

Relatório de Projeto

Redes de Computadores II



Docentes: Armando Ventura, João Tavanez, Pedro Moreira

Feito por: Martinho Caeiro (23917), Paulo Abade (23919)

Índice

Introdução	1
Desenvolvimento do Projeto	1
Endereços de Rede Utilizados	1
Topologia do Projeto	2
Configuração Router 1	2
Port Knocking.....	4
Regras Firewall.....	5
Configuração do Router 2.....	6
Regras de Firewall.....	8
Configuração do Router 3.....	10
Conclusão	12
Webgrafia	12

Índice de Imagens

Figura 1 - Topologia do Projeto	2
Figura 2 - Adaptadores do Router 1	2
Figura 3 - DHCP Client para receber um IP automaticamente	3
Figura 4 - Configuração das Interfaces Físicas e da Loopback	3
Figura 5 - Configuração do srcnat masquerade.....	3
Figura 6 - Configuração do OSPF.....	4
Figura 7 - Configuração do Port Knocking no Router 1	5
Figura 8 - Impede a comunicação entre o Router 2 e o Router 3	5
Figura 9 - Impedir que a Máquina do Cliente 1 aceda à Internet fora de horas	5
Figura 10 - Adaptadores do Router 2	6
Figura 11 - Configuração das Interfaces, da Loopback e do srcnat masquerade	6
Figura 12 - Configuração do OSPF do Router 2	7
Figura 13 - Configuração do DHCP Server com um range específico	8
Figura 14 - Firewall do Router 2 (Total).....	8
Figura 15 - Regra da Firewall para aceder apenas aos IPs permitidos.....	9
Figura 16 - Horas em que pode aceder aos sites do ips permitidos.....	9
Figura 17 - Configuração das Interfaces Físicas e Virtuais	10
Figura 18 - Configuração do OSPF do Router 3	10
Figura 19 - ACL's do Router 3	11
Figura 20 - Acesso por Telnet.....	11

Índice de Tabelas

Tabela 1 - Endereços de Rede Utilizados	1
---	---

Introdução

Neste projeto iremos fazer uma topologia que é composta por dois routers Mikrotik e um router Cisco. Nesta rede haverá três VLANs no router Cisco, incluindo a nativa, e serão abordadas outras funcionalidades como Firewall, ACLs, Port Knocking, entre outras.

Desenvolvimento do Projeto

Endereços de Rede Utilizados

Para obter os nossos endereços de rede, iremos utilizar o número do Martinho Caeiro (23917), então o nosso “F” será $23917 \% 200 = 117$.

Endereço de Rede	Range (Espaços)	Máscara	Wildcard
Rede A – 117.20.20.0	117.20.20.1-117.20.20.4	255.255.255.252	0.0.0.3
Rede B – 117.21.20.0	117.21.20.1-117.21.20.4	255.255.255.252	0.0.0.3
Rede C – 117.22.10.0 VLAN1	117.22.10.1-117.22.10.254	255.255.255.0	0.0.0.255
Rede C – 117.22.50.0 VLAN50	117.22.50.1-117.22.50.254	255.255.255.0	0.0.0.255
Rede C – 117.22.100.0	117.22.100.1-117.22.100.254	255.255.255.0	0.0.0.255
Rede D – 10.117.40.0	10.117.40.0-10.117.40.63	255.255.255	
Loopback R1	117.1.21.1	255.255.255.255	0.0.0.0
Loopback R2	117.1.22.1	255.255.255.255	0.0.0.0
Loopback R3	117.1.23.1	255.255.255.255	0.0.0.0

Tabela 1 - Endereços de Rede Utilizados

Topologia do Projeto

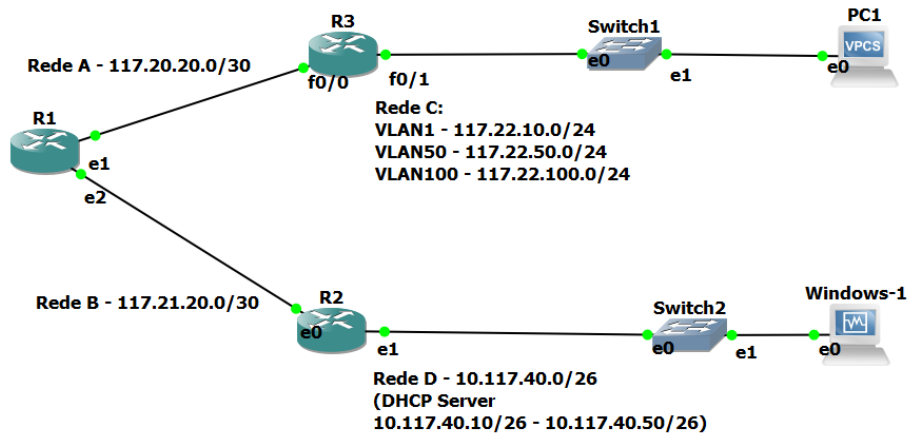


Figura 1 - Topologia do Projeto

Configuração Router 1

Descrição

O Router 1 será o router encarregado por receber a Internet e distribuir a Internet pela topologia. Este router é um MikroTik v6.49.10 x86 com 3 entradas, uma Adapter Bridge e duas Generic Drivers. A ether2 fará conexão com o Router 3, um router Cisco, enquanto a ether3 fará conexão com o Router 2, outro Mikrotik

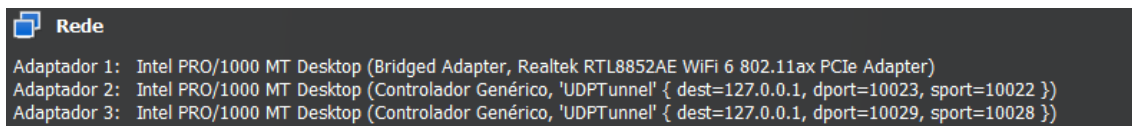


Figura 2 - Adaptadores do Router 1

Interfaces do Router

A porta ether1 estará associada com um DHCP Client, para receber um IP automaticamente e assim este router terá acesso à internet. A porta ether2 terá o IP - 117.20.20.1/30 e a porta ether3 terá o IP - 117.21.20.1/30

DHCP Client

DHCP Client DHCP Client Options

Release Renew

Interface	Use P...	Add D...	IP Address	Expires After	Status
ether1	yes	yes	192.168.1.83/24	00:48:11	bound

Figura 3 - DHCP Client para receber um IP automaticamente

Address List

Address	Network	Interface
117.1.21.1	117.1.21.1	Loopback
117.20.20.1/30	117.20.20.0	ether2
117.21.20.1/30	117.21.20.0	ether3
192.168.1.83/24	192.168.1.0	ether1

Bridge

Bridge Ports Port Extensions VLANs MSTIs

Settings

Name	Type
R Loopback	Bridge

Figura 4 - Configuração das Interfaces Físicas e da Loopback

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Reset Counters Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interf...	Out. Inte...
0	mas...	srcnat							ether1

Figura 5 - Configuração do srcnat masquerade

Encaminhamento Dinâmico

No Winbox, na instância default, é necessário alterar a Default Distributing Route para “Always as Type 2”, e é necessário inserir as redes vizinhas, ou seja, a rede A e a rede B, e ambas estão na área 0.0.0.0.

The first screenshot shows the 'OSPF Instance <default>' configuration window. The 'General' tab is active, showing the Name as 'default' and Router ID as '117.20.20.1'. The 'Redistribute Default Route' is set to 'always (as type 2)'. Other options like 'Redistribute Connected Routes', 'Redistribute Static Routes', 'Redistribute RIP Routes', 'Redistribute BGP Routes', and 'Redistribute Other OSPF Routes' are all set to 'no'. The 'In Filter' is 'ospf-in' and the 'Out Filter' is 'ospf-out'. The 'Routing Table' and 'Use DN' are empty. The 'enabled' checkbox is checked.

The second screenshot shows the 'OSPF' configuration window with the 'Areas' tab selected. It displays a table with the following data:

Area Name	Instance	Area ID	Type	Default Co...	Interfaces	Active I...	Neighb...
backbone	default	0.0.0.0	default		3	3	2

The third screenshot shows the 'OSPF' configuration window with the 'Networks' tab selected. It displays a table with the following data:

Network	Area
117.1.21.1	backbone
117.20.20.0/30	backbone
117.21.20.0/30	backbone

The fourth screenshot shows the 'OSPF' configuration window with the 'Networks' tab selected. It displays a table with the following data:

Interface	Cost	Priority	Authentica...	Authentication ...	Network Type	Instance	Area	Neigh...	State
DP Loopback	10	1	none	*****	broadcast	default	backbone	0	passive
D ether2	10	1	none	*****	broadcast	default	backbone	1	designated ro...
D ether3	10	1	none	*****	broadcast	default	backbone	1	backup

Figura 6 - Configuração do OSPF

Port Knocking

Neste router haverá Port Knocking, que consiste que o utilizador apenas possa entrar no modo de configuração do Router, seja por SSH ou por Winbox, se e só se, acertar a combinação de portas indicada pelo docente (3000-4000-5000). Para isto ser feito, foi necessário criar duas listas temporárias para que verificar se a combinação das portas estava a ser feita corretamente. Após passar para a terceira e última porta, caso o utilizador acerte a última porta, o seu IP será adicionado à lista de IP confiáveis durante 30 minutos, depois desse tempo, precisa voltar a fazer a combinação de portas.

Firewall															
Filter Rules															
NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols															
+ - ✓ ✕ 📄 🔍 ⌂ Reset Counters ⌂ Reset All Counters															
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interf...	Out. Inte...	In. Interf...	Out. Inte...	Src. Ad...	Dst. Ad...	Bytes	Packets
0	✓ acc...	input			6 (tcp)		8291,22	ether1				trusted-i...		123.8 KiB	1 323
--- Fase 1															
1	✕ add ...	input			6 (tcp)		3000	ether1						208 B	4
--- Fase 2															
2	✕ add ...	input			6 (tcp)		4000	ether1				fase1-k...		208 B	4
--- Fase 3															
3	✕ add ...	input			6 (tcp)		5000	ether1				fase2-k...		208 B	4
--- Bloqueia os ip's de quem não cumpriu															
4	✕ drop	input			6 (tcp)		8291,22	ether1						2392 B	46

Figura 7 - Configuração do Port Knocking no Router 1

Regras Firewall

Configuração da firewall de modo que as máquinas cliente de redes diferentes não possam comunicar entre si.

5	✕ drop	forward						ether2	ether3					2452 B	32
---	--------	---------	--	--	--	--	--	--------	--------	--	--	--	--	--------	----

Figura 8 - Impede a comunicação entre o Router 2 e o Router 3

Foi necessário adicionar ainda estas duas regras para impedir que a Máquina do Cliente 1, com o IP 117.22.100.2/24 só consiga aceder à Internet entre as 17h00 e as 23h00, de segunda a sexta-feira.

6	✓ acc...	forward	117.22.100.2		6 (tcp)	80,443								0 B	0
7	✕ drop	forward	117.22.100.2		6 (tcp)	80,443								0 B	0

Time

Time: 17:00:00 - 23:00:00

Days: ☐ sun ☒ mon ☒ tue ☒ wed ☒ thu ☒ fri ☐ sat

Queue List

Simple Queues

Interface Queues

Queue Tree

Queue Types

+ - ✓ ✕ 📄 🔍 ⌂ Reset Counters ⌂ Reset All Counters

#	Name	Target	Upload Max Limit	Download Max Limit
0	queue1	117.22.100.2	1M	1M

Figura 9 - Impedir que a Máquina do Cliente 1 aceda à Internet fora de horas

Configuração do Router 2

Descrição

Este router terá apenas duas interfaces, a ether1 que está ligada ao Router 1 e a ether2 que está ligada a um switch que poderá ter até 40 utilizadores, que terão o seu IP automaticamente por DHCP Server.

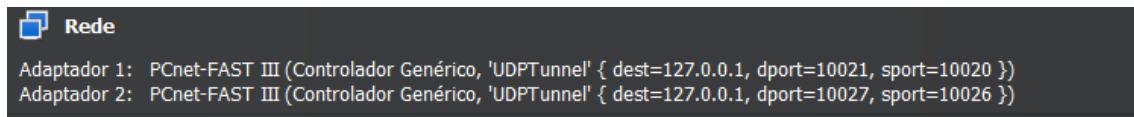


Figura 10 - Adaptadores do Router 2

Interfaces do Router

A porta ether1 terá o IP de 117.21.20.2/30 e a porta ether2 terá o IP de 10.117.10.1/26.

Foi escolhido o endereço de rede 10.117.10.0/26 devido ao número de espaços do DHCP Server, que são 40. Se fosse utilizada a máscara /27, não iria haver o número de espaços necessários, então com a /26 temos 62 endereços de IP disponíveis e na configuração do DHCP Server foi limitada a atribuição de IPs entre 10.117.40.10/26 e 10.117.40.50/26.

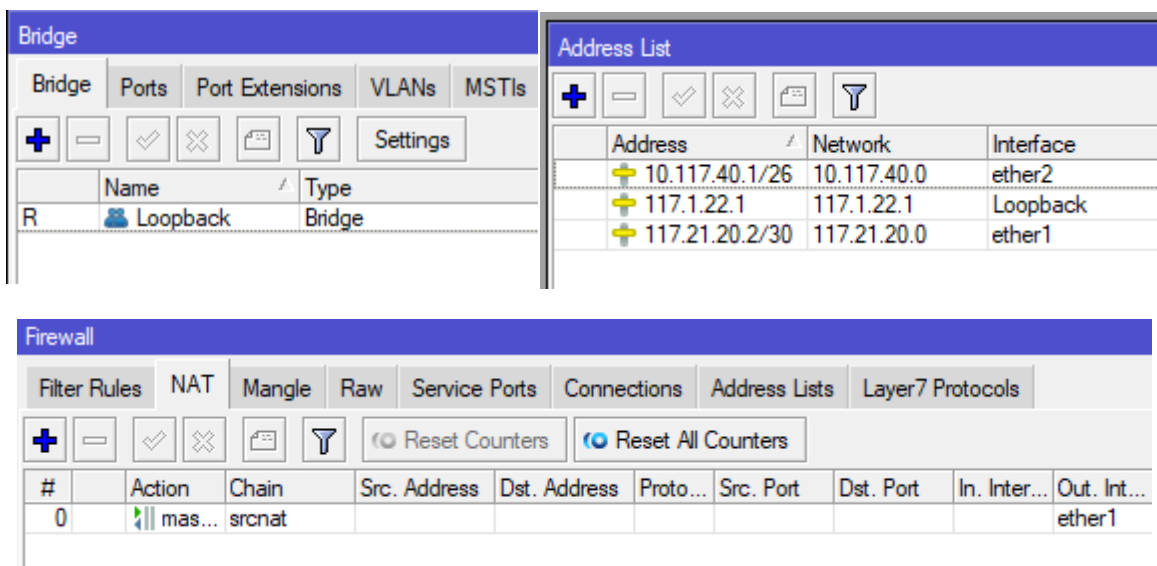


Figura 11 - Configuração das Interfaces, da Loopback e do srcnat masquerade

Encaminhamento Dinâmico

No encaminhamento dinâmico deste router precisamos apenas adicionar as redes vizinhas, a Rede B e a Rede D. Nesta parte, não é necessário adicionar uma Default Route.

OSPF

Interfaces	Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors
+ - ✓ ✗ 📁 🗑️						
Name	Router ID	Running				
default	117.21.20.2	yes				

OSPF Instance <default>

General Metrics MPLS Status

Name: default

Router ID: 117.21.20.2

Redistribute Default Route: never

Redistribute Connected Routes: no

Redistribute Static Routes: no

Redistribute RIP Routes: no

Redistribute BGP Routes: no

Redistribute Other OSPF Routes: no

In Filter: ospf-in

Out Filter: ospf-out

Routing Table:

Use DN:

OK Cancel Apply Disable Comment Copy Remove

enabled default

OSPF								
Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	
+ - ✓ ✗ 📁 🗑️								
Area Name	Instance	Area ID	Type	Default C...	Interfac...	Active I...	Neighb...	
backbone	default	0.0.0.0	default		3	3	1	

OSPF			
Instances	Networks	Areas	Area R
+ - ✓ ✗ 📁 🔄			
Network	Area		
10.117.40.0/26	backbone		
117.1.22.1	backbone		
117.21.20.0/30	backbone		

Figura 12 - Configuração do OSPF do Router 2

DHCP Server

Para fazer o DHCP Server foi necessário escolher a IP Range entre 10.117.40.10/26 até 10.117.40.50/26.

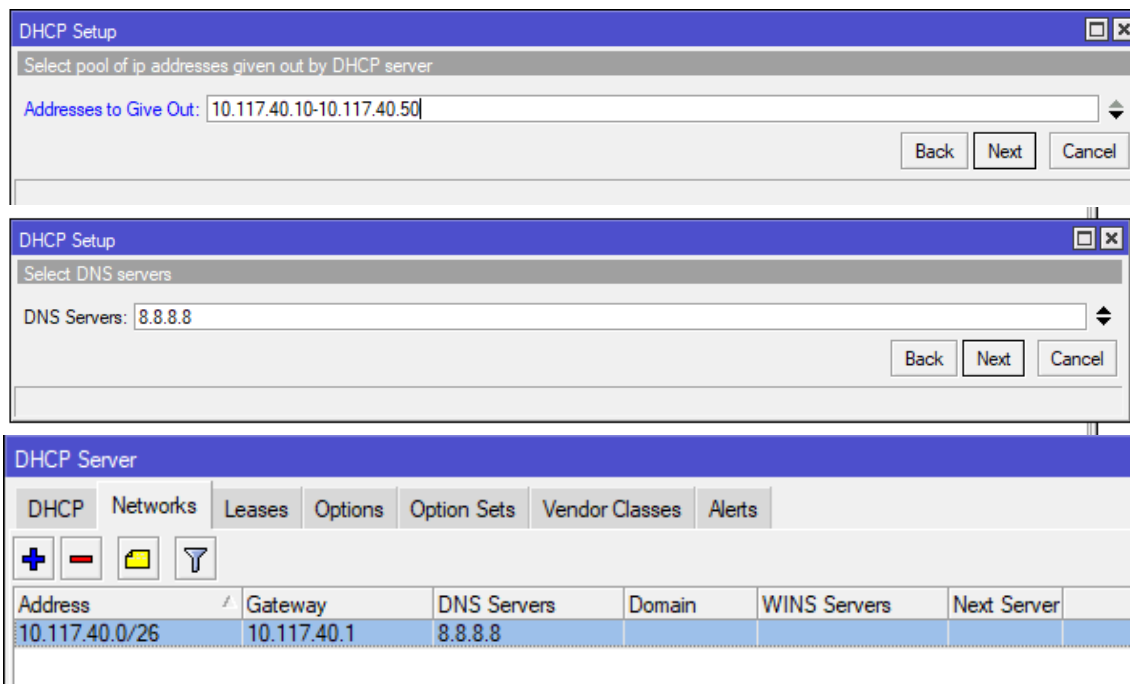


Figura 13 - Configuração do DHCP Server com um range específico

Regras de Firewall

Com o objetivo que a máquina virtual ligada ao router 2 apenas tenha acesso ao site das Finanças e da Segurança Social durante um certo período.

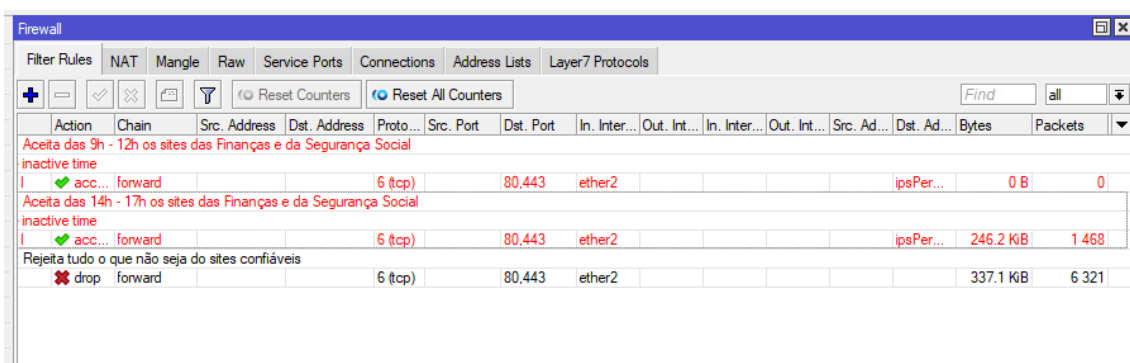


Figura 14 - Firewall do Router 2 (Total)

Firewall Rule <80,443>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐ 80,443

Any. Port:

In. Interface: ☐ ether2

Out. Interface:

In. Interface List:

Firewall Rule <80,443>

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List: ☐ ipsPermitidos

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

Figura 15 - Regra da Firewall para aceder apenas aos IPs permitidos

É definido as horas e os dias em que os utilizadores podem aceder aos sites pré-determinados.

Firewall Rule <80,443>

General Advanced Extra Action Statistics

Connection Limit:

Limit:

Dst. Limit:

Nth:

Time: -

Days: ☒ sun ☒ mon ☒ tue ☒ wed ☒ thu ☒ fri ☒ sat

Firewall Rule <80,443>

General Advanced Extra Action Statistics

Connection Limit:

Limit:

Dst. Limit:

Nth:

Time: -

Days: ☒ sun ☒ mon ☒ tue ☒ wed ☒ thu ☒ fri ☒ sat

Figura 16 - Horas em que pode aceder aos sites do ips permitidos

Configuração do Router 3

Interfaces do Router 3

As interfaces foram definidas da seguinte forma: a FastEthernet 0/0 tem a conexão com o Router 1, a FastEthernet 0/1 é a VLAN nativa, e as outras duas FastEthernet 0/1.50 e a FastEthernet 0/1.100 são as outras VLANs, e têm o encapsulamento dot1Q. Por fim, a Loopback também foi definida.

```
interface Loopback3
 ip address 117.1.23.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 117.20.20.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 117.22.10.1 255.255.255.0
 ip access-group 117 in
 duplex auto
 speed auto
!
interface FastEthernet0/1.50
 encapsulation dot1Q 50
 ip address 117.22.50.1 255.255.255.0
 ip access-group 117 in
!
interface FastEthernet0/1.100
 encapsulation dot1Q 100
 ip address 117.22.100.1 255.255.255.0
 ip access-group 117 in
!
```

Figura 17 - Configuração das Interfaces Físicas e Virtuais

Encaminhamento Dinâmico

Novamente, adicionamos todas as redes vizinhas, incluindo as VLANs e o Loopback.

```
router ospf 117
 log-adjacency-changes
 network 117.1.23.1 0.0.0.0 area 0.0.0.0
 network 117.20.20.0 0.0.0.3 area 0.0.0.0
 network 117.22.10.0 0.0.0.255 area 0.0.0.0
 network 117.22.50.0 0.0.0.255 area 0.0.0.0
 network 117.22.100.0 0.0.0.255 area 0.0.0.0
```

Figura 18 - Configuração do OSPF do Router 3

ACL's

Nestas ACL's foi seguida a seguinte ordem: Permitir o acesso à Internet pelas portas 80 e 443, permitir que as VLAN's comuniquem com a própria subrede, remover a comunicação entre VLAN's e depois permitir o acesso à internet com a última linha.

```
access-list 117 permit tcp any any eq www
access-list 117 permit tcp any any eq 443
access-list 117 permit ip 117.22.10.0 0.0.0.255 117.22.10.0 0.0.0.255
access-list 117 permit ip 117.22.100.0 0.0.0.255 117.22.100.0 0.0.0.255
access-list 117 permit ip 117.22.50.0 0.0.0.255 117.22.50.0 0.0.0.255
access-list 117 deny ip 117.22.10.0 0.0.0.255 117.22.0.0 0.0.255.255
access-list 117 deny ip 117.22.50.0 0.0.0.255 117.22.0.0 0.0.255.255
access-list 117 deny ip 117.22.100.0 0.0.0.255 117.22.0.0 0.0.255.255
access-list 117 permit ip any any
```

Figura 19 - ACL's do Router 3

Acesso por Telnet

Para aceder por Telnet ao Router 3, foi necessário configurar uma palavra-passe para ao entrar no Router e ao entrar no terminal do router. Para aumentar a segurança do router, ainda foi encriptada a palavra-passe com o comando:

“service password-encryption”

```
line con 0
exec-timeout 0 0
privilege level 15
password 7 08334F1C
logging synchronous
login
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
password 7 0519055D
login
```

Figura 20 - Acesso por Telnet

Conclusão

Este trabalho foi interessante de ser realizado e aprendemos mais sobre esta área da Informática. Nunca tínhamos ouvido falar sobre o conceito de Port Knocking e como este funcionava, porém consideramos que o resultado deste projeto foi satisfatório.

Webgrafia

[Página da Unidade Curricular de Redes de Computadores 2](#)

[Port Knocking no Youtube - Wilmer Almazan](#)

[Página do Software Oracle VirtualBox](#)

[Página do Software GNS3](#)

[Página da Mikrotik](#)

[Página da Cisco](#)