

# **PROJETO TEMÁTICO EM ADMINISTRAÇÃO DE SISTEMAS**

## **RELATÓRIO FINAL**

### **Grupo GR3**

Carlos Azinhaga - 69468

Paulo Silva - 61999

Paulo Silva - 62201

Pedro Marquinhos - 70445

**2º Semestre 2012/13**

# **PROJETO TEMÁTICO EM ADMINISTRAÇÃO DE SISTEMAS**

## **RELATÓRIO FINAL**

### **Grupo GR3**

Carlos Azinhaga - 69468

---

Paulo Silva - 61999

---

Paulo Silva - 62201

---

Pedro Marquinhos - 70445

---

### **Orientador de Projeto**

Joaquim Ferreira

**2º Semestre 2012/13**

# ÍNDICE

1 - Introdução.....	1
1.1 - Cliente .....	1
1.2 - Objetivos .....	1
2 - Arquitetura de Rede.....	3
2.1 - Solução proposta.....	3
3 - Planeamento .....	5
3.1 - Requisitos .....	5
3.2 - Tarefas.....	6
3.3 - Orçamento .....	8
4 - Implementação .....	9
4.1 - Lista de Hardware utilizado.....	9
4.2 - Lista de Software utilizado .....	9
4.3 - Configuração das aplicações/serviços instalados .....	10
4.3.1 - Encaminhamento .....	10
4.3.2 - DNS.....	11
4.3.3 - DHCP.....	13
4.3.4 - Proxy.....	15
4.3.5 - HTTP .....	16
4.3.6 - VPN.....	17
4.3.7 - Firewall .....	19
4.3.8 - Backup.....	20
4.3.9 - Active Directory.....	20



5 - Validação e Verificação .....	21
5.1 - Testes de Sistema.....	21
5.1.1 - Encaminhamento .....	21
5.1.2 - DNS.....	21
5.1.3 - DHCP.....	22
5.1.4 - Proxy.....	22
5.1.5 - HTTP .....	22
5.1.6 - VPN.....	23
5.1.7 - FIREWALL .....	23
5.1.8 - BACKUP .....	24
5.2 - Validação de requisitos .....	24
6 - Conclusão .....	25
7 - Fontes e Material de Referência .....	27

## **LISTA DE SIGLAS E ABREVIATURAS**

**DNS** - Domains Name Server

**DHCP** - Dynamic Host Configuration Protocol

**HTTP** - Hypertext Transfer Protocol

**VPN** - Virtual Private Network

**IP** - Internet Protocol

**WAN** - Wide Area Network

**LAN** - Local Area Network

**Netmask** - Máscara de Rede

**SSH** - Secure Shell



## **1 - INTRODUÇÃO**

Na introdução serão abordados os seguintes tópicos: o Cliente e os Objetivos.

O projeto consiste no desenvolvimento de um protótipo funcional da futura rede de uma empresa, construída com base no enunciado previamente tratado. Integra-se no módulo de projeto temático em Administração de Sistemas, do qual faz parte a disciplina de Redes e Sistemas Operativos.

### **1.1 - CLIENTE**

O cliente é a Empresa XPTO<sup>2</sup> e o seu representante é o orientador do Projeto.

### **1.2 - OBJETIVOS**

O principal objetivo será a aplicação prática dos conhecimentos adquiridos ao longo do semestre na cadeira Redes e Sistemas Operativos, nomeadamente:

- Desenvolvimento de uma estrutura de rede;
- Correções de instalação e/ou configuração de redes;
- Planeamento e desenvolvimento de competências no trabalho em equipa;
- Documentação e apresentação correta do projeto.



universidade de aveiro

escola superior de tecnologia e  
gestão de água



## 2 - ARQUITETURA DE REDE

Neste tópico apenas é abordada a solução proposta para a arquitetura de rede.

### 2.1 - SOLUÇÃO PROPOSTA

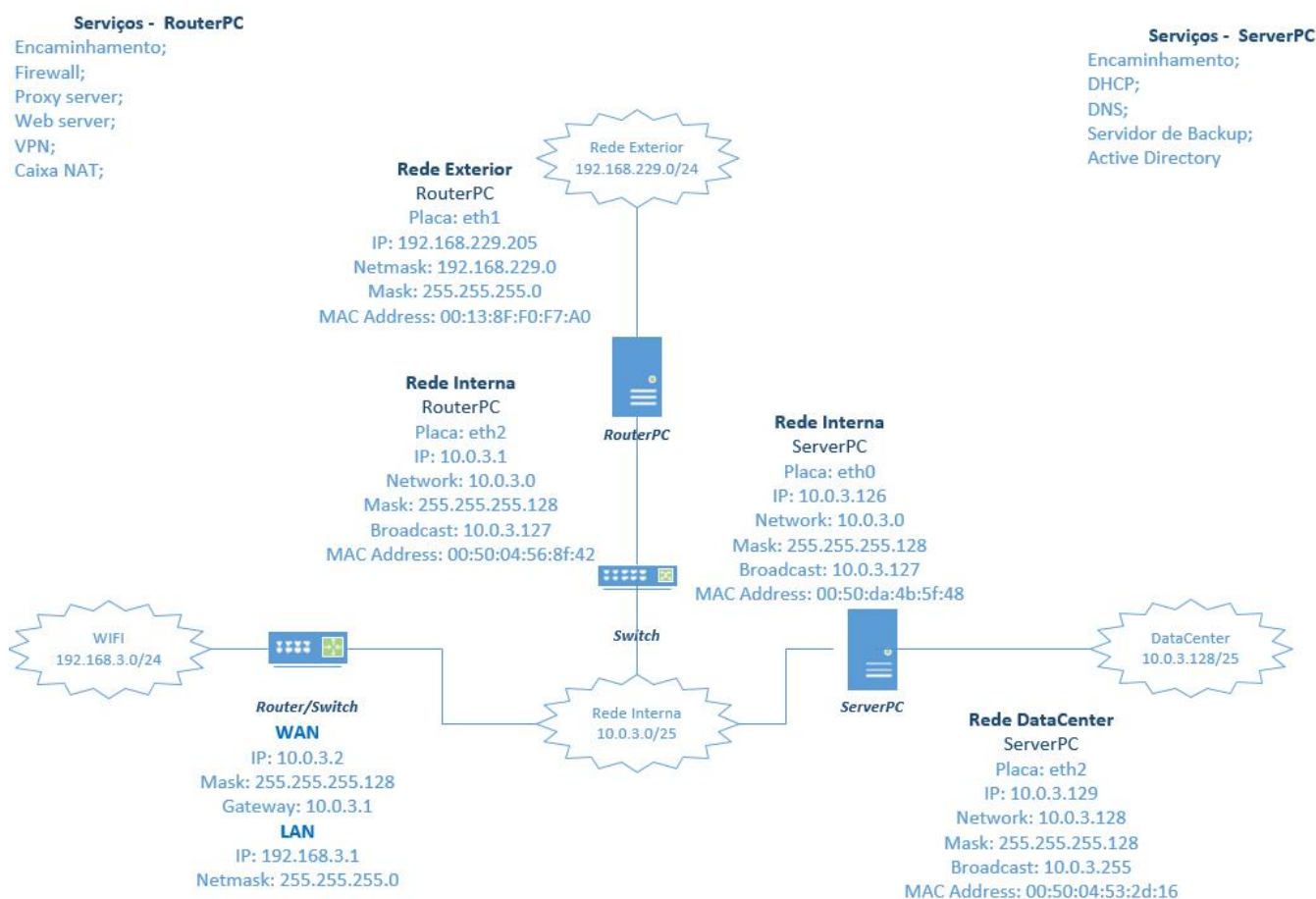


Diagrama 1 - Diagrama de rede





universidade de aveiro

escola superior de tecnologia e  
gestão de água



### 3 - PLANEAMENTO

No Planeamento serão abordados três tópicos: Requisitos, Tarefas (este divide-se em três subtópicos) e Orçamento.

#### 3.1 - REQUISITOS

O levantamento dos requisitos foi efetuado com base no enunciado do projeto e refere-se a algumas funcionalidades que a rede deve conter, como enumera a seguinte tabela:

Tabela 1 - Requisitos do Projeto

Código	Requisito
1	Serviço de encaminhamento
2	Serviço de tradução de nomes
3	Serviço para atribuição de endereços dinâmicos
4	Serviço para proteger a rede
5	Serviço para possibilitar o acesso à rede, a partir do exterior
6	Servidores com Sistema Operativo baseado em Linux
7	Serviço para alojar a página web da empresa
8	Serviço de backup
9	Rede sem fios com autenticação
10	Serviço de proxy



### 3.2 - TAREFAS

Neste tópico serão abordados temas como a definição, a divisão e a calendarização das tarefas.

#### 3.2.1 - DEFINIÇÃO DE TAREFAS

A definição das tarefas aqui apresentada engloba todo o trabalho desenvolvido desde o início do projeto.

Na seguinte tabela estão descritas todas as tarefas que foram realizadas para a conclusão deste projeto consoante os requisitos apresentados anteriormente.

Tabela 2 - Definição das tarefas

Código	Tarefas	
A	Gestão do Projeto	
	1	Levantamento dos requisitos
	2	Planeamento
	3	Divisão e calendarização de tarefas
	4	Orçamento
	5	Relatório
	6	Entrega
B	Instalação Sistemas Operativos	
C	Configuração da rede	
	1	Configuração - Encaminhamento
	2	Instalação e configuração - DNS
	3	Instalação e configuração - DHCP
	4	Instalação e configuração - Proxy
	5	Instalação e configuração - HTTP
	6	Instalação e configuração - VPN
	7	Instalação e configuração - Firewall
	8	Instalação e configuração - Backup
	9	Instalação e configuração - Active Directory
D	Fase de Testes	



A tarefa A divide-se em seis subtarefas para uma melhor gestão do projeto, assim como a tarefa C para que a divisão das configurações de rede fosse possível. Cada elemento do grupo participou ativamente em uma ou mais configurações.

### 3.2.2 - DIVISÃO DE TAREFAS

Com base nas tarefas definidas procedeu-se à divisão das mesmas, existindo tarefas comuns e individuais.

A tabela seguinte representa a divisão de tarefas:

Tabela 3 – Divisão de tarefas

Código	Tarefas		Membro do grupo	Tempo previsto (dias)
A	Gestão do Projeto			81
	1	Levantamento dos requisitos	Todos	5
	2	Planificação	Todos	4
	3	Divisão e calendarização de tarefas	Todos	3
	4	Orçamentação	Todos	2
	5	Relatório	Todos	75
	6	Entrega	Todos	1
B	Instalação Sistemas Operativos		Todos	5
C	Configuração da rede			72
	1	Configuração - Encaminhamento	PE,PA,CA	*
	2	Instalação e configuração - DNS	PA,Pa	*7
	3	Instalação e configuração - DHCP	PE,CA	*21
	4	Instalação e configuração - Proxy	Pa	*14
	5	Instalação e configuração - HTTP	Pa	*8
	6	Instalação e configuração - VPN	PE,CA	*7
	7	Instalação e configuração - Firewall	PA,PE	*10
	8	Instalação e configuração - Backup	PA	*19
	9	Instalação e configuração - Active Directory	PA,Pa	*21
D	Fase de Testes		Todos	72



### 3.2.3 - CALENDARIZAÇÃO DE TAREFAS

A calendarização das tarefas está representada no seguinte diagrama de Gantt.

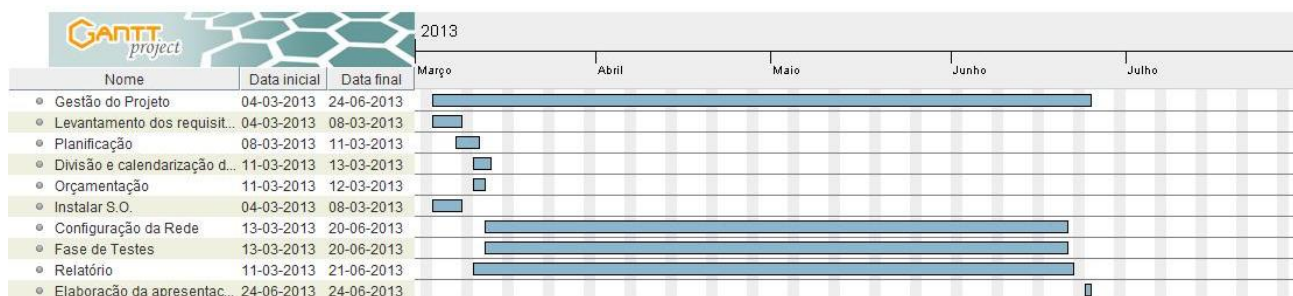


Diagrama 2 - Calendarização das tarefas

### 3.3 - ORÇAMENTO

Segundo os requisitos estipulados, consta na tabela seguinte o orçamento do equipamento.

Tabela 4 - Orçamento

Equipamento	Descrição	Quantidade	Preço
Switch	TP-LINK GIGABIT SWITCH 24P SG1024D	2	€ 219,98
Router	ASUS RT-AC66U (802.11AC DUAL-BAND AC1750 GIGABIT ROUTER)	1	€ 182,99
Servidor	HP PROLIANT BL260C G5 - INTEL XEON E5420 QUAD-CORE 2,50 GHZ,	2	€ 2 799,98
Mão-obra	Instalação e configuração (€ 5/h)	<sup>(1)</sup> 648	€ 3 240
Opcional	Manutenção dos serviços prestados (Anual)	---	€ 1 999,99
<b>Total:</b>			<b>€ 8 442,94</b>

<sup>(1)</sup> Horas (81\*8 = 648)



## 4 - IMPLEMENTAÇÃO

A implementação divide-se em três tópicos, nomeadamente a Lista de hardware utilizado, a Lista de software utilizado e a Configuração das aplicações/serviços instalados.

### 4.1 - LISTA DE HARDWARE UTILIZADO

Para a implementação do projeto foram-nos facultadas três máquinas, sendo duas delas mais potentes com o objetivo de serem utilizadas como servidores.

A terceira serviria para cliente, mas acabou por não ser utilizada devido a problemas de instalação do Sistema Operativo.

Em termos de equipamentos de rede, utilizámos apenas dois: um switch e um router/switch.

O switch permite a ligação local aos funcionários da empresa, enquanto o router/switch funciona como Access Point para a rede sem fios.

Utilizámos cabos de rede (RJ-45) para a conexão de todo o hardware.

### 4.2 - LISTA DE SOFTWARE UTILIZADO

O cliente exigiu que fossem utilizados Sistemas Operativos baseados em Linux, para diminuição de custos, nos servidores.

Na tabela seguinte estão descritos os Sistemas Operativos.

Tabela 5 - Lista de Sistemas Operativos utilizados

Servidor	Nome
RouterPC	Debian Server 2.30.2
ZentyalServer	Zentyal Server 3.0



Inicialmente, tínhamos instalado o Sistema Operativo Debian Server 2.30.2 nos dois servidores, mas devido à implementação do Active Directory (descrito posteriormente) tivemos que instalar o Zentyal .

O software utilizado para a implementação de serviços foi:

- bind9 (DNS - sendo descartado aquando da instalação do Zentyal);
- isc-dhcpd-server (DHCP - sendo descartado aquando da instalação do Zentyal);
- firestarter (firewall - sendo descartado posteriormente);
- squid (proxy);
- pptpd (VPN);

## 4.3 - CONFIGURAÇÃO DAS APLICAÇÕES/SERVIÇOS INSTALADOS

### 4.3.1 - Encaminhamento

O encaminhamento serve para que as máquinas tenham rede entre si e também acesso à Internet. Sem isto, nenhuma máquina da rede *10.0.3.128* teria acesso à rede *10.0.3.0* e à Internet.

Para tal, é necessário adicionar a seguinte instrução no ficheiro *interfaces* na pasta */etc/network*:

```
post-up route add -net 10.0.3.128 netmask 255.255.255.128 gw 10.0.3.126
```

Para que os servidores sejam reconhecidos como routers é necessário "descomentar" a seguinte linha no ficheiro *sysctl.conf* na pasta */etc*:

```
net.ipv4.ip_forward=1
```



#### 4.3.2 - DNS

##### Configuração inicial:

Inicialmente, tínhamos o servidor ServerPC com o Sistema Operativo Debian, mas devido a conflitos do Active Directory fomos forçados a instalar outro Sistema Operativo baseado em Linux, o Zentyal.

O DNS tem como principal função fazer a tradução de nomes para endereços IPs, isto é converter *www.google.com* em *173.194.45.31*, por exemplo. Neste sentido, é necessário instalar o pacote do *bind9* através do seguinte comando:

```
apt-get install bind
```

As principais configurações para este serviço são:

- Atribuição do servidor de nomes (ns1r.gr3.estga.ua.pt - 10.0.3.126);
- Configuração de domínio (gr3.lr.estga.ua.pt);
- Criação e configuração da zona primária e zona inversa.

A atribuição do nome do servidor e seu domínio é configurado no ficheiro da zona primária, que se encontra em */etc/bind/zones/gr3.lr.estga.ua.pt*.

Por sua vez, o ficheiro da zona inversa encontra-se em */etc/bind/zones/10.0.3.rev*.

É de notar que o DNS estava bem configurado e funcional, mas com a alteração do Sistema Operativo voltamos ao princípio. No entanto, ficámos com a vantagem de o mais difícil estar feito, visto que apenas adaptamos os conteúdos dos ficheiros utilizados pelo Debian para a interface gráfica do Zentyal.





### **Configuração Final**

Antes de iniciar a configuração deste serviço é necessário ativar o módulo do Sistema Operativo.

As principais configurações necessárias para este serviço são:

- Configurar o nome do servidor de nomes (*ztserver.gr3.lr.estga.ua.pt*);
- Ativar o "*Enable transparent DNS cache*";
- Estipular o *forwarder* como um endereço de nomes da UA (193.136.172.20 - por exemplo);
- Configurar o domínio do *DNS* (*gr3.lr.estga.ua.pt*);

Devido a alguns erros de compatibilidade entre Sistemas Operativos é necessário a adição de um conjunto de registo do tipo *SRV* (fornece informações sobre os serviços disponíveis no domínio). Os registos adicionados foram os seguintes:

*\_ldap.\_tcp.dc.\_msdcs.nomedomínio IN SRV 0 0 389 nome\_DC*

*\_ldap.\_udp.dc.\_msdcs.nomedomínio IN SRV 0 0 389 nome\_DC*

*\_kerberos-master.\_udp.dc.\_msdcs.nomedomínio IN SRV 100 100 8880 nome\_DC*

*\_kpasswd.\_tcp.dc.\_msdcs.nomedomínio IN SRV 100 100 8464 nome\_DC*

*\_kpasswd.\_udp.dc.\_msdcs.nomedomínio IN SRV 100 100 8464 nome\_DC*



### 4.3.3 - DHCP

#### Configuração inicial:

A seguinte configuração do DHCP deixou de ter efeito após a alteração do Sistema Operativo.

O DHCP tem como principal função atribuir endereços IPs às máquina que estão ligadas na rede. Deste modo, é necessário instalar o pacote *isc-dhcp* através do seguinte comando:

```
apt-get install isc-dhcp-server
```

O processo de configuração deste serviço passa pelo ficheiro *dhcpd.conf*, que está localizado na pasta */etc/dhcp*.

Neste ficheiro configura-se a gama de endereços a serem utilizados pelas máquina que se ligarem à rede, como demonstra o seguinte código:

```
subnet 10.0.3.0 netmask 255.255.255.128 { # Para a rede 10.0.3.0

    range 10.0.3.1 10.0.3.126;

}

subnet 10.0.3.128 netmask 255.255.255.128 { # Para a rede 10.0.3.128

    range 10.0.3.129 10.0.3.254;

}
```

Como o serviço de DNS e o DHCP estão interligados, é necessário que o servidor de nomes esteja indicado no ficheiro acima referido para que os computadores da rede possam fazer a tradução de endereços (é necessário que esteja referido para as duas redes). Para que isso aconteça apenas é necessário acrescentar o seguinte código:

```
option routers nslr.gr3.lr.estga.ua.pt;
```



Os servidores utilizam endereços IPs fixos para que não haja conflitos internos. No entanto, é importante e necessário que o servidor DHCP o saiba, criando exceções, da seguinte maneira:

```
host router {  
  
    hardware ethernet 00:50:04:56:8F:42; #eth2 - RouterPC  
  
    fixed-address 10.0.3.1;  
  
}  
  
host router {  
  
    hardware ethernet 00:50:da:4b:5f:48; #eth0 - ServerPC  
  
    fixed-address 10.0.3.126;  
  
}
```

### **Configuração Final**

Para este serviço estar ativo é necessário fazer a ativação do módulo no *Zentyal*.

Em primeiro lugar, é necessário especificar a interface e o seu endereço fixo. Por exemplo, a interface *eth0* fica com o endereço fixo *10.0.3.126* e a *eth2* com o *10.0.3.129*.

Após a conclusão da operação, torna-se necessário fazer uma configuração mais detalhada de cada interface. Isto é, definir o *gateway* da máquina, o endereço do servidor de nomes (*DNS*) e ainda o servidor de samba.

É de salientar que na página de configuração do DHCP ainda podemos configurar a gama para as redes e suas exceções.



#### 4.3.4 - Proxy

O serviço de proxy é necessário para controlar o que se passa na rede. O cliente faz um pedido Web, o servidor proxy é que fica encarregue de carregar a página ao cliente. Se a página estiver em cache, o servidor carrega imediatamente, senão tem que pedir ao servidor externo.

A instalação do pacote squid faz-se da seguinte maneira:

```
apt-get squid
```

O principal ficheiro de configuração deste serviço está localizado na pasta */etc/squid*, mais propriamente no ficheiro *squid.conf*. Neste ficheiro é indicada a porta por qual a comunicação é efetuada e o tipo de proxy, neste caso transparente.

```
http_port 3128 transparent
```

O nome do servidor de proxy e respetivo endereço IP é:

```
visible_hostname servidorProxy
```

```
acl localhost src 127.0.0.1/255.255.255.255
```

E ainda exceções da rede, isto é, o bloqueio de sites e/ou palavras chave e extensões.

```
acl bloq_sites url regex -i "/etc/squid/sites"
```

```
http_access deny bloq_sites
```

```
acl_bloq_palavras url regex -i "/etc/squid/palavras"
```

```
http_access deny palavras
```

```
acl_bloq_ext url regex -i "/etc/squid/bloq_ext"
```

```
http_access deny bloq_ext
```



#### 4.3.5 - HTTP

O serviço HTTP é necessário para que a empresa possa ter uma página web alojada. Este serviço foi configurado no Zentyal de forma gráfica com as configurações pré-definidas, embora tivéssemos que ativar o módulo do serviço.

O HTTP funciona da seguinte maneira: o cliente faz um pedido ao servidor e este responde ao pedido feito pelo cliente. É um sistema de pedido-resposta.

O Zentyal utiliza o Apache para fazer a administração do servidor HTTP, que, por padrão, utiliza o porto 80 para comunicar com os clientes.

Para colocar a página web "online" é necessário colocá-la no diretório */var/www*.

Para aceder à página web da máquina que tem o serviço ativo, apenas é necessário colocar: *localhost/index.html*.

Para aceder à página web de outra máquina é necessário introduzir no URL o IP do servidor HTTP. Por exemplo:

*10.0.3.126/index.html*



#### 4.3.6 - VPN

Este serviço permite a ligação à rede a partir do exterior. A configuração deste serviço divide-se em duas fases: a configuração do servidor e a configuração do cliente.

##### Servidor

Para instalar este serviço é necessário utilizar o seguinte comando:

```
apt-get install pptpd
```

O IP do servidor e do cliente é configurado no ficheiro *pptpd.conf* na pasta */etc*, onde o *localip* é o endereço do servidor e o *remoteip* a gama de endereços disponíveis para o cliente, como demonstra o seguinte código:

```
localip 10.0.3.1
```

```
remoteip 10.0.3.2-125
```

No ficheiro *pptpd-options* define-se o endereço do servidor de DNS.

```
ms-dns 10.0.3.126
```

Este serviço precisa de uma autenticação, sendo definida no ficheiro *chap-secrets*.

```
#client server secret IP addresses
```

```
teste * teste *
```

O significado da linha anterior é nome do utilizador, servidor, password, endereço IP.



### Cliente

A configuração do Cliente foi realizada numa máquina com Windows 7, com os seguintes passos:

- Centro de Rede e Partilha;
- Configurar uma nova ligação ou rede;
- Ligar a uma área de trabalho;
- Criar nova ligação;
- Utilizar a minha ligação à Internet;
- Digitar o endereço IP do Servidor e nome da VPN;
- Digitar utilizador e password;
- Ligar.

Para que o serviço funcione corretamente, foi necessário fazer uma configuração adicional:

- Propriedades "nome da VPN" (configurado anteriormente);
- Propriedades Protocolo TCP/IPv4;
- Avançadas -> Retirar "visto" de "Utilizar gateway predefinido na rede remota".



#### 4.3.7 - Firewall

Para implementar a firewall o grupo optou, primeiramente, por instalar o pacote firestarter. Este pacote tem uma interface gráfica para a criação de exceções na firewall. Após a instalação deste pacote, o grupo considerou que este não preenchia os requisitos pedidos. Assim sendo, e a conselho do orientador de projeto, o grupo começou a aventurar-se pelas iptables.

Inicialmente começamos a criar as regras na linha de comandos e, para não as perder, estas foram guardadas num ficheiro. A instrução para guardar as regras num ficheiro é a seguinte:

```
iptables-save > /etc/Firewall.sh
```

Cada vez que criávamos uma regra era necessário fazer o "restore" do ficheiro, para que a nova regra entrasse em vigor com a instrução:

```
iptables-restore < /etc/Firewall.sh
```

A principal lógica das iptables é a seguinte: existem as regras de entrada e as regras de saída e o forward no meio. Se a saída apanha uma regra é porque a entrada assim o deixou. O forward serve apenas de mediador. Em baixo, apresentamos alguns exemplos de regras de entrada e regras de saída.

```
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
```

A regra de entrada em cima serve para que um pedido de *ssh* passe pela firewall.

A regra de saída em baixo serve para que um pedido de DNS possa sair pela firewall.

```
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
```

Para evitar o carregamento deste ficheiro, todas as vezes que se liga a máquina onde este serviço está instalado, é necessário associar o ficheiro, onde estas regras estão acordadas, ao arranque da máquina. Para tal, coloca-se a seguinte instrução no ficheiro *rc.local* situado na pasta */etc*:

```
iptables-restore < /etc/Firewall.sh
```





#### 4.3.8 - Backup

O serviço de Backup serve para guardar em segurança os ficheiros da rede. Para este serviço funcionar é necessário ativá-lo no Zentyal.

As configurações mais importantes são: a localização do ficheiro de backup (localmente ou remotamente), a autentificação, a frequência do Backup (por exemplo: semanalmente e à Quarta-Feira), a hora a que o processo é iniciado e, ainda, o número de Backups anteriormente guardados.

#### 4.3.9 - Active Directory

Este serviço foi configurado no *Zentyal*, sendo necessário ativar o seu módulo.

A partir do *Active Directory* é possível criar grupo e utilizadores. Na criação do grupo podemos especificar, por exemplo, o diretório da pasta partilhada e quais os utilizadores membros do grupo. Na criação do utilizador, os campos mais importantes são o nome, o utilizador e palavra passe, a quota, o tráfego e a que grupo pertencem (se pertencem a um).

Para que o utilizador aceda à pasta partilhada é necessário que faça a autentificação com o domínio previamente criado.



## 5 - VALIDAÇÃO E VERIFICAÇÃO

### 5.1 - TESTES DE SISTEMA

#### 5.1.1 - Encaminhamento

O teste mais rápido e eficaz de testar este serviço é fazer *ping* de uma máquina ligada na rede 10.0.3.0 a uma máquina que esteja ligada à rede 10.0.3.128, e vice-versa.

Por ventura, podemos ligar uma máquina à rede 10.0.3.128 para testar a sua conexão à Internet. Visto que neste ponto ainda não tínhamos o DNS configurado, tivemos que usar o servidor de DNS da UA para testar o acesso à Internet.

#### 5.1.2 - DNS

As principais ferramentas usadas pelo grupo para a validação e verificação do serviço de DNS foram o *nslookup* e o *named-checkzone*.

O comando *nslookup* é utilizado para descobrir o servidor de nomes do domínio. A sua sintaxe é a seguinte:

```
nslookup www.google.com
```

A resposta deste pedido será algo deste género:

```
Server: 10.0.3.126
```

```
Address: 10.0.3.126#53
```

O comando *named-checkzone* serve para verificar se os ficheiros de configuração das zonas contêm erros ou não.

```
named-checkzone gr3.lr.estga.ua.pt /etc/bind/zones/gr3.lr.estga.ua.pt
```

A instrução acima teria um resultado igual ao mencionado em baixo, caso estivesse correto.

```
zone gr3.lr.estga.ua.pt/IN: loaded serial 1
```

```
Ok
```



### 5.1.3 - DHCP

Após a instalação e configuração do serviço de DHCP procedemos aos testes.

Para verificar se o serviço está corretamente configurado poderá ligar-se várias máquinas à rede e constatar que o endereço IP pertence à gama correta. Se o endereço IP atribuído ao cliente estiver na gama da rede a que este se ligou, então o DHCP foi configurado corretamente.

### 5.1.4 - Proxy

Para a verificação do funcionamento da Proxy, usámos dois métodos:

- introduzir o endereço de um website, previamente bloqueado, no browser;
- utilizar a ferramenta *wget*;

O objetivo da Proxy era ser transparente, isto é, não haver necessidade de configurar manualmente o endereço do servidor Proxy e sua porta (10.0.3.1 - 3128) em cada cliente.

No entanto, não foi isto que aconteceu. Assim, para testar se a Proxy estava ativa, configurou-se o browser do cliente com os dados acima referidos.

Com a Proxy a funcionar, testou-se imediatamente o funcionamento do bloqueio de sites, que foi funcional.

A ferramenta *wget* testa se o tráfego fica em cache. Por exemplo, numa imagem:

```
wget -r http://bairradigital.pt/blog/wp-content/uploads/2011/03/estga.gif
```

### 5.1.5 - HTTP

Para testar se este serviço está ativo, criámos uma pequena página web e guardámo-la na pasta do servidor.

Para aceder localmente (mesma máquina que o servidor *HTTP*) à página de teste, foi apenas necessário colocar a seguinte instrução no browser:

```
127.0.0.1/index.html
```



Caso estejamos numa máquina diferente temos que indicar o *IP* do servidor HTTP e depois a página.

*10.0.3.126/index.html*

#### **5.1.6 - VPN**

Em primeiro lugar, é necessário referir que este serviço não foi verificado dado a impossibilidade de acesso devido às configurações dos servidores do laboratório de redes.

Caso fosse possível fazer a verificação deste serviço, teríamos que tentar a conexão a partir do cliente (este tinha que estar ligado à rede do laboratório).

Para a conexão é necessário fazer a autentificação e verificar se era feita com sucesso.

#### **5.1.7 - FIREWALL**

Na validação e verificação deste serviço o grupo optou por criar a regra e testá-la imediatamente para minimizar eventuais erros.

Primeiramente, criámos uma regra que "fechou" todo o tráfego da rede e sucessivamente fomos criando as exceções para cada um dos serviços necessários.

Por exemplo, no "fecho" do tráfego da rede, se introduzirmos um endereço de uma página web ([www.google.com](http://www.google.com)), haveria erro de DNS, pois o serviço estava bloqueado. Mas se introduzíssemos o seu endereço IP (173.194.45.31), a página web carregaria sem problemas.



### 5.1.8 - BACKUP

Para verificar o funcionamento deste serviço apenas é necessário aceder à pasta onde o *Backup* seria guardado (previamente configurado) e verificar a existência do ficheiro.

## 5.2 - VALIDAÇÃO DE REQUISITOS

Tabela 1 - Requisitos do Projeto

Código	Requisito	Estado
1	Serviço de encaminhamento	✓
2	Serviço de tradução de nomes	✓
3	Serviço para atribuição de endereços dinâmicos	✓
4	Serviço para proteger a rede	✓
5	Serviço para possibilitar o acesso à rede, a partir do exterior	✓
6	Servidores com Sistema Operativo baseado em Linux	✓
7	Serviço para alojar a página web da empresa	✓
8	Serviço de backup	✓
9	Rede sem fios com autenticação	✓ x
10	Serviço de proxy	✓

Como se pode verificar pela tabela acima, todos os requisitos propostos foram concluídos (apenas a autenticação na rede sem fios tem alguns problemas).



## 6 - CONCLUSÃO

Este relatório descreve todos os procedimentos necessários para a conclusão deste projeto.

Inicialmente, o grupo teve algumas dificuldades para definir as suas metas de trabalho o que atrasou a sua elaboração. Após a conclusão do levantamento dos requisitos e sua divisão entre os elementos do grupo, começámos realmente a implementar os conhecimentos que íamos adquirindo ao longo das aulas da unidade curricular de Redes e Sistemas Operativos.

Tivemos alguns imprevistos, nomeadamente a mudança de Sistema Operativo em um dos servidores, algumas dificuldades técnicas com os serviços que necessitávamos e ainda erros físicos dos aparelhos de rede. Neste sentido, a ajuda dos colegas e orientadores de projeto foi fulcral para o sucesso do mesmo.

Em suma, todos os elementos do grupo que participaram ativamente no projeto têm a mesma opinião sobre o mesmo, considerando-o importante e gratificante, já que nenhum de nós tinha experiência com administração de sistemas.



universidade de aveiro

escola superior de tecnologia e  
gestão de água



## 7 - FONTES E MATERIAL DE REFERÊNCIA

Para a instalação e configuração dos serviços utilizámos várias fontes, nomeadamente:

- [www.moodle.ua.pt](http://www.moodle.ua.pt) - Slides da unidade curricular de Redes e Sistema Operativos;
- <http://www.cyberciti.biz/tips/configuring-static-routes-in-debian-or-red-hat-linux-systems.html> - Configuração do encaminhamento;
- <http://doc.zentyal.org/en/> - Configuração dos serviços de *DNS*, *DHCP*, *Active Directory* e *Backup*;
- <http://www.hardware.com.br/livros/servidores-linux/criando-uma-configuracao-basica.html> - Configuração da *Proxy*;
- <http://www.howtogeek.com/51237/setting-up-a-vpn-pptp-server-on-debian/> - Configuração do servidor e cliente de *VPN*.