IP externo ou para o próprio router ISP, de forma a verificar se o IP existe e/ou se aceita os pedidos. Como se pode ver na imagem abaixo, se enviarmos um pedido ao router ISP (IP 192.168.1.1), ao 8.8.8.8 e ao DNS do Google, a resposta é positiva. No entanto, se o pedido for direcionado para o IP 1.1.1.1 a resposta já é distinta. O pedido é descartado pelo router ISP, o que significa que a firewall está a descartar os pacotes supostos (Figura 34).

```
PC-1> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=254 time=39.004 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=254 time=50.002 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=254 time=50.545 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=254 time=48.517 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=254 time=32.029 ms

PC-1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=43 time=88.581 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=43 time=109.559 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=43 time=496.450 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=43 time=176.137 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=43 time=70.543 ms

PC-1> ping 1.1.1.1
*192.168.1.1 icmp_seq=1 ttl=254 time=44.511 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.1 icmp_seq=2 ttl=254 time=49.012 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.1 icmp_seq=3 ttl=254 time=19.016 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.1 icmp_seq=4 ttl=254 time=59.553 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.1 icmp_seq=5 ttl=254 time=33.998 ms (ICMP type:3, code:13, Communication administratively prohibited)

PC-1> ping google.com
google.com resolved to 172.217.16.238
84 bytes from 172.217.16.238 icmp_seq=1 ttl=54 time=112.082 ms
84 bytes from 172.217.16.238 icmp_seq=2 ttl=54 time=58.023 ms
84 bytes from 172.217.16.238 icmp_seq=3 ttl=54 time=88.628 ms
84 bytes from 172.217.16.238 icmp_seq=4 ttl=54 time=100.626 ms
84 bytes from 172.217.16.238 icmp_seq=5 ttl=54 time=96.587 ms
```

Figura 35 - Teste se a firewall está funcional

4.6 Proxy

A proxy funciona como intermediário entre as máquinas e a internet. Todas as máquinas estão ligadas ao servidor Proxy, “obedecendo” às regras definidas por este. Desta forma os pedidos (ex. páginas web, ficheiros, etc) são feitos pelo Proxy (e não diretamente pela máquina de origem), com isto, é possível ter controle absoluto sobre o tráfego da internet e realizar bloqueios (ou liberações) de acordo com as políticas estabelecidas na proxy.

No projeto utilizou-se a proxy web, este permite controlar os pedidos que são efetuados no web browser através do protocolo http. Uma vez que o GNS3 não permite a criação de servidores proxy recorremos a uma máquina virtual em Linux onde configuramos o proxy com o software “Squid” (servidor proxy com a principal função de suportar os protocolos HTTP, HTTPS, FTP, entre outros).

4.6.1 Instalação e configuração do programa Squid

Primeiramente começa-se pela instalação do Squid. Para tal executa-se o terminal e neste insere-se o comando “sudo apt-get install squid squid-common”.

```
File Edit View Search Terminal Help
rodrigo@rodrigo-VirtualBox ~ $ sudo apt-get install squid squid-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
123The following additional packages will be installed:
  libcap3 squid-langpack
Suggested packages:
  squidclient squid-cgi squid-purge winbindd
The following NEW packages will be installed:
  libcap3 squid squid-common squid-langpack
0 upgraded, 4 newly installed, 0 to remove and 324 not upgraded.
Need to get 2656 kB of archives.
After this operation, 10,8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Abort.
rodrigo@rodrigo-VirtualBox ~ $ sudo apt-get install squid squid-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libcap3 squid-langpack
Suggested packages:
  squidclient squid-cgi squid-purge winbindd
The following NEW packages will be installed:
  libcap3 squid squid-common squid-langpack
0 upgraded, 4 newly installed, 0 to remove and 324 not upgraded.
Need to get 2656 kB of archives.
After this operation, 10,8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu xenial/main amd64 libcap3 amd64 1.0.1-3ubuntu3 [16,7 kB]
Get:2 http://archive.ubuntu.com/ubuntu xenial/main amd64 squid-langpack all 20150704-1 [145 kB]
Get:3 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 squid-common all 3.5.12-1ubuntu7.5 [176 kB]
Get:4 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 squid amd64 3.5.12-1ubuntu7.5 [2317 kB]
Fetched 2656 kB in 5s (470 kB/s)
Selecting previously unselected package libcap3:amd64.
(Reading database ... 197948 files and directories currently installed.)
Preparing to unpack .../libcap3_1.0.1-3ubuntu3_amd64.deb ...
Unpacking libcap3:amd64 (1.0.1-3ubuntu3) ...
```

Figura 36 - Instalação Squid

Após o término do comando de instalação dá-se início ao programa utilizando o comando “sudo service squid start”. Tendo assim o programa em execução começa-se a configuração do mesmo, para tal teve-se de localizar o ficheiro de configurações do squid, que se encontra na localização “/etc/squid” com o nome “squid.conf”. Abre-se esse ficheiro e começa-se então a configuração. Localiza-se primeiramente a linha “TAG: visible_hostname” e em seguida coloca-se “visible_hostname Grupo2ProxyServer”, assim quando o utilizador tentar aceder a uma página web que não seja permitida irá ser mostrado o nome do grupo assim como o erro de tentativa bloqueada.

```
5489 # This option is not recommended by the Squid Team.
5490 # Our preference is for administrators to configure a secure
5491 # user account for squid with UID/GID matching system policies.
5492 #Default:
5493 # Use system group memberships of the cache_effective_user account
5494
5495 # TAG: httpd_suppress_version_string on/off
5496 # Suppress Squid version string info in HTTP headers and HTML error pages.
5497 #Default:
5498 # httpd_suppress_version_string off
5499
5500 # TAG: visible_hostname
5501 visible_hostname Grupo2ProxyServer
5502 # If you want to present a special hostname in error messages, etc,
5503 # define this. Otherwise, the return value of gethostname()
5504 # will be used. If you have multiple caches in a cluster and
5505 # get errors about IP-forwarding you must set them to have individual
5506 # names with this setting.
5507 #Default:
5508 # Automatically detect the system host name
5509
5510 # TAG: unique_hostname
5511 # If you want to have multiple machines with the same
5512 # 'visible_hostname' you must give each machine a different
```

Figura 37 - Hostname Proxy

Localiza-se em seguida a parte onde indica quais as redes internas que vão estar afetas a estas configurações e comenta-se as que não nos interessam.


```
967
968 # Example rule allowing access from your local networks.
969 # Adapt to list your (internal) IP networks from where browsing
970 # should be allowed
971 acl [localnet] src 10.0.0.0/8 # RFC1918 possible internal network
972 #acl [localnet] src 172.16.0.0/12 # RFC1918 possible internal network
973 #acl [localnet] src 192.168.0.0/16 # RFC1918 possible internal network
974 acl [localnet] src fc00::/7 # RFC 4193 local private network range
975 |acl [localnet] src fe80::/10 # RFC 4291 link-local (directly plugged) machines
976
```

Figura 38 - Lista de redes afetadas pelo proxy

Para se bloquear os websites basta adicionar uma linha com o código “acl block_websites dstdomain” e em seguida os domínios dos websites. Exemplo: “acl block_websites dstdomain .msn.com .yahoo.com”. Desta forma cria-se uma lista de domínios que se pretende bloquear e em seguida tem de se dar o comando para ele bloquear esta mesma lista “http_access deny block_websites”.

Concluída a configuração da proxy tem agora de se parar a execução do programa e voltar a ligar, de forma a assumir as configurações todas configurações.

4.7 TFTP

O Trivial File Transfer Protocol, ou TFTP, é um método leve para mover pequenos arquivos dentro de uma rede local, sendo o mais adequado para tal efeito. O protocolo não estabelece uma conexão e usa menos recursos em relação ao File Transfer Protocol (FTP), que é uma opção semelhante, porém mais conhecida para a transferência de arquivos.

Tal como qualquer protocolo de transporte, o TFTP monta pacotes de dados. Esses mesmos protocolos podem ser o Transmission Control Protocol (TCP) ou o User Datagram Protocol (UDP). O FTP, rival direto do protocolo TFTP, utiliza o TCP, que estabelece uma conexão entre os dois pontos finais da transferência e verifica se os pacotes de dados chegam fora de sequência, ou se estão corrompidos ou em falta. Por outro lado, o UDP não faz nenhuma dessas verificações nem estabelece nenhuma conexão. Apesar do protocolo TFTP necessitar de enviar dados em vários pacotes, este usa o UDP, ao invés do TCP, por norma mais adequado, visto que o seu objetivo é ser rápido, simples e leve.

No protocolo TFTP todos os arquivos são enviados em blocos de 512 bytes. Um pacote que seja enviado com um tamanho inferior a 512 bytes significa que este é o último pacote a ser enviado na transmissão de ficheiros. Este protocolo é normalmente denominado por “protocolo de sintonia”, o que significa que cada um dos lados só pode agir depois do outro lado ter concluído a sua ação. O servidor envia um pacote e aguarda até que o cliente envie uma confirmação. Isto faz com que o servidor envie o pacote seguinte e assim por diante. Se o servidor não receber uma confirmação dentro de um determinado período de tempo, esse mesmo pacote é então transmitido novamente até ser confirmado.

O seu tamanho de bloco de 512 bytes e a sua total ausência de quaisquer recursos de segurança tornam o protocolo TFTP inadequado para a transferência de grandes arquivos pela Internet. O principal uso do protocolo é a transferência de um pequeno arquivo de inicialização ou arquivo de configuração para a inicialização de estações de trabalho sem disco, ou como parte do endereço IP rotinas de alocação do Dynamic Host Configuration Protocol (DHCP).

Em cada router foi configurado de forma a que faça diariamente o backup para o servidor.

Cada backup possui um nome correspondente a cada router individualmente.

Após o backup ser efetuado será então guardado na pasta de destino “grupo2_ftp”. Com um Shell script é alterado o nome do backup e movido para uma pasta comparando com os já efetuados anteriormente (caso seja igual aos já existentes este será descartado).

4.8 SNMP

O SNMP (Simple Network Management Protocol) é um protocolo com origem na RFC 1067, em 1988, criado com o intuito de facilitar a monitorização e o gerenciamento de redes. Estando atualmente na versão 3, é hoje um dos protocolos mais usados para esse fim, já que permite trabalhar com produtos e serviços de diversos fabricantes. Hoje em dia, as principais soluções de monitorização de redes fornecem alertas como SMS, e-mails ou PUSH para comunicar falhas na infraestrutura de rede. As ferramentas mais avançadas já apresentam painéis visuais (dashboards). Estes painéis apresentam indicadores críticos do funcionamento da rede através de gráficos em tempo real. O protocolo SNMP é a maneira mais fácil de aceder às informações de diferentes sistemas de modo a visualizar a monitorização.

Trata-se de um protocolo da camada de aplicação (a camada sete do modelo OSI - Open System Interconnection) que usa normalmente a porta 161 do protocolo de transporte UDP. Essa característica permite a abstração das outras camadas e o gerenciamento de dispositivos que estejam fora da rede de origem. Em suma, a função básica do protocolo SNMP é de facilitar a troca de informações de gerenciamento entre os dispositivos da rede. Para isso, fornece dados dos estados (status) dos elementos ativos da rede e estatísticas importantes para o seu funcionamento. O protocolo consome poucos recursos da rede e do processamento, o que levou à sua disseminação e inclusão até em equipamentos simples como impressoras.

O SNMP permite que uma ou mais máquinas da rede sejam designadas como gerentes/administradores. Esse dispositivo recebe informações dos demais itens da rede, que se tornam agentes. Com o processamento dessas informações, é possível administrar a integridade do sistema e facilmente detetar defeitos. Para isso, é comum o uso da Management Information Base (MIB): uma árvore hierárquica organizada pelos vários tipos de informação.

Nela ficam gravadas todas as informações necessárias para a gestão de cada dispositivo, usando as variáveis requeridas pelo gerente. O protocolo SNMP define apenas como os dados serão transmitidos, já que as informações adquiridas pela máquina gerente estão armazenadas nos próprios agentes. Assim, a sua arquitetura consiste numa coleção de estações de gerenciamento e elementos de rede, e o SNMP transporta a informação entre essas estações.

O SNMP é simples e robusto ao mesmo tempo, além de suficientemente poderoso e capaz de gerenciar até redes heterogéneas. Como as tarefas mais complexas de processamento e armazenamento de dados ficam com o gerente, o protocolo requer pouco processamento e pouco software. Por não ser orientado a conexão, ou seja, por não requerer ação prévia nem posterior ao envio de mensagens, não há garantia de que as informações chegarão ao destino. Por outro lado, o facto de não existir conexão faz com que ambos precisam um do outro para operar. As informações obtidas através do SNMP são fundamentais para o administrador da rede na hora de definir estratégias e tomar decisões. São essas informações que garantem, afinal, que o funcionamento do sistema vai ocorrer sem imprevistos e com impacto mínimo sobre o restante da operação.

4.9 VPN

Uma VPN (Virtual Private Network), como o próprio nome sugere, é uma forma de conectar dois computadores utilizando uma rede pública, como a Internet. As ligações VPN são normalmente utilizadas em grandes empresas de modo a interligar duas de suas filiais, sendo uma alternativa a:

Comprar equipamentos wireless e conectar as filiais através de um link de rádio;

Conectar ambas as filiais através de um cabo de rede, o que pode ser totalmente inviável dependendo da distância entre estas;

Pagar por uma linha privada para que as filiais possam comunicar entre si.

Estes são os recursos mais utilizados por empresas, mas alguns deles podem tornar-se financeira ou geograficamente irrealizáveis. A melhor solução, na maioria dos casos, acaba por ser a VPN, pois o custo é pequeno comparado às outras opções.

Como a Internet é uma rede pública, é preciso criar alguns mecanismos de segurança para que as informações trocadas entre os computadores de uma VPN não possam ser lidas por outras pessoas. A proteção mais utilizada é a criptografia, pois essa garante que os dados transmitidos por um dos computadores da rede sejam os mesmo que as demais máquinas irão receber. Depois de criptografados, os dados são encapsulados e transmitidos pela Internet, utilizando o *tunnel protocol*, até encontrarem o seu destino.

Para criar uma rede VPN não é preciso mais do que dois (ou mais) computadores conectados à Internet e um programa de VPN instalado em cada máquina. O processo para o envio dos dados é o seguinte:

Os dados são criptografados e encapsulados.

Algumas informações extra, como o número de IP da máquina remetente, são adicionadas aos dados que serão enviados para que o computador recetor possa identificar quem mandou o pacote de dados.

O pacote que contém todos os dados é enviado através do “túnel” criado até ao computador de destino.

A máquina recetora identifica o computador remetente através das informações anexadas ao pacote de dados.

Os dados são recebidos e desencapsulados.

Finalmente os dados são descriptografados e armazenados no computador de destino.

As redes VPN são muito utilizadas por grandes empresas, principalmente aquelas em que os funcionários viajam com frequência ou trabalham em casa, por exemplo. Mas nada impede os usuários comuns de, no seu dia-a-dia, utilizem as redes privadas virtuais.

No entanto, se o tempo de transmissão dos dados é crucial para a empresa ou para o usuário, este tipo de rede pode não ser o mais indicado, pois elas dependem diretamente da velocidade da Internet disponível, o que pode acarretar em atrasos e problemas sobre os quais o técnico ou usuários não terão qualquer tipo de controlo.

4.10 Web Server

Qualquer pessoa que utiliza a Internet, seja para aceder a um site, conferir e-mails ou interagir numa rede social, está interagindo, de alguma forma, com um Web Server. O Servidor Web (Web Server) é responsável por responder a todas as solicitações feitas para um endereço na Internet, sendo o coração de qualquer empresa de hospedagem de sites. Sem ele, a Internet como a conhecemos provavelmente não existiria.

De maneira simplificada, podemos dizer que um Web Server é um computador que hospeda um ou mais websites/aplicações na internet. No entanto, este termo pode-se referir tanto ao equipamento físico (hardware) como ao programa (software) contido neste equipamento, ou até mesmo a ambos os casos (hardware e software).

Um website é composto por uma compilação de arquivos digitais que são interpretados pelo navegador e exibidos no ecrã de um computador/dispositivo. Para que possa ser acedido por qualquer pessoa, os arquivos de um site precisam de estar armazenados em algum lugar, mais precisamente num computador que esteja ligado à Internet 24 horas por dia. Este computador é conhecido como Web Server. Um servidor possui componentes internos semelhantes aos que são encontrados num computador pessoal, como por exemplo um HD, memória RAM, motherboard, etc. Entretanto, a arquitetura deste é otimizada para executar as tarefas de um servidor.

Os servidores do tipo equipamento físico podem ser encontrados de duas formas distintas: torre e rack. Durante anos, os servidores do tipo torre eram o padrão, no entanto, com o aumento da demanda e com a criação dos grandes datacenters, os servidores do tipo rack tornaram-se muito mais populares. Razão disto é a alta capacidade de expansão que o formato rack proporciona, já que é possível agrupar e interligar, numa única coluna de rack, dezenas de servidores.

Assim como em qualquer computador pessoal, um Web Server também possui um sistema operativo e diversos programas podem ser instalados nele, incluindo programas específicos para executar determinadas tarefas, tais como: enviar páginas de um site pela internet, enviar e receber e-mails, armazenar e fornecer arquivos, entre outras. A esses programas, também atribuímos o nome de servidor web.

Ao aceder a um site na internet, o navegador comunica com o servidor, solicitando e recebendo os dados da página em questão. O servidor físico possui programas específicos para responder ao tipo de solicitação realizada: no caso de um site, esta solicitação é feita através do protocolo HTTP. Todos os sites na internet trafegam utilizando este protocolo (ou sua versão segura, conhecida como HTTPS). Assim, existem programas específicos para responder às solicitações do tipo HTTP. Este tipo de programa também é conhecido como servidor web. Alguns tipos de Web Servers (software) frequentemente encontrados em Web Servers (hardware) são, por exemplo:

Servidor HTTP – envia os arquivos que compõem um site.

Servidor FTP – realiza upload e download de arquivos entre computadores e servidores.

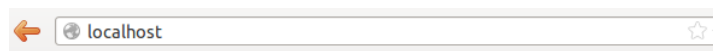
Servidor de e-mail – envia, recebe e armazena e-mails.

Servidor de banco de dados – armazena dados em uma estrutura específica.

Assim, quando requisitamos uma página na internet, o pedido será enviado para o servidor que contém os arquivos do site em questão. Quando a requisição chega ao servidor, o software nele contido responsabilizar-se-á por processar as informações solicitadas e responder de acordo. Um servidor web pode receber solicitações e enviar arquivos para milhares de usuários simultaneamente ou dentro de um curto espaço de tempo.

4.10.1 Implementação do Web Server

Para a implementação do Web Server começou-se por abrir o terminal e instalar o apache2 através do comando “apt-get install apache2”. Após isso podemos abrir uma página localhost num browser de modo a verificar que o servidor apache já se encontra a correr.



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

Figura 41 – Index default do servidor apache

De forma a configurar o index.html do servidor apache, e por razões de boas, paramos o servidor através do comando `/etc/init.d/apache2 stop`, assim deste modo podemos prosseguir para a construção html da página.

```

1 <!DOCTYPE html>
2 <html>
3 <title>Grupo 2 - PTRC</title>
4 <meta charset="UTF-8">
5 <meta name="viewport" content="width=device-width, initial-scale=1">
6 <link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">
7 <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Raleway">
8 <style>
9 body,h1 {font-family: "Raleway", sans-serif}
10 body,html {height: 100%}
11 .bgimg {
12     background-image: url('www.123.242.161.52/w3images/IMG/forestbridge.jpg');
13     min-height: 100%;
14     background-position: center;
15     background-size: cover;
16 }
17 </style>
18 <body>
19
20 <div class="bgimg w3-display-container w3-animate-opacity w3-text-white">
21   <div class="w3-display-middle">
22     <h1 style="color: black;" class="w3-jumbo w3-animate-top">Grupo 2 - PTRC</h1>
23     <hr class="w3-border-grey" style="margin:auto;width:40%">
24     <p style="color: black;" class="w3-large w3-center">Carlos Girão</p>
25     <p style="color: black;" class="w3-large w3-center">Cláudio Cruz</p>
26     <p style="color: black;" class="w3-large w3-center">Ricardo Balreira</p>
27     <p style="color: black;" class="w3-large w3-center">Rodrigo Tavares</p>
28     <p style="color: black;" class="w3-large w3-center">Pedro Moreno</p>
29   </div>
30 </div>
31
32 </body>
33 </html>

```

Figura 42 – Código HTML do servidor Apache

Após a alteração do código html na página do Web Server, iniciamos novamente o nosso servidor através do comando `/etc/init.d/apache2 restart`, assim podemos aceder através de um browser ao IP do inet adress, o que nos vai mostrar a nossa nova página html.



Figura 43 - Index final do servidor Apache

5. Bibliografia

Amadeu, R. (23 de Março de 2004). Economize Tempo e Melhore suas Notas com o Cite This For Me, a ferramenta número um para fazer Referências. Obtido de Cite This For Me: <http://www.citethisforme.com/pt/cite/website>

Arshad, S. (16 de Fevereiro de 2014). Configuring Cisco Router as DNS Server. Obtido de Youtube: <https://www.youtube.com/watch?v=1HICzKxS5GY>

augustineCPU. (3 de Novembro de 2016). How to configure a DHCP server on a Cisco Router (GNS3). Obtido de Youtube: https://www.youtube.com/watch?v=2Jc_SI0Px8

Beal, V. (s.d.). NAT - Network Address Translation. Obtido de Webopedia: <https://www.webopedia.com/TERM/N/NAT.html>

Bombal, D. (2 de Fevereiro de 2017). GNS3 Talks: Use the NAT node to connect GNS3 to the Internet easily! Obtido de Youtube: <https://www.youtube.com/watch?v=2zeoC2Q4mW0>

Chaturvedi, N. (20 de Junho de 2016). How to configure DHCP server on GNS3. Obtido de Youtube: <https://www.youtube.com/watch?v=dKEc5vgb784>

Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2. (31 de Outubro de 2013). Obtido de Cisco: https://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/ro ute_ospf.html

Cisco IOS IP Configuration Guide, Release 12.2 . (12 de Fevereiro de 2014). Obtido de Cisco: https://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html

Configure NAT – GNS3 Lab. (24 de Maio de 2011). Obtido de CCNA Training: <http://www.9tut.com/configure-nat-gns3-lab>

Configuring Network Address Translation: Getting Started. (2 de Maio de 2014). Obtido de Cisco: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>

Dias, H. (s.d.). DNS - O que é e para que serve? | Pplware Kids. Obtido de Kids.pplware.sapo.pt: <http://kids.pplware.sapo.pt/o-meu-computador/dns-o-que-e-e-para-que-serve/>

Dynamic Host Configuration Protocol. (s.d.). Obtido de Wikipédia: https://pt.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

GNS3 Labs for CCNA: DHCP Server Configuration and Verification. (s.d.). Obtido de Intense School: <http://resources.intenseschool.com/gns3-labs-for-ccna-dhcp-server-configuration-and-verification/>

GNS3vault . (s.d.). All Labs. Obtido de GNS3vault: <https://gns3vault.com/labs/>

GoDaddy. (2 de Fevereiro de 2017). What Is DNS? | GoDaddy. Obtido de Youtube: <https://www.youtube.com/watch?v=HsQOWfc3Wic>

IP Addressing: DNS Configuration Guide, Cisco IOS Release 15M&T . (25 de Janeiro de 2018). Obtido de Cisco: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/15-mt/dns-15-mt-book/dns-config-dns.html

NAT (Network Address Translation) - Current network security features used today. (s.d.). Obtido de Internet-Computer-Security.com : <http://www.internet-computer-security.com/Firewall/NAT.html>

Pereira, A. P. (12 de Maio de 2009). O que é DHCP? Obtido de No Zebra Network LTDA: <https://www.tecmundo.com.br/internet/2079-o-que-e-dhcp-.htm>

Significado de DHCP. (10 de Setembro de 2013). Obtido de Significados: <https://www.significados.com.br/dhcp/>

ThinkITSolutions.MinderaHandbook.pdf. (s.d.). Obtido de Google Docs: <https://drive.google.com/file/d/0B454eHGtsBnKZHViUjRQVXNINzg/view>

Videos, D. M. (27 de Fevereiro de 2012). DNS Explained. Obtido de YouTube: <https://www.youtube.com/watch?v=72snZctFFtA&t>

Anexos



Orçamento

[Proposta para Fornecimento de Equipamento.]

Equipamentos Informáticos

[#20182679]

N/REFa: 20182679

Obra: Equipamentos Informáticos

Assunto: Proposta para Fornecimento de Equipamento

Exmos. Senhores,

Vimos pela presente submeter à apreciação de V. Exas., a nossa proposta para o fornecimento do equipamento mencionado em epígrafe.

Como representantes em Portugal de marcas de tão elevada confiança e prestígio internacional, estamos confiantes que, tanto a tecnologia de futuro, como a qualidade da nossa assistência pós-venda, serão a melhor garantia de plena satisfação dos vossos interesses.

Esperando que esta proposta possa merecer a Vossa preferência, subscrevemo-nos com os melhores cumprimentos.

Atentamente,

Grupo2, Lda

Equipamentos Informáticos

	COMPONENTE	DESCRIÇÃO	QTD	VALOR	TOTAL
	Switch	D-Link DGS-1210-28	7	160,43 €	1123,01 €
	Router	Draytek DT-V2960	4	488,49 €	1953,96 €
	AP	Ubiquiti Uap-Ac-Pro	2	142 €	284 €
	Servidor	Proliant ML350	1	2,083.33 €	2 083.33 €
				TOTAL	5.123,44

Nota: A configuração e instalação não estão incluídas.

Condições Gerais da Proposta

PREÇOS

Os preços fornecidos são em Euros, para equipamentos/trabalhos colocados na instalação em causa, estando sujeitos ao IVA à data do fornecimento, tal como a taxa de Ecovalor (DL n.º 62/2001) e EcoREEE (DL n.º 230/2004). Será acrescido valores de portes de envio, caso seja solicitado a entrega do material por transportadora.

CONDIÇÕES DE PAGAMENTO

Pagamento a 30 dias.

PRAZO DE ENTREGA / INÍCIO DOS TRABALHOS

A entrega de equipamentos é de 3 a 5 dias (Exceto rutura de Stock).

ASSISTÊNCIA TÉCNICA

A empresa Grupo2, garante, por técnicos credenciados, a manutenção corretiva aos equipamentos/sistemas sempre que para tal seja solicitada.

GARANTIA

Os equipamentos fornecidos têm 12 meses de garantia após a sua entrega/instalação, nos termos do disposto no artigo 921º do Código Civil, contra defeitos de fabrico ou instalação, desde que se verifique que a sua origem não é devida a erros de manuseamento por parte do cliente, má conservação do equipamento e descargas elétricas anormais.

Durante o prazo de garantia a Grupo2 compromete-se a reparar o artigo vendido que apresente defeito de funcionamento devendo este ser entregue nas instalações do Grupo2.

Caso o cliente pretenda que a reparação seja efetuada nas suas instalações, ou na impossibilidade de o artigo ser retirado do local onde se encontra implantado, será devido o custo da respetiva deslocação.

Após o período de garantia esta prestação de serviços poderá efetuar-se em regime de intervenção pontual, por solicitação do Cliente, com custos a debitar caso a caso, ou através de um Contrato de Assistência Técnica.

VALIDADE DA PROPOSTA

A presente proposta é válida por 30 dias a contar da data de emissão.

