Blue Team Final Project

🡪R1

enable

config terminal

hostname R1

no ip domain lookup

security passwords min-length 8

enable secret cisco123

line console 0

password cisco123

login

aaa authentication login CONSOLE local

line console 0

login authentication CONSOLE

exit

ip domain-name Router1

crypto key generate rsa

!!!!!!!!How many bits in the modulus [512]: 1024

username mahmoud privilege 15 secret mahmoud

line vty 0 4

login local

transport input ssh

exit

service password-encryption

banner motd $ Authorized Users Only! $

int s0/1/0

ip add 10.10.10.177 255.255.255.252

no sh

int s0/1/1

ip add 10.10.10.185 255.255.255.252

no sh

int g0/0/1

ip add 10.10.10.181 255.255.255.252

no sh

interface g0/0/0

no shutdown

exit

interface g0/0/0.10

encapsulation dot1Q 10

ip address 10.10.10.1 255.255.255.240

interface g0/0/0.20

encapsulation dot1Q 20

ip address 10.10.10.17 255.255.255.240

interface g0/0/0.99

encapsulation dot1Q 99

ip address 10.10.10.33 255.255.255.240

* **OSPF**

router ospf 10

network 10.10.10.0 0.0.0.15 area 0

network 10.10.10.16 0.0.0.15 area 0

network 10.10.10.32 0.0.0.15 area 0

network 10.10.10.176 0.0.0.3 area 0

network 10.10.10.184 0.0.0.3 area 0

network 10.10.10.180 0.0.0.3 area 0

* **OSPF authentication (MD5)**

Interface s0/1/0

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

Interface s0/1/1

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

* **IPV6**

ipv6 unicast-routing

interface s0/1/1

ipv6 address 2000:1:2:1::2/64

no shutdown

exit

ipv6 route 2000:1:2:3::/64 s0/1/1

ipv6 route 2000:1:2:4::/64 s0/1/1

ipv6 route 2000:1:2:2::/64 s0/1/1

**🡪DHCP**

ip dhcp excluded-address 10.10.10.1

ip dhcp excluded-address 10.10.10.17

ip dhcp pool VLAN10

network 10.10.10.0 255.255.255.240

default-router 10.10.10.1

ip dhcp pool VLAN20

network 10.10.10.16 255.255.255.240

default-router 10.10.10.17

**🡪vpn**

1. **Define the interesting traffic**

access-list 110 permit ip 10.10.10.0 0.0.0.15 10.10.10.64 0.0.0.15

access-list 110 permit ip 10.10.10.16 0.0.0.15 10.10.10.64 0.0.0.15

access-list 110 permit ip 10.10.10.32 0.0.0.15 10.10.10.64 0.0.0.15

access-list 110 permit ip 10.10.10.0 0.0.0.15 10.10.10.80 0.0.0.15

access-list 110 permit ip 10.10.10.16 0.0.0.15 10.10.10.80 0.0.0.15

access-list 110 permit ip 10.10.10.32 0.0.0.15 10.10.10.80 0.0.0.15

2) Phase 1 (ISAKMP Policy)

crypto isakmp policy 10

encr aes 256

hash sha

authentication pre-share

group 5

lifetime 3600

3) Pre-Shared Key

crypto isakmp key cisco12345 address 10.10.10.190

! 4) Phase 2 (IPSec Transform-set)

crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac

5) Crypto Map

crypto map CMAP 10 ipsec-isakmp

set peer 10.10.10.190

set transform-set TS

match address 110

set pfs group5

set security-association lifetime seconds 3600

6) Apply Crypto Map on the outside interface

interface S0/1/0

crypto map CMAP

🡪R2

enable

config terminal

hostname R2

no ip domain lookup

enable secret cisco

line console 0

password cisco

login

ip domain-name Router2

crypto key generate rsa

!!!!!!!!How many bits in the modulus [512]: 1024

username mahmoud privilege 15 secret mahmoud

line vty 0 4

login local

transport input ssh

exit

service password-encryption

banner motd $ Authorized Users Only! $

int s0/1/0

ip add 10.10.10.178 255.255.255.252

no sh

int s0/1/1

ip add 10.10.10.189 255.255.255.252

no sh

int g0/0/0

ip address 10.10.10.49 255.255.255.240

no sh

int g0/0/1

ip add 10.10.10.193 255.255.255.252

no sh

* **Loopback int**

interface loopback 0

ip address 10.10.10.201 255.255.255.252

no shutdown

* **OSPF**

router ospf 10

network 10.10.10.48 0.0.0.15 area 0

network 10.10.10.176 0.0.0.3 area 0

network 10.10.10.188 0.0.0.3 area 0

network 10.10.10.192 0.0.0.3 area 0

* **OSPF authentication (MD5)**

Interface s0/1/0

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

Interface s0/1/1

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

Interface g0/0/1

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

**🡪NTP**

ntp authenticate

ntp trusted-key 1

ntp authentication-key 1 md5 cisco123

ntp server 10.10.10.50 key 1

end

show ntp associations

show ntp status

show clock

**🡪SYSLOG**

service timestamps log datetime msec

logging 10.10.10.50

logging trap debugging

**🡪 server based aaa authentication**

aaa new-model

radius server radius1

address ipv4 10.10.10.60 auth-port 1645

key mahmoud 123

exit

aaa authentication login default group radius local

line console 0

login authentication default

🡪R3

enable

config terminal

hostname R3

no ip domain lookup

enable secret cisco

line console 0

password cisco

login

ip domain-name Router3

crypto key generate rsa

!!!!!!!!How many bits in the modulus [512]: 1024

username mahmoud privilege 15 secret mahmoud

line vty 0 4

login local

transport input ssh

exit

service password-encryption

banner motd $ Authorized Users Only! $

int s0/1/0

ip add 10.10.10.190 255.255.255.252

no sh

int s0/1/1

ip add 10.10.10.197 255.255.255.252

no sh

int g0/0/0

ip address 10.10.10.81 255.255.255.240

no sh

int g0/0/1

ip add 10.10.10.65 255.255.255.240

no sh

ip dhcp excluded-address 10.10.10.65

ip dhcp pool VLAN1

network 10.10.10.64 255.255.255.240

default-router 10.10.10.65

**🡪OSPF**

router ospf 10

network 10.10.10.64 0.0.0.15 area 0

network 10.10.10.80 0.0.0.15 area 0

network 10.10.10.188 0.0.0.3 area 0

network 10.10.10.196 0.0.0.3 area 0

* **OSPF authentication (MD5)**

Interface s0/1/0

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

Interface s0/1/1

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

* **IPV6**

ipv6 unicast-routing

interface s0/1/1

ipv6 address 2000:1:2:2::2/64

no shutdown

exit

ipv6 route 2000:1:2:3::/64 s0/1/1

ipv6 route 2000:1:2:4::/64 s0/1/1

ipv6 route 2000:1:2:1::/64 s0/1/1

**🡪VPN**

**1)define the interesting traffic**

access-list 110 permit ip 10.10.10.64 0.0.0.15 10.10.10.0 0.0.0.15

access-list 110 permit ip 10.10.10.64 0.0.0.15 10.10.10.16 0.0.0.15

access-list 110 permit ip 10.10.10.64 0.0.0.15 10.10.10.32 0.0.0.15

access-list 110 permit ip 10.10.10.80 0.0.0.15 10.10.10.0 0.0.0.15

access-list 110 permit ip 10.10.10.80 0.0.0.15 10.10.10.16 0.0.0.15

access-list 110 permit ip 10.10.10.80 0.0.0.15 10.10.10.32 0.0.0.15

**2) Phase 1 (ISAKMP Policy)**

crypto isakmp policy 10

encr aes 256

hash sha

authentication pre-share

group 5

lifetime 3600

exit

**3) Pre-Shared Key**

crypto isakmp key cisco12345 address 10.10.10.177

**4)Phase 2 (IPSec Transform-set)**

crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac

**5) Crypto Map**

crypto map CMAP 10 ipsec-isakmp

set peer 10.10.10.177

set transform-set TS

match address 110

set pfs group5

set security-association lifetime seconds 3600

**6) Apply Crypto Map on the outside interface**

interface S0/1/0

crypto map CMAP

**🡪ZPF**

zone security public

exit

zone security private

ex

zone security dmz

exit

interface s0/1/0

zone-member security public

exit

interface g0/0/0

zone-member security dmz

exit

interface g0/0/1

zone-member security private

access-list 100 permit ip 10.10.10.64 0.0.0.15 any

class-map type inspect match-all inside-class-map

match access-group 100

policy-map type inspect in-to-out-pmap

class type inspect inside-class-map

inspect

zone-pair security in-to-out-zpair source private destination public

service-policy type inspect in-to-out-pmap

access-list 102 permit icmp any 10.10.10.80 0.0.0.15

access-list 102 permit tcp any 10.10.10.80 0.0.0.15 eq 80

access-list 102 permit tcp any 10.10.10.80 0.0.0.15 eq 443

class-map type inspect match-all pub-to-dmz-class-map

match access-group 102

policy-map type inspect pub-to-dmz-pmap

class type inspect pub-to-dmz-class-map

inspect

zone-pair security pub-to-dmz-zpair source public destination dmz

service-policy type inspect pub-to-dmz-pmap

🡪R4

enable

config terminal

hostname R4

no ip domain lookup

enable secret cisco

line console 0

password cisco

login

ip domain-name Router4

crypto key generate rsa

!!!!!!!!How many bits in the modulus [512]: 1024

username mahmoud privilege 15 secret mahmoud

line vty 0 4

login local

transport input ssh

exit

service password-encryption

banner motd $ Authorized Users Only! $

int g0/0/0

ip address 10.10.10.194 255.255.255.252

no sh

int g0/0/1

ip add 10.10.10.97 255.255.255.240

no sh

**🡪OSPF**

router ospf 10

network 10.10.10.96 0.0.0.15 area 0

network 10.10.10.192 0.0.0.3 area 0

* **OSPF authentication (MD5)**

Interface g0/0/0

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

* **Creating Views**

enable view

conf t

aaa new-model

parser view ADMIN

secret cisco123

commands exec include show ip interface brief

commands exec include show running-config

commands exec include configure terminal

exit

parser view MONITOR

secret monitor123

commands exec include show ip interface brief

exit

Router> enable view MONITOR

Password: monitor123

**🡪IPS**

---from enable mode

mkdir ipsdir

---from conf t mode

ip ips config location ipsdir

ip ips name drop\_ping

ip ips notify log

**🡪NTP**

ntp authenticate

ntp trusted-key 1

ntp authentication-key 1 md5 cisco123

ntp server 10.10.10.50 key 1

ex

**🡪SYSLOG**

service timestamps log datetime msec

logging 10.10.10.50

---signature category

ip ips signature-category

category all

retired true

ex

category ios\_ips basic

retired false

ex

int g0/0/0

ip ips drop\_ping in

---add a signature to drop the ping

ip ips signature-definition

signature 2004 0

status

enabled true

retired false

ex

engine

event-action produce-alert

event-action deny-packet-inline

ex

ex

ex

🡪R5

enable

config terminal

hostname R5

no ip domain lookup

enable secret cisco

line console 0

password cisco

login

ip domain-name Router5

crypto key generate rsa

!!!!!!!!How many bits in the modulus [512]: 1024

username mahmoud privilege 15 secret mahmoud

line vty 0 4

login local

transport input ssh

exit

service password-encryption

banner motd $ Authorized Users Only! $

int s0/2/0

ip add 10.10.10.198 255.255.255.252

no sh

int s0/2/1

ip add 10.10.10.186 255.255.255.252

no sh

int g0/0/0

ip address 10.10.10.113 255.255.255.240

no sh

int g0/0/1

ip add 10.10.10.129 255.255.255.240

no sh

**🡪OSPF**

router ospf 10

network 10.10.10.112 0.0.0.15 area 0

network 10.10.10.128 0.0.0.15 area 0

network 10.10.10.184 0.0.0.3 area 0

network 10.10.10.196 0.0.0.3 area 0

* **OSPF authentication (MD5)**

Interface s0/2/0

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

Interface s0/2/1

ip ospf message-digest-key 1 md5 mahmoud 12345

ip ospf authentication message-digest

**🡪IPV6**

ipv6 unicast-routing

interface s0/2/1

ipv6 address 2000:1:2:1::1/64

no shutdown

exit

interface s0/2/0

ipv6 address 2000:1:2:2::1/64

no shutdown

exit

interface GigabitEthernet0/0/0

ipv6 enable

ipv6 address 2000:1:2:3::1/64

no shutdown

exit

interface GigabitEthernet0/0/1

ipv6 enable

ipv6 address 2000:1:2:4::1/64

no shutdown

exit

🡪ASA

enable

config terminal

hostname ASA

no dns domain-lookup

enable password cisco

domain-name ASA

crypto key generate rsa modulus 1024

username admin password pass

aaa authentication ssh console LOCAL

ssh 10.10.10.144 255.255.255.240 inside

ssh timeout 60

password encryption

banner login Authorized Users Only!

int g1/1

nameif outside

security-level 0

ip add 10.10.10.182 255.255.255.252

no sh

int g1/2

nameif dmz

security-level 50

ip address 10.10.10.161 255.255.255.240

no sh

int g1/3

nameif inside

security-level 100

ip add 10.10.10.145 255.255.255.240

no sh

route outside 0.0.0.0 0.0.0.0 10.10.10.181

🡪DHCP

dhcpd address 10.10.10.146-10.10.10.158 inside

dhcpd enable inside

**🡪NATTING**

object network INSIDE-NET

subnet 10.10.10.144 255.255.255.240

nat (inside,outside) dynamic interface

object network DMZ-NET

subnet 10.10.10.160 255.255.255.240

nat (dmz,outside) dynamic interface

**🡪Static nat for the web server**

object network WEB-SERVER

host 10.10.10.164

nat (dmz,outside) static 10.10.10.182

**🡪ACL**

access-list OUTSIDE\_IN permit tcp any host 10.10.10.164 eq 80

access-list OUTSIDE\_IN permit tcp any host 10.10.10.164 eq 443

access-group OUTSIDE\_IN in interface outside

access-list INSIDE\_OUT permit ip any any

access-group INSIDE\_OUT out interface inside

access-list DMA\_OUT permit ip any any

access-group DMZ\_OUT out interface dmz

! ICMP INSPECTION

policy-map global\_policy

class inspection\_default

inspect icmp

service-policy global\_policy global

**R1 LAN**

🡪Core SW

enable

configure terminal

hostname CoreSW

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

1. 🡪 **Creating the vlans**
2. vlan 10
3. exit

vlan 20

1. exit

vlan 99

1. name Management
2. exit
3. vlan 1000
4. name Native
5. exit

int vlan 99

ip address 10.10.10.34 255.255.255.240

no shutdown

ip default-gateway 10.10.10.33

**🡪Trunk ports**

Interface range g0/1-2

switchport trunk encapsulation dot1q

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

interface f0/24

switchport trunk encapsulation dot1q

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

**🡪Shutdoun the unused interfaces**

1. vlan 500
2. exit
3. Interface range f0/1-23
4. switchport access vlan 500
5. sh
6. exit

**🡪 DHCP Snooping**

ip dhcp snooping

ip dhcp snooping vlan 10,20

interface f0/24

ip dhcp snooping trust

interface range g0/1-2

ip dhcp snooping limit rate 20

**🡪STP Security**

spanning-tree vlan 1,10,20,99,1000 root primary

Int range f0/24 , g0/1-2

spanning-tree guard root

**🡪DAI**

ip arp inspection vlan 10,20

interface f0/24

ip arp inspection trust

🡪Sw1

enable

configure terminal

hostname Sw1

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

1. 🡪 **Creating the vlans**
2. vlan 10
3. exit

vlan 20

1. exit

vlan 99

1. name Management
2. exit
3. vlan 1000
4. name Native
5. exit

int vlan 99

ip address 10.10.10.35 255.255.255.240

no shutdown

ip default-gateway 10.10.10.33

**🡪Trunk ports**

Interface range g0/1-2

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

Interface range f0/23-24

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

**🡪Shutdoun the unused interfaces**

1. vlan 500
2. exit
3. Interface range f0/1-22
4. switchport access vlan 500
5. switchport mode access
6. switchport nonegotiate
7. sh
8. exit

**🡪 DHCP Snooping**

ip dhcp snooping

ip dhcp snooping vlan 10,20

interface g0/2

ip dhcp snooping trust

interface f0/23

ip dhcp snooping trust

interface f0/24

ip dhcp snooping limit rate 10

interface g0/1

ip dhcp snooping limit rate 10

**🡪STP Security**

Int range f0/23-24 , g0/1

spanning-tree guard root

**🡪DAI**

ip arp inspection vlan 10,20

interface range g0/2 , f0/23

ip arp inspection trust

🡪Sw2

enable

configure terminal

hostname Sw2

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

1. 🡪 **Creating the vlans**
2. vlan 10
3. exit

vlan 20

1. exit

vlan 99

1. name Management
2. exit
3. vlan 1000
4. name Native
5. exit

int vlan 99

ip address 10.10.10.36 255.255.255.240

no shutdown

ip default-gateway 10.10.10.33

**🡪Trunk ports**

Interface range g0/1-2

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

Interface range f0/23-24

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

**🡪Shutdoun the unused interfaces**

1. vlan 500
2. exit
3. Interface range f0/1-22
4. switchport access vlan 500
5. switchport mode access
6. switchport nonegotiate
7. sh
8. exit

**🡪 DHCP Snooping**

ip dhcp snooping

ip dhcp snooping vlan 10,20

interface g0/1

ip dhcp snooping trust

interface f0/24

ip dhcp snooping trust

interface f0/23

ip dhcp snooping limit rate 10

interface g0/2

ip dhcp snooping limit rate 10

**🡪STP Security**

Int range f0/23 , g0/2

spanning-tree guard root

**🡪DAI**

ip arp inspection vlan 10,20

interface range g0/1 , f0/24

ip arp inspection trust

🡪Sw3

enable

configure terminal

hostname Sw3

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

1. 🡪 **Creating the vlans**
2. vlan 10
3. exit

vlan 20

1. exit

vlan 99

1. name Management
2. exit
3. vlan 1000
4. name Native
5. exit

int vlan 99

ip address 10.10.10.37 255.255.255.240

no shutdown

ip default-gateway 10.10.10.33

**🡪Trunk ports**

Interface g0/1

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

Interface f0/1

switchport mode access

switchport nonegotiate

switchport access vlan 10

**🡪Shutdoun the unused interfaces**

1. vlan 500
2. exit
3. Interface range f0/2-24
4. switchport access vlan 500
5. switchport mode access
6. switchport nonegotiate
7. sh
8. exit
9. Interface range g0/2
10. switchport access vlan 500
11. switchport mode access
12. switchport nonegotiate
13. sh
14. exit

**🡪 DHCP Snooping**

ip dhcp snooping

ip dhcp snooping vlan 10,20

interface g0/1

ip dhcp snooping trust

interface range f0/1

ip dhcp snooping limit rate 3

**🡪STP Security**

Int f0/1

spanning-tree portfast

spanning-tree bpduguard enable

**🡪DAI**

ip arp inspection vlan 10,20

interface g0/1

ip arp inspection trust

* **PortSecurity**

interface fastEthernet0/1

switchport port-security

switchport port-security violation shutdown

switchport port-security mac-address sticky

🡪Sw4

enable

configure terminal

hostname Sw4

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

1. 🡪 **Creating the vlans**
2. vlan 10
3. exit

vlan 20

1. exit

vlan 99

1. name Management
2. exit
3. vlan 1000
4. name Native
5. exit

int vlan 99

ip address 10.10.10.38 255.255.255.240

no shutdown

ip default-gateway 10.10.10.33

**🡪Trunk ports**

Interface g0/1

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

Interface f0/1

switchport mode access

switchport nonegotiate

switchport access vlan 20

**🡪Shutdoun the unused interfaces**

1. vlan 500
2. exit
3. Interface range f0/2-24
4. switchport access vlan 500
5. switchport mode access
6. switchport nonegotiate
7. sh
8. exit
9. Interface range g0/2
10. switchport access vlan 500
11. switchport mode access
12. switchport nonegotiate
13. sh
14. exit

**🡪 DHCP Snooping**

ip dhcp snooping

ip dhcp snooping vlan 10,20

interface g0/1

ip dhcp snooping trust

interface range f0/1

ip dhcp snooping limit rate 3

**🡪STP Security**

Int f0/1

spanning-tree portfast

spanning-tree bpduguard enable

**🡪DAI**

ip arp inspection vlan 10,20

interface g0/1

ip arp inspection trust

* **PortSecurity**

interface fastEthernet0/1

switchport port-security

switchport port-security violation shutdown

switchport port-security mac-address sticky

🡪Sw5

enable

configure terminal

hostname Sw5

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

1. 🡪 **Creating the vlans**
2. vlan 10
3. exit

vlan 20

1. exit

vlan 99

1. name Management
2. exit
3. vlan 1000
4. name Native
5. exit

int vlan 99

ip address 10.10.10.39 255.255.255.240

no shutdown

ip default-gateway 10.10.10.33

**🡪Trunk ports**

Interface g0/1

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

Interface f0/1

switchport mode access

switchport nonegotiate

switchport access vlan 10

**🡪Shutdoun the unused interfaces**

1. vlan 500
2. exit
3. Interface range f0/2-24
4. switchport access vlan 500
5. switchport mode access
6. switchport nonegotiate
7. sh
8. exit
9. Interface range g0/2
10. switchport access vlan 500
11. sh
12. exit

**🡪 DHCP Snooping**

ip dhcp snooping

ip dhcp snooping vlan 10,20

interface g0/1

ip dhcp snooping trust

interface range f0/1

ip dhcp snooping limit rate 3

**🡪STP Security**

Int f0/1

spanning-tree portfast

spanning-tree bpduguard enable

Int g0/1

spanning-tree guard root

**🡪DAI**

ip arp inspection vlan 10,20

interface g0/1

ip arp inspection trust

* **PortSecurity**

interface fastEthernet0/1

switchport port-security

switchport port-security violation shutdown

switchport port-security mac-address sticky

🡪Sw6

enable

configure terminal

hostname Sw6

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

1. 🡪 **Creating the vlans**
2. vlan 10
3. exit

vlan 20

1. exit

vlan 99

1. name Management
2. exit
3. vlan 1000
4. name Native
5. exit

int vlan 99

ip address 10.10.10.40 255.255.255.240

no shutdown

ip default-gateway 10.10.10.33

**🡪Trunk ports**

Interface g0/1

switchport mode trunk

switchport nonegotiate

switchport trunk native vlan 1000

switchport trunk allowed vlan 10,20,99

exit

Interface f0/1

switchport mode access

switchport nonegotiate

switchport access vlan 20

**🡪Shutdoun the unused interfaces**

1. vlan 500
2. exit
3. Interface range f0/2-24
4. switchport access vlan 500
5. switchport mode access
6. switchport nonegotiate
7. sh
8. exit
9. Interface range g0/2
10. switchport access vlan 500
11. switchport mode access
12. switchport nonegotiate
13. sh
14. exit

**🡪 DHCP Snooping**

ip dhcp snooping

ip dhcp snooping vlan 10,20

interface g0/1

ip dhcp snooping trust

interface range f0/1

ip dhcp snooping limit rate 3

**🡪STP Security**

Int f0/1

spanning-tree portfast

spanning-tree bpduguard enable

**🡪DAI**

ip arp inspection vlan 10,20

interface g0/1

ip arp inspection trust

* **PortSecurity**

interface fastEthernet0/1

switchport port-security

switchport port-security violation shutdown

switchport port-security mac-address sticky

**R2 LAN**

🡪SW-1

enable

configure terminal

hostname Sw-1

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

* **SVI**

int vlan 1

ip address 10.10.10.62 255.255.255.240

no shutdown

ex

ip default-gateway 10.10.10.49

**🡪802.1x**

aaa new-model

radius-server host 10.10.10.60 auth-port 1645 key cisco123

aaa authentication dot1x default group radius

dot1x system-auth-control

int f0/1

switchport mode access

authentication port-control auto

dot1x pae authenticator

**R3 Inside LAN**

SW-3

enable

configure terminal

hostname Sw-3

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

int vlan 1

ip address 10.10.10.78 255.255.255.240

no shutdown

ex

ip default-gateway 10.10.10.65

**R3 DMZ LAN**

SW-4

enable

configure terminal

hostname Sw-4

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

int vlan 1

ip address 10.10.10.94 255.255.255.240

no shutdown

ex

ip default-gateway 10.10.10.81

**R4 LAN**

SW-8

enable

configure terminal

hostname Sw-8

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

int vlan 1

ip address 10.10.10.110 255.255.255.240

no shutdown

ex

ip default-gateway 10.10.10.97

**R5 LEFT LAN**

SW-12

enable

configure terminal

hostname Sw-12

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

int vlan 1

ip address 10.10.10.126 255.255.255.240

no shutdown

ex

ip default-gateway 10.10.10.113

**R5 Right LAN**

SW-13

enable

configure terminal

hostname Sw-13

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

int vlan 1

ip address 10.10.10.142 255.255.255.240

no shutdown

ex

ip default-gateway 10.10.10.129

**ASA INSIDE LAN**

SW-7

enable

configure terminal

hostname Sw-7

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

int vlan 1

ip address 10.10.10.158 255.255.255.240

no shutdown

ex

ip default-gateway 10.10.10.145

**ASA DMZ LAN**

SW-8

enable

configure terminal

hostname Sw-8

no ip domain-lookup

enable secret cisco

line con 0

password cisco

login

exit

line vty 0 4

password cisco

login

banner motd # Authorized Users Only! #

int vlan 1

ip address 10.10.10.174 255.255.255.240

no shutdown

ex

ip default-gateway 10.10.10.161

Show commands

🡪DHCP

show ip dhcp snooping

show ip dhcp snooping binding

* DTP

Sh dtp

* AAA 802.1x

show dot1x

show authentication sessions

* STP

sh spanning-tree summary

sh spanning-tree

show spanning-tree inconsistentports

show errdisable recovery

* To check

spanning-tree vlan 99 root primary

🡪DAI

show ip arp inspection

show ip dhcp snooping binding

🡪ntp

show ntp associations

show ntp status