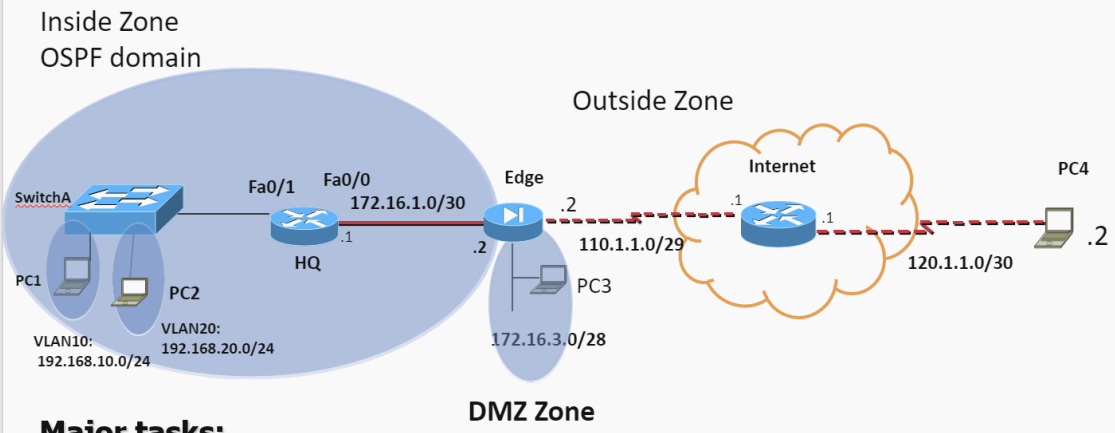
COMP4056 Project A



Major tasks:

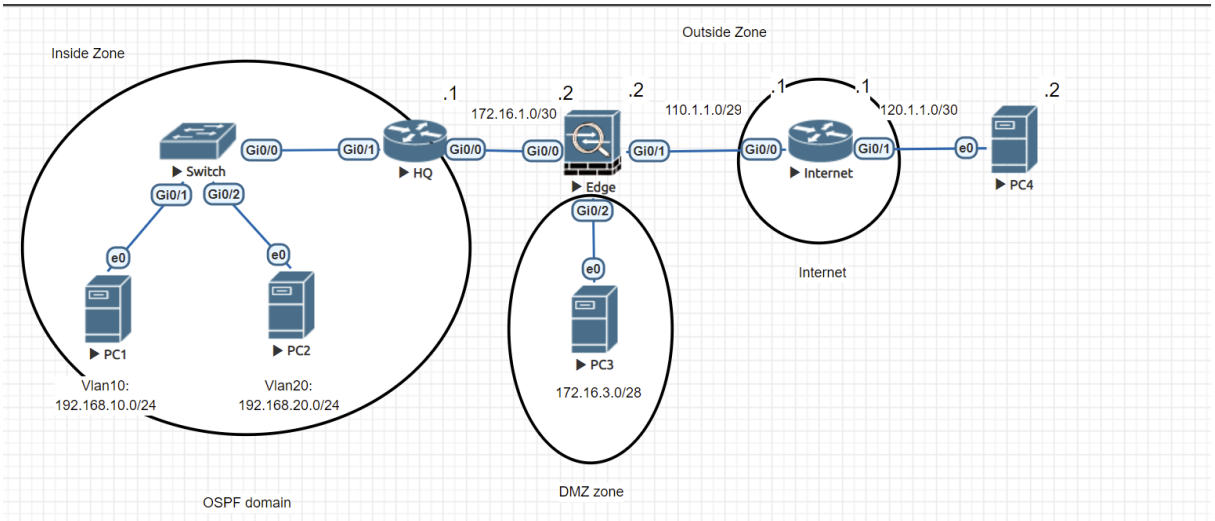
A. Analyze the above network design. Choose the right system devices for project implementation. Update the physical topology map based on your ports chosen.

B. Set up OSPF domain to form the Inside Zone. Create DMZ zone to host a Web server/PC3. Connect outside zone to Internet.

C. Test IP connectivity within each security level zone. Verify/configure HQ/Edge IP routes to reach out other zones/domains.

D. Create traffic filter so that VLAN 10 and 20 hosts are not allowed to access 172.16.1.0/30 network. The rest of traffic flows from VLAN10 and VLAN 20 are all allowed.

E. Apply the right settings to allow PC4 to browse the PC3--Web server, also allow PC4 to VNC view PC1.



A. Analyze the above network design. Choose the right system devices for project implementation. Update the physical topology map based on your ports chosen.
B. Set up OSPF domain to form the Inside Zone. Create DMZ zone to host a Web server/PC3. Connect outside zone to Internet.
C. Test IP connectivity within each security level zone. Verify/configure HQ/Edge IP routes to reach out other zones/domains.
D. Create traffic filter so that VLAN 10 and 20 hosts are not allowed to access 172.16.1.0/30 network. The rest of traffic flows from VLAN10 and VLAN 20 are all allowed.
E. Apply the right settings to allow PC4 to browse the PC3--Web server, also allow PC4 to VNC view PC1

Version:

Cisco Adaptive Security Appliance Software Version 9.8(3)

Config on Edge:

```
nat (inside,outside) after-auto source dynamic any interface

nat (dmz,outside) after-auto source dynamic any interface

route outside 0.0.0.0 0.0.0.0 110.1.1.1

policy-map global_policy

class inspection_defaultinspect icmp
debug icmp trace

!
object network WWW-EXThost 110.1.1.3

object network WWW-INThost 172.16.3.1

nat (DMZ,outside) static WWW-EXT service tcp www www

access-list OUTSIDE extended permit tcp any object WWW-INT eq wwwaccess-group
OUTSIDE in interface outside
!

object network VNC-EXThost 110.1.1.4

object network VNC-INThost 192.168.10.2

nat (inside,outside) static VNC-EXT service tcp www www

access-list OUTSIDE extended permit tcp any object VNC-INT eq wwwaccess-group
OUTSIDE in interface outside
```

sh nat

```
Edge# sh nat

Auto NAT Policies (Section 2)
1 (DMZ) to (outside) source static WWW-INT WWW-EXT  service tcp www www
    translate_hits = 0, untranslate_hits = 4
2 (inside) to (outside) source static VNC-INT VNC-EXT  service tcp www www
    translate_hits = 0, untranslate_hits = 7

Manual NAT Policies (Section 3)
1 (DMZ) to (outside) source dynamic any interface
    translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic any interface
    translate_hits = 0, untranslate_hits = 0
Edge#
```

sh xl

```
Edge# sh xl
Edge# sh xlate
4 in use, 4 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from outside:0.0.0.0/0 to DMZ:0.0.0.0/0
    flags sIT idle 4:58:54 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 4:58:54 timeout 0:00:00
TCP PAT from DMZ:172.16.3.1 80-80 to outside:110.1.1.3 80-80
    flags sr idle 0:05:58 timeout 0:00:00
TCP PAT from inside:192.168.10.2 80-80 to outside:110.1.1.4 80-80
    flags sr idle 0:04:52 timeout 0:00:00

Edge#
```

sh ospf neighbor

```
Edge# sh ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.20.1      1   FULL/DR         0:00:32    172.16.1.1      inside
Edge#
```

```
HQ>sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.3.2        1   FULL/BDR        00:00:32    172.16.1.2      GigabitEtherne
t0/0
HQ>
```

sh access-list

```
Edge# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTSIDE; 2 elements; name hash: 0x97f9426
access-list OUTSIDE line 1 extended permit tcp any object WWW-INT eq www (hitcnt=4) 0x12d0f299
  access-list OUTSIDE line 1 extended permit tcp any host 172.16.3.1 eq www (hitcnt=4) 0x12d0f299
access-list OUTSIDE line 2 extended permit tcp any object VNC-INT eq www (hitcnt=7) 0x2bec261b
  access-list OUTSIDE line 2 extended permit tcp any host 192.168.10.2 eq www (hitcnt=7) 0x2bec261b
Edge#
```

```
HQ#sh access-lists
Extended IP access list blockacl
    10 deny tcp 192.168.10.0 0.0.0.255 172.16.1.0 0.0.0.3
    20 deny tcp 192.168.20.0 0.0.0.255 172.16.1.0 0.0.0.3
    30 permit ip any any
HQ#
```

sh int trunk

```
Switch#sh interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Gi0/0       10,20

Port        Vlans allowed and active in management domain
Gi0/0       10,20

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       10,20
Switch#
```

sh vlan

```
Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/3, Gi1/0, Gi1/1, Gi1/2
                                                 Gi1/3
10   vlan10                            active    Gi0/1
20   vlan20                            active    Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

packet-tracer input outside tcp 110.1.1.4 1234 110.1.1.3 http detailed

packet-tracer input outside tcp 110.1.1.5 1234 110.1.1.4 http detailed

sh router

```
Edge# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 110.1.1.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 110.1.1.1, outside
C        110.1.1.0 255.255.255.248 is directly connected, outside
L        110.1.1.2 255.255.255.255 is directly connected, outside
C        172.16.1.0 255.255.255.252 is directly connected, inside
L        172.16.1.2 255.255.255.255 is directly connected, inside
C        172.16.3.0 255.255.255.240 is directly connected, DMZ
L        172.16.3.2 255.255.255.255 is directly connected, DMZ
O        192.168.10.0 255.255.255.0 [110/11] via 172.16.1.1, 01:07:12, inside
O        192.168.20.0 255.255.255.0 [110/11] via 172.16.1.1, 01:07:12, inside
```

```
HQ#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      110.0.0.0/29 is subnetted, 1 subnets
O        110.1.1.0 [110/11] via 172.16.1.2, 01:06:48, GigabitEthernet0/0
      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C        172.16.1.0/30 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
O        172.16.3.0/28 [110/11] via 172.16.1.2, 01:07:26, GigabitEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/1.10
L        192.168.10.1/32 is directly connected, GigabitEthernet0/1.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, GigabitEthernet0/1.20
L        192.168.20.1/32 is directly connected, GigabitEthernet0/1.20
HQ#
```

```
Internet>sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      110.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        110.1.1.0/29 is directly connected, GigabitEthernet0/1
L        110.1.1.1/32 is directly connected, GigabitEthernet0/1
      120.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        120.1.1.0/30 is directly connected, GigabitEthernet0/0
L        120.1.1.1/32 is directly connected, GigabitEthernet0/0
Internet>
```

Edge# packet-tracer input outside tcp 110.1.1.4 1234 110.1.1.3 http

Phase: 1

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

object network WWW-INT

nat (DMZ,outside) static WWW-EXT service tcp www www

Additional Information:

NAT divert to egress interface DMZ

Untranslate 110.1.1.3/80 to 172.16.3.1/80

Phase: 2

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group OUTSIDE in interface outside

access-list OUTSIDE extended permit tcp any object WWW-INT eq www

Additional Information:

Phase: 3

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 4

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 5

Type: QOS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 6

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

object network WWW-INT

nat (DMZ,outside) static WWW-EXT service tcp www www

Additional Information:

Phase: 7

Type: QOS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 10

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 5, packet dispatched to next module

Result:

input-interface: outside

input-status: up

input-line-status: up

output-interface: DMZ

output-status: up

output-line-status: up

Action: allow

Edge# packet-tracer input outside tcp 110.1.1.5 1234 110.1.1.4 http

Phase: 1

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

object network VNC-INT

nat (inside,outside) static VNC-EXT service tcp www www

Additional Information:

NAT divert to egress interface inside

Untranslate 110.1.1.4/80 to 192.168.10.2/80

Phase: 2

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group OUTSIDE in interface outside

access-list OUTSIDE extended permit tcp any object VNC-INT eq www

Additional Information:

Phase: 3

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 4

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 5

Type: QOS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 6

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

object network VNC-INT

nat (inside,outside) static VNC-EXT service tcp www www

Additional Information:

Phase: 7

Type: QOS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 10

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 20, packet dispatched to next module

Result:

input-interface: outside

input-status: up

input-line-status: up

output-interface: inside

output-status: up

output-line-status: up

Action: allow