

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
CTeSP em Redes e Sistemas Informáticos

Projeto e Análise de Políticas de Segurança
Projeto

Guilherme Rodrigues Vieira

Beja

24/01/2022

Índice

1. Introdução	5
2. Topologia da Rede.....	5
3. Tabela de VLSM	7
4. Instalação e Configuração IPfire.....	8
5. Configuração do Router	16
6. Configuração do Switch.....	17
7. Configuração dos Hosts.....	20
7.1 VPCs	20
7.2 Servidor TFTP	22
7.3 Máquina Windows	24
8. Monitorização	25
8.1 Instalação e Configuração do Zabbix	25
8.2 Configurar utilizadores no Zabbix	28
8.2.1 Máquina Windows	28
8.2.2 Máquina TFTP.....	30
9. Aplicação das ACLs	33
10. Guardar todas as configurações aplicadas ao Router	36
11. Políticas	37
11.1 Política de Segurança Física e Ambiental.....	37
11.2 Política de Controlo de Acessos à Informação	38
11.3 Política de Gestão das Operações e das Comunicações.....	38
11.4 Política de Gestão de Incidentes.....	39
12. Conclusão	39

Lista de Tabelas

Tabela 1 – VLSM	7
Tabela 2 – Endereços de Todas as Interfaces.....	7

Lista de Figuras

Figura 1 – Rede da empresa	6
Figura 2 – Representação da localização das máquinas	6
Figura 3 – Interface Green e Red.....	8
Figura 4 – Interface Red.....	8
Figura 5 – Interface Green.....	9
Figura 6 – Interface Green não fazer DHCP.....	9
Figura 7 – Atribuição de IP para interface Red.....	10
Figura 8 – Ping da interface Red do IPfire para o google	10
Figura 9 – Acesso á interface do IPfire	11
Figura 10 – Acesso ao URL Filter.....	12
Figura 11 – Configuração do URL Filter	12
Figura 12 – Antes de ser aplicada o filtro de URL.....	13
Figura 13 – Configuração Web do URL Filter.....	13
Figura 14 – Configurar a largura de banda.....	14
Figura 15 – Configuração do proxy na máquina Windows	14
Figura 16 – Confirmação do bloqueio de URLs	15
Figura 17 – Configuração básica do router	16
Figura 18 – Configuração de Vlans no router	16
Figura 19 – Todas as subinterfaces do Router	17
Figura 20 – Encaminhamento do router para o IPfire.....	17
Figura 21 – Criação de Vlans no switch	18
Figura 22 – Interfaces configuradas para cada Vlan	19
Figura 23 – Guardar as configurações do Switch	19
Figura 24 – Pings VPC design/paginação.....	20
Figura 25 – Pings VPC Administração Comercial.....	20
Figura 26 – Pings VPC Direção	21
Figura 27 – Pings VPC Redação.....	21
Figura 28 – Guardar configurações dos VPCs.....	21
Figura 29 – Instalação do TFTP	22
Figura 30 – Comandos para configurar o TFTP.....	22
Figura 31 – Configurar o /etc/default/tftpd-hpa.....	23
Figura 32 – Atribuição de endereço á máquina TFTP e ping ao 8.8.8.8.....	23
Figura 33 – Configurar a interface da máquina Windows (departamento de informática)	24
Figura 34 – Pingar a internet com a máquina Windows	24

Figura 35 – Acesso á interface gráfica do Zabbix	26
Figura 36 – Finalização da configuração do servidor Zabbix.....	26
Figura 37 – Configuração da interface da máquina Zabbix.....	27
Figura 38 – Ping ao servidor TFTP e ping ao google	27
Figura 39 – Instalação do Zabbix agente na máquina Windows	28
Figura 40 – Restart do Zabbix agent.....	28
Figura 41 – Inserir a máquina Windows no Zabbix	29
Figura 42 – Verificação da implementação da máquina no Zabbix	29
Figura 43 – Instalação do Zabbix agent na máquina TFTP	30
Figura 44 – Configuração do ficheiro Zabbix_agentd.conf - 1	30
Figura 45 – Configuração do ficheiro Zabbix_agentd.conf - 2	31
Figura 46 – Inserir o servidor TFTP no Zabbix	31
Figura 47 – Mapa Zabbix	33
Figura 48 – Criação das ACLs estendidas.....	33
Figura 49 – Confirmação da aplicação das ACLs - Redação.....	34
Figura 50 – Confirmação da aplicação das ACLs – Design/Paginação.....	34
Figura 51 – Confirmação da aplicação das ACLs – Zabbix	35
Figura 52 – Guardar configurações dentro do servidor TFTP	36

1. Introdução

Este trabalho teve como objetivo preparar os alunos para uma situação profissional, no caso estes tinham de realizar uma topologia de rede bem estruturada que conseguisse suportar as necessidades de uma empresa de comunicação social “JORNAL INVICTUS”, esta empresa como o nome indica é do ramo do jornalismo, a rede projetada para esta empresa precisa de pelo menos suportar 15 máquinas para 5 departamentos diferentes, no caso 7 para a redação, 3 para o departamento de design gráfico/paginação, 2 para o departamento de Administrativo e Comercial, 2 para o departamento de IT e segurança informática e 1 para o diretor. Com estas exigências em mente foi criada uma topologia de rede que as suportasse, rede essa que possui um sistema de monitorização que serve para monitorizar as máquinas importantes/críticas da empresa, foram ainda aplicadas medidas de segurança como é o caso do IPfire, este filtra a comunicação da rede e ACLs que bloqueiam a comunicação entre certas máquinas da rede com outras máquinas.

2. Topologia da Rede

Esta rede é composta por 1 Cloud, 1 máquina com IPfire, 1 máquina TFTP, 1 máquina Zabbix, 1 máquina Windows do departamento de informática.

A máquina servidor IPfire está situada mais perto da cloud a fim de filtrar a informação/dados provenientes da internet com o intuito de proteger a rede interna de possíveis pacotes ou ataques maliciosos e bloquear sites perigosos.

A máquina TFTP foi algo extra que implementei no projeto com o objetivo de poder guardar backups, nomeadamente guardei o backup do router pois caso o mesmo se estragasse a empresa poderia mais facilmente repor as configurações do router noutro equipamento fazendo com que a interruptibilidade dos serviços da empresa fosse menos afetada, poupando assim algum tempo.

A máquina Zabbix é usada como serviço de monitorização, esta apenas consegue monitorizar 2 máquinas (Windows e TFTP) pois são as únicas máquinas sem contar com a máquina Zabbix e IPfire que são máquinas virtuais, o resto são VPCs (computadores virtuais), esta prática foi adotada por mim pois apenas considero que as máquinas virtuais sejam elementos críticos da minha rede interna.

Os VPCs representam diferentes departamentos como se pode visualizar na figura 1, apenas não inseri todas as máquinas de cada departamento porque iria dificultar a interpretação da rede, para tal tenho a figura 2 que mostra em que parte do edifício da empresa vai ficar cada máquina.

No router e o switch foram criadas e aplicadas Vlans para conseguir comunicar entre Vlans de cada departamento, foram ainda aplicadas ACLs para bloquear a comunicação entre os VPCs e as máquinas servidor.

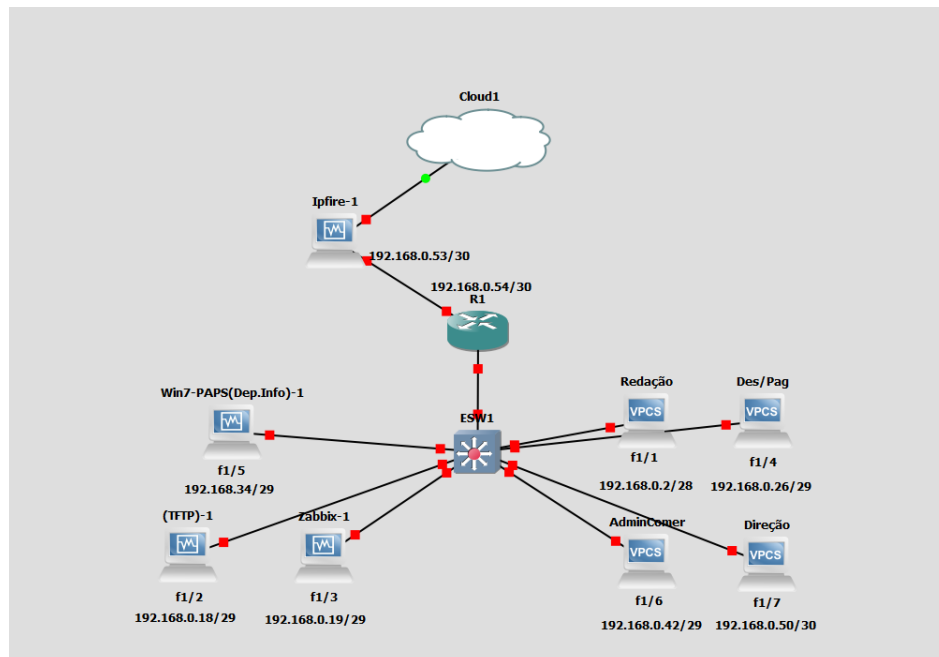


Figura 1 - Rede da empresa

A figura 2 é uma demonstração da disposição das máquinas da empresa, sendo que a redação têm 7 máquinas, o departamento de design tem 3, o departamento administrativo tem 2 máquinas, o departamento informático tem 4 máquinas dentro de si, 2 são os servidores TFTP e Zabbix que pertencem ao datacenter e as outras duas são máquinas Windows e por fim a direção que apenas tem uma máquina.

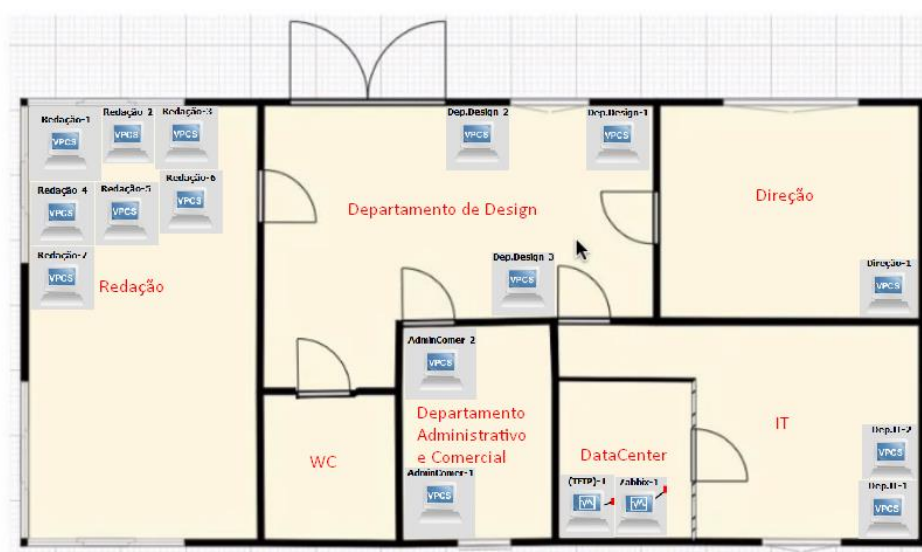


Figura 2 – Representação da localização das máquinas

3. Tabela de VLSM

Antes de começar o projeto propriamente dito foi necessário em primeiro lugar definir os endereços necessários para a rede, depois de definidos foi possível começar a atribuí-los á rede.

Na tabela 1 estão os endereços de cada segmento da rede, no caso começa-se pela redação pois é o segmento da rede interna com maior tamanho de endereços, nesse segmento de rede escolhi possibilitar até 14 possíveis computadores na Vlan pois tenho em mente o crescimento da empresa e como tal é melhor dar alguma margem de crescimento. Nas Vlans até chegar á direção e IPfire escolhi dar 6 possíveis endereços dando assim espaço para um possível crescimento de máquinas e por fim na direção e no IPfire como apenas são as únicas máquinas nas suas Vlans apenas atribuí 2 endereços, 1 para a própria máquina e outro para a interface gateway de cada Vlan.

Na tabela 2 encontram-se os endereços de cada interface de cada dispositivo, esta tabela foi criada com o objetivo de facilitar a interpretação de cada interface, endereço, máscara, Vlan e a respetiva porta que a máquina estava conectada no switch.

TABELA DE VLSM - Jornal Invictus									
Subnet Name	Needed Size	Allocated Size	Total Size	Address	Mask	Dec Mask	Assignable Range	Broadcast	WildCard
Redação	7	14	16	192.168.0.0	255.255.255.240	/28	192.168.0.1 - 192.168.0.14	192.168.0.15	0.0.0.15
Data Center	2	6	8	192.168.0.16	255.255.255.248	/29	192.168.0.17 - 192.168.0.22	192.168.0.23	0.0.0.7
Departamento de Design Gráfico / Paginação	3	6	8	192.168.0.24	255.255.255.248	/29	192.168.0.25 - 192.168.0.30	192.168.0.31	0.0.0.7
Departamento de IT e Segurança Informática	2	6	8	192.168.0.32	255.255.255.248	/29	192.168.0.33 - 192.168.0.38	192.168.0.39	0.0.0.7
Departamento Administrativo e Comercial	2	6	8	192.168.0.40	255.255.255.248	/29	192.168.0.41 - 192.168.0.46	192.168.0.47	0.0.0.7
Direção	1	2	4	192.168.0.48	255.255.255.252	/30	192.168.0.49 - 192.168.0.50	192.168.0.51	0.0.0.3
IpFire	1	2	4	192.168.0.52	255.255.255.252	/30	192.168.0.53 - 192.168.0.54	192.168.0.55	0.0.0.3

Tabela 1 - VLSM

TABELA DE ENCAMINHAMENTO ESTÁTICO					
Subnet Name	Interface	Address	Mask	Vlans	Porta
Redação	E0/0	192.168.0.2	255.255.255.240	2	f1/1
TFTP	E0/0	192.168.0.18	255.255.255.248	3	f1/2
Zabbix	E0/0	192.168.0.19	255.255.255.248	3	f1/3
Des/Pag	E0/0	192.168.0.26	255.255.255.248	4	f1/4
Win7-PAPS-Dep.Info	E0/0	192.168.0.34	255.255.255.248	5	f1/5
AdminComercial	E0/0	192.168.0.42	255.255.255.248	6	f1/6
Direção	E0/0	192.168.0.50	255.255.255.252	7	f1/7
R1	F0/0	192.168.0.54	255.255.255.252		
	F0/1				
IpFire	E0/0	192.168.0.53	255.255.255.252		

Tabela 2 - Endereços de Todas as Interfaces

4. Instalação e Configuração IPfire

Na configuração das interfaces de rede foi necessário configurar a Red para conseguir comunicar com a internet e a green para comunicar com a rede interna.

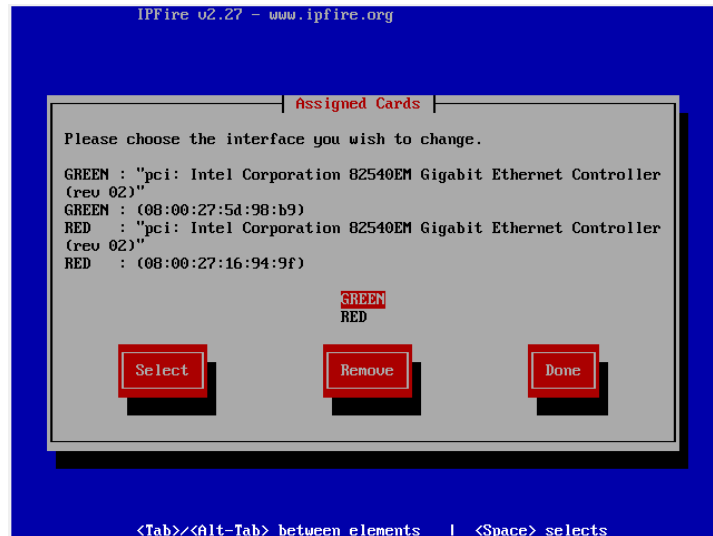


Figura 3 – Interface Green e Red

Na figura 4 é configurada a interface Red, esta vai aceder á internet e para tal é necessário configurar a mesma por DHCP para depois ser-lhe atribuída um IP, na figura 4 é possível visualizar a escolha de DHCP, caso fosse implementada a configuração errada era apenas necessário acabar a configuração da IPfire e depois escrever setup na linha de comandos e depois ir em interfaces e modificar a Red.

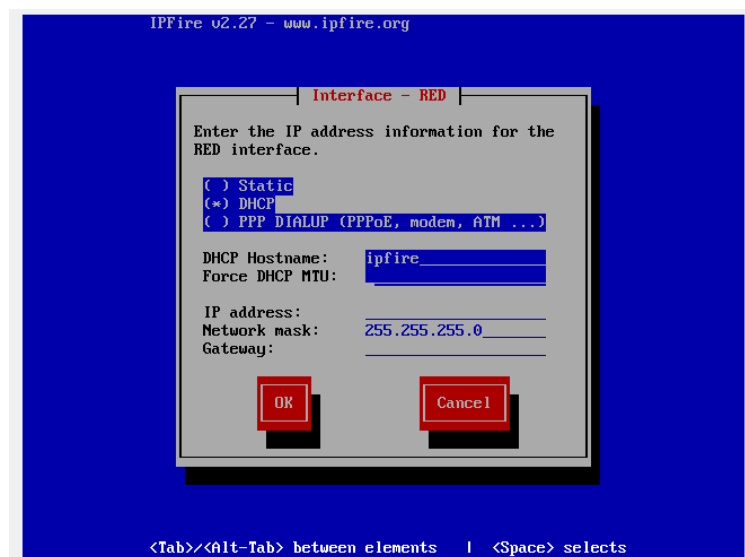


Figura 4 – Interface Red

A interface Green vai fazer o contacto entre a interface Red e a rede interna, como tal é preciso atribuir um IP dentro da gama da rede, no meu caso escolhi o IP 192.168.0.53 e a máscara 255.255.255.0.

Durante o desenvolvimento do projeto cheguei a ter um problema relacionado com a máscara da interface Green, conseguia fazer ping do router para a internet porém não conseguia que os VPCs fizessem ping para a internet, depois de algum tempo a testar resolvi mudar a máscara de rede de 255.255.255.252 para 255.255.255.0 e foi aí que começou a funcionar a internet nos VPCs e dos servidores para a internet.

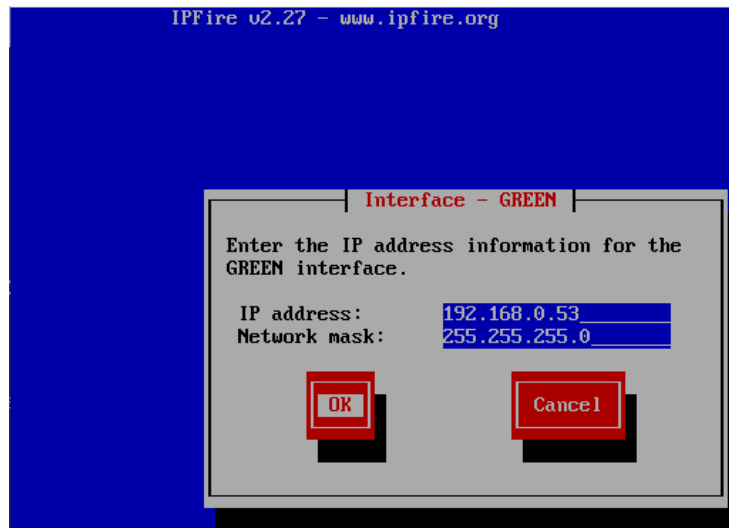


Figura 5 – Interface Green

Na configuração da interface Green do IPfire foi necessário apenas clicar OK na parte da configuração do DHCP para assim não ser atribuído o DHCP dentro da rede interna.

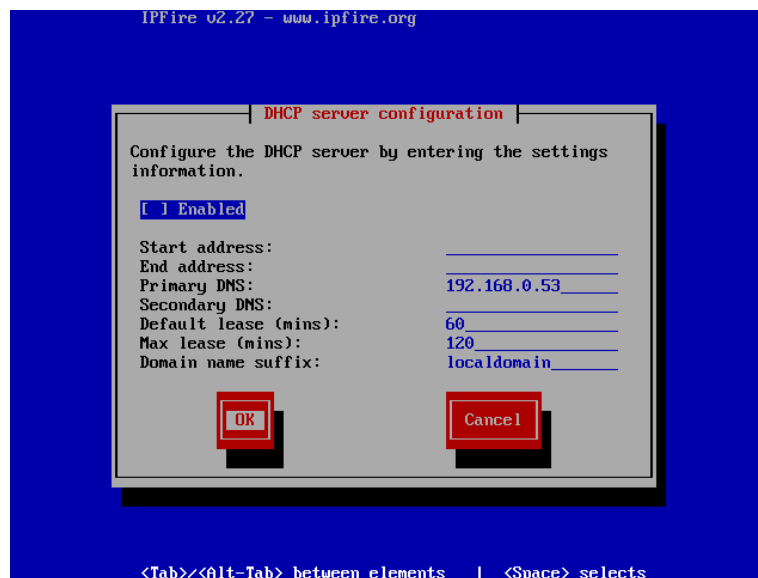


Figura 6 – Interface Green não fazer DHCP

Depois de aplicadas as configurações nas interfaces, a máquina é reiniciada e depois se tudo for bem configurado atribui um IP via DHCP á interface Red como é possível ver na figura 7.

```
Interface "green0" added with 1000 Mbit bandwidth limit.
-> 2 new interfaces found.
Limits can be modified using the configuration file. See "man vnstat.conf".
Unwanted interfaces can be removed from monitoring with "vnstat --remov[ OK ]
Starting kernel log daemon... [ OK ]
Starting system log daemon... [ OK ]
Saving Bootlog... [ OK ]
Starting Unbound DNS Proxy... [ OK ]
Starting ACPI daemon... [ OK ]
Enabling S.M.A.R.T.: sda [ OK ]
Bringing up the green0 interface...
Adding IPv4 address 192.168.0.53 to the green0 interface... [ OK ]
Bringing up the red0 interface...
Starting dhcpcd on the red0 interface... [ OK ]
DHCP Assigned Settings for red0:
IP Address: 192.168.137.246
Hostname: ipfire
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.137.1
DNS Server: 192.168.137.1
Error: ipv4: FIB table does not exist.
Flush terminated
RTNETLINK answers: No such file or directory
Adding static routes... [ OK ]
Adding static routes... [ OK ]
Mounting network file systems... [ OK ]
Starting the Cyrus SASL Server... [ OK ]
Setting time on boot... [ OK ]
Starting ntpd... [ OK ]
```

Figura 7 – Atribuição de IP para interface Red

Foi feito um ping á internet a partir da máquina IPfire assim testando a conectividade com a cloud através da interface Red.

```
[root@ipfire ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=23.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=24.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=21.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=23.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=22.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=58 time=22.5 ms
^C
--- 8.8.8.8 ping statistics ---
```

Figura 8 – Ping da interface Red do IPfire para o google

Neste passo do projeto já tinha a máquina Windows do departamento de informática a funcionar assim usado a mesma para configurar o IPfire, mais abaixo são mostradas todas as configurações que foram aplicadas nesta mesma máquina.

Na figura 9 é possível ver que existe acesso ao IPfire via máquina cliente, para aceder ao IPfire apenas foi necessário inserir o seguinte IP do servidor 192.168.0.53:444.

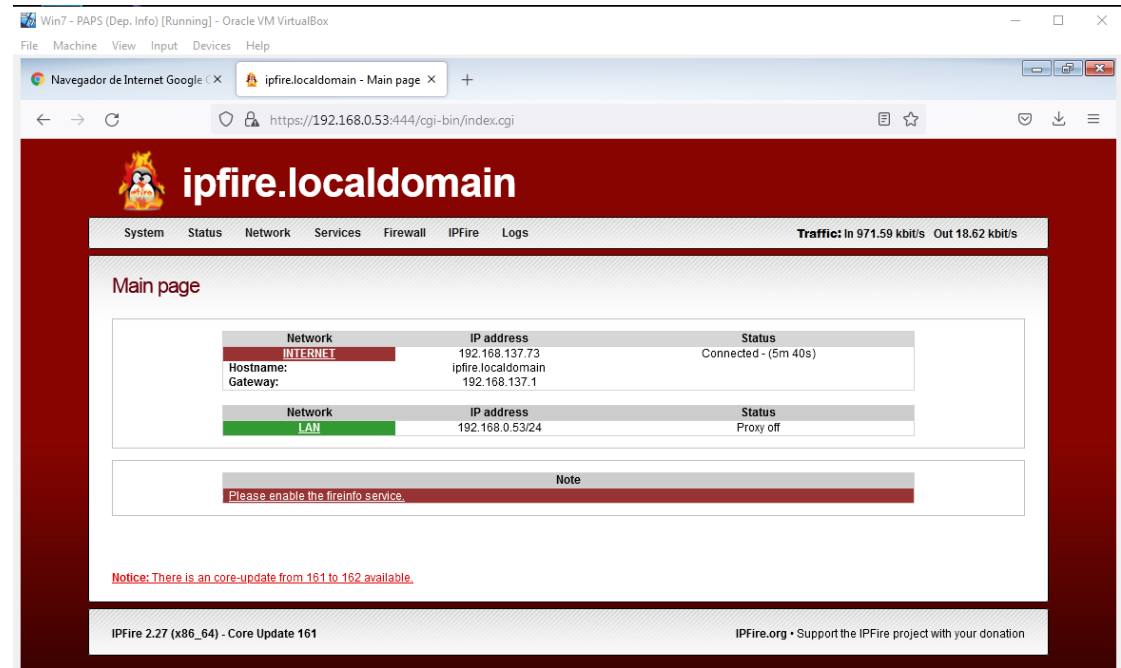


Figura 9 – Acesso á interface do IPfire

Na figura 12 é possível ver que era possível aceder aos sites antes de estes serem colocados dentro da lista negra de sites do IPfire.

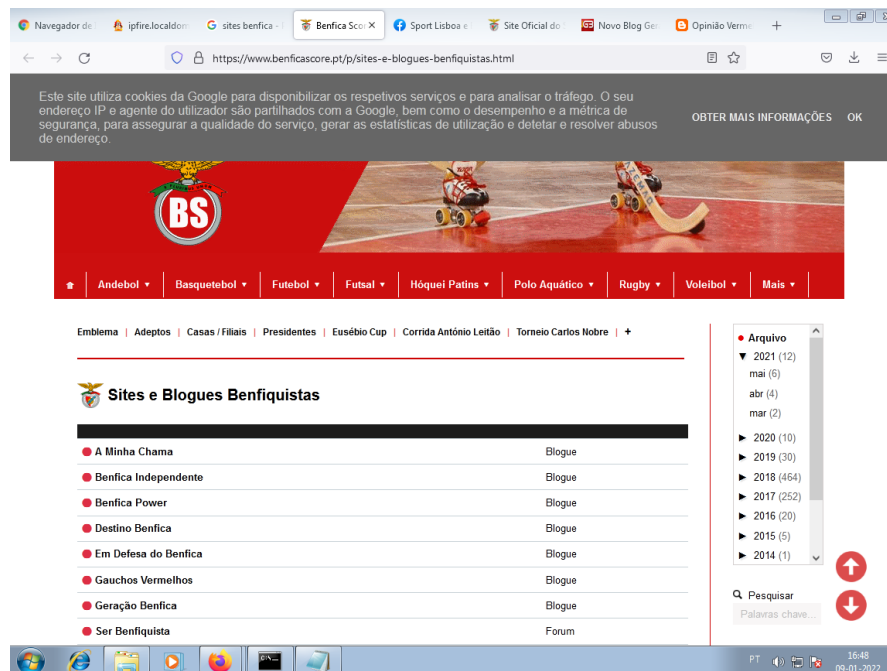


Figura 12 – Antes de ser aplicada o filtro de URL

Para serem aplicadas as configurações de bloqueio de URL acima mostradas, foi necessário aplicar as opções abaixo assinaladas.

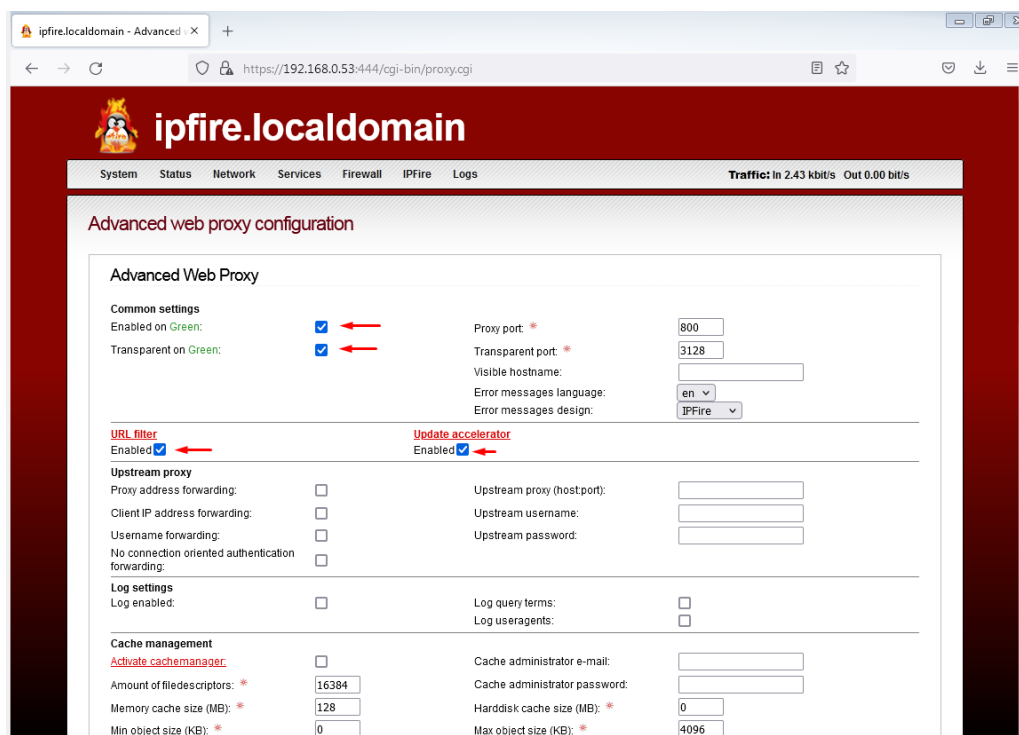


Figura 13 – Configuração Web do URL Filter

Estas 2 opções não foram aplicadas no projeto porém é interessante saber que é possível limitar a largura de banda usada.

ipfire.localdomain - Advanced x Novo separador x +

← → ↻ https://192.168.0.53:444/cgi-bin/proxy.cgi

Unrestricted IP addresses (one per line):
Unrestricted MAC addresses (one per line):

Banned IP addresses (one per line):
Banned MAC addresses (one per line):

Classroom extensions Enabled: ☐

Web Proxy Auto-Discovery Protocol (WPAD) / Proxy Auto-Config (PAC)
Excluded IP Subnets (one per line):
Excluded URL's (one per line):

e.g. 192.168.2.0/255.255.255.0 e.g. *.ipfire.org*

Open PAC File: <http://192.168.0.53:81/wpad.dat>

Notice: For WPAD/PAC to work properly, further changes need to be made. Please see the [Wiki](#).

Time restrictions
Access Mon Tue Wed Thu Fri Sat Sun From To
allow [x] [x] [x] [x] [x] [x] [x] 00 00 24 00

Transfer limits
Max download size (KB): * 0 Max upload size (KB): *

Figura 14 – Configurar a largura de banda

Depois de todos os passos aplicados acima, está na altura de testar o funcionamento dos bloqueios, para tal foi necessário ir nas definições do browser que estava a usar na minha máquina cliente Windows e adicionar o endereço de proxy da máquina IPfire, depois de aplicado, foi a altura de testar o funcionamento do mesmo.

ipfire.localdomain - URL filter x sl benfica - Pesquisa Google x Definições x Problema ao carregar página x +

← → ↻ Firefox about:preferences

Definições de ligação

Configurar acesso proxy à Internet

☐ Sem proxy
☐ Detetar automaticamente as definições de proxy para esta rede
☐ Utilizar definições de proxy do sistema
☒ Configuração manual de proxy

Proxy HTTP 192.168.0.53 Porta 800
☒ Utilizar também este proxy para HTTPS

Proxy HTTPS 192.168.0.53 Porta 800

Servidor SOCKS Porta 0
☐ SOCKS v4 ☒ SOCKS v5

☐ URL de configuração automática de proxy
Recarregar

Nenhum proxy para

Exemplo: mozilla.org, net.nz, 192.168.1.0/24
A ligações a localhost, 127.0.0.1/8, e ::1 não passam pelo proxy.

OK Cancelar Ajuda

Figura 15 – Configuração do proxy na máquina Windows

Como é possível ver os websites que anteriormente funcionavam agora estão bloqueados, já não conseguem ser acedidos, assim é possível verificar que as restrições estão a ser devidamente aplicadas.

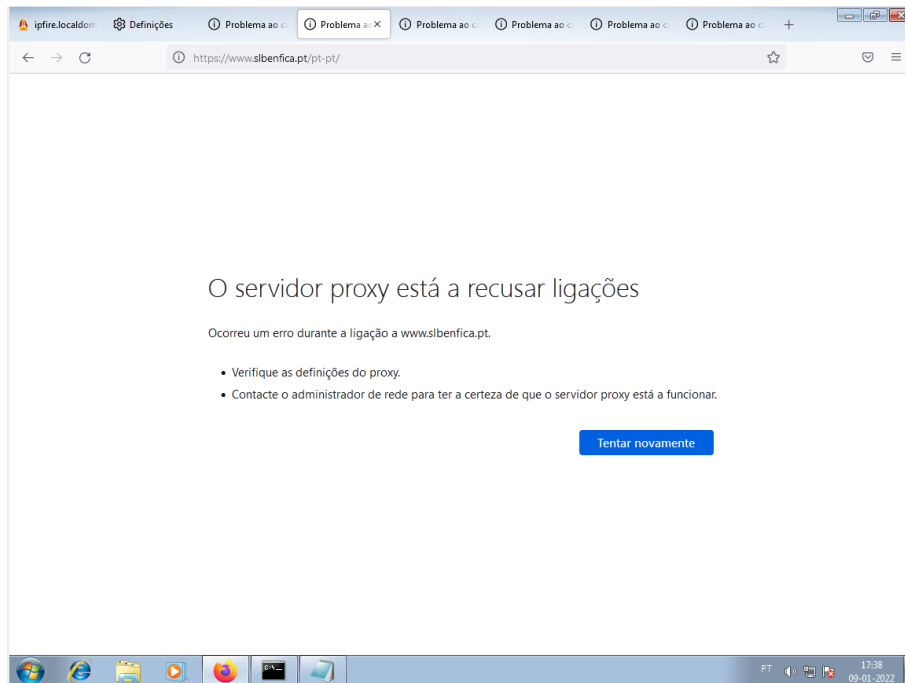


Figura 16 – Confirmação do bloqueio de URLs

5. Configuração do Router

Como é possível ver na figura foi configurada uma password no modo EXEC, o banner message-of-the-day, login message e as ligações vty.

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret cisco
R1(config)#banner motd #Projeto!!!!#
R1(config)#banner login #Bem-vindo!!!#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
```

Figura 17 – Configuração básica do router

Na figura 18 é atribuído o IP 192.168.0.54 255.255.255.252 á interface f0/0, interface essa que está diretamente ligada com a interface green do IPfire, ambas pertencem á mesma sub-rede. Depois foram aplicados os devidos comandos para possibilitar o funcionamento das Vlans dentro do router.

```
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#no ip address dhcp
R1(config-if)#ip address 192.168.0.54 255.255.255.252
R1(config-if)#ex
R1(config)#exi
R1#show ip route
R1(config-if)#
*Mar 1 00:10:27.555: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP address 192.168.137.65,
55.0, hostname R1
R1(config)#int f0/1
R1(config-if)#no shutdown
R1(config-if)#exi
*Mar 1 00:13:48.759: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 00:13:49.759: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1(config)#int f0/1.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#ip address 192.168.0.1 255.255.255.240
R1(config-subif)#exit
R1(config)#int f0/1.3
R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#ip address 192.168.0.17 255.255.255.248
R1(config-subif)#exit
R1(config)#int f0/1.4
R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#encapsulation dot1q 4
R1(config-subif)#ip address 192.168.0.25 255.255.255.248
R1(config-subif)#exit
R1(config)#int f0/1.5
R1(config-subif)#encapsulation dot1q 5
R1(config-subif)#ip address 192.168.0.33 255.255.255.248
R1(config-subif)#exit
R1(config)#int f0/1.6
R1(config-subif)#encapsulation dot1q 6
R1(config-subif)#ip address 192.168.0.41 255.255.255.248
R1(config-subif)#exit
R1(config)#int f0/1.7
R1(config-subif)#encapsulation dot1q 7
R1(config-subif)#ip address 192.168.0.49 255.255.255.252
R1(config-subif)#exit
R1(config)#exit
```

Figura 18 – Configuração de Vlans no router

Na figura 19 podemos ver as Vlans já configuradas em cada uma das subinterfaces do router.

```
R1#show ip interface br
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          192.168.0.54    YES manual up          up
FastEthernet0/1          unassigned      YES unset up          up
FastEthernet0/1.2        192.168.0.1     YES manual up          up
FastEthernet0/1.3        192.168.0.17    YES manual up          up
FastEthernet0/1.4        192.168.0.25    YES manual up          up
FastEthernet0/1.5        192.168.0.33    YES manual up          up
FastEthernet0/1.6        192.168.0.41    YES manual up          up
FastEthernet0/1.7        192.168.0.49    YES manual up          up
R1#
```

Figura 19 – Todas as subinterfaces do Router

Depois de concluída a etapa das Vlans apliquei o ip route para depois o router saber redirecionar a informação que vai da rede interna para si e depois para o IPfire e posteriormente para internet e vice-versa.

```
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.53
R1(config)#exit
```

Figura 20 – Encaminhamento do router para o IPfire

6. Configuração do Switch

Foram criadas Vlans para cada segmento de rede dentro do switch assim possibilitando a separação virtual de cada departamento da empresa, como é possível visualizar foram criadas 6 Vlans, cada interface do switch tem atribuída a si a sua respetiva Vlan, como explicado no início do relatório não foram atribuídas as 15 máquinas no projeto por questões de organização e interpretação, porém apenas era necessário adicionar mais interfaces ao switch para conseguir ter as 15 máquinas mais as duas máquinas do datacenter e depois colocar cada máquina numa interface do switch e configurar as mesmas com as suas respetivas Vlans. O comando "Apply" que se encontra escrito depois da criação das Vlans é bastante importante e por vezes este pode ser esquecido podendo causar confusão e a não perceção de onde está o problema, este deve ser sempre aplicado depois da criação de todas as Vlans para assim estas ficaram corretamente criadas. Depois de atribuídas as Vlans a cada interface é necessário ir a uma interface neste caso á interface f1/15 e fazer switchport mode trunk pois é necessário que a interface que comunique com o router esteja configurada para passar a comunicação de cada Vlan.

```
ESW1#vlan database
ESW1(vlan)#vlan 2 name redacao
VLAN 2 added:
    Name: redacao
ESW1(vlan)#vlan 3 name datacenter
VLAN 3 added:
    Name: datacenter
ESW1(vlan)#vlan 4 name des/pag
VLAN 4 added:
    Name: des/pag
ESW1(vlan)#vlan 5 name dep.info
VLAN 5 added:
    Name: dep.info
ESW1(vlan)#vlan 6 name admin
VLAN 6 added:
    Name: admin
ESW1(vlan)#vlan 7 name direcao
VLAN 7 added:
    Name: direcao
ESW1(vlan)#apply
APPLY completed.
ESW1(vlan)#ex
APPLY completed.
Exiting....
ESW1#conf
Configuring from terminal, memory, or network
Enter configuration commands, one per line
ESW1(config)#int f1/1
ESW1(config-if)#description redacao
ESW1(config-if)#duplex full
ESW1(config-if)#switchport access vlan 2
ESW1(config-if)#ex
ESW1(config)#int f1/2
ESW1(config-if)#description datacenter
ESW1(config-if)#duplex full
ESW1(config-if)#switchport access vlan 3
ESW1(config-if)#ex
ESW1(config)#int f1/3
ESW1(config-if)#description datacenter
ESW1(config-if)#duplex full
ESW1(config-if)#switchport access vlan 3
ESW1(config-if)#ex
ESW1(config)#int f1/4
ESW1(config-if)#description des/pag
ESW1(config-if)#switchport access vlan 4
ESW1(config-if)#duplex full
ESW1(config-if)#ex
ESW1(config)#int f1/5
ESW1(config-if)#description dep.info
ESW1(config-if)#duplex full
ESW1(config-if)#switchport access vlan 5
ESW1(config-if)#ex
ESW1(config)#int f1/6
ESW1(config-if)#description admin
ESW1(config-if)#duplex full
ESW1(config-if)#switchport access vlan 6
ESW1(config-if)#ex
ESW1(config)#int f1/7
ESW1(config-if)#description direcao
ESW1(config-if)#duplex full
ESW1(config-if)#switchport access vlan 7
ESW1(config-if)#ex
ESW1(config)#int f1/15
ESW1(config-if)#switchport mode trunk
ESW1(config-if)#
```

Figura 21 – Criação de Vlans no switch

Na figura 22 é possível ver as interfaces que foram aplicadas a cada Vlan, para visualizar as Vlans é necessário aplicar o comando `show Vlan-switch`, no meu caso a Vlan datacenter que tem 2 interfaces configuradas, uma para o servidor TFTP e a outra para o Zabbix e todas as outras Vlans apenas tem atribuída uma interface pois apenas tem uma máquina conectada. A escolha dos números para cada Vlan é meramente escolha pessoal, não foi baseada em nenhum requisito do projeto.

VLAN	Name	Status	Ports
1	default	active	Fa1/0, Fa1/8, Fa1/9, Fa1/10 Fa1/11, Fa1/12, Fa1/13, Fa1/14
2	redacao	active	Fa1/1
3	datacenter	active	Fa1/2, Fa1/3
4	des/pag	active	Fa1/4
5	dep.info	active	Fa1/5
6	admin	active	Fa1/6
7	direacao	active	Fa1/7
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Figura 22 – Interfaces configuradas para cada Vlan

Depois de aplicados todos os comandos necessários no switch as suas configurações são guardadas na startup-config, depois de guardadas exportei uma cópia das configurações para dentro de uma pasta dentro da pasta do projeto, caso houvesse algum problema teria um ficheiro de backup que poderia depois ser aplicado noutra switch, para simular um ambiente real exportei este mesmo ficheiro para dentro da máquina cliente Windows, visto que este não podia ser exportado para dentro da máquina TFTP.

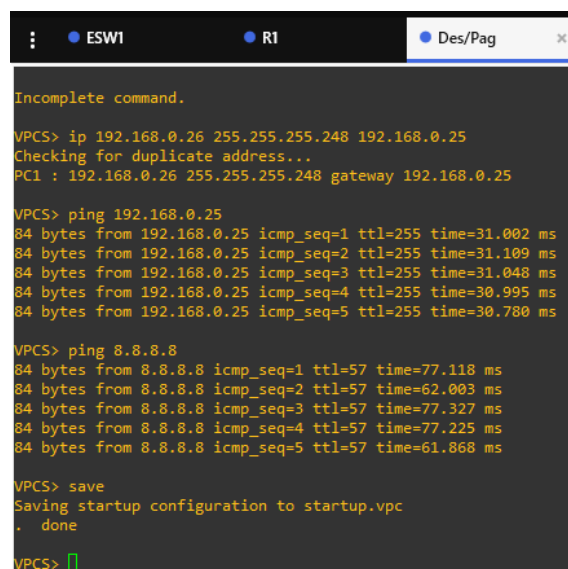
```
ESW1#copy ru
ESW1#copy running-config star
ESW1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ESW1#
```

Figura 23 – Guardar as configurações do Switch

7. Configuração dos Hosts

7.1 VPCs

Em cada VPC foi configurado o seu endereço a sua respetiva máscara e a gateway da Vlan do seu departamento, em cada uma das figuras é possível ver que todos os VPCs conseguem fazer ping á interface de gateway e à internet sendo possível dizer que as Vlans estão a funcionar corretamente. Na figura 24 o VPC do departamento de design gráfico/paginação, na figura 25 o VPC representante do departamento de administração comercial, a figura 26 mostra o da direção e por fim a figura 27 é o VPC redação.



```
Incomplete command.

VPCS> ip 192.168.0.26 255.255.255.248 192.168.0.25
Checking for duplicate address...
PC1 : 192.168.0.26 255.255.255.248 gateway 192.168.0.25

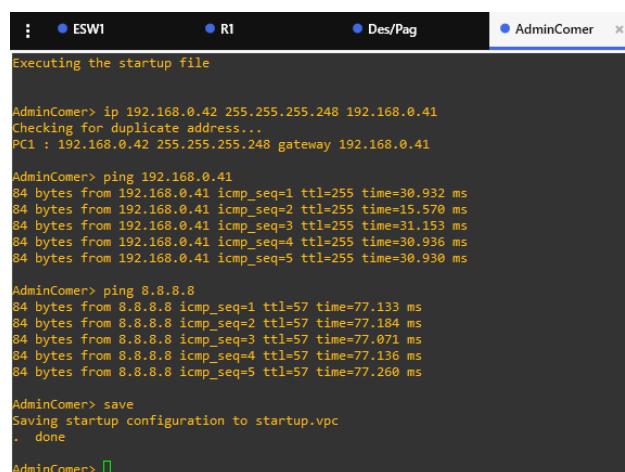
VPCS> ping 192.168.0.25
84 bytes from 192.168.0.25 icmp_seq=1 ttl=255 time=31.002 ms
84 bytes from 192.168.0.25 icmp_seq=2 ttl=255 time=31.109 ms
84 bytes from 192.168.0.25 icmp_seq=3 ttl=255 time=31.048 ms
84 bytes from 192.168.0.25 icmp_seq=4 ttl=255 time=30.995 ms
84 bytes from 192.168.0.25 icmp_seq=5 ttl=255 time=30.780 ms

VPCS> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=57 time=77.118 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=57 time=62.003 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=57 time=77.327 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=57 time=77.225 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=57 time=61.868 ms

VPCS> save
Saving startup configuration to startup.vpc
. done

VPCS> 
```

Figura 24 – Pings VPC design/paginação



```
Executing the startup file

AdminComer> ip 192.168.0.42 255.255.255.248 192.168.0.41
Checking for duplicate address...
PC1 : 192.168.0.42 255.255.255.248 gateway 192.168.0.41

AdminComer> ping 192.168.0.41
84 bytes from 192.168.0.41 icmp_seq=1 ttl=255 time=30.932 ms
84 bytes from 192.168.0.41 icmp_seq=2 ttl=255 time=15.570 ms
84 bytes from 192.168.0.41 icmp_seq=3 ttl=255 time=31.153 ms
84 bytes from 192.168.0.41 icmp_seq=4 ttl=255 time=30.936 ms
84 bytes from 192.168.0.41 icmp_seq=5 ttl=255 time=30.930 ms

AdminComer> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=57 time=77.133 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=57 time=77.184 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=57 time=77.071 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=57 time=77.136 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=57 time=77.260 ms

AdminComer> save
Saving startup configuration to startup.vpc
. done

AdminComer> 
```

Figura 25 – Pings VPC Administração Comercial

```
ESWI R1 Des/Pag AdminComer Direção
Executing the startup file

Direção> ip 192.168.0.50 255.255.255.252 192.168.0.49
Checking for duplicate address...
PC1 : 192.168.0.50 255.255.255.252 gateway 192.168.0.49

Direção> ping 192.168.0.49
64 bytes from 192.168.0.49 icmp_seq=1 ttl=255 time=31.238 ms
64 bytes from 192.168.0.49 icmp_seq=2 ttl=255 time=31.007 ms
64 bytes from 192.168.0.49 icmp_seq=3 ttl=255 time=31.307 ms
64 bytes from 192.168.0.49 icmp_seq=4 ttl=255 time=30.890 ms
64 bytes from 192.168.0.49 icmp_seq=5 ttl=255 time=30.945 ms

Direção> ping 8.8.8.8
8.8.8.8 icmp_seq=1 timeout
64 bytes from 8.8.8.8 icmp_seq=2 ttl=57 time=77.463 ms
64 bytes from 8.8.8.8 icmp_seq=3 ttl=57 time=61.528 ms
64 bytes from 8.8.8.8 icmp_seq=4 ttl=57 time=77.388 ms
64 bytes from 8.8.8.8 icmp_seq=5 ttl=57 time=77.261 ms

Direção> save
Saving startup configuration to startup.vpc
. done
Direção> 
```

Figura 26 – Pings VPC Direção

```
R1 Redação Des/Pag AdminComer Direção
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mnrnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.
Executing the startup file

Checking for duplicate address...
PC1 : 192.168.0.2 255.255.255.240 gateway 192.168.0.1
Redação> ping 8.8.8.8
64 bytes from 8.8.8.8 icmp_seq=1 ttl=56 time=77.456 ms
64 bytes from 8.8.8.8 icmp_seq=2 ttl=56 time=61.680 ms
64 bytes from 8.8.8.8 icmp_seq=3 ttl=56 time=62.176 ms
64 bytes from 8.8.8.8 icmp_seq=4 ttl=56 time=62.031 ms
64 bytes from 8.8.8.8 icmp_seq=5 ttl=56 time=77.273 ms

Redação> 
```

Figura 27 – Pings VPC Redação

Ao contrário do Packet Tracer onde não é necessário guardar cada configuração feita nos PCs, no caso dos VPCs do GNS3 é necessário aplicar o comando Save para guardar os endereços, máscara e gateway que foi aplicada em cada VPC, caso o comando não seja aplicado assim que o VPC for desligado e voltar a ser ligado este não consegue pingar outros dispositivos porque não tem um endereço configurado.

```
VPCS> save
Saving startup configuration to startup.vpc
. done
VPCS> 
```

Figura 28 – Guardar configurações dos VPCs

7.2 Servidor TFTP

A instalação dos seguintes serviços foi feita antes da máquina TFTP ser inserida dentro do projeto de GNS3, para instalar os serviços abaixo foi necessário inserir uma interface NAT e foi instalado o nano como editor de texto.

Foi efetuado o apt update antes de serem instalados os serviços de TFTP como é demonstrado na figura 29.

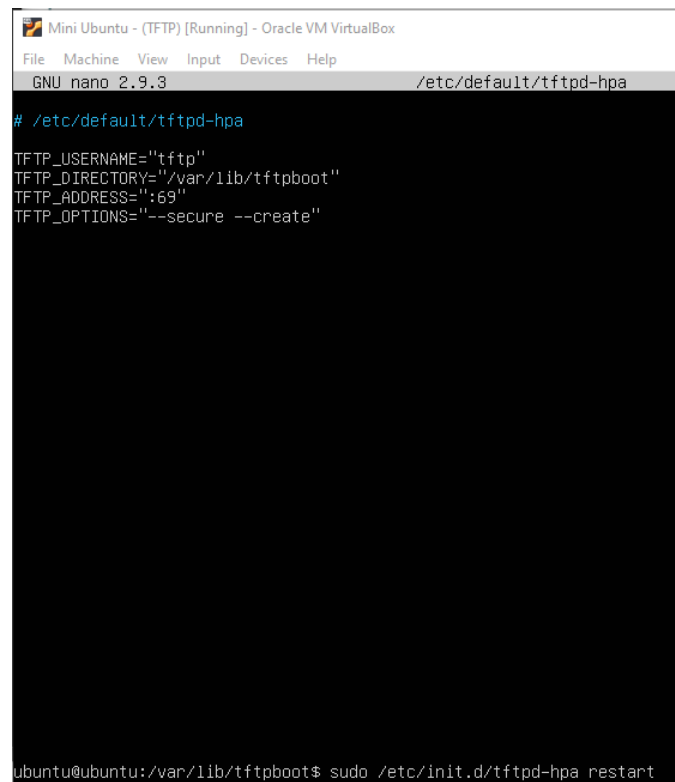
```
ubuntu@ubuntu:~$ sudo apt install tftp-hpa tftpd-hpa
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libwrap0
Suggested packages:
  pxelinux
The following NEW packages will be installed
  libwrap0 tftp-hpa tftpd-hpa
0 to upgrade, 3 to newly install, 0 to remove and 0 not to upgrade.
Need to get 104 kB of archives.
After this operation, 279 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

Figura 29 – Instalação do TFTP

Na figura 30 é possível visualizar que depois de instalados os serviços de tftp e tftpd são aplicados os comandos para criar a diretoria onde vai ficar guardado os backups.

```
Mini Ubuntu - (TFTP) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Get:3 http://pt.archive.ubuntu.com/ubuntu bionic/main amd64 tftpd-hpa amd64 5.2+20150808-1
9.1 kB]
Fetched 104 kB in 10s (10.1 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libwrap0:amd64.
(Reading database ... 56239 files and directories currently installed.)
Preparing to unpack .../libwrap0_7.6.q-27_amd64.deb ...
Unpacking libwrap0:amd64 (7.6.q-27) ...
Selecting previously unselected package tftp-hpa.
Preparing to unpack .../tftp-hpa_5.2+20150808-1ubuntu3_amd64.deb ...
Unpacking tftp-hpa (5.2+20150808-1ubuntu3) ...
Selecting previously unselected package tftpd-hpa.
Preparing to unpack .../tftpd-hpa_5.2+20150808-1ubuntu3_amd64.deb ...
Unpacking tftpd-hpa (5.2+20150808-1ubuntu3) ...
Setting up libwrap0:amd64 (7.6.q-27) ...
Setting up tftp-hpa (5.2+20150808-1ubuntu3) ...
Setting up tftpd-hpa (5.2+20150808-1ubuntu3) ...
Processing triggers for systemd (237-3ubuntu10.53) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1.4) ...
ubuntu@ubuntu:~$ cd /var/lib/tftpboot/
ubuntu@ubuntu:/var/lib/tftpboot$ sudo mktemp -d XXXXX --suffix=-outgoing
dEp19-outgoing
ubuntu@ubuntu:/var/lib/tftpboot$ sudo chmod 755 dEp19-outgoing
ubuntu@ubuntu:/var/lib/tftpboot$ ls -la
total 12
drwxr-xr-x  3 root nogroup 4096 Jan  6 17:40 .
drwxr-xr-x 36 root root    4096 Jan  6 17:38 ..
drwxr-xr-x  2 root root    4096 Jan  6 17:40 dEp19-outgoing
ubuntu@ubuntu:/var/lib/tftpboot$ sudo mktemp -d XXXXX --suffix=-incoming dEp19-incoming
mktemp: too many templates
Try 'mktemp --help' for more information.
ubuntu@ubuntu:/var/lib/tftpboot$ sudo mktemp -d XXXXX --suffix=-incoming
xFuEX-incoming
ubuntu@ubuntu:/var/lib/tftpboot$ sudo chown tftp:tftp xFuEX-incoming
ubuntu@ubuntu:/var/lib/tftpboot$ _
```

Figura 30 – Comandos para configurar o TFTP



```
Mini Ubuntu - (TFTP) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.9.3 /etc/default/tftpd-hpa

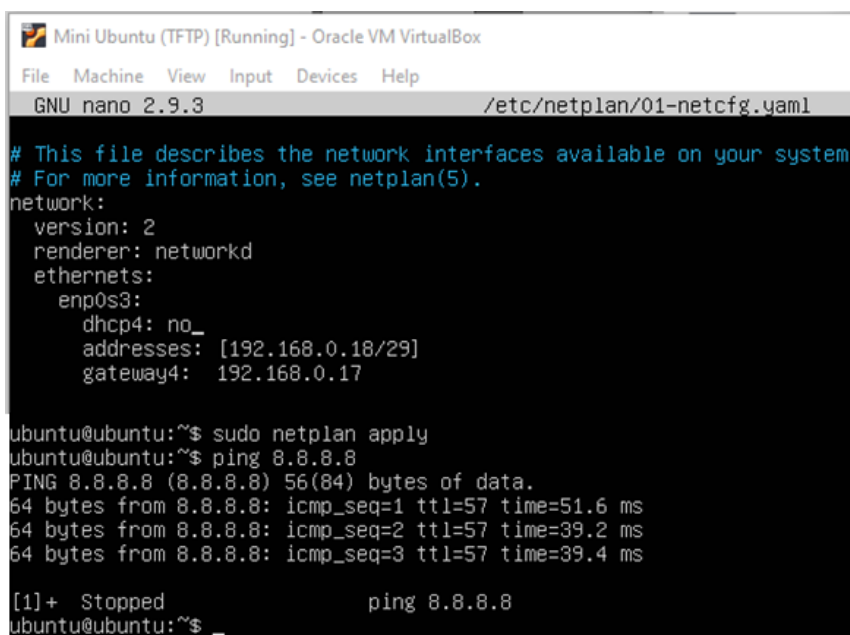
# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/var/lib/tftpboot"
TFTP_ADDRESS="::69"
TFTP_OPTIONS="--secure --create"

ubuntu@ubuntu:/var/lib/tftpboot$ sudo /etc/init.d/tftpd-hpa restart
```

Figura 31 – Configurar o /etc/default/tftpd-hpa

Quando todos os pacotes/serviços já estiveram instalados é altura de importar para dentro do GNS a máquina e depois dar o IP escolhido na tabela de endereços, 192.168.0.18.



```
Mini Ubuntu (TFTP) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.9.3 /etc/netplan/01-netcfg.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no_
      addresses: [192.168.0.18/29]
      gateway4: 192.168.0.17

ubuntu@ubuntu:~$ sudo netplan apply
ubuntu@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=51.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=39.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=39.4 ms

[1]+  Stopped                  ping 8.8.8.8
ubuntu@ubuntu:~$ _
```

Figura 32 – Atribuição de endereço à máquina TFTP e ping ao 8.8.8.8

7.3 Máquina Windows

A máquina Windows já estava dentro do projeto de GNS3, apenas foi necessário adicionar o IP escolhido anteriormente na tabela de endereços e escolher a gateway, que no caso é o endereço da subinterface criada dentro do router.

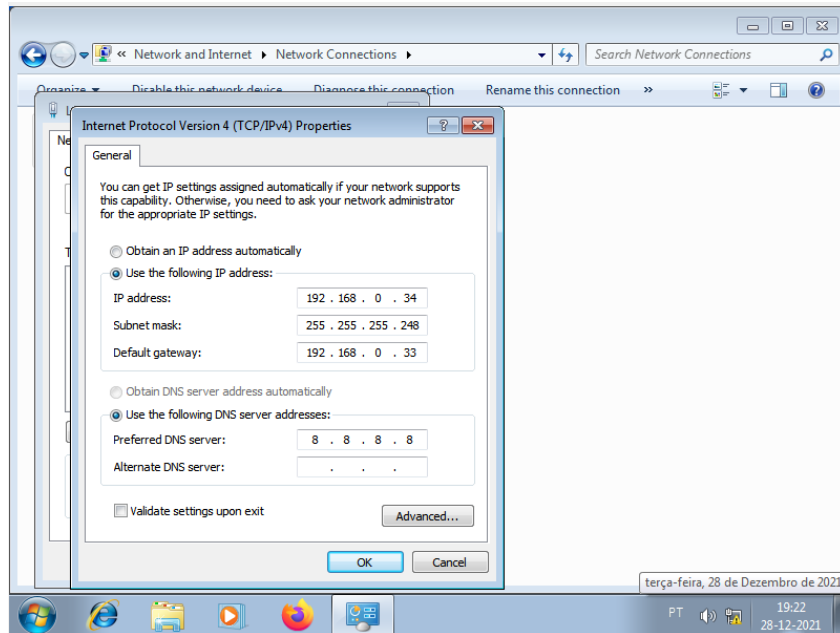


Figura 33 – Configurar a interface da máquina Windows (departamento de informática)

Depois de aplicado o endereço á máquina Windows foi testado o ping á gateway do segmento de rede do servidor TFTP conseguindo obter sucesso.

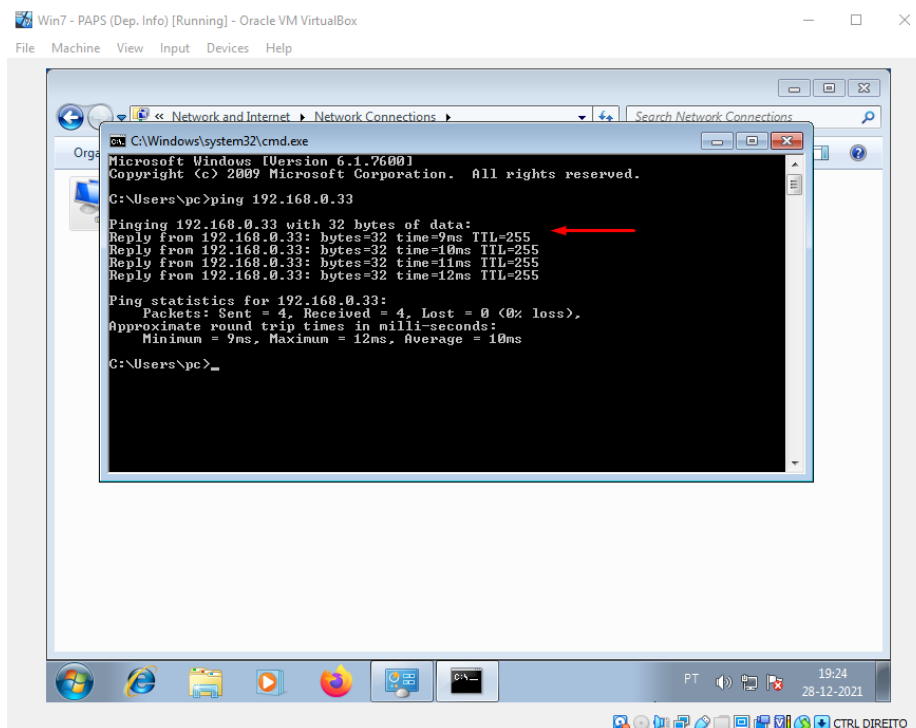


Figura 34 – Pingar a internet com a máquina Windows

8. Monitorização

8.1 Instalação e Configuração do Zabbix

Para instalação do Zabbix foram feitos bastante comandos, por isso mesmo achei melhor mostrar os comandos apenas em texto visto que as figuras iriam ocupar bastante espaço desnecessário.

Os 3 comandos abaixo escritos foram aplicados para instalar pacotes/serviços dentro da máquina:

- `Sudo apt update` – este comando serve para fazer possíveis atualizações em falta á máquina
- `sudo apt-get -y install nano` – instalar o editor de texto nano que facilita a aplicação de comandos
- `sudo apt install mysql-server` – Instalação do serviço mysql dentro da máquina

Os seguintes comandos foram aplicados para instalar e criar as pastas destinadas aos serviços Zabbix:

- `wget https://repo.zabbix.com/zabbix/5.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.4-1+ubuntu18.04_all.deb`
- `sudo dpkg -i zabbix-release_5.4-1+ubuntu18.04_all.deb`
- `apt update`
- `apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent`
- `sudo su`
- `mysql -uroot -p`
- `create database zabbix character set utf8 collate utf8_bin;`
- `create user zabbix@localhost identified by 'password';`
- `grant all privileges on zabbix.* to zabbix@localhost;`
- `quit;`
- `zcat /usr/share/doc/zabbix-sql-scripts/mysql/create.sql.gz | mysql -u zabbix -p zabbix`
- `sudo nano /etc/zabbix/zabbix_server.conf` e modificar o comando `DBPassword` para `DBPassword=password`

Por fim quando aplicados todos os comandos de instalação e configuração dos serviços do Zabbix foi a vez de reiniciar e aplicar todas as alterações á máquina:

- `systemctl restart zabbix-server zabbix-agent apache2`
- `systemctl enable zabbix-server zabbix-agent apache2`

Para testar se os serviços estavam funcionais foi necessário ir à máquina Windows e inserir o endereço do servidor Zabbix, como está disposto na figura 35 o serviço está funcional e pronto configurar. Na figura 36 foi finalizada a configuração do Zabbix.

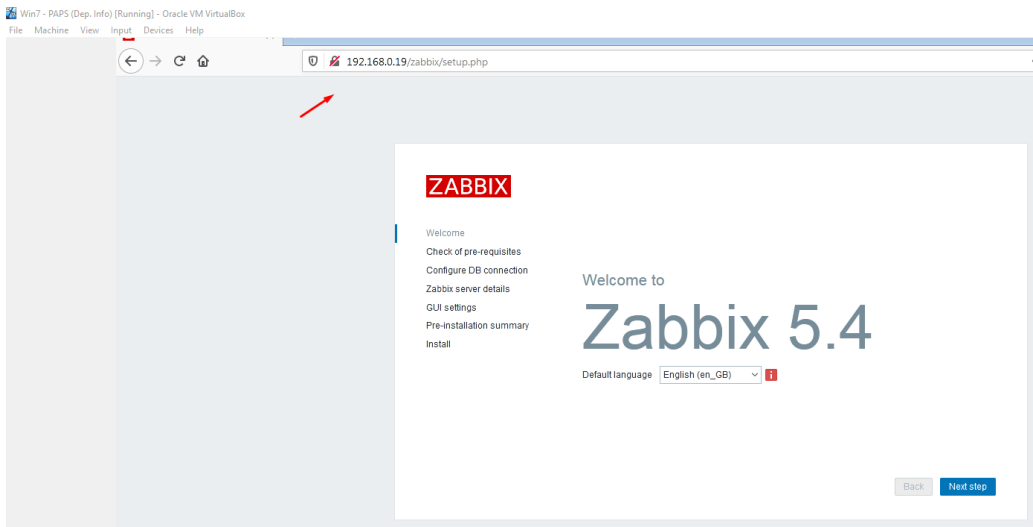


Figura 35 – Acesso á interface gráfica do Zabbix

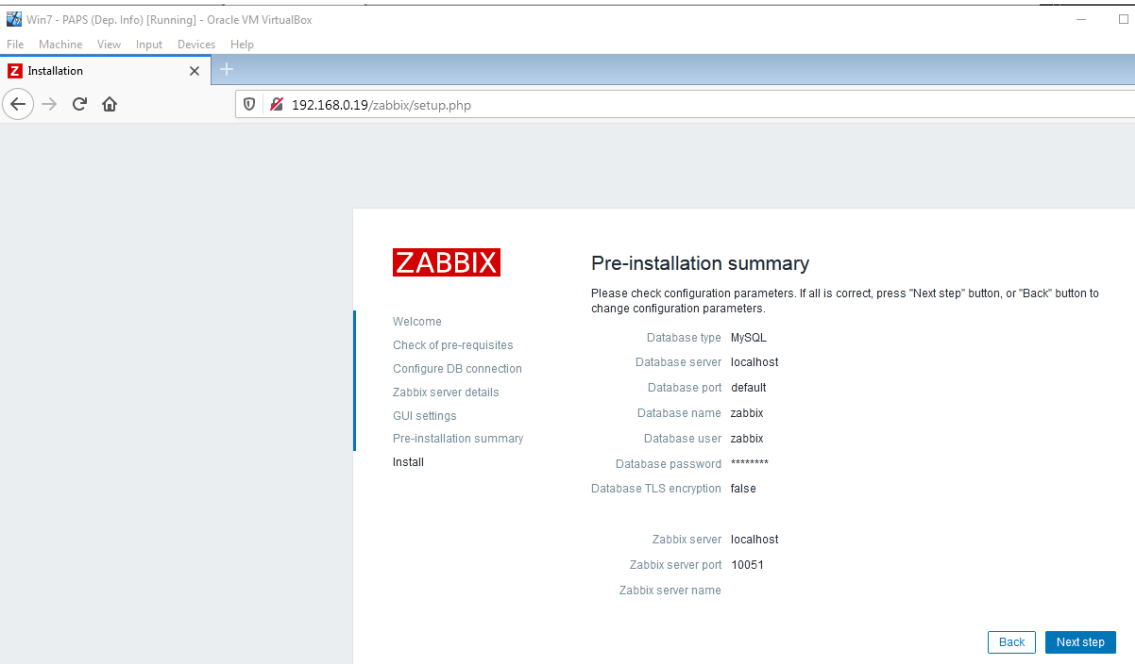
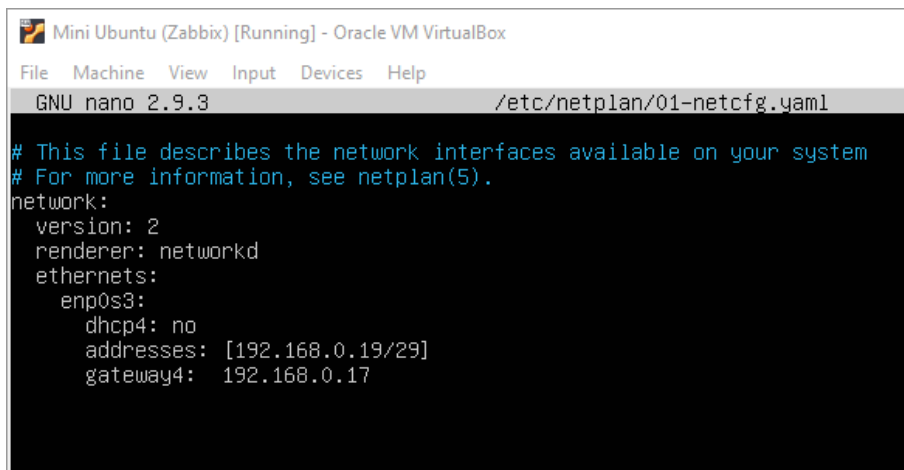


Figura 36 – Finalização da configuração do servidor Zabbix

A interface do Zabbix foi configurada tal como está demonstrado na figura 37, foi configurada na Vlan do datacenter.

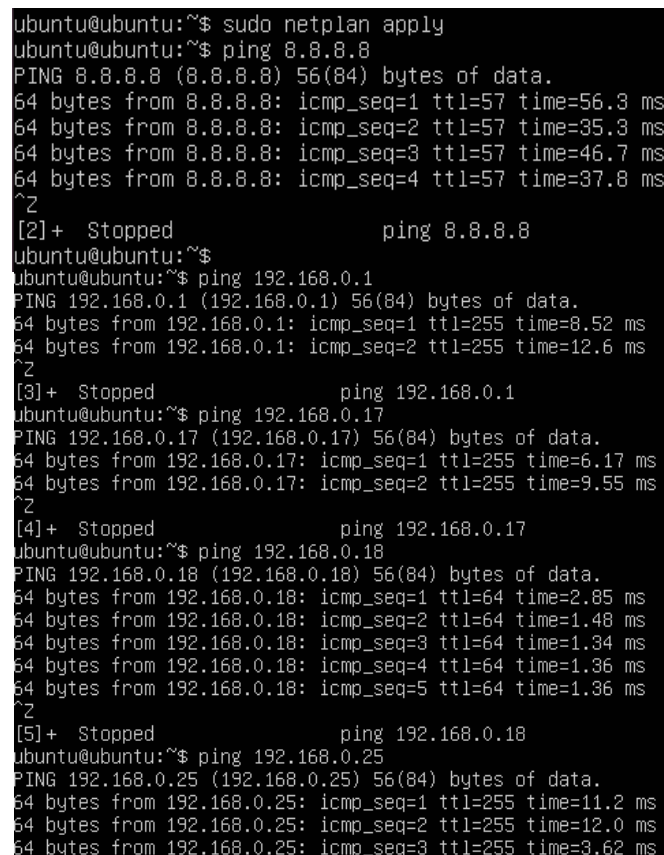


```
Mini Ubuntu (Zabbix) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.9.3 /etc/netplan/01-netcfg.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.0.19/29]
      gateway4: 192.168.0.17
```

Figura 37 – Configuração da interface da máquina Zabbix

Depois de inserido o ip como está feito na figura acima podemos ver que é possível pingar tanto o 8.8.8.8 quanto outros hosts dentro da rede.



```
ubuntu@ubuntu:~$ sudo netplan apply
ubuntu@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=56.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=35.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=46.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=57 time=37.8 ms
^Z
[2]+  Stopped                  ping 8.8.8.8
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=8.52 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=12.6 ms
^Z
[3]+  Stopped                  ping 192.168.0.1
ubuntu@ubuntu:~$ ping 192.168.0.17
PING 192.168.0.17 (192.168.0.17) 56(84) bytes of data.
64 bytes from 192.168.0.17: icmp_seq=1 ttl=255 time=6.17 ms
64 bytes from 192.168.0.17: icmp_seq=2 ttl=255 time=9.55 ms
^Z
[4]+  Stopped                  ping 192.168.0.17
ubuntu@ubuntu:~$ ping 192.168.0.18
PING 192.168.0.18 (192.168.0.18) 56(84) bytes of data.
64 bytes from 192.168.0.18: icmp_seq=1 ttl=64 time=2.85 ms
64 bytes from 192.168.0.18: icmp_seq=2 ttl=64 time=1.48 ms
64 bytes from 192.168.0.18: icmp_seq=3 ttl=64 time=1.34 ms
64 bytes from 192.168.0.18: icmp_seq=4 ttl=64 time=1.36 ms
64 bytes from 192.168.0.18: icmp_seq=5 ttl=64 time=1.36 ms
^Z
[5]+  Stopped                  ping 192.168.0.18
ubuntu@ubuntu:~$ ping 192.168.0.25
PING 192.168.0.25 (192.168.0.25) 56(84) bytes of data.
64 bytes from 192.168.0.25: icmp_seq=1 ttl=255 time=11.2 ms
64 bytes from 192.168.0.25: icmp_seq=2 ttl=255 time=12.0 ms
64 bytes from 192.168.0.25: icmp_seq=3 ttl=255 time=3.62 ms
```

Figura 38 – Ping ao servidor TFTP e ping ao google

8.2 Configurar utilizadores no Zabbix

8.2.1 Máquina Windows

Para a máquina Windows ser monitorizada foi necessário instalar o Zabbix-agent dentro da máquina.

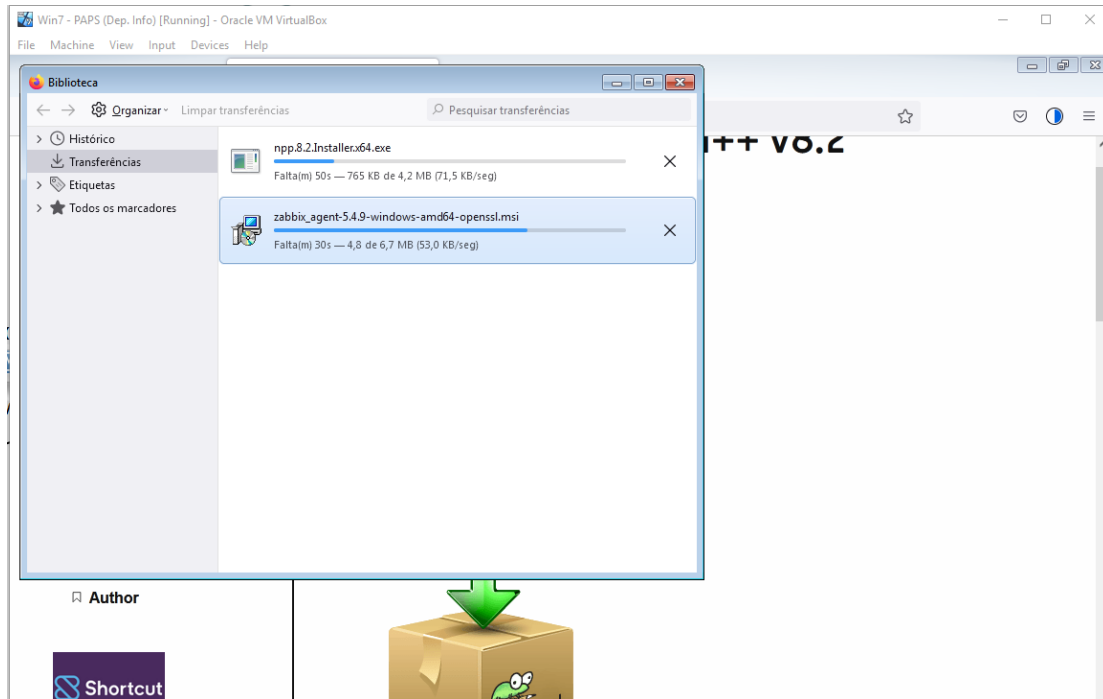


Figura 39 – Instalação do Zabbix agente na máquina Windows

Depois de instalado e configurado foi a vez de dar restart nos serviços do Zabbix agent para começar a funcionar.

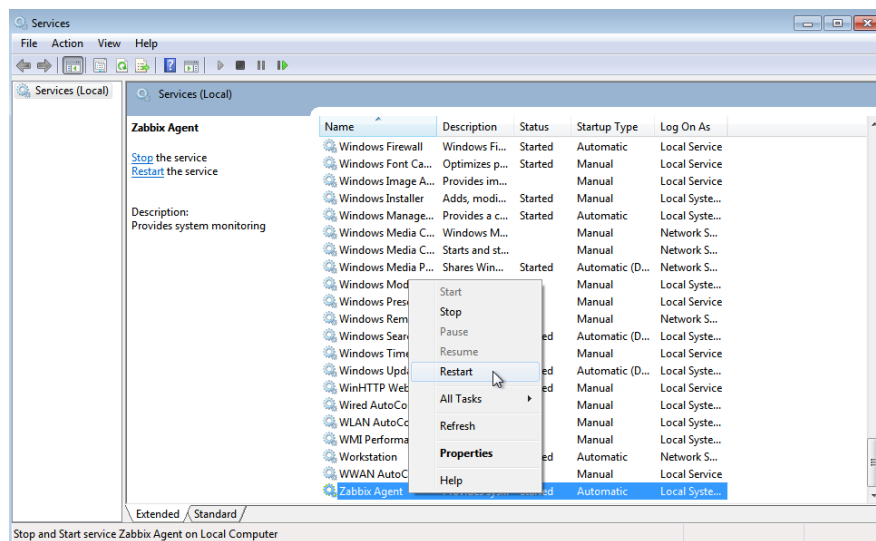


Figura 40 – Restart do Zabbix agent

Depois do Zabbix agent estar a funcionar, este foi inserido dentro dos hosts do Zabbix.

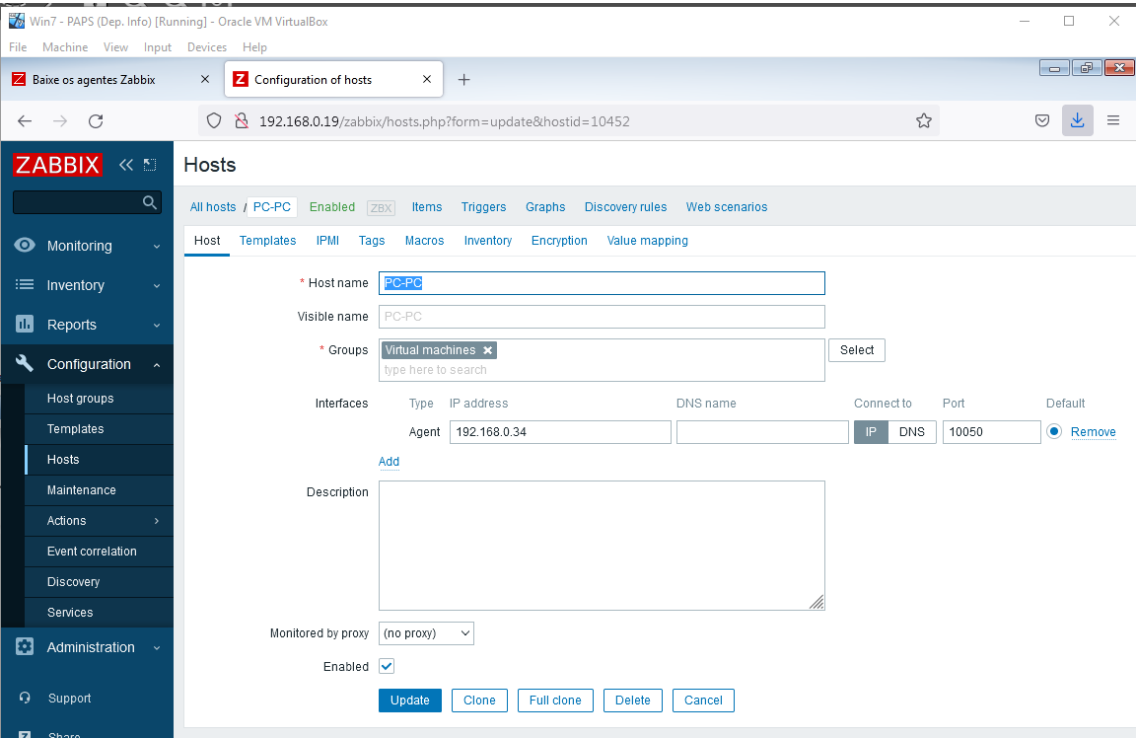


Figura 41 – Inserir a máquina Windows no Zabbix

Na figura 42 é possível visualizar as 2 máquinas já dentro do Zabbix, neste caso a própria máquina Zabbix e a máquina Windows.

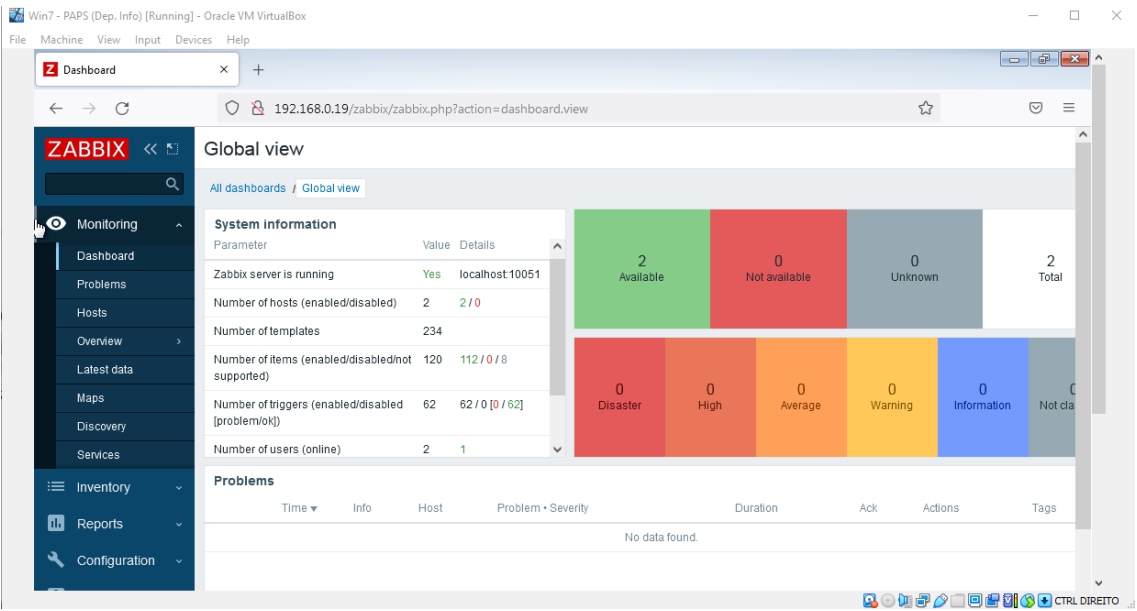


Figura 42 – Verificação da implementação da máquina no Zabbix

8.2.2 Máquina TFTP

Instalação do Zabbix agent na máquina TFTP

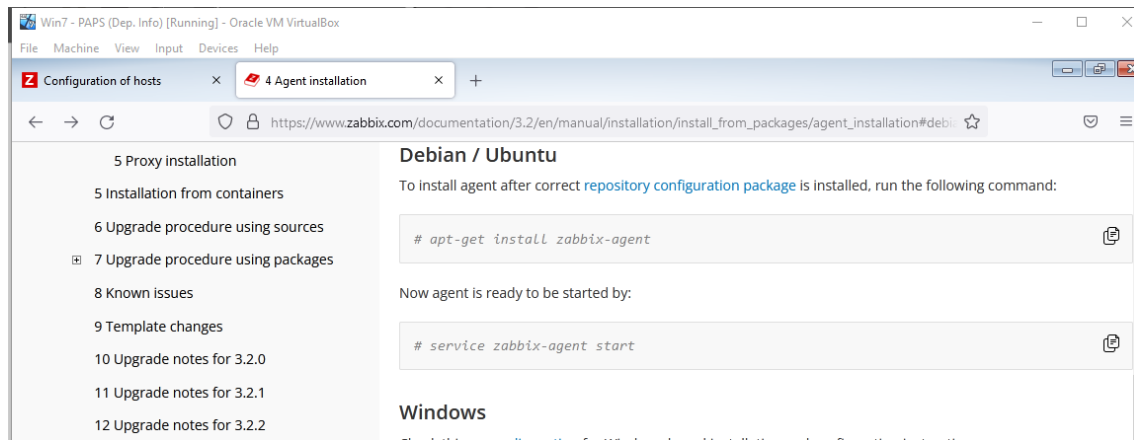


Figura 43 – Instalação do Zabbix agent na máquina TFTP

Dentro do ficheiro que está na figura 44 é necessário inserir o IP da máquina Zabbix para assim a máquina TFTP saber quem é o server e na figura 45 é atribuído hostname à máquina do TFTP dentro dos serviços Zabbix.

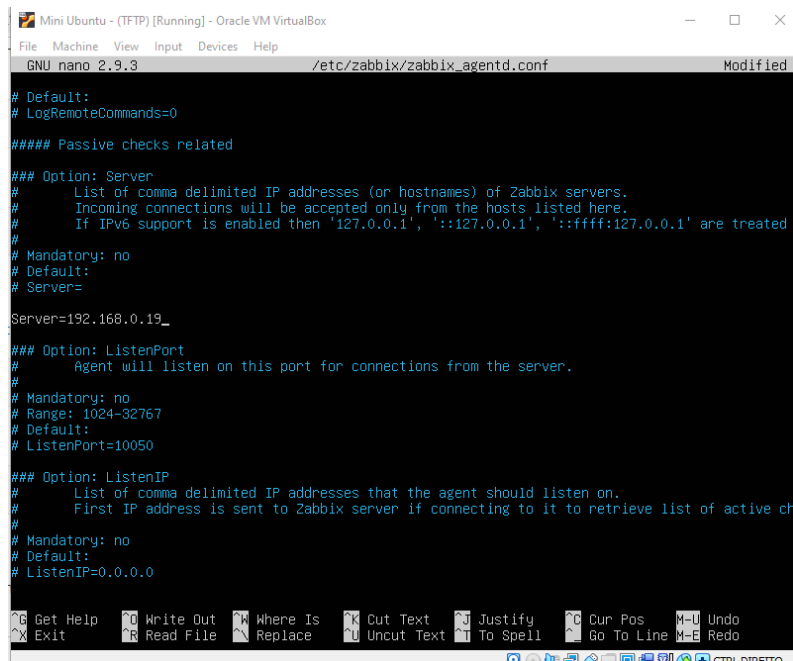
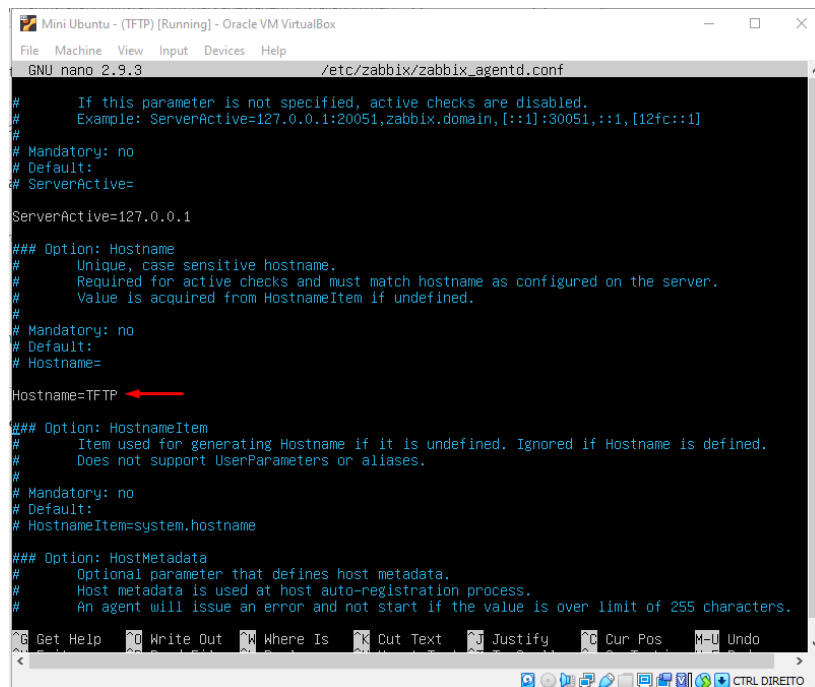


Figura 44 – Configuração do ficheiro Zabbix_agentd.conf - 1



```
GNU nano 2.9.3 /etc/zabbix/zabbix_agentd.conf

# If this parameter is not specified, active checks are disabled.
# Example: ServerActive=127.0.0.1:20051,zabbix.domain,[:11]:30051,::1,[12fc::1]
#
# Mandatory: no
# Default:
# ServerActive=

ServerActive=127.0.0.1

### Option: Hostname
# Unique, case sensitive hostname.
# Required for active checks and must match hostname as configured on the server.
# Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=

Hostname=TFTP

### Option: HostnameItem
# Item used for generating Hostname if it is undefined. Ignored if Hostname is defined.
# Does not support UserParameters or aliases.
#
# Mandatory: no
# Default:
# HostnameItem=system.hostname

### Option: HostMetadata
# Optional parameter that defines host metadata.
# Host metadata is used at host auto-registration process.
# An agent will issue an error and not start if the value is over limit of 255 characters.
```

Figura 45 – Configuração do ficheiro Zabbix_agentd.conf - 2

Depois de configurados todos os parâmetros da instalação da máquina TFTP esta foi inserida dentro dos hosts do Zabbix.

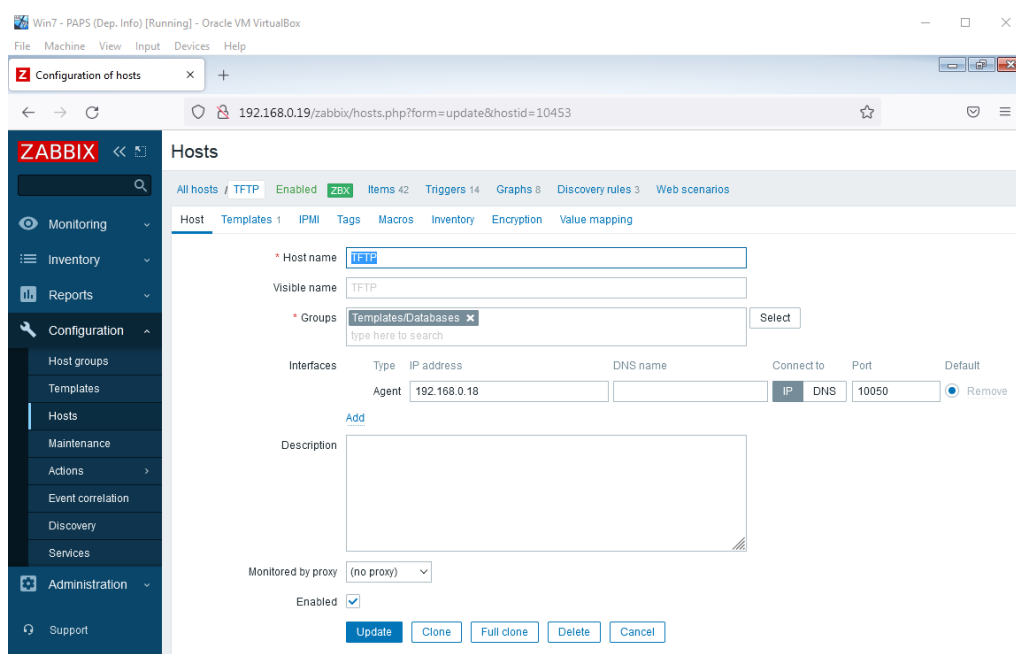


Figura 46 – Inserir o servidor TFTP no Zabbix

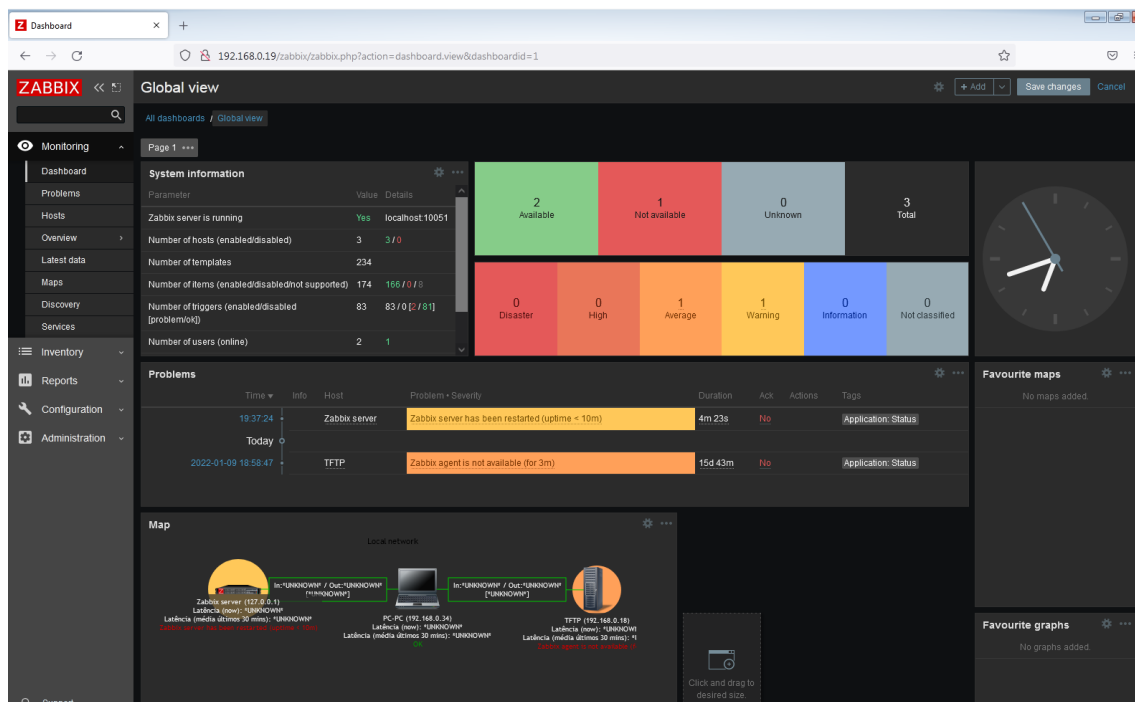
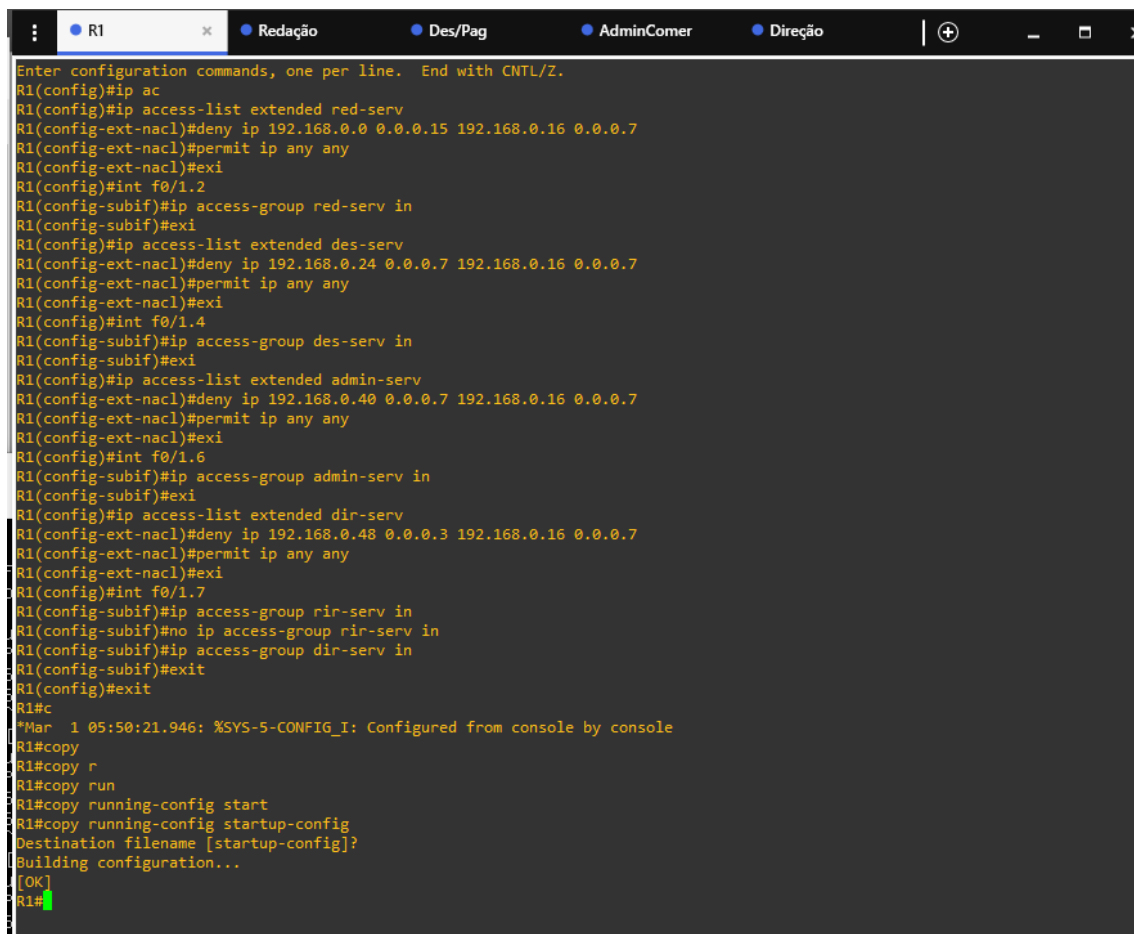


Figura 47 – Mapa Zabbix

9. Aplicação das ACLs

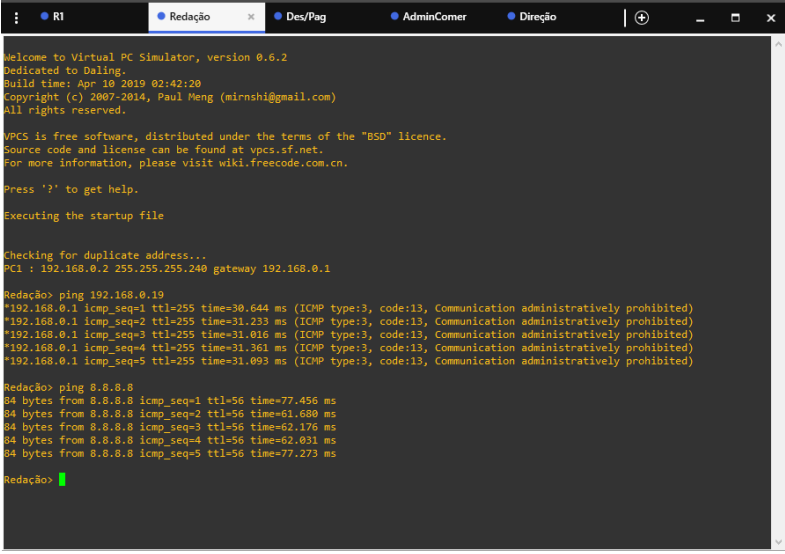
Foram aplicadas ACLs no projeto para bloquear a comunicação dos departamentos da empresa que contém as máquinas críticas, fazendo com que apenas as máquinas Windows do departamento de informática consigam comunicar com as máquinas que se encontram no datacenter. Esta medida de segurança foi aplicada para bloquear a comunicação entre os departamentos que não sejam relacionados com a informática com as máquinas do datacenter, se alguma destas máquinas dos outros departamentos ficar infetada estas como não conseguem infetar os servidores.



```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip ac
R1(config)#ip access-list extended red-serv
R1(config-ext-nacl)#deny ip 192.168.0.0 0.0.0.15 192.168.0.16 0.0.0.7
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#int f0/1.2
R1(config-subif)#ip access-group red-serv in
R1(config-subif)#exit
R1(config)#ip access-list extended des-serv
R1(config-ext-nacl)#deny ip 192.168.0.24 0.0.0.7 192.168.0.16 0.0.0.7
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#int f0/1.4
R1(config-subif)#ip access-group des-serv in
R1(config-subif)#exit
R1(config)#ip access-list extended admin-serv
R1(config-ext-nacl)#deny ip 192.168.0.40 0.0.0.7 192.168.0.16 0.0.0.7
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#int f0/1.6
R1(config-subif)#ip access-group admin-serv in
R1(config-subif)#exit
R1(config)#ip access-list extended dir-serv
R1(config-ext-nacl)#deny ip 192.168.0.48 0.0.0.3 192.168.0.16 0.0.0.7
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#int f0/1.7
R1(config-subif)#ip access-group dir-serv in
R1(config-subif)#no ip access-group dir-serv in
R1(config-subif)#ip access-group dir-serv in
R1(config-subif)#exit
R1(config)#exit
R1#
*Mar 1 05:50:21.946: %SYS-5-CONFIG_I: Configured from console by console
R1#copy
R1#copy r
R1#copy run
R1#copy running-config start
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Figura 48 – Criação das ACLs estendidas

Depois de aplicadas as regras das ACLs estendidas foram testadas as mesmas nos VPCs das figuras 49 e 50, onde é obtida a mensagem de pacotes a ser bloqueados, “Communication administratively prohibited”.



```

Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 192.168.0.2 255.255.255.240 gateway 192.168.0.1

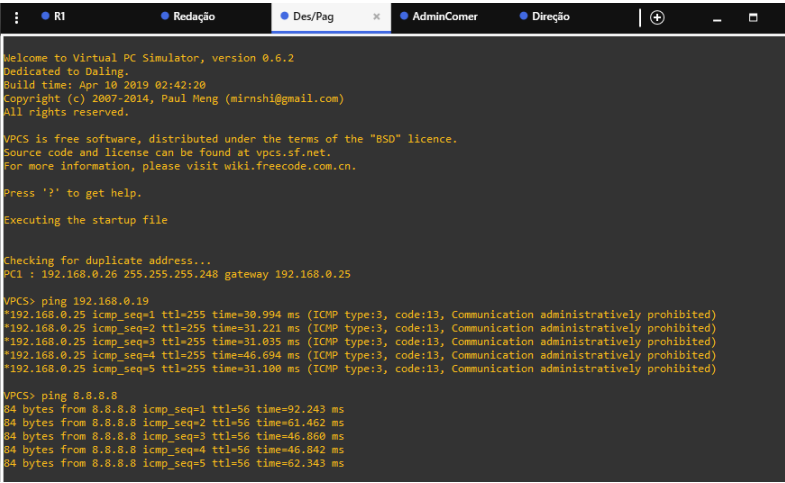
Redação> ping 192.168.0.19
*192.168.0.1 icmp_seq=1 ttl=255 time=30.644 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.0.1 icmp_seq=2 ttl=255 time=31.233 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.0.1 icmp_seq=3 ttl=255 time=31.016 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.0.1 icmp_seq=4 ttl=255 time=31.361 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.0.1 icmp_seq=5 ttl=255 time=31.093 ms (ICMP type:3, code:13, Communication administratively prohibited)

Redação> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=56 time=77.456 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=56 time=61.680 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=56 time=62.176 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=56 time=62.031 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=56 time=77.273 ms

Redação>

```

Figura 49 – Confirmação da aplicação das ACLs - Redação



```

Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 192.168.0.26 255.255.255.248 gateway 192.168.0.25

VPCS> ping 192.168.0.19
*192.168.0.25 icmp_seq=1 ttl=255 time=30.994 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.0.25 icmp_seq=2 ttl=255 time=31.221 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.0.25 icmp_seq=3 ttl=255 time=31.035 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.0.25 icmp_seq=4 ttl=255 time=46.694 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.0.25 icmp_seq=5 ttl=255 time=31.100 ms (ICMP type:3, code:13, Communication administratively prohibited)

VPCS> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=56 time=92.243 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=56 time=61.462 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=56 time=46.860 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=56 time=46.842 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=56 time=62.343 ms

```

Figura 50 – Confirmação da aplicação das ACLs – Design/Paginação

Na figura 51 é possível visualizar que a máquina Zabbix mesmo que queira não consegue comunicar com o VPC do departamento Administrativo e Comercial.

```
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 192.168.0.42 255.255.255.248 gateway 192.168.0.41

AdminComer> ping 192.168.0.19

Mini Ubuntu - Zabbix [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check
or proxy settings

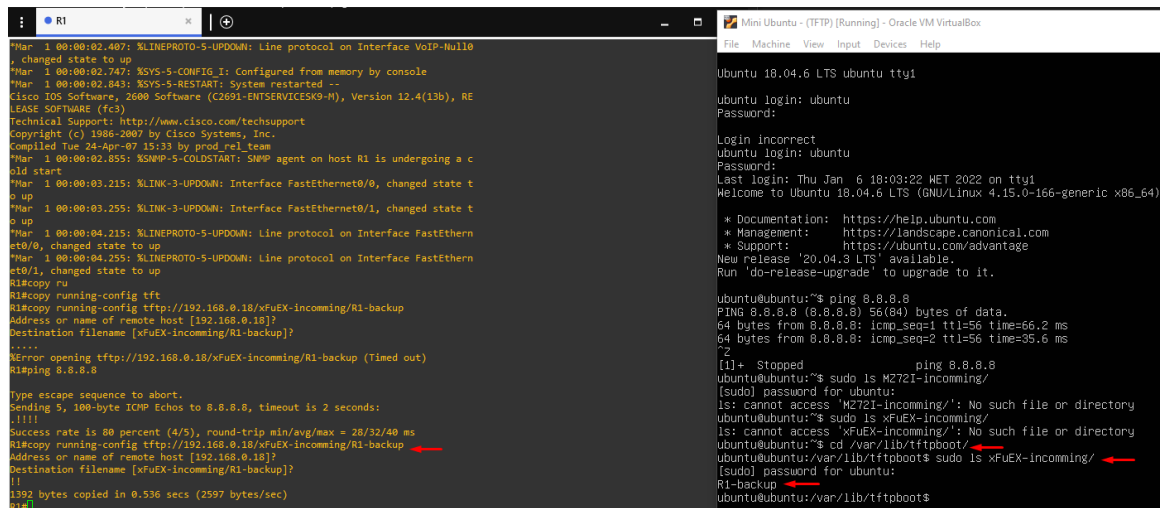
ubuntu@ubuntu:~$ ping 192.168.0.18
PING 192.168.0.18 (192.168.0.18) 56(84) bytes of data.
64 bytes from 192.168.0.18: icmp_seq=1 ttl=64 time=1.37 ms
64 bytes from 192.168.0.18: icmp_seq=2 ttl=64 time=1.11 ms
^C
[1]+ Stopped ping 192.168.0.18
ubuntu@ubuntu:~$ ping 192.168.0.19
PING 192.168.0.19 (192.168.0.19) 56(84) bytes of data.
64 bytes from 192.168.0.19: icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from 192.168.0.19: icmp_seq=2 ttl=64 time=0.035 ms
^C
[2]+ Stopped ping 192.168.0.19
ubuntu@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=41.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=25.4 ms
^C
[3]+ Stopped ping 8.8.8.8
ubuntu@ubuntu:~$ ping 192.168.0.42
PING 192.168.0.42 (192.168.0.42) 56(84) bytes of data.
^C
--- 192.168.0.42 ping statistics ---
0 packets transmitted, 0 received, 100% packet loss, time 8198ms

ubuntu@ubuntu:~$ ping 192.168.0.34
PING 192.168.0.34 (192.168.0.34) 56(84) bytes of data.
64 bytes from 192.168.0.34: icmp_seq=1 ttl=127 time=57.0 ms
64 bytes from 192.168.0.34: icmp_seq=2 ttl=127 time=62.1 ms
64 bytes from 192.168.0.34: icmp_seq=3 ttl=127 time=46.8 ms
^C
```

Figura 51 – Confirmação da aplicação das ACLs – Zabbix

10. Guardar todas as configurações aplicadas ao Router

Depois de finalizado todas as configurações do router e no projeto em geral foram transferidas as configurações para dentro da máquina TFTP para assim salvaguardar todos os comandos sendo útil caso o router preciso de ser removido ou substituído por outro.



```

R1
*Mar 1 00:00:02.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Nul10
, changed state to up
*Mar 1 00:00:02.747: %SYS-5-CONFIG-I: Configured from memory by console
*Mar 1 00:00:02.843: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 2600 Software (C2691-ENTSERVICESK9-M), Version 12.4(13b), RE
LEASE SOFTWARE (fc)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 24-Apr-07 15:33 by prod_rel_team
*Mar 1 00:00:02.855: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a c
old start
*Mar 1 00:00:03.215: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar 1 00:00:03.255: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar 1 00:00:04.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
*Mar 1 00:00:04.255: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
R1#copy ru
R1#copy running-config tft
R1#copy running-config tftp://192.168.0.18/xFuEX-incoming/R1-backup
Address or name of remote host [192.168.0.18]?
Destination filename [xFuEX-incoming/R1-backup]?
.....
Error opening tftp://192.168.0.18/xFuEX-incoming/R1-backup (Timed out)
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/32/40 ms
R1#copy running-config tftp://192.168.0.18/xFuEX-incoming/R1-backup
Address or name of remote host [192.168.0.18]?
Destination filename [xFuEX-incoming/R1-backup]?
11
1392 bytes copied in 0.536 secs (2597 bytes/sec)
R1#

Mini Ubuntu - (TFTP) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu 18.04.6 LTS ubuntu tty1
ubuntu login: ubuntu
Password:
Login incorrect
ubuntu login: ubuntu
Password:
Last login: Thu Jan 6 18:03:22 MET 2022 on tty1
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-166-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

ubuntu@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=66.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=35.6 ms
^C
[1]+  Stopped                  ping 8.8.8.8
ubuntu@ubuntu:~$ sudo is M272I-incoming/
[sudo] password for ubuntu:
is: cannot access 'M272I-incoming/': No such file or directory
ubuntu@ubuntu:~$ sudo is xFuEX-incoming/
is: cannot access 'xFuEX-incoming/': No such file or directory
ubuntu@ubuntu:~$ cd /var/lib/tftpboot/
ubuntu@ubuntu:/var/lib/tftpboot$ sudo is xFuEX-incoming/
[sudo] password for ubuntu:
R1-backup
ubuntu@ubuntu:/var/lib/tftpboot$
```

Figura 52 – Guardar configurações dentro do servidor TFTP

11. Políticas

11.1 Política de Segurança Física e Ambiental

De forma a proteger fisicamente os equipamentos críticos da rede, ou seja, máquinas servidor Zabbix, TFTP, IPfire, router e switch encontram-se todos dentro de uma divisão do departamento informático, dentro da sala do datacenter, esta sala é interdita a todos na empresa com exceção do pessoal do departamento informático, estes conseguem aceder a esta sala com recurso a uma porta corta fogo com autenticação fingerprint. Com esta medida limita-se muito as pessoas que conseguem entrar dentro da sala, para proteger as máquinas de possíveis danos foram implementados vários equipamentos, tais como as 5 unidades de UPS (Uninterruptible Power Supply) que servem para alimentar as máquinas caso haja um corte de eletricidade, esta medida protege possíveis danos internos nas máquinas, para além disso foi adicionado um termómetro que serve para monitorizar a temperatura da sala, algo que é essencial para as máquinas pois estas podem se estragar se atingiram temperaturas altas, com isso em mente foram instalados 2 ar condicionados que estão automatizados para começar a funcionar caso a temperatura da sala atingir certos valores, dependendo das temperaturas caso estas aumentam, o ar condicionado irá ligar e trabalhar numa velocidade pré estabelecida, no caso se a sala atingir 28°C este irá ligar e ficar a 30%, caso a temperatura aumente para 32/33°C os ar condicionados vão trabalhar a 50% e por aí em diante. Para conseguir expelir o ar quente que está dentro do datacenter foi necessário criar uma pequena ventilação para cada ar condicionado expelir o ar quente para a rua, como estas ventilações estão feitas num dado ângulo não irá de todo entrar chuva pela ventilação. Para além do ar condicionado vai ser também aplicado um sensor de fumo e de humidade que irá acusar caso algo dentro da sala começa a queimar ou haja muita humidade, obviamente os técnicos que operam nesta sala não poderão de todo trazer algo ou fazer algo na sala que acione estes sensores.

Todos estes sensores estão automatizados e podem ser monitorizados a partir de uma aplicação que irá informar tanto os técnicos como o diretor das temperaturas/condições da sala em tempo real.

Em relação á organização do gabinete, este terá concentrado em si todas as máquinas já faladas anteriormente, este será um gabinete que proporciona uma boa entrada e saída de ar para tal este terá os seus painéis perfurados, todos os cabos e portas do switch e router estarão devidamente identificados e organizados com patch panels e guias de cabos, isto irá facilitar a identificação de possíveis problemas e acelerar a resolução de possíveis problemas. As UPS estarão na parte inferior do gabinete enquanto o resto do material estará por cima.

Com a aplicação de todas estas medidas já referidas será possível diminuir drasticamente possíveis ameaças de ataques externos e internos.

11.2 Política de Controlo de Acessos à Informação

Uma das medidas mais importantes é a sensibilização dos empregados, com isto refiro-me a educar os trabalhadores da empresa sobre as boas práticas que estes devem aplicar quando estão a trabalhar dentro da instituição, para assim salvaguardar os dados dos mesmos e prevenir possíveis ataques/ameaças a estes e à empresa, esta na minha opinião é a mais importante política de segurança que deve ser logo instruída dentro dos elementos da empresa porque por vezes estes não sabem que podem estar em risco ou a pôr outros em risco, esta sensibilização passa tanto por ensinar que não se deve clicar em emails que parecem maliciosos assim como não aceder a sites sem certificação https até estes não serem alvos de engenharia social, para estes não entregarem informações críticas a terceiros.

Apenas os trabalhadores do departamento de informática tem acesso ao controlo dos servidores pois foram os únicos a não serem bloqueados pelas ACLs implementadas na rede, assim como apenas estes é que têm acesso a informações de como proceder caso aconteça problemas dentro do datacenter, para assim limitar o acesso á sala e ás informações e procedimentos que devem ser tomados dependente de cada situação que aconteça. Caso estes procedimentos fossem conhecidos por todos estes podiam ser explorados por pessoas mal intencionadas, conseguindo assim provocar ataques ou até conseguindo descobrir maneiras de atacar mesmo quando os técnicos estiveram a resolver os problemas.

11.3 Política de Gestão das Operações e das Comunicações

Para gerir a comunicação que passa na rede vai ser usado IPfire para poder proteger as máquinas da rede interna de possíveis acessos a sites perigosos, assim como esta irá monitorizar e tentar encontrar padrões de ataque nos pacotes que estejam a ser trocados entre a internet e a rede interna.

Na rede interna foi aplicado a atribuição de endereços às máquinas de forma manual para assim gerir uma a uma as máquinas que estão a comunicar na rede. Caso alguma máquina seja adicionada na rede esta tem de ser configurada pelos técnicos informáticos para assim conseguir funcionar, não foi criada nenhuma sub-rede de convidados pois não se justifica num ambiente empresarial destes ter uma sub-rede dessas, para além que ter uma sub-rede de convidados é outro ponto de abertura para invadir a rede.

11.4 Política de Gestão de Incidentes

Ainda haverá uma manta corta-fogo para ser utilizada antes de ser utilizado um institor, pois esta não causará tantos danos nos equipamentos, comparativamente a um pequeno institor, que estará na parede ao lado da entrada da sala.

Para além de todas as medidas já ditas ainda é preciso haver diretrizes de atuação consoante as situações/incidentes que aparecem, no caso será necessário haver documentos escritos que documentam o que fazer para cada situação, para assim saber quais os melhores processos a aplicar para cada situação que possa ocorrer, assim como haverá um plano de recuperação de incidentes quer estes sejam físicos ou computacionais.

12. Conclusão

Inicialmente tive alguma dificuldade em configurar corretamente o IPfire, porém assim que percebi que o problema era da máscara que tinha escolhido na interface green, apenas tive de alterar a sua terminação de .252 para .0 e consegui começar a pingar todos os equipamentos dentro da rede, o que anteriormente não conseguia, apenas conseguia pingar do router á internet, tive também umas pequenas dificuldades em configurar as Vlans, porém foi algo que consegui mais tarde ultrapassar.

Neste projeto criei uma rede com atribuição manual de endereços a cada máquina de modo a proteger a rede de instruções internas, configurei o servidor IPfire algo que não havia ainda feito em nenhum projeto, o uso deste mesmo verificou-se bastante importante pois este contém muitos recursos para proteger a rede, configurei também um servidor de TFTP para guardar o ficheiro de configuração do router dentro dele mesmo, configurei uma máquina com os serviços do Zabbix para assim monitorizar e gerir a rede, configurei uma máquina Windows no departamento de informática, máquina que servia para simular a gestão das máquinas servidor assim como o IPfire.

Com todos estes pontos que acabei de referir quero deixar claro que este projeto foi bastante importante para desenvolver de maneira mais aprofundada o meu conhecimento, adquirir novas ferramentas de trabalho e desenvolver as minhas capacidades de resolução de problemas.