

**How to configure Cisco IOS Zone Based Firewall**

How to create Zones

To create three Zones, "INSIDE", "OUTSIDE" and "DMZ", follow these configuration steps.

Aptech1#configure terminal

Aptech1(config)#zone security INSIDE

Aptech1(config-sec-zone)#exit

Aptech1(config)#zone security OUTSIDE

Aptech1(config-sec-zone)#exit

Aptech1(config)#zone security DMZ

Aptech1(config-sec-zone)#exit

Aptech1(config)#exit

Aptech1#

How to assign IP addresses and apply interfaces to zones

Aptech1#configure terminal

Aptech1(config)#interface gigabitEthernet 0/0

Aptech1(config-if)#ip address 172.16.0.1 255.255.0.0

Aptech1(config-if)#no shutdown

Aptech1(config-if)#zone-member security INSIDE

Aptech1(config-if)#exit

Aptech1(config)#exit

Aptech1#

Aptech1#configure terminal

Aptech1(config)#interface gigabitEthernet 1/0

Aptech1(config-if)#ip address 192.168.15.1 255.255.255.0

Aptech1(config-if)#no shutdown

Aptech1(config-if)#zone-member security DMZ

Aptech1(config-if)#exit

Aptech1(config)#exit

Aptech1#

Aptech1#configure terminal

Aptech1(config)#interface gigabitEthernet 2/0

Aptech1(config-if)#ip address 122.175.156.1 255.255.255.0

Aptech1(config-if)#no shutdown

Aptech1(config-if)#zone-member security OUTSIDE

Aptech1(config-if)#exit

Aptech1(config)#exit

Aptech1#

Create Zone Pairs and specify the direction of traffic

In this example, we are going to create only one Zone pair, having its direction from "INSIDE" to "OUTSIDE". To create a Zone pair with direction from "INSIDE" to "OUTSIDE", follow these steps.

Please visit the following link to learn what are Zones and Zone Pairs.

Aptech1#configure terminal

Aptech1(config)#zone-pair security IN-to-OUT source INSIDE destination OUTSIDE

Aptech1(config-sec-zone-pair)#exit

Aptech1(config)#exit

Aptech1#

How to create Interzone Firewall Access Policy

Cisco IOS Zone Based Firewall Access Policies are made using class maps, policy maps and service policies. Please visit following link to learn what are class maps, policy maps and service policies.

Class maps are used to identify the traffic. To create a class map to match protocols HTTP, HTTPS, FTP and ICMP follow these steps.

Aptech1#configure terminal

Aptech1(config)#class-map type inspect match-any OMNISECU-CMAP-IN-to-OUT

Aptech1(config-cmap)#match protocol http

Aptech1(config-cmap)#match protocol https

Aptech1(config-cmap)#match protocol ftp

Aptech1(config-cmap)#match protocol dns

Aptech1(config-cmap)#match protocol icmp

Aptech1(config-cmap)#exit

Aptech1(config)#exit

Aptech1#

Above configuration steps create a class-map "APTECHDL-CMAP-IN-to-OUT", which matches the network traffic HTTP, HTTPS, FTP, DNS and ICMP.

match-any and match-all are the two configuration parameters used in class-map configuration. match-any is used to match any of the criteria in the class map. match-all is used to match all the criteria in the class map. If we specify match-all in above class-map configuration there will not be a match, because there is no traffic which match HTTP, HTTPS, FTP, DNS and ICMP together.

Policy maps are used to define what we want to do with the traffic identified using Class map. To create a Policy map to inspect the HTTP, HTTPS, FTP DNS and ICMP traffic (which are identified using Class map in previous steps), follow these steps.

Aptech1#configure terminal

Aptech1(config)#policy-map type inspect OMNISECU-PMAP-IN-to-OUT

Aptech1(config-pmap)#class type inspect OMNISECU-CMAP-IN-to-OUT

Aptech1(config-pmap-c)#inspect

Aptech1(config-pmap-c)#exit

Aptech1(config-pmap)#exit

Aptech1(config)#exit

Aptech1#

Please note that "inspect" command is used to configure stateful inspection, which will allow the matching return traffic. If stateful inspection is configured, there is no need to create another policy in opposite direction, because the matching traffic is allowed.

Finally, create a service policy and apply the Policy map inside the Zone pair along its direction. Zone based Firewall is uni-directional. To create Service policy, follow these steps.

Aptech1#configure terminal

Aptech1(config)#zone-pair security IN-to-OUT s source INSIDE destination OUTSIDE

Aptech1(config-sec-zone-pair)#service-policy type inspect OMNISECU-PMAP-IN-to-OUT

Aptech1(config-sec-zone-pair)#exit

Aptech1(config)#exit

Aptech1#f