ASA Firewall Lab Manual

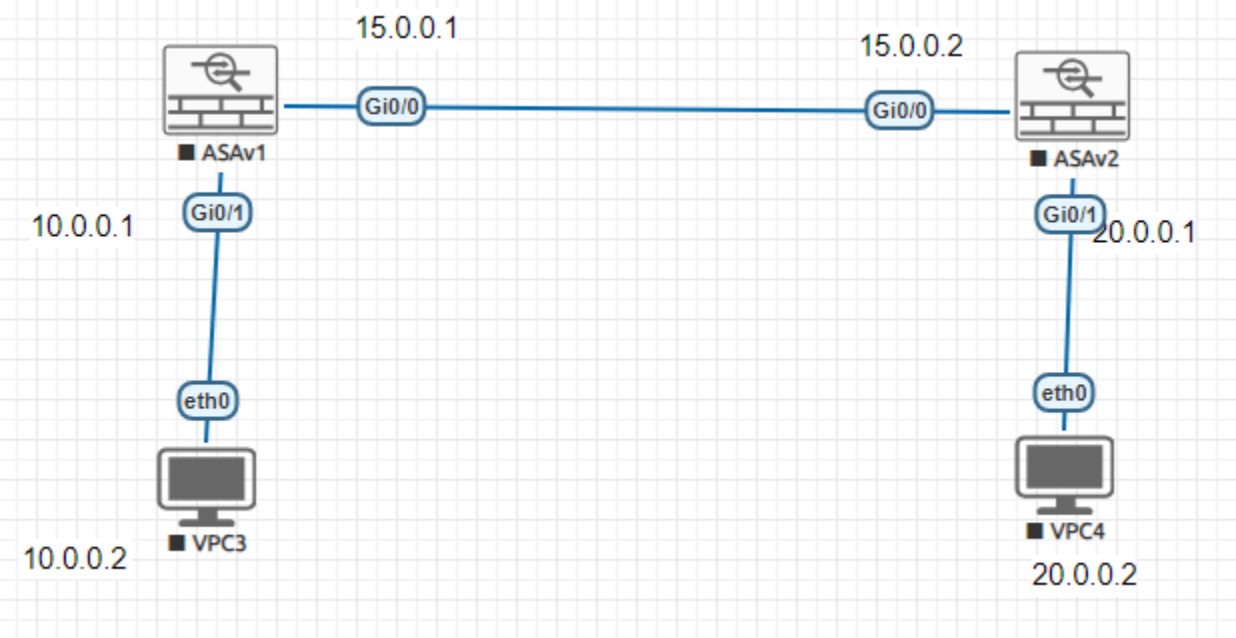
Developed By: Waleed Adlan

Lab 1

Cisco ASA Firewall Initialization

Task 1:

Connect the network as shown below in Eve-ng



Task 2:

Configure ASA1 & ASA2 interfaces with the depicted ip addresses and assign security-level 100 and name it inside for LAN interface, then security-level 0 and name it outside for WAN interfaces.

!ASA1
enable
conf t
interface G0/1
no shutdown
ip address 10.0.0.1 255.0.0.0
nameif inside

```
security-level 100
exit
interface G0/0
no shutdown
ip address 15.0.0.1 255.0.0.0
nameif outside
security-level 0
exit


!ASA2
enable
conf t
interface G0/1
no shutdown
ip address 20.0.0.1 255.0.0.0
nameif inside
security-level 100
exit
interface G0/0
no shutdown
ip address 15.0.0.2 255.0.0.0
nameif outside
security-level 0
exit
```

Task 3:

Configure static route for both firewalls pointing to the LAN networks of the other ASA LAN network

```
!ASA1
Route outside 20.0.0.0 255.0.0.0 15.0.0.2

!ASA2
Route outside 10.0.0.0 255.0.0.0 15.0.0.1
```

Task 4:

Configure access-list to permit icmp traffic in outside interfaces

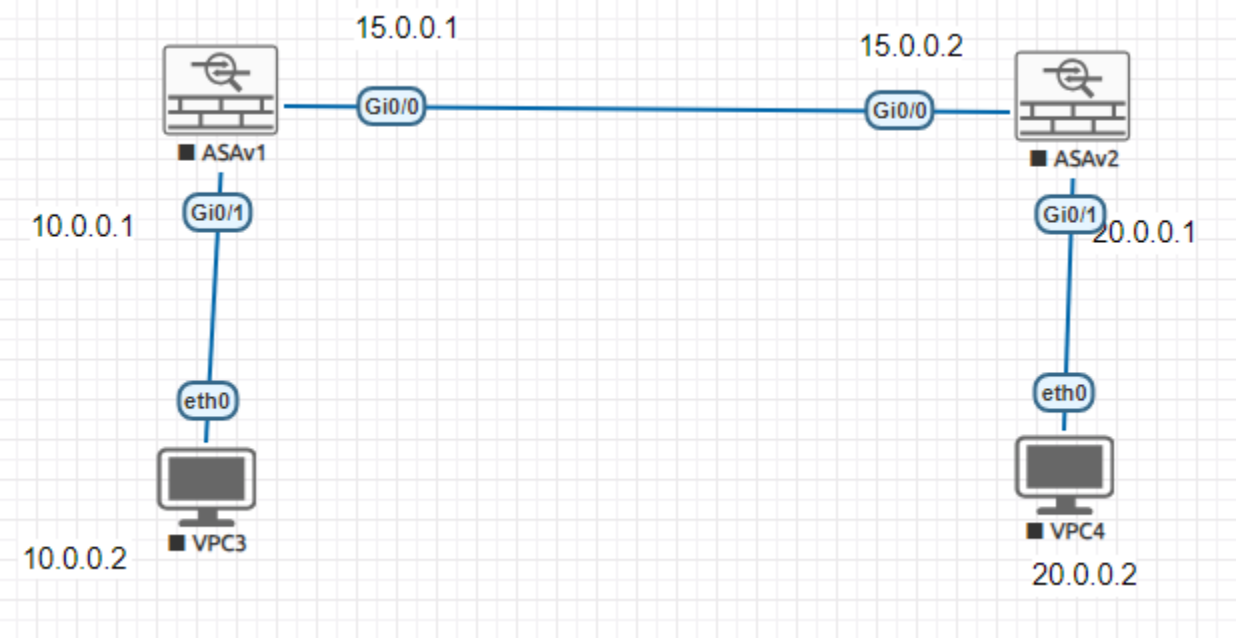
!ASA1/ASA2
Access-list test extended permit icmp any any
Access-group test in interface outside

Lab 2

Default Routing on ASA Firewall

Task 1:

Connect the network below network in eve-ng



Task 2:

Configure both Firewalls with IP addresses, name interfaces and assign the appropriate security levels for inside and outside interfaces and configure ACL allowing icmp traffic in outside interfaces

!ASA1
Interface g0/1
No shut
Nameif inside
Security-level 100
Ip address 10.0.0.1 255.0.0.0
Interface g0/0

No shut
Nameif outside
Security-level 0
Ip address 15.0.0.1 255.0.0.0
Exit
Access-list test extended permit icmp any any
Access-group test in interface outside

!ASA2
Interface g0/1
No shut
Nameif inside
Security-level 100
Ip address 20.0.0.1 255.0.0.0
Interface g0/0
No shut
Nameif outside
Security-level 0
Ip address 15.0.0.2 255.0.0.0
Exit
Access-list test extended permit icmp any any
Access-group test in interface outside

Task 3:

Configure Default route on both ASA firewalls to complete the network connectivity

!ASA1
Route outside 0.0.0.0 0.0.0.0 15.0.0.2

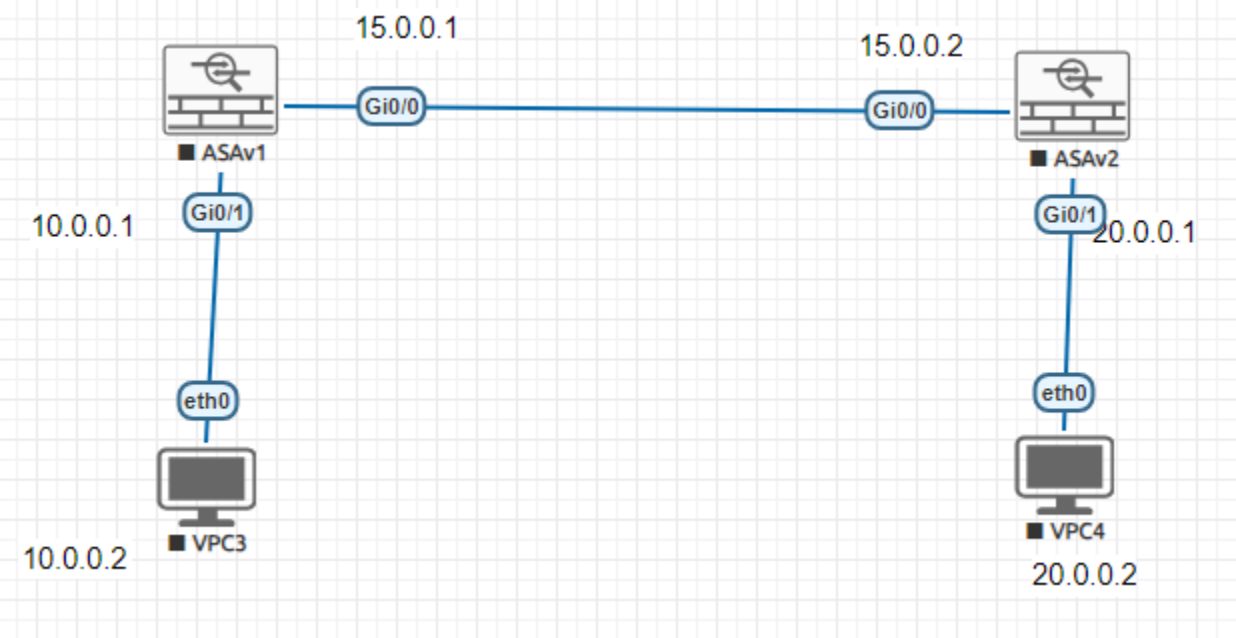
!ASA2
Route outside 0.0.0.0 0.0.0.0 15.0.0.1

Lab 3

Dynamic Routing Protocols on ASA

Task 1:

Connect the network as shown in the eve-ng



Task 2:

Configure both ASAs interfaces with shown ip addresses, security-level and interface names. Then configure Access-list to permit icmp traffic in outside interfaces.

!ASA1
Interface g0/1
No shut
Nameif inside
Security-level 100
Ip address 10.0.0.1 255.0.0.0
Interface g0/0

No shut
Nameif outside
Security-level 0
Ip address 15.0.0.1 255.0.0.0
Exit
Access-list test extended permit icmp any any
Access-group test in interface outside

!ASA2
Interface g0/1
No shut
Nameif inside
Security-level 100
Ip address 20.0.0.1 255.0.0.0
Interface g0/0
No shut
Nameif outside
Security-level 0
Ip address 15.0.0.2 255.0.0.0
Exit
Access-list test extended permit icmp any any
Access-group test in interface outside

Task 3:

Configure RIP as routing protocol on Both ASA firewalls and ensure connectivity

!ASA1
Router rip
Version 2
Network 10.0.0.0
Network 15.0.0.0
No auto-summary

!ASA2
Router rip
Version 2

Network 20.0.0.0
Network 15.0.0.0
No auto-summary

Task 4:

Remove RIP, then configure EIGRP as routing protocol on Both ASA firewalls and ensure connectivity

!ASA1
No Router rip
Router eigrp 100
Network 10.0.0.0
Network 15.0.0.0
No auto-summary

!ASA2
No Router rip
Router eigrp 100
Network 20.0.0.0
Network 15.0.0.0
No auto-summary

Task 5:

Remove EIGRP, then configure OSPF as routing protocol on Both ASA firewalls and ensure connectivity

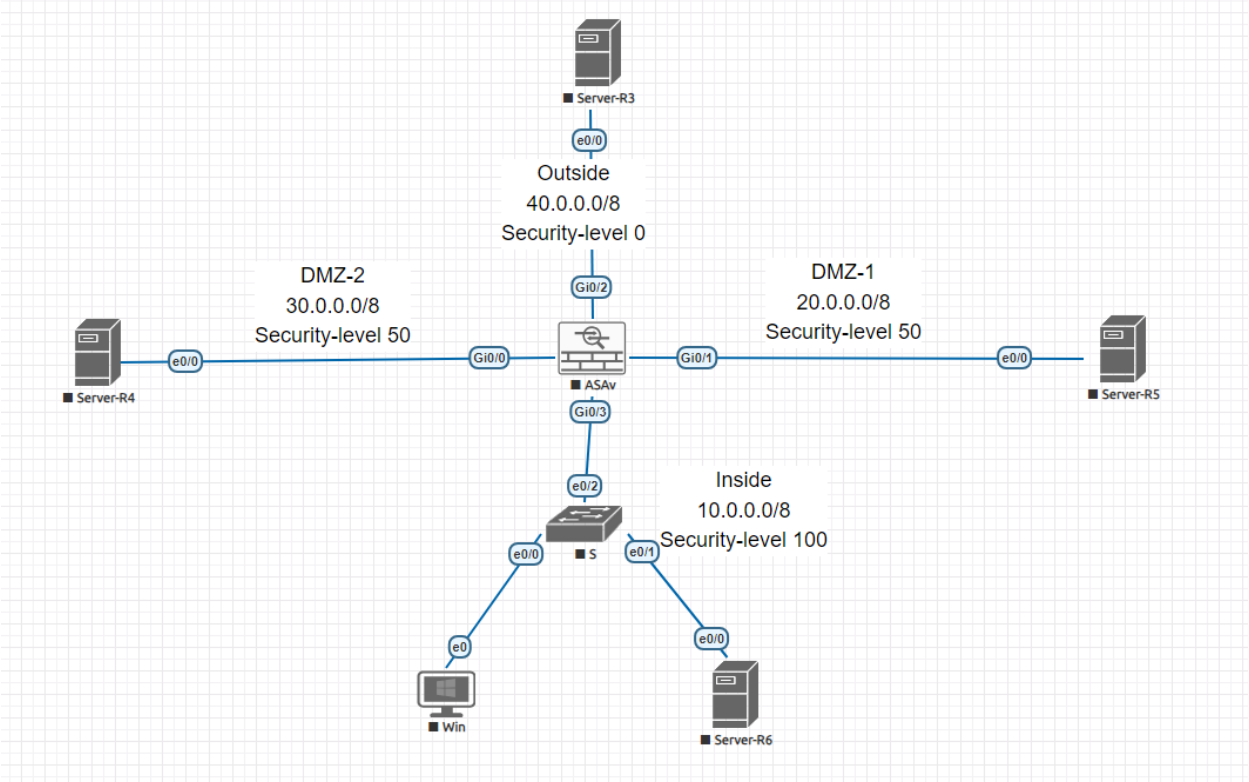
!ASA1
No Router Eigrp 100
Router ospf 1
Network 10.0.0.0 255.0.0.0 area 0
Network 15.0.0.0 255.0.0.0 area 0
No auto-summary

!ASA2

No Router Eigrp 100
Router ospf 1
Network 20.0.0.0 255.0.0.0 area 0
Network 15.0.0.0 255.0.0.0 area 0
No auto-summary

Lab 4

Access-list and Traffic Handling on ASA



Task 1:

Connect the network as shown above and assign ip addresses as depicted.
For the Firewall configure the interface names and security-level as shown.

!ASA1
Interface g0/3
No shut
Ip add 10.0.0.1 255.0.0.0
Nameif inside
Security-level 100
!

```
Int g0/1
No shut
Ip add 20.0.0.1 255.0.0.0
Nameif DMZ-1
Security-level 50
!
Int g0/0
No shut
Ip add 30.0.0.1 255.0.0.0
Nameif DMZ-2
Security-level 50
!
Interface g0/2
No shut
Ip add 40.0.0.1 255.0.0.0
Nameif outside
Security-level 0
```

Task 2:

Make a test of a ping from the firewall to the directly connected ip and vice versa

Task 3:

Configure HTTP on Server-R3, Server-R4, Server-R5 & Server-6

```
!Servers
Username ccnp privilege 15 password cisco
Ip http server
Ip http authentication local
```

Task 4:

Configure Telnet on Server-R4 & Server-R5 & allow same security interface traffic between DMZ-1 & DMZ-2

```
!Server4&Server5
Line vty 0 4
```

Password cisco
Transport input telnet
Login
!ASA
same-security-traffic permit inter-interface

Task 5:

Modify the configuration on the ASA firewall so that icmp to the outside interface is only allowed from 40.0.0.3

!ASA
icmp permit host 40.0.0.3 outside

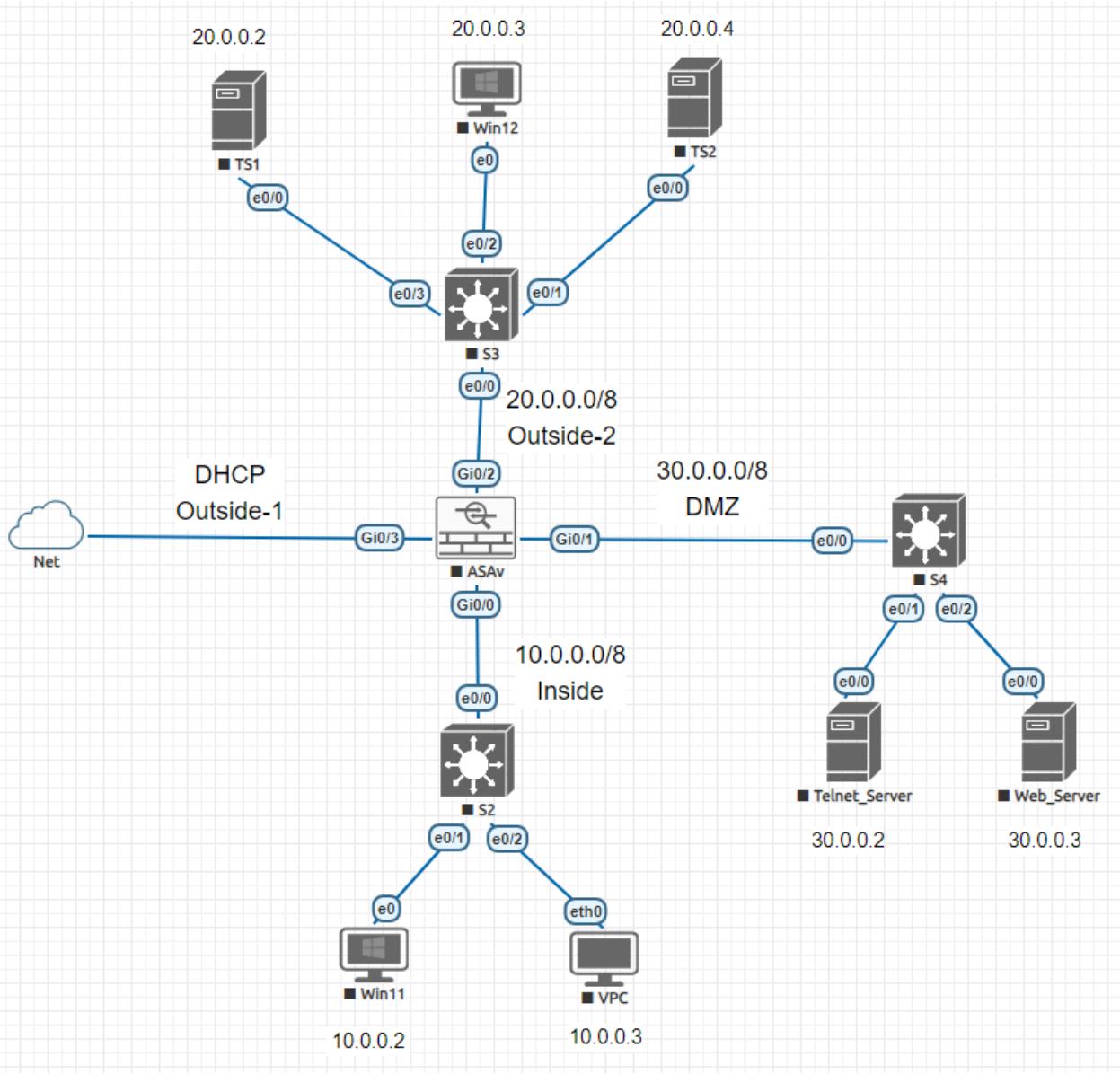
Task 6:

Modify the configuration on the ASA firewall, so that icmp is inspected when moving from inside to outside

!ASA
policy-map global_policy
class inspection_default
inspect icmp

Lab 5

Network Address Translation



Task 1:

Connect the network as shown and assign ip addresses as shown. For telnet Server, web server, TS1 and TS2 configure default route. Outside-1 interface Should get a dhcp ip address with default route

```
!ASA1
Interface g0/1
No shut
Nameif dmz
Ip address 30.0.0.1 255.0.0.0
Security-level 50
!
Interface g0/3
No shutdown
Nameif outside-1
Ip address dhcp setroute
!
Interface g0/0
No shutdown
Nameif inside
Ip address 10.0.0.1 255.0.0.0
!
Interface g0/2
No shutdown
Nameif outside-2
Security-level 0
Ip address 20.0.0.1 255.0.0.0
```

Task 2:

Configure ASA1 to inspect icmp traffic for testing

```
!ASA1
policy-map global_policy
class inspection_default
inspect icmp
```

Task 3:
Configure Dynamic NAT on ASA, so that traffic from 10.0.0.0 network going to internet (Outside-1) should be natted with the range of IPs (192.168.100.10 – 192.168.100.20)

```
!ASA
Object network pool-public
Range 192.168.10 192.168.1.20
!
Object network subnet-10.0.0.0
Subnet 10.0.0.0 255.0.0.0
Nat (inside,outside-1) dynamic pool-public
```

Task 4:
Modify the configuration so that traffic from 10.0.0.0 network going to the outside-1 is Pat natted to the outside-1 interface

```
!ASA
Object network subnet-10.0.0.0
No Nat (inside,outside-1) dynamic pool-public
Nat (inside,outside-1) dynamic interface
```

Task 5:
Configure ASA, so that traffic to telnet server & Web_server is static natted to 20.0.0.10 and 20.0.0.20 and should be accessible from outside-2 network. Don't forget to enable http and telnet on the webserver

```
!Telnet-Server
Enable password cisco
Line vty 0 4
Password cisco
Transport input telnet
Login

!Web-server
```

Username ccnp privilege 15 password ciscoIp http server
Ip http authentication local

!ASA
Object network telnet-server
Host 30.0.0.2
Nat (dmz,outside-2) static 20.0.0.10
!
Object network web-server
Host 30.0.0.3
Nat (dmz,outside-2) static 20.0.0.20
!
Access-list nat extended permit ip any host 30.0.0.2
Access-list nat extended permit ip any host 30.0.0.3
!
Access-group nat in outside-2

Task 6:
Modify the NAT on ASA so that both Telnet-server and web-server got natted to 20.0.0.10 using different ports (port forwarding) and modify the acl accordingly

!ASA
Object network telnet-server
Host 30.0.0.2
No Nat (dmz,outside-2) static 20.0.0.10
Nat (dmz,outside-2) static 20.0.0.10 service tcp 23 23
!
Object network web-server
Host 30.0.0.3
No Nat (dmz,outside-2) static 20.0.0.20
Nat (dmz,outside-2) static 20.0.0.10 service tcp 80 80
!
No access-list nat extended permit ip any host 30.0.0.2
No access-list nat extended permit ip any host 30.0.0.3
Access-list nat extended permit tcp any host 30.0.0.2 eq 23
Access-list nat extended permit tcp any host 30.0.0.3 eq 80

!
Access-group nat in interface outside

Task 7:

Modify the configuration so that telnet service and http service are mapped to ports 8823 8880 (Port Redirection)

!ASA
Object network telnet-server
Host 30.0.0.2
No Nat (dmz,outside-2) static 20.0.0.10 service tcp 23 23
Nat (dmz,outside-2) static 20.0.0.10 service tcp 23 8823
!
Object network web-serverHost 30.0.0.3
No Nat (dmz,outside-2) static 20.0.0.10 service tcp 80 80
Nat (dmz,outside-2) static 20.0.0.10 service tcp 80 8880
!

Task 8:

Modify the VPC configuration that not to have a default gateway. Then configure static destination nat that 20.0.0.3 is translated to 10.0.0.100

!ASA
Object network h-20.0.0.3
Host 20.0.0.3
Nat (outside-2,inside) static 10.0.0.100

Task 9:

Configure Policy NAT so that 10.0.0.2 is translated 20.0.0.50 when accessing TS1 and 20.0.0.6 when accessing TS2. Configure Telnet service on TS1 & TS2 for testing purpose.

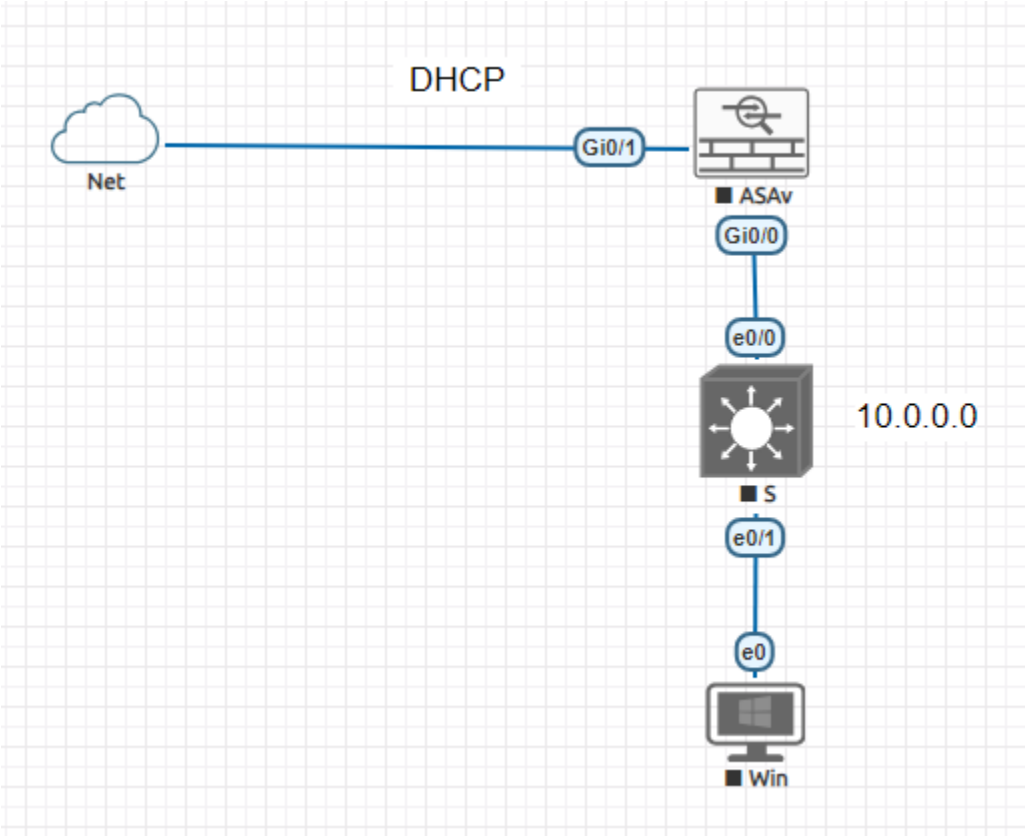
!TS1 & TS2
Enable password cisco
Line vty 0 4
Transport input telnet
Password cisco

Login

```
!ASA
Object network H
Host 10.0.0.2
!
Object network x1
Host 20.0.0.50
!
Object network x2
Host 20.0.0.60
!
Object network d1
Host 20.0.0.2
!
Object network d2
Host 20.0.0.4
!
Nat (inside,outside-2) source static H x1 destination static d1 d1
Nat (inside,outside-2) source static H x2 destination static d2 d2
```

Lab 6

Remote Access Management



Task 1:
Connect the network and assign ip addresses as shown in the figure

Task 2:
Enable telnet on the inside network for the 10.0.0.0 network
!ASA
telnet 10.0.0.0 255.0.0.0 inside
Passwd Cisco123

Task 3:
Configure SSH on the inside network for 10.0.0.0 network
!ASA
Ssh 10.0.0.0 255.0.0.0 inside

Username ccnp password Cisco123 privilege 15
Domain-name cisco.com
Crypto key generate rsa modulus 1024
Aaa authentication ssh console LOCAL

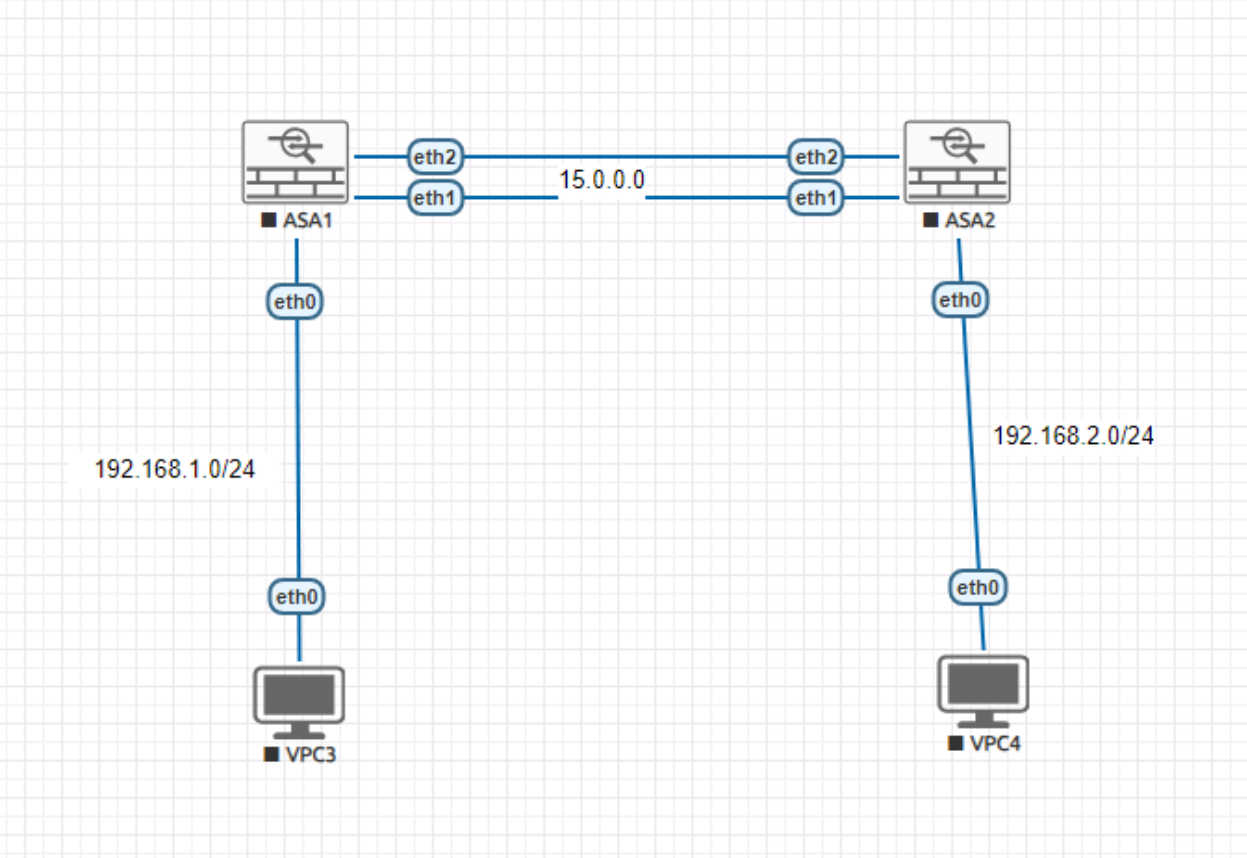
Task 4:
Enable ASDM on the inside interface for the network 10.0.0.0/8
!ASA
Http server enable
http 10.0.0.0 255.0.0.0 inside
username ccnp password cisco123 privilege 15
aaa authentication http console LOCAL

Lab 7

ASA Redundant Interfaces/Ether-channel

Task 1:

Connect the network below, and assign IP addresses to the PCs and configure two interfaces as redundant interfaces. Then enable static routes between the two firewalls, and confirm connectivity.



!ASA1
enable
conf t
int e0
no shut
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!

```
Int e1
No shut
!
Int e2
No shut
!
Int redundant 1
Member-interface e1
Member-interface e2
Ip address 15.0.0.1 255.0.0.0
Nameif outside
Exit
!
Route outside 192.168.2.0 255.255.255.0 15.0.0.2
!
access-list test extended permit icmp any any
access-group test in interface outside

!ASA2
enable
conf t
int e0
no shut
nameif inside
security-level 100
ip address 192.168.2.1 255.255.255.0
!
Int e1
No shut
!
Int e2
No shut
!
Int redundant 1
Member-interface e1
Member-interface e2
Ip address 15.0.0.2 255.0.0.0
```

Nameif outside
Exit
!
Route outside 192.168.1.0 255.255.255.0 15.0.0.1
!
access-list test extended permit icmp any any
access-group test in interface outside

Task 2:
First Remove the redundant interface, then configure Ether-channel Between the two ASA Firewalls using LACP Protocol

!ASA1
No interface redundant 1
!
Int e1
No shut
Channel-group 1 mode active
!
Int e2
No shut
Channel-group 1 mode active
!
Int port-channel 1
Ip address 15.0.0.1 255.0.0.0
Nameif outside
Exit
!
Route outside 192.168.2.0 255.255.255.0 15.0.0.2
!
access-list test extended permit icmp any any
access-group test in interface outside

!ASA2
No interface redundant 1
!
Int e1

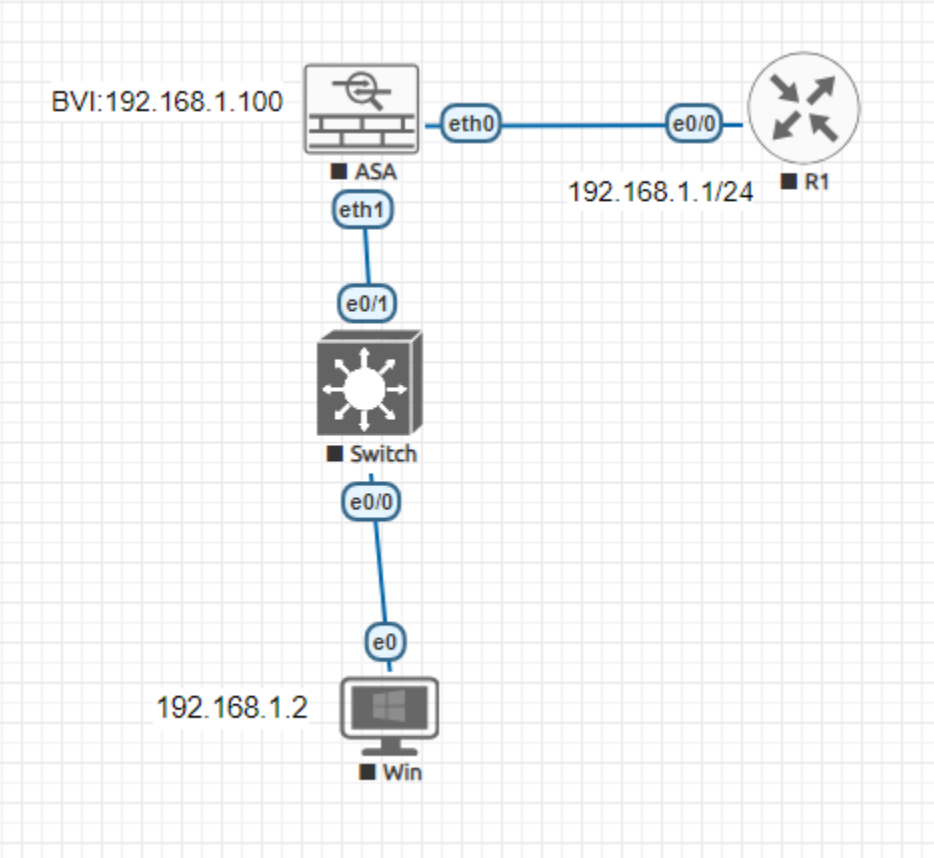
```
No shut
Channel-group 1 mode passive
!
Int e2
No shut
Channel-group 1 mode passive
!
Int port-channel 1
Ip address 15.0.0.2 255.0.0.0
Nameif outside
Exit
!
Route outside 192.168.1.0 255.255.255.0 15.0.0.1
!
access-list test extended permit icmp any any
access-group test in interface outside
!
```

Lab 8

Transparent Firewall

Task 1:

Connect the network below, and assign IP addresses as shown, and name the interfaces as described. Configure the firewall as transparent firewall, and their interfaces to bridge group 1. Configure ACL in the outside interface to allow the icmp traffic.



!R1
interface e0/0
no shut
ip add 192.168.1.1 255.255.255.0

!ASA
enable

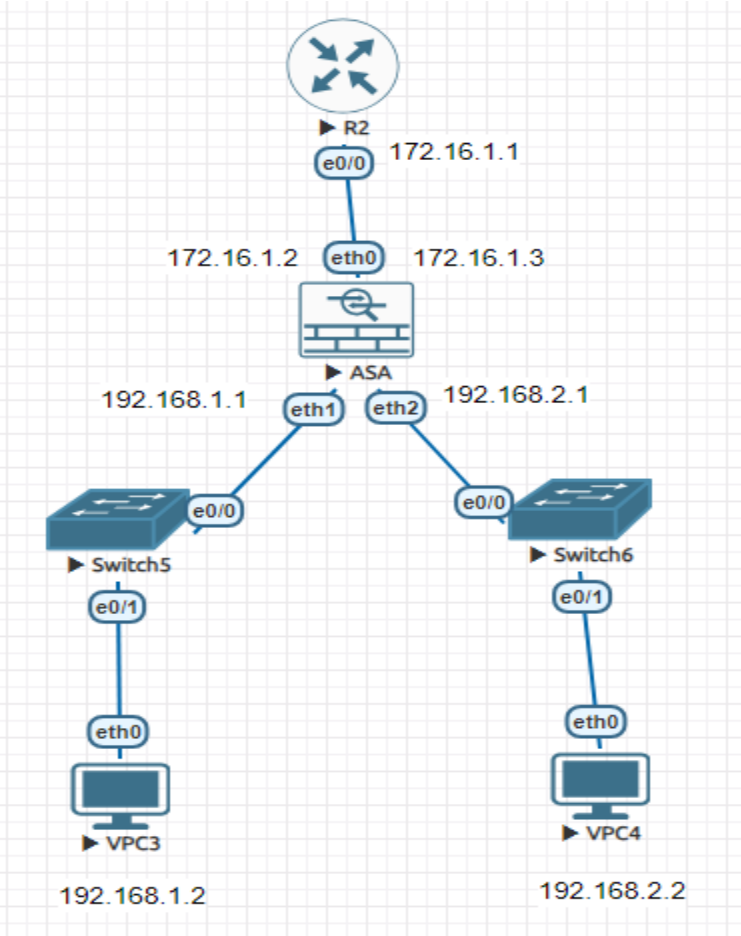
```
conf  t
!
firewall transparent
!
int e1
no shut
nameif inside
bridge-group 1
!
int e0
no shut
nameif outside
bridge-group 1
!
interface bvi 1
ip add 192.168.1.100 255.255.255.0
exit
!
access-list test extended permit icmp any any
access-group test in interface outside
```

Lab 9

Security Context

Task 1:

Connect the network below, and assign IP address to the router as shown, divide the firewall into two virtual firewalls c1 & C2. C1 is connected to computer 1 while C2 is having the other PC. Make interface e0 as shared interface between the two contexts. Make access-list to allow icmp traffic from outside interface to the inside in both virtual firewalls.



!R1
enable
!
conf t
!

```
int e0/0
no shut
ip add 172.16.1.1 255.255.255.0
exit
!
ip route 192.168.1.0 255.255.255.0 172.16.1.2
!
ip route 192.168.2.0 255.255.255.0 172.16.1.3


!ASA
enable
conf t
!
mode multiple
!
int e0
no shut
!
int e1
no shut
!
int e2
no shut
!
context c1
allocate-interface e1
allocate-interface e0
config-url disk0:/c1.cfg
!
context c2
allocate-interface e2
allocate-interface e0
config-url disk0:/c2.cfg
exit
!
changeto context c1
```

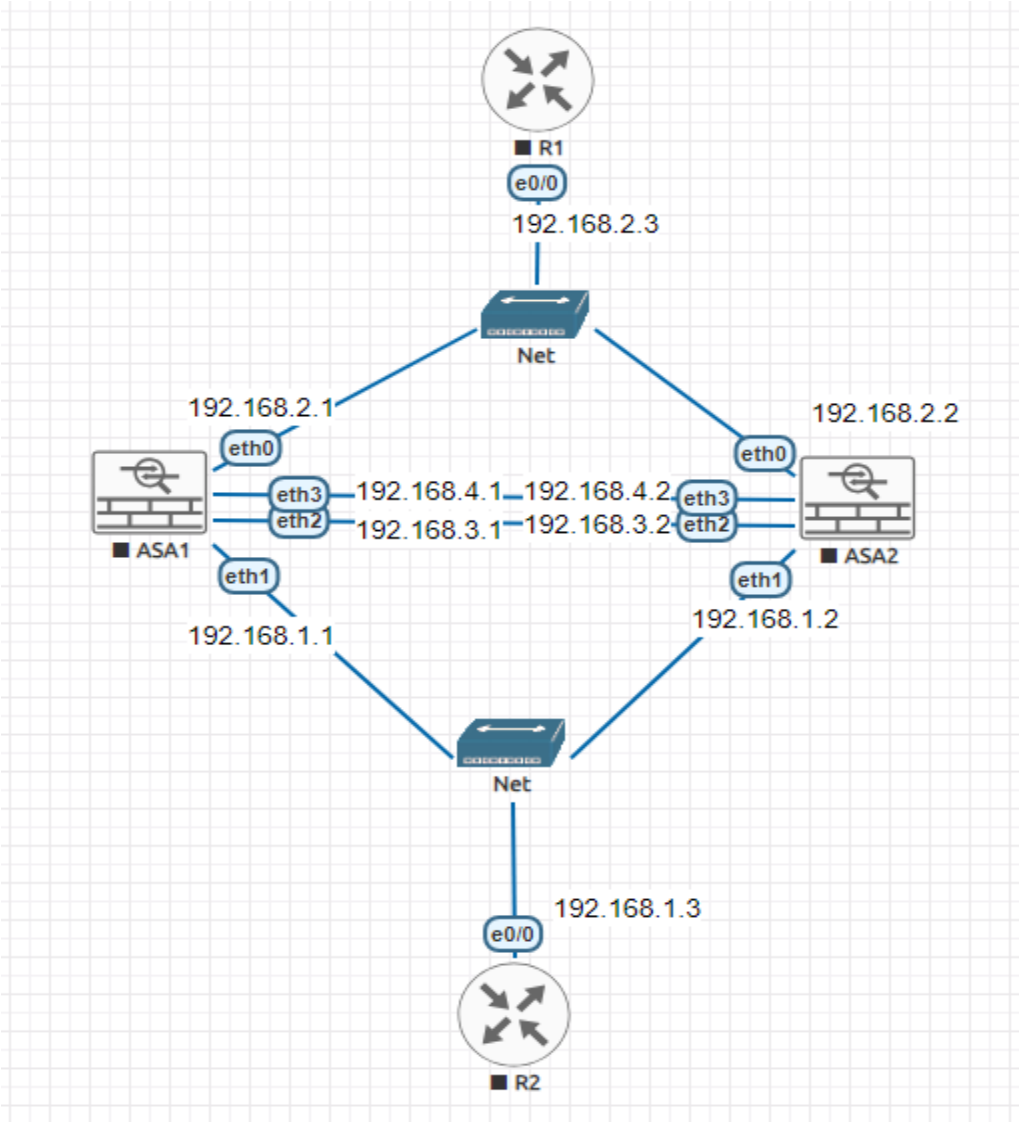
```
int e1
nameif inside
ip add 192.168.1.1 255.255.255.0
!
int e0
nameif outside
ip add 172.16.1.2 255.255.255.0
mac-address 5000.0000.0002
exit
!
access-list test1 extended permit icmp any any
access-group test1 in interface outside
!
changeto context c2
!
int e2
nameif inside
ip add 192.168.2.1 255.255.255.0
!
int e0
nameif outside
ip add 172.16.1.3 255.255.255.0
mac-address 5000.0000.0003
exit
!
access-list test2 extended permit icmp any any
access-group test2 in interface outside
```

Lab 10

ASA Failover (Active/Standby)

Task 1:

Connect the network below, and configure the first firewall as primary firewall, and the second one as secondary firewall. The two links between the two firewalls should be configured as failover Lan & stateful lan links. The IP addresses should be configured as shown in the diagram. Configure also the router with the depicted ip addresses with default route in R2 pointing to 192.168.1.1. Also enable Telnet on R1



```
!R1
Interface e0/0
No shutdown
Ip address 192.168.2.3 255.255.255.0
!
Line vty 0 4
Password cisco
Login
Transport input telnet

!R2
Interface e0/0
No shutdown
Ip address 192.168.1.3 255.255.255.0
!
Ip route 0.0.0.0 0.0.0.0 192.168.1.1


!ASA1
enable
conf t
!
interface e0
no shut
!
interface e1
no shut
!
interface e2
no shut
!
interface e3
no shut
!
failover lan unit primary
failover lan interface LANfo e2
```

```
failover interface ip LANfo 192.168.3.1 255.255.255.0 standby 192.168.3.2
failover key cisco
failover
!
failover link stateful e3
failover interface ip stateful 192.168.4.1 255.255.255.0 standby 192.168.4.2
!
interface e1
nameif inside
ip add 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
interface e0
nameif outside
ip add 192.168.2.1 255.255.255.0 standby 192.168.2.2
!


!ASA2

enable
conf t
!
interface e0
no shut
!
interface e1
no shut
!
interface e2
no shut
!
interface e3
no shut
!
failover lan unit secondary
failover lan interface LANfo e2
failover interface ip LANfo 192.168.3.1 255.255.255.0 standby 192.168.3.2
```

failover key cisco
failover
!

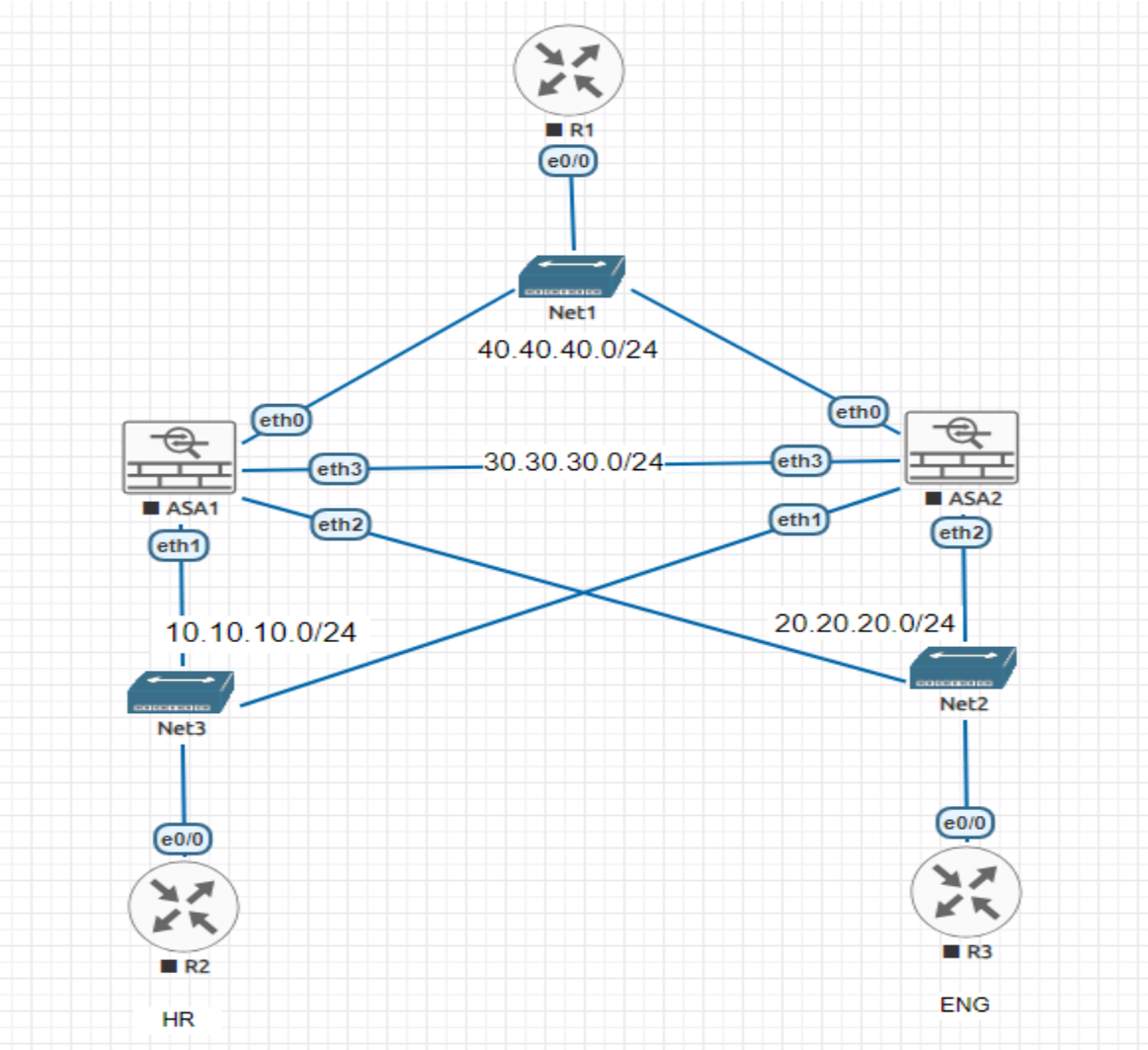
Task 2:
Configure Dynamic NAT on ASA1 (Active), so that traffic on network 192.168.1.0 will be natted to a range of IPs 192.168.2.10 – 192.168.2.20.
!ASA1
Object network Public
Range ip 192.168.2.10 192.168.2.20
!
Object network local
Subnet 192.168.1.0 255.255.255.0
Nat (inside,outside) dynamic Public

Lab 11

ASA Failover (Active/Active)

Task 1:

Connect the below network, Configure IP addresses in the three routers and make telnet enabled on R1. Configure default routes on R2 & R3. Configure both ASAs as multiple mode with two security contexts HR and ENG. Eth1 in ASA should be assigned to HR, Eth2 to ENG and Eth0 shared interface



```
!R1
Int eth0/0
No shut
Ip add 40.40.40.3 255.255.255.0
Exit
!
Line vty 0 4
Password cisco
Login
Transport input telnet

!R2
Int e0/0
No shut
Ip add 10.10.10.3 255.255.255.0
Exit
!
Ip route 0.0.0.0 0.0.0.0 10.10.10.1

!R3
Int e0/0
No shut
Ip add 20.20.20.3 255.255.255.0
Exit
!
Ip route 0.0.0.0 0.0.0.0 20.20.20.1


!ASA1/ASA2
Mode multiple
!

!ASA1
Context HR
Allocate-interface e0
Allocate-interface e1
Config-url disk0:/hr.cfg
```

Context ENG
Allocate-interface e0
Allocate-interface e2
Config-url disk0:/eng.cfg
!

Task 2:
Configure the ASA firewall ip addresses in each context, and enable mac automatic generation in shared interfaces. Then configure dynamic Nat in each context to be dynamically natted to the 40.40.40.0 network.
!

!ASA
Mac-address auto
!
Changeto context HR
Int e0
No shut
Nameif outside
Ip address 40.40.40.1 255.255.255.0 standby 40.40.40.2
!
Int e1
No shut
Nameif inside
Ip address 10.10.10.1 255.255.255.0 standby 10.10.10.2
!
Object network public
Range 40.40.40.10 40.40.40.20
!
Object network private
Subnet 10.10.10.0 255.255.255.0
Nat (inside,outside) dynamic public
!
Mac-address auto
!
Changeto context ENG

```
Int e0
No shut
Nameif outside
Ip address 40.40.40.5 255.255.255.0 standby 40.40.40.6
!
Int e1
No shut
Nameif inside
Ip address 20.20.20.1 255.255.255.0 standby 20.20.20.2
!
Object network public
Range 40.40.40.10 40.40.40.20
!
Object  network private
Subnet 20.20.20.0 255.255.255.0
Nat (inside,outside) dynamic public
```

Task 3:

Enable ASA Failover by using failover group. So that ASA1 is the active for HR security context and ASA2 is the active for ENG security context. Use link Eth3 as failover lan and stateful link between the two ASA firewalls.

```
!ASA1
Changedto system
Failover lan unit primary
Failover lan interface LANfo eth3
Failover interface ip LANfo 30.30.30.1 255.255.255.0 standby 30.30.30.2
Failover link LANfo eth3
Failover key cisco123
Failover

!ASA2
Failover lan unit secondary
Failover lan interface LANfo eth3
Failover interface ip LANfo 30.30.30.1 255.255.255.0 standby 30.30.30.2
```

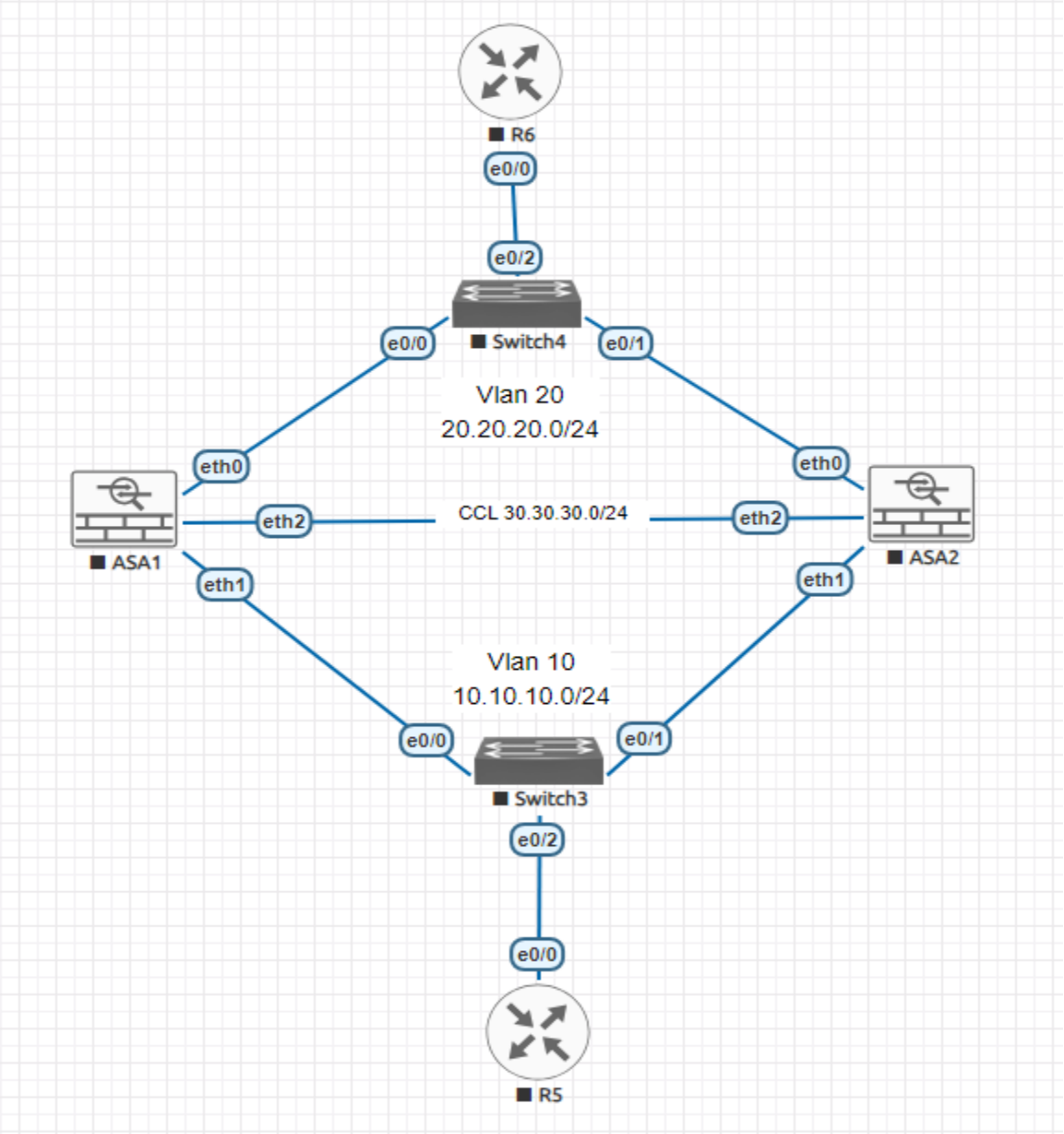
```
Failover link LANfo eth3
Failover key cisco123



!ASA1
Failover group 1
Primary
Preempt
!
Failover group 2
Secondary
Preempt
!
Context HR
Join-failover-group 1
!
Context Eng
Join-failover-group 2
Failover
```

Lab 12

ASA Clustering Spanned Mode

Task 1:

Connect the below network, and assign IP addresses for R5 & R6 in the relevant subnet. Configure R5 with default route pointing to ASA, R6 with telnet.



!R5
Interface eth0/0
No shut
Ip address 10.10.10.3 255.255.255.0
!
Ip route 0.0.0.0 0.0.0.0 10.10.10.1

!R6
Interface eth0/0
No shut
Ip address 20.20.20.1 255.255.255.0
!
Line vty 0 4
Password cisco
Transport input telnet
Login

Task 2:
Configure SW3 & SW4 in the relevant VLANs and configure etherchannel in ports eth0/0 & eth1.

!SW3
Vlan 10
Interface range eth0/0 – 1
Switchport mode access
Switchport access vlan 10
!
Interface range eth0/0 – 1
Channel-group 10 mode active
!
Interface port-channel 10
Switchport mode access
Switchport access vlan 10

!SW4
Vlan 20
Interface range eth0/0 – 1
Switchport mode access
Switchport access vlan 20
!
Interface range eth0/0 – 1
Channel-group 20 mode active
!
Interface port-channel 20
Switchport mode access
Switchport access vlan 20

Task 3:
Configure ASA1 & ASA2 to work in Clustering Spanned Mode.

!ASA1
Cluster interface-mode spanned
!
Interface eth2
No shutdown
!
Cluster group aaa
Local-unit primary
Cluster-interface eth2 ip 30.30.30.1 255.255.255.0
Priority 1
Key cisco123
Enable
!

!ASA2
Cluster interface-mode spanned
!
Interface eth2
No shutdown
!
Cluster group aaa

Local-unit secondary
Cluster-interface eth2 ip 30.30.30.2 255.255.255.0
Priority 2
Key cisco123
Enable
!

Task4

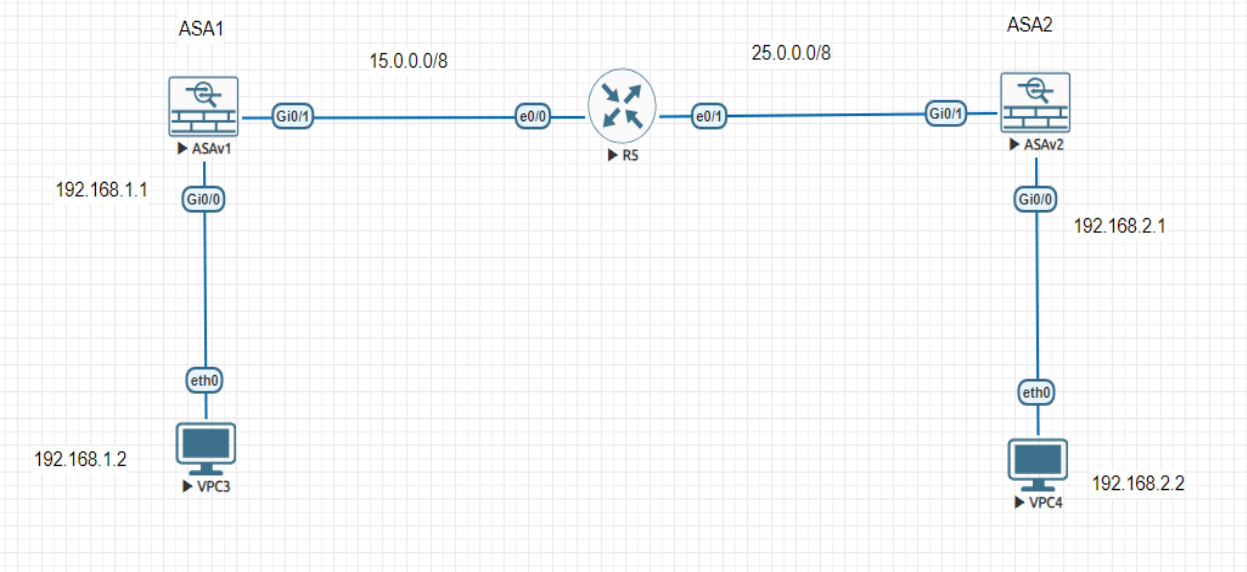
Configure Port-channel on ASA then enable inside and outside interfaces and NAT for private network to be natted through 20.20.20.0 network pool

!ASA1
Interface eth 1
No shut
Channel-group 10 mode active
!
Int eth 0
No shut
Channel-group 20 mode active
!
Interface port-channel 10
Port-channel span-cluster
Nameif inside
Ip add 10.10.10.1 255.255.255.0
Mac-address aaaa.aaaa.aaaa
No shut
!
Interface port-channel 20
Port-channel span-cluster
Nameif outside
Ip add 20.20.20.1 255.255.255.0
Mac-address bbbb.bbbb.bbbb
No shut
!
Object network public
Range 20.20.20.10 20.20.20.20

!
Object network private
Subnet 10.10.10.0 255.255.255.0
Nat (inside,outside) dynamic public

Lab 13

IPSec VPN Between ASA Firewalls



Task 1:
Connect the network as shown above, configure ip addresses, default route on ASA1 & ASA2 toward R5

!ASA1
Hostname ASA1
Interface g0/0
No shutdown
Ip address 192.168.1.1 255.255.255.0
Nameif inside
!
Interface g0/1
No shutdown
Ip address 15.0.0.1 255.0.0.0
Nameif outside
!
Route outside 0.0.0.0 0.0.0.0 15.0.0.2

!ASA2
Hostname ASA2

Interface g0/0
No shutdown
Ip address 192.168.2.1 255.255.255.0
Nameif inside
!
Interface g0/1
No shutdown
Ip address 25.0.0.3 255.0.0.0
Nameif outside
!
Route outside 0.0.0.0 0.0.0.0 25.0.0.2

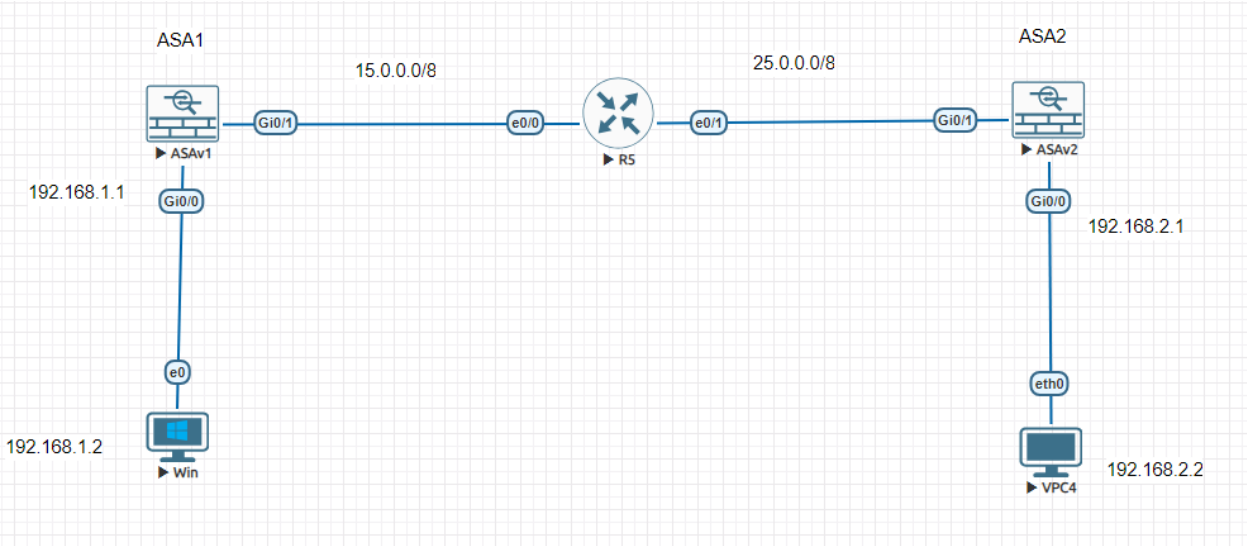
Task 2:
Configure IPSec Site to Site VPN on ASA1 & ASA2

!ASA1
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash md5
group 2
lifetime 600
!
tunnel-group 25.0.0.3 type ipsec-l2l
tunnel-group 25.0.0.3 ipsec-attributes
ikev1 pre-shared-key cisco123
!
access-list 100 extended permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
!
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
!
crypto map my-map 1 match address 100
crypto map my-map 1 set peer 25.0.0.3
crypto map my-map 1 set ikev1 transform-set myset
crypto map my-map interface outside

```
!

!ASA2
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash md5
group 2
lifetime 600
!
tunnel-group 15.0.0.1 type ipsec-l2l
tunnel-group 15.0.0.1 ipsec-attributes
ikev1 pre-shared-key cisco123
!
access-list 100 extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0
!
crypto ipsec ikev1 transform-set myset esp-aes-256 esp-sha-hmac
!
crypto map my-map 1 match address 100
crypto map my-map 1 set peer 15.0.0.1
crypto map my-map 1 set ikev1 transform-set myset
crypto map my-map interface outside
```

Lab 14

IPSec VPN Between ASA Firewalls Using ASDM



Task 1:
Connect the network as shown, assign ip addresses configure default routes on the ASA towards R5

!ASA1
Hostname ASA1
Interface g0/0
No shut
Ip address 192.168.1.1 255.255.255.0
Nameif inside
!
Interface g0/1
No shutdownIp address 15.0.0.1 255.0.0.0
Nameif outside
Exit
!
Route outside 0.0.0.0 0.0.0.0 15.0.0.2

!ASA2
Hostname ASA2

Interface g0/0
No shut
Ip address 192.168.2.1 255.255.255.0
Nameif inside
!
Interface g0/1
No shutdown
Ip address 25.0.0.3 255.0.0.0
Nameif outside
Exit
!
Route outside 0.0.0.0 0.0.0.0 25.0.0.2

Task 2:
Configure ASA1 & ASA2 for remote management through ASDM!ASA1
http server enable
http 192.168.1.0 255.255.255.0 inside
aaa authentication http console LOCAL
username ccnp password cisco privilege 15
!ASA2
http server enable
http 192.168.1.0 255.255.255.0 outside
aaa authentication http console LOCAL
username ccnp password cisco privilege 15

Task 3:
Configure Static route on R5 toward 192.168.1.0 subnet to allow ASA2 be managed from 192.168.1.2 host
!R5
Ip route 192.168.1.0 255.255.255.0 15.0.0.1

Task 4:
Configure ASA1 & ASA2 IPSec Site to Site VPN GUI VPN Wizard
!ASA1
Wizard>VPN Wizard>Site to Site VPN WizardPeer IP address:25.0.0.3
Local Network: 192.168.1.0/24
Remote Network: 192.168.2.0/24

Pre-shared Key: cisco123
Enable NAT Exemption
!ASA2
Wizard>VPN Wizard>Site to Site VPN Wizard
Peer IP address:15.0.0.1
Local Network: 192.168.2.0/24
Remote Network: 192.168.1.0/24
Pre-shared Key: cisco123
Enable NAT Exemption

Task 5:
Repeat Previous lab of Doing same step but configure IPSec Site to Site Through VPN configuration not wizard

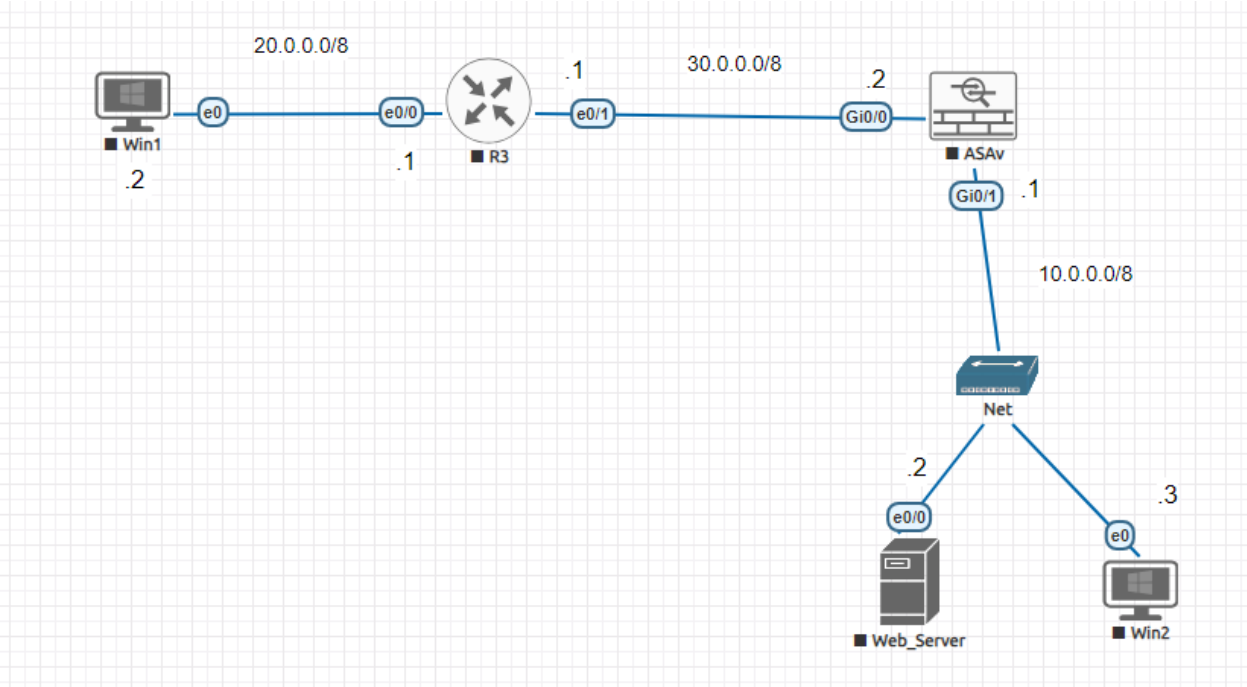
!ASA1
Configuration> Site to Site VPN
Enable Ikev1 outside
Add Connection Profile:
Peer IP: 25.0.0.3Interface: Outside
Local Network: 192.168.1.0/24
Remote Network: 192.168.2.0/24
Enable IKEv1 only
Preshared key: cisco123
Select IKE Policy
Select IPSec Proposal
Enable NAT Exemption

!ASA2
Configuration> Site to Site VPN
Enable Ikev1 outside
Add Connection Profile:
Peer IP: 15.0.0.1
Interface: Outside
Local Network: 192.168.2.0/24
Remote Network: 192.168.1.0/24
Enable IKEv1 only
Preshared key: cisco123

Select IKE Policy
Select IPSec Proposal
Enable NAT Exemption

Lab 15

Web VPN (SSL VPN)



Task 1:
Connect the network as shown above. All devices are configured except the ASA. Do the initial configuration for the ASA

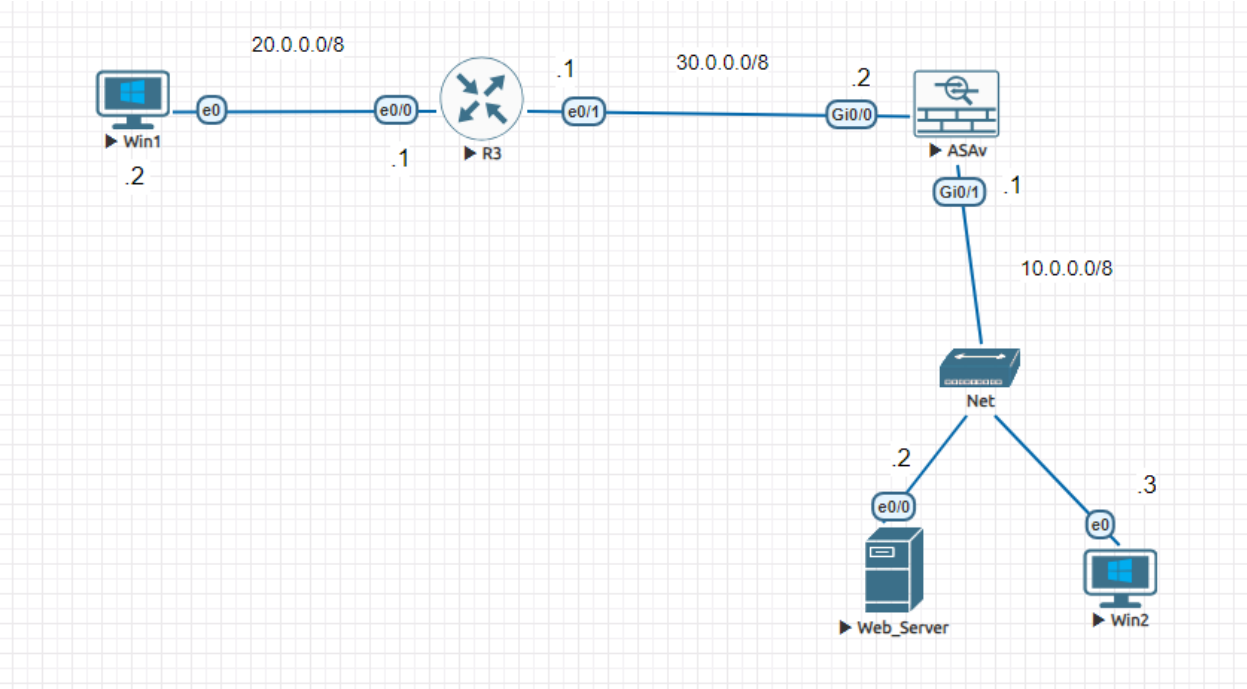
!ASA
Hostname ASA
!
Interface g0/0
No shut
Nameif outside
Ip address 30.0.0.2 255.0.0.0!
Interface g0/1
No shutdown
Nameif inside
Ip address 10.0.0.1 255.0.0.0
Exit
Route outside 20.0.0.0 255.0.0.0 30.0.0.1

Task 2:
Configure ASA to enable webvpn on its outside interface allowing http access to Web Server

```
!ASA
webvpn
enable outside
group-policy Eng internal
group-policy Eng attributes
vpn-tunnel-protocol ssl-clientless
banner value "Only authorized users are allowed !!!"
username ccnp password cisco
username ccnp attributes
vpn-group-policy Eng
```

Lab 16

Remote Access VPN (Anyconnect VPN)



Task 1:
Connect the network as shown above. All devices are configured except the ASA. Do the initial configuration for the ASA

!ASA
Hostname ASA
!
Interface g0/0
No shut
Nameif outside
Ip address 30.0.0.2 255.0.0.0
!
Interface g0/1
No shutdown
Nameif inside
Ip address 10.0.0.1 255.0.0.0

Exit
Route outside 20.0.0.0 255.0.0.0 30.0.0.1

Task 2:
Enable ASDM GUI Management on the ASA

!ASA
http server enable
http 10.0.0.0 255.0.0.0 inside
aaa authentication http console LOCAL
username ccnp password cisco privilege 15

Task 3:
Configure Remote Access VPN using ASDM
!ASA
Wizard>VPN Wizard> Anyconnect VPN Wizard
Connection Profile Name: Anyconnect Profile Remote
VPN Access Interface: Outside
Enable SSL & IPSecAdd Digital Certificate: New Identity Certificate – Self Signed
Locate Anyconnect Image
Username: CCNP
Pool Name: Private Pool
Pool Starting IP address: 10.0.0.220
Pool Ending IP address: 10.0.0.250
Pool Mask: 255.0.0.0
NAT Exempt: Enabled