Equipo	Usuario	Contraseña	Contraseña Modo privilegiado
R1	AdminR1	RouR1passR1	RouR1passen
R2	AdminR2	Rou2R2passR2	RouR2passen
R3	AdminR3	RouR3passR3	RouR3passen
S1	AdminS1	SwitS1passS1	SwitS1passen
S2	AdminS2	SwitS2passS2	SwitS2passen
S3	AdminS3	SwitS3passS3	SwitS3passen
ASA	AdminASA	ASApassA	

Dispositivo	Interfaz	Dirección	Máscara	Gateway por defecto
R1	Se0/1/0	10.10.11.1	255.255.255.252	N/A
	Gi0/0	172.20.11.1	255.255.255.0	N/A
	Gi0/1	209.165.200.233	255.255.255.248	N/A
R2	Se0/1/0	10.10.11.2	255.255.255.252	N/A
	Se0/1/1	10.20.11.2	255.255.255.252	N/A
R3	Se 0/1/0	10.20.11.1	255.255.255.252	N/A
	Gi 0/0	172.30.11.1	255.255.255.0	N/A
PC-A	FA0	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	FA0	192.168.10.5	255.255.255.0	192.168.10.1
PC-C	FA0	172.30.11.2	255.255.255.0	172.30.11.1
PC-D	FA0	172.20.11.2	255.255.255.0	172.20.11.1

En el router R1

Router ospf 1

Network 172.20.11.0 0.0.0.255 area 0

Network 10.10.11.0 0.0.0.3 area 0

Network 209.165.200.232 0.0.0.7 area 0

Security password min-length 10

Enable secret SwitR1passen

Username AdminR1 secret RouR1passR1

Login local

Exec-timeout 5 0

Ip domain-name examen.com

Line vty 0 4

Privilege level 15

Login block-for 180 attemps 3 within 180

Aaa new-model

aaa authentication login default local

crypto key rsa general-keys modulus 1024

ip ssh versión 2

license boot module c1900 technology-package securityk9

crypto isakmp enable

crypto isakmp policy 10

authentication pre-share

group 5

lifetime 3600

encryption aes 256

crypto isakmp key ciscovpnpa55 address 10.20.11.1

crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac

crypto ipsec security-association lifetime seconds 3600

access-list 100 permit ip 172.20.11.0 0.0.0.255 172.30.11.0 0.0.0.255

crypto map CMAP 10 ipsec-isakmp

match address 100

set peer 10.20.11.1

set pfs group5

set transform-set VPN-SET

set security-association lifetime seconds 3600

int se0/1/0

crypto CMAP

En Router 2

Router ospf 1

Network 172.30.11.0 0.0.0.255 area 0

Network 10.20.11.0 0.0.0.3 area 0

Security password min-length 10

Enable secret SwitR2passen

Username AdminR2 secret RouR2passR2

Login local

Exec-timeout 5 0

Ip domain-name examen.com

Line vty 0 4

Privilege level 15

Login block-for 180 attemps 3 within 180

Aaa new-model

aaa authentication login default local

crypto key rsa general-keys modulus 1024

ip ssh versión 2

license boot module c1900 technology-package securityk9

En el router 3

Router ospf 1

Network 172.20.11.0 0.0.0.255 area 0

Network 10.10.11.0 0.0.0.3 area 0

Network 209.165.200.232 0.0.0.7 area 0

Security password min-length 10

Enable secret SwitR1passen

Username AdminR1 secret RouR1passR1

Login local

Exec-timeout 5 0

Ip domain-name examen.com

Line vty 0 4

Privilege level 15

Login block-for 180 attemps 3 within 180

Aaa new-model

aaa authentication login default local

crypto key rsa general-keys modulus 1024

ip ssh versión 2

license boot module c1900 technology-package securityk9

Router 3

Router ospf 1

Network 172.30.11.0 0.0.0.255 area 0

Network 10.20.11.0 0.0.0.3 area 0

Security password min-length 10

Enable secret SwitR3passen

Username AdminR3 secret RouR3passR3

Login local

Exec-timeout 5 0

Ip domain-name examen.com

Line vty 0 4

Privilege level 15

Login block-for 180 attemps 3 within 180

Aaa new-model

aaa authentication login default local

crypto key rsa general-keys modulus 1024

ip ssh versión 2

license boot module c1900 technology-package securityk9

crypto isakmp enable

crypto isakmp policy 10

hash sha

authentication pre-share

lifetime 3600

group 5

encryption aes 256

crypto isakmp key ciscovpnpa55 address 10.10.11.1

crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac

crypto ipsec security-association lifetime seconds 3600

access-list 100 permit ip 172.30.11.0 0.0.0.255 172.20.11.0 0.0.0.255

crypto map CMAP 10 ipsec-isakmp

 set pfs group5

set transform-set VPN-SET

set security-association lifetime seconds 3600

exit

En el Switch 1

Security password min-length 10

Enable secret SwitS1passen

Username AdminS1 secret SwitS1passS1

Login local

Exec-timeout 5 0

Ip domain-name examen.com

Line vty 0 4

Privilege level 15

Login block-for 180 attemps 3 within 180

Vlan 99

Name vlan-Nativa

Int fa0/1

Switchport mode trunk

Switchport trunk native vlan 99

No shut

Switchport nonegotiate

Int range 0/3-24

Shutdown

Int fa0/6

Spanning-tree portfast deafult

switchport port-security mac-address sticky

En el Switch 2

Security password min-length 10

Enable secret SwitS2passen

Username AdminS2 secret SwitS2passS2

Login local

Exec-timeout 5 0

Ip domain-name examen.com

Line vty 0 4

Privilege level 15

Login block-for 180 attemps 3 within 180

Vlan 99

Name vlan-Nativa

Int fa0/2

Switchport mode trunk

Switchport trunk native vlan 99

No shut

Switchport nonegotiate

En el ASA

Hostname ASA

Interface vlan 1

Nameif inside

Ip address 192.168.10.0 255.255.255.0

Security-level 100

No shut

Exit

Interface vlan 2

Nameif outside

Ip address 209.165.200.232 255.255.255.248

Security-level 0

No shut

Exit

Interface et0/1

Switchport Access vlan 1

No shut

Exit

Et0/0

Switchport Access vlan 2

No shut

route outside 0.0.0.0 0.0.0.0 209.165.200.233

object network inside-net

subnet 192.168.10.0 255.255.255.0

nat (inside, outside) dynamic interface

end

class-map inspection-default

match default-inspection-traffic

exit

policy-map global-policy

class inspection-default

inspect icmp

exit

service-policy global-policy global

dhcp address 192.168.10.2-192.168.10.20 inside

dhcp enable inside

username AdminASA password ASApassA

aaa authentication ssh console local

crypto key generate rsa modulus 1024

ssh 192.168.10.0 255.255.255.0 inside

ssh 172.30.11.0 255.255.255.0 outside

interface vlan 3

ip address 172.20.11.0 255.255.255.0

no forward interface vlan 1

nameif dmz

security-level 70

no shut