**CISCO Adaptive security appliance (ASA)**

A firewall is a network security system which takes actions on the ingoing or outgoing packets based on the defined rules on the basis of IP address, port numbers. Cisco calls its firewall as Adaptive Security Appliance (ASA). The Cisco Adaptive Security Appliance (ASA) is an advanced network security device that integrates a stateful firewall, VPN, and other capabilities.

**The Cisco ASA 5500 series has models:**

Cisco ASA 5505, Cisco ASA 5510, Cisco ASA 5515-X, Cisco ASA 5520, Cisco ASA 5525-X, Cisco ASA 5540, Cisco ASA 5550, Cisco ASA 5555-X, Cisco ASA 5585-X.

**The ASA creates three security interfaces:**

1). Outside, 2). Inside, and 3). DMZ. It provides outside users limited access to the DMZ and no access to inside resources. Inside users can access the DMZ and outside resources.

**Adaptive Security Appliance (ASA) –**

ASA is Cisco security device that can perform basic firewall capabilities with VPN capabilities, antivirus and many other features. Some of the features of ASA are:

1. **Packet filtering –**

Packet filtering is a simple process of filtering the incoming or outgoing packet on the basis of rules defined on the ACL which has been applied to the device. It consists of various permit or deny conditions. If the traffic matches one of the rule, no other rule is matched and the matched rule is executed.

1. **Stateful filtering –**

By default, ASA performs stateful tracking of the packet if the packet is generated from higher security level to lower security level.

By default, if the traffic is initiated by the devices in higher security levels for lower security levels device (as destination), TCP and UDP reply traffic will be allowed and will able to, say, telnet the other device in Lower security level. This is because a stateful database is maintained (in which an entry about the source and destination device information such as IP address, port numbers are maintained) as stateful inspection is enabled by default.

1. **Routing support –**

ASA can perform static routing, Default routing also dynamic routing protocols like EIGRP, OSPF and RIP.

1. **Transparent firewall –**  
   ASA can operate in two modes:
   * ***Routed mode*:** In this mode, ASA acts like a layer 3 device (router hop) and needs to have two different IP address (means two different subnets) on its both interface.
   * ***Transparent mode*:** In this mode, ASA operates at layer 2 and only a single IP address is needed to manage ASA management purpose as both the interfaces (inside and outside) acts like a bridge.
2. **AAA support –**

ASA supports AAA services either using its local database or using a external server like ACS (Access Control Server).

1. **VPN support –**

ASA supports policy-bases VPNs like point-to-point IPsec VPN (site-to-site VPN and remote-access VPN) and SSL based VPNs.

1. **Supports IPv6 –**

ASA (new versions) supports IPv6 routing such as static, dynamic.

1. **VPN load Balancing –**

It is a Cisco proprietary feature of Cisco ASA. Multiple clients can be shared across multiple ASA units at the same time.

1. **Stateful failover –**

ASA supports high availability of pair of Cisco ASA devices. If one of the ASA goes down, the other ASA device will perform the operations without any interruption. When stateful failover is enabled, the active unit continuously passes connection state information to the backup device. After the failover occurs, same connection information is available on the new active unit.

1. **Clustering –**

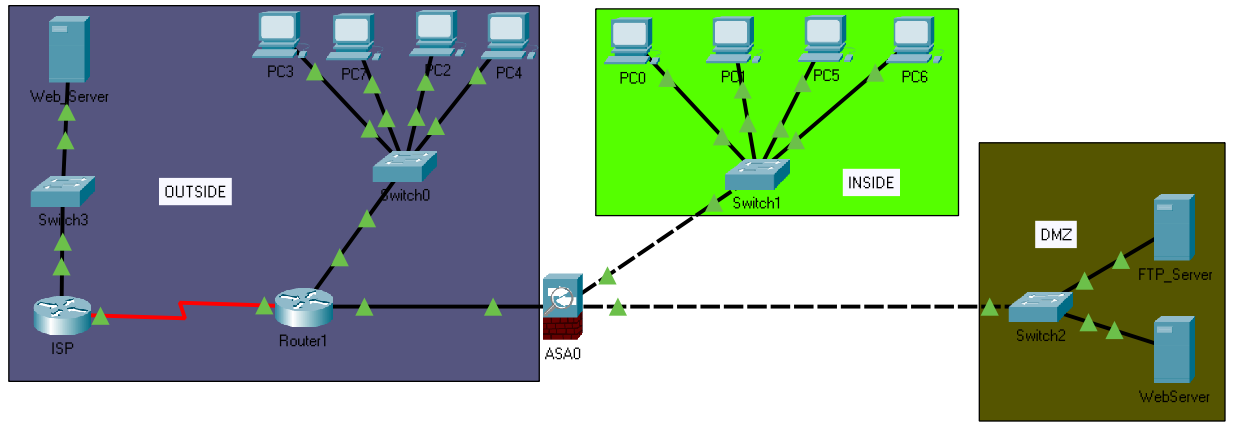
Cisco ASA let’s us configure multiple ASA devices as a single logical device. cluster can consists of maximum 8 cohesive units. This results in high throughput and at the same time, provides redundancy.

1. **Advance Malware Protection (AMP) –**

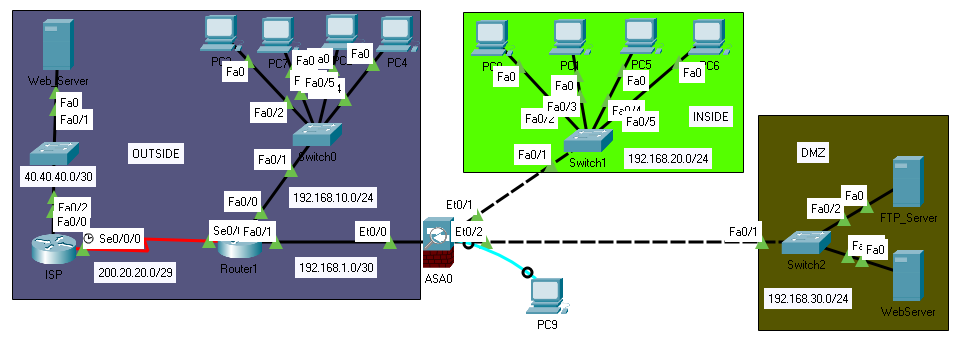
Cisco ASA provides support for Next-Generation firewall features which can provide protection advanced malware protection in a single device as the classic firewall features are combined with NGFWs features.

1. **Modular Policy Framework (MPF) –**

MPF is used to define policies for different traffic flows. Its used in ASA to utilize advanced firewall features like QOS, Policing, prioritising etc.  
For using MPF, we define Class-map for identifying the type of traffic, policy-map for identifying what action should be taken like prioritize and service-policy for where it should be applied.



The focus of this lab is the configuration of the ASA as a basic firewall. Other devices will receive minimal configuration to support the ASA portion of this lab. This lab uses the ASA CLI, which is similar to the IOS CLI, to configure basic device and security settings.



ciscoasa(config)#hostname PNTL

PNTL(config)#domain-na

PNTL(config)#domain-name peoplentech.com

PNTL(config)#ena

PNTL(config)#enable pas

PNTL(config)#enable password 1234

PNTL(config)#clock set 19:02:00 July 06 2021

PNTL(config)#interface gigabitEthernet 1/1

PNTL(config-if)#ip address 192.168.1.1 255.255.255.0

PNTL(config-if)#nameif outside

INFO: Security level for "outside" set to 0 by default.

PNTL(config-if)#security-level 0

PNTL(config-if)#no shutdown

PNTL(config)#interface gigabitEthernet 1/2

PNTL(config-if)#ip address 192.168.20.1 255.255.255.0

PNTL(config-if)#nameif inside

INFO: Security level for "inside" set to 100 by default.

PNTL(config-if)#security-level 100

PNTL(config-if)#no shutdown

PNTL(config)#interface gigabitEthernet 1/3

PNTL(config-if)#ip address 192.168.30.1 255.255.255.0

PNTL(config-if)#nameif dmz

INFO: Security level for "dmz" set to 0 by default.

PNTL(config-if)#security-level 70

PNTL(config-if)#no shutdown

PNTL(config)#dhcpd address 192.168.20.5-192.168.20.30 inside

PNTL(config)#dhcpd dns 8.8.8.8

PNTL(config)#dhcpd enable inside

PNTL(config)#route outside 0.0.0.0 0.0.0.0 192.168.1.2

PNTL(config)#object network ccna

PNTL(config-network-object)#subnet 192.168.20.0 255.255.255.0

PNTL(config-network-object)#nat (inside,outside) dynamic interface

PNTL(config)#object network dmz-server

PNTL(config-network-object)#subnet 192.168.30.0 255.255.255.0

PNTL(config-network-object)#nat (dmz,outside) dynamic interface

PNTL(config)# object network ex-ip

PNTL(config-network-object)# host 50.50.50.1

PNTL(config)# object network web

PNTL(config-network-object)# host 192.168.30.3

PNTL(config-network-object)# nat (dmz,outside) static 50.50.50.1

mahmud(config)#access-list OUTSIDE extended permit icmp any any echo-reply

mahmud(config)#access-list OUTSIDE extended permit icmp any any unreachable

mahmud(config)#access-list OUTSIDE extended permit tcp any object web eq www

mahmud(config)#access-list OUTSIDE extended permit tcp any host 50.50.50.1 eq www

mahmud(config)#access-list OUTSIDE extended permit ip any any

PNTL(config)# access-group OUTSIDE in interface outside