CONTENTS

1. Overview

In this project we have designed and implemented a network between two Branch offices. Zone based policy Firewall is implemented and has INSIDE, OUTSIDE and DMZ zones connected to it. To access the DMZ from public network the NAT is implemented. Site-to-site access IPsec VPN between two Branch office routers is configured for specific network so that all the traffic between networks stays encrypted till it reaches the other end-point. The switches are configured with port-security for the security purpose.

2. Policy Requirements

The following is a short list of policies that would be typical of security policy. The design and implementation must incorporate these policies.

- In the topology we have two branch office. If IT department of branch office 1 wants to access IT department of branch office 2 for http protocol then it needs to establish IPsec tunnel between routers.
- Branch office 2 does not have a budget and for that Zone Based Policy Firewall needs to be implemented on the router.
- The server in the DMZ zone should be accessible from public and Branch office 1 network for http, https protocol.
- In branch office 1 IT department and finance department should be accessible to each other.
- Switches should be hardened with port-security in branch office 1 and 2.
- All access to and from the Internet must connect via NAT.

3. Topology

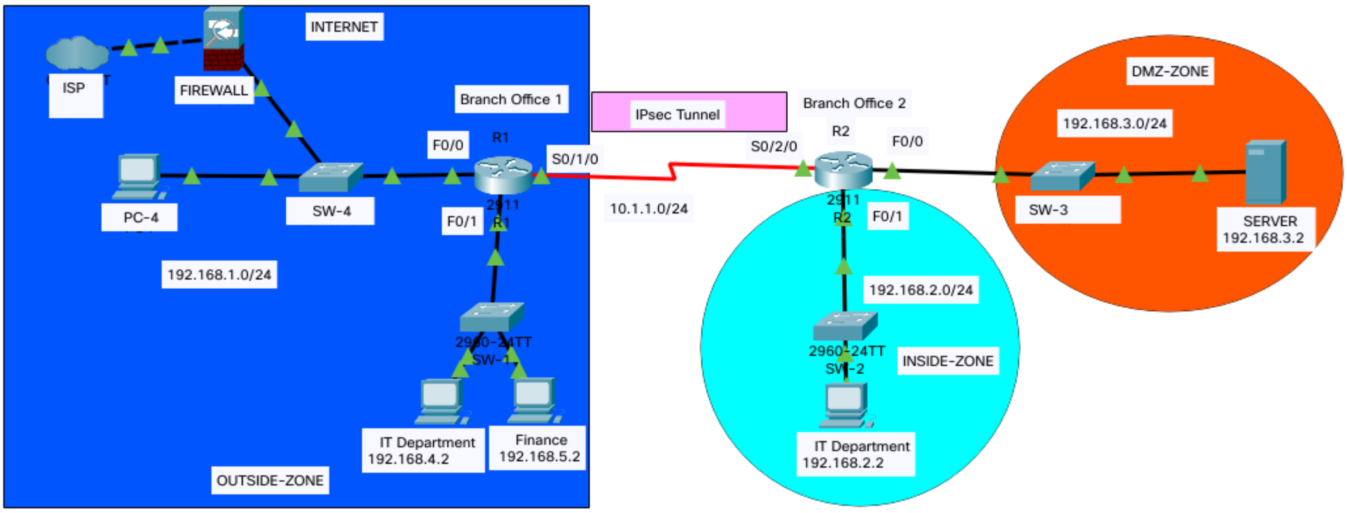


Figure 1 Network Topology

The above topology is an illustration of actual topology implemented in lab. The hardware devices used to build the network in lab are as follows:

- 2 cisco 2800 series router
- 4 cisco catalyst 2960 switch
- 4 PC

4. Configuration

As it can be seen from the topology the following things are implemented in it:

- Basic configuration of routers and network addresses.
- Zone based policy firewall.
- Site-to-site access IPsec VPN between R1 and R2.
- Switch configuration.
- Router configuration.

4.1 Basic configuration:

On Branch office 2 router R2:

- Assigned an ip address on Fa0/0 as 192.168.3.1 255.255.255.0 and turned it on, for 192.168.3.0/24 this interface will be gateway. The server available on this interface has given address 192.168.3.2.
- Assigned an ip address on Fa0/1 as 192.168.2.1 255.255.255.0 and turned it on, for 192.168.2.0/24 this interface will be gateway. The PC available on this interface has given ip address 192.168.2.2.
- Assigned an ip address on S0/2/0 as 10.1.1.2 255.255.255.0 and turned it on.

On Branch office 1 router R1

- Interface Fa0/0 gets the ip address from DHCP in the 192.168.1.0/24 range.
- Assigned an ip address on S0/1/0 as 10.1.1.1 255.255.255.0 and turned it on.

4.2 Configuring router information protocol:

- In the topology Branch office 1 and 2 routers should know the networks connected with them, for this purpose we have implemented RIP protocol as follows:

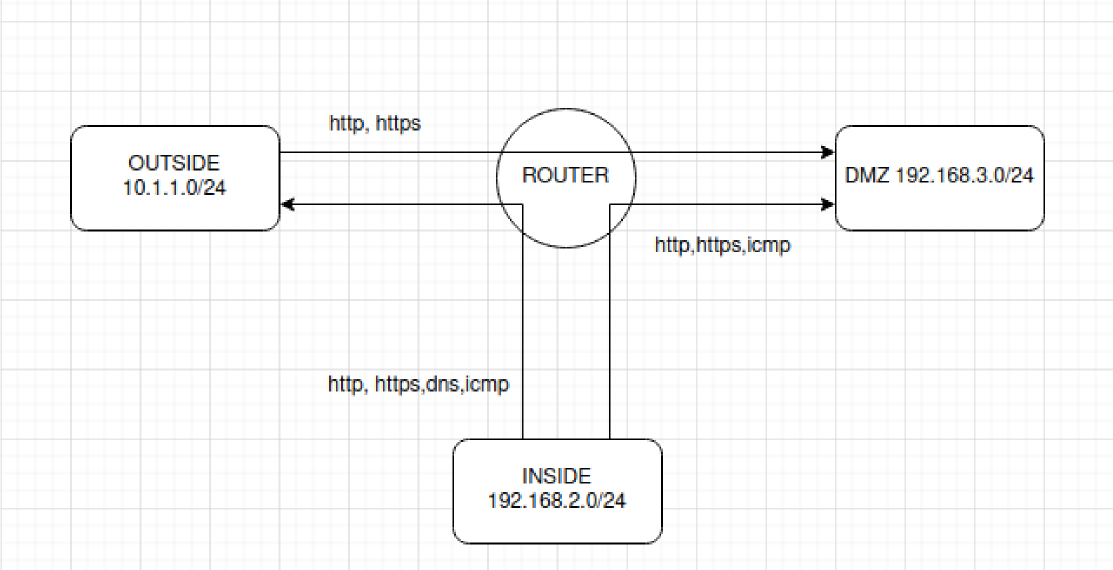
```
R1(config)#router rip
R1(config-router)#network 192.168.4.0
R1(config-router)#network 192.168.5.0
R1(config-router)#network 10.1.1.0

R1(config)#router rip
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.2.0
R1(config-router)#network 10.1.1.0
```

4.3 Zone based policy firewall:

- The Branch office 2 does not have a firewall, so we need to implement ZPF on router R2.
- The ZPF deals with the security zones, where we can assign the router interfaces to various security zones. The traffic will be dynamically inspected as it passes through zones. ZPF makes it easy to implement the security by assigning the zones.
  a) Configuration of zones
  b) Assigning router interfaces to zones
  c) Create zone pairs
  d) Configure inter-zone access policies(class-map and policy-map)
  e) Apply policy maps to zone pairs

Configuration scenario:



In this example we have three zones:

- Inside zone – Private LAN
- DMZ zone – DMZ host
- Outside zone – Internet

Here the rule defined are as follows:

- From INSIDE to OUTSIDE – http, https, dns, icmp is allowed.
- From INSIDE to DMZ – http, https, dns, icmp is allowed.
- From OUTSIDE to DMZ – http, https, icmp is allowed.

i. Configuring zones
Three zones INSIDE, OUTSIDE, DMZ are configured using the following command on cisco IOS router.

```
R2(config)# zone security INSIDE
R2(config)# zone security OUTSIDE
R2(config)# zone security DMZ
```

ii. Assigning router interfaces to zones
Here in this topology router interface Fa0/1 is assigned to INSIDE zone, Fa0/0 is assigned to DMZ zone, S0/2/0 is assigned to OUTSIDE zone.

iii. Create zone pairs
If we want two zones to communicate we have to create zone pairs. In the above scenario the traffic flows between:

- INSIDE to OUTSIDE
- INSIDE to DMZ
- OUTSIDE to DMZ

We have created three zone pairs using the following command:

Zone-pair security zone-pair-name source {source-zone-name | self} destination {destination-zone-name | self}

```
R2(config)# zone-pair security IN-OUT source INSIDE destination OUTSIDE
```

```
R2(config)# zone-pair security IN-DMZ source INSIDE destination DMZ
```

```
R2(config)# zone-pair security OUT-DMZ source OUTSIDE destination DMZ
```

iv. Configure inter-zone access policies (Class-map and policy-map)
Here we classify the traffic and apply the firewall policies. Class-map and Policy-map configurations are carried out in this task.
Class-map: This classifies the traffic.
Policy-map: This decides the action of the traffic.

Class-map configuration:
Calss-map sort out the traffic using access-group, protocols. Here we are going to define
ACL, protocols to associate it with class-map.

a) For OUTSIDE to DMZ we are creating an ACL as follows

```
R2(config)# ip access-list extended DMZ_ACL
R2(config-ext-nacl)#permit tcp any 192.168.3.0 0.0.0.255 eq www
R2(config-ext-nacl)#permit tcp any 192.168.3.0 0.0.0.255 eq 443
R2(config-ext-nacl)#permit icmp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R2(config-ext-nacl)#permit tcp any eq www 192.168.3.0 0.0.0.255
R2(config-ext-nacl)#permit tcp any eq 443 192.168.3.0 0.0.0.255
```

The above ACL is implemented for the communication between OUTSIDE to DMZ and the class-map will be as follows:

```
R2(config)# class-map type inspect match-any OUT-DMZ
R2(config-cmap)# match access-group DMZ_ACL
```

b) For INSIDE to OUTSIDE we are matching the protocols inside the class-map.

```
R2(config)# class-map type inspect match-any HTTP_TRAFFIC
R2(config-cmap)# match protocol http
R2(config-cmap)# match protocol https
R2(config-cmap)# match protocol dns
R2(config-cmap)# match protocol icmp
```

c) For INSIDE to DMZ we are using the same class-map defined as HTTP_TRAFFIC

Policy-map configuration:
Policy-maps will apply the firewall policy to the class-map that is configured previously. Three actions can be taken using policy-map; inspect, drop, pass we are using inspect.

a) Policy-map for OUTSIDE to DMZ

```
R2(config)# policy-map type inspect OUT-DMZ-POLICY
R2(config-pmap)# class type inspect OUT-DMZ
```

```
R2(config-pmap)# inspect
R2(config-pmap)# class class-default
```

b) Policy-map for INSIDE to OUTSIDE

```
R2(config)# policy-map type inspect IN-OUT-POLICY
R2(config-pmap)# class type inspect HTTP_TRAFFIC
R2(config-pmap)# inspect
R2(config-pmap)# class class-default
```

c) Policy-map for INSIDE to DMZ

```
R2(config)# policy-map type inspect IN-DMZ -POLICY
R2(config-pmap)# class type inspect HTTP_TRAFFIC
R2(config-pmap)# inspect
R2(config-pmap)# class class-default
```

v. Apply policy maps to zone pairs

Here the previously created policy-maps are attached to the zone pairs as follows:

a)
```
R2(config)# zone-pair security OUT-DMZ source OUTSIDE destination DMZ
R2(config-sec-zone-pair)# service-policy type inspect OUT-DMZ-POLICY
```

b)
```
R2(config)# zone-pair security IN-OUT source INSIDE destination OUTSIDE
R2(config-sec-zone-pair)# service-policy type inspect IN-OUT –POLICY
```

c)
```
R2(config)# zone-pair security IN-OUT source INSIDE destination DMZ
R2(config-sec-zone-pair)# service-policy type inspect IN-DMZ-POLICY
```

4.4 Site-to-site access IPsec VPN between R1 and R2:

The VPN between R1 and R2 is implemented using the 4 steps as follows:

i. Create an interesting traffic
ii. ISAKMP policy phase 1
iii. ISAKMP policy phase 2
iv. Create a crypto-map
v. Applying crypto-map on an interface

All the above mentioned five steps need to be implemented on both R1 and R2 of our topology.

i. Create an interesting traffic on R1: In this step the interesting traffic which is to be encrypted while transferring from source to destination is defined.

```
R1(config)#access-list 105 permit ip host 192.168.4.1 host 192.168.2.1
```

Create an interesting traffic on R2:

```
R2(config)#access-list 106 permit ip host 192.168.2.1 host 192.168.4.1
```

ii. ISAKMP policy phase 1 on R1: In this step the ISAKMP policy lists the security associations (SAs) that the router is willing to use to establish the IKE Phase 1 tunnel. The SAs are consists of encryption standard, hash type, authentication type, Diffie-hellman group, lifetime. In order to establish connection the SAs should be same on the both sides.

```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# lifetime 1800
R1(config-isakmp)# end
```

The pre-share key is as follows:

```
R1(config)#crypto isakmp key vpnpass address 10.1.1.2
```

ISAKMP policy phase 1 on R2:

```
R2(config)# crypto isakmp policy 1
R2(config-isakmp)# encryption aes 256
R2(config-isakmp)# hash sha
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 5
R2(config-isakmp)# lifetime 1800
R2(config-isakmp)# end
```

The pre-share key is as follows:

```
R2(config)#crypto isakmp key vpnpass address 10.1.1.1
```

iii. ISAKMP policy phase 2 on R1: In this step the set of encryption and hashing that will be used to transform the data through IPsec tunnel is set. During the phase 2 negotiations, the peers agree on the IPsec transform set to be used for protecting interesting traffic.

```
R1(config)# crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac
```

ISAKMP policy phase 2 on R2:

```
R2(config)# crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac
```

iv. Create a crypto-map on R1: Now that the interesting traffic is defined, and an IPsec transform set is configured, it is time to bind those configurations with the rest of the IPsec policy in a crypto map.

```
R1(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R2
R1(config-crypto-map)# match address 105
R1(config-crypto-map)# set transform-set R1-R2
R1(config-crypto-map)# set peer 10.1.1.1
R1(config-crypto-map)# set pfs group5
R1(config-crypto-map)# set security-association lifetime seconds 1000
```

Create a crypto-map on R2:

```
R2(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
```

```
R2(config-crypto-map)# description VPN connection to R1
R2(config-crypto-map)# match address 106
R2(config-crypto-map)# set transform-set R1-R2
R2(config-crypto-map)# set peer 10.1.1.2
R2(config-crypto-map)# set pfs group5
R2(config-crypto-map)# set security-association lifetime seconds 1000
```

v. Applying crypto-map on an interface for R1: To apply the crypto map, enter interface configuration mode for the outbound interface and configure the crypto map.

```
R1(config)#interface S0/1/0
R1(config-if)#crypto map R1-R2_MAP
```

Applying crypto-map on an interface for R2:

```
R2(config)#interface S0/2/0
R2(config-if)#crypto map R1-R2_MAP
```

4.5 NAT implementation on router:

- On branch office 1 router interface Fa0/1 to translate inside local address to inside global address and from interface S0/1/0 to translate into inside global addresses. we need to implement NAT on R1. And for public network DMZ should be accessible for that, we need static NAT on R1.
- We have sub-interfaces on Fa0/1 as Fa0/1.20 for 192.168.4.0/24 network, Fa0/1.30 for 192.168.5.0/24 network and Fa0/1.99 for native.
- All the address will be overloaded on interface Fa0/0 which gets the ip address from dhcp.

a)
```
R1(config)#interface Fa0/1.20
R1(config-if)#encapsulation dot1Q 20
R1(config-if)# ip address 192.168.4.1 255.255.255.0
R1(config-if)#ip nat inside
```

b)
```
R1(config)#interface Fa0/1.30
R1(config-if)#encapsulation dot1Q 30
R1(config-if)# ip address 192.168.5.1 255.255.255.0
R1(config-if)#ip nat inside
```

c)
```
R1(config)#interface Fa0/1.99
R1(config-if)#encapsulation dot1Q 99 native
```

d)
```
R1(config)#interface Fa0/0
R1(config-if)#ip address dhcp
R1(config-if)#ip nat outside
```

e)
```
R1(config)#interface S0/1/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)#ip nat inside
```

f) Now for address translation one access-list is used here and we need static nat for outside to DMZ access.

```
R1(config)#access-list 10 permit 192.168.2.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.3.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.4.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.5.0 0.0.0.255

R1(config)#ip nat inside source list 10 interface Fa0/0 overload
R1(config)#ip nat inside source static tcp 192.168.3.2 80 interface Fa0/0 80
```

4.6 Switch configuration:

- On switch-1 connected to R1 two networks are connected 192.168.4.0/24 and 192.168.5.0/24 with separate VLAN20 & VLAN30 respectively, to make the both network communicate VLANS are made and G0/1 interface of switch is configured as Trunk. A trunk connection is simply said nothing more but a normal link but it is able to pass traffic from different VLANs and has a method to separate traffic between VLANs.
- Configuration of VLANs and assigning the switch interfaces to VLANs as follows:

a)
```
SW1(config)#vlan 20
SW1(config-vlan)#name testing
SW1(config)#vlan 30
SW1(config)#vlan 99
```

b)
```
SW1(config)#interface range Fa0/1 – 12
SW1(config-if-range)#switchport access vlan 20
```

c)
```
SW1(config)#interface range Fa0/13 – 24
SW1(config-if-range)#switchport access vlan 30
```

d)
```
SW1(config)#interface G0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 99
SW1(config-if)#switchport trunk allowed vlan 20,30
```

- Now after dealing with VLANs and Trunk we have implemented Port-security and port-fast on the switch SW1. Port-security makes it sure not to accept the connection from more than certain number of PC mac-addresses or defined PC mac-addresses. If new PC with mac-address tries to connect the port it results in violation shutdown mode and the port gets shutdown. To enable immediate transition into the forwarding state, we enabled the STP port fast feature.

a)
```
SW1(config)# interface range Fa0/1 – 12
SW1(config-if-range)# switchport mode access
SW1(config-if-range)# spanning-tree portfast
SW1(config-if-range)# switchport port-security
SW1(config-if-range)# switchport port-security maximum 4
```

```
SW1(config-if-range)# switchport port-security mac-address sticky
SW1(config-if-range)# switchport port-security violation shutdown
```

b)

```
SW1(config)# interface range Fa0/13 – 24
SW1(config-if-range)# switchport mode access
SW1(config-if-range)# spanning-tree portfast
SW1(config-if-range)# switchport port-security
SW1(config-if-range)# switchport port-security maximum 4
SW1(config-if-range)# switchport port-security mac-address sticky
SW1(config-if-range)# switchport port-security violation shutdown
```

4.6 Router configuration:

- The router R1 and R2 assigned with an IP addresses and since on R1 Fa0/1 interfaces there are two VLANs connected to switch the sub-interfaces are configured. Routers have privilege level 15 user as admin with secret password.

a)

```
R1(config)#username admin privilege 15 secret cisco
```

b)

```
R1(config)#interface Fa0/1.20
R1(config-if)#encapsulation dot1Q 20
R1(config-if)# ip address 192.168.4.1 255.255.255.0
R1(config-if)#no shutdown
```

c)

```
R1(config)#interface Fa0/1.30
R1(config-if)#encapsulation dot1Q 30
R1(config-if)# ip address 192.168.5.1 255.255.255.0
R1(config-if)#no shutdown
```

d)

```
R1(config)#interface Fa0/1.99
R1(config-if)#encapsulation dot1Q 99 native
R1(config-if)#no shutdown
```

e)

```
R1(config)#interface Fa0/0
R1(config-if)#ip address dhcp
R1(config-if)#no shutdown
```

f)

```
R1(config)#interface S0/1/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)#no shutdown
```

g)

```
R2(config)#username admin privilege 15 secret cisco
```

h)

```
R2(config)#interface Fa0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
```

i)

```
R2(config)#interface Fa0/0
R2(config-if)# ip address 192.168.3.1 255.255.255.0
```

```
R2(config-if)#no shutdown
```

j)

```
R2(config)#interface S0/2/0
R2(config-if)#ip address 10.1.1.2 255.255.255.0
R2(config-if)#no shutdown
```

5. Future implementation:

- The hosts connected to the router can get the addresses from dhcp server.
- The router and switches can be managed remotely.
- Two separate servers for authentication accounting and authorization at both branch offices can be implemented.
- Snort can be enabled on routers to detect the signature attacks.