UNIVERSIDADE da MADEIRA

CTeSP CURSOS TÉCNICOS SUPERIORES PROFISSIONAIS

TRABALHO

TÍTULO DO TRABALHO

Joel Alexandre Fernandes Figueira
Nº 2014818

CTeSP Tecnologias e Programação de Sistemas de Informação

UNIDADE CURRICULAR:
Segurança Informática

DOCENTE:
Filipe Freitas

DATA:
07 de 01 de 2020

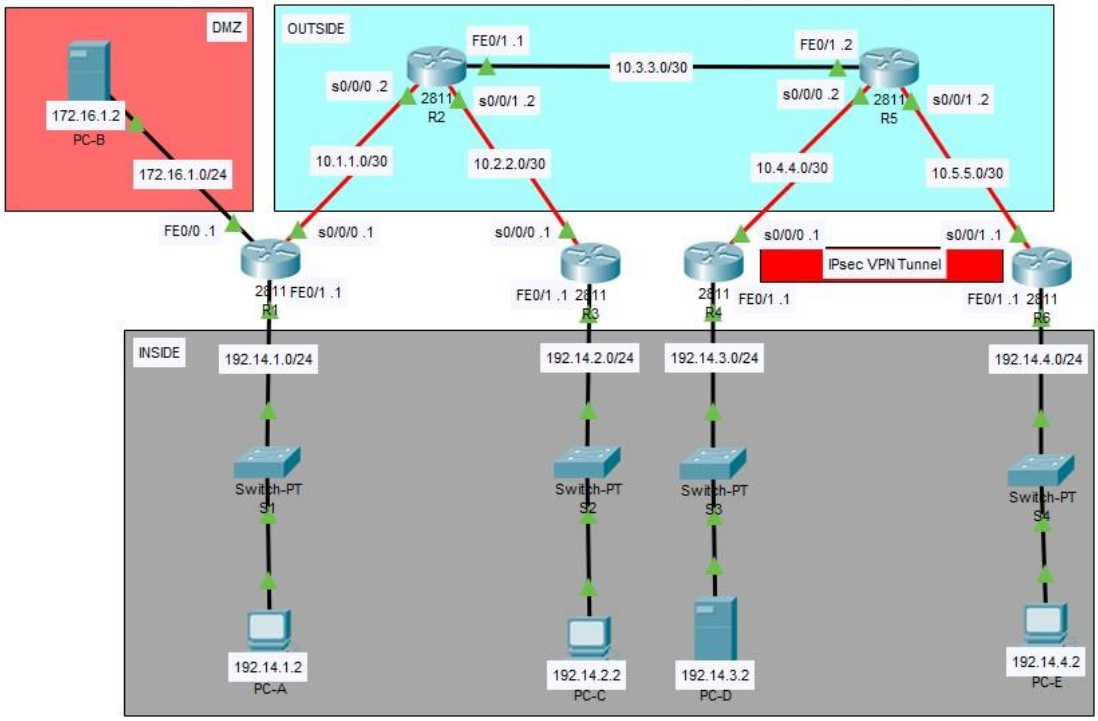
ESCOLA SUPERIOR DE TECNOLOGIAS E GESTÃO

Cofinanciado por:

MADEIRA 14-20 — REGIÃO AUTÓNOMA DA MADEIRA — PORTUGAL 2020 — UNIÃO EUROPEIA Fundo Social Europeu

índice

Diagrama de Topologia



Endereçamento

Inside Zone

	IP Address: 192.14.0.0		**Subnet Mask:** /24 255.255.255.0		
#	**Subnet**	**Gateway**	**First Host**	**Last Host**	**Broadcast**
1	192.14.1.0 /24	192.14.1.1	192.14.1.2	192.14.1.254	192.14.1.255
2	192.14.2.0 /24	192.14.2.1	192.14.2.2	192.14.2.254	192.14.2.255
3	192.14.3.0 /24	192.14.3.1	192.14.3.2	192.14.3.254	192.14.3.255
4	192.14.4.0 /24	192.14.4.1	192.14.4.2	192.14.4.254	192.14.4.255

Demilitarized Zone (DMZ)

	IP Address: 172.16.0.0		**Subnet Mask:** /24 255.255.255.0		
#	**Subnet**	**Gateway**	**First Host**	**Last Host**	**Broadcast**
1	172.16.1.0 /24	172.16.1.1	172.16.1.2	172.16.1.254	172.16.1.255

Outside Zone

	IP Address: 10.0.0.0		**Subnet Mask:** /30 255.255.255.252	
#	**Subnet**	**First Host**	**Last Host**	**Broadcast**
1	10.1.1.0 /30	10.1.1.1	10.1.1.2	10.1.1.3
2	10.2.2.0 /30	10.2.2.1	10.2.2.2	10.2.2.3
3	10.3.3.0 /30	10.3.3.1	10.3.3.2	10.3.3.3
4	10.4.4.0 /30	10.4.4.1	10.4.4.2	10.4.4.3
5	10.5.5.0 /30	10.5.5.1	10.5.5.2	10.5.5.3

Routers & Switches (Global Config.)

Configurações aplicadas em todos os Routers e Switches.

Credenciais

Enable secret	*cisco12345*
Enable password	*ciscopa12345*

Lista de Utilizadores Locais

#	Username	Privilege	Password
1	admin	15	*cisco12345*

Observação Sobre o Acesso Remoto SSH

O acesso remoto por SSH foi restrito apenas para o PC-A pode conectar em todos os routers através de SSH.

Servidor RADIUS

O Servidor RADIUS foi aplicado no PC-D e também foi criado um utilizador.

RADIUS Users

#	Username	Password
1	RadAdmin	*RadAdminpa55*

Model Authentication Authorization Accounting (AAA)

Modelo (AAA) foi aplicado aos Routers R1 e R2. Quando o servidor RADIUS estiver offline ou se acontecer algo entre a conexão com servidor, o router irá acabar por exceder o número máximo de tentativas para se conectar ao servidor e como backup o utilizador pode utilizar o user local (user local). Caso o router conseguir conectar-se ao servidor RADIUS, o utilizador apenas deve utilizar os users que estão guardados no servidor RADIUS (radius users).

#	Client Name	Client IP	Server Type	Key
1	R1	172.16.1.1	RADIUS	*cisco12345*
2	R3	10.2.2.1	RADIUS	*cisco12345*

IPsec VPN Tunnel

Foi implementado uma IPsec VPN entre os routers R4 e R6, para encriptar p tráfico entre a LAN (192.14.3.2) e a LAN (192.14.4.2), com os seguintes parâmetros.

	R4	**R6**
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authrntication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	10.5.5.1	10.4.4.1
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp
ISAKMP Key	vpnpa55	vpnpa55

Zone Base Firewall

ZBF aplicada no router R1, consiste em 3 zonas: INSIDE, DMZ e INTERNET. Entre a zona INSIDE para a zona INTERNET é permitido os protocolos TCP, UDP e ICMP. Entre a zona DMZ e INTERNET é permitido os protocolos DNS, HTTP e HTTPS.

IOS Intrusion Prevention System (IPS)

IPS aplicada no router R2 na interface FE0/1 para tráfico outbound. SYSLOG host configurado para o PC-D.