UNIVERSIDADE da MADEIRA

CTeSP CURSOS TÉCNICOS SUPERIORES PROFISSIONAIS

TRABALHO

RELATÓRIO DO TRABALHO DE SISTEMAS GESTORES DE BASES DE DADOS

Miguel Arcanjo Gouveia da Silva

Nº 2025121

Curso Técnico Superior em Tecnologias e Programação de Sistemas de Informação

UNIDADE CURRICULAR:

Segurança Informática

DOCENTE:

Milton Aguiar

DATA:

15/01/2023

ESCOLA SUPERIOR DE TECNOLOGIAS E GESTÃO

Memória descritiva

Etapa 1 :

Mudar o nome do Router :

- enable

-configure terminal

- hostname Router1

Etapa 2:

- enable

- configure terminal

- banner motd % Router do Arcanjo 1%

Colocar password no modo previligiado:

- enable secret cisco

(depois passou a cisco12345)

Colocar password à ligação por consola

- line console 0

password cisco

login

Colocar a senha da linha virtual

line vty 04

password cisco

login

(depois com o passo de colocar senha minimo 10 caracteres a password é cisco12345)

Etapa 3:

PC0 - 192.31.1.1/24

PC1 - 172.16.1.1 /24

PC2 - 192.31.2.1/24

PC3 - 192.31.3.1/24

PC4 - 192.31.4.1/24

PC5 - 192.31.5.1/24

Etapa 4:

configuração interface do Router1

R1: enable

R1: configure terminal

R1: interface fa 0/0

R1: ip address 192.31.1.2 255.255.255.0

R1: no shutdown

R1: end

R1: interface serial 0/0/0

R1: ip address 10.1.1.1 255.255.255.252

R1: no shutdown

R1: end

Configuração interface do Router2

R2: enable

R2: configure terminal

R2: interface fa 0/0

R2: ip address 192.31.2.2 255.255.255.0

R2: no shutdown

R2: end

R2: interface serial 0/0/1

R2: ip address 10.2.2.1 255.255.255.252

Configuração interface do Router3

R3: enable

R3: configure terminal

R3: interface fa 0/0

R3: ip address 192.31.3.2 255.255.255.0

R3: no shutdown

R3: end

R3: interface serial 0/0/0

R3: ip address 10.4.4.2 255.255.255.252

Configuração interface do Router4

R4: enable
R4: configure terminal
R4: interface fa 0/0

R4: ip address 192.31.4.2 255.255.255.0

R4: interface serial 0/0/1

R4: ip address 10.5.5.1 255.255.255.252

Configuração interface do Router5

R5: enable
R5: configure terminal
R5: interface gig 0/0

R5: ip address 10.6.6.2 255.255.255.252

R5: interface gig 0/1

R5: ip address 192.31.5.2 255.255.255.0

R5: interface gig 0/2

R5: ip address 172.16.1.2 255.255.255.0

Configuração interface do Router6

R6: interface serial 0/0/0
R6: ip address 10.4.4.1 255.255.255.252

R6: interface serial 0/0/1
R6: ip address 10.5.5.2 255.255.255.252

R6: interface fa 0/0
R6: ip address 10.3.3.1 255.255.255.252

Configuração interface do Router7

R7: enable
R7: configure terminal

R7: interface serial 0/0/0
R7: ip address 10.1.1.2 255.255.255.252

R7: interface fa 0/1
R7: ip address 10.6.6.1 255.255.255.252

R7: interface fa 0/0
R7: ip address 10.3.3.2 255.255.255.252

R7: interface serial 0/0/1
R7: ip address 10.2.2.2 255.255.252

router 1

R1: ip route 0.0.0.0 0.0.0.0 s0/0/0

R1: ip route 10.3.3.0 255.255.255.252 s0/0/0

router2

R2: ip route 0.0.0.0 0.0.0.0 s0/0/1

R2: ip route 10.3.3.0 255.255.255.252 s0/0/1

router3

R3: ip route 0.0.0.0 0.0.0.0 s0/0/0
R3: ip route 10.3.3.0 255.255.255.252 s0/0/0

router4
R4: ip route 0.0.0.0 0.0.0.0 s0/0/1
R4: ip route 10.3.3.0 255.255.255.252 s0/0/1

router 5
R5: ip route 0.0.0.0 0.0.0.0 g0/0

router6

R6: ip route 192.31.1.0 255.255.255.0 10.1.1.1
R6: ip route 192.31.2.0 255.255.255.0 10.2.2.1
R6: ip route 192.31.3.0 255.255.255.0 10.4.4.2
R6: ip route 192.31.4.0 255.255.255.0 10.5.5.1
R6: ip route 192.31.5.0 255.255.255.0 10.6.6.2
R6: ip route 172.16.1.0 255.255.255.0 10.6.6.2
R6: ip route 0.0.0.0 0.0.0.0 10.3.3.2

router 7

R7: ip route 192.31.5.0 255.255.255.0 10.6.6.2
R7: ip route 172.16.1.0 255.255.255.0 10.6.6.2
R7: ip route 192.31.1.0 255.255.255.0 10.1.1.1
R7: ip route 192.31.2.0 255.255.255.0 10.2.2.1
R7: ip route 192.31.3.0 255.255.255.0 10.4.4.2
R7: ip route 192.31.4.0 255.255.255.0 10.5.5.1

R7: ip route 0.0.0.0 0.0.0.0 10.3.3.1
R7: ip route 10.3.3.0 255.255.255.252 g/0/0

Etapa 5:

service password-encryption

security passwords min-length 10

login block-for 120 attempts 3 within 60

Etapa 6:

enable

configure terminal

enable secrect cisco12345

Etapa 7:

username Admin privilege 15 secret cisco123456

username arcanjo privilege 15 secret cisco123456

line console 0

login local

exit

line vty 0 4

privilege level 15

login local

transport input ssh

exit

ip domain name span.com

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

exit

Etapa 8:

Ip address 192.31.1.2

Username : Admin

Configurar time outs e paramentos do ssh

ip ssh time-out 90

ip ssh authentication-retries 2

ip access-list standard TASK-5

permit 192.31.1.1 0.0.0.0

deny 192.31.2.1 0.0.0.0

deny 192.31.3.1 0.0.0.0

deny 192.31.4.1 0.0.0.0

deny 192.31.5.1 0.0.0.0

deny 172.16.1.1 0.0.0.0

line vty 0 4

login local

transport input ssh

access-class TASK-5 in

end

Etapa 9:

aaa new-model

aaa authentication login default group radius local

exit

configure terminal

aaa new-model

aaa authentication login default group radius local

radius-server host 192.31.1.1 auth-port 1645 key cisco

username RadAdmin password RadAdminpa55

end

Etapa 10:

Configuração do Radius no roteador r3:

R3: aaa new-model

R3: aaa authentication login default group radius local

R3: exit

R3: configure terminal

R3: aaa new-model

R3: aaa authentication login default group radius local

R3: radius-server host 192.31.3.1 auth-port 1645 key cisco

R3: username Router3 password Router12345

R3: end

Ir ao server ->services->aaa-> on e criar

cliente Name - Router3 cliente ip -> 192.31.1.2

secret cisco3

criar os utilizadores ->

Username- Router3 pass: cisco

Etapa 11:

1-

acess-list standard STND-1

deny 10.1.1.0 0.0.03

deny 10.4.4.0 0.0.0.3

permit any

ip access-group STND-1 out

2-

R3: access-list 100 permit tcp any any eq 80

R3: access-list 100 permit tcp any any eq 443

R3: access-list 100 permit tcp any any eq 53

R3: acess-list 100 deny ip any any

R3: interface serial s0/0/0

R3: ip access-group 100 in

3-

R3: acess-list standard STND-2

R3: permit tcp host 10.3.3.0 host 10.3.3.0 eq 21

R3: interface serial 0/0/0

R3: ip access-group STND-2 out

ETAPA 14

R3(config)#crypto isakmp enable

R3(config)#crypto isakmp policy 10

R3(config-isakmp)#hash sha

R3(config-isakmp)#authentication pre-share

R3(config-isakmp)#group 5

R3(config-isakmp)#lifetime 3600

R3(config-isakmp)#encryption aes 256

R3(config-isakmp)#end

R3(config)#crypto isakmp key cisco123 address 10.5.5.1
R3(config)#crypto ipsec transform-set R3-R4 esp-aes 256 esp-sha-hmac

R3(config)#crypto ipsec security-association lifetime seconds 1800
R3(config)#access-list 101 permit ip 192.31.3.0 0.0.0.255 192.31.4.0 0.0.0.255

R3(config)# crypto map CMAP 10 ipsec-isakmp

R3(config-crypto-map)# match address 101

R3(config-crypto-map)# set peer 10.5.5.1

R3(config-crypto-map)# set pfs group5

R3(config-crypto-map)# set transform-set R3-R4

R3(config-crypto-map)# set security-association lifetime seconds 900 R3(config-crypto-map)# exit

R3(config)#interface s0/0/0

R3(config-if)#crypto map CMAP

R3(config-if)#end R4(config)#crypto isakmp enable

R4(config)#crypto isakmp policy 10

R4(config-isakmp)#hash sha

R4(config-isakmp)#authentication pre-share

R4(config-isakmp)#group 5

R4(config-isakmp)#lifetime 3600

R4(config-isakmp)#encryption aes 256

R4(config-isakmp)#end

R4(config)#crypto isakmp key cisco123 address 10.4.4.2

R4(config)#crypto ipsec transform-set R3-R4 esp-aes 256 esp-sha-hmac
R4(config)#crypto ipsec security-association lifetime seconds 1800
R4(config)#access-list 101 permit ip 192.31.4.0 0.0.0.255 192.31.3.0 0.0.0.255

R4(config)#crypto map CMAP 10 ipsec-isakmp

R4(config-crypto-map)#match address 101

R4(config-crypto-map)#set peer 10.4.4.2

R4(config-crypto-map)#set pfs group5

R4(config-crypto-map)#set transform-set R3-R4

R4(config-crypto-map)#set security-association lifetime seconds 900
R4(config-crypto-map)#exit

R4(config)#interface s0/0/1

R4(config-if)#crypto map CMAP

R4(config-if)#end