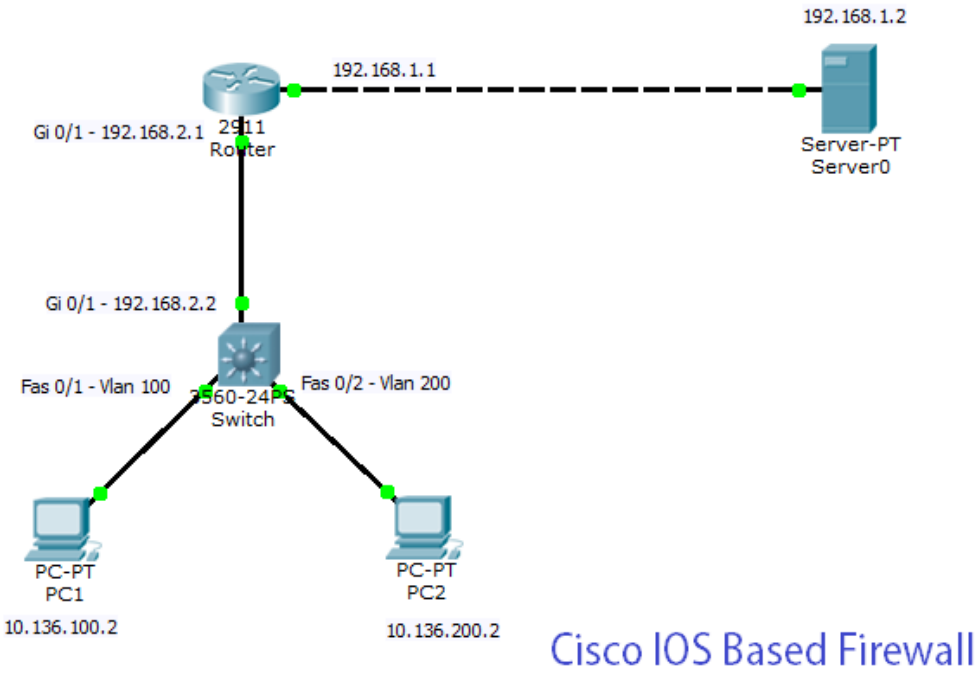
Cisco IOS Zone Based Firewall

Cisco IOS based firewall available in Cisco IOS starting from 12.4(6)T or later . IOS Zone based firewalls are similar to classic zone based firewalls. Router interfaces are put into zones and traffic between same zones is allowed by default .However traffic between the zones is blocked. We need to configure the policy to allow traffic between zones. Zone policies are configured using Class Based Policy Language which is similar to Modular QoS Command line interface.

Configuring Zone Based Firewalls on Cisco IOS.

We will use below diagram to configure the Zone based firewalls on Cisco IOS.



Cisco IOS Based Firewall

We have configured the basic IP connectivity and used static routing on router . PC1 is in sales Vlan and PC2 is in Marketing Vlan as under:

Server Configuration:

IP Address :192.168.1.2

Services : http, ftp.

Router Configuration:

```
interface GigabitEthernet0/0
description Connected to Server
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
description Connected to Switch
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
ip route 10.136.100.0 255.255.255.0 192.168.2.2
ip route 10.136.200.0 255.255.255.0 192.168.2.2
```

Switch Configuration

```
interface FastEthernet0/1
description sales
switchport access vlan 100
switchport mode access
!
interface FastEthernet0/2
description marketing
switchport access vlan 200
switchport mode access
interface GigabitEthernet0/1
no switchport
ip address 192.168.2.2 255.255.255.0
duplex auto
speed auto
interface Vlan100
ip address 10.136.100.1 255.255.255.0
!
interface Vlan200
ip address 10.136.200.1 255.255.255.0
!
```

ip classless
ip route 0.0.0.0 0.0.0.0 192.168.2.1
Now for configuring Zone based Firewall, our requirement is like this:

1. Only http access to server (192.168.1.2) should be allowed from PC1.

2. Ping should be allowed from both PC's .

3. FTP should be only working from PC2.

Router Configuration:
Zone security LAN
Description LAN ZONE
Zone security WAN
Description WAN ZONE
interface gi 0/0
zone-member security WAN
interface gi 0/1
zone-member security LAN
Define access lists:
ip access-list extended LAN_SALES
permit ip 10.136.100.0 0.0.0.255 any
ip access-list extended LAN_MARK
permit ip 10.136.200.0 0.0.0.255 any
Define class map and necessary action:
class-map type inspect match-all server_http
match access-group name LAN_SALES
match protocol http
class-map type inspect match-all server_ftp
match access-group name LAN_MARK
match protocol ftp
class-map type inspect match-all server_icmp
match access-group name LAN_SALES
match access-group name LAN_MARK
match protocol icmp
Next we need to create the policy Maps:
policy-map type inspect Lan_Wan
class type inspect server_http
inspect

class type inspect server_ftp
inspect
class type inspect server_icmp
inspect
Note Inspect command or action, we tell the router which class-map to look for the interesting traffic. Also at the end of each policy map there is a class-default which drops all other traffic

Next we need to assign the policy to the zone pair

zone-pair security internal source LAN destination WAN
service-policy type inspect Lan_Wan