Departamento de Engenharia Informática e de Sistemas

Instituto Superior de Engenharia de Coimbra

**Licenciatura em Engenharia Informática**

**Segurança 2020/2021**

****

**Configuração Avançada de um Equipamento**

Diogo Costa - 2018016581

Filipe Oliveira - 2018018618

Nuno Aparício - 2014014661

Índice

[Topologia 5](#_Toc73014223)

[Introdução 6](#_Toc73014224)

[Utilizadores 7](#_Toc73014225)

[Telnet & SSH 7](#_Toc73014226)

[Rotas 7](#_Toc73014227)

[AAA e Logging 7](#_Toc73014228)

[Configuração do Radius 7](#_Toc73014229)

[Configuração do Syslog 9](#_Toc73014230)

[Configurações básicas de segurança 9](#_Toc73014231)

[Banners 9](#_Toc73014232)

[Restrições nos inicios de sessão 10](#_Toc73014233)

[Privilégios de administração 10](#_Toc73014234)

[Utilizador Operador (oper) 11](#_Toc73014235)

[Utilizador Administrador (adm) 11](#_Toc73014236)

[Utilizador Gestor (manager) 11](#_Toc73014237)

[Configuração das Firewalls 11](#_Toc73014238)

[Anti-spoofing a partir da internet 11](#_Toc73014239)

[Anti-spoofing e RFC1918 para a internet 12](#_Toc73014240)

[Time-Based 12](#_Toc73014241)

[Reflexive 12](#_Toc73014242)

[CBAC 13](#_Toc73014243)

[Dynamic 14](#_Toc73014244)

[Zone-based 15](#_Toc73014245)

[Configuração do NAT 17](#_Toc73014246)

[Conclusão 18](#_Toc73014247)

Índice de Figuras

[Figura 1 Topologia 5](file:///C:\Users\nuno-\OneDrive\Documentos\GitHub\S-ISEC\relatorio_tpseguranca.docx#_Toc73014737)

[Figura 2 WinRadius 8](#_Toc73014738)

[Figura 3 Configuração AAA 8](#_Toc73014739)

[Figura 4 Configuração Radius 8](#_Toc73014740)

[Figura 5 Ambiente de Syslog 9](#_Toc73014741)

[Figura 6 configuração syslog 9](#_Toc73014742)

[Figura 7 Log de login 9](#_Toc73014743)

[Figura 8 Banner MOTD e Login 10](#_Toc73014744)

[Figura 9 Banner EXEC 10](#_Toc73014745)

[Figura 10 Bloqueio de tentativas 10](#_Toc73014746)

[Figura 11 Privilégios de Utilizador 10](#_Toc73014747)

[Figura 12 Configuração de privilégios 10](#_Toc73014748)

[Figura 13 Permissões do oper 11](#_Toc73014749)

[Figura 14 Permissões adm 11](#_Toc73014750)

[Figura 15 ACL Spoofing 11](#_Toc73014751)

[Figura 16 Anti-Spoofing e RFC1918 12](#_Toc73014752)

[Figura 17 Aplicação de time-range a uma ACL 12](#_Toc73014753)

[Figura 18 Configuração time-range 12](#_Toc73014754)

[Figura 19 Configuração da ACL Reflected 13](#_Toc73014755)

[Figura 20 ACL Reflected 13](#_Toc73014756)

[Figura 21 syslog e radius ACL 13](#_Toc73014757)

[Figura 22 Permissão ICMP com CBAC 13](#_Toc73014758)

[Figura 23 Atribuição CBAC na Interface 13](#_Toc73014759)

[Figura 24 Configuração Dynamic na ACL 14](#_Toc73014760)

[Figura 25 Utilizador myaccess 14](#_Toc73014761)

[Figura 26 ACL atribuída nas diferentes zonas 15](#_Toc73014762)

[Figura 27 Criação de zonas 15](#_Toc73014763)

[Figura 28 Atribuição das Zonas às Interfaces 15](#_Toc73014764)

[Figura 29 Criação das Classes e atribuição das ACL's 15](#_Toc73014765)

[Figura 30 Criação Policy-map e atribuição das classes 16](#_Toc73014766)

[Figura 31 Criação da Zone-Pair 16](#_Toc73014767)

[Figura 32 Atribuição de Outside e Inside nas Interfaces 17](#_Toc73014768)

[Figura 33 ACL de IP's Privados 17](#_Toc73014769)

[Figura 34 Configuração do NAT na Interface f0/0 17](#_Toc73014770)

Índice de Tabelas

[Tabela 1 Endereços 6](#_Toc73014721)

[Tabela 2 Utilizadores dos routers 7](#_Toc73014722)

[Tabela 3 Utilizadores de VPCS 7](#_Toc73014723)

# Topologia

Figura Topologia

# Introdução

Neste trabalho prático, o objetivo principal é conseguir estimular a aplicação prática dos conhecimentos adquiridos no âmbito das aulas de segurança, assim como promover a pesquisa de soluções técnicas que promovam as melhores práticas de segurança em redes.

Relativamente aos routers, foram apenas utilizados routers c7200 devido a ter problemas sendo todos os comandos do router *Externos* testados num router c2600 para verificar a sua compatibilidade. Seguem-se os IP’s de cada router.

|  |  |
| --- | --- |
| Externo1 | f0/0: 192.168.101.2 |
| Externos | f0/0: 193.136.2.2  f0/1: 192.168.101.1 |
| Docente1 | f0/0: 192.168.100.2 |
| Docentes | f0/0: 193.136.1.2  f0/1 :192.168.101.1 |
| WAN | e1/1: 193.136.2.1  e1/3:193.136.1.1  e1/0: 193.136.5.1  f0/0: 193.137.1.2 |
| ISP | f0/0: 193.137.2.1  f0/1: 193.137.1.1 |
| Malorie | f0/0: 193.137.2.2 |
| Core-Servicos | f0/0: 193.136.5.2  f0/1: 193.136.6.6 |
| DNS | f0/0: 193.136.6.2 |
| HTTP | f0/0: 193.136.6.3 |
| SSH | f0/0: 193.136.6.4 |
| DeepZone | f0/0: 193.136.6.5  f0/1: 192.168.200.254 |
| SoftLoopback | 192.168.200.2 |

Tabela Endereços

# Utilizadores

|  |  |
| --- | --- |
| Nome de Utilizador | Password |
| oper | operpwd |
| adm | admpwd |
| manager | manpwd |

Routers

Tabela Utilizadores dos routers

|  |  |
| --- | --- |
| Nome de Utilizador | Password |
| oper | operpwd |

Routers de VPCS

Tabela Utilizadores de VPCS

A password do Enable em todos os equipamentos é “myenapwd”.

# Telnet & SSH

Apenas dois routers possuem telnet nomeadamente o *Externos*, devido a este ser um router c2600 e não aceitar SSH, e o *WAN* pois foi necessário para a implementação da ACL Dynamic. Como o protocolo de aplicação telnet é pouco seguro decidimos aplicar nos restantes routers SSH e bloquear o telnet.

Ao reiniciar a topologia, a key de SSH não é guardada. Para que possa ser feito SSH aos equipamentos é necessário gerar a key nos equipamentos que o permitem com o seguinte comando:

**crypto key generate rsa general-keys modulus 1024**

# Rotas

O Router *WAN* tem rota default para sair para o router *ISP*.

*WAN* tem uma rota para a rede de *Docentes*, *Externos* e *Core-Servicos*.

*Core-Servicos* tem rotas para a *WAN*, rede abaixo (193.136.6.0/29) e rotas de saída para o *ISP*.

Relativamente ao Router *Deepzone* apenas tem rotas de saída.

# AAA e Logging

## Configuração do Radius

Para esta configuração resolvemos usar o Radius que é um protocolo que opera nas portas 1812 e 1813, que fornece a autenticação centralizada, a autorização e a gestão contabilística (AAA) para os utilizadores que se ligam e utilizam o serviço de rede. A sua principal função é autenticar utilizadores. Com a autenticação AAA, vai permitir que o Administrador da rede consiga configurar e acessar o dispositivo.

Usámos o Radius nos routers *Deepzone*, *Core-serviços*, *Wan*, *Externos* e *Docentes*. Sempre que exista uma autenticação realizada com sucesso ou falhada o Radius mostrará essa informação.

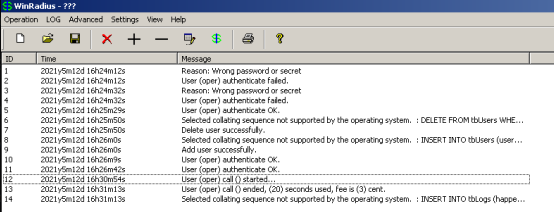


Figura WinRadius

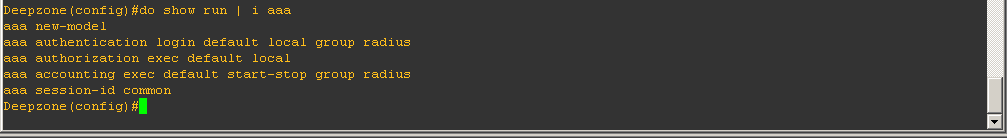


Figura Configuração AAA

A key utilizada para o servidor radius é “myradiuspwd”.



Figura Configuração Radius

## Configuração do Syslog

O Servidor de Syslog foi configurado no IP 192.168.200.2.

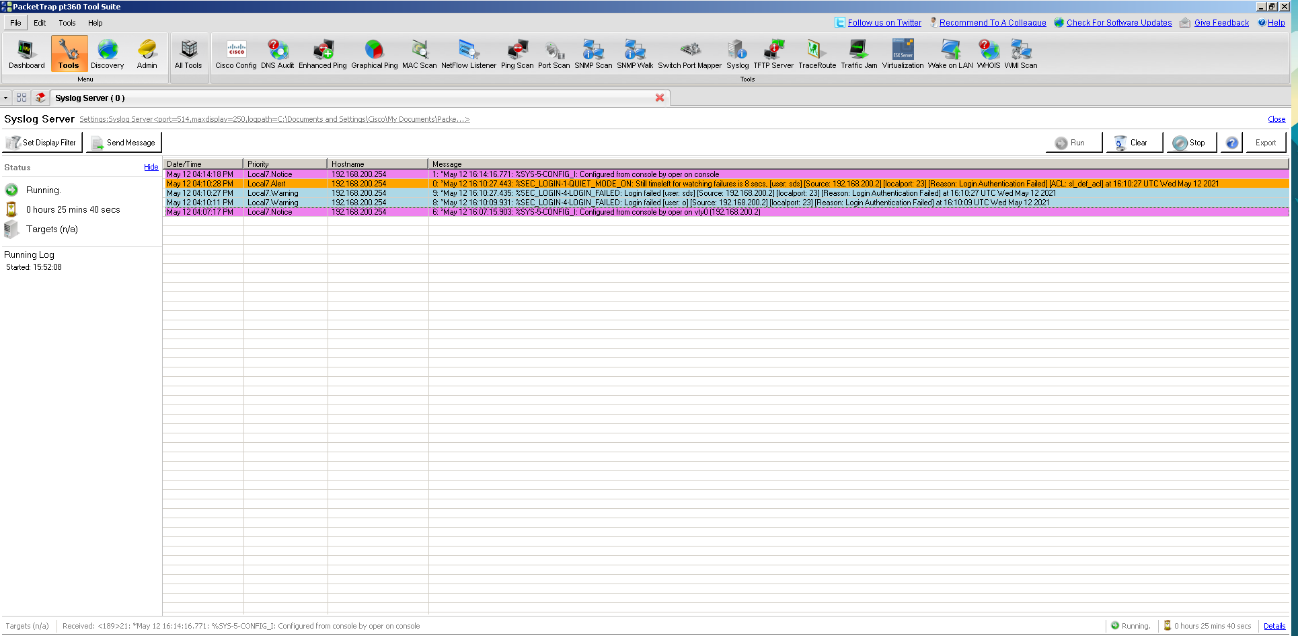


Figura Ambiente de Syslog

A configuração do Syslog foi realizada nos routers *Deepzone*, *Core-serviços*, *WAN*, *Externos* e *Docentes*. Foi ativado o log de sucesso e insucesso do login.



Figura configuração syslog



Figura Log de login

# Configurações básicas de segurança

## Banners

Sempre que for iniciado um router aparecerão dois banners no qual serão indicadas algumas informações básicas.

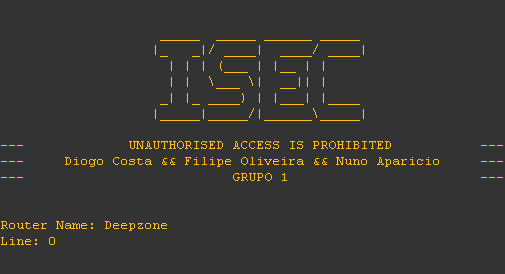


Figura Banner MOTD e Login

Seguidamente o utilizador terá de fazer login, em que posteriormente aparecerá os IPs que cada interface tem.

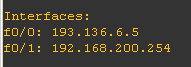


Figura Banner EXEC

## Restrições nos inicios de sessão

No caso de se enganar a iniciar sessão num router haverá um bloqueio de 10 minutos e prazo de 1 minuto no caso de falhar 3 tentativas de acesso.



Figura Bloqueio de tentativas

# Privilégios de administração



Figura Privilégios de Utilizador

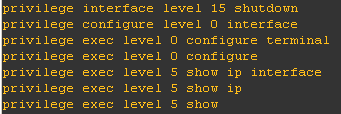


Figura Configuração de privilégios

No router *Externos* não foram realizadas as restrições pois o router c2600 não suporta vistas.

## Utilizador Operador (oper)

Este utilizador apenas pode aceder à interface de dentro e alterar a sua descrição. Devido a apenas ter essas permissões, deixámos a possibilidade de ser realizado um “show running-config”.

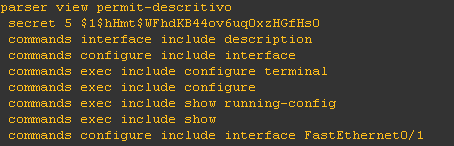


Figura Permissões do oper

## Utilizador Administrador (adm)

Este utilizador pode fazer as alterações que quiser nas interfaces sendo que apenas não pode ligar ou desligar as mesmas. O mesmo, pode também verificar as informações acerca das interfaces.

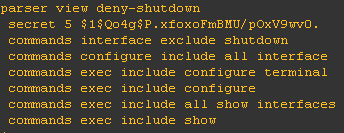


Figura Permissões adm

## Utilizador Gestor (manager)

Este utilizador como tem controlo total sobre o equipamento, foi apenas definido que tem o nível de privilégio 15.

# Configuração das Firewalls

## Anti-spoofing a partir da internet

Para impedir o spoofing vindo do exterior bloqueámos todos os dados vindos da rede Malorie (Restrição 30).

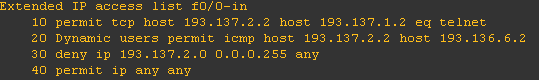


Figura ACL Spoofing

## Anti-spoofing e RFC1918 para a internet

Para resolver este problema criamos uma ACL standard em que negamos a passagem de dados de IPs Privados (RFC1918).

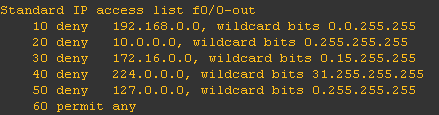


Figura 16 Anti-Spoofing e RFC1918

## Time-Based

Aplicámos a ACL Time-Based, para definir o período em que os utilizadores tenham a permissão de aceder à internet. Não sendo permitido qualquer ligação do exterior para estas redes.

O comando para configurar a ACL, baseada no tempo, é o time-range. Usado para especificar o período de tempo em que a declaração ACL é válida.

Nenhuma descrição disponível.

Figura Aplicação de time-range a uma ACL

Ao executar este comando, é colocado no modo de configuração da lista de acesso no qual especificamos um intervalo de tempo periódico em que é bloqueado o acesso das 0h00m às 23h59m ao fim de semana.

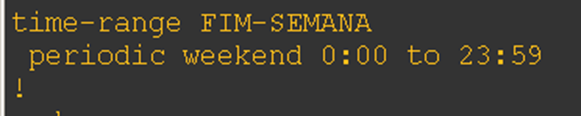


Figura Configuração time-range

A declaração da lista de acesso só será processada quando a hora do router se enquadrar dentro do período especificado.

## Reflexive

Ao utilizar a access-list reflexive, o router acompanhará as ligações de saída e permitirá automaticamente o tráfego de retorno.

Para começar criámos uma access-list que vai permitir o telnet apenas através do soft-loopback.

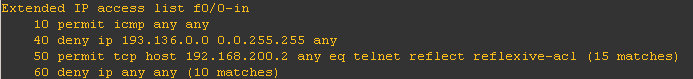


Figura Configuração da ACL Reflected

Depois de realizarmos um telnet à lista de acesso, esta irá criar a seguinte lista de acesso.



Figura ACL Reflected

Para permitir o tráfego de Radius & Syslog demos permissão apenas às portas de UDP 1812, 1813 e 514.

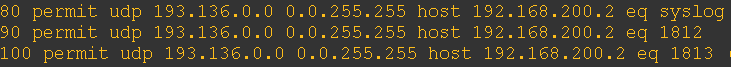


Figura syslog e radius ACL

## CBAC

O CBAC é capaz de verificar até a camada 7 do modelo OSI (Aplicação) e pode criar regras dinâmicas para permitir o tráfego de retorno. É semelhante à lista de acesso reflexive, mas uma das principais diferenças é que a ACL reflexive apenas verifica até à camada 4 (Transporte).

Primeiramente definimos os pacotes que queremos dar Inspect e assim permitir o ICMP com o CBAC.



Figura Permissão ICMP com CBAC

E por fim definimos a interface que queremos que o CBAC atue.

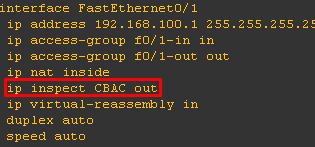


Figura Atribuição CBAC na Interface

O CBAC teve de ser usado na rede Docentes devido aos routers c2600 não o permitirem.

## Dynamic

Para permitir que o *Malorie* consiga pingar o servidor DNS foi criado uma access-list dynamic para que, ao fazer telnet e entrar com as credenciais do myaccess o mesmo irá perder conexão e ativar o ICMP do *Malorie* para o DNS. Esta ligação de ICMP dura apenas 2 minutos.

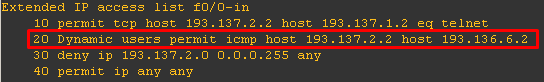


Figura Configuração Dynamic na ACL

Foi criado o utilizador myaccess com o comando “autocommand” para que este ative a dynamic.



Figura Utilizador myaccess

Por aconselhamento do professor a ZBF deve ser aplicada no router *core-serviços*. Por consequência a ZBF não é compatível com a extended na mesma interface e como tal decidimos criar a dynamic na *WAN* permitindo assim o ping para o DNS a partir do *Malorie*.

## Zone-based

Na firewall Zone-Based a ideia é não atribuir listas de acesso a interfaces, mas criar diferentes zonas. Nas interfaces serão atribuídas as diferentes zonas e as políticas de segurança serão atribuídas ao tráfego entre as mesmas.

Primeiramente foi criada uma access-list extended numerada que será aplicada nas zonas criadas.

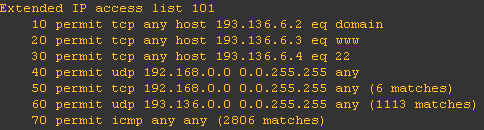


Figura ACL atribuída nas diferentes zonas

De seguida foram criadas 2 zonas.

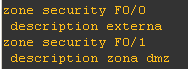


Figura Criação de zonas

O próximo passo foi atribuir as zonas às interfaces adequadas.

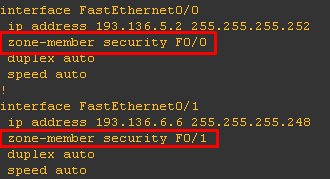


Figura Atribuição das Zonas às Interfaces

De seguida criámos as classes e atribuímos as respetivas access-lists a cada uma das classes.

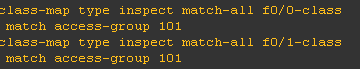


Figura Criação das Classes e atribuição das ACL's

Depois criámos a policy-map e demos permissão para o “inspect” de cada uma das classes

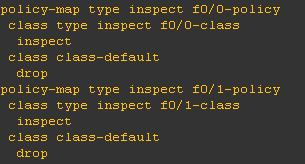


Figura Criação Policy-map e atribuição das classes

Por fim definimos a nossa “zone-pair” atribuindo as zonas de source e destination. Demos também permissão à policy criada anteriormente.

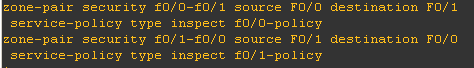


Figura Criação da Zone-Pair

## Configuração do NAT

Ao configurar o NAT permitimos às redes privadas que utilizam endereços IP não registados se conectem à Internet. O NAT opera nos Routers *Externos* e *Docentes*, e traduz os endereços privados na rede interna em endereços legais, antes de os pacotes serem encaminhados para outra rede.

Por exemplo, a rede *Externos* (192.168.101.0/30) envia um pacote para a rede externa. Sem a configuração do NAT este pacote sairia com o IP privado. Ao aplicar o NAT no router *Externos* definimos que todos os pacotes que saiam da rede 192.168.101.0 saiam com o IP público. Este IP está presente na interface f0/0 do router *Externos*. O mesmo se aplica para a rede *Docentes*.

1º Define-se quais as interfaces de saída e de entrada.

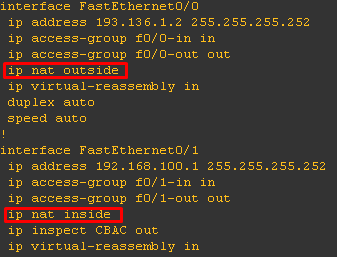


Figura Atribuição de Outside e Inside nas Interfaces

2º Em seguida, configurámos uma ACL que inclui uma lista dos endereços de origem internos que serão traduzidos.



Figura ACL de IP's Privados

3º Por fim, ativamos o NAT.



Figura Configuração do NAT na Interface f0/0

# Conclusão

Baseado no que acabámos por realizar neste trabalho prático, uma pessoa com conhecimentos básicos de GNS3 e CISCO, conseguirá através deste relatório espelhar na sua imagem Windows XP exatamente os mesmos procedimentos que nós utilizámos e assim entender mais acerca de serviços de segurança com aplicação de firewalls, logging, autenticação, autorização bem como a configuração do NAT.