Lesson 8

Firewall

Outline

1. What is an intrusion?
2. Port security
3. DHCP snooping
4. WiFi Security
5. What are firewalls?
6. Types of Firewalls
7. Labs.

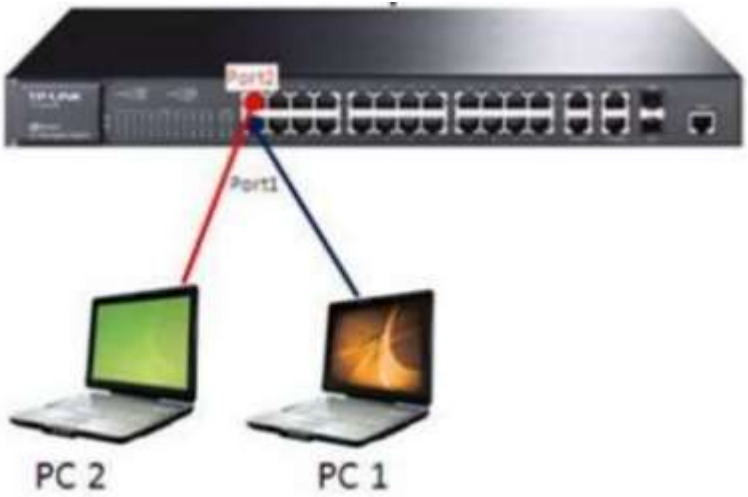
What is an intrusion?

- Intrusion can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of resource.

- In the context of info systems, intrusion refers to any unauthorized access, unauthorized attempt to access or damage or malicious use of info resources.

Port Security

● Secured ports restrict a port to a user-defined group of stations.



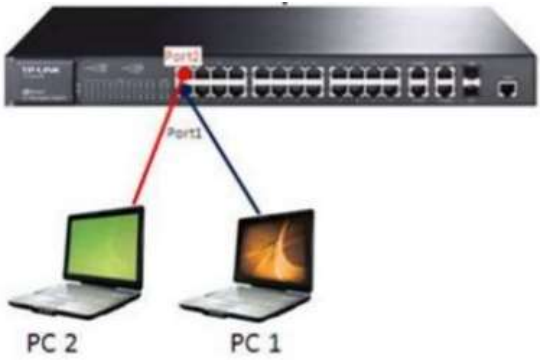
Port Security

Interface :Port to secure.

Security :Enable port security on the port.

Trap :Issue a trap when an address-security violation occurs.

Shutdown Port :Disable the port when an address-security violation occurs.



Port Security

- Commands:

SW(config)#interface Fa0/1

SW(config-if)#switchport mode access

SW(config-if)#switchport port-security

SW(config-if)#switchport port-security maximum 1

SW(config-if)#switchport port-security mac-address H.H.H | Sticky

SW(config-if)#switchport port-security violation shutdown

SW(config)#errdisable detect cause all

SW(config)#errdisable recovery cause all

SW(config)#errdisable recovery interval 30

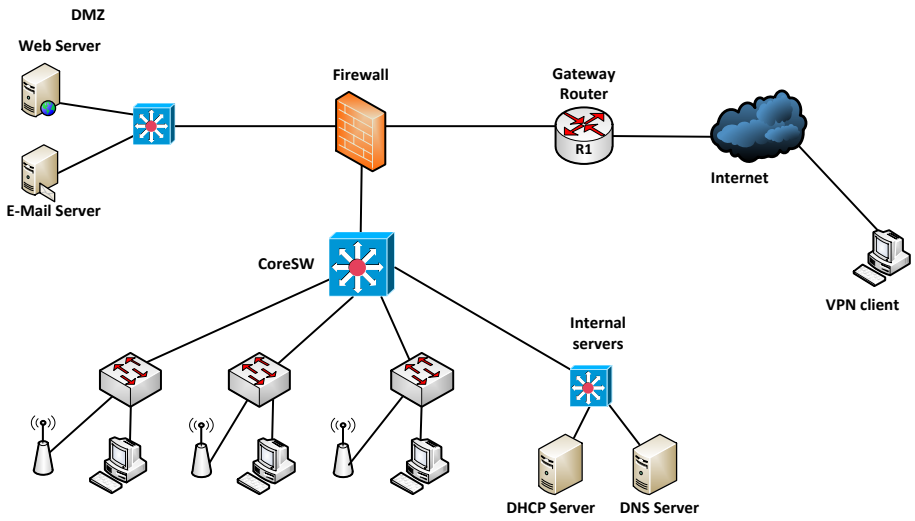
Lab 1: Port Security

DHCP Snooping

- To prevent a Man-in-the-middle attack on our network

- Fake DHCP Servers can respond to DHCPDISCOVER messages before the real server has time to respond.

- DHCP Snooping allows switches on the network to trust the port a DHCP server is connected to (this could be a trunk) and not trust the other ports.



DHCP Snooping

- Commands:

SW(config)#ip dhcp snooping

SW(config)#ip dhcp snooping vlan 1

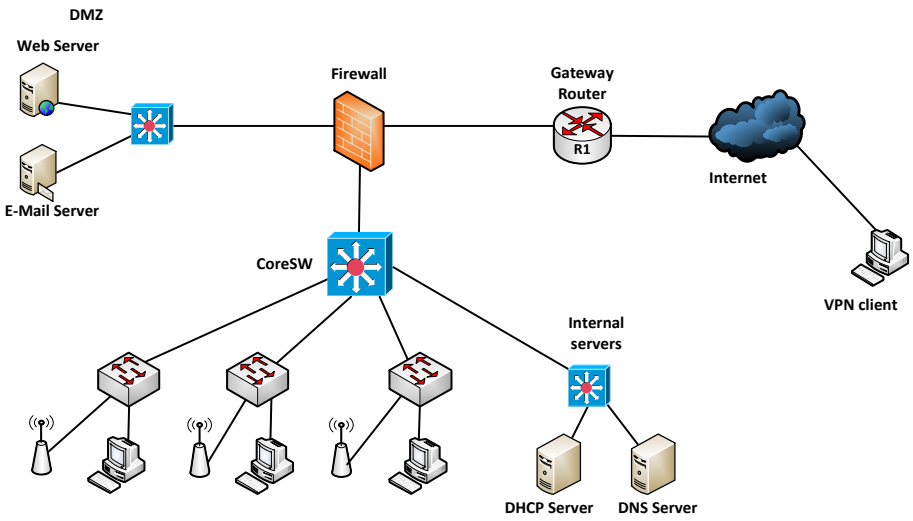
SW(config)#interface Fa0/1 → connect to real DHCP server

SW(config-if)#ip dhcp snooping trust

SW(config-if)#ip dhcp snooping limit rate 25

Verify the configuration:

SW#show ip dhcp snooping



Lab 2. DHCP Snooping

A Brief History of Wi-Fi Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Next Generation 802.11ax is also called "Wi-Fi 6"

Wi-Fi 6 is a "Generations" Approach similar to the Cellular Industry naming.

Telecommunications Industry "generations" 3G,4G,4GLTE, 5G…

IEEE
Advancing Technology for Humanity

Wi Fi 6™
CERTIFIED

802.11ax	**Wi-Fi 6**
802.11ac	Wi-Fi 5
802.11n	Wi-Fi 4

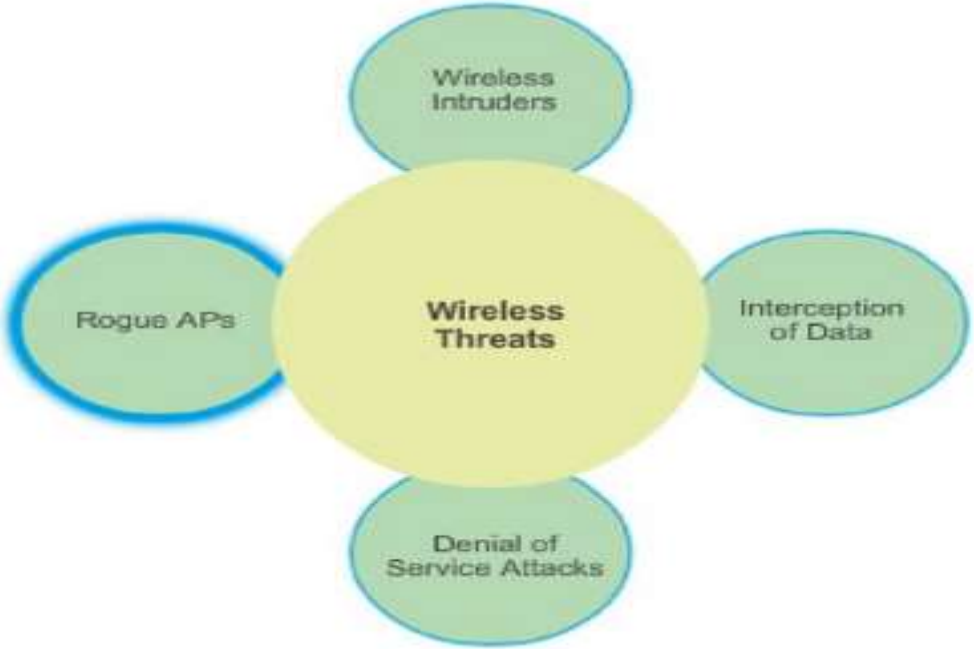
Note: 802.11ax and Wi-Fi 6 are interchangeable Engineering and Marketing Terms for same thing.

You may sometimes hear the term "HEW" High Efficiency Wireless also used.

Wireless Security Overview

- concerns for wireless security are similar to those found in a wired environment
- security requirements are the same:
  - confidentiality, integrity, availability, authenticity, accountability
  - most significant source of risk is the underlying communications medium

Wireless Network Threats



identity theft (MAC spoofing)

man-in-the middle attacks

denial of service (DoS)

Securing Wireless Transmissions

- principal threats are eavesdropping, altering or inserting messages, and disruption
- countermeasures for eavesdropping:
  - signal-hiding techniques
  - encryption
- the use of encryption and authentication protocols is the standard method of countering attempts to alter or insert transmissions

Securing Wireless Networks

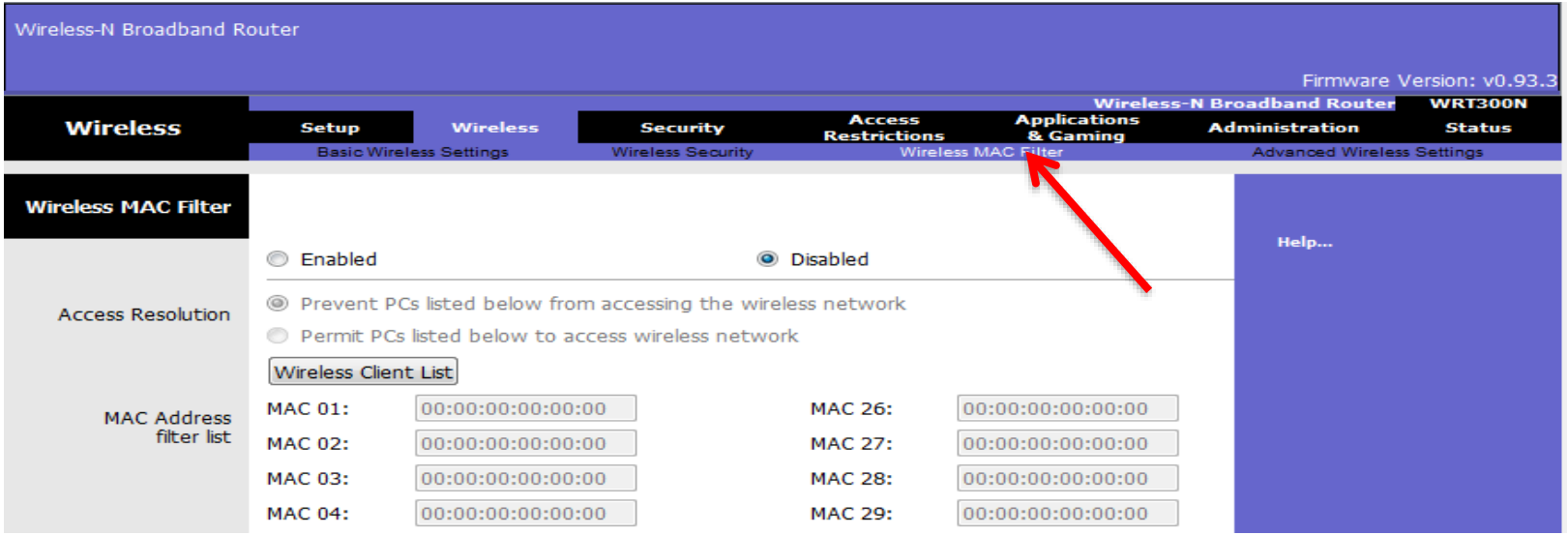
- the main threat involving wireless access points is unauthorized access to the network
- principal approach for preventing such access is the IEEE 802.1X standard for port-based network access control
  - provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
- use of 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

Wireless Security Techniques

- use encryption
- allow only specific computers to access your wireless network
- use anti-virus and anti-spyware software and a firewall
- change your router’s pre-set password for administration
- turn off identifier broadcasting
- change the identifier on your router from the default

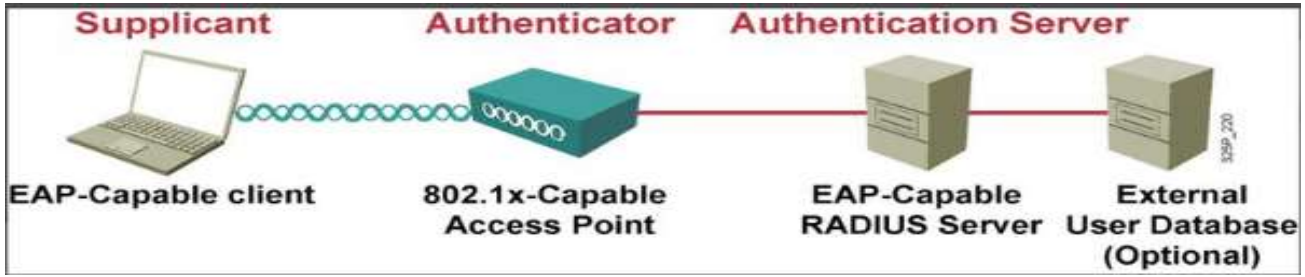
MAC Address filtering

- Method of limiting/controlling WLAN access
- Media Access Control (MAC) address filtering
  - Used by nearby all wireless AP vendors
  - Permits or blocks devices based on MAC address



WiFi Protect Access 2 (WPA2)

- Introduced in 2004
- Uses AES
- Support both PSK (personal) and 802.1x (enterprise) authentication



WPA3

- WPA3 is promising to improve security in multiple ways, over WPA2

Firewalls

- A part of computer system or network designed to stop unauthorized traffic flowing from one network to another.
- Separate trusted and untrusted components of a network.
- Differentiate networks within a trusted network.
- Main functionalities are filtering data, redirecting traffic and protecting against network attacks.

Requirements of a firewall

- All the traffic between trust zones should pass through firewall.
- Only authorized traffic, as defined by the security policy, should be allowed to pass through.
- The firewall itself must be immune to penetration, which implies using a hardened system with secured Operating Systems.

Firewall Policy

- User control: Controls access to the data based on the role of the user who is attempting to access it. Applied to users inside the firewall perimeter.
- Service control: Controls access by the type of service offered by the host. Applied on the basis of network address, protocol of connection and port numbers.
- Direction control: Determines the direction in which requests may be initiated and are allowed to flow through the firewall. It tells whether the traffic is “inbound” (From the network to firewall) or vice-versa “outbound”

Firewall actions

Accepted: Allowed to enter the connected network/host through the firewall.

Denied: Not permitted to enter the other side of firewall.

Rejected: Similar to “Denied”, but tells the source about this decision through ICMP packet.

Ingress filtering: Inspects the incoming traffic to safeguard an internal network and prevent attacks from outside.

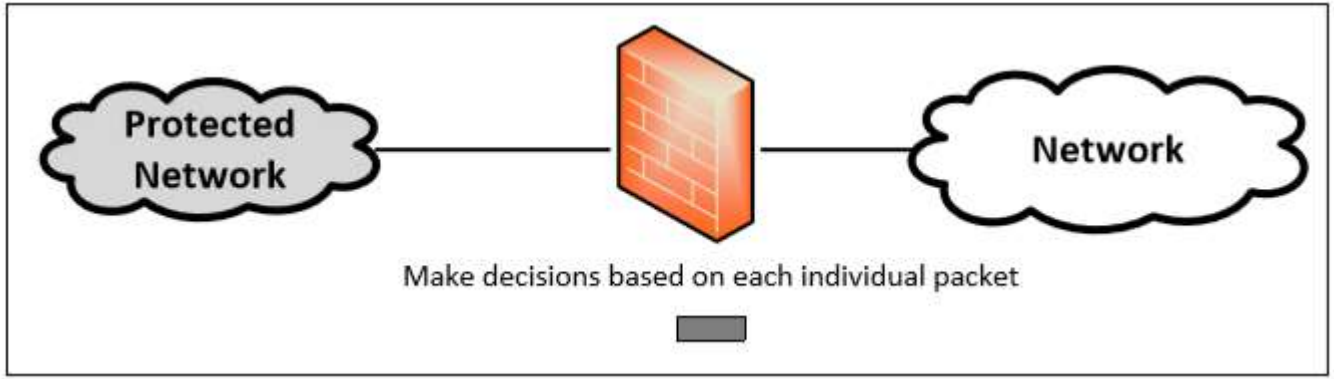
Egress filtering: Inspects the outgoing network traffic and prevent the users in the internal network to reach out to the outside network. For example like blocking social networking sites in school

Types of filters

Depending on the mode of operation, there are three types of firewalls :

- Packet Filter Firewall
- Stateful Firewall
- Application/Proxy Firewall

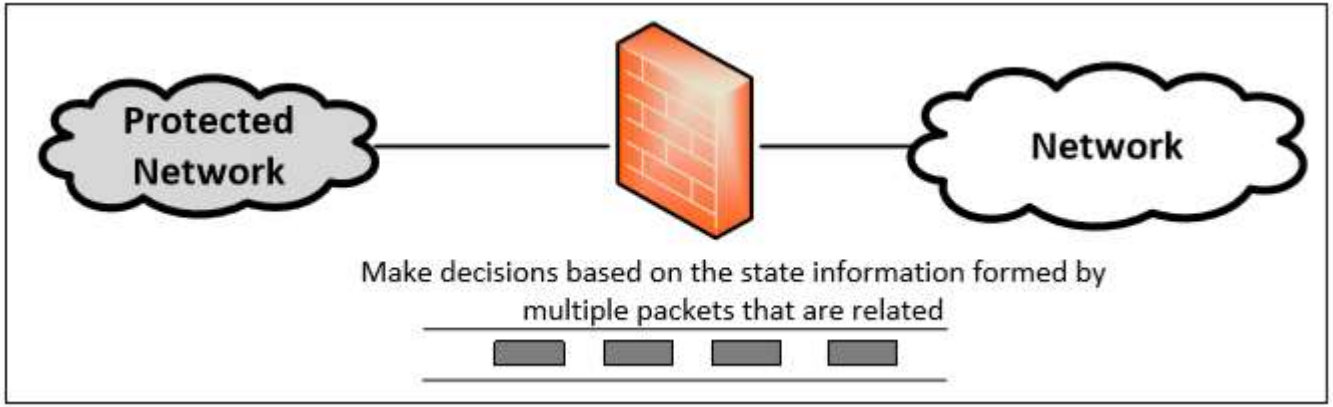
Packet Filter Firewall



- Controls traffic based on the information in packet headers, without looking into the payload that contains application data.

- Doesn’t pay attention to if the packet is a part of existing stream or traffic.
- Doesn’t maintain the states about packets. Also called Stateless Firewall.

Stateful Firewall

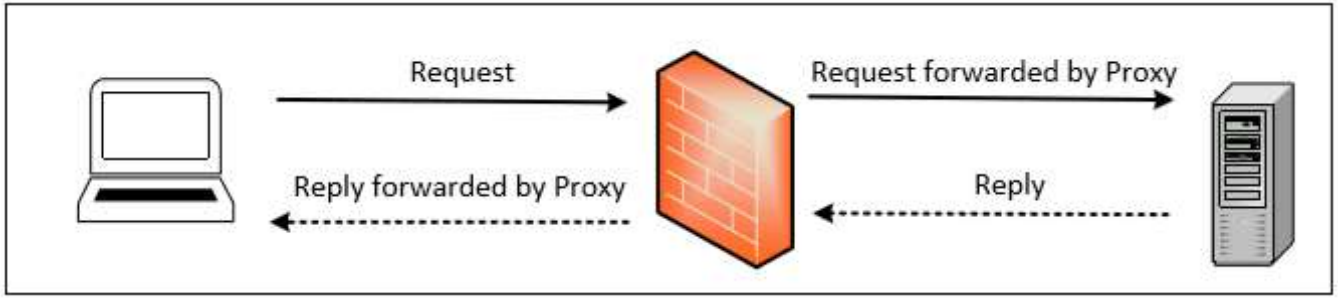


- Tracks the state of traffic by monitoring all the connection interactions until is closed.

- Connection state table is maintained to understand the context of packets.

- Example : Connections are only allowed through the ports that hold open connections.

Application/Proxy Firewall



- The client's connection terminates at the proxy and a separate connection is initiated from the proxy to the destination host.

- Data on the connection is analyzed up to the application layer to determine if the packet should be allowed or rejected.

- Controls input, output and access from/to an application or service.

- Acts an intermediary by impersonating the intended recipient.

Lab. FW

Configuring FW

Inside, Outside, DMZ

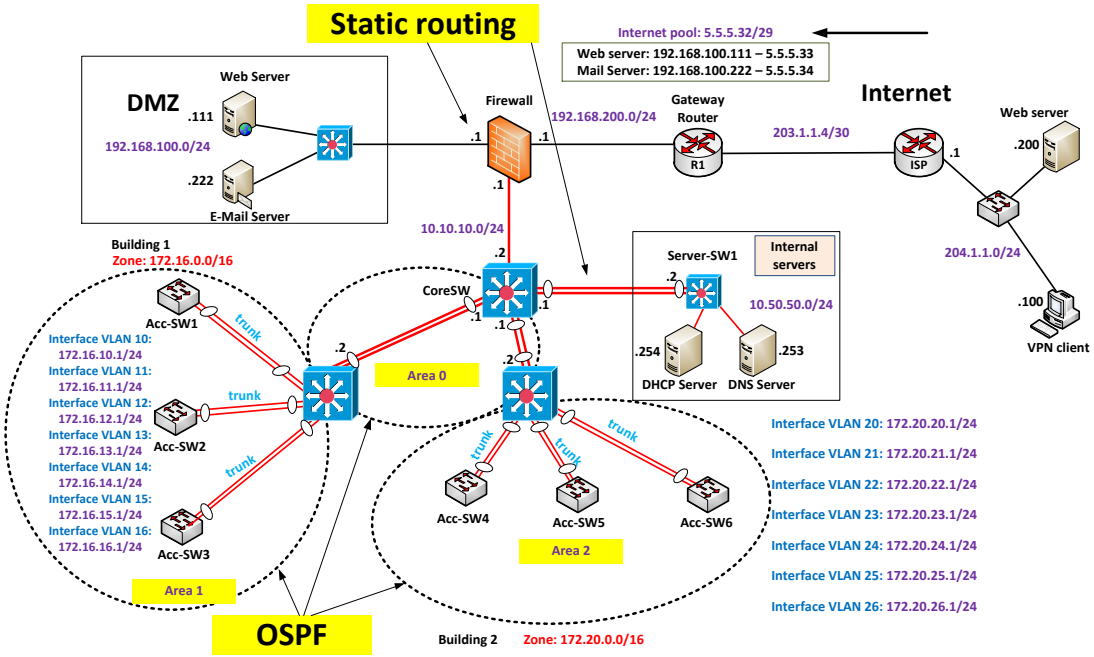
Step1. Configure interface

Int Gi1/1

nameif inside

security-level 100

.....



Step 2. Routing: ASA(config)#route inside 172.16.0.0 255.255.0.0 10.10.10.2

Step 3. Rules

#access-list allow-all permit ip any any

#access-group allow-all in interface inside

#access-group allow-all in interface outside

#access-group allow-all in interface dmz