isec
Engenharia

Licenciatura em Engenharia Informática

Ramo de Redes e Administração de Sistemas
Unidade Curricular de Segurança

Relatório do Trabalho Prático

Ano Letivo de 2020/2021

João Pedro Correia Fernandes - Nº 2019129402
João Pedro Verdete Santos - Nº 2017011382
Rafael de Jesus Saraiva - Nº 2017010339
Rodrigo José Machado Faustino - Nº 2019140987

Índice

Índice ***1***

Implementação ***3***

Radius 3

Syslog 3

Utilizadores e Vistas 4

Banners 6

AAA e Logging 7

Logging 8

Firewalls **9**

Spoofing 9

Bloqueio Externo 9

Rede Docentes e Externos 10

Core-Servicos 10

DeepZone 11

Outros 12

Não Implementado **14**

Introdução

O nosso trabalho prático baseou-se na seguinte topologia:

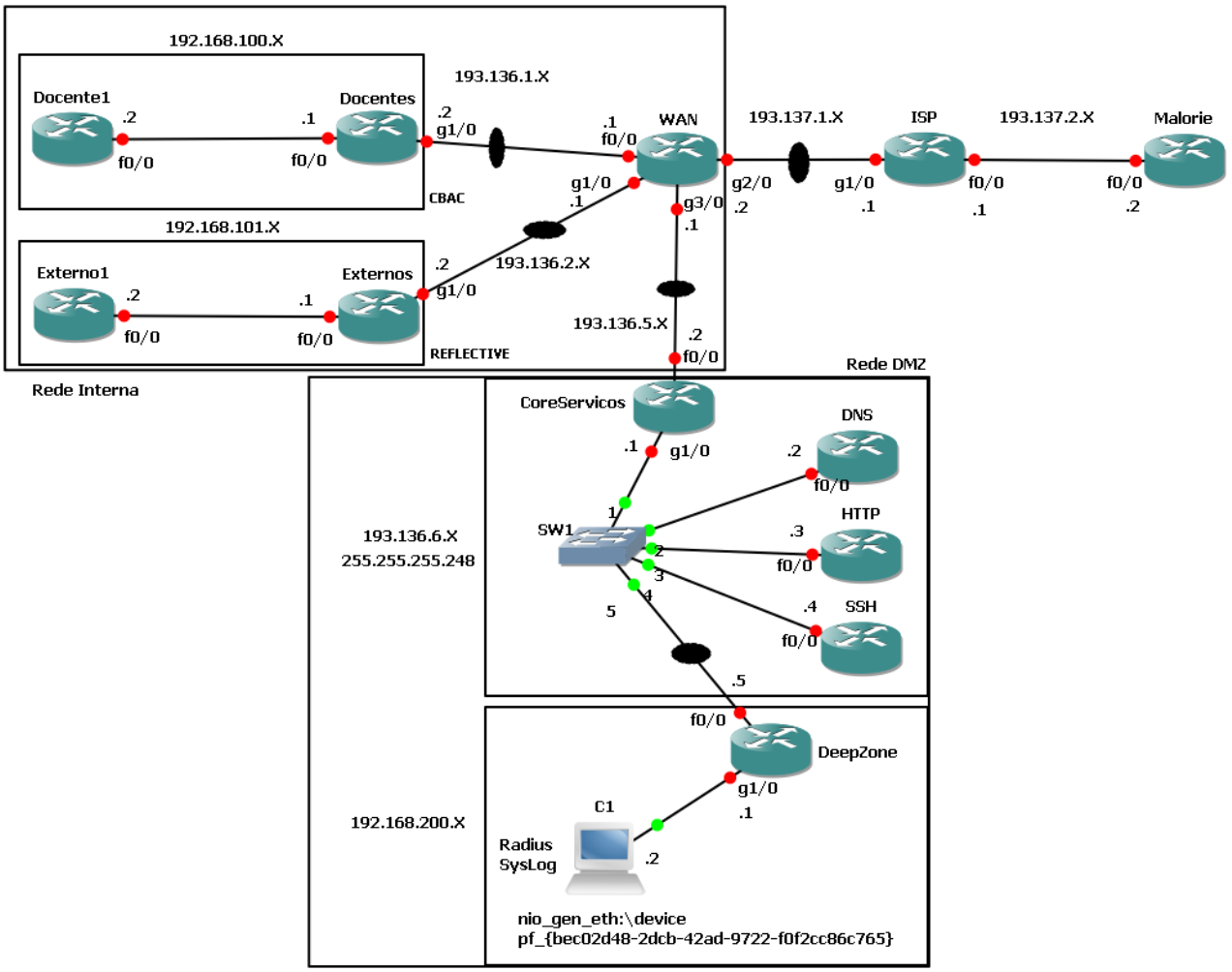

Figura 1 - Ilustração da topologia

Legenda:

Ligações Upper-Link

Implementação

Radius

A **implementação do Radius** decidimos implementar na rede da Deepzone pois como é uma rede em que é suposto o gestor da rede se ligar achamos que seria o mais correto. Na configuração do Radius como host colocamos o IP do PC do gestor que se liga à nossa rede Deepzone, ou seja, 192.168.200.2 com a password myradiuspwd e com os default ports (1812 e 1813). Para isto utilizamos o seguinte comando:

```
radius-server host 192.168.200.2 auth-port 1812 acct-port 1813 key myradiuspwd
```

Figura 2 - Especificação do endereço e chave do servidor Radius

---

Syslog

Na **implementação do Syslog** colocamos também na rede da Deepzone de maneira ao gestor que se ligar a essa rede tenha acesso a todos os logs de todos os routers internos da nossa topologia. Para isto colocou-se vários comandos tanto no router da Deepzone como nos routers internos da nossa topologia. Os comandos são os seguintes:

```
logging source-interface GigabitEthernet1/0
logging 192.168.200.2
```

Figura 3 - Ativação do logging e indicação do servidor central

Os comandos acima identificam qual o nosso host, ou seja, o IP do PC do nosso gestor e também qual a interface do router Deepzone que vai comunicar com o PC do gestor. No print não é referido, porém também foi implementado um comando onde especifica qual o nivel de detalhe dos logs, ou seja, logging trap informational (nível 6), onde apenas mostra mensagens informativas.

Nos routers internos da topologia foram implementados os seguintes comandos:

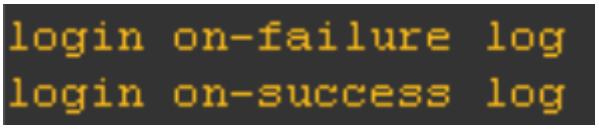

Figura 4 - Comandos relativos ao log do utilizador

Os comandos acima servem para o gestor saber se em qualquer router foi feito login com sucesso ou se falhou o login no router. O gestor só consegue saber estas informações se for também implementado o comando logging host 192.168.200.2, este foi implementado em todos os routers inclusive o da Deepzone.

Utilizadores e Vistas

Para o **acesso aos routers** foram criados utilizadores com diversos privilégios e funções. Em todos os routers internos (Wan, Core-Serviços) da topologia foram criados os utilizadores oper, adm e manager.

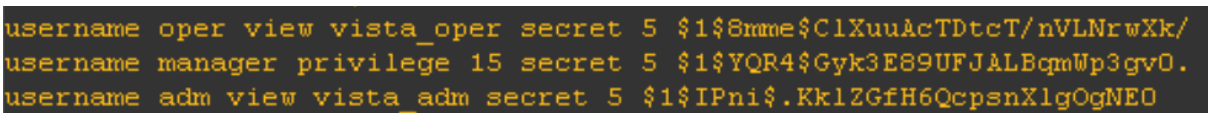

Figura 5 - Utilizadores presentes nos routers WAN e CORE-SERVIÇOS

Nos routers finais (Docentes, Externos e Deepzone) apenas criamos o utilizador oper.

Figura 6 - Utilizadores presentes nos routers finais

De maneira a limitar a tentativa de acesso aos routers decidimos colocar o seguinte comando:

Figura 7 - Medida que limita tentativas de acesso

O comando acima serve para bloquear o acesso durante 10 minutos(o equivalente a 600 segundos) a determinado equipamento após haver 3 tentativas de login falhadas, num prazo de 60 segundos.

Para o **utilizador 'oper'** foi criada uma view onde apenas pode visualizar as interfaces dos routers à exceção dos Upper-links, ou seja, as interfaces ligadas a routers mais perto do exterior (Internet), indicadas na topologia com uma bola preta. O 'oper' também pode apenas alterar a descrição das interfaces. Este utilizador foi configurado da seguinte maneira:

```
parser view vista_oper
 secret 5 $1$mjLY$PQFInOAb1YDedWZ.L69fQO
 commands interface include description
 commands configure include interface
 commands exec include configure terminal
 commands exec include configure
 commands exec include show running-config
 commands exec include show
 commands configure include interface FastEthernet0/0
 commands configure exclude interface GigabitEthernet1/0
```

Figura 8 - Comandos implementados na vista associada ao utilizador "oper"

Para o **utilizador adm** foi criada uma view onde consegue ver todos os interfaces podendo fazer todos os comandos dentro da interface à exceção do shutdown com os seguintes comandos:

```
parser view vista_adm
 secret 5 $1$xuii$7ue8saMCvhcTI1lXItkec/
 commands interface exclude shutdown
 commands configure include all interface
 commands exec include configure terminal
 commands exec include configure
 commands exec include show running-config
 commands exec include show
```

Figura 9 - Comandos implementados na vista associada ao utilizador "adm"

No utilizador manager foram-lhe atribuídos todos os privilégios, ou seja, privilégio total sobre o equipamento em questão:

```
username manager privilege 15 secret 5 $1$YQR4$Gyk3E89UFJALBqmWp3gv0.
```

Figura 10 - Linha implementada ao utilizador "maganer"

Para o requisito **“fecho de serviços desnecessários”** após alguma pesquisa decidimos implementar os seguintes comandos: no ip bootp server, no ip source-route, no service pad, no service finger, no ip identd, no service tcp-small-servers e por fim no service udp-small-servers em todos os routers.

Banners

Na **criação de banners** criamos dois tipos, o banner exec(que aparecerá numa fase inicial, sem que seja preciso o acesso ao equipamento com uma password) e o banner login(que será visualizado após uma autenticação com sucesso) onde colocamos o seguinte:

```
banner exec ^C -------Router CoreServicos-------
Rede: 192.136.6.X, 192.136.5.X
Possiveis destinos: 192.136.6.X, 192.168.100.X
Interfaces incorporadas: g1/0 (Rede 193.136.6.X), f0/0 (WAN)
^C
banner login ^C       -------G4-------
Rodrigo Faustino-201914098720191409 87
Rafael Saraiva-2017010339
Joao Santos-2017011382
Joao Fernandes-2019129402

Cuidados a ter:
[1] Nao partilhar passwords
[2] Manter o sistema atualizado
[3] Realizar Backups
^C
```

Figura 11 - Banners referidos acima

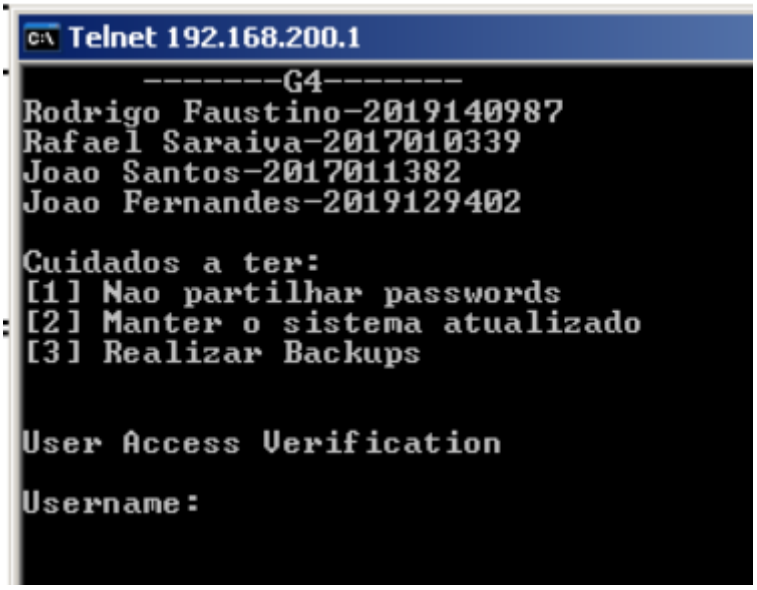

Figura 12 - Banner 'login'

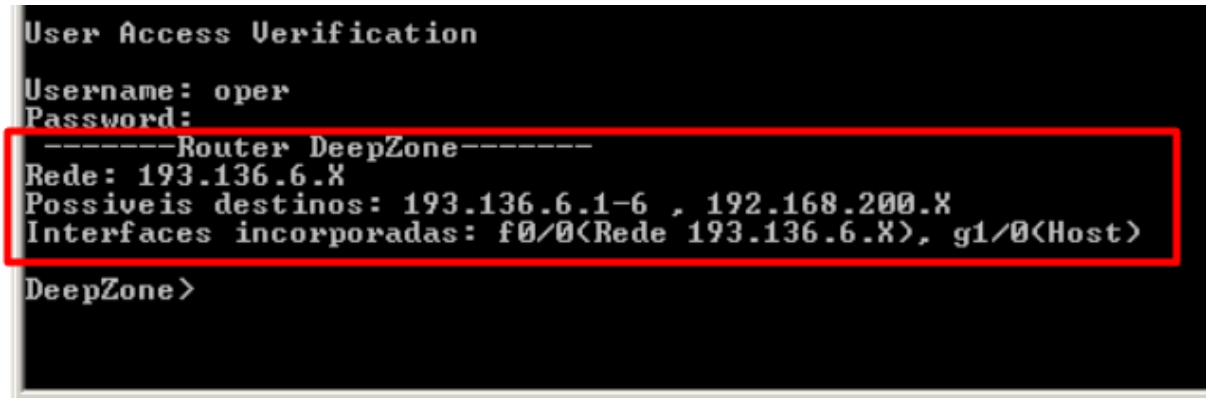

Figura 13 - Banner 'exec'

AAA e Logging

AAA

De modo a ativar o modelo authorization, authentication, accounting:

```
aaa new-model
```

Para configurar o método de autenticação implementamos o seguinte comando:

```
aaa authentication login default local group radius
 line vty 0 4
   login authentication default
```

De forma a monitorizar quando um determinado utilizador entra e sai do equipamento:

```
aaa accounting exec default start-stop group radius
```

Logging

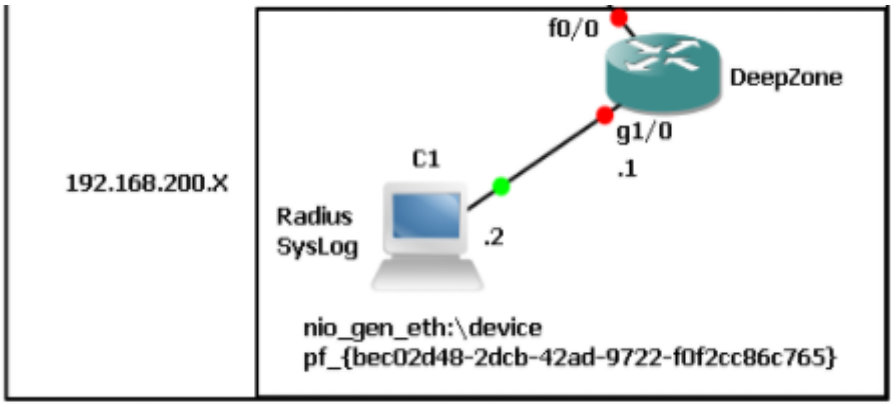

Figura 12 - Visualização da interface e endereço da respectiva rede

logging source-interface GigabitEthernet1/0 (os logs provêm desta interface)
logging 192.168.200.2 (servidor central de syslog)
logging trap informational (Nível de debug introduzido = informational = 6)

Firewalls

Spoofing

Nas access-lists seguintes, presentes no router WAN, é feito bloqueio do spoofing para dentro e fora da rede interna.

```
ip access-list extended anti_spoofing_in
 deny   ip 193.136.1.0 0.0.0.3 any
 deny   ip 193.136.2.0 0.0.0.3 any
 deny   ip 193.136.5.0 0.0.0.3 any
 deny   ip 193.136.6.0 0.0.0.7 any
 deny   ip 192.168.100.0 0.0.0.3 any
 deny   ip 192.168.101.0 0.0.0.3 any
 deny   ip 192.168.200.0 0.0.0.3 any
 deny   ip host 0.0.0.0 any
 deny   ip 127.0.0.0 0.255.255.255 any
 permit ip any any
```

```
ip access-list extended anti_spoofing_out
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 172.16.0.0 0.15.255.255 any
 deny   ip 193.137.2.0 0.0.0.3 any
 permit ip any any
```

Bloqueio Externo

Na access-lists seguintes, apresenta-se o bloqueio de qualquer comunicação oriunda do exterior da rede, para o interior do router WAN.

O bloqueio é feito por ACLs do tipo CBAC e reflexivas.

```
ip access-list extended deny_cbac_g1/0_in
 deny   ip 193.137.1.0 0.0.0.3 any
 deny   ip 193.137.2.0 0.0.0.3 any
 permit ip 192.168.200.0 0.0.0.3 any
```

```
ip access-list extended deny_outside_g1/0_in
 evaluate rede_externo
 permit ip 192.168.200.0 0.0.0.3 any
 permit ip 193.136.2.0 0.0.0.3 any
 deny   ip any any
```

No caso do router WAN e rede DMZ, os mesmos têm ACLs que fazem permissão de outro tipo de tráfego, desse modo o telnet e ssh estão bloqueados por defeito.

Rede Docentes e Externos

No caso do bloqueio de qualquer ligação a estas redes, o mesmo está explícito na secção anterior.

Para as ligações TCP, UDP e ICMP os mesmos têm permissão de acesso com as seguintes regras.

```
 permit ip any 193.136.6.0 0.0.0.7
 permit ip any 192.168.200.0 0.0.0.3
 permit ip any 193.136.5.0 0.0.0.3
```

Core-Servicos

A permissão aos diversos serviços internos segue-se da seguinte maneira.

```
access-list 151 permit tcp any host 193.136.6.2 eq domain
access-list 151 permit tcp any host 193.136.6.3 eq www
access-list 151 permit tcp any host 193.136.6.4 eq 22
```

Para ser possível pingar o DNS pelo Malorie, recorre-se a uma ACL dinâmica, que pelo login numa consola telnet no router Core-Servicos, o utilizador fica com uma sessão ativa de acesso ICMP ao DNS.

```
access-list 151 dynamic core_dynamic_f0/0_in permit icmp
193.137.2.0 0.0.0.3 host 193.136.6.2
```

DeepZone

A permissão ao acesso dos serviços de Radius e Syslog é feita por estas regras na seguinte ACL.

```
ip access-list extended perm_radSys_f0/0_in
 permit udp any 192.168.200.0 0.0.0.3 eq 1812
 permit udp any 192.168.200.0 0.0.0.3 eq 1813
 permit udp any 192.168.200.0 0.0.0.3 eq syslog
```

A partir desta rede, é possível realizar telnet e ssh para os equipamentos da rede interna.

```
ip access-list extended perm_ssh_telnet_internos_f0/0_out
 permit tcp 192.168.200.0 0.0.0.3 193.136.5.0 0.0.0.3 eq 22
 permit tcp 192.168.200.0 0.0.0.3 193.136.5.0 0.0.0.3 eq telnet
 permit tcp 192.168.200.0 0.0.0.3 193.136.1.0 0.0.0.3 eq 22
 permit tcp 192.168.200.0 0.0.0.3 193.136.1.0 0.0.0.3 eq telnet
 permit tcp 192.168.200.0 0.0.0.3 193.136.2.0 0.0.0.3 eq 22
 permit tcp 192.168.200.0 0.0.0.3 193.136.2.0 0.0.0.3 eq telnet
 permit tcp 192.168.200.0 0.0.0.3 192.168.100.0 0.0.0.3 eq 22
 permit tcp 192.168.200.0 0.0.0.3 192.168.100.0 0.0.0.3 eq telnet
 permit tcp 192.168.200.0 0.0.0.3 192.168.101.0 0.0.0.3 eq 22
 permit tcp 192.168.200.0 0.0.0.3 192.168.101.0 0.0.0.3 eq telnet
```

E de seguida os equipamentos internos podem ser pingados com o uso destas regras na ACL.

```
 permit icmp 192.168.200.0 0.0.0.3 193.136.6.0 0.0.0.7
 permit icmp 192.168.200.0 0.0.0.3 193.136.5.0 0.0.0.3
 permit icmp 192.168.200.0 0.0.0.3 193.136.1.0 0.0.0.3
 permit icmp 192.168.200.0 0.0.0.3 193.136.2.0 0.0.0.3
 permit icmp 192.168.200.0 0.0.0.3 192.168.100.0 0.0.0.3
 permit icmp 192.168.200.0 0.0.0.3 192.168.101.0 0.0.0.3
```

Outros

Relativamente ao bloqueio do acesso à Internet para os utilizadores docentes e externos, o mesmo é feito com esta regra *time-based* na ACL do router respectivo.

```
permit ip any 193.137.1.0 0.0.0.3 time-range dias_uteis
```

Foram usados os seguintes tipos de firewalls, tipo *Standard*, *Extended*, *Dynamic*, *Reflexive*, *Time-based* e *CBAC*.

Standard, no router Docentes:

```
access-list 1 deny   192.168.101.0 0.0.0.3
access-list 1 permit any
```

Extended, em múltiplos routers (Docentes, Externos, Wan, ...):

```
ip access-list extended dmz_in
 permit ip 192.168.200.0 0.0.0.3 any
 permit ip any any
```

Dynamic, no router Core-Servicos:

```
access-list 151 dynamic core_dynamic_f0/0_in permit icmp
193.137.2.0 0.0.0.3 host 193.136.6.2
```

Reflexive, no router Externos (ACL comprimida):

```
ip access-list extended deny_outside_g1/0_in
 evaluate rede_externo
 (...)
 deny   ip any any
ip access-list extended deny_outside_g1/0_out
 permit ip any 193.137.1.0 0.0.0.3 time-range dias_uteis reflect
rede_externo timeout 300
 permit ip any 193.137.2.0 0.0.0.3 reflect rede_externo timeout
10
 (...)
```

Time-based, nos routers Externos e Docentes:

```
permit ip any 193.137.1.0 0.0.0.3 time-range dias_uteis
```

CBAC, no router Docentes:

```
ip inspect name doc_serv tcp
ip inspect name doc_serv udp
ip inspect name doc_serv icmp

interface GigabitEthernet1/0
 (...)
 ip inspect doc_serv out

ip access-list extended deny_cbac_g1/0_in
 deny ip 193.137.1.0 0.0.0.3 any
 deny ip 193.137.2.0 0.0.0.3 any
```

Para o NAT (Overload/PAT), de modo a possibilitar o acesso ao exterior a partir da rede Interna(Docentes, Externos):

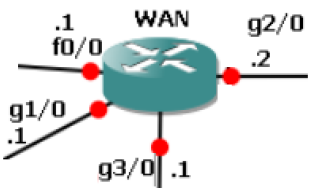

Figura 13 - Visualização das interfaces referidas imediatamente de seguida.

interface GigabitEthernet2/0 (Interface de saída)
ip nat outside
interface FastEthernet0/0 (Interface de entrada)
ip nat inside
interface GigabitEthernet1/0 (Interface de entrada)
ip nat inside

ip nat inside source list 1 interface GigabitEthernet2/0 overload (Interface de saída)

access-list 1 permit 192.168.100.0 0.0.0.3 (Rede Docente1 - Docente)
access-list 1 permit 192.168.101.0 0.0.0.3 (Rede Externo1 - Externos)

Não Implementado

- Uma vez que nos deparamos com problemas nos routers externos, pois estes não arrancavam, decidimos mudar os **routers C2600** para os **C7200**.

  NOTA: Uma vez que os routers C2600 não permitem a aplicação do comando *'secret'* utilizámos o comando *'password',* juntamente com o comando *'service password-encryption'* de modo a encriptar todas as palavras-passe com o nível 7.
- Não foi implementada a access list Zone-Based, pois quando a implementamos no router Core-Serviços algumas access-lists deixaram de funcionar, no entanto deixamos de seguida a tentativa realizada nesse mesmo router:

```
zone security F0/0
     desc DMZ
zone security G1/0
     desc Core_Dentro
int f0/0
     zone-member security F0/0
int g1/0
     zone-member security G1/0
access-list 101 permit tcp any host 193.136.6.2 eq 53
access-list 101 permit tcp any host 193.136.6.3 eq 80
access-list 101 permit tcp any host 193.136.6.4 eq 22
class-map type inspect f0/0_class
     match access-group 101
policy-map type inspect F0/0
     class type inspect f0/0_class
         inspect
zone-pair security F0/0-G1/0 source F0/0 destination G1/0
     service-policy type inspect F0/0
```

- A 'configuração do servidor de ssh e limitação a apenas este protocolo para os equipamentos que o permitam' também não foi implementada pois não percebemos o pretendido.