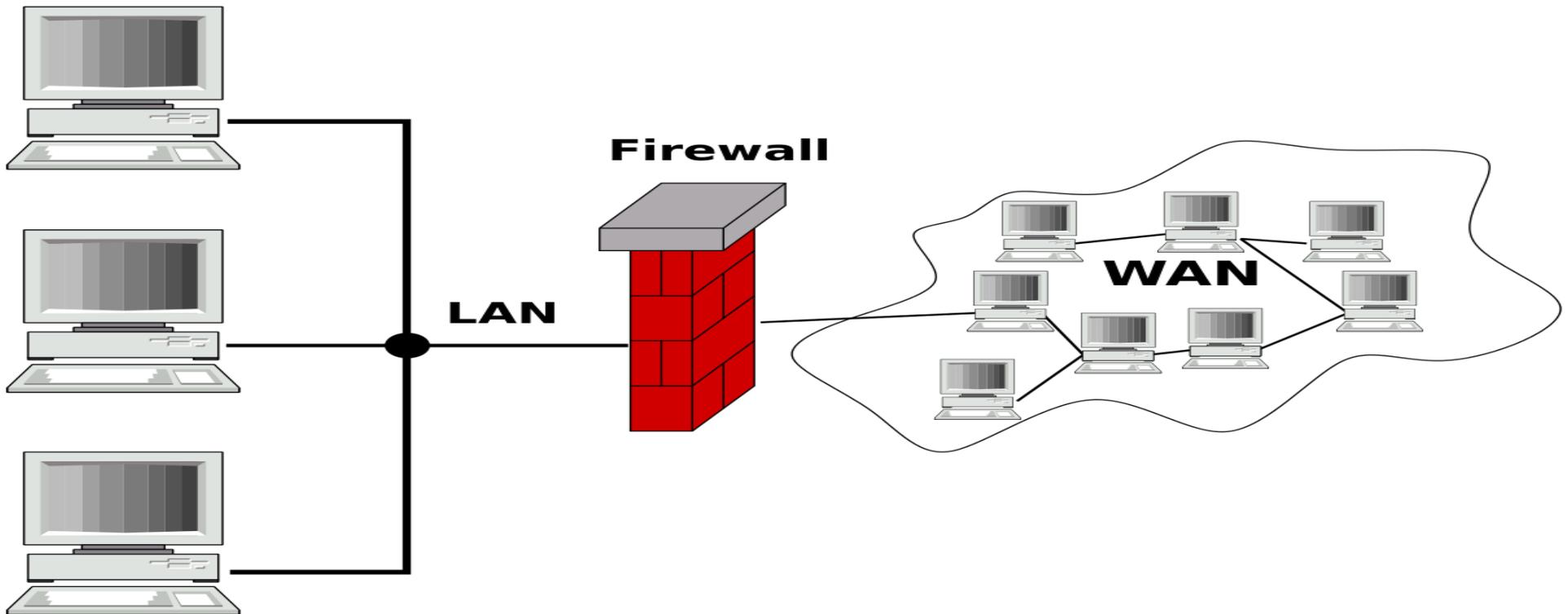


# Network Professional Training center

Providing Job Role Training in one of Fastest Growing IT Jobs Sector



## NPTC Cisco ASA & FTD Training Video Guide

# Table of Content

Recap of Routing Protocol under networking .....	5
Recap of Redundancy Protocol under Networking .....	8
Introduction to Firewall .....	12
ASA ASDM Initial Config .....	30
Using ASDM for Basic Config .....	34
Introduction to ACL .....	41
ASA ACL Project using ASDM .....	46
How to Create ACL with Network and Service Object Groups .....	51
ASA ACL Project using Cli .....	58
Introduction to NAT.....	73
Dynamic NAT Project Task .....	76
PAT(NAT Overload) Project Task .....	86
Static NAT Project Task .....	101
Static NAT Port Forwarding .....	107
Introduction ISP to Firewall Architecture Design .....	113
Dual WAN on Cisco ASA .....	118

<b>ASA Policy Base Routing (PBR) with Dual ISP (Base on Destination Protocol).....</b>	<b>131</b>
<b>ASA Policy Base Routing (PBR) with Dual ISP (Base on Source Network) .....</b>	<b>141</b>
<b>Introduction to Firewall Redundancy .....</b>	<b>149</b>
<b>Active/Standby ASA Cli Project.....</b>	<b>154</b>
<b>ASA Failover Config with ASDM .....</b>	<b>169</b>
<b>Introduction to ASA Redundancy Interface.....</b>	<b>171</b>
<b>ASA Redundant Interface Project .....</b>	<b>173</b>
<b>Cisco ASA Botnet Filtering .....</b>	<b>177</b>
<b>Introduction to VPN.....</b>	
<b>Clientless VPN on ASA Project Task.....</b>	
<b>SSL Anyconnect VPN Project.....</b>	
<b>IPsec Client VPN Project .....</b>	
<b>IPsec Site to Site VPN Project .....</b>	
<b>VPN Best Practice.....</b>	
<b>VPN Troubleshooting Scenarios .....</b>	
<b>FTD Initial Setup .....</b>	
<b>FTD- Creating Access List Policies .....</b>	

**IPS and Malware .....  
FTD-PAT and Static NAT Port Forwarding.....  
High Availability (HA) with FTD .....  
Site to Site VPN with FTD .....  
Day to Day activities of an Engineer.....**

# Computer Network Revision

## Routing

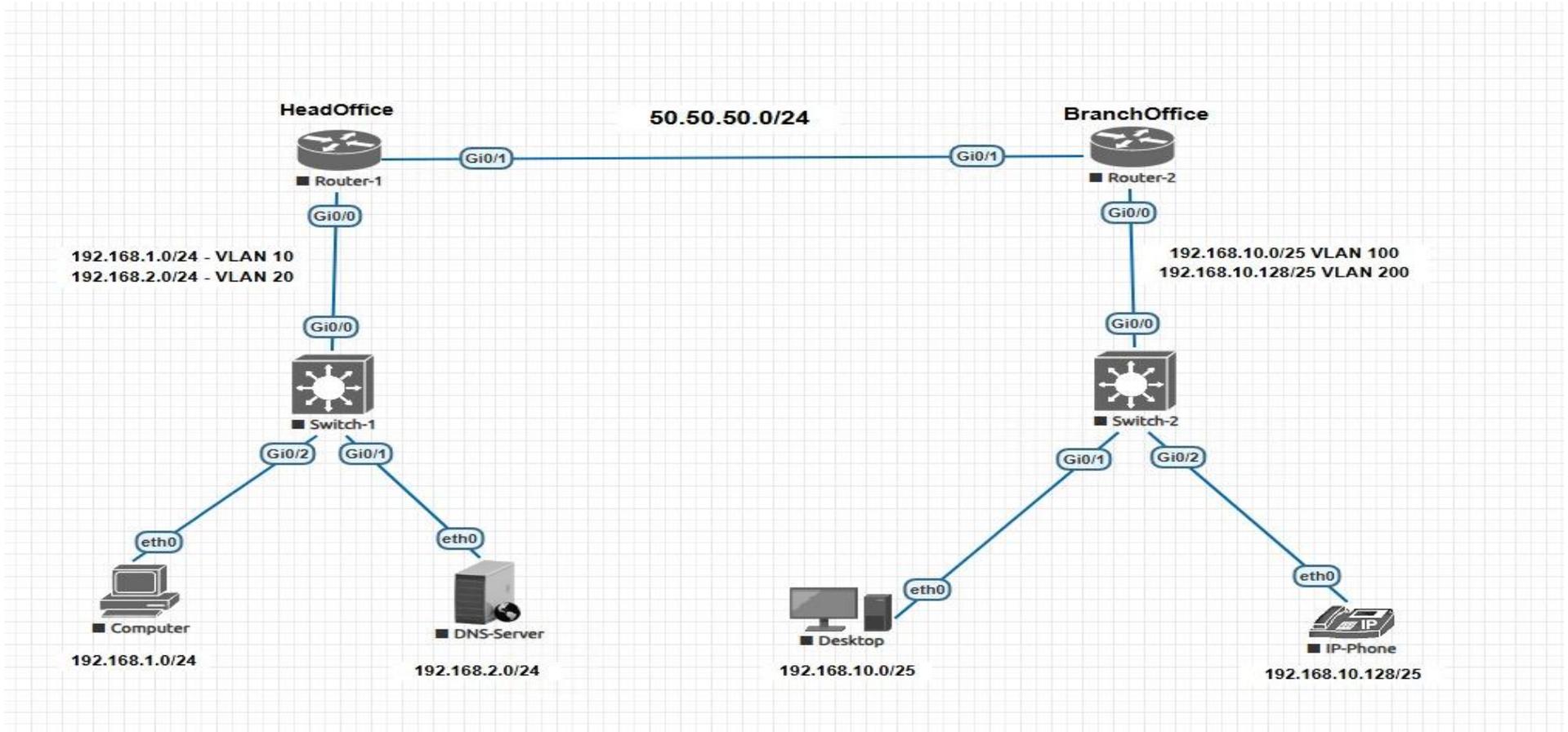
Routing protocols are used to determine how data is transmitted between networks. They can be categorized as link state, distance vector, or exterior gateway protocols.

In simple terms, routing protocols determine how routers communicate with each other to share information about network topology. They allow routers to dynamically adapt to changes, such as link failures or network congestion, ensuring reliable and efficient data delivery. Understanding these protocols is crucial for network engineers and administrators tasked with maintaining seamless connectivity.

### Routing Protocols

These are protocols which help Routing Protocols to carry their information from one router to another example: **Static routing** and **dynamic routing** such as OSPF, EIGRP, RIP, IS-IS and BGP to figure out what paths traffic should take

# Network Routing Recap Project



## Global Configuration

1. Configure the hostname base on the Network Diagram

2. Disable the dns lookup feature.
3. Assign IKE as the Secret password.
4. Direct the Cisco IOS to encrypt any passwords stored in clear-text.

### **Console Port**

5. Configure the console port on all devices to log input synchronously
6. Set password to NPTC
7. Configure the idling timeout to 30 mins

### **VTY Ports**

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to V
11. Configure idling timeout to 30 mins and 10 seconds
12. Save config

### **Verify the above steps using the proper Show command**

13. Assigning IP Addresses and port description
- 14.
15. Configure the Branch Office to act as DHCP Server and exclude 10 IP addresses from the Vlan 200 Scope

### **Vlan and Trunk**

16. Configure Vlan 10 and 20 on Switch 1 and name it as Desktop and Servers respectively
17. Configure Vlan 100 and 200 on Switch 2 and name them as Desktop and VOIP respectively
18. Configure the switch virtual interface (SVI) using respective vlan on the Switch
19. Configure a Switch Default Gateway
20. Configure Trunk Port base on the topology
21. Configure Access port base on the topology
22. Disable all port on the switches which are not connected.

## **First Hop Redundancy Protocol" (FHRP)**

A "First Hop Redundancy Protocol" (FHRP) is a networking protocol designed to provide redundancy for the default gateway on a network, ensuring seamless connectivity even if the primary router fails by allowing multiple routers to share a virtual IP address and act as a backup for one another, with only one active at a time; essentially, it protects against single points of failure at the first hop of a network connection

### **Key points about FHRP:**

#### **Purpose:**

To maintain network connectivity by automatically switching to a backup router if the primary gateway becomes unavailable.

#### **Virtual IP Address:**

All routers in an FHRP group share a single "virtual IP address" which is used as the default gateway by devices on the network.

### **Active and Standby Routers:**

Within an FHRP group, only one router is designated as "active" and handles traffic, while the others remain in "standby" mode, ready to take over if needed.

#### **Failover Mechanism:**

When the active router fails, the FHRP protocol detects the issue and automatically elects a new active router from the standby group, ensuring minimal disruption to network traffic.

### **TYPES of FHRP**

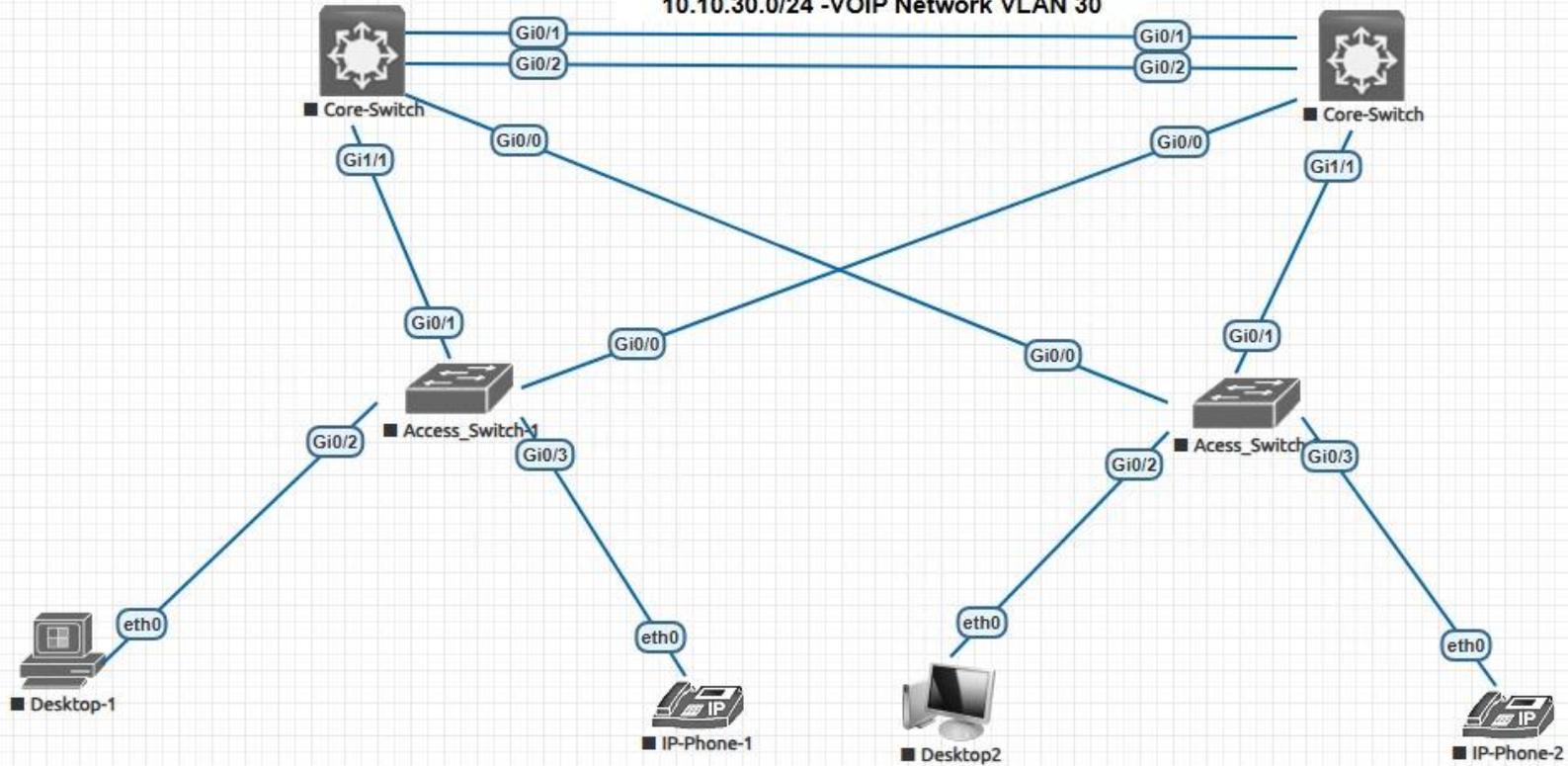
**Hot Standby Router Protocol (HSRP):** A Cisco proprietary protocol considered the most widely used FHRP.

**Virtual Router Redundancy Protocol (VRRP):** An industry standard FHRP with similar functionality to HSRP.

**Gateway Load Balancing Protocol (GLBP):** Allows for load balancing across multiple active routers, not just failover.

## **Redundancy Protocol Project**

10.10.10.0/24 - Management Network-VLAN 10  
10.10.20.0/24 - Computer Network VLAN 20  
10.10.30.0/24 -VOIP Network VLAN 30



## **Global Configuration**

1. Configure the hostname base on the topology
2. Disable the dns lookup feature.
3. Assign Cisc0 as the Secret password.

## **Console Port**

4. Configure the console port on all devices to log input synchronously
5. Set password to Cisc0
6. Configure the idling timeout to 30 mins

## **VTY Ports**

7. Allow 5 concurrent sessions of remote access
8. Configure the vty ports to log input synchronously
9. Set password to Cisc0
10. Configure idling timeout to 60 mins

## **VLAN Configuration**

11. Configure below vlan as follow and allow them to propagate to the access switch

Vlan 10 - Management Vlan - **10.10.10.0/24**

Vlan 20 - Computer Vlan – **10.10.20.0/24** and create as **Multicast**

Vlan 30 - VOIP Vlan – **10.10.30.0/24**

## **Trunk Configuration**

12. Configure the trunk port base on the topology

## **VlanTrunking Protocol (VTP) Configuration**

13. Configure the vtp mode of the access switch as Client

14. Configure the vtp domain name and password on both Core switch as follow

Domain Name – NPTC

Password- secret

### **Etherchannels**

15. Configure etherchannel using PAgP with ON mode on Core\_SW1 and ON mode on Core\_SW2.

### **Redundancy Configuration**

16. Configure your network using HSRP the above ether channel topology

### **IP Routing**

17. Enable ip routing on the two Core switches

### **Access Port**

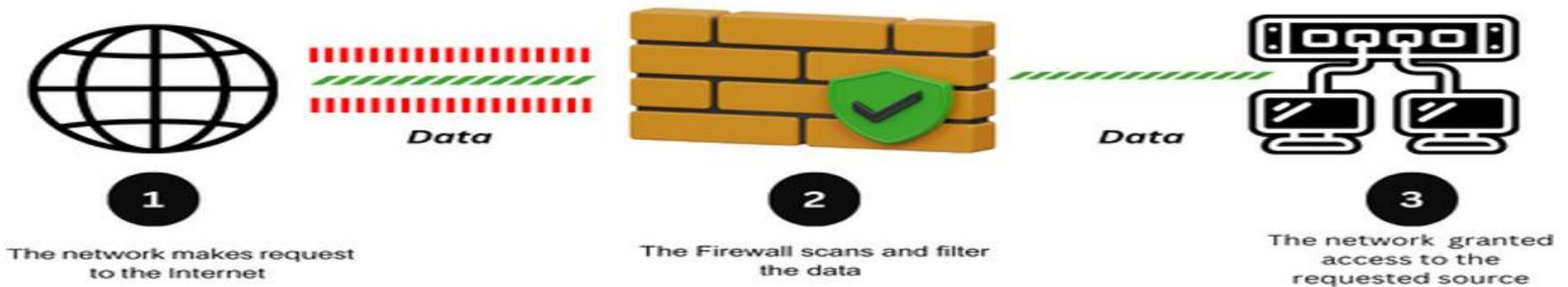
18. Configure all access port for auto settings

## **Introduction of Firewall in Computer Network**

In networking, a firewall is a security device that monitors and controls network traffic, acting as a barrier between a trusted internal network and untrusted external networks, based on predefined security rules. The main purpose of a firewall is to separate a secured area (Higher security Zone / Inside Network) from a less secure area (Low security Zone / Outside Network etc.) and to control communication between the two. Firewall also controls inbound and outbound communications across devices.

They work by examining incoming and outgoing data packets and comparing them against a set of rules. Based on these rules, the firewall can either allow or block the traffic.

## How Firewalls Work



In large corporate network environments, you can also place a network firewall within your internal LAN in order to provide segmentation of private LAN IP subnets (e.g you can isolate servers LAN from users LAN for example).

Throughout the years firewalls started to include IDS and IPS functions including Anti-X and Web content filtering services.

# Firewall Products

- Cisco
- SonicWALL
- Palo Alto Networks
- Juniper
- Watchguard
- Checkpoint
- Fortinet



## **Competitors to Cisco ASA**

Cisco ASA with Firepower services is a premium security product for Enterprise Networks and according to gartner.com and spiceworks.com there are only three direct competitors to these Cisco products. They are Palo Alto, Fortinet and Checkpoint.

### **Palo Alto**

Palo Alto next generation firewalls provide similar features to Cisco ASA firewalls through their PAN-OS operating system. The Palo Alto firewalls, and firewall clusters can be managed by their Firewall management system known as Panorama.

### **Fortinet**

Fortinet has a very large range of firewall models aimed at every size network from entry level to cloud data centers. These firewalls run the Fortigate operating system. Fortinet is one of the fast-growing security firms worldwide and they manufacture all kinds of security products, such as firewalls, antivirus, email security, SIEM, Wi-Fi etc.

### **Checkpoint**

Checkpoint has taken a unified approach to network security through a suite of products that include Next Generation Firewalls known as the Infinity architecture.

This architecture is made up of five sections which are Quantum, Cloud guard, Harmony and Infinity Vision which surrounds their Security Intelligence center known as Infinity Threat Cloud. Checkpoint has a large offering of 15 different Firewall models.

## **Advantages of using Firewall**

1. **Protection from unauthorized access:** Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors from easily accessing a network or system. Protection from unwanted access.
2. **Prevention of malware and other threats:** Malware and other threat prevention: Firewalls can be set up to block traffic linked to known malware or other security concerns, assisting in the defense against these kinds of attacks.
3. **Control of network access:** By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.
4. **Monitoring of network activity:** Firewalls can be set up to record and keep track of all network activity. This information is essential for identifying and looking into security problems and other kinds of shady behavior.
5. **Regulation compliance:** Many industries are bound by rules that demand the usage of firewalls or other security measures. Organizations can comply with these rules and prevent any fines or penalties by using a firewall.
6. **Network segmentation:** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

## Types of Firewall Base How to Deploy

1. **Dedicated hardware appliances** are generally used in data centers.
2. **Software on a machine** as used by home users. e.g., Windows Firewall
3. **Managed firewall services** have many options, including a premises-, network-, or **cloud-based service (Firewall as a Service)**. In this case, the firewall manufacturer or service provider takes care of the network and is responsible for firewall administration, log monitoring, etc.

## Types of Firewall Based on Method of Operation

1. **Packet Filtering/Stateless:** As the name suggests, the user can either allow or drop packets based on source and destination IP, IP protocol ID, etc., from entering the internal network. This type of filtering works at the network transport layer.
2. **Proxy:** It offers more security than other types of filtering. In proxy filtering, the client connects with a proxy instead of a target system and initiates a new connection. This makes it harder for an attacker to discover the network, as they are not getting the response from the target system.
3. **Stateful Inspection:** In this type of inspection, systems maintain a state table (maintains active connections), analyze incoming and outgoing packets, and drop accordingly.
4. **Application Layer Firewalls –**  
These firewalls can examine application layer (of OSI model) information like an HTTP request. If finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.
5. **Next-generation Firewalls –**  
These firewalls are called intelligent firewalls. These firewalls can perform all the tasks that are performed by the other types of firewalls that we learned previously but on top of that, it includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

---

## Firewall Modes

Cisco ASA can be used in 2 modes which are Routed Mode and Transparent Mode

### **Routed Firewall Mode**

In routed mode (default mode), the ASA is considered to be a router in the network. Routed mode supports many interfaces. Each interface is on a different subnet. The ASA acts as a router between connected networks, and each interface requires an IP address on different subnet.

### **Transparent Firewall Mode.**

ASA in Transparent firewall mode, works a layer 2 switch/bridge while still providing firewall benefits (intrusion prevention, packet inspection etc).

Only management interface can received an IP address when ASA is working in Transparent Mode. The ASA connects the same network between it interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network without having to making any change in network

### **Initial Configuration**

```
Asa(config)# firewall transparent
```

## Characteristics of Transparent Mode

- Transparent firewall mode supports only two interfaces (inside and outside)
- The firewall bridges packets from one VLAN to the other instead of routing them.
- MAC lookups are performed instead of routing table lookups.
- Can run in single firewall context or in multiple firewall contexts.
- A management IP address is required on the ASA.
- The management IP address must be in the same subnet as the connected network.
- Each interface of the ASA must be a different VLAN interface.
- Even though the appliance acts as a Layer 2 bridge, Layer 3 traffic cannot pass through the security appliance from a lower security level to a higher security level interface.
- The firewall can allow any traffic through by using normal extended Access Control Lists (ACL).

## Benefits of using firewall in transparent mode –

- No change required on existing IP addressing
- Protocols such as HSRP, VRRP, and GLBP can pass.
- Multicast streams can traverse
- Non-IP traffic can be allowed (IPX, MPLS, BPDUs etc.)
- Routing protocols can establish adjacencies through the firewall

## Cisco Firewall Models

## Cisco PIX 500 Series (legacy)

**Models:** 501 (user based), 506, 510, 525, 535

**Security Licensing Services:** Statefull Firewall, IPsec VPN (Client, Site), Application Inspection (Using Fixups)



## Cisco ASA 5500 Series

**Models:** 5505 (user based), 5510, 5520/5530/5540/5550, 558X series

**Security Licensing Services :**( Verification command = **Show license features**)

Stateful Firewall • IPSec VPN (Client, Site) • SSL VPN (Client) • Application Inspection (using MQC- same as QOS in IOS) • Virtualization (using Contexts) • Modes: Transparent, Routed • Content Security ( Anti-Spam, Anti-Phishing , Anti-Virus , Anti-Spyware , File Blocking ,URL Filtering)• IPS



## Cisco ASA Components

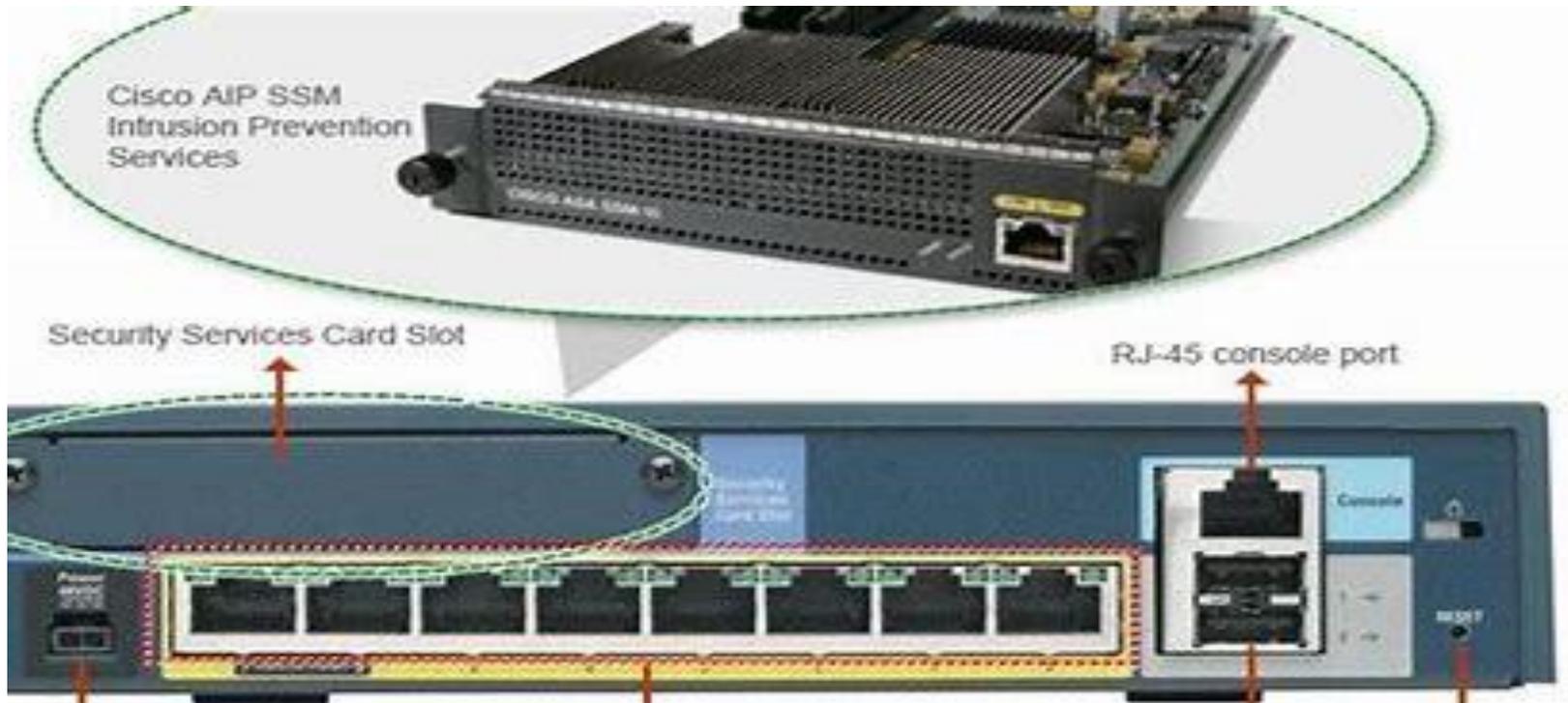
Ethernet ports

Management port

Console port

Flash Memory

Security Expansion



## ASA Security Models (for mid-range ASA Firewall)

- **SSC (Security Services Card)**
  - ASA 5505
  - Services: IPS



- **SSM (Security Services Module)**
  - ASA 5510, 5520, 5540
  - Services: IPS, Content Security



## **ASA Security Models (for High-end ASA Firewall)**

- **SSP (Security Services Processors)**
  - ASA 5580, 5585
  - IPS services

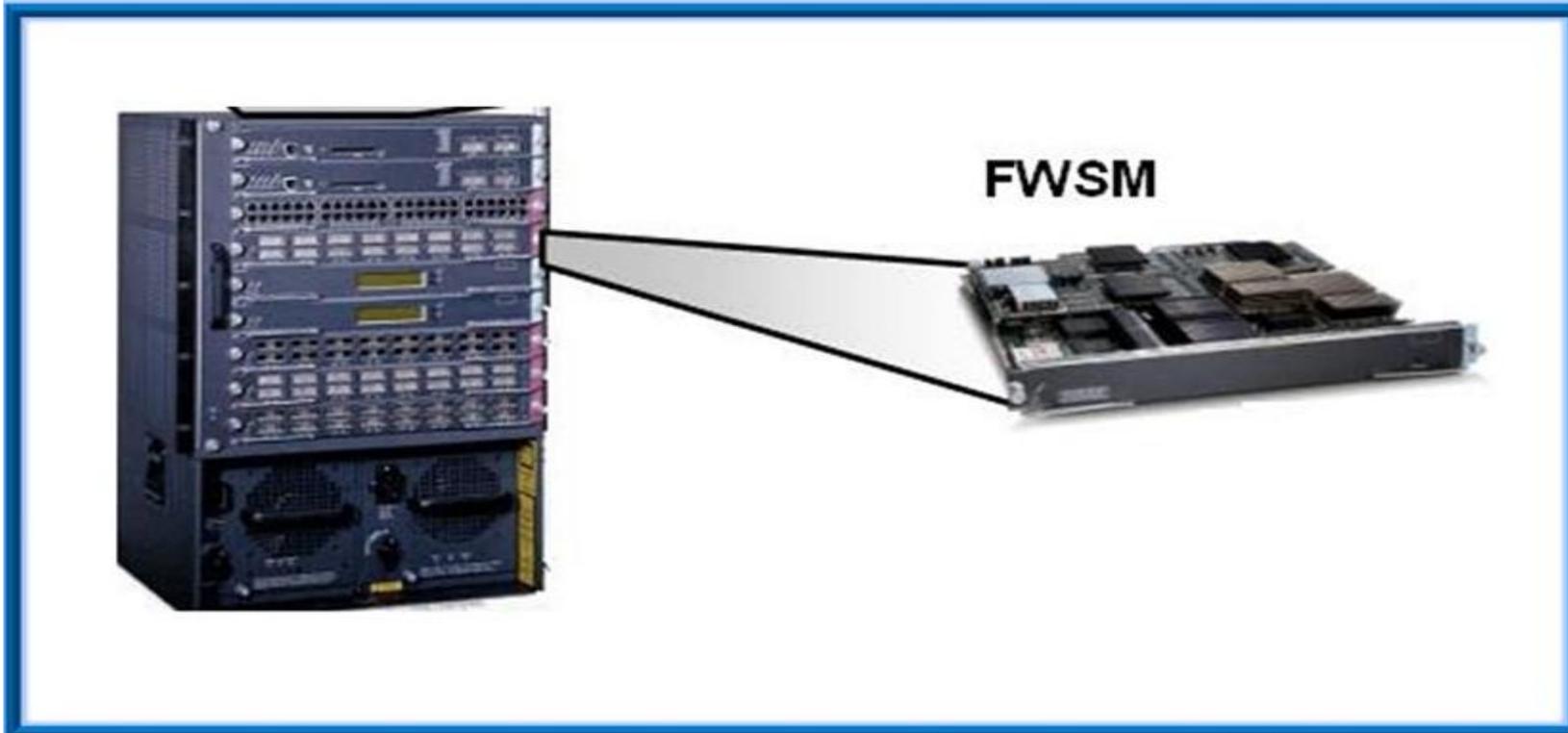


## **Service Modules (Cisco Catalyst 6500)**

**FWSM**-Firewall service models- This models normally don't have vpn features, The **WEB VPN services module** support up to 32,000 SSL VPN users and up to 4 modules can be used in single chassis

**ACE**- Application Control Engine Module for Cisco 6500 Series and 7600 Series routers (ACE supports translation and load balancing)

**CSM**-Content Switching Module



## Performance Metric Consideration

- Firewall and VPN Services
  - Using one or the other not both!

High-end Network Security Appliances		Mid-range Network Security Appliances			
Cisco ASA 5500 Series Model/License	Cisco ASA 5505 Base / Security Plus	Cisco ASA 5510 Base / Security Plus	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
Product Image (click to enlarge)					
Network Location	Small Business, Branch Office, Enterprise Teleworker	Internet Edge	Internet Edge	Internet Edge	Internet Edge, Campus
Performance Summary					
Maximum Firewall throughput (Mbps)	150 Mbps	300 Mbps	450 Mbps	650 Mbps	1 Gbps (real-world HTTP), 1.2 Gbps
Maximum Firewall Connections	10,000 / 25,000	50,000 / 130,000	280,000	400,000	650,000
Maximum Firewall Connections/Second	4000	9000	12,000	25,000	36,000
Packets Per Second (64 byte)	85,000	190,000	320,000	500,000	600,000
Maximum 3DES/AES VPN Throughput	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps

## Cisco ASA Firewall Security Levels

The Cisco ASA Firewall uses so-called “security levels” that indicate how trusted an interface is compared to another interface. The higher the security level, the more trusted the interface is. Each interface on the ASA is a security zone so by using these security levels we have different trust levels for our security zones.

An interface with a high-security level can access an interface with a low-security level, but the other way around is not possible unless we configure an access-list that permits this traffic.

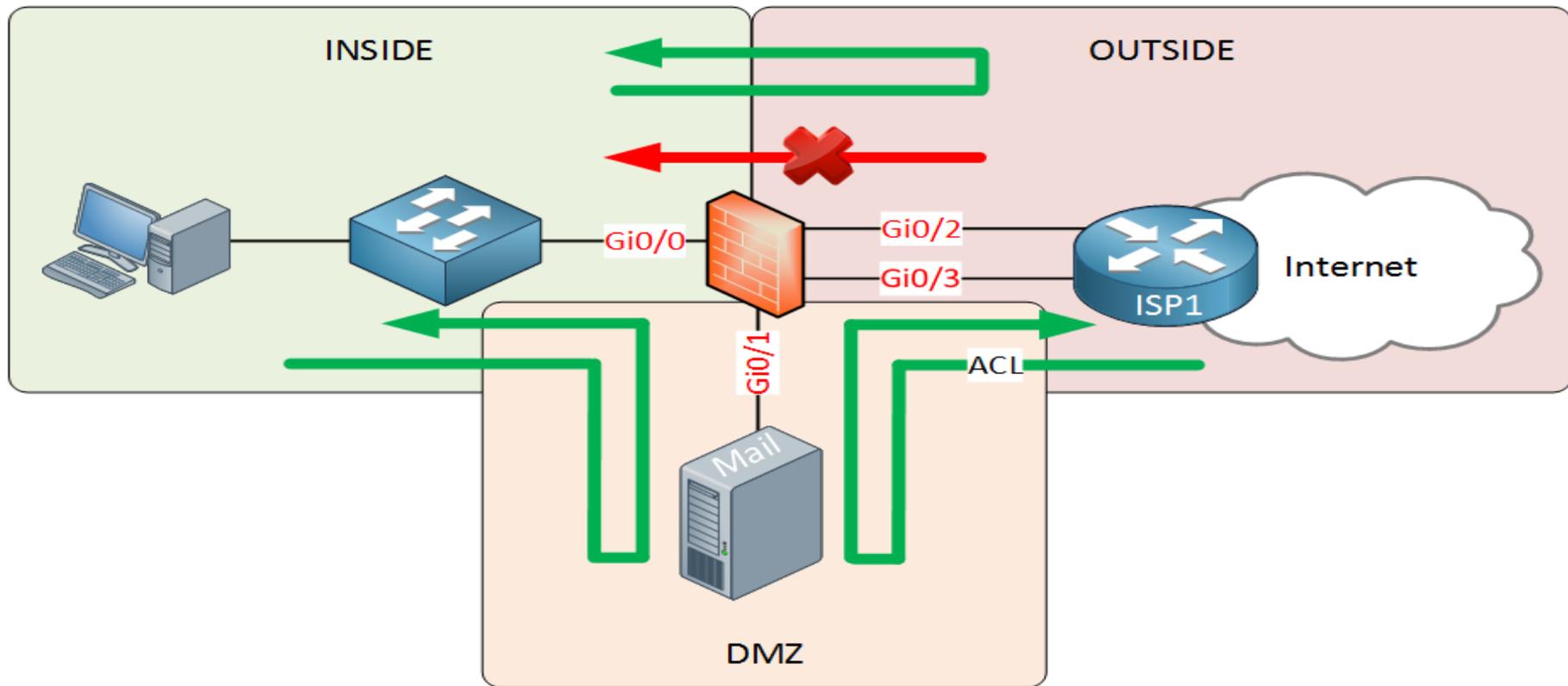
Here are a couple of examples of security levels:

- **Security level 0:** This is the lowest security level there is on the ASA, and by default, it is assigned to the “outside” interface. Since there is no lower security level, this means that traffic from the outside is unable to reach any of our interfaces unless we permit it within an access-list.
- **Security level 100:** This is the highest security level on our ASA, and by default, this is assigned to the “inside” interface. We usually use this for our “LAN”. Since this is the highest security level, by default, it can reach all the other interfaces.
- **Security level 1 – 99:** We can create any other security levels that we want, for example, we can use security level 50 for our DMZ. This means that traffic is allowed from our inside network to the DMZ (security level 100 -> 50) and also from the DMZ to the outside (security level 50 -> 0). Traffic from the DMZ, however, can't go to the inside (without an access-list) because traffic from security level 50 is not allowed to reach security level 100. You can create as many security levels as you want...

## Rules

In short, this is how the security levels work:

- Traffic from a **higher security level to a lower security level is allowed**. For example, traffic from the inside is allowed to reach the outside. Of course, it's possible to restrict this with access-lists.
- Traffic from a **lower security level to a higher security level is not allowed**. This could be traffic from the outside headed towards the inside. You can also change this with an access-list. This might be useful if you have servers in the DMZ that you want to reach from the outside.
- Traffic between interfaces with the **same security level is not allowed**. For example, if you have an interface called "DMZ1" with security level 50 and another one called "DMZ2" with the same security level, then traffic between the two will be dropped. You can change this behavior with the global **same-security-traffic permit inter-interface** command.
- Our LAN is our trusted network, which would have a high security level. The WAN is untrusted so it will have a low security level. This means that traffic from our LAN > WAN will be permitted. Traffic from the WAN to our LAN will be denied. Since the firewall is stateful, it keeps track of outgoing connections and will permit the return traffic from our LAN.
- If you want to make an exception, and permit traffic from the WAN to the LAN then this can be accomplished with an access-list.
- Most companies will have one or more servers that should be reachable from the Internet. Perhaps a mail or web server. Instead of placing these on the INSIDE, we use a third zone called the **DMZ (Demilitarized Zone)**. Take a look at the picture below:



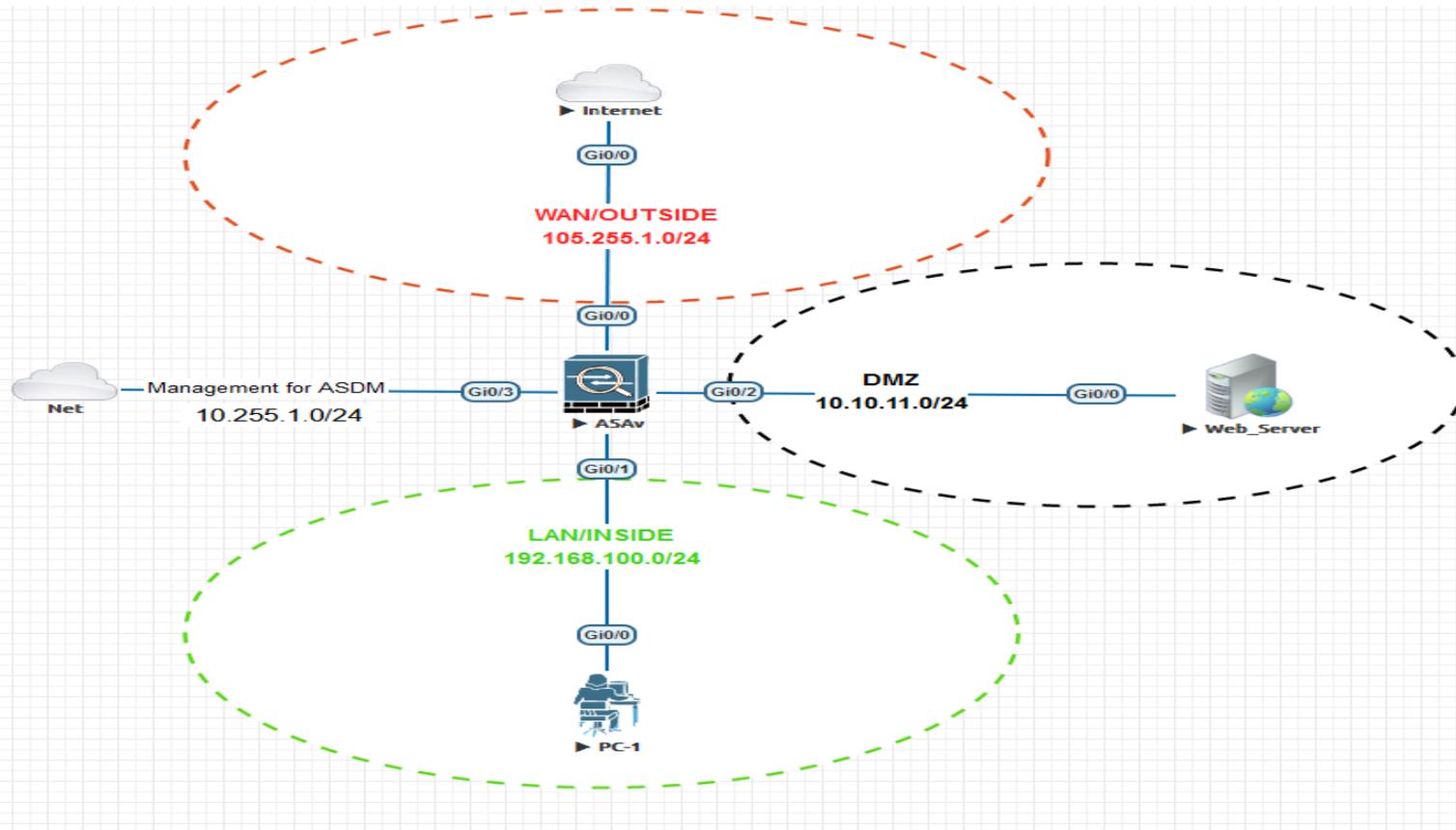
- Traffic from INSIDE to OUTSIDE is permitted.
- Traffic from INSIDE to DMZ is permitted.
- Traffic from DMZ to OUTSIDE is permitted.
- Traffic from DMZ to INSIDE is denied.
- Traffic from OUTSIDE to DMZ is denied.
- Traffic from OUTSIDE to INSIDE is denied.

# Cisco ASA ASDM Initial Configuration

Cisco's ASDM (Adaptive Security Device Manager) is the GUI that Cisco offers to configure and monitor your Cisco ASA firewall.

## 1. TASK: Apply the initial setup to get the ASDM working for management

### ASDM Initial Setup Lab Project\_1



1. Assign IP address on the management interface to be use for the GUI, by default ASA use 192.168.1.1 which can be changed

```
Boston-ASAFW(config)# interface GigabitEthernet0/3
```

```
Boston-ASAFW(config-if)#nameif OUTSIDE
```

```
Boston-ASAFW(config-if)#security-level 0
```

```
Boston-ASAFW(config-if)#ip address 10.255.1.101 255.255.255.0
```

2. ASDM requires HTTP and it's disabled by default, let's enable it:

```
Boston-ASAFW (config)#http server enable
```

3. Instead of giving everyone access to the HTTP server we will specify which network and interface are permitted to use the HTTP server:

```
ASA-FW(config)# http 10.255.1.0 255.255.255.0 Management
```

4. Create a user account to be use by the ASDM

```
ASA-FW(config)#Username admin pass cisco
```

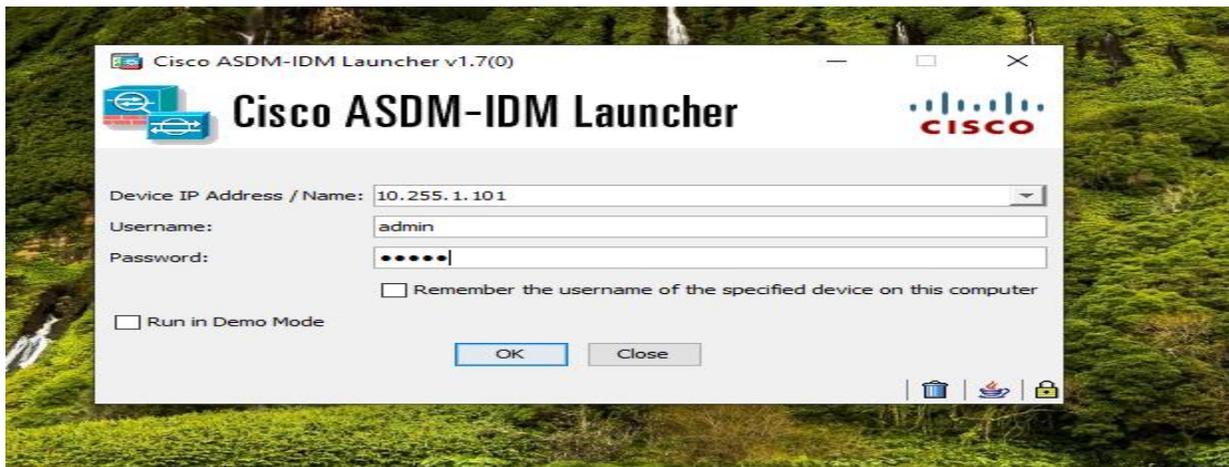
That's all we have to do on the ASA. Now you can open a web browser on your computer. Open the following URL:

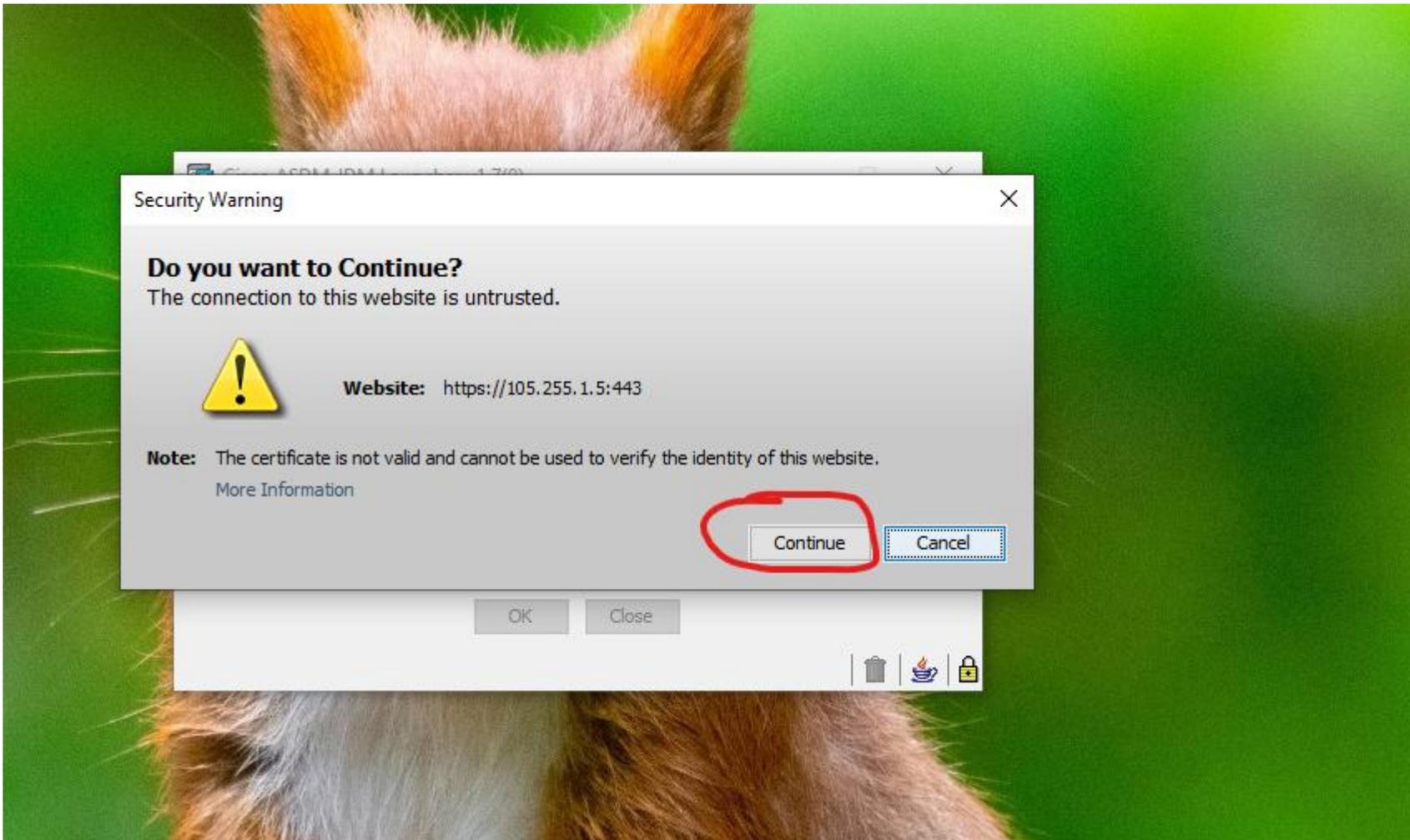
The ASA uses a self-signed certificate so that's why you see this error above. Just click on Continue to this website and you will see the following screen:

`https://10.255.1.101`

- 1. You now have two options...you can run ASDM directly from the ASA's flash memory or you can install it on your computer first. This lab has it installed already**

Enter the IP address of the ASA and the username/password that we created earlier. Click on OK and you will see this:





Cisco ASDM 7.6(1) for ASA - 10.255.1.101

96.32.243.58

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List Bookmarks Home

Device List Add Delete Connect

Find: 10.255.1.75 10.255.1.76 10.255.1.101

Device Dashboard Firewall Dashboard

### Device Information

General License Virtual Resources

Host Name: **ciscoasa**  
 ASA Version: **9.6(1)**  
 ASDM Version: **7.6(1)**  
 Firewall Mode: **Routed**  
 Total Flash: **8192 MB**

Device Uptime: **0d 0h 23m 30s**  
 Device Type: **ASAv**  
 Number of vCPUs: **1**  
 Total Memory: **2048 MB**

### Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
Management	10.255.1.101/24	up	up	2

Select an interface to view input and output Kbps

### VPN Summary

Ipssec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 [Details](#)

### System Resources Status

Total Memory Usage Total CPU Usage Core Usage Details

#### Memory Usage (MB)

1234 MB

#### Connections Per Second Usage

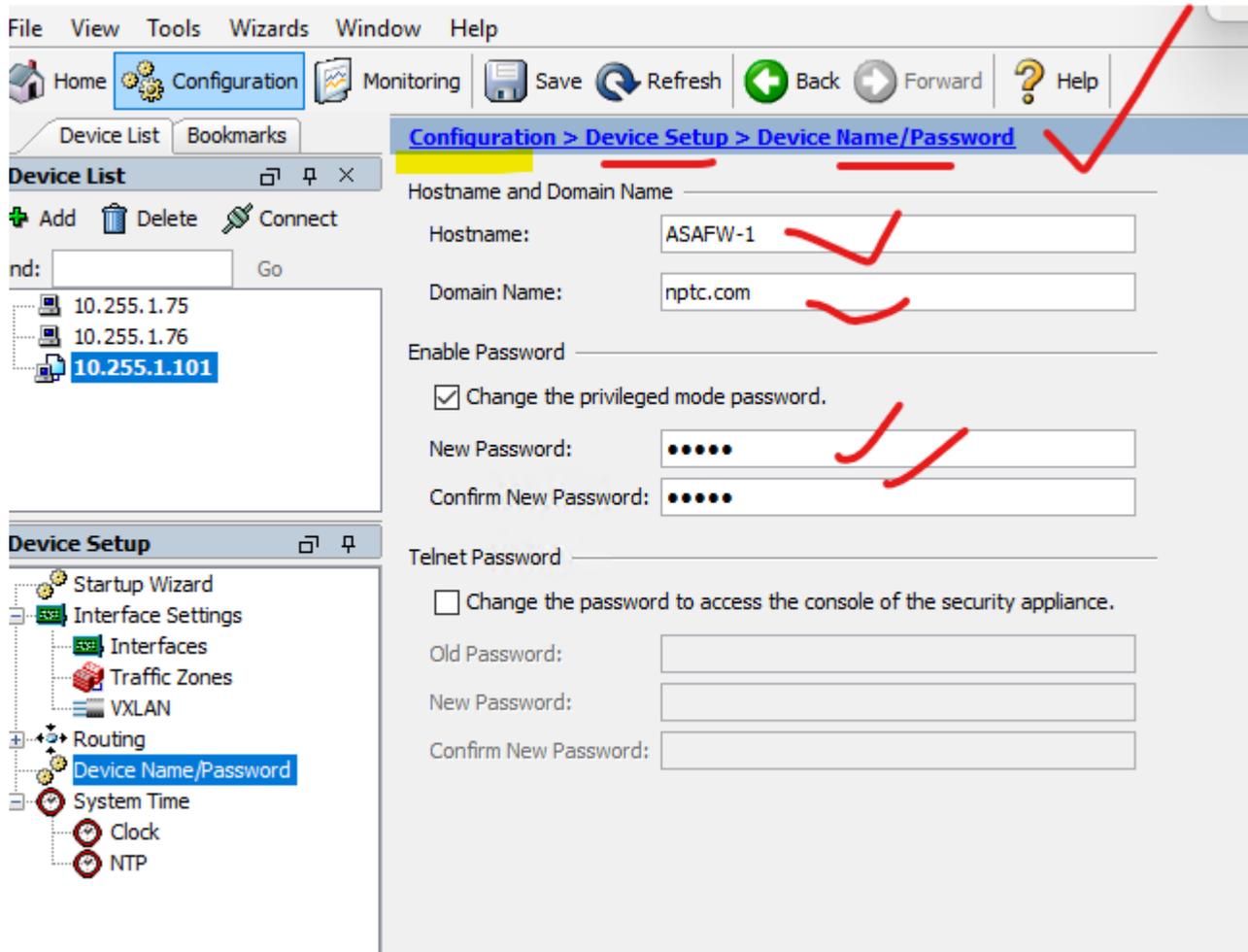
#### 'Management' Interface Traffic Usage (Kbps)

### Latest ASDM Syslog Messages

ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

# Using ASDM for Basic Configuration and AAA access

## 1. Configure the hostname , domain name and the enable password



## 2. Configure the clock time , date and time zone

Configuration > Device Setup > System Time > Clock

Configure the ASA date and clock.

Time Zone: (GMT-05:00)(Eastern Time) Indianapolis, Montreal, New York ✓

Date: 7 Mar, 2025 ✓

Time: 14 : 14 : 00 hh:mm:ss (24-hour) ✓

Firewall time is set by the NTP Server 10.255.1.1 with reference clock 23.168.136.132. Clock will be automatically adjusted for daylight saving changes.

Update Displayed Time ✓

## 3. Configure the NTP server

Configuration > Device Setup > System Time > NTP

Configure NTP servers and define authentication keys and values.

IP Address
10.255.1.1

Add ✓

Edit

Delete

**Edit NTP Server Configuration**

IP Address: 10.255.1.1 ✓  Preferred

Interface: Management ✓

Authentication Key

Key Number: -- None --  Trusted

Key Value:

Re-enter Key Value:

OK ✓ Cancel Help

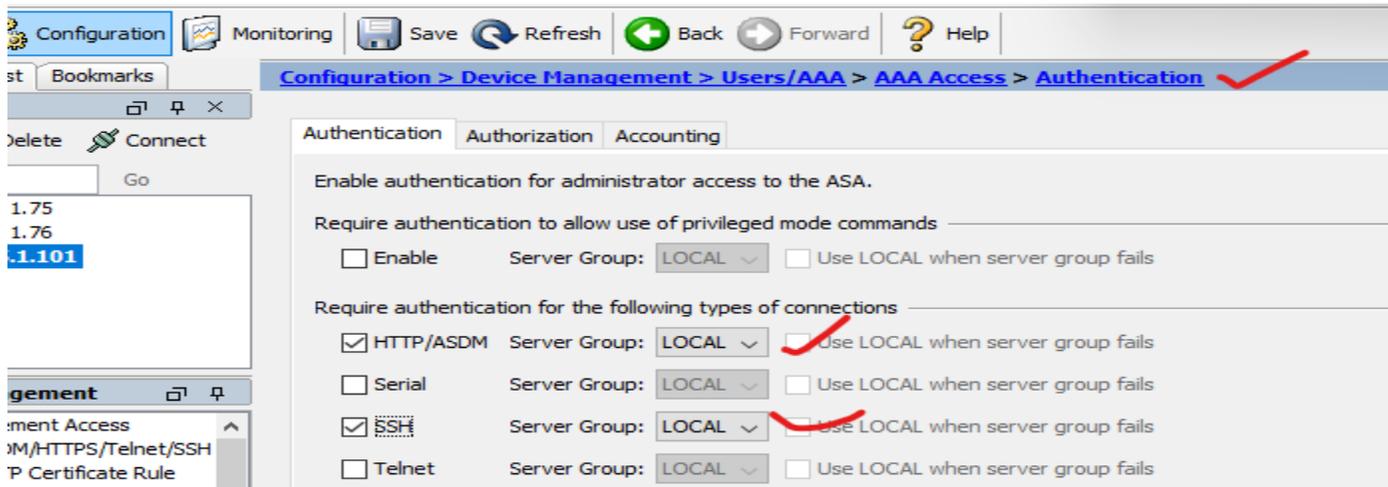
#### 4. Create a user account

The screenshot shows the Cisco configuration interface for creating a user account. The breadcrumb navigation at the top is "Configuration > Device Management > Users/AAA > User Accounts". The main heading is "Add User Account". On the left, there is a tree view with "Identity" selected, containing "Public Key Authentication", "Public Key Using PKF", and "VPN Policy". Below the tree is a list of usernames: "enable\_15" and "admin", with "admin" selected. The main form area contains the following fields and options:

- Username: SuperAdmin
- Password: \*\*\*\*\*
- Confirm Password: \*\*\*\*\*
- Access Restriction: Select one of the options below to restrict ASDM, SSH, Telnet and Console. Note: All users have network access, regardless of these settings.
  - Full access(ASDM, SSH, Telnet and Console)
- Privilege level is used with command authorization.
- Privilege Level: 15

Red checkmarks are visible over the "SuperAdmin" username, the password fields, the "Full access" radio button, and the "15" privilege level dropdown.

#### 5. Giving AAA access to an Account



## 6. Configure the identity certificate

Issued To	Issued By	Expiry Date	Associated Trustpoints

Find:     Match Case

Certificate Expiration Alerts

Send the first alert before :  (days)

Repeat Alert Interval :  (days)

Public CA Enrollment

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate

### Add Identity Certificate

Trustpoint Name:

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

Certificate Subject DN:

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

## 7. Adding a AAA Server to your ASA

The first step is to create the server group and add the a server to the group

Configuration > Device Management > Users/AAA > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				

Add AAA Server Group

AAA Server Group: AAAServerGroup

Protocol: RADIUS

Accounting Mode: RADIUS

Reactivation Mode: SDI

Dead Time:

Max Failed Attempts:

Enable interim accounting update

Update Interval: 24 Hours

Now we can add a server to the group

Configuration > Device Management > Users/AAA > AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
AAAserverGroup	RADIUS	Single	Depletion	10	3

Find:   Match Case

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
---------------------------	-----------	---------

**Add AAA Server**

Server Group: AAAserverGroup  
Interface Name: Management  
Server Name or IP Address: 10.255.1.1  
Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645  
Server Accounting Port: 1646  
Retry Interval: 10 seconds  
Server Secret Key: \*\*\*\*\*  
Common Password: \*\*\*\*\*  
ACL Netmask Convert: Standard  
Microsoft CHAPv2 Capable:

SDI Messages  
Message Table

OK Cancel Help

Management Access

- ASDM/HTTPS/Telnet/SSH
- HTTP Certificate Rule
- Command Line (CLI)
- File Access
- ICMP
- Management Interface
- Management Session Queue
- SNMP
- Management Access Rule
- Licensing
- Smart Licensing
- System Image/Configuration
- High Availability and Scalability
- Logging
- Smart Call-Home
- Cloud Web Security
- Users/AAA
  - AAA Server Groups**
  - LDAP Attribute Map
  - Authentication Prompt
  - AAA Access
  - Dynamic Access Policies
  - User Accounts
  - Password Policy
  - Change My Password
  - Certificate Management
  - Identity Certificates

10.255.1.75  
10.255.1.76  
**10.255.1.101**

Add  
Edit  
Delete

Add  
Edit  
Delete  
Move Up  
Move Down  
Test

## 8. Enable access to the box with the new group

The screenshot shows the Cisco ASDM configuration interface. The breadcrumb navigation at the top reads: Configuration > Device Management > Users/AAA > AAA Access > Authentication. A red checkmark is placed next to the 'Authentication' breadcrumb. The left sidebar shows the 'Device List' with IP addresses 10.255.1.75, 10.255.1.76, and 10.255.1.101. The 'Device Management' tree is expanded to 'Management Access' > 'Command Line (CLI)'. The main configuration area has tabs for 'Authentication', 'Authorization', and 'Accounting'. Under the 'Authentication' tab, there are three sections:

- Enable authentication for administrator access to the ASA.** This section is currently disabled.
- Require authentication to allow use of privileged mode commands.** This section is enabled. The 'Server Group' is set to 'AAAServerGroup' and 'Use LOCAL when server group fails' is unchecked. A red checkmark is next to the 'Server Group' dropdown.
- Require authentication for the following types of connections.** This section is enabled. The following table summarizes the configuration for each connection type:

Connection Type	Server Group	Use LOCAL when server group fails
<input checked="" type="checkbox"/> HTTP/ASDM	AAAServerGroup	<input checked="" type="checkbox"/>
<input type="checkbox"/> Serial	AAAServerGroup	<input type="checkbox"/>
<input checked="" type="checkbox"/> SSH	AAAServerGroup	<input checked="" type="checkbox"/>
<input type="checkbox"/> Telnet	AAAServerGroup	<input type="checkbox"/>

The 'SSH' row has a red checkmark next to the 'Use LOCAL when server group fails' checkbox.

## Cisco ASA Access Control-List (Firewall Policy)

The Cisco ASA firewall uses access-lists that are similar to the ones on IOS routers and switches. Without any access-lists, the ASA will allow traffic **from a higher security level to a lower security level**. All other traffic is dropped

Access-lists are created globally and then applied with the **access-group** command. They can be applied in- or outbound.

In firewalls, an Access Control List (ACL) is a set of rules that determines which network traffic is allowed or denied based on source and destination, acting as a gatekeeper for network access and security.

### **How it works:**

Each rule in an ACL specifies a condition (e.g., source IP address, destination port, protocol) and an action (allow or deny). When traffic arrives at the firewall, it's compared against the ACL rules, and the specified action is taken.

### **Purpose:**

ACLs are used to control which users or devices can access specific network resources or services, enhancing security by restricting unauthorized access.

### **Examples**

An ACL might allow only specific IP addresses or group of IP address to access a web server. While denying traffic from other IP addresses.

An ACL might deny all traffic to a specific port.

An ACL might allow traffic from a untrusted network to access internal resources.

An ACL might block all traffic on port 21 (FTP) except for traffic from a trusted network.

## **Benefits of using ACLs:**

**Enhanced Security:** ACLs help to prevent unauthorized access to network resources.

**Traffic Control:** ACLs allow administrators to control the flow of network traffic, improving network performance and security.

**Granular Control:** ACLs provide granular control over network traffic, allowing administrators to fine-tune security policies.

## **Types ACL**

ACLs come in 2 main types used in ASAs: Standard, Extended. Each ACL type has a different application, depending on where it's deployed.

**Standard.** A standard ACL is designed to protect a network using only the destination address. These are typically used in simple deployments, and are used by only a few protocols like VPN filters and route maps (though route maps can also use extended ACLs, so it's rarely used in this case either). Standard ACLs do not provide robust security.

**Extended.** Building on a standard ACL, using extended ACLs means you can also allow or block source addresses in addition to destination. Extended ACLs can also be applied to traffic based on a variety of protocols: IP, ICMP, TCP, and UDP, as well as service policies, AAA rules, WCCP, Botnet Traffic Filter, and VPN group and DAP policies. Among the most common ACLs you will encounter.

## Firewall rules

Firewall rules are often based on port numbers, specifying which ports can be accessed from specific IP addresses or networks.

By controlling which ports are open, firewalls can prevent unauthorized access to services and applications, protecting the network from malicious traffic.

## Port Numbers

In the context of firewalls, port numbers are crucial for identifying specific services or applications on a network, allowing firewalls to control network traffic based on which ports are being used.

Port number is not a physical connection but a logical connection that is use by **programs** and **services** to exchange information.

It basically determines which program or services on a computer or server is going to be used.

Port numbers ranges from, 0 – 65535

Port number is always associated with an IP address to exchange data. The IP address determines the location of the server or computer and the port number determines which application or program on the server it wants to use

## Systems or Well-Known Ports

Ranges from 0-1023

## **Commonly used TCP PORT**

80,443 – Web pages (HTTP, HTTPS)

21- FTP (File Transfer Protocol)

25- Email (SMTP)

53 – DNS communication

## **TCP Real life applications**

Web browsing, Email, FTP, Remote Desktop

## **UDP Real Life applications**

Online Gaming, Voice over IP, Streaming Video, DNS

## **Register Ports or User Port**

Ranges from 1024 – 49151, these are ports that can be registered by companies and developers for particular services.

1102 – Adobe Server

1433- Microsoft SQL Server

1416- Novell

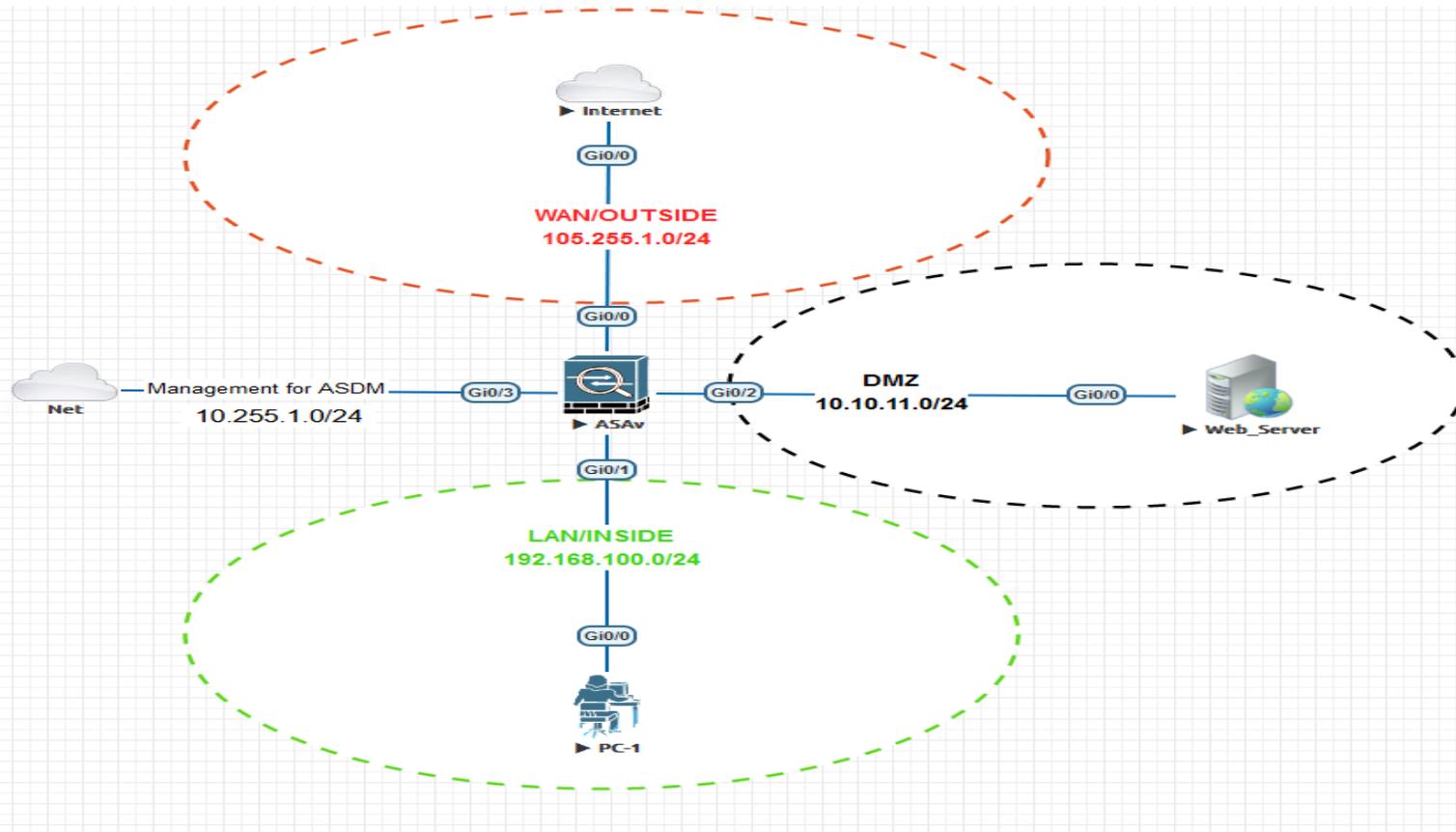
1527 – Oracle

## **Dynamic Port Numbers**

Ranges 49152 – 65535, these are ports that your computer assigns temporarily to itself during a session. They are client side ports which are free to use.

To check active connections on your computer type `netstat -n / netstat-an` (if your computer is acting as server)

# ACL -Lab Project \_1



- 1. Project Task 1:** Configure firewall policy that will permit any source outside ( any IP address ) access a web server 10.10.11.2 on TCP port 80 (WWW) using ASDM

# 1. Assign IP address to the LAN , DMZ and the outside interface base on the topology using ASDM

Configuration>Device setup >interfaces

The screenshot shows the ASDM configuration interface. The breadcrumb navigation is Configuration > Device Setup > Interface Settings > Interfaces. A table lists the interfaces, with GigabitEthernet0/0 selected. The 'Edit Interface' dialog is open for GigabitEthernet0/0, showing the following configuration:

Interface	Name	Zone	Route Map	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Secondary VLAN	Redu
GigabitEthernet0/0				No					No
GigabitEthernet0/1				No					No
GigabitEthernet0/2									
GigabitEthernet0/3	Manage...								
GigabitEthernet0/4									
GigabitEthernet0/5									
GigabitEthernet0/6									
Management0/0									

**Edit Interface**

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/0 Configure Hardware Properties...

Interface Name: Outside

Zone: -- None -- Manage ... ⊗ Threat Detection is enabled.

Route Map: -- None -- Manage ...

Security Level: 0

Dedicate this interface to management only

VTEP source interface

Enable Interface

IP Address

Use Static IP  Obtain Address via DHCP  Use PPPoE

IP Address: 105.255.1.1

Subnet Mask: 255.255.255.0

Description: link to the Internet

## 2. Repeat the same process for the remaining interfaces

The screenshot shows the Cisco ASDM 7.6(1) for ASA - 10.255.1.101 interface configuration page. The breadcrumb navigation is Configuration > Device Setup > Interface Settings > Interfaces. A table lists the interface configurations, with the row for GigabitEthernet0/2 highlighted in blue and circled in red.

Interface	Name	Zone	Route Map	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Secondary VLAN	Redunda
GigabitEthernet0/0	OUTSIDE			Yes	0	105.255.1.1	255.255.255.0		No
GigabitEthernet0/1	INSIDE			Yes	100	192.168.100.1	255.255.255.0		No
GigabitEthernet0/2	DMZ			Yes	50	10.10.11.1	255.255.255.0		No
GigabitEthernet0/3	Manage...			Yes	80	10.255.1.101	255.255.255.0		No
GigabitEthernet0/4				No					No
GigabitEthernet0/5				No					No
GigabitEthernet0/6				No					No
Management0/0				No					No

**NB: But users from the LAN with higher security level can communicate on the service port 80**

**PC-1#10.10.11.2 80**

**Trying 10.10.11.2, 80 ... Open**

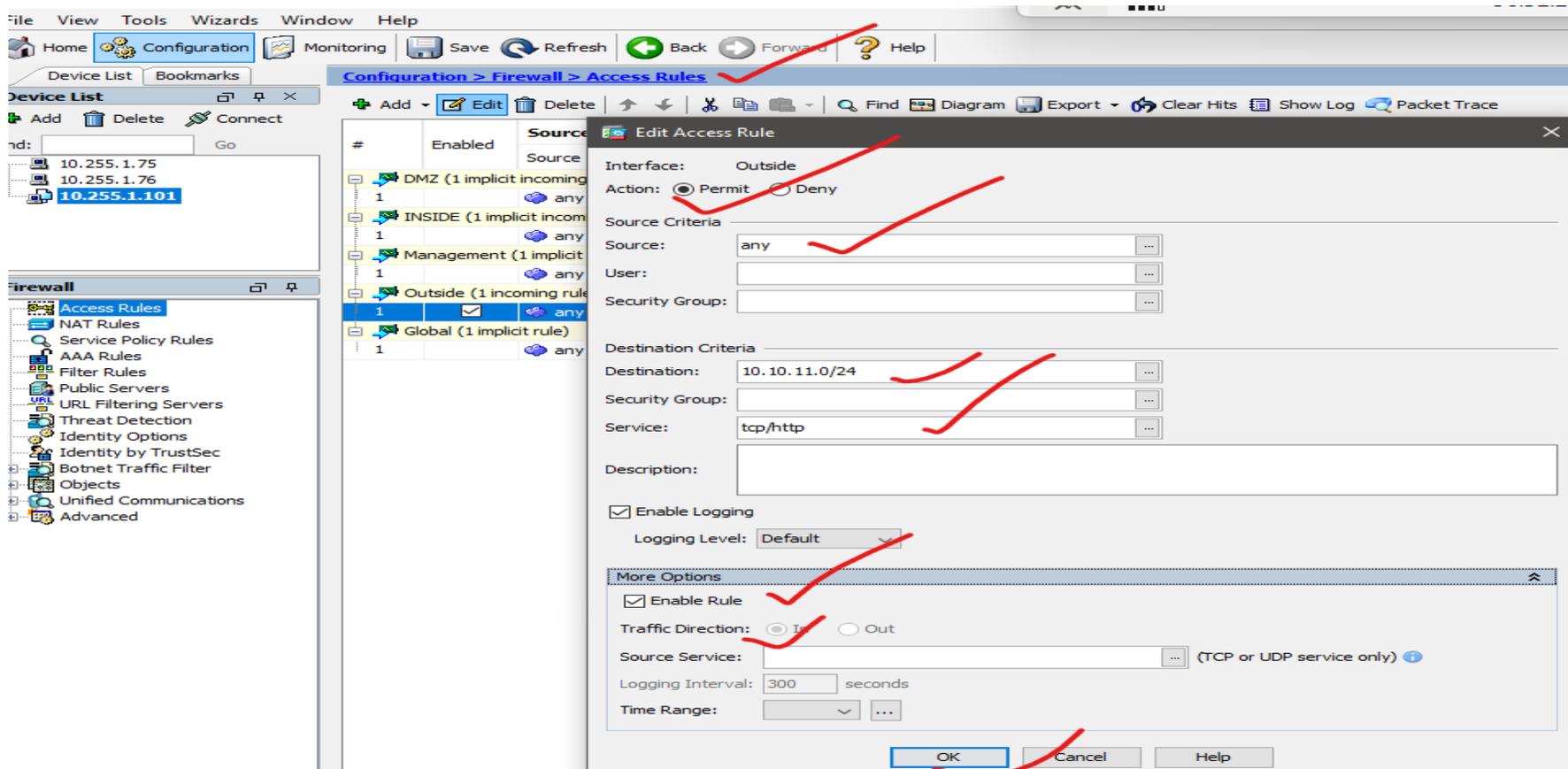
Now let's test if port 80 is open out the internet

**Internet#10.10.11.2 80**

**Trying 10.10.11.2, 80 ...**

**% Connection timed out; remote host not responding**

This traffic is deny by default, because is coming from low Security Zone to high Security zone. Let's create an access-list that allow HTTP traffic. We'll create something so that users on the internet are allowed to connect to the Webserver on port 80. All other traffic will be deny



Let's do the testing on the internet to see if the port can open

Internet#

Internet#

Internet#10.10.11.2 80

Trying 10.10.11.2, 80 ... Open

## Network object in Cisco ASA firewall

In a Cisco ASA firewall, network objects are reusable components that represent IP addresses, subnets, or FQDNs, simplifying configuration and maintenance by allowing you to reference them in multiple rules and policies instead of repeating the same values.

Imagine you have to manage a Cisco ASA firewall that has hundreds of hosts and dozens of servers behind it, and for each of these devices we require access-list rules that permit or deny traffic.

With so many devices you will have a LOT of access-list statements and it might become an administrative nightmare to read, understand and update the access-list.

To make our lives a bit easier, Cisco introduced the **object-group** on Cisco ASA Firewalls (and also on IOS routers since IOS 12.4.20T).

### **Purpose:**

Network objects are designed to make firewall configuration easier and more manageable.

### **What they represent:**

They can represent a single IP address, a range of IP addresses, a subnet (CIDR notation), or a fully qualified domain name (FQDN).

### **How they are used:**

Once defined, network objects can be used in various configurations, such as access control lists (ACLs), Network Address Translation (NAT) rules, and service policies.

## **Benefits:**

**Simplified Configuration:** Instead of typing IP addresses or subnets multiple times, you can simply use the object name.

**Centralized Management:** If you need to change an IP address or subnet, you only need to modify the object definition, and the change will be reflected everywhere it's used.

**Improved Readability:** Using descriptive object names makes the configuration easier to understand and maintain.

## **Types of Network Objects:**

**Host:** A single IP address.

**Network:** A subnet or range of IP addresses.

**FQDN:** A fully qualified domain name.

## **Example:**

Imagine you have a group of servers with IP addresses in the 192.168.1.0/24 network. Instead of specifying this subnet in every access rule, you can create a network object named "WebServers" and use that object in the rules.

## Object Groups:

You can also group multiple network objects into object groups, which can further simplify configuration and management.

### Examples of object-group:

- **icmp-type** can be used to select all the different ICMP types, for example echo, echo-reply, traceroute, unreachable, etc.
- **Network** is used to select IP addresses and/or network addresses.
- **Protocol** lets you select an entire protocol. For example, TCP, UDP, GRE, ESP, AH, OSPF, EIGRP, and many others.
- **Security** is used for Cisco TrustSec.
- **Service** is used to select TCP and/or UDP port numbers.
- **User** is to select local user groups for Identity Firewall.

## **Service Objects in Cisco ASA Firewall**

On a Cisco ASA firewall, a service object defines a specific protocol and port combination, which can then be used in access control lists (ACLs) and other security configurations, simplifying rule creation and maintenance.

### **Example:**

A service object named "Web" could represent the TCP protocol on port 80 (HTTP).

### **Purpose:**

Service objects are reusable components that represent a specific service or protocol (like HTTP, SSH, or FTP) and its associated port(s).

## **Service Groups:**

### **Concept:**

You can also create service groups, which are collections of service objects.

### **Example:**

A "Web Services" group could contain service objects for HTTP (port 80), HTTPS (port 443), and potentially other web-related services.

### **Benefits:**

Service groups further simplify ACLs by allowing you to refer to a group of services instead of individual ones.

## Project Task2: Use same topology to create network object group for Webservers

Configure>firewall>object>network object

The screenshot shows the Mikrotik WinBox configuration interface. The main window displays the configuration path: Configuration > Firewall > Objects > Network Objects/Groups. The left sidebar shows the configuration tree with 'Network Objects/Groups' selected. The main area shows the 'Add Network Object Group' dialog box.

The dialog box has the following fields and options:

- Group Name: WEB-SERVERS
- Description: (empty)
- Existing Network Objects/Groups: (radio button selected)
- Members in Group: (table)
- Create new Network Object member: (radio button selected)

The 'Members in Group' table is as follows:

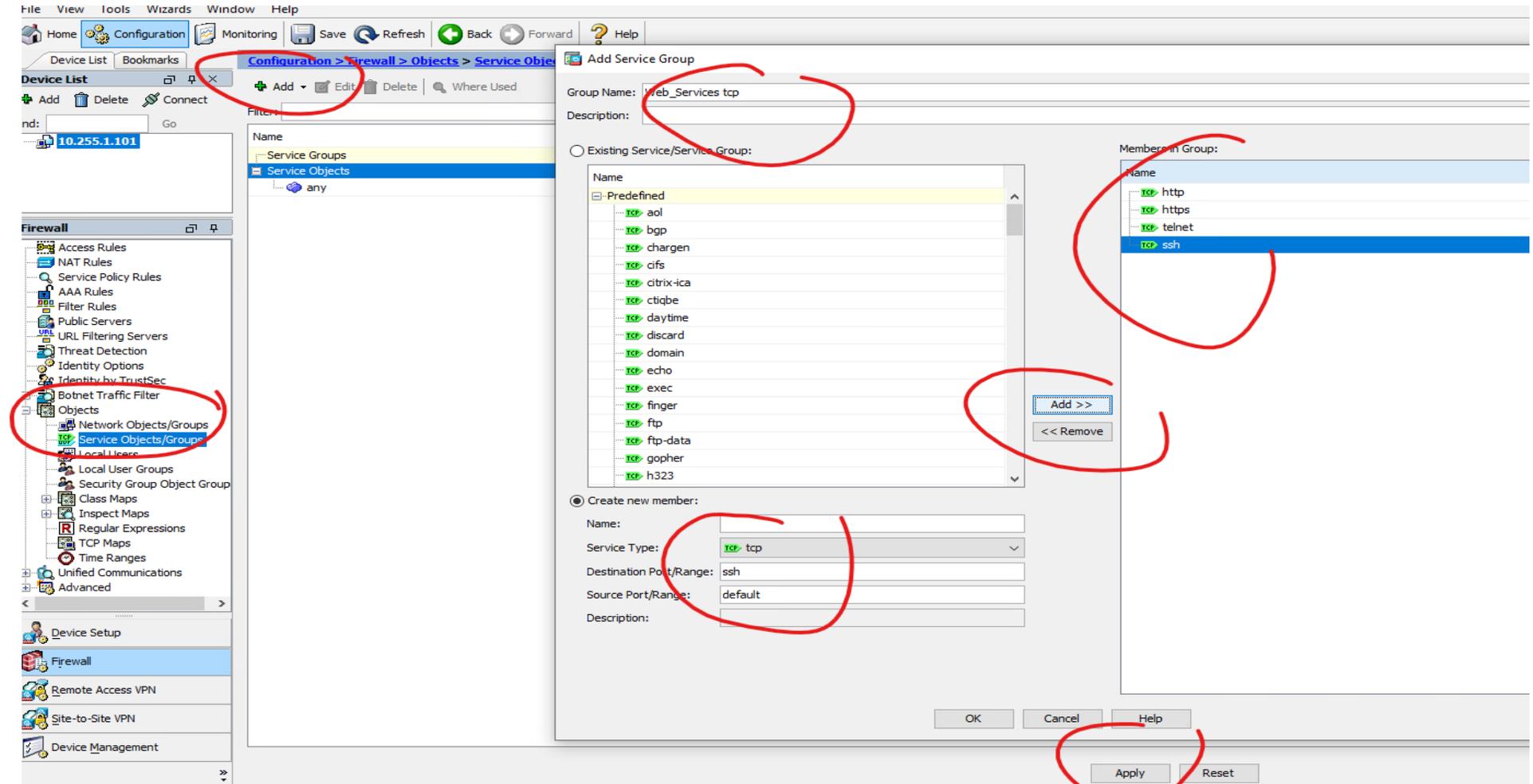
Name	IP Address	NetmaskPrefix Length	De
Server1	10.10.11.2		
Server2	10.10.11.3		
Server3	10.10.11.4		
Server4	10.10.11.5		

The 'Create new Network Object member' section has the following fields:

- Name: (optional) Server4
- Type: Host
- IP Version: IPv4 (selected), IPv6
- IP Address: 10.10.11.5
- Description: (empty)

The 'Add >>' button is circled in red. Red checkmarks are placed over the 'Group Name', 'Description', 'Server4', 'Host', 'IPv4', and '10.10.11.5' fields.

### Project Task3: Use same topology to create Service object group for Webservers



## Project Task4: Configure a firewall policy allowing all users from the internet to access all the DMZ web servers on the following port 80,443

The screenshot displays the Cisco ASDM 7.6(1) for ASA - 10.255.1.101 interface. The main window shows the 'Configuration > Firewall > Access Rules' section. A table lists existing rules, including implicit rules for DMZ, INSIDE, and OUTSIDE, and a rule for 'Global'. The 'Add Access Rule' dialog box is open, showing the configuration for a new rule on the 'OUTSIDE' interface. The rule is set to 'Permit' action, with 'any' source and 'WEEB\_SERVERS' destination. The service is 'Web\_Servicestcp'. The 'Enable Logging' checkbox is checked, and the logging level is 'Default'. The 'OK' button is highlighted.

#	Enabled	Source Criteria:	Destination Criteria:	Service	Action	Hits	Logging	Time	Description
		Source	User	Security Group	Destination	Security Group			
1		any							Implicit rule: P
1		any							Implicit rule: P
1		any							Implicit rule: P
1		any							Implicit rule

**Add Access Rule**

Interface: **OUTSIDE**

Action:  Permit  Deny

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: **WEEB\_SERVERS**

Security Group:

Service: **Web\_Servicestcp**

Description:

Enable Logging

Logging Level: **Default**

More Options

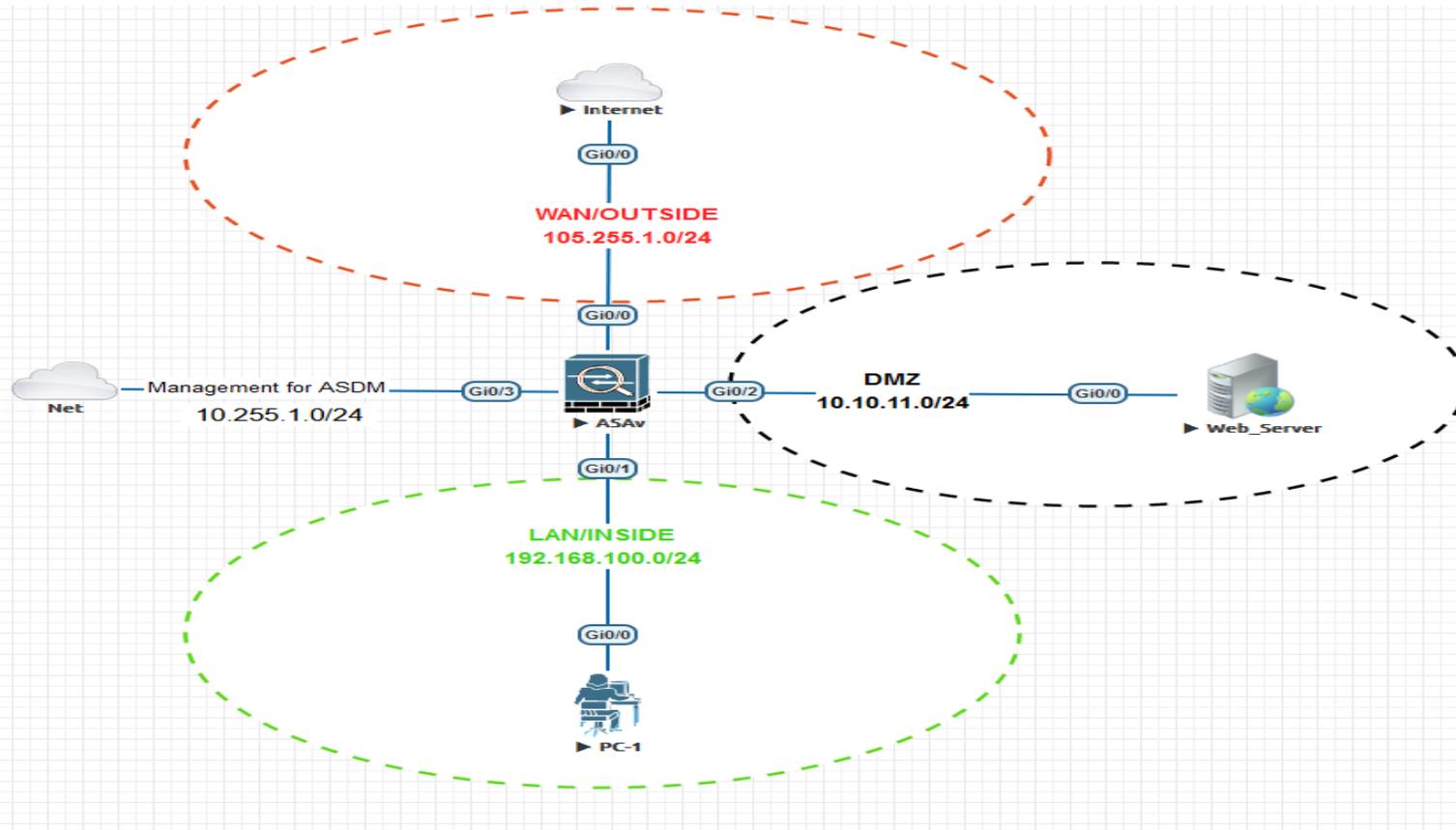
**OK** Cancel Help

Now let's test if the ACL is working

```
Internet#  
Internet#telnet 10.10.11.2 80 ✓  
Trying 10.10.11.2, 80 ... Open ✓  
X  
HTTP/1.1 400 Bad Request  
Date: Fri, 14 Mar 2025 17:35:18 GMT  
Server: cisco-IOS  
Accept-Ranges: none  
  
400 Bad Request  
[Connection to 10.10.11.2 closed by foreign host]  
Internet#telnet 10.10.11.2 443 ✓  
Trying 10.10.11.2, 443 ... Open ✓  
X  
.....
```

## ASA ACL Project Using Cli

### ACL -Lab Project \_1



**3. Project Task 1:** Configure firewall policy that will permit any source outside ( any IP address ) access a web server 10.10.11.2 on TCP port 80 (WWW) using Cli

## 2. Apply basic Config on cisco ASA Boston Office using cli

- **Host name** – configure hostname which provide identity for the ASA device

```
Ciscoasa> en
```

```
Password: hit enter to go to privileged mode
```

```
Ciscoasa# conf t
```

```
Ciscoasa(config)# hostname ASA-FW1
```

- **Enable password** - configures an enable password for the Cisco ASA that is required for users to access the privileged mode to configure all ASA features.

```
ASA-FW1 (config)# enable password nptc123
```

- **Timezone:** configures the time-zone and day-light savings time the firewall will use for logging and other events.

```
ASA-FW1 (config) # clock timezone EST -5 0
```

```
ASA-FW1 (config) # clock summer-time EST recurring
```

- **Username and Password:** adds a user account with a username, password, and privilege level. Privilege level 15 allows our user to login directly into the enabled mode of the ASA to perform configuration changes.

```
ASA-FW1 (config) #username admin password cisco privilege 15
```

## 3. Configure AAA to use the local ASA database for telnet and ssh user authentication

```
ASA-FW1 (config) # aaa authentication ssh console LOCAL
```

```
ASA-FW1 (config) # aaa authentication telnet console LOCAL
```

#### 4. Configure your inside, outside and dmz network

ASA-FW1 (config) # Int g0/0

ASA-FW1 (config) # Des link to Internet

ASA-FW1 (config) # Nameif outside

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

ASA-FW1 (config) # Security-level 0

ASA-FW1 (config) # ip add 105.255.1.1 255.255.255.0

ASA-FW1 (config) # No shut

ASA-FW1 (config) # Int g0/1

ASA-FW1 (config)# Des LAN

ASA-FW1 (config) # Nameif Inside

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

ASA-FW1 (config) # Security-level 100

ASA-FW1 (config) # Ip add 192.168.100.1 255.255.255.0

ASA-FW1 (config) # No shut

Int

ASA-FW1 (config) # Int g0/2

ASA-FW1 (config) # Des DMZ-Servers

ASA-FW1 (config) # Nameif DMZ

ASA-FW1 (config) # security-level 50

ASA-FW1 (config) # ip add 10.10.11.1 255.255.255.0

ASA-FW1 (config) # no shut

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	105.255.1.1	YES	manual	up	up
GigabitEthernet0/1	192.168.100.1	YES	manual	up	up
GigabitEthernet0/2	10.10.11.1	YES	manual	up	up

```
ASA-FW1# show nameif
```

Interface	Name	Security
GigabitEthernet0/0	OUTSIDE	0
GigabitEthernet0/1	INSIDE	100
GigabitEthernet0/2	DMZ	50

## 5. Configure telnet

To enable Telnet we will specify which hosts or subnets can telnet into the ASA including which interface we can telnet to. As a best practice telnet will only be enabled on our inside interface for any computer on the inside subnet (192.168.100.0) to telnet into the ASA. Telnet 192.168.100.0 255.255.252.0 inside

```
ASA-FW1 (config) # telnet 192.168.100.0 255.255.252.0 inside
```

## 6. Configure SSH

Next we will enable SSH the same way we enabled telnet, but first we need to configure the domain name and generate our local RSA keys (1024 bits).

```
ASA-FW1 (config) # domain-name nptc.com
```

```
ASA-FW1 (config) # crypto key generate rsa modulus 1024
```

NB: Once our RSA keys has been generated we will enable SSH access for any host from the inside network (192.168.100.0) and a host located outside the network (105.255.1.0).

```
ASA-FW1 (config)# ssh 105.255.1.101 255.255.255.0 outside
ASA-FW1 (config) # ssh 192.168.100.0 255.255.255.0 inside
```

## 7. Configure firewall policy that will permit any source ( any IP address ) access a web server 10.10.11.2 on TCP port 80 (WWW)

Now let's test if port 80 is open out the internet

```
Internet#telnet 10.10.11.2 80
Trying 10.10.11.2, 80 ...
% Connection timed out; remote host not responding
```

This traffic is deny by default, because is coming from low Security Zone to high Security zone. Let's create an access-list that allow HTTP traffic. We'll create something so that users on the internet are allowed to connect to the Webserver on port 80. All other traffic will be deny

```
ASA-FW1 (config)# access-list OUTSIDE_DMZ extended permit tcp any host 10.10.11.2 eq 80
ASA-FW1 (config)# access-group OUTSIDE_DMZ in interface OUTSIDE
```

Let's verify if the ACL is working

```
Internet#telnet 10.10.11.2 80
Trying 10.10.11.2, 80 ... Open
```

```
ASA-FW1(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list OUTSIDE_DMZ; 1 elements; name hash: 0xf68adb0a
access-list OUTSIDE_DMZ line 1 extended permit tcp any host 10.10.11.2 eq www (hitcnt=1) 0xdba32ba0
```

## Global Access-List

The global access-list is useful when you have many interfaces and you don't want to enable an access-list on each one of them. When you use this, you create an access-list like you normally do but instead of enabling on an interface, we enable it globally.

When you do this...the access-list is applied to **all outbound traffic on all interfaces**. It doesn't work for outbound traffic.

```
Texas-ASAFW (config)# no access-group OUTSIDE_DMZ in interface OUTSIDE
```

```
Texas-ASAFW (config)# access-group OUTSIDE_DMZ global
```

**And it will achieve the same result**

```
Internet#telnet 10.10.11.2 80  
Trying 10.10.11.2, 80 ... Open
```

Now I will create a network object-group using host ip addresses of mail servers at the DMZ:

```
ASA-FW1 (config) # object-group network WEB_SERVERS  
  
ASA-FW1 (config-network-object-group) # network-object host 10.10.11.2  
  
ASA-FW1 (config-network-object-group) # network-object host 10.10.11.3  
  
ASA-FW1 (config-network-object-group) # network-object host 10.10.11.4  
  
ASA-FW1 (config-network-object-group) # network-object host 10.10.11.5  
  
ASA-FW1 (config-network-object-group) # network-object host 10.10.11.5
```

```
ASA-FW1(config)# show run object-group
object-group network WEB_SERVERS
network-object host 10.10.11.2
network-object host 10.10.11.3
network-object host 10.10.11.4
network-object host 10.10.11.5
network-object host 10.10.11.6
```

Now let's configure the firewall policy or ACL using the object group to allow users from outside access the internet

```
ASA-FW1 (config)# access-list HTTP_TO_DMZ permit tcp any object-group WEB_SERVERS eq 80
```

Without the object group the ACL will have 5 lines instead of the above

```
ASA-FW1(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
    alert-interval 300
access-list HTTP_TO_DMZ; 5 elements; name hash: 0x6ce713ae
access-list HTTP_TO_DMZ line 1 extended permit tcp any object-group WEB_SERVERS eq www (hitcnt=0) 0x0964f55b
access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.2 eq www (hitcnt=0) 0xbe25da03
access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.3 eq www (hitcnt=0) 0xbace7e6d
access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.4 eq www (hitcnt=0) 0x303325f3
access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.5 eq www (hitcnt=0) 0x29dcf20a
access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.6 eq www (hitcnt=0) 0x967a574d
```

We can also will create Service object-group that combines all our TCP ports. Eg port 22, 23, and 80,443 and apply it to the Webservers we have at the DMZ

```
ASA-FW1 (config) # object-group service WEB_SERVICES tcp
```

```
ASA-FW1 (config-service-object-group) # port-object eq 22
```

```
ASA-FW1 (config-service-object-group) # port-object eq 23
```

```
ASA-FW1 (config-service-object-group) # port-object eq 80
```

```
ASA-FW1 (config-service-object-group) # port-object eq 443
```

```
ASA-FW1(config-service-object-group)# show run object-group
```

```
object-group network WEB_SERVERS
```

```
network-object host 10.10.11.2
```

```
network-object host 10.10.11.3
```

```
network-object host 10.10.11.4
```

```
network-object host 10.10.11.5
```

```
network-object host 10.10.11.6
```

```
object-group service DMZ_WEB_SERVICES tcp
```

```
port-object eq ssh
```

```
port-object eq telnet
```

```
port-object eq www
```

```
port-object eq https
```

Let's now configure the ACL using both the **network object group** and the **service object group**

```
ASA-FW1 (config) # access-list HTTP_TO_DMZ permit tcp any object-group WEB_SERVERS object-group  
DMZ_WEB_SERVICES
```

Let's apply the ACL to an interface

```
ASA-FW1 (config) # access-group HTTP_TO_DMZ global
```

```
ASA-FW1(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
    alert-interval 300
access-list HTTP_TO_DMZ; 20 elements; name hash: 0x6ce713ae
access-list HTTP_TO_DMZ line 1 extended permit tcp any object-group WEB_SERVERS object-group DMZ_WEB_SERVICES (hitcnt=0) 0x25002ebc
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.2 eq ssh (hitcnt=0) 0x588491df
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.2 eq telnet (hitcnt=0) 0x8fa088ea
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.2 eq www (hitcnt=0) 0xbe25da03
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.2 eq https (hitcnt=0) 0x624a41a8
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.3 eq ssh (hitcnt=0) 0x6a506109
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.3 eq telnet (hitcnt=0) 0x26f11125
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.3 eq www (hitcnt=0) 0xbace7e6d
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.3 eq https (hitcnt=0) 0xf49f500a
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.4 eq ssh (hitcnt=0) 0x6367c289
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.4 eq telnet (hitcnt=0) 0x587077f8
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.4 eq www (hitcnt=0) 0x303325f3
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.4 eq https (hitcnt=0) 0x6653c3c2
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.5 eq ssh (hitcnt=0) 0x569d9d04
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.5 eq telnet (hitcnt=0) 0xab6d8651
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.5 eq www (hitcnt=0) 0x29dcf20a
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.5 eq https (hitcnt=0) 0x07087f43
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.6 eq ssh (hitcnt=0) 0x7b8c9500
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.6 eq telnet (hitcnt=0) 0xfd4356a2
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.6 eq www (hitcnt=0) 0x967a574d
    access-list HTTP_TO_DMZ line 1 extended permit tcp any host 10.10.11.6 eq https (hitcnt=0) 0x2c3e6a5f
```

Activate Window  
Go to Settings to activ

## Cisco ASA Remove Access-List

If you want to remove an access-list from a Cisco ASA Firewall then you'll find out that removing it doesn't work the same as on Cisco IOS routers or switches. Let me give you an example of creating an access-list and then try to remove it:

```
ASA-FW1(config)# no access-list OUTSIDE_DMZ
ERROR: % Incomplete command
```

Using "no" in front of it doesn't work...the ASA thinks that we want to remove a single entry, not delete the entire access-list. The following command will work or you can apply no using the complete ACL command

```
ASA-FW1(config)# clear configure access-list OUTSIDE_DMZ
```

Use the **clear configure** command to get rid of the entire access-list, let's verify this:

```
ASA-FW1(config)# clear configure access-list OUTSIDE_DMZ
ASA-FW1(config)# show run ac
ASA-FW1(config)# show run access-l
ASA-FW1(config)#
```

```
ASA-FW1(config)# show run access-g
```

**NB: this configuration will also affect the access-group interface and should not be done on production**

## **Cisco ASA ACL Best Practices**

### **1. Always apply ACLs inbound on all interfaces**

I don't like to apply ACLs outbound on the interfaces because I want to use the firewall's internal compute and memory resources as efficiently as possible.

### **2. Name the ACL after the interface on which the rule will be applied**

Eg OUTSIDE-to-DMZ, inside-to-in , https-to-DMZ

### **3. Use remarks in your ACLs to internally document your intentions**

The more you can make the configuration of your firewall self-documenting, the easier it will be to manage it going forward

### **4. Use object groups**

For example, I might want to block a particular set of malicious IP addresses from ever accessing my network from the outside. If I use the same object-group on the inside interface, I can also prevent anybody inside my network from ever accessing these same malicious external hosts. And if I add a new host to that object-group, I automatically update both those inbound and outbound rules.

Only use object-groups when you have several TCP/UDP ports or source/destination addresses that need to be grouped. Always using object-groups even for rules that have low amount of services or network defined might eventually make the configuration harder to read

## **5. Make your ACL as specific as possible.**

Don't permit "any" hosts if you can narrow it down. Make those "permit" rules as specific as possible. The same goes for protocols. Don't permit all IP protocols if you really mean a particular protocol. So don't undermine your security.

Generally, I like to build my ACLs in a structured way. First, I include a relatively small and very specific whitelist. It includes things that I know are always allowed, and overrides any blacklist rules that might come later.

## **6. The blacklist**

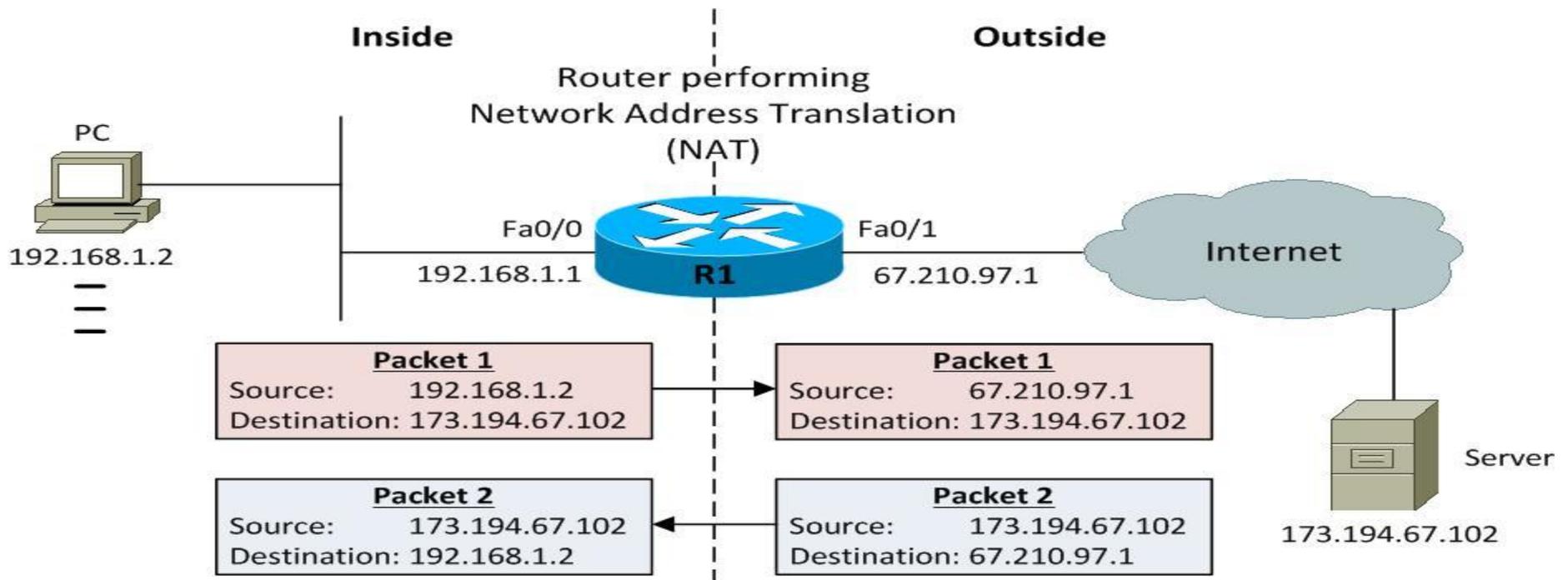
My general blacklist is usually a list of sites or IP address ranges representing geographic regions that I will never accept anything

# Cisco ASA NAT Configuration

Network Address Translation (NAT) is a service that enables private IP networks to use the internet and cloud. NAT translates private IP addresses in an internal network to a public IP address before packets are sent to an external network.

Network Address Translation (NAT) is a service that operates on an edge (Router, Firewall) to connect private networks to public networks like the internet. NAT is often implemented at the WAN edge to enable internet access in core, campus, branch, and colocation sites

## How it Works



## What are the Situations where Nat is required?

1. When we need to connect to the internet and our host don't have globally unique IP addresses
2. When we want to hide Internal IP addresses from outside for security purpose
3. A company is going to merge in another company which uses same address space

## Advantages of NAT

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.
- Nat also allow individuals and organizations use to establish cost effective and simple connection
- Nat prevents IP address overlapping

## Disadvantage of NAT

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

## Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:

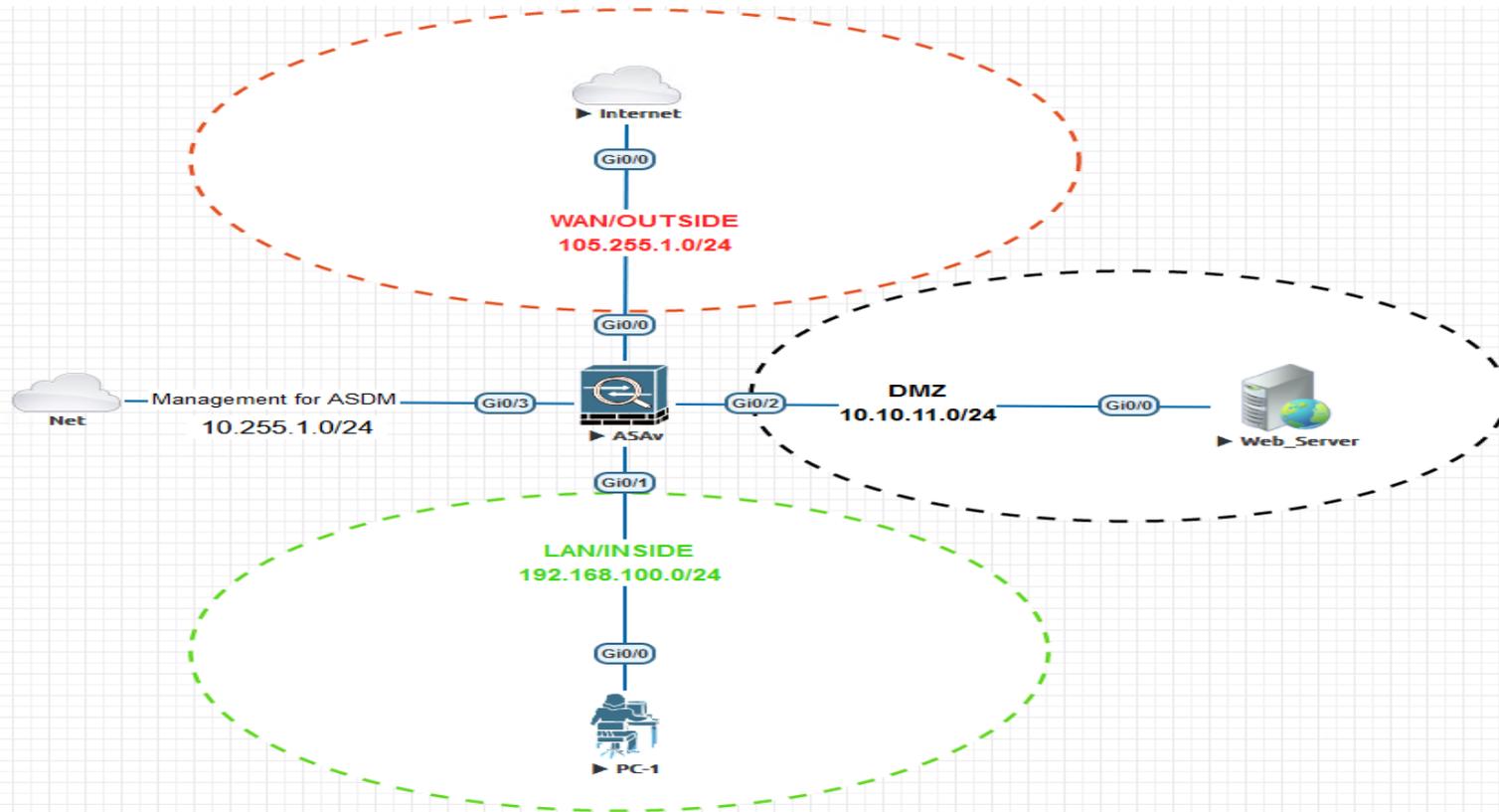
**Static NAT** – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.

**Dynamic NAT** – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.

Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

**Port Address Translation (PAT)** – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

# Dynamic NAT Project



## Network Object

In ASA every configuration of NAT requires object. When a packet enters the ASA, both the source and destination IP addresses are checked against the network object NAT rules. Object represents any one item.

- **Network Object**- Represents a single **IP address, Subnet or Range**
- **Service Object** – Represents a single Port/Protocol

**Port**- eq=equal,gt=greater than,lt=less than, neq=not equal, range  
**Protocol**-tcp, udp, icmp, gre,esp etc

### Dynamic Nat Project

1. Configure **network object** ip pool to be use for dynamic NAT for both public pool and DMZ pool

```
ASA-FW1(config)# object network Public_Pool
```

```
ASA-FW1(config-network-object)# range 105.255.1.100 105.255.1.200
```

```
ASA-FW1(config-network-object)# object network DMZ_Pool
```

```
ASA-FW1(config-network-object)# range 10.10.11.100 10.10.11.200
```

## 2. Configure dynamic NAT for users over the internet to access the Application of Web facing servers on port 23

```
ASA-FW1(config)# object network DMZ_TO_OUTSIDE
ASA-FW1(config-network-object)# subnet 10.10.11.0 255.255.255.0
ASA-FW1(config-network-object)# nat (DMZ,outside) dynamic Public_Pool
```

## 3. Generate traffic the DMZ to the internet to see if their IP packets are correctly translated.

```
Web_Server#telnet 105.255.1.2 23
Trying 105.255.1.2 ... Open
```

```
*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****
```

User Access Verification

Password:

**We have a connection, so let's see if we have a translation:**

```
ASA-FW1(config-network-object)# show nat
```

Auto NAT Policies (Section 2)

```
1 (DMZ) to (outside) source dynamic DMZ_TO_OUTSIDE Public_Pool  
translate_hits = 1, untranslate_hits = 0
```

```
ASA-FW1(config-network-object)# show nat
```

Auto NAT Policies (Section 2)

```
1 (DMZ) to (outside) source dynamic DMZ_TO_OUTSIDE Public_Pool  
translate_hits = 2, untranslate_hits = 0
```

```
ASA-FW1(config-network-object)# show nat de
```

Auto NAT Policies (Section 2)

```
1 (DMZ) to (outside) source dynamic DMZ_TO_OUTSIDE Public_Pool  
translate_hits = 2, untranslate_hits = 0  
Source - Origin: 10.10.11.0/24, Translated: 105.255.1.100-105.255.1.200
```

```
ASA-FW1(config-network-object)#show xlate
```

```
1 in use, 1 most used
```

```
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,  
s - static, T - twice, N - net-to-net
```

```
NAT from DMZ: 10.10.11.2 to outside: 105.255.1.157 flags i idle 0:05:01 timeout 3:
```

#### 4. Remove the following and use ASDM to configure same

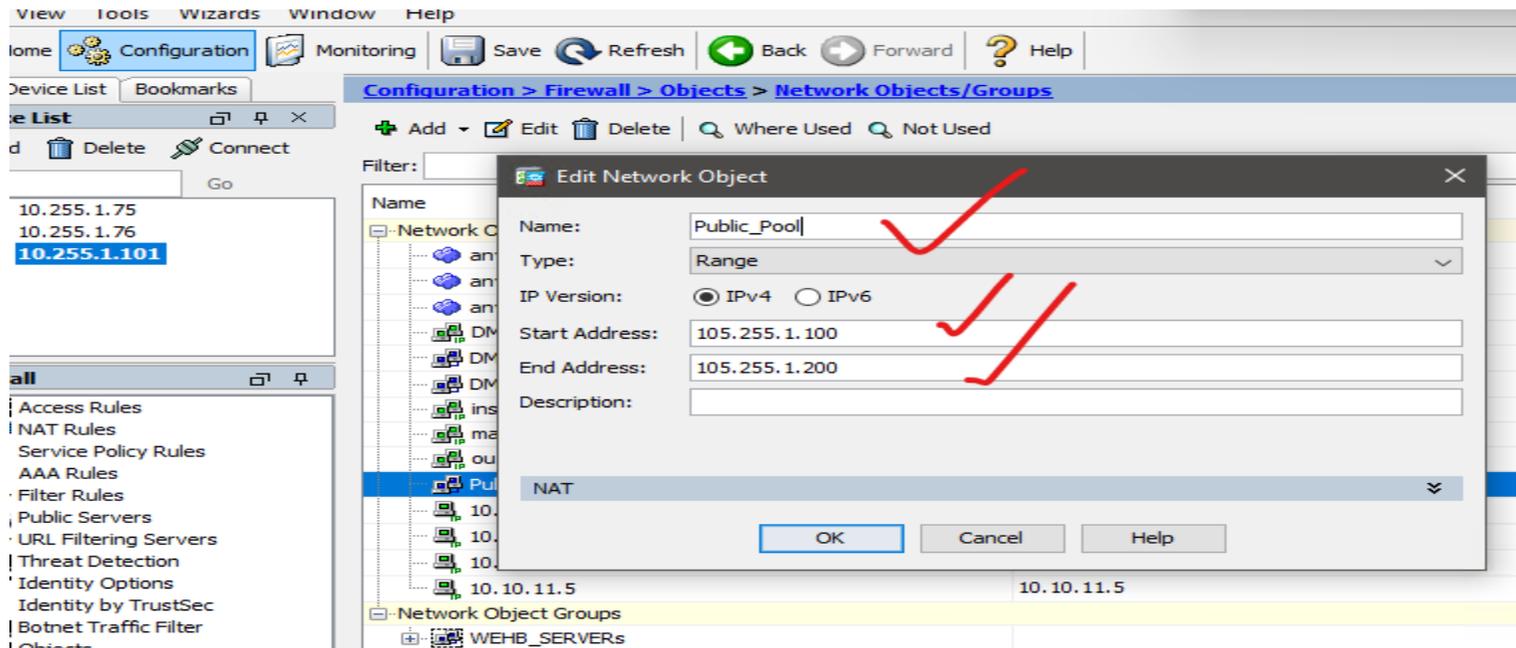
- a. NAT config –under nat rules
- b. Nat object – under object

#### 5. Apply ASDM configuration to configure same by remove nat configuration on cli

Using ASDM to create dynamic Nat

#### Step 1 Create your public object pool

Configuration > firewall > object> Add > add network object



## Step 2 Configure the Nat object for the outside

The screenshot displays the Cisco Firepower configuration interface. The main window is titled "Configuration > Firewall > NAT Rules". The left sidebar shows the "Firewall" configuration tree, with "NAT Rules" selected and highlighted in blue. A red checkmark is placed next to "NAT Rules" in the tree. Below the tree, the "Device Setup" section is visible, with "Firewall" selected and highlighted in blue, also marked with a red checkmark. The "Device List" section at the top left shows a search for "105.255.1.5". The main content area shows the "Add" menu for NAT Rules, with the following options: "Add NAT Rule Before 'Network Object' NAT Rules...", "Add 'Network Object' NAT Rule...", "Add NAT Rule After 'Network Object' NAT Rules...", "Insert...", and "Insert After...". A red checkmark is placed over the "Add" button, and a red arrow points to the "Add 'Network Object' NAT Rule..." option. A table with columns "Service" and "Action:" is partially visible on the right side of the main content area.

Service	Action:
	Source

Configuration > Firewall > NAT Rules

Match Criteria: Original Packet      Action: Translated Packet

#	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	Options	Description
"Network Object" NAT (No rules)										

**Add Network Object**

Name: DMZ-TO\_OUTSIDE ✓  
Type: Network ✓  
IP Version:  IPv4  IPv6 ✓  
IP Address: 10.10.11.0 ✓  
Netmask: 255.255.255.0 ✓  
Description:

**NAT**

Add Automatic Address Translation Rules

Type: Dynamic ✓

Translated Addr: ✓

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range

Enable Block Allocation

Block size of 512 and maximum block allocation per host 4 has been configured. To change click here

Fall through to interface PAT (dest intf): DMZ

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

**Browse Translated Addr**

Filter:  Filter Clear

Name	IP Address	Netmask	Description	Object NAT Address
Network Objects				
DMZ_Pool	10.10.11.100-10.11...			
Public_P...	105.255.1.100-10...			
10.10.1...	10.10.11.2			
10.10.1...	10.10.11.3			
10.10.1...	10.10.11.4			
10.10.1...	10.10.11.5			
Network Object Groups				
WEHB_...				
Interfaces				
DMZ				
inside				
manage...				
outside				

Selected Translated Addr

Translated Addr -> Public\_Pool ✓

OK Cancel

### Step3: apply the interface for the NAT

Click on the Nat rule > click on advance > apply on the right interface

The screenshot shows a network configuration interface with the following components:

- Configuration > Firewall > NAT Rules** (Breadcrumbs)
- Toolbar: Add, Edit, Delete, Find, Diagram, Packet Trace
- Match Criteria: Original Packet** table:

#	Source Intf	Dest Intf	Source	Destination	Service
1	Any	Any	DMZ-TO_OU...	any	any
- Action: Translated Packet** table:

Source	Destination	Service	Options	Description
Public				
- Edit Network Object** dialog:
  - Name: DMZ-TO\_OUTSIDE
  - Type: Network
  - IP Version: IPv4 (selected)
  - IP Address: 10.10.11.0
  - Netmask: 255.255.255.0
- NAT** configuration:
  - Add Automatic Address Translation Rules
  - Type: Dynamic
  - Translated Addr: Public\_Pool
  - Use one-to-one address translation
  - PAT Pool Translated Address: [empty]
  - Round Robin
  - Extend PAT uniqueness to per destination instead of per interface
  - Translate TCP and UDP ports into flat range 1024-65535
  - Enable Block Allocation
  - Fall through to interface PAT(dest intf): DMZ
  - Use IPv6 for interface PAT
- Advanced NAT Settings** dialog:
  - Translate DNS replies for rule
  - Interface: [empty]
  - Source Interface: DMZ
  - Destination Interface: outside

# 1. Step 4. Generate traffic from the internet to DMZ using packet tracer to test if the NAT is working.

Configuration > Firewall > Objects > Network Objects/Groups

ter: \_\_\_\_\_

ame \_\_\_\_\_ IP Addr \_\_\_\_\_

Network Objects

- any
- any4
- any6
- DMZ-network 10.10.1
- DMZ-TO\_OUTSIDE 10.10.1
- DMZ\_Pool 10.10.1
- inside-network 192.168
- management-network 10.255.
- outside-network 105.255
- Public\_Pool 105.255
- 10.10.11.2 10.10.1
- 10.10.11.3 10.10.1
- 10.10.11.4 10.10.1
- 10.10.11.5 10.10.1

Network Object Groups

- WEHB\_SERVERS

Cisco ASDM Packet Tracer - 10.255.1.101

Select the packet type and supply the packet parameters. Click Start to trace the packet.

Interface: DMZ Packet Type  TCP  UDP  SCTP  ICMP  IP

SGT number \_\_\_\_\_ (0-65535)

Source: IP Address 10.10.11.2 Destination: IP Address 105.255.1.2

Source Port: 23 Destination Port: 23

Show animation

DMZ AT Lookup NAT Lookup IP Options Lookup QOS QOS NAT Lookup IP Options Lookup Flow creation outside

Phase	Action
ROUTE-LOOKUP	✓
NAT	✓
NAT	✓
IP-OPTIONS	✓
QOS	✓
QOS	✓
NAT	✓
IP-OPTIONS	✓
FLOW-CREATION	✓
RESULT - The packet is allowed.	✓

Input Interface: DMZ Line + Link +

Output Interface: outside Line + Link +

Info:

Close Help

## Verify on the cli

ASA-FW1# **show nat**

Auto NAT Policies (Section 2)

1 (DMZ) to (outside) source dynamic DMZ-TO\_OUTSIDE Public\_Pool  
translate\_hits = 1, untranslate\_hits = 0

ASA-FW1# **show nat de**

Auto NAT Policies (Section 2)

1 (DMZ) to (outside) source dynamic DMZ-TO\_OUTSIDE Public\_Pool  
translate\_hits = 1, untranslate\_hits = 0

Source - Origin: 10.10.11.0/24, Translated: 105.255.1.100-105.255.1.200

ASA-FW1# **show xlate**

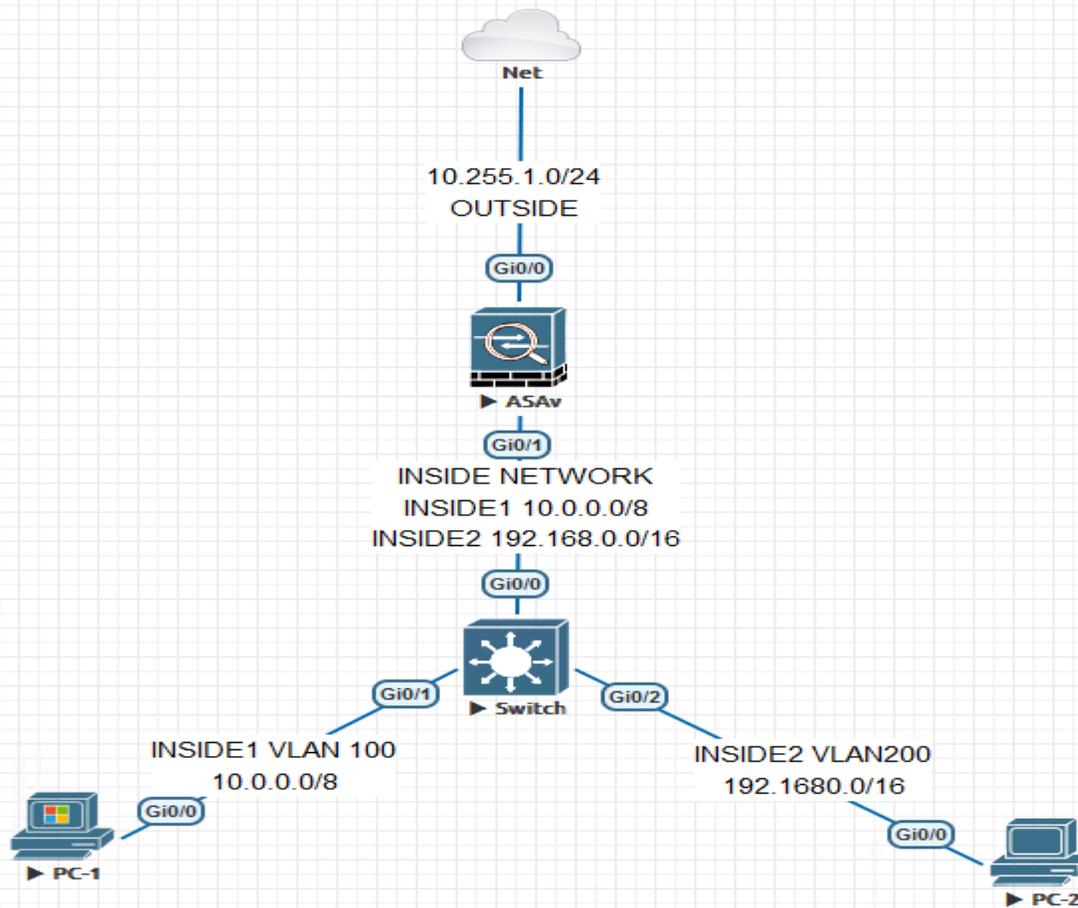
1 in use, 1 most used

Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,  
s - static, T - twice, N - net-to-net

NAT from DMZ: 10.10.11.2 to outside: 105.255.1.105 flags i idle 0:01:11 timeout 30

## PAT (NAT Overload)

PAT is primarily required when LAN users are translated to public IP (interface IP or IP from Public Pool). This type of **Dynamic NAT/PAT** configuration is used to provide internet access to LAN Users by translating LAN Subnet with Outside Interface of Firewall or any Public IP address.



## 1. Configuring ASDM access using the OUTSIDE interface for management and use the ASDM to create your LAN

```
ciscoasa(config)# int g0/0
ciscoasa(config-if)# des link to the Internet
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip add 10.255.1.201 255.255.255.0
ciscoasa(config-if)# no shut
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)# http server enable
ciscoasa(config)# http 10.255.1.0 255.255.255.0 outside
ciscoasa(config)# username admin pass cisco
```

**NB: With this configuration we can now access the ASDM**

## 2. Using the ASDM to Create the Interfaces for the LAN

Configure > Device setup > interface settings > interfaces > add

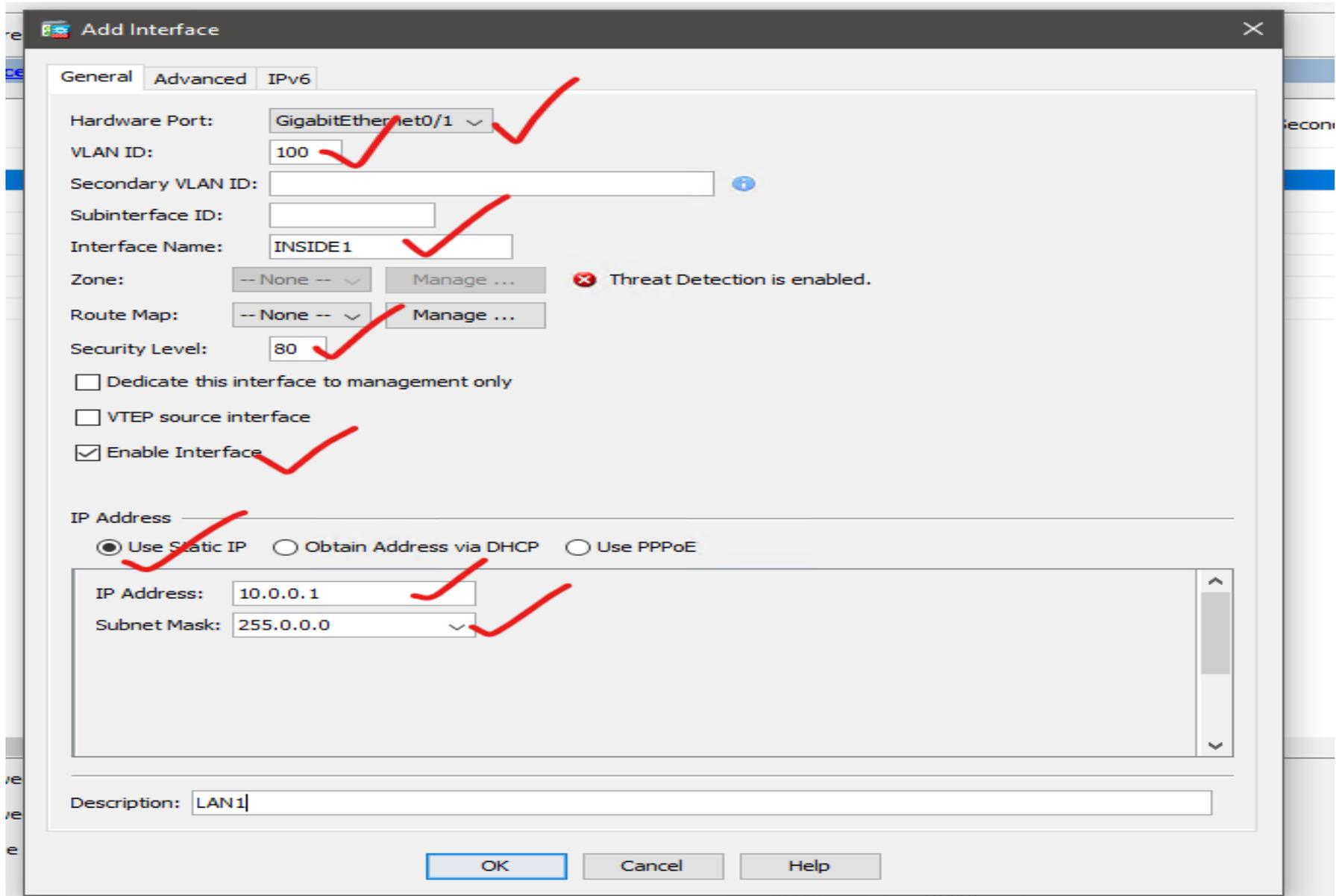
The screenshot shows the Cisco ASDM interface configuration page. The breadcrumb navigation is Configuration > Device Setup > Interface Settings > Interfaces. The left sidebar shows the navigation tree with 'Interface Settings' and 'Interfaces' highlighted. The main table lists interfaces from GigabitEthernet0/0 to Management0/0. The 'GigabitEthernet0/1' row is selected. A red checkmark is next to the 'Configuration' menu item. Another red checkmark is next to the 'Interfaces' folder in the sidebar. A third red checkmark is next to the 'Device Setup' folder in the sidebar. A red checkmark is also next to the 'Interface...' option in the 'Add' dropdown menu. The table below is a reproduction of the interface list shown in the screenshot.

Interface	Name	Zone	Route Map	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Secondary VLAN	Redundant	Member
GigabitEthernet0/0	outside			Yes		0 10.255.1.201	255.255.255.0		No	No
GigabitEthernet0/1				No					No	No
GigabitEthernet0/2				No					No	No
GigabitEthernet0/3				No					No	No
GigabitEthernet0/4				No					No	No
GigabitEthernet0/5				No					No	No
GigabitEthernet0/6				No					No	No
Management0/0				No					No	No

Below the table, there are three checkboxes:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface
- Enable jumbo frame reservation

Buttons for 'Apply' and 'Reset' are visible at the bottom.



### 3. Repeat same for the second sub interface using vlan 200

**Edit Interface**

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/1.200

VLAN ID: 200

Secondary VLAN ID: Separate multiple values with comma or space ⓘ

Subinterface ID: 200

Interface Name: INSIDE2

Zone: -- None -- Manage ... ❌ Threat Detection is enabled.

Route Map: -- None -- Manage ...

Security Level: 100

Dedicate this interface to management only

VTEP source interface

Enable Interface

IP Address

Use Static IP  Obtain Address via DHCP  Use PPPoE

IP Address: 192.168.0.1

Subnet Mask: 255.255.0.0

Description: LNA2

OK Cancel Help

## Verify with the command line

```
ASA-FW1 (config-if)# show int ip br
```

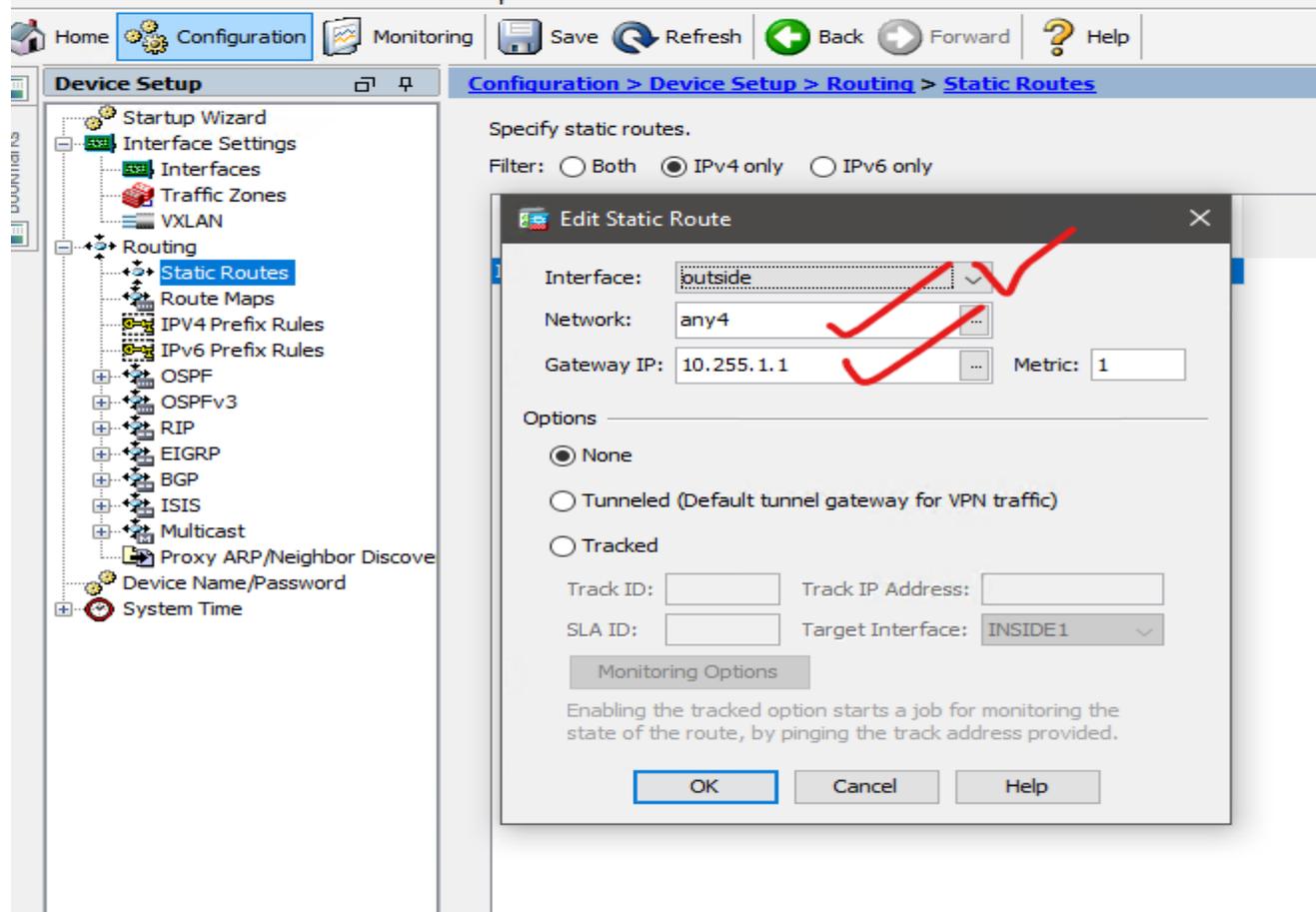
Interface	IP-Address	OK?	Method	Status	Prot
ocol					
GigabitEthernet0/0	10.255.1.101	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/1.100	10.0.0.1	YES	manual	up	up
GigabitEthernet0/1.200	192.168.0.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	up
GigabitEthernet0/3	unassigned	YES	unset	administratively down	up
GigabitEthernet0/4	unassigned	YES	unset	administratively down	up
GigabitEthernet0/5	unassigned	YES	unset	administratively down	up
GigabitEthernet0/6	unassigned	YES	unset	administratively down	up
Management0/0	unassigned	YES	unset	administratively down	up

```
ASA-FW1 (config-if)# show nameif
```

Interface	Name	Security
GigabitEthernet0/0	outside	0
GigabitEthernet0/1.100	INSIDE1	80
GigabitEthernet0/1.200	INSIDE2	100

## 4. Configure default route using ASDM

Configure >device setup>static route >add



## 5. Configure PAT as your NAT protocol to give internet access to your inside network

Let's create for inside1 on network of 10.0.0.0/16

The screenshot shows the Mikrotik WinBox configuration interface. The main window displays the NAT Rules configuration page. A table lists two NAT rules:

#	Match Criteria: Original Packet	Action: Translated Packet								
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	Options	Description
1	Any	outside	INSIDE1	any	any	any	any	any		
2	Any	outside	INSIDE2	any	any	any	any	any		

An 'Edit Network Object' dialog box is open, showing the configuration for the 'INSIDE1' network object. The fields are as follows:

- Name: INSIDE1
- Type: Network
- IP Version: IPv4 (selected)
- IP Address: 10.0.0.0
- Netmask: 255.255.0.0
- Description: (empty)

The NAT configuration section is also visible:

- Add Automatic Address Translation Rules
- Type: Dynamic PAT (Hide)
- Translated Addr: outside
- Use one-to-one address translation
- PAT Pool Translated Address: (empty)
- Round Robin
- Extend PAT uniqueness to per destination instead of per interface
- Translate TCP and UDP ports into flat range 1024-65535
- Include range 1-1023
- Enable Block Allocation
- Block size of 512 and maximum block allocation per host 4 has been configured. To change click [here](#).
- Fall through to interface PAT(dest intf): INSIDE1
- Use IPv6 for interface PAT

Red checkmarks are drawn over the 'INSIDE1' name, 'Network' type, 'IPv4' radio button, '10.0.0.0' IP address, '255.255.0.0' netmask, and the 'Add Automatic Address Translation Rules' checkbox.

## Let's create for inside2 on network of 192.168.0.0/16

The screenshot displays the Cisco Firepower configuration interface. The main window is titled "Configuration > Firewall > NAT Rules". The "Match Criteria: Original Packet" table is visible, showing two rules:

#	Source Intf	Dest Intf	Source	Des
1	Any	outside	INSIDE1	
2	Any	outside	INSIDE2	

The "Edit Network Object" dialog box is open, showing the configuration for the "INSIDE2" network object:

- Name: INSIDE2
- Type: Network
- IP Version: IPv4 (selected)
- IP Address: 192.168.0.0
- Netmask: 255.255.0.0
- Description: (empty)

The NAT configuration section is expanded, showing:

- Add Automatic Address Translation Rules
- Type: Dynamic PAT (Hide)
- Translated Addr: outside
- Use one-to-one address translation

The "Device List" on the left shows the IP address 10.255.1.101 selected. The "Firewall" tree on the left shows the "NAT Rules" configuration path.

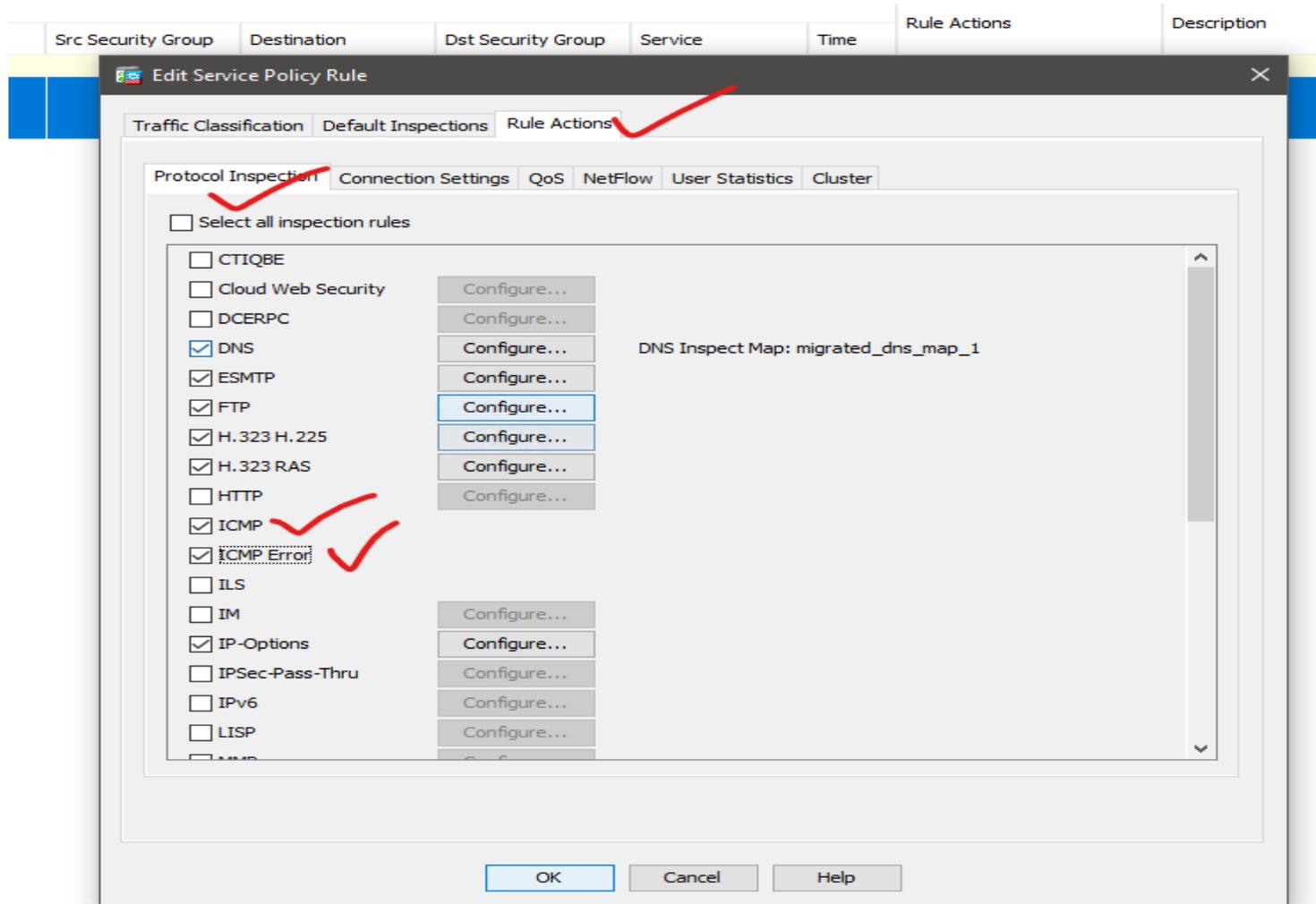
## 6. Configure ICMP inspection on ASDM to allow ping access

### Configure>firewall>Service Policy Rules

The screenshot displays the ASDM configuration interface for Firewall Service Policy Rules. The left sidebar shows the navigation tree with 'Service Policy Rules' selected. The main area shows a table of traffic classification rules. A rule named 'inspection\_de...' is highlighted in blue. Red handwritten annotations include a checkmark on the 'Service Policy Rules' menu item, a checkmark on the 'inspection\_de...' rule name, and a checkmark on the 'Match' column of the rule. The rule's actions include 'Inspect DNS Map migrate...' and 'Inspect ESMTMP (13 more inspect actions)'.

Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	Rule Actions	Description
Global; Policy: global_policy											
inspection_de...			Match	any		any		default-inspec...		Inspect DNS Map migrate... Inspect ESMTMP (13 more inspect actions)	

1. Select Rule Actions
2. Click Protocol Inspection
3. Check "ICMP" and "ICMP Error" and hit OK



Now we can verify on both PCs for internet access

### Configurations to be done on the switch

```
SW1(config)#interface g0/0
```

```
SW1(config-if)#switchport trunk encapsulation dot1q
```

```
SW1(config-if)#switchport mode trunk
```

```
SW1(config)#interface g0/1
```

```
SW1(config-if)#switchport mode access
```

```
SW1(config-if)#switchport access vlan 100
```

### Router USERS Configuration as seen on the topology

```
PC-1(config)#hostname PC1
```

```
PC-1(config)#int g0/0
```

```
PC-1(config-if)#ip add 10.0.0.2 255.255.0.0
```

```
PC-1(config-if)#no shut
```

```
PC-1(config-if)#ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

PC-1(config)#**ip domain-lookup ( Do be able to ping a domain name)**

PC-1(config)#**ip name-server 8.8.8.8 ( to give access to public DNS Server)**

PC1(config)#**do ping 8.8.8.8**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 30/32/34 ms

PC1(config)#**do ping facebook.com**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 31.13.66.35, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 27/34/41 ms

## PC2 Configuration

PC-2(config)#**int g0/0**

PC-2(config-if)#**ip add 192.168.0.2 255.255.0.0**

PC-2(config-if)#**no shut**

PC-2(config-if)#**ip route 0.0.0.0 0.0.0.0 192.168.0.1**

PC-2(config)#ip domain-lookup( Do be able to ping a domain name)

PC-2(config)#ip name-server 8.8.8.8 ( to give access to public DNS Server)

PC2 (config)#do ping 8.8.8.8

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/33 ms

PC2(config)#do ping ghanaweb.com

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 104.21.41.135, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/33/41 ms

## Let's now verify the NAT on the ASA

ASA-FW1 (config-if)# **show nat**

Auto NAT Policies (Section 2)

1 (any) to (outside) source dynamic **INSIDE1 interface**  
**translate\_hits = 5**, untranslate\_hits = 0

2 (any) to (outside) source dynamic **INSIDE2 interface**  
**translate\_hits = 3**, untranslate\_hits = 0

ASA-FW1 (config-if) #**show xlate**

1 in use, 3 most used

Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,  
s - Static, T - twice, N - net-to-net

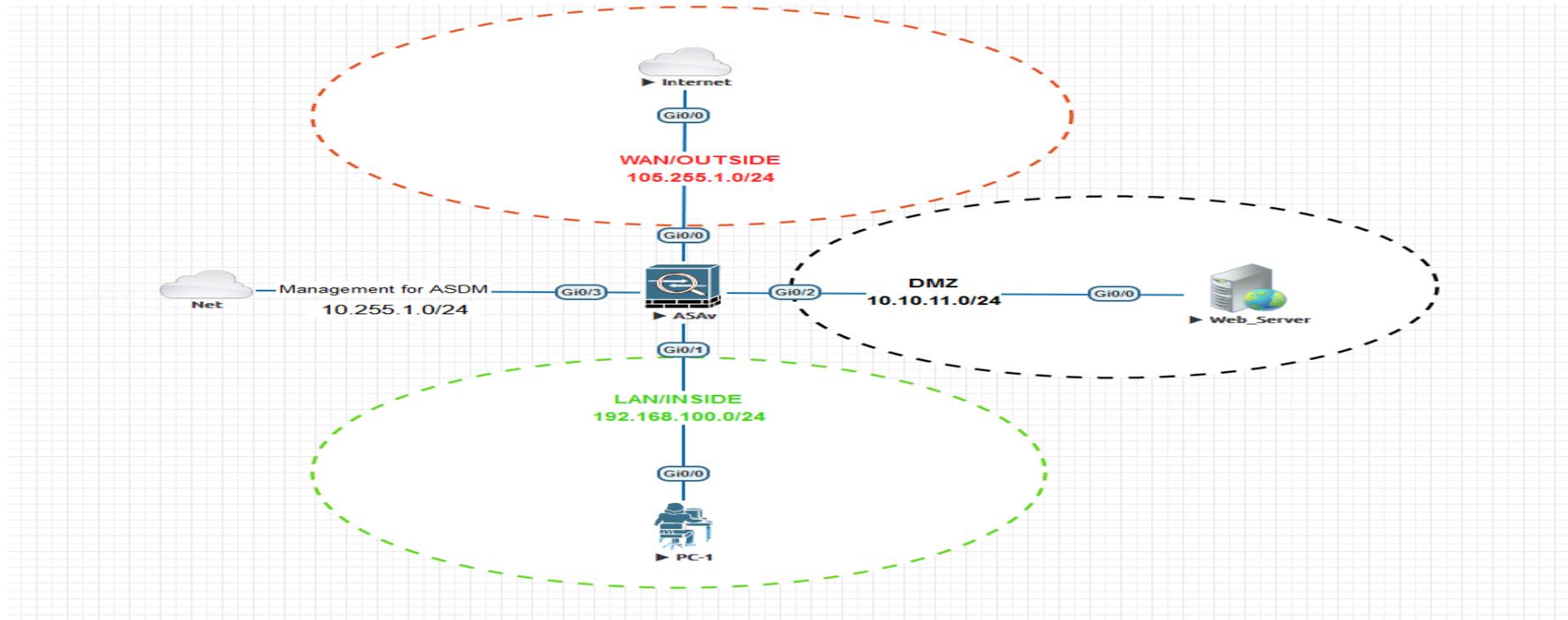
ICMP PAT from any: **192.168.0.2/6** to **outside:10.255.1.101/6** flags ri idle 0:00:04 timeout 0:00:30

## STATIC NAT PROJECT

Static NAT is primarily required when a Data Center or Hub site has WEB Facing Server in **DMZ Zone** or **Inside Zone** and Users over the **Internet** need to access the Application of Web Facing server. The applications may be **Web (HTTP/HTTPS) Server**, **Email Server** or even **FTP server**. Below is a sample scenario where an Application server is hosted in DMZ Zone and needs to be accessed from outside (Internet)

**Project Task.** Configure an inbound rule to allow users on the internet to connect to our DMZ E-Commerce Webserver (10.10.11.2) listening on port 443

### Static NAT Project LAB



**Step 1.** First, we will create a network object that defines our “webserver” in the DMZ and also configure to what IP address it should be translated

```
ASA-1(config) # object network WEB-SERVER
```

```
ASA-1(config-network-object) # host 10.10.11.2
```

```
ASA-1(config-network-object) # nat (DMZ, OUTSIDE) static 105.255.1.200
```

**NB:** The configuration above tells the ASA that whenever an outside device connects to IP address 105.255.1.200, it should be translated to IP address 10.10.11.2. This takes care of NAT, but we still have to create an access-list or traffic will be dropped

```
ASA1(config)# access-list OUTSIDE_TO_DMZ extended permit tcp any host 10.10.11.2 eq 443
```

```
ASA1 (config)# access-group OUTSIDE_TO_DMZ in interface OUTSIDE
```

This enables the access-list on the outside interface

```
Internet#telnet 105.255.1.200 443
```

```
Trying 105.255.1.200, 443 ... Open
```

ASA-FW1(config)# **show access-list**

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)

    alert-interval 300

access-list outside\_access\_in; 1 elements; name hash: 0x6892a938

access-list outside\_access\_in line 1 extended permit tcp any object Web\_Server eq https (hitcnt=1) 0xf2417cc4

ASA-FW1(config)# **show xlate**

1 in use, 1 most used

Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,

    s - Static, T - twice, N - net-to-net

NAT from DMZ: 10.10.11.2 to outside: 105.255.1.200

    Flags s idle 0:00:09 timeout 0:00:00

## Apply same configuration using ASDM the same Project Task

Step-1 create a network object that defines our “webserver” in the DMZ and also configure to what IP address it should be translated.

The screenshot displays the ASDM configuration interface for NAT rules. The main window shows the 'Add Network Object' dialog box, which is used to define a network object named 'WEB-SERVER' of type 'Host' with IP address '10.10.11.2'. The 'Advanced NAT Settings' dialog box is also open, showing the configuration for the NAT rule. The 'NAT' section is checked, and the 'Add Automatic Address Translation Rules' checkbox is selected. The 'Type' is set to 'Static' and the 'Translated Addr' is '10.255.1.200'. The 'Source Interface' is 'DMZ' and the 'Destination Interface' is 'outside'. The 'Service' is 'TCP' and the 'Protocol' is 'tcp'. The 'Real Port' and 'Mapped Port' fields are empty. The 'Advanced NAT Settings' dialog box also shows options for 'Translate DNS replies for rule', 'Disable Proxy ARP on egress interface', and 'Lookup route table to locate egress interface', all of which are unchecked. The 'Interface' section shows 'Source Interface: DMZ' and 'Destination Interface: outside'. The 'Service' section shows 'Protocol: tcp' and 'Real Port: ' and 'Mapped Port: '.

Configuration > Firewall > NAT Rules

Match Criteria: Original Packet

#	Source Intf	Dest Intf	Source	Destination	Service	Action
						"Network Object" NAT (No rules)

Add Network Object

Name: WEB-SERVER ✓

Type: Host

IP Version:  IPv4  IPv6

IP Address: 10.10.11.2 ✓

Description:

Advanced NAT Settings

Translate DNS replies for rule

Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Interface

Source Interface: DMZ ✓

Destination Interface: outside ✓

Service

Protocol: tcp ✓

Real Port:

Mapped Port:

OK Cancel Help

NAT

Add Automatic Address Translation Rules

Type: Static ✓

Translated Addr: 10.255.1.200 ✓

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Ind

Enable Block Allocation

Block size of 512 and maximum block allocation per host 4 has been configured. To change click [here](#).

Fall through to interface PAT(dest intf): DMZ

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

## Step.2 Apply ACL allow inbound traffic

The screenshot displays the 'Edit Access Rule' dialog box within a network configuration interface. The dialog is titled 'Edit Access Rule' and is divided into 'Source Criteria' and 'Destination Criteria' sections. The 'Interface' is set to 'outside'. The 'Action' is set to 'Permit'. The 'Source Criteria' section shows 'Source' as 'any', 'User' as an empty field, and 'Security Group' as an empty field. The 'Destination Criteria' section shows 'Destination' as 'Web\_Server', 'Security Group' as an empty field, and 'Service' as 'tcp/https'. The 'Description' field is empty. The 'Enable Logging' checkbox is checked, and the 'Logging Level' is set to 'Default'. The 'More Options' section is collapsed. The 'OK', 'Cancel', and 'Help' buttons are at the bottom. Red checkmarks are drawn over the 'any' source, 'Web\_Server' destination, 'tcp/https' service, and the 'OK' button.

Configuration > Firewall > Access Rules

Device List

Device List

10.255.1.75  
10.255.1.76  
10.255.1.101

Access Rules

NAT Rules

Service Policy Rules

AAA Rules

Filter Rules

Public Servers

URL Filtering Servers

Threat Detection

Identity Options

Identity by TrustSec

Botnet Traffic Filter

Objects

Network Objects/Groups

Service Objects/Groups

Local Users

Local User Groups

Security Group Object Group

Class Maps

Inspect Maps

Regular Expressions

TCP Maps

Time Ranges

Unified Communications

Advanced

DMZ

inside

man

outside

Global

Interface: outside

Action:  Permit  Deny

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: Web\_Server

Security Group:

Service: tcp/https

Description:

Enable Logging

Logging Level: Default

More Options

OK Cancel Help

Internet#telnet 105.255.1.200 443

Trying 105.255.1.200, 443 ... Open

ASA-FW1(config)# show access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)

alert-interval 300

access-list outside\_access\_in; 1 elements; name hash: 0x6892a938

access-list outside\_access\_in line 1 extended permit tcp any object Web\_Server eq https (hitcnt=1) 0xf2417cc4

ASA-FW1(config)# show xlate

1 in use, 1 most used

Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,

s - Static, T - twice, N - net-to-net

NAT from DMZ: 10.10.11.2 to outside: 105.255.1.200

Flags s idle 0:00:09 timeout 0:00:00

## STATIC NAT Port Forwarding

NAT Port Forwarding is useful when you have a single public IP address and multiple devices behind it that you want to reach from the outside world

**Project Task-1:** Whenever someone connects on IP address 105.255.1.1 TCP port 80 we will forward them to 10.10.11.2 TCP port 80.

**Step-1:** We create a network object that specifies the real IP address of the web server and then we create our NAT rule. By using the keyword **interface** we tell the ASA to use the IP address on the (outside) interface. The first port number is the port that the server is **listening on**, the second port number is the outside port number

Using command Line to configure

```
ASA-1(config) # object network WEB-SERVER
```

```
ASA-1(config-network-object) #host 10.10.11.2
```

```
ASA-1(config-network-object) # nat (DMZ,OUTSIDE) static interface service tcp 80 80
```

We can also use the keyword **interface** we tell the ASA to use the IP address on the (outside) interface.

**Step 2:** let's configure Access List to allow traffic from the outside to the sever

```
ASA-1(config)# access-list out_DMZ extended permit tcp any host 192.168.3.1 eq 80
```

```
ASA1(config)# access-group out_DMZ in interface OUTSIDE
```

Let's generate some traffic for testing

```
Internet#telnet 105.255.1.200 80
```

```
Trying 105.255.1.200, 80 ... Open
```

```
X
```

```
ASA-FW1(config)# show xlate
```

```
1 in use, 2 most used
```

```
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
```

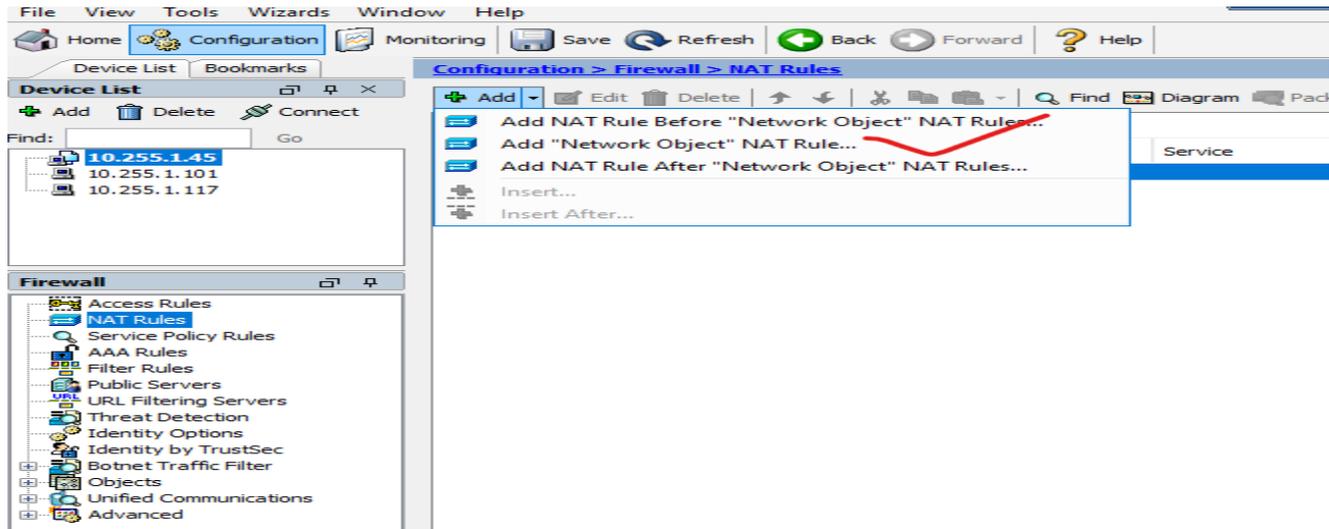
```
      s - static, T - twice, N - net-to-net
```

```
TCP PAT from DMZ: 10.10.11.2 80-80 to outside: 105.255.1.1 80-80
```

```
flags sr idle 0:00:18 timeout 0:00:00
```

## Using ASDM to configure same

### Step 1; Creating the static Nat port forwarding on port 80 80



Monitoring Save Refresh Back Forward Help

Configuration > Firewall > NAT Rules

Add Edit Delete Find Diagram Packet Trace

Match Criteria: Original Packet

#	Source Intf	Dest Intf	Source	Destination	Service	Action
"Network Object" NAT (Rule 1)						
1	DMZ	outside	WEB_SERVER	any	tcp http	105.255.1.200
	outside	DMZ	any	105.255.1.200	tcp http	-- Origin

### Edit Network Object

Name: WEB\_SERVER

Type: Host

IP Version:  IPv4  IPv6

IP Address: 10.10.11.2

Description:

---

**NAT**

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 105.255.1.200

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range

Enable Block Allocation

Block size of 512 and maximum block allocation per host 4 has been configured. To change click [here](#)

Fall through to interface PAT(dest intf): DMZ

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

### Advanced NAT Settings

Translate DNS replies for rule

Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Interface

Source Interface: DMZ

Destination Interface: outside

Service

Protocol: tcp tcp

Real Port: 80

Mapped Port: 80

OK Cancel Help

## Let generate traffic on the internet

```
Internet#telnet 105.255.1.200 80
Trying 105.255.1.200, 80 ... Open
```

## Let's take look at the ASA NAT table

```
ciscoasa(config)# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
TCP PAT from DMZ:10.10.11.2 80-80 to outside:105.255.1.200 80-80
      flags sr idle 0:00:17 timeout 0:00:00
```

```
ciscoasa(config)# show nat
```

### Auto NAT Policies (Section 2)

```
1 (DMZ) to (outside) source static WEB_SERVER 105.255.1.200 service tcp www www
  translate_hits = 1, untranslate_hits = 0
```

```
ciscoasa(config)# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
TCP PAT from DMZ:10.10.11.2 80-80 to outside:105.255.1.200 80-80
      flags sr idle 0:03:36 timeout 0:00:00
```

## Introduction Firewall Architecture Design

These are different design topologies where we describe how a customer is connected (using BGP or default route) to one or more ISPs.

### Various ISP Connection Types

- **Single homed:** you are connected to a single ISP using a single link.
- **Dual homed:** you are connected to a single ISP using dual links.
- **Single multi-homed:** you are connected to two ISPs using single links.
- **Dual multi-homed:** you are connected to two ISPs using dual links

### Single Homed Architecture

The single homed design means you have a single connection to a single ISP. With this design, you don't need BGP since there is only one exit path in your network. You might as well just use a static default route that points to the ISP.

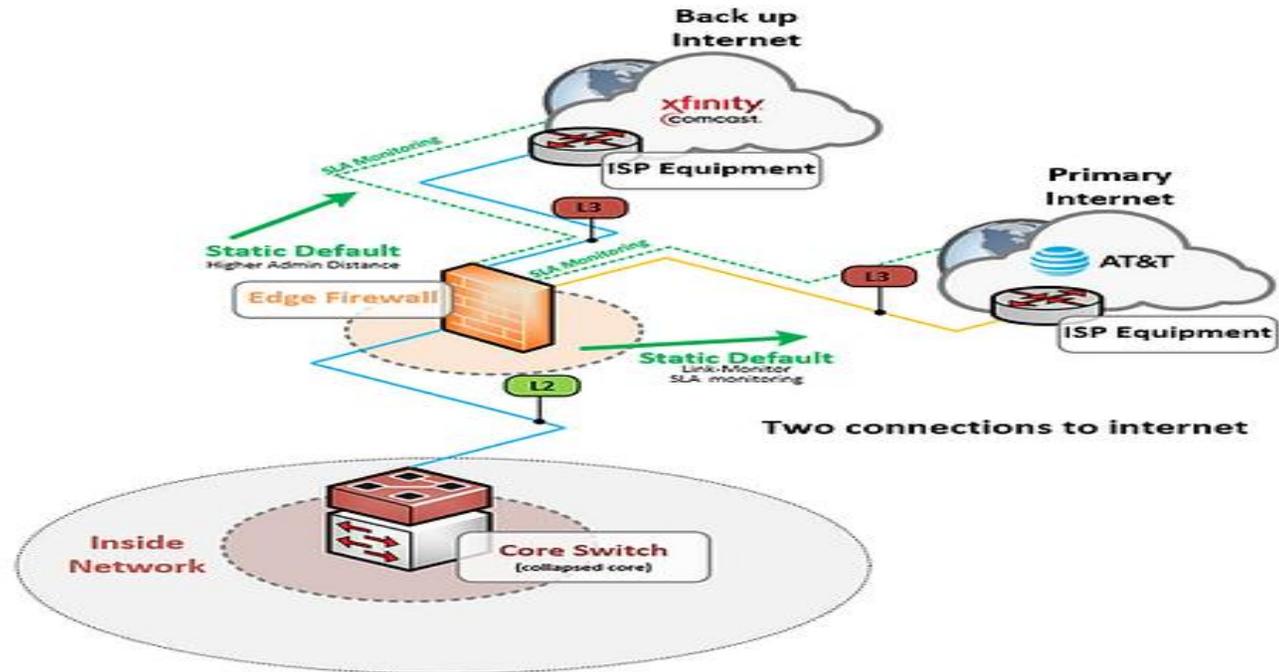
The advantage of a single-homed link is that it's cost effective, the disadvantage is that you don't have any redundancy. Your link is a single point of failure but so is using a single ISP



## Single Multi-homed Architecture

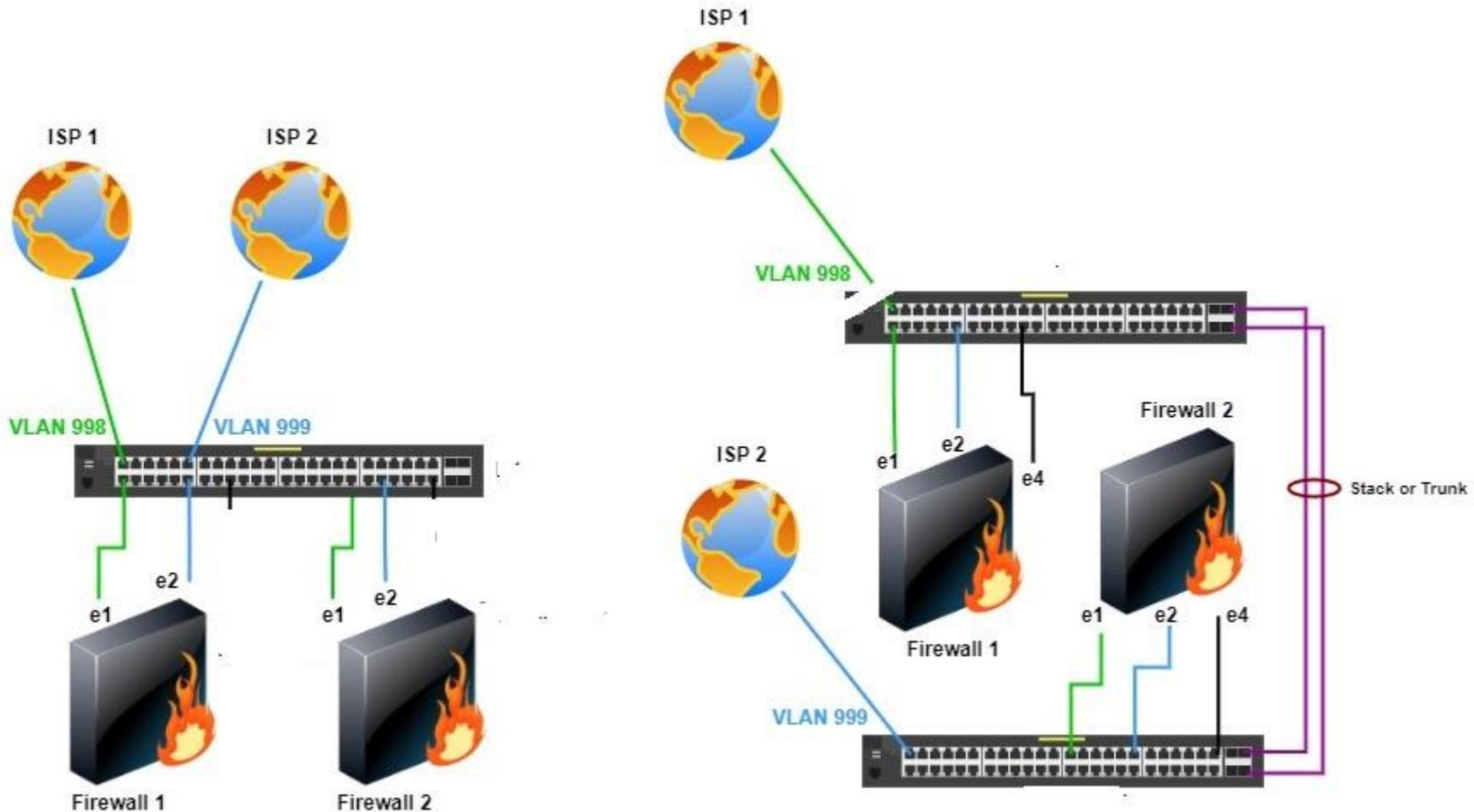
Multihomed means we are connected to at least two different ISPs. The simplest design looks like this:

### High Level SMB



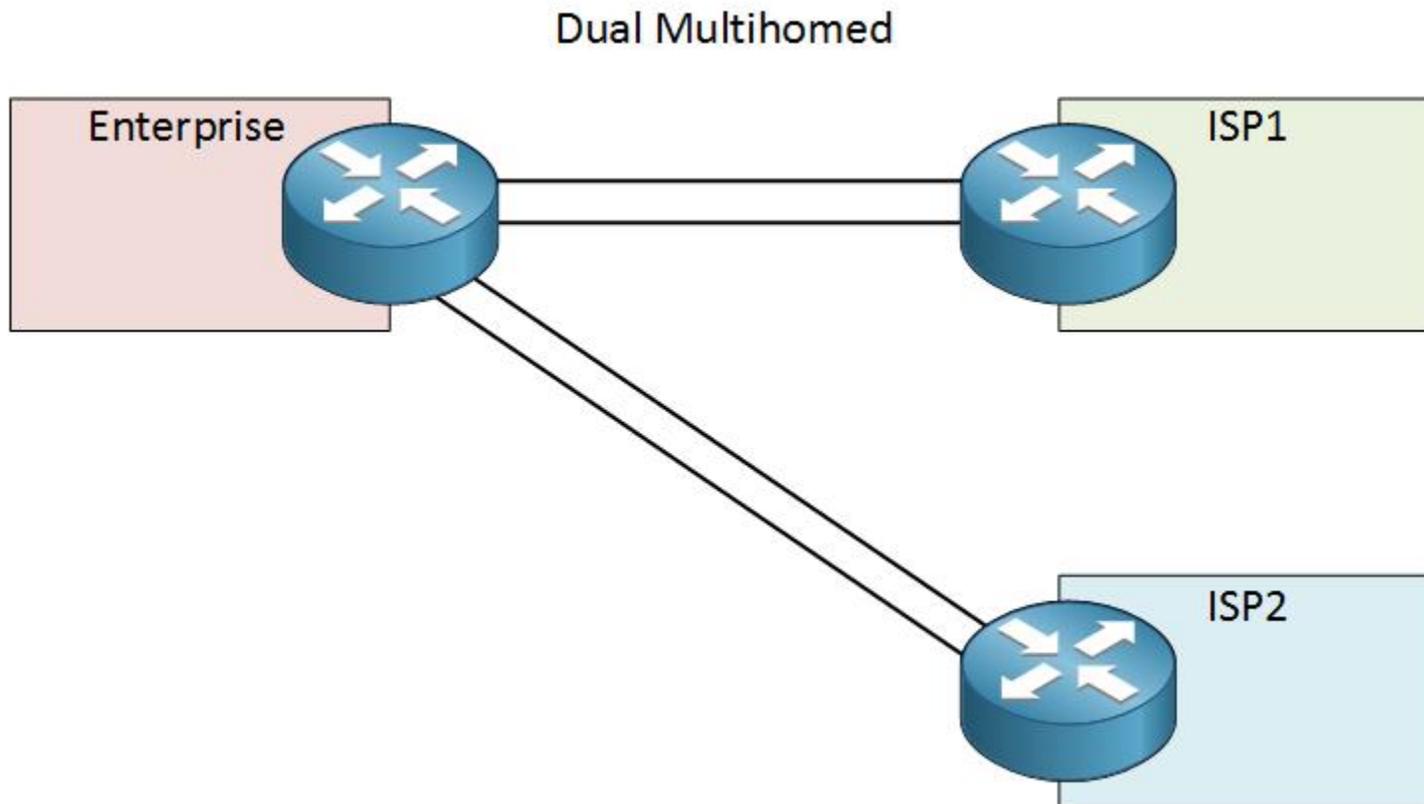
Above you see that we have a single ASA or Router at the customer, connected to two different ISPs. The single point of failure in this design is that you only have one ASA at the customer. When it fails, you won't be able to connect to any ISP.

We can improve this by adding a second ASA shown below, this is a pretty good design, we only use single links, but we are connected to two different ISPs using different routers.



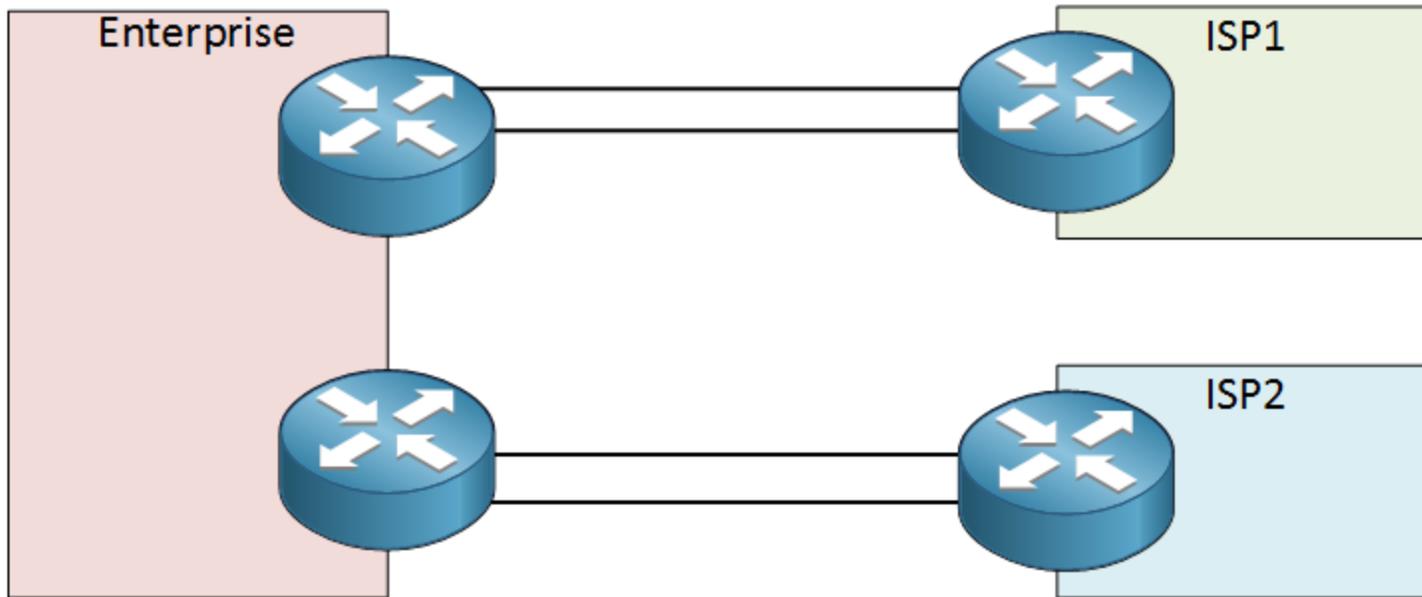
## Dual Multihomed

The dual multihomed designs means we are connected to two different ISPs, and we use redundant links. There are some variations, here's the first one



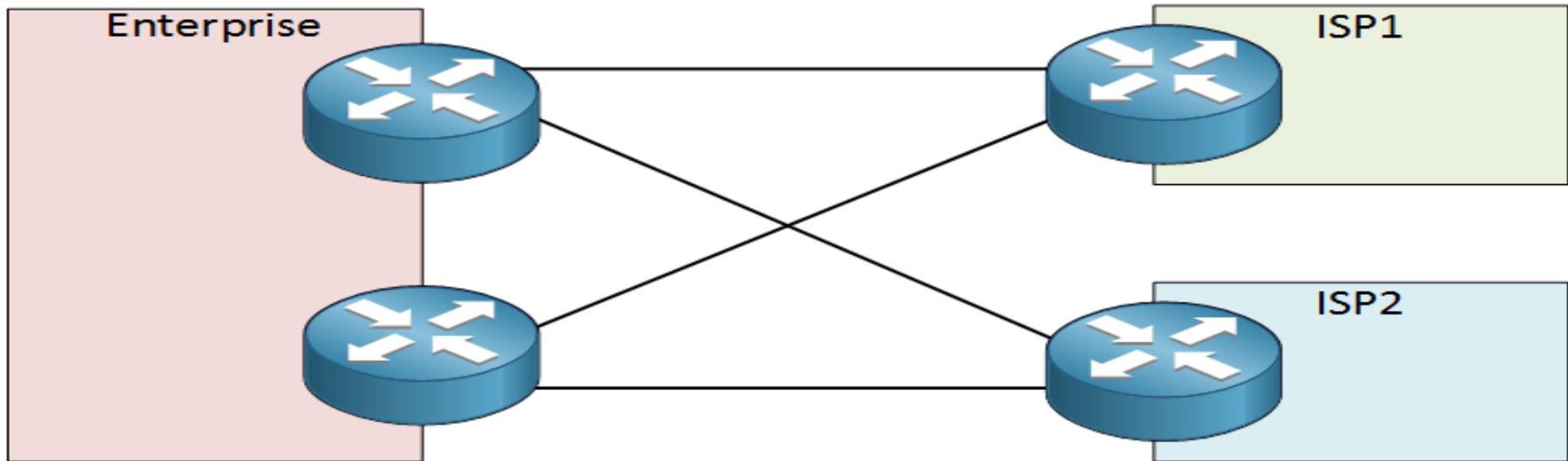
Using one router and two links to each ISP. We have redundant ISPs and links, but the router is still a single point of failure. We can improve this by adding a second router

## Dual Multihomed



The design above is better; it has two customer routers. One disadvantage, however, is that once one of your router fails, you will lose the connection to one of the ISPs. Using the same number of routers and links, the following design might be better:

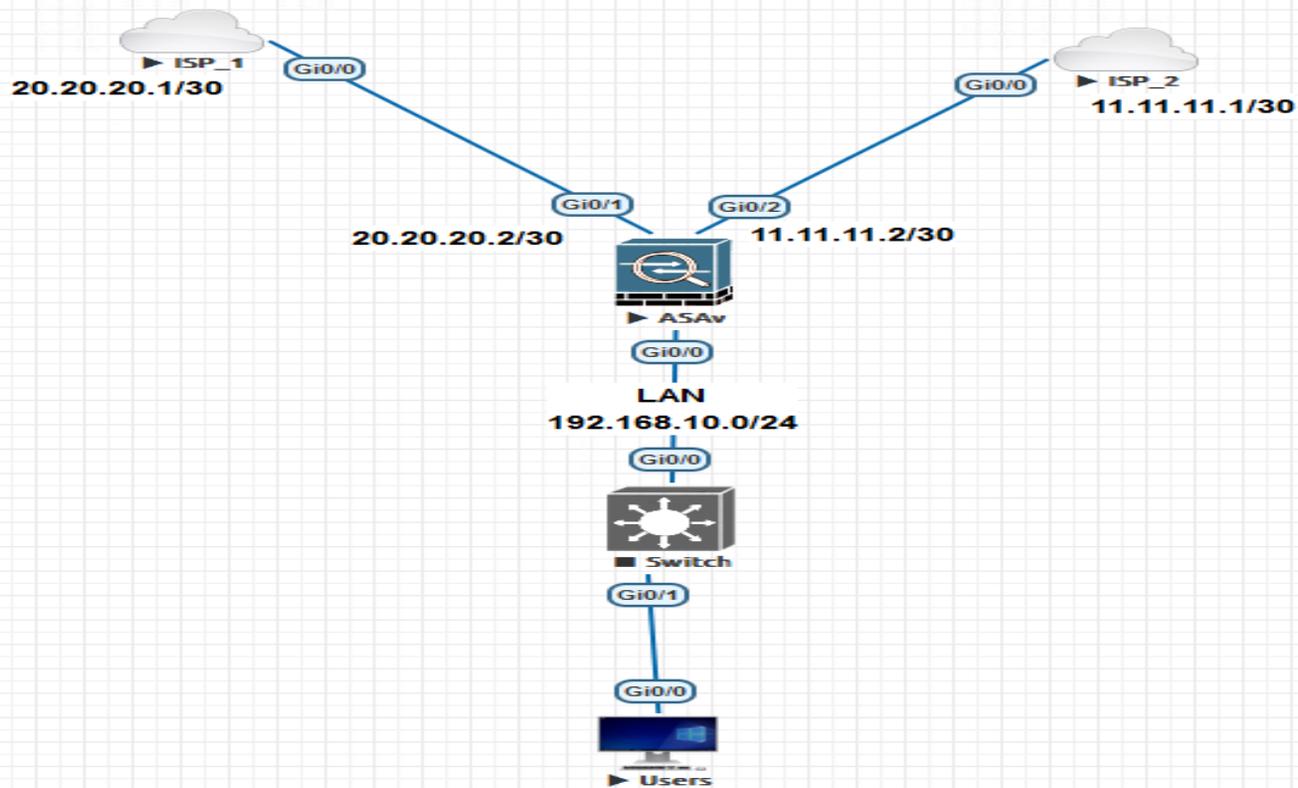
## Dual Multihomed



This design has redundant ISPs, routers, and links. Both customer routers are connected to both ISPs. This design does offer the highest redundancy but it's also an expensive option.

## DUAL WAN ON CISCO ASA

Cisco ASA 5500 series firewall supports now the **Dual-ISP** capability. You can connect two interfaces of the firewall to two different ISPs and use the new “**SLA Monitor**” feature (SLA=Service Level Monitoring) to monitor the link to the primary ISP, and if that fails, the traffic is routed to the Backup ISP.



## 1. Configure all interfaces required including the one to be use for secondary ISP

```
ciscoasa(config-if)# interface GigabitEthernet0/0
```

```
ciscoasa(config-if)# nameif inside
```

```
ciscoasa(config-if)# security-level 100
```

```
ciscoasa(config-if)# ip address 192.168.10.1 255.255.255.0
```

```
ciscoasa(config-if)# no shut
```

```
ciscoasa(config-if)# interface GigabitEthernet0/1
```

```
ciscoasa(config-if)# nameif outside
```

```
ciscoasa(config-if)# security-level 0
```

```
ciscoasa(config-if)# ip address 20.20.20.2 255.255.255.252
```

```
ciscoasa(config-if)# no shut
```

```
ciscoasa(config-if)# interface GigabitEthernet0/2
cocoas(config-if)# nameif outside_backup00
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 11.11.11.2 255.255.255.252
cocoasa(config-if)# no shut
```

## 2. Configure the two ISP routers base on the topology and define a default route

```
Router(config)#hostname ISP
ISP-1(config)#int g0/0
ISP-1(config-if)#ip add 20.20.20 .1 255.255.255.252
ISP-1(config-if)#no shut
ISP-1(config-if)#int l0
ISP-1(config-if)#ip add 8.8.8.8 255.255.255.255
ISP-1(config-if)#ip route 0.0.0.0 0.0.0.0 20.20.20.2
ISP-1(config)#do ping 20.20.20.2
```

Typ escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 20.20.20.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/8 ms

Router(config)#hostname ISP\_2

ISP-2(config-if)#ip add 11.11.11.1 255.255.255.252

ISP-2(config-if)#no shut

ISP-2(config-if)#

ISP-2(config-if)#int l0

ISP-2(config-if)#ip add 8.8.8.8 255.255.255.255

ISP-2(config-if)#

ISP-2(config-if)#ip route 0.0.0.0 0.0.0.0 11.11.11.2

ISP-2(config)#do ping 11.11.11.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 11.11.11.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/8 ms

```
USER1(config)# Hostname USER1
```

```
USER1(config)#int g0/0
```

```
USER1(config-if)#ip add 192.168.10.2 255.255.255.0
```

```
USER1(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

```
USER1(config)#do ping 192.168.10.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/15 ms

### 3. Enable icmp inspection on the cisco ASA to allow users to ping across the ASA

```
policy-map global_policy  
class inspection_default  
inspect icmp
```

```
USER1(config)#do ping 20.20.20.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:

```
!!!!
```

```
USER1 (config)#do ping 11.11.11.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 11.11.11.1, timeout is 2 seconds:

```
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 18/22/33

**Let's test for 8.8.8.8 that is not supposed to work till we define the Active path**

```
USER1 (config)#do ping 8.8.8.8
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

#### 4. Configure monitoring of the ISP's availability

In order for the firewall **Cisco ASA** to monitor the availability of the primary channel, we need to configure the “**ip sla monitor**” function. It allows to send a ping request (an **ICMP** echo request) to the ISP 1's gateway address at configured time intervals. Receiving a response (**ICMP** echo reply) will mean that the channel is available.

##### Additional information:

**timeout 3000** – is the timeframe within which Cisco ASA will await for an **ICMP** response. **3000 => 3 seconds**

**frequency 10** – how often to send the requests. Here is every **10 seconds**

```
ciscoasa(config)# sla monitor 100
ciscoasa (config-sla-monitor)# type echo protocol iplcmpEcho 20.20.20.1 interface outside
ciscoasa (config-sla-monitor-echo)# timeout 3000
ciscoasa (config-sla-monitor-echo)# frequency 10
ciscoasa (config)# sla monitor schedule 100 life forever start-time now
ciscoasa (config)# track 1 rtr 100 reachability
```

## 5. Configure the default gateway for the backup ISP

Just like with the primary ISP, the backup ISP needs to have its **default gateway** configured on the **Cisco ASA**, so that the firewall will send all the unknown packets in its direction. The only difference is that this gateway should **only** be used in case the **primary** ISP is unavailable and not clog the routing table in all other cases. To achieve this, we need to change the **administrative distance** of the route – make it bigger, thus **lowering** the priority of this route. By default, all static routes have an administrative distance of **1**. We will configure an administrative distance of **254** for our **backup** channel, bringing it closer to the highest possible value

```
ciscoasa(config-if)# route outside 0.0.0.0 0.0.0.0 20.20.20.1 1 track 1
```

```
ciscoasa(config)# route outside_backup 0.0.0.0 0.0.0.0 11.11.11.1 254
```

## 6. Checking the IP SLA monitoring function state

```
ciscoasa(config)# show sla monitor operational-state
```

Entry number: 100

Modification time: 21:14:48.683 UTC Mon Sep 23 2024

Number of Octets Used by this Entry: 1456

Number of operations attempted: 30

Number of operations skipped: 0

Current seconds left in Life: Forever

Operational state of entry: Active

Last time this entry was reset: Never

Connection loss occurred: FALSE

Timeout occurred: TRUE

Over thresholds occurred: FALSE

Latest RTT (milliseconds): NoConnection/Busy/Timeout

Latest operation start time: 01:49:18.706 UTC Tue Sep 24 2024

Latest operation return code: Timeout

## 7. Test to see if the users can access the internet

```
USER1#ping 8.8.8.8
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

```
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 15/20/29 ms





## Cisco ASA Policy Based Routing (PBR) with Dual ISP

Policy Based Routing (PBR) is a feature that has been supported on Cisco Routers for ages. However, Cisco ASA firewalls didn't support this until version 9.4.1 and later. **Policy-based routing (PBR)** is a technique used to make [routing](#) decisions based on policies set by the network administrator.

When a router receives a packet it normally decides where to forward it based on the destination address in the packet, which is then used to look up an entry in a routing table. However, in some cases, there may be a need to forward the packet based on other criteria

PBR allows routing to be performed based on criteria other than destination IP address. The traditional form of routing (which is used by default on any routing device) is based on the destination IP address of the packet.

With PBR, the network device can make routing decisions based on various other criteria such as source IP address, source port, protocol, destination port etc. and also combination of these.

This means for example that a routing device can receive a packet and look at its source IP address (instead of destination) and route the packet according to its PBR policy.

Many Enterprises utilize two ISP connections for redundancy and for bandwidth efficiency reasons.

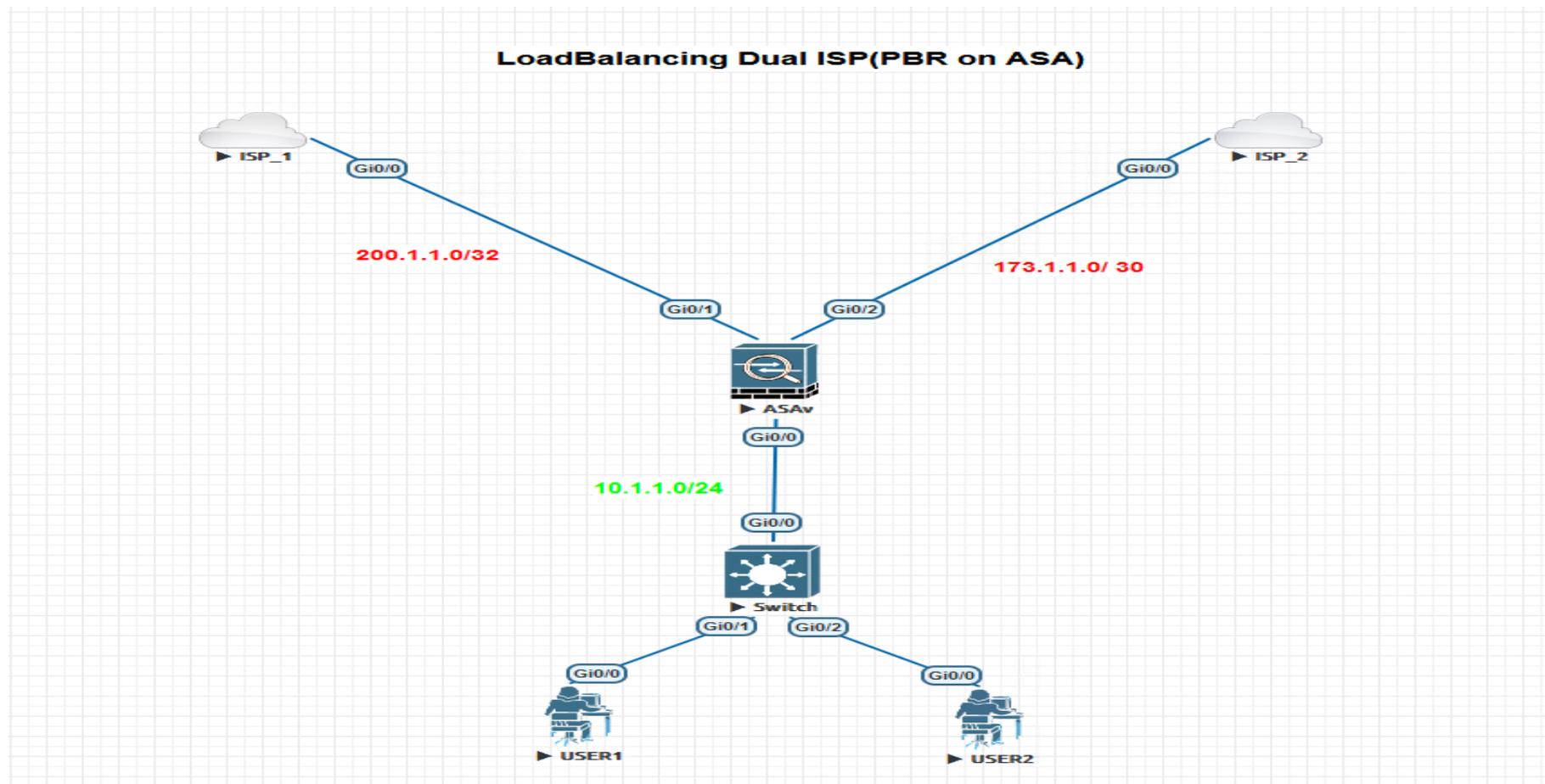
One popular scenario therefore is to route some traffic to ISP1 and some other traffic to ISP2. For example, you can route all Web traffic (HTTP, HTTPS) through ISP1 and all other traffic through ISP2.

Another example could be to route traffic originating from the Engineering department via ISP1 and traffic originating from the Accounting department to go through ISP2.

## Policy Based Routing According to the Destination Protocol

Many Enterprises utilize two ISP connections for redundancy and for bandwidth efficiency reasons.

One popular scenario therefore is to route some traffic to ISP1 and some other traffic to ISP2. For example, you can route all Web traffic (HTTP, HTTPS) through ISP1 and all other traffic through ISP2.



**Project Task: The requirement is to route Web traffic (HTTP port 80 and HTTPS port 443) via ISP01 and all the other Internet traffic via ISP02.**

**Step1. First configure the interfaces**

**ciscoasa(config)# int g0/0**

ciscoasa(config-if)# des link to LAN

ciscoasa(config-if)# nameif inside

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

ciscoasa(config-if)# security-level 100

ciscoasa(config-if)# ip add 10.1.1.1 255.255.255.0

ciscoasa(config-if)# no shut

**ciscoasa(config-if)# int g0/1**

ciscoasa(config-if)# des link to ISP\_1

INFO: Security level for "ISP01" set to 0 by default.

ciscoasa(config-if)# security-level 0

ciscoasa(config-if)# ip add 200.1.1.2 255.255.255.252

ciscoasa(config-if)# no shut

```
ciscoasa(config-if)# int g0/2
```

```
ciscoasa(config-if)# nameif ISP02
```

```
INFO: Security level for "ISP02" set to 0 by default.
```

```
ciscoasa(config-if)# security-level 0
```

```
ciscoasa(config-if)# ip add 173.1.1.2 255.255.255.252
```

```
ciscoasa(config-if)# no shut
```

## **Step2. Configure both ISPs with the following**

```
Router(config)#hostname ISP_1
```

```
ISP_1(config)#
```

```
ISP_1(config)#int g0/0
```

```
ISP_1(config-if)#ip add 200.1.1.1 255.255.255.252
```

```
ISP_1(config-if)#no shut
```

```
ISP_1(config)#ip route 0.0.0.0 0.0.0.0 200.1.1.2
```

```
ISP_1(config)#ip http server
```

```
ISP_1(config)#ip http secure-server
```

```
ISP_1(config)#do ping 200.1.1.2
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 200.1.1.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 3/8/23 ms

**Router(config)#hostname ISP\_2**

ISP\_2(config)#int g0/0

ISP\_2(config-if)#ip add 173.1.1.1 255.255.255.252

ISP\_2(config-if)#no shut

**ISP\_2(config)#ip route 0.0.0.0 0.0.0.0 173.1.1.2**

**ISP\_2(config)#ip dns server**

**ISP\_2(config-if)#line vty 0 4**

ISP\_2(config-line)#pass cisco

ISP\_2(config-line)#transport input telnet

ISP\_2(config-line)#login local

**Router(config)#hostname USER1**

USER1(config)#int g0/0

USER1(config-if)#ip add 10.1.1.2 255.255.255.0

USER1(config-if)#no shut

**USER1(config-if)#ip route 0.0.0.0 0.0.0.0 10.1.1.1**

USER1(config)#do ping 10.1.1.1

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/18 ms

**USER2(config)#int g0/0**

USER2(config-if)#ip add 10.1.1.3 255.255.255.0

USER2(config-if)#no shut

**USER2(config-if)#ip route 0.0.0.0 0.0.0.0 10.1.1.1**

USER2(config)#do ping 10.1.1.1

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!

**Step.3 : Define a default route on the ASA with http and https traffic via ISP01 using a AD 50 and all other traffic to ISP02 with AD of 1**

```
Cocoasa (config-if) # route ISP01 0 0 200.1.1.1 50
```

```
Ciscoasa(config) # route ISP02 0 0 173.1.1.1 1
```

```
ciscoasa(config)# show route
```

Gateway of last resort is 173.1.1.1 to network 0.0.0.0

```
S* 0.0.0.0 0.0.0.0 [1/0] via 173.1.1.1, ISP02
```

```
C 10.1.1.0 255.255.255.0 is directly connected, inside
```

```
L 10.1.1.1 255.255.255.255 is directly connected, inside
```

```
C 173.1.1.0 255.255.255.252 is directly connected, ISP02
```

```
L 173.1.1.2 255.255.255.255 is directly connected, ISP02
```

```
C 200.1.1.0 255.255.255.252 is directly connected, ISP01
```

```
L 200.1.1.2 255.255.255.255 is directly connected, ISP01
```

**Step 4 Configure NAT rules (PAT) using the corresponding outgoing interface of the ASA for traffic going from “inside” to “ISP01” and also for “inside” to “ISP02”.**

```
ciscoasa(config)# nat (inside,ISP01) 1 source dynamic any interface
```

```
ciscoasa(config)# nat (inside,ISP02) 2 source dynamic any interface
```

```
ciscoasa(config)# sho nat de
```

Manual NAT Policies (Section 1)

1 (inside) to (ISP01) source dynamic any interface

translate\_hits = 0, untranslate\_hits = 0

Source - Origin: 0.0.0.0/0, Translated: 200.1.1.2/30

2 (inside) to (ISP02) source dynamic any interface

translate\_hits = 0, untranslate\_hits = 0

Source - Origin: 0.0.0.0/0, Translated: 173.1.1.2/30

**Step 5 Create an Access Control List (ACL) which will match the traffic that we want to be handled by our PBR policy.**

## create an object group for ports 80,443

```
ciscoasa(config)# object-group service WEB-ports tcp
```

```
ciscoasa(config-service-object-group)# port-object eq 443
```

```
ciscoasa(config-service-object-group)# port-object eq 80
```

```
ciscoasa(config)# access-list PBR_ACL extended permit tcp any any object-group WEB-ports
```

The ACL above matches traffic from any inside network having destination ports of 80 and 443

**Step 6 we need to create a route-map which will match the traffic in ACL created above and then apply a routing policy to this traffic flow.**

```
ciscoasa(config)# route-map PBR permit 2
```

```
match ip address PBR_ACL (match the traffic identified in ACL created above)
```

```
ciscoasa(config-route-map)# set ip next-hop 200.1.1.1 (set the next hop of the traffic to be ISP01)
```

```
ciscoasa(config)# show route-map
```

```
route-map PBR, permit, sequence 2
```

```
Match clauses:
```

```
ip address (access-lists): PBR_ACL
```

```
Set clauses:
```

```
ip next-hop 200.1.1.1
```

**Step 7. Apply the PBR policy to the “Ingress” interface that we want to enforce this routing policy**

```
ciscoasa(config-route-map)# int g0/0
```

```
ciscoasa(config-if)# policy-route route-map PBR (apply the PBR policy to this interface)
```

```
ciscoasa(config-if)# show run int g0/0
```

```
interface GigabitEthernet0/0
```

```
nameif inside
```

```
security-level 100
```

```
ip address 10.1.1.1 255.255.255.0
```

```
policy-route route-map PBR
```

**Let generate traffic to test connection**

USER!**#telnet 8.8.8.8 443**  
Trying 8.8.8.8, 443 ... Open

USER!**#telnet 8.8.8.8 80**  
Trying 8.8.8.8, 80 ... Open

### Test Connection using Packet-TRACER

**ciscoasa(config-if)# packet-tracer input inside tcp 10.1.1.2 1 8.8.8.8 443**

#### Result:

input-interface: inside

input-status: up

input-line-status: up

**output-interface: ISP01**

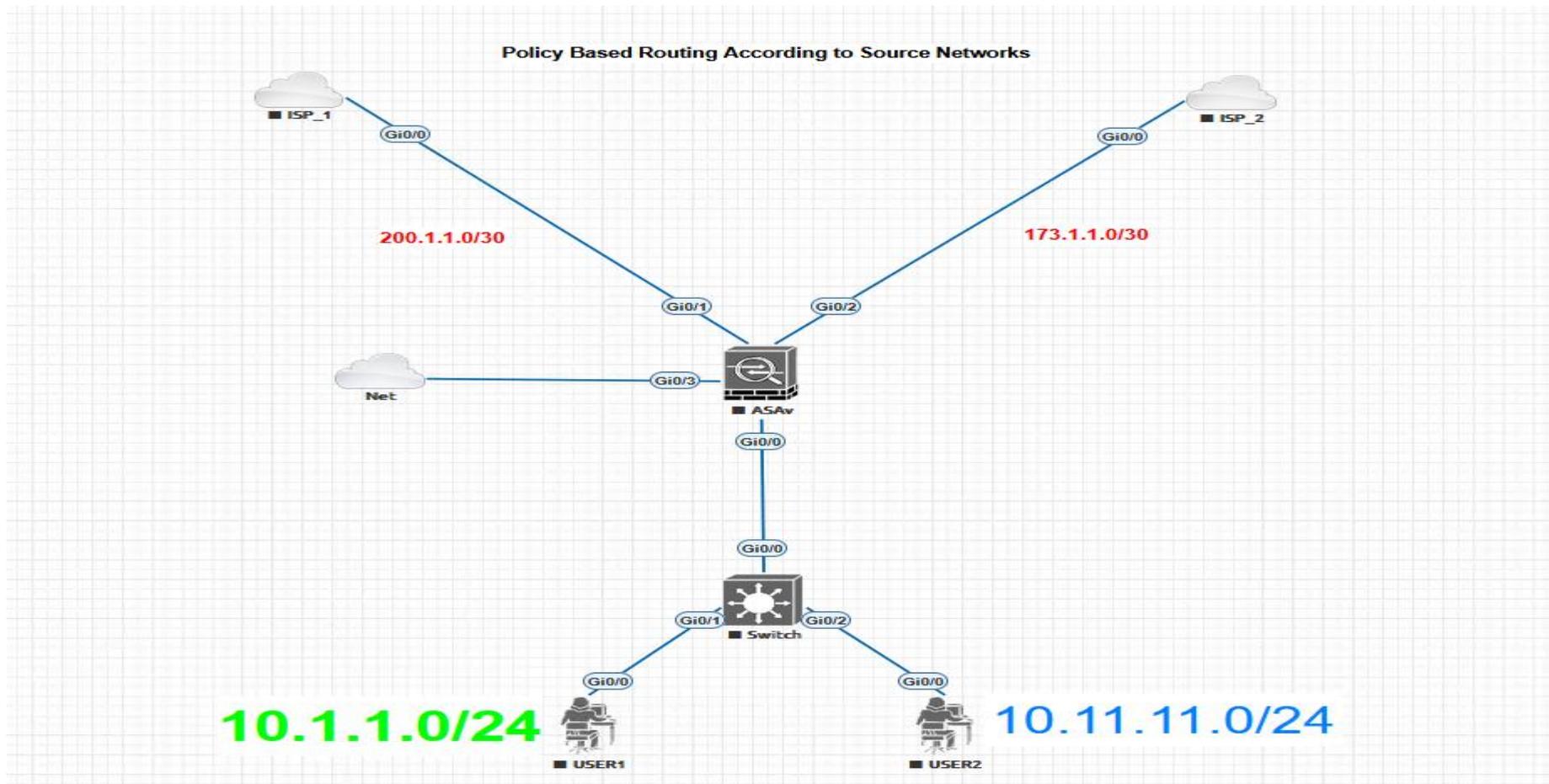
output-status: up

output-line-status: up

Action: allow

## Policy Based Routing According to Source Networks

Another example could be to route traffic originating from the Engineering department via ISP1 and traffic originating from the Accounting department to go through ISP2.



**Project Task: The requirement is to route traffic originating from the Engineering department via ISP1 and traffic originating from the Accounting department to go through ISP2**

**Step1.Create the interface for the LAN1 and LAN2**

**ciscoasa(config)# interface GigabitEthernet0/0**

ciscoasa(config-if)# no nameif

ciscoasa(config-if)# no security-level

ciscoasa(config-if)# no ip address

ciscoasa(config-if)# do show run no shut

**ciscoasa(config-if)# interface GigabitEthernet0/0.100**

ciscoasa(config-subif)# vlan 100

ciscoasa(config-subif)# nameif LAN1

ciscoasa(config-subif)# security-level 100

ciscoasa(config-subif)# ip address 10.1.1.1 255.255.255.0

```
ciscoasa(config-subif)# interface GigabitEthernet0/0.200
```

```
ciscoasa(config-subif)# vlan 200
```

```
ciscoasa(config-subif)# nameif LAN2
```

```
ciscoasa(config-subif)# security-level 100
```

```
ciscoasa(config-subif)# ip address 10.11.11.1 255.255.255.0
```

**Step.2 Create an Access Control List (ACL) which will match the traffic that we want to be handled by our PBR policy.**

```
ciscoasa(config)#access-list PBR_ACL1 extended permit ip 10.1.1.0 255.255.255.0 any
```

```
ciscoasa(config)#access-list PBR_ACL2 extended permit ip 10.11.11.0 255.255.255.0 any
```

**Step-3 we'll configure the route-map which will match the traffic in ACLs created above and then apply a routing policy to the traffic flows.**

```
route-map PBR permit 2 create the route-map and give it a name "PBR"
```

```
match ip address PBR_ACL1<- match the traffic of LAN1 identified in ACL1 created
```

```
set ip next-hop 200.1.1.1<- set the next hop of LAN1 traffic to be ISP1
```

```
route-map PBR permit 3<- create another entry in the same route-map
```

```
match ip address PBR_ACL2<- match the traffic of LAN2 identified in ACL2 created
```

```
set ip next-hop 173.1.1.1<- set the next hop of LAN2 traffic to be ISP2
```

**Step.4 Apply the PBR policy to the “Ingress” interfaces that we want to enforce this routing policy. In our case we will apply the same policy to both internal networks (LAN1, LAN2)**

**interface GigabitEthernet0/0.100**

policy-route route-map PBR

**interface GigabitEthernet0/0.200**

policy-route route-map PBR

**Step-5 Again, we need to take care of NAT since we must translate the private internal IP networks to public IP address in order to access the Internet.**

nat (LAN1,ISP01) source dynamic any interface

nat (LAN2,ISP02) source dynamic any interface

lets verify

**packet-tracer input LAN2 tcp 10.11.11.3 80 8.8.8.8 80**

Phase: 1

Type: PBR-LOOKUP

Subtype: policy-route

Result: ALLOW

Config:

```
route-map PBR permit 3
```

```
match ip address PBR_ACL2
```

```
set ip next-hop 173.1.1.1
```

Additional Information:

Matched route-map PBR, sequence 3, permit

Found next-hop 173.1.1.1 using egress ifc ISP02

Phase: 2

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (LAN2,ISP02) source dynamic any interface
```

Additional Information:

Dynamic translate 10.11.11.3/80 to 173.1.1.2/8

Result:

output-interface: ISP02

output-status: up

output-line-status: up

Action: allow

**ciscoasa(config)# packet-tracer input LAN1 tcp 10.1.1.3 1 8.8.8.8 80**

Phase: 1

Type: PBR-LOOKUP

Subtype: policy-route

Result: ALLOW

Config:

route-map PBR permit 2

match ip address PBR\_ACL1

set ip next-hop 200.1.1.1

Additional Information:

Matched route-map PBR, sequence 2, permit

Found next-hop 200.1.1.1 using egress ifc ISP01

Phase: 2

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (LAN1,ISP01) source dynamic any interface
```

Additional Information:

```
Dynamic translate 10.1.1.3/1 to 200.1.1.2/1
```

Result:

output-interface: ISP01

output-status: up

output-line-status: up

Action: allow

## **Firewall redundancy**

Using just a single ASA is a single point of failure and usually catastrophically reflects in the network when the device experiences common setbacks such as hardware issues, link/cable problems, or just a simple misconfiguration.

Therefore, using a second ASA to the primary one will provide a backup solution in case something goes wrong with the active unit

Overall, the deployment of multiple firewalls offers a variety of benefits, ranging from greater performance to enhanced security. If your security environment warrants this type of scenario, it's definitely an option worth considering.

There are 3 common Firewall redundancy designs generally practice in the industries.

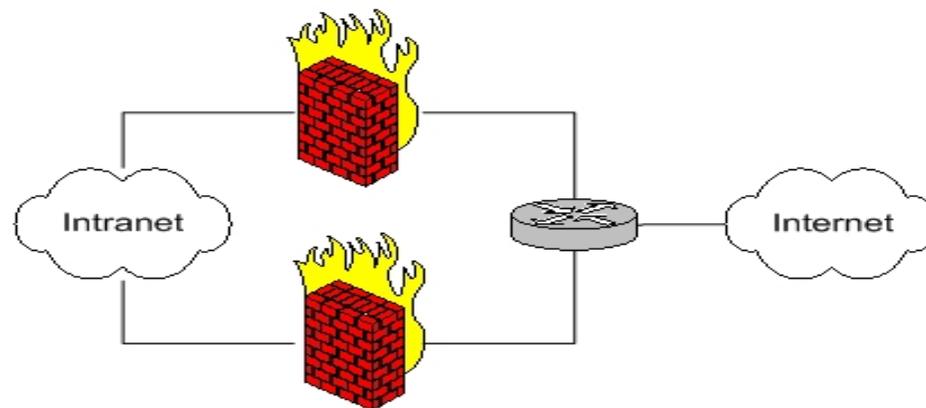
### **Common Deployment scenarios**

1. Fault tolerance and load balancing
2. Enhanced perimeter protection
3. Protected subnets Redundancy firewall Design

## Deployment scenarios and benefits

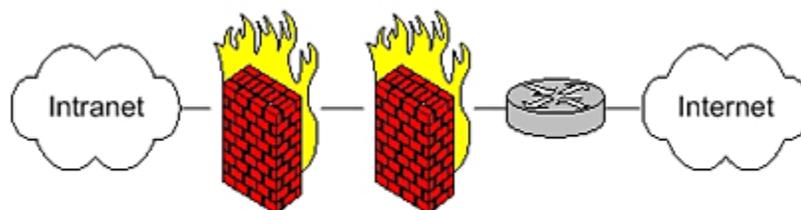
### 1. Fault tolerance and load balancing Redundancy Firewall Design

Many organizations choose to implement dual firewalls in a parallel fashion, as shown in the figure below. When the router is properly configured, this provides the added benefits of fault tolerance and load balancing. Both firewalls should be configured to "fail-safe," that is, in the event of a failure, they should automatically block all traffic. When configured in this fashion, the firewalls provide fault tolerance; when one fails, the other is able to carry the network traffic and keep the failure transparent to users.



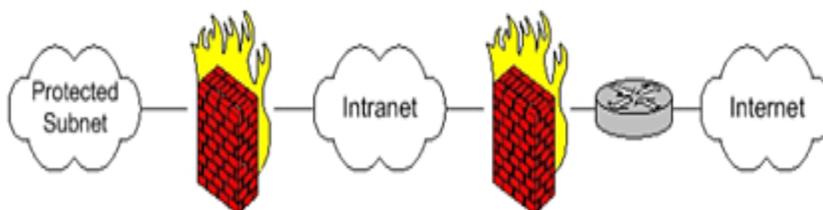
## 2. Enhanced perimeter protection Redundancy Firewall design

It's also possible to deploy the two firewalls in a series circuit, as shown in the illustration below. When configured in this fashion, all traffic passing into or out of the network must pass through both firewalls. This setup is sometimes deployed in high-security environments to protect against firewall-specific vulnerabilities. In this case, the two firewalls are from different vendors and may even run on different operating systems.



## 3. Protected subnets Redundancy firewall Design

The final scenario we'll discuss is shown in the figure below. In this case, secondary firewall(s) are used to protect subnets of the internal network that have greater security requirements than the network as a whole. This type of scenario may be used, for example, to provide an accounting department added protection for sensitive financial data they wish to protect from other internal users.



## ASA Failover

ASA failover refers to the capability of Cisco Adaptive Security Appliances (ASAs) to automatically switch to a backup unit in the event of a primary unit failure. It creates a seamless transition, maintaining network connectivity without any noticeable interruption. ASA failover operates in Active/Standby and Active/Active modes.

### Cisco ASA Failover Modes

ASA supports two failover modes, Active/Active failover and Active/Standby failover.

In **Active/Standby** failover, one device functions as the **Active Unit** and passes the traffic. The second **Standby Unit** does not actively pass traffic. When a failover occurs, the Standby unit assumes the active role and starts passing the traffic.

In an **Active/Active** failover **both** ASAs can pass traffic. Please note that Active/Active failover is **only** available to ASAs in **multiple context models**. In Active/Active failover, you divide the security contexts on the ASA into 2 failover groups. A failover group is simply a logical group of one or more security contexts. One group is assigned to be Active on the primary ASA, and the other group is assigned to be active on the Secondary ASA. When a failover occurs, it occurs at the failover group level

### Failover Types

**Within these two different failover modes, there are also two different failover types: stateless and stateful.**

When using **stateless failover**, if a failover should need to occur, all active connections will be dropped and will have to be reestablished to continue communications.

When using **stateful failover**, connection state information is exchanged between the failover partners (or groups). If a failover should need to occur, the active connections (that are supported) can be seamlessly transferred and will not need to be reestablished.

## Failover Triggers

Failover can be triggered at the unit level if one of the following events occurs:

- The unit has a hardware failure.
- The unit has a power failure.
- The unit has a software failure.

## ASA Failover Requirement

If you want to use failover, you must meet the following requirements:

### Hardware:

- ASA failover platform must be the same model. For example, 2x ASA 5510 or 2x ASA 5522.
- ASA failover platform must have the same number and types of interfaces.
- ASA failover platform must have the same modules installed (if any are to be installed).
- ASA failover platform must have the same amount of RAM installed (it is also preferred if the Flash sizes are the same as well).

### Software:

- Both ASA failover platform must be using the same firewall mode (routed or transparent).
- Both ASA failover platform must be using the same context mode (single or multiple).
- Both ASA failover platform must be using the same major and minor software version (there are exceptions during upgrade).
- Both ASA failover platform must use the same AnyConnect images.

The failover mechanism is stateful which means that the active ASA sends all stateful connection information state to the standby ASA. This includes TCP/UDP states, NAT translation tables, ARP table, VPN information and more.

## Benefits of Cisco ASA Failover

ASA Failover offers numerous benefits for businesses.

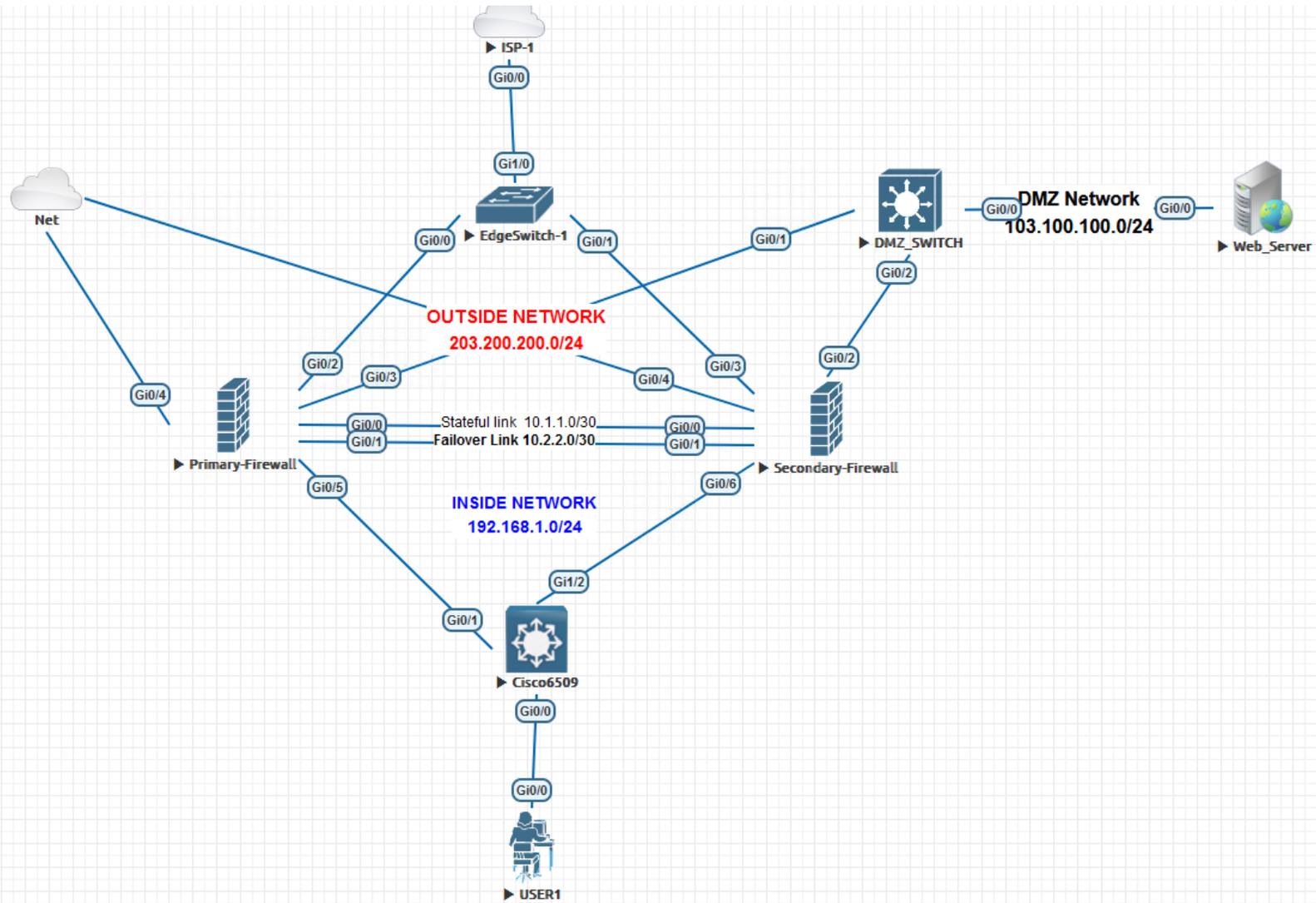
**Enhanced Network Uptime:** Organizations can achieve uninterrupted network connectivity with Cisco ASA failover. In the event of a primary unit failure, the secondary unit seamlessly takes over, ensuring minimal disruption to network operations.

**ASA Failover enhances security** by providing seamless failover for security policies, preventing potential vulnerabilities during critical moments

**Load Balancing:** Cisco ASA failover enables load balancing, distributing incoming network traffic across multiple units. This optimizes resource utilization and prevents any single unit from becoming overloaded.

**Improved Scalability:** Failover setup allows for easy scalability, as additional units can be added to the configuration. This helps accommodate growing network demands without compromising on security or performance.

# Active/Standby ASA Firewall Project



## ASA Failover Configuration Guide

### Active Unit Configuration:

Note: Always start with the active ASA first.

#### Step-1 Assign IP address to outside interface. During Failover the primary IP address will be assigned to Standby Unit

```
PrimaryFW(config-if)# int g0/2
```

```
PrimaryFW(config-if)# des to ISP
```

```
PrimaryFW(config-if)# nameif outside
```

```
PrimaryFW(config-if)# security-level 0
```

```
PrimaryFW(config-if)# ip add 203.200.200.1 255.255.255.0 standby 203.200.200.2
```

#### Step-2 Assign IP address to inside interface. During Failover the primary IP address will be assigned to Standby Unit

```
PrimaryFW(config-if)# int g0/5
```

```
PrimaryFW(config-if)# des to CoreSwitch
```

```
PrimaryFW(config-if)# nameif inside
```

```
PrimaryFW(config-if)# security-level 100
```

```
PrimaryFW(config-if)# ip add 192.168.1.1 255.255.255.0 standby 192.168.1.2
```

### Step-3 Assign IP address to DMZ interface. During Failover the primary IP address will be assigned to Standby Unit

```
PrimaryFW(config-if)# int g0/3
```

```
des link to DMZ
```

```
nameif DMZ
```

```
ip add 103.100.100.1 255.255.255.0 standby 103.100.100.2
```

```
no shut
```

### Step-4 Configure routing protocol to allow users to communicate to the ISP

```
route outside 0.0.0.0 0.0.0.0 203.200.200.3
```

```
router eigrp 10
```

```
network 192.168.1.0 255.255.255.0
```

```
network 103.100.100.0 255.255.255.0
```

```
redistribute static
```

```
USER#ping 8.8.8.8
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

```
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 15/17/19 ms

```
USER#ping 103.100.100.3
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 103.100.100.3, timeout is 2 seconds:

```
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 13/15/21 ms

### Step-5 Set ASA1 as primary unit

```
PrimaryFW(config-if)# failover lan unit primary
```

### Step-6 Define Failover Interface.

**NB:** used to determine the operating status of each unit, as well as to replicate and synchronize any configuration between both units in the pair.

In order to accomplish this, a dedicated Ethernet interface must be used on each Cisco ASA, which will be used exclusively for passing failover information. The connection between these interfaces on the ASAs can either be a direct link or through a switch.

```
PrimaryFW(config-if)# failover lan interface FAILOVER-LINK G0/1
```

INFO: Non-failover interface config is cleared on GigabitEthernet0/1 and its sub-interfaces

## Step-7 Assign IP address to Failover Interfaces

```
PrimaryFW(config-if)# failover interface ip FAILOVER-LINK 10.2.2.1 255.255.255.252 standby 10.2.2.2
```

## Step-8 Define stateful Failover interface

NB: Without this data, anytime a failover happens, all end-user applications must re-establish connections and there will be an interruption from the client's point of view. The stateful failover interface can either be a dedicated interface or shared with any other interface including the LAN failover interface .

Some of the information exchanged over the stateful failover link is:

- Network Address Translation (NAT) table
- Address Resolution Protocol (ARP) table
- TCP connection table
- UDP connection table
- HTTP connection table
- MAC address table

```
PrimaryFW(config-if)# failover link Stateful-link G0/0
```

INFO: Non-failover interface config is cleared on GigabitEthernet0/0 and its subs-interfaces

## Step-9 Assign IP addresses to Stateful Failover interfaces

```
PrimaryFW(config-if)# failover interface ip stateful-link 10.1.1.1 255.255.255.252 standby 10.1.1.2
```

## Step-10 Enable Failover

```
PrimaryFW(config-if)# failover
```

Note: Issue the failover command on the primary device first, and then issue it on the secondary device. After you issue the failover command on the secondary device, the secondary device immediately pulls the configuration from the primary device and sets itself as standby.

The primary ASA stays up and passes traffic normally and marks itself as the active device. From that point on, whenever a failure occurs on the active device, the standby device comes up as active.

## Step-11 Enable the interfaces for Failover and State Link

```
PrimaryFW(config-if)# int g0/0
```

```
PrimaryFW(config-if)# no shut
```

```
PrimaryFW(config-if)# int g0/1
```

Lets verify what is configured

```
PrimaryFW(config-if)# show run failover
```

```
failover
```

```
failover lan unit primary
```

```
failover lan interface FAILOVER-LINK GigabitEthernet0/1
```

```
failover link Stateful-link GigabitEthernet0/0
```

```
failover interface ip FAILOVER-LINK 10.2.2.1 255.255.255.252 standby 10.2.2.2
```

```
failover interface ip Stateful-link 10.1.1.1 255.255.255.252 standby 10.1.1.2
```

**The ASA requires something that triggers the failover mechanism. An interface that fails is a good trigger. When the inside or outside interface fails, we should failover. By default all physical interfaces are monitored but let me show you the command anyway:**

```
PrimaryFW(config)# monitor-interface inside
```

```
PrimaryFW(config)# monitor-interface outside
```

```
PrimaryFW(config)# monitor-interface DMZ
```

## **Configuration on Secondary ASA**

### **Step-1 Set ASA1 as primary unit**

```
SecondaryFW(config-if)# failover lan unit Secondary
```

### **Step-2 Define Failover Interface.**

```
SecondaryFW(config-if)# failover lan interface FAILOVER-LINK G0/1
```

INFO: Non-failover interface config is cleared on GigabitEthernet0/1 and its

### **Step-3 Assign IP address to Failover Interfaces**

```
SecondaryFW(config-if)# failover interface ip FAILOVER 10.2.2.1 255.255.255.252 standby 10.2.2.2
```

#### Step-4 Enable the interfaces for Failover and State Link

```
SecondaryFW(config-if)# int g0/0
```

```
SecondaryFW(config-if)# no shut
```

```
SecondaryFW(config-if)# int g0/1
```

```
SecondaryFW(config-if)# no shut
```

#### Step-5 Enable Failover

```
SecondaryFW(config-if)# failover
```

#### Step-6 Change the prompt to show primary or secondary

Once the configuration is replicated on both ASAs, they both use the same hostname. This means that every time you access the ASAs over a console, Secure Shell (SSH), or Telnet connection, it will not be easy to differentiate between the units being managed.

Therefore, it is recommended to change the CLI prompt to include additional information next to the hostname, such as the priority and state of the managed device

```
PrimaryFW(config-if)# prompt hostname priority state
```

```
PrimaryFW/pri/act(config)#
```

```
PrimaryFW/pri/act(config)#
```

Now let's check on Secondary FW

```
PrimaryFW/sec/stby>
```

```
PrimaryFW/sec/stby>
```

**This is what you will see on Primary ASA1**

```
PrimaryFW(config)#
```

```
Switchover enabled
```

```
Configuration has changed, replicate to mate.
```

```
Beginning configuration replication: Sending to mate.
```

```
End Configuration Replication to mate
```

```
Switching to Standby
```

```
Primary: Switching to Ok for reason Interface check.
```

```
Switching to Active
```

## This is what you will see on Secondary ASA2

Switchover enabled

Configuration has changed, replicate to mate.

State check detected an Active mate

Beginning configuration replication from mate.

End configuration replication from mate.

**PrimaryFW(config)# show failover**

PrimaryFW/pri/act(config)# show failover

Failover On

Failover unit Primary

Failover LAN Interface: FAILOVER-LINK GigabitEthernet0/1 (up)

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 4 of 61 maximum

MAC Address Move Notification Interval not set

Version: Ours 9.6(1), Mate 9.6(1)

Serial Number: Ours 9AQFS5U27GJ, Mate 9AKXX77E3FA

Last Failover at: 22:40:12 UTC Oct 7 2024

**This host: Primary - Active**

Active time: 5576 (sec)

slot 0: empty

Interface outside (203.200.200.1): Normal (Monitored)

Interface dmz (103.100.100.1): Normal (Monitored)

Interface Management (10.255.1.201): Normal (Monitored)

Interface inside (192.168.1.1): Normal (Monitored)

**Other host: Secondary - Standby Ready**

Active time: 0 (sec)

Interface outside (203.200.200.2): Normal (Monitored)

Interface dmz (103.100.100.2): Normal (Monitored)

Interface Management (10.255.1.202): Normal (Monitored)

## PrimaryFW/pri/act(config)# show monitor-interface

### This host: Primary - Active

Interface outside (203.200.200.1): Normal (Monitored)

Interface dmz (103.100.100.1): Normal (Monitored)

Interface Management (10.255.1.201): Normal (Monitored)

Interface inside (192.168.1.1): Normal (Monitored)

### Other host: Secondary - Standby Ready

Interface outside (203.200.200.2): Normal (Monitored)

Interface dmz (103.100.100.2): Normal (Monitored)

Interface Management (10.255.1.202): Normal (Monitored)

Interface inside (192.168.1.2): Normal (Monitored)

## Verification

Ping the internet and power off the Primary FW

```
Router#ping 8.8.8.8 re 1000
```

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
```

```
*Oct 8 00:21:39.809: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.1.1 (GigabitEthernet0/0) is down: peer restarted...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
*Oct 8 00:21:44.588: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.1.1 (GigabitEthernet0/0) is up: new adjacency!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

## Failover exec

To execute a command on a specific unit in a failover pair, use the **failover exec** command in privileged EXEC or global configuration mode.

### PrimaryFW/pri/act(config)# failover exec standby show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: FAILOVER_LINK GigabitEthernet0/1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 61 maximum
MAC Address Move Notification Interval not set
Failover replication http
Version: Ours 9.6(1), Mate 9.6(1)
Serial Number: Ours 9AKXX77E3FA, Mate 9AQFS5U27GJ
Last Failover at: 01:21:45 UTC Oct 10 2024
This host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: empty
    Interface outside (203.200.200.2): Normal (Monitored)
    Interface DMZ (103.100.100.2): Normal (Monitored)
    Interface Management (10.255.1.202): Normal (Monitored)
    Interface inside (192.168.1.2): Normal (Monitored)
Other host: Primary - Active
    Active time: 225420 (sec)
    Interface outside (203.200.200.1): Normal (Monitored)
```

PrimaryFW/pri/act(config)#**failover exec mate show running-config failover**

failover

failover lan unit secondary

failover lan interface FAILOVER\_LINK GigabitEthernet0/1

failover replication http

failover link Stateful-link GigabitEthernet0/0

failover interface ip FAILOVER\_LINK 10.2.2.1 255.255.255.252 standby 10.2.2.2

failover interface ip Stateful-link 10.1.1.1 255.255.255.252 standby 10.1.1.2

PrimaryFW/pri/act(config)#**failover exec standby show interface**

PrimaryFW/pri/act(config)#**failover reload-standby**

# Using ASDM to Configure ASA Failover

## Set up standby ip address

The screenshot shows the ASDM configuration interface for ASA Failover. The breadcrumb path is Configuration > Device Management > High Availability and Scalability > Failover. The 'Setup' tab is selected, showing a table of interface configurations. A red arrow points to the 'Standby IP Address' field for the 'outside' interface, which is currently set to 203.200.200.2. Below the table is a checkbox for 'Enable monitor interface service module' which is unchecked.

Interface Name	Name	Active IP Address	Subnet Mask/Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/2	outside	203.200.200.1	255.255.255.0	203.200.200.2	<input checked="" type="checkbox"/>
GigabitEthernet0/3	DMZ	103.100.100.1	255.255.255.0	103.100.100.2	<input checked="" type="checkbox"/>
GigabitEthernet0/4	management	10.255.1.201	255.255.255.0	10.255.1.202	<input checked="" type="checkbox"/>
GigabitEthernet0/5	inside	192.168.1.1	255.255.255.0	192.168.1.2	<input checked="" type="checkbox"/>

Enable monitor interface service module

## Step.2 Configure failover for Primary ASA

The screenshot displays the ASA configuration interface for failover. The left sidebar shows the navigation tree with 'Device Management' selected. The main content area is titled 'Configuration > Device Management > High Availability and Scalability > Failover'. The 'Setup' tab is active, showing the following configuration:

- Enable failover
- Shared Key: [Redacted]  Use 32 hexadecimal character key
- IPsec Preshared Key: [Redacted]
- Note: The shared key and the IPsec preshared key can not be configured concurrently.
- Disable configuration changes on the standby unit

**LAN Failover**

Interface:	GigabitEthernet0/1	Logical Name:	FAILOVER-LINK
Active IP:	10.2.2.1	Standby IP:	10.2.2.2
Subnet Mask:	255.255.255.252	Preferred Role:	<input checked="" type="radio"/> Primary <input type="radio"/> Secondary

**State Failover**

Interface:	GigabitEthernet0/0	Logical Name:	Stateful-link
Active IP:	10.1.1.1	Standby IP:	10.1.1.2
Subnet Mask:	255.255.255.252	<input type="checkbox"/> Enable HTTP replication	

**Replication**

Replication Rate (connections per second): [Empty field]

Minimum value is 833  
Maximum value is 20000  
Default value is 20000

Use Default

Buttons: Apply, Reset

### Step3. Verify your config

Monitoring > Properties > Failover > Status

Failover state of the system:

```
failover on
Failover unit Secondary
Failover LAN Interface: FAILOVER-LINK GigabitEthernet0/1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 61 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.6(1), Mate 9.6(1)
Serial Number: Ours 9AKXX77E3FA, Mate 9AQFS5U27GJ
Last Failover at: 00:27:50 UTC Oct 8 2024
    This host: Secondary - Active
                Active time: 481 (sec)
                slot 0: empty
```

Make Active    Make Standby    Reset Failover    Reload Standby

Refresh

## **ASA Redundant Interface**

A logical redundant interface consists of a pair of physical interfaces: an active and a standby interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the [ASA](#) reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as device-level failover if desired.

The logical redundant interface is only available on ASA platforms and not on devices running FirePower.

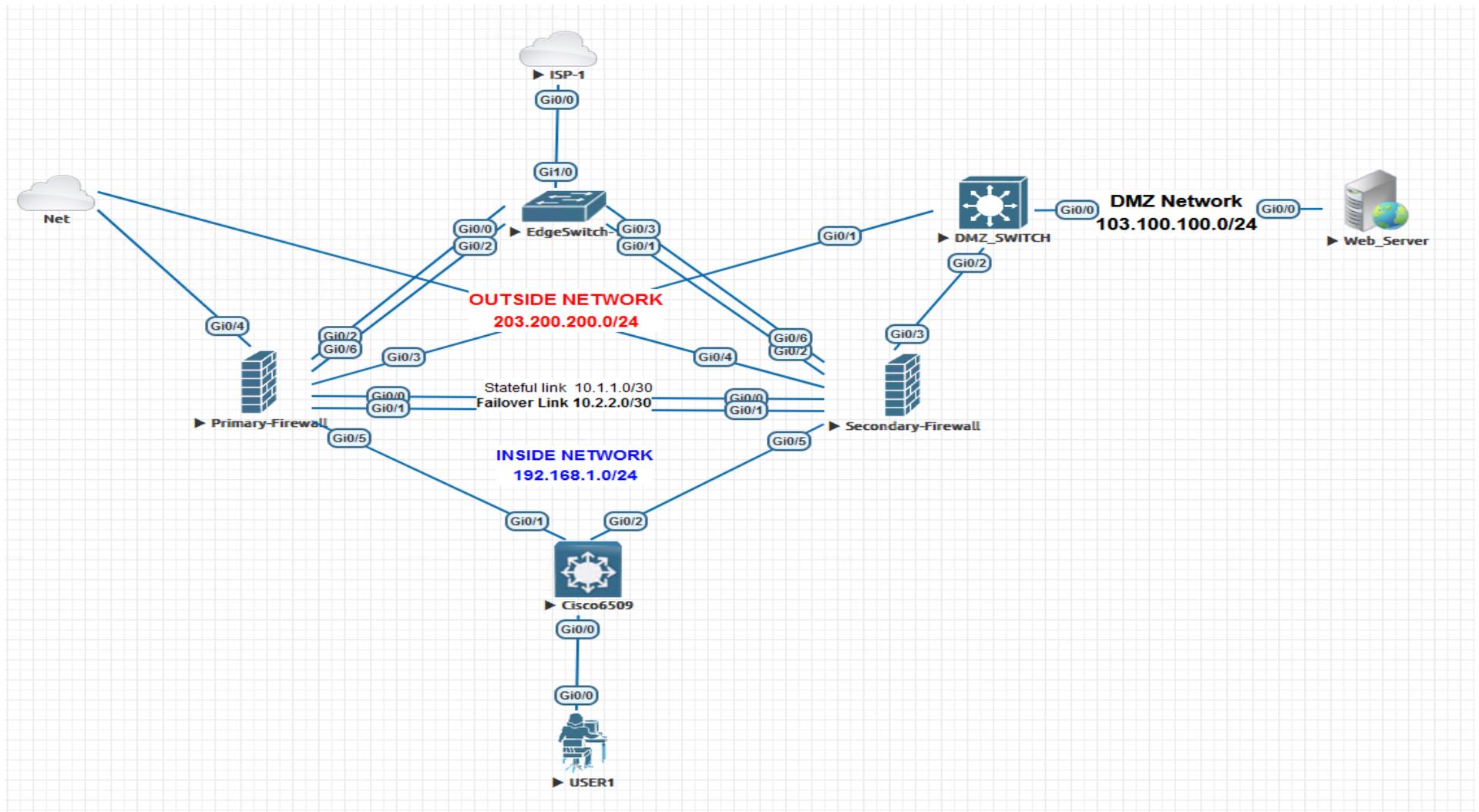
We can configure upto 8 redundant interfaces.

Redundant interface are number from 1 to 8 and have the name redundant X. When adding physical interfaces to the redundant pair, please make sure there is no configuration on it and interface is also in no shutdown state. This is just a precaution, the firewall will remove these settings when adding the physical interface to a new group.

The logical redundant interface will take the MAC address of the first interface added to the group. This MAC address is not changed with the member interface failures, but changes when you swap the order of the physical interfaces to the pair.

Once we have configured a redundant interface, we can assign it a name and a security level, followed by an IP address. The procedure is the same as with any interface in the system.

# ASA Redundant Interface Project



## Using Command Line

```
interface GigabitEthernet0/2
```

```
no nameif
```

```
no security-level
```

```
no ip address
```

```
interface GigabitEthernet0/6
```

```
no nameif
```

```
no security-level
```

```
no ip address
```

```
interface Redundant1
```

```
member-interface GigabitEthernet0/2
```

```
member-interface GigabitEthernet0/6
```

```
nameif outside
```

```
security-level 0
```

```
ip address 203.200.200.1 255.255.255.0 standby 203.200.200.2
```

## Using ASDM to configure redundant interface

Configure> device setup> interfaces>add

NB: Please make sure there is no configuration on it and interface is also in no shutdown state

**Edit Redundant Interface**

General Advanced IPv6

Redundant ID: 1

Primary Interface: GigabitEthernet0/2

Secondary Interface: GigabitEthernet0/6

Interface Name: outside

Zone: -- None -- Manage ... Threat Detection is enabled.

Route Map: -- None -- Manage ...

Security Level: 0

Dedicate this interface to management only

VTEP source interface

Enable Interface

IP Address

Use Static IP  Obtain Address via DHCP  Use PPPoE

IP Address: 203.200.200.1

Subnet Mask: 255.255.255.0

Description: ISP

OK Cancel Help

## Verify

**PrimaryFW/pri/act(config)# show run int r1**

```
interface Redundant1
  description ISP
  member-interface GigabitEthernet0/2
  member-interface GigabitEthernet0/6
  nameif outside
  security-level 0
  ip address 203.200.200.1 255.255.255.0 standby 203.200.200.2
```

**PrimaryFW/pri/act(config)# show interface redundant1**

Interface Redundant1 "outside", is up, line protocol is up

Hardware is i82540EM rev03, BW 1000 Mbps, DLY 10 usec

Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)

Input flow control is unsupported, output flow control is off

Description: ISP

Redundancy Information:

Member GigabitEthernet0/2(Active), GigabitEthernet0/6

Last switchover at 20:37:17 UTC Oct 14 2024

**You can also force failover on the interface**

**PrimaryFW/pri/act(config)# redundant-interface redundant 1 active-member GigabitEthernet0/6**

PrimaryFW/pri/act(config)# show int r1

Redundancy Information:

Member GigabitEthernet0/6(Active), GigabitEthernet0/2

Last switchover at 22:59:28 UTC Oct 14 2024

## **Cisco ASA BotNet Filtering**

Cisco ASA Adaptive Security Appliance is a Cisco proprietary firewall appliance device. ASA offers features like inspection, policing & prioritizing traffic, filters packet based on ACL's and Anti-X protection. The Anti-X features, enables us to configure botnet attack filter in Cisco ASA.

### **Botnet Filtering**

The Cisco ASA Botnet Traffic Filter is an effective tool that enterprises can use to gain insights in one of today's leading threats. In conjunction with accurate threat data provided by Cisco Security Intelligence Operations and Cisco Global Correlation for IPS, the Botnet Traffic Filter offers an industry-leading solution to combat modern botnet threats in a dynamic business environment. These lists are stored in a database as per their reputations. Cisco ASA accesses the database, performing reputation based filtering to identify the hacker

#### **Traffic classifications:**

Traffic that passes through the Botnet Traffic Filter is classified into four categories:

##### **Blacklist:**

This is traffic to or from an IP address that is considered to be malicious. This IP address can be either an IP address/network entry in the dynamic blacklist or administrator-configured blacklist or it can be a snooped IP address that was found in a DNS reply for a blacklisted domain.

##### **Whitelist:**

This is traffic to or from an IP address that is considered to be good. It is part of the administrator-configured lists.

## **Greylist:**

These addresses are associated with multiple domain names, but not all of these domain names are on the blacklist.

## **Unknown/None:**

An IP address that does not map to a domain in either a blacklist or whitelist, and no syslog's will be generated for this traffic.

**NB: Unlisted addresses do not generate any syslog messages, but addresses on the blacklist, whitelist, and greylist generate syslog messages**

Enabling Adaptive Security Appliance to use Botnet Filtering requires a certain set of processes. Please remember, this feature works only with a license. The Cisco ASA appliance with the Botnet Traffic Filter should be deployed at the edge of the enterprise, as the botnet database contains information only about external botnets. It is also best to address the external threat as close to the source as possible. This feature is restricted to IPv4 traffic. The Botnet Traffic Filter is supported in all firewall modes (single and multiple) and in routed and transparent modes.

## **Requirement for Botnet Filtering**

Cisco ASA Firewall must have valid Botnet Filtering license and have access to Cisco's Security Intelligence Operation (CSIO) dynamic database, which is in the internet. This is essential as Botnet Filtering features would communicate with CSIO dynamic database and verify with its White & Black listed database

### **DNS is required on ASA primarily for two reasons**

To make sure the ASA is capable of resolving the Cisco Security Intelligence Operations server IP

Allow to have a static whitelist site, even if the site is blacklisted

## Configuration Steps

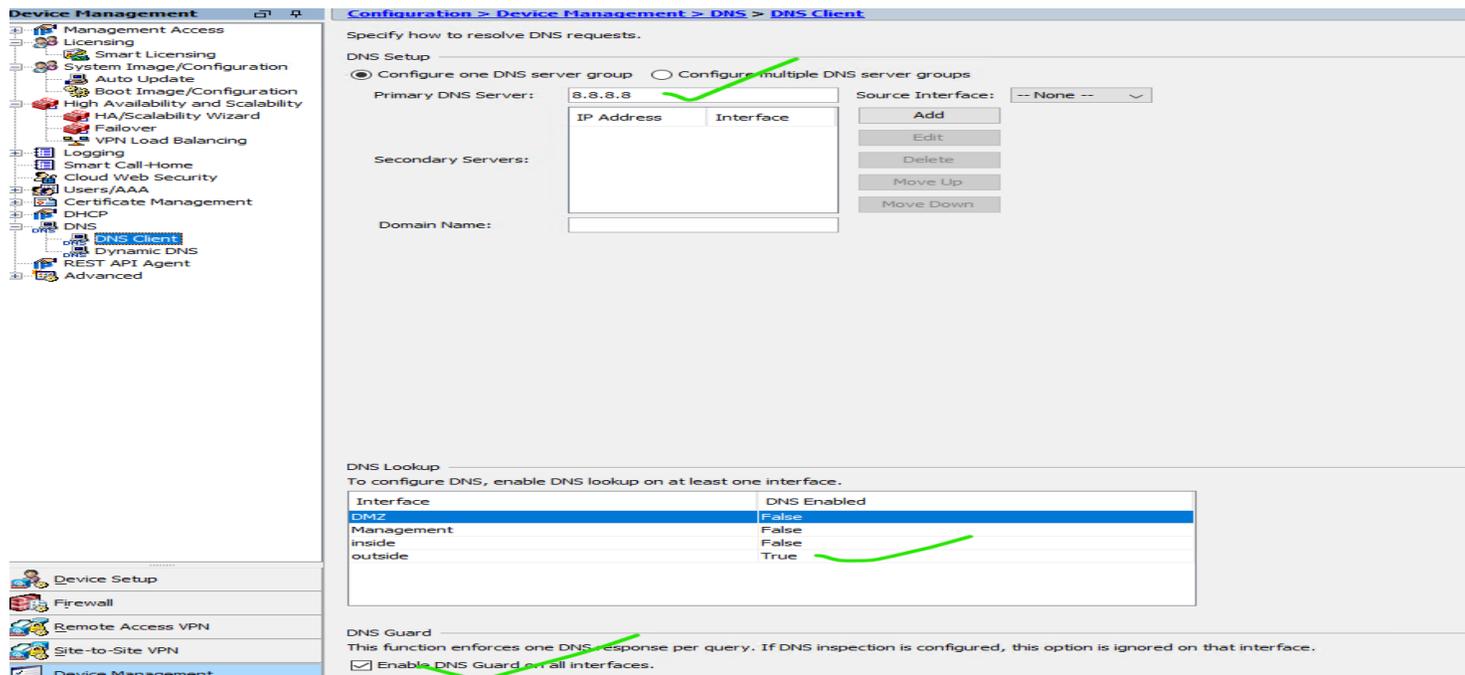
1. Enable DNS on the ASA
2. Configure dynamic database
3. Configure the static database
4. Enable DNS snooping
5. Enable the Botnet traffic filter

### Step.1 Configure the dynamic database

Via ASDM the database can be configured through:

#### Step-1 Enable DNS on the ASA

Configuration ► Device Management ► DNS ► DNS client



The screenshot shows the ASDM configuration page for the DNS Client. The left sidebar displays the navigation tree with 'DNS Client' selected. The main content area is titled 'Configuration > Device Management > DNS > DNS Client' and contains the following sections:

- Specify how to resolve DNS requests.**
- DNS Setup:** Two radio buttons are present: 'Configure one DNS server group' (selected) and 'Configure multiple DNS server groups'.
- Primary DNS Server:** A table with two columns: 'IP Address' and 'Interface'. The 'IP Address' field contains '8.8.8.8'. A green checkmark is visible above the table.
- Source Interface:** A dropdown menu currently set to '-- None --'. Below it are 'Add', 'Edit', 'Delete', 'Move Up', and 'Move Down' buttons.
- Secondary Servers:** An empty table with the same 'IP Address' and 'Interface' columns.
- Domain Name:** An empty text input field.
- DNS Lookup:** A section with the instruction 'To configure DNS, enable DNS lookup on at least one interface.' Below this is a table:

Interface	DNS Enabled
DMZ	False
Management	False
inside	False
outside	True

A green checkmark is visible to the right of the 'outside' row.
- DNS Guard:** A section with the instruction 'This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.' Below this is a checked checkbox labeled 'Enable DNS Guard on all interfaces.' A green checkmark is visible below the checkbox.

## Step-2 Turn on Enable DNS Snooping

Configuration ► Firewall ► Botnet Traffic Filter ► DNS Snooping

Under Botnet Traffic Filter select DNS Snooping.

For global DNS Snooping, simply check the DNS Snooping Enabled option under the global interface

This procedure enables inspection of DNS packets and enables Botnet Traffic Filter snooping, which compares the domain name with those on the dynamic database or static database, and adds the name and IP address to the Botnet Traffic Filter DNS reverse lookup cache. This cache is then used by the Botnet Traffic Filter when connections are made to the suspicious address.

DNS snooping should only be enabled for DNS traffic. Failure to do so will result in non-DNS traffic being dropped because it is not

Adhering to the DNS protocol. DNS snooping should only be enabled for the interface that is facing the Internet, since the Botnet Traffic Filter database is aimed at addressing the external threat of botnets.

Interface	Source	Destination	Service	DNS Snooping Enabled	DNS Map Name	Description
global	any	any	default-inspection	<input checked="" type="checkbox"/>	default_dns_map	

### Step-3 Enable the client and use the dynamic database

Configuration ▶ Firewall ▶ Botnet Traffic Filter ▶ Botnet Database

Enabling ASA for being a client, this will download all dynamic databases from SIO and then make decision based on the downloaded dynamic database. Failing this setting, ASA will not have an updated database to verify with.

[Configuration > Firewall > Botnet Traffic Filter > Botnet Database](#)

Dynamic Database Update

Enabling the Botnet updater client will fetch the latest database from Cisco update server. After the initial fetch, the ASA will poll for changes automatically.

Enable Botnet Updater Client

Dynamic Database Configuration

Use Botnet data dynamically downloaded from updater server

Dynamic Database Management

The database can be fetched at any time. This will not affect the local database maintained in the administrator's lists.

The database can be purged at anytime. This will not affect the local database maintained in the administrator's lists.

Search Dynamic Database

The search will return a single exact match or up to two partial matches, if any.

#### Step-4 Configure the static database (Optional)

Configuration ▶ Firewall ▶ Botnet Traffic Filter ▶ blacklist and Whitelist

This procedure lets you augment the dynamic database with domain names or IP addresses that you want to blacklist or whitelist.

[Configuration](#) > [Firewall](#) > [Botnet Traffic Filter](#) > [Black and White Lists](#)

Add or remove hostname or IP address in the administrator's list.

The names and IP addresses in the white list will be allowed and not checked against the Botnet dynamic database or the administrator's black list.

The names and IP addresses in the black list will be used in conjunction with the Botnet dynamic database and will be monitored by Botnet traffic filter.

White List	Black List
nptc.com	

Buttons: Add, Edit, Delete (for both lists)

## Step-5 Turn on the actions for Botnet Traffic Filter and traffic Classification

Configuration ▶ Firewall ▶ Botnet Traffic Filter ▶ Traffic settings

This procedure enables the Botnet Traffic Filter, which compares the source and destination IP address in each initial connection packet to the IP addresses in the dynamic database, static database, DNS reverse lookup cache, and DNS host cache, and sends a syslog message or drops any matching traffic.

### Traffic Classification

Given to us dynamically from the database by default is (Medium , High, Very high)

Static black list by default are rated very high

The screenshot displays the configuration interface for the Botnet Traffic Filter. The main window is titled "Configuration > Firewall > Botnet Traffic Filter > Traffic Settings".

**Traffic Classification**  
Define Botnet traffic classification for individual interfaces and/or globally.

Interface	Traffic Classified	ACL Used
Global (All Interfaces)	<input type="checkbox"/>	--DISABLED--
DMZ	<input type="checkbox"/>	--DISABLED--
outside	<input checked="" type="checkbox"/>	--ALL TRAFFIC--
Management	<input type="checkbox"/>	--DISABLED--
inside	<input type="checkbox"/>	--DISABLED--

**Ambiguous Traffic Handling**  
 Treat ambiguous (greylisted) traffic as malicious (blacklisted) traffic.

**Blacklisted Traffic Actions**  
Define blacklisted traffic actions.

Buttons: Add, Edit, Delete

Interface	Action
outside	Drop

**Edit Blacklisted Traffic Action**

Interface: Drop malicious (blacklisted) traffic on interfaces where Botnet Traffic Filter traffic classification is enabled.

Interface: outside

Action: Drop

**Threat Level**  
Specify threat level for traffic to be dropped. Default is moderate and above.

Default

Value: Very High

Range: Very Low - Very High

**ACL Used**  
Select an ACL to define traffic to be dropped. The ACL used here must be a subset of the ACL used in traffic classification.

ACL Used: --ALL TRAFFIC--

Buttons: OK, Cancel, Help

It is also possible to only filter specific traffic, this can be done by selecting Manage ACL and defining the appropriate traffic. It's also possible to specific what level of traffic will be dropped.

## Monitoring the Botnet Traffic Filter

Whenever a known address is classified by the Botnet Traffic Filter, then a syslog message is generated. You can also monitor Botnet Traffic Filter statistics and other parameters by entering commands on the ASA.

### Lab verification result

```
PrimaryFW/pri/act(config)# show dynamic-filter reports top malware-sites
```

Malware Sites (since last clear)

Site	Connections	Logged	Dropped	Threat-level	Category
------	-------------	--------	---------	--------------	----------

---

### Sample output from the show dynamic-filter reports top malware-sites command in real life concept

```
ciscoasa# show dynamic-filter reports top malware-sites
```

Site	Connections	logged	dropped	Threat Level	Category
bad1.example.com (10.67.22.34)	11	0	2		Botnet
bad2.example.com (209.165.200.225)	8	8	3		Virus
bad1.cisco.example (10.131.36.158)	6	6	3		Virus
bad2.cisco.example (209.165.201.1)	2	2	3		Trojan
horrible.example.net (10.232.224.2)	2	2	3		Botnet
nono.example.org (209.165.202.130)	1	1	3		Virus

ciscoasa# **show dynamic-filter reports top malware-ports**

Port	Connections logged
tcp 1000	617
tcp 2001	472
tcp 23	22
tcp 1001	19
udp 2000	17
udp 2001	17
tcp 8080	9
tcp 80	3
tcp >8192	2

ciscoasa# **show dynamic-filter reports top infected-hosts**

Host	Connections logged
10.10.10.51(inside)	1190
10.12.10.10(inside)	10
10.10.11.10(inside)	5

## Verification to check on domain name black listed or whitelisted

**PrimaryFW/pri/act(config-llist)# show run dynamic-filter**

dynamic-filter updater-client enable

dynamic-filter use-database

dynamic-filter enable interface outside

dynamic-filter drop blacklist interface outside

dynamic-filter whitelist

name nptc.com

dynamic-filter blacklist

name bad.com

## Impact of Botnet Filtering

Post implementing the entire process of Botnet Filtering, there is a high chance that, Botnet Filtering can drop some websites which are most commonly used for business needs. Thus it is mandatory for us to get an analysis done post the implementation.

- Infrastructure analysis
- Scheduling a downtime
- Run a pilot test
- Recovery action

## Recovery Action

Cisco Security Intelligent Operations (CSIO) has the list of updated botnet hackers collected across the globe. It includes websites of various risk levels – low to medium to high. There is a possibility that some websites which one may need for business is also in the list of CSIO database hence get blocked. It is the administrator's responsibility to analyze the risk factor of any given website with their respective infrastructure security team. This will enable one to decide if the website can be added under static whitelist if it is important for a business.

## Virtual private network (VPN) - Customer Provision VPNs

A VPN is a technology use to extend access to a private network to users who do not have direct access to it, such as an office network allowing secure access from off-site over the Internet.

This is achieved by creating a link between computer networks by the use of network [tunneling\\_protocols](#). The goal of a virtual private network is to allow network hosts (PCs, servers, etc.) to exchange network messages across another network to access private content, as if they were part of the same network

### How a VPN Works:

**Connection:** Your device connects to a VPN server, which is usually located in a different geographical location.

**Encryption:** The VPN encrypts all your internet traffic before it leaves your device.

**Tunneling:** The encrypted data is sent through a secure tunnel to the VPN server.

**Decryption:** The VPN server decrypts the data and sends it to its intended destination.

**Masked IP Address:** Your IP address is masked by the VPN server, so your original IP address is not visible.

## **Benefits of Using a VPN:**

### **Enhanced Privacy:**

VPNs encrypt your data and hide your IP address, making it harder for third parties to track your online activities and personal information.

### **Increased Security:**

VPNs protect your data when using public Wi-Fi networks, which are often insecure.

### **Access to Geographically Restricted Content:**

VPNs can bypass regional restrictions and allow you to access content from different locations.

### **Secure Remote Access:**

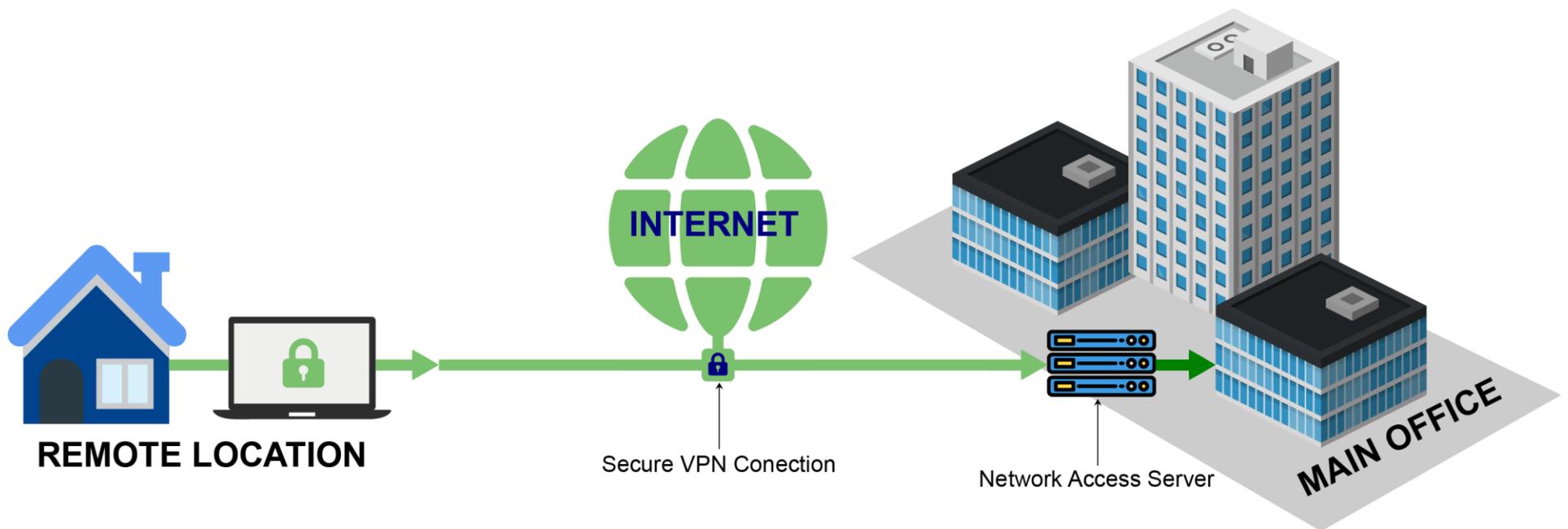
VPNs allow users to access private networks and company resources securely from remote locations

## Types of VPN.

**Remote Access:** This method use to a host to network, this type of extension provides computer access to [local area network](#) of a remote site, or any wider enterprise networks.

This may be employed for [remote workers](#), or to enable people accessing their private company resources without exposing them to the public Internet.

Remote-access VPNs, which are typically user-initiated, may use [passwords](#), [biometrics](#), [two-factor authentication](#), or other [cryptographic](#) methods.

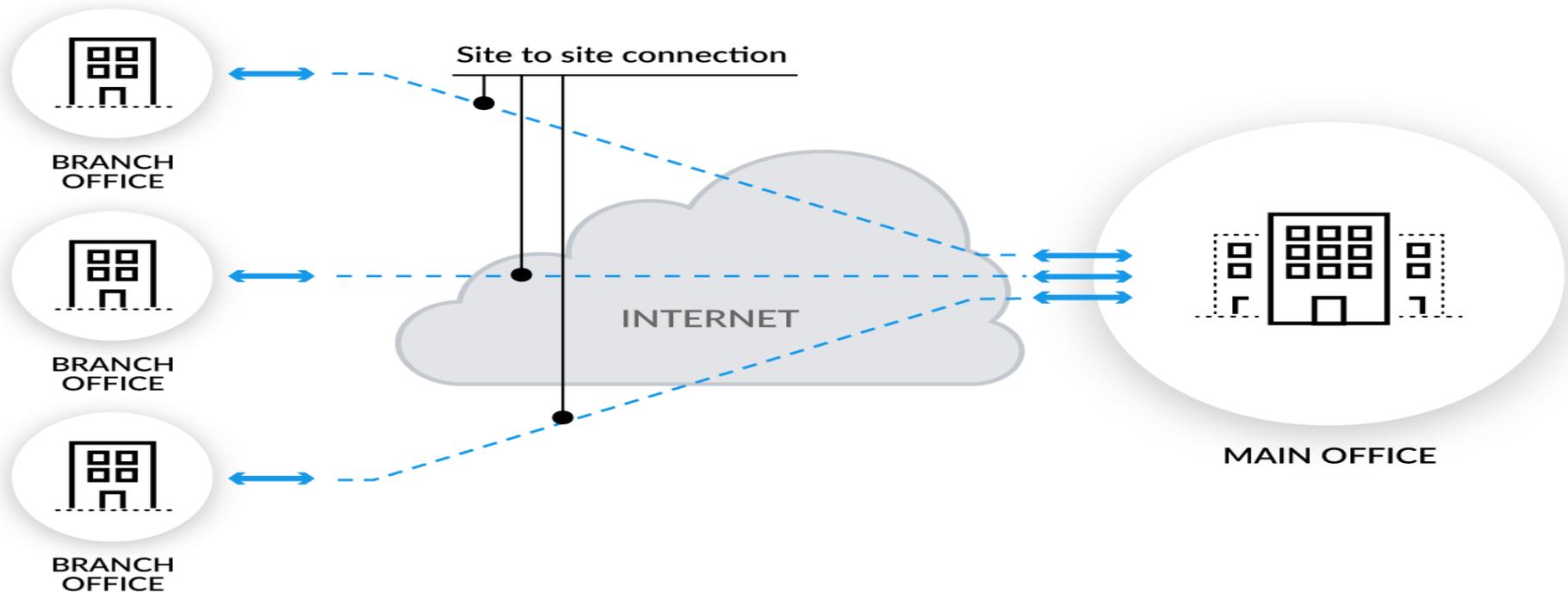


**Site-to-site:** This method is used to connect two networks. Tunneling is only done between two devices (like routers, firewalls, VPN Concentrators, Servers, etc.) located at both network locations.

Businesses tend to make use of site-to-site connections for business-to-business, cloud computing, and branch office scenarios.

Site-to-site VPNs often use passwords (pre-shared keys) or digital certificates. Depending on the VPN protocol, they may store the key to allow the VPN tunnel to establish automatically, without intervention from the administrator.

### Site to Site VPN



## VPN Technologies Used

A virtual private network is based on a tunneling protocol. Cisco ASA support two types **Internet Protocol Security (IPsec) VPN** and **Secure Sucket Tunnel SSL/TLS VPN** tunnel protocols.

### Site to Site

**Site to Site VPN** uses IPsec tunnels to protect data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

### Remote Access VPN

Remote access can use either SSL or IPsec technology for the remote secure connections.

**SSL VPN-** There are mainly two types of SSL VPNs supported by Cisco devices

**Clientless Mode WebVPN:** This is the first implementation of SSL WebVPN supported. Let's users establish a secure remote access VPN tunnel using just a Web browser. There is no need for a software or hardware VPN client. However, only limited applications can be accessed remotely.

**Any Connect WebVPN:** A special Java based client is installed on the user's computer. Providing an SSL secure tunnel to the central site. Provides full network connectivity (similar with IPsec Remote Access client).All applications and network resources at the central site can be accessed remotely.

## Implementing SSL AnyConnect VPN on Cisco ASA

Cisco AnyConnect is a Virtual Private Network (VPN) client software that allows users to establish a secure, encrypted connection to a corporate network from off-campus locations

### **Key Features and Functionality:**

#### **Secure VPN Connection:**

AnyConnect uses encryption protocols like SSL and IPSec to create a secure, private tunnel for data transmission between the user's device and the corporate network.

#### **Client-Side Software:**

It's a software application that users install on their devices (Windows, macOS, iOS, Android).

#### **Authentication Options:**

It supports various authentication methods, including username/password, two-factor authentication, and digital certificate

#### **Network Roaming:**

AnyConnect can seamlessly re-establish the VPN connection after network changes or device standby

## **Use Cases:**

### **Remote Access to Corporate Resources:**

Allows users to access email, file servers, databases, and other restricted resources from off-campus locations.

### **Secure Remote Work:**

Enables employees to work securely from anywhere by connecting to the corporate network.

### **University/School Access:**

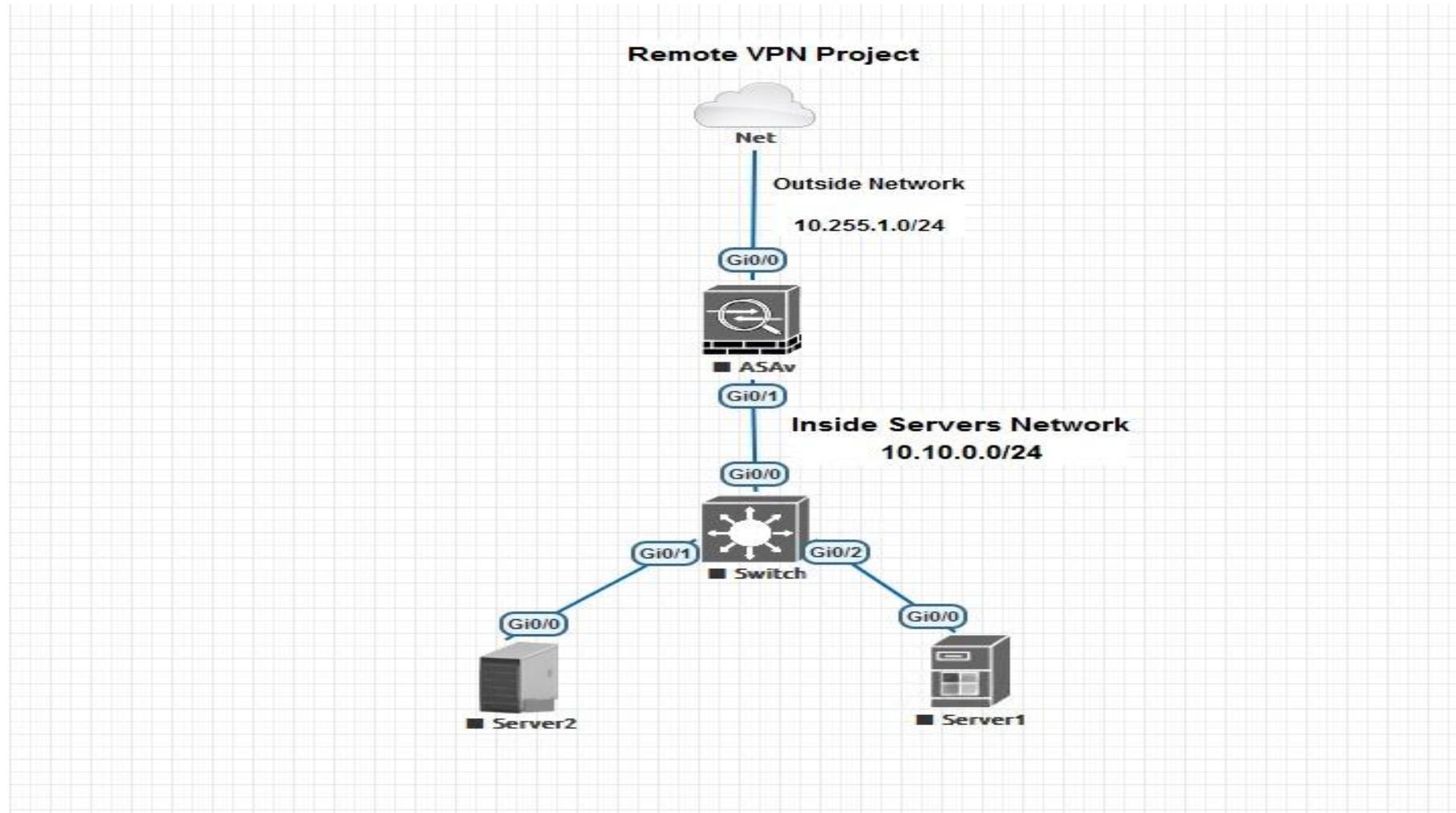
Provides students and faculty with secure access to university networks and resources.

### **Secure Application Connectivity:**

Allows users to access specific applications on the corporate network, even if the applications are not directly exposed to the internet.

## SSL AnyConnect VPN Project Task

Project Task: Create SSL Anyconnect VPN client using the Topology below

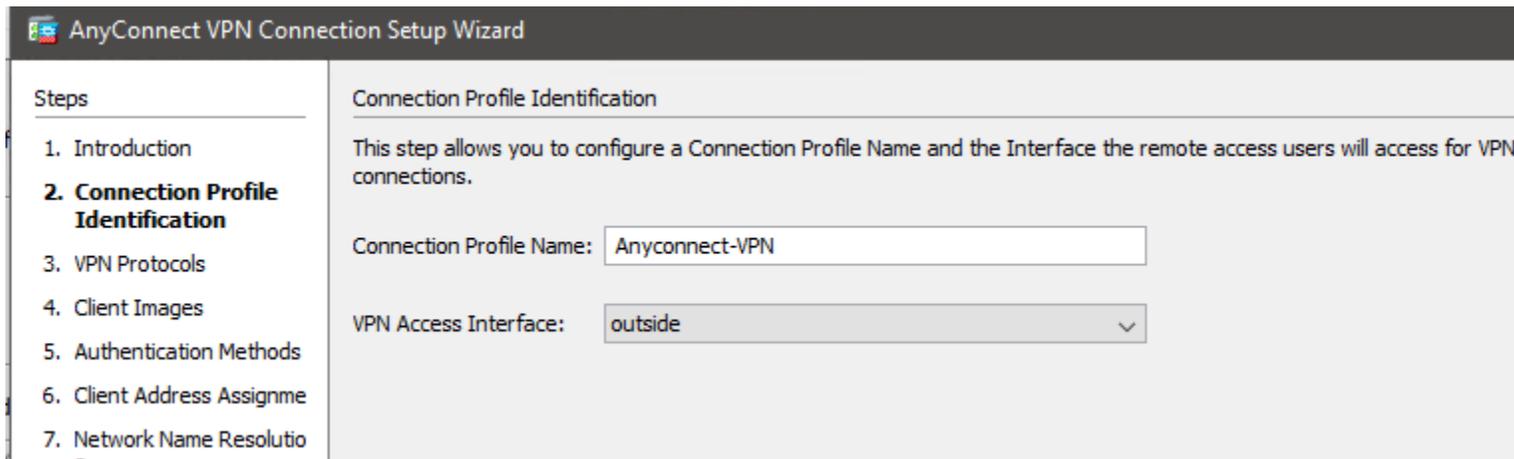


## SSL AnyConnect VPN Project Task

Create SSI Anyconnect VPN client using the Topology above

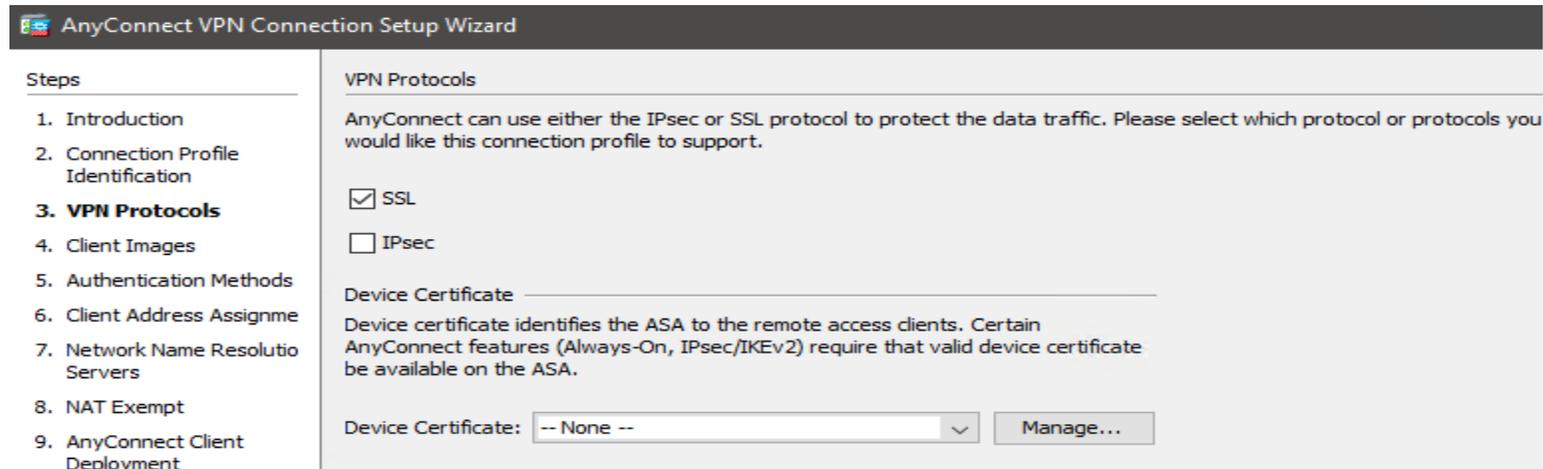
Step 1. Use the wizard to create a new SSL anyconnect

Define connection profile name



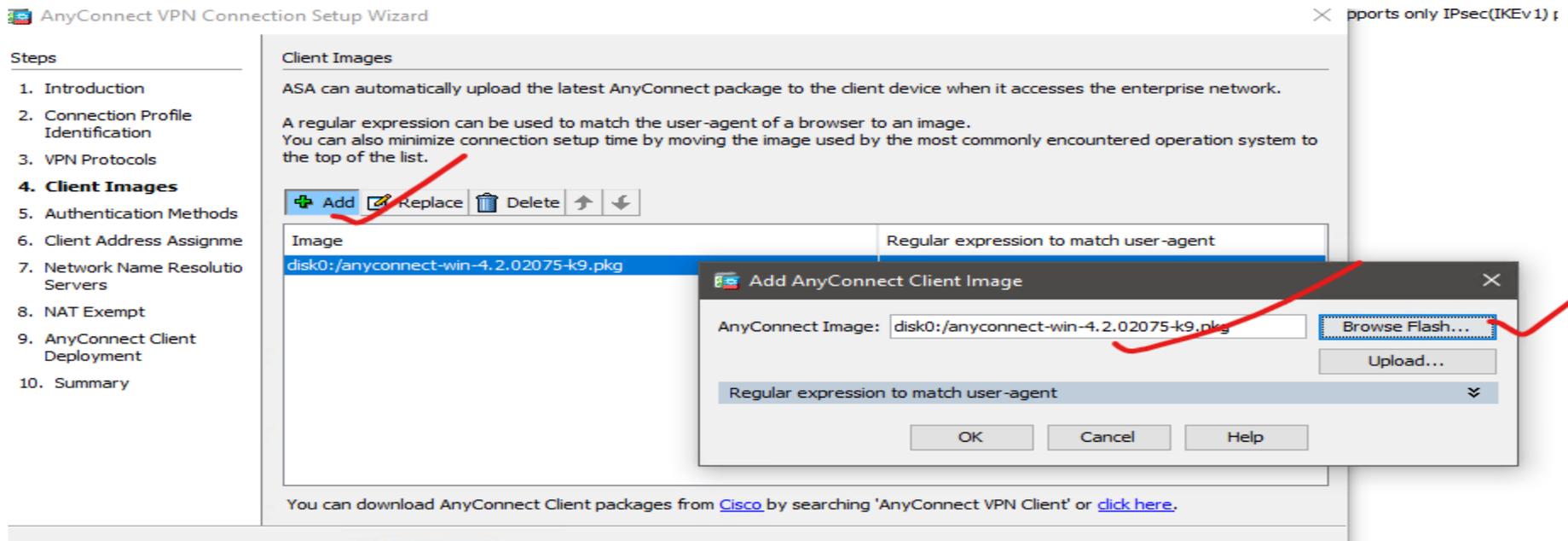
The screenshot displays the 'AnyConnect VPN Connection Setup Wizard' interface. On the left, a 'Steps' sidebar lists the following steps: 1. Introduction, 2. **Connection Profile Identification**, 3. VPN Protocols, 4. Client Images, 5. Authentication Methods, 6. Client Address Assignme, and 7. Network Name Resolutio. The main area is titled 'Connection Profile Identification' and contains the following text: 'This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.' Below this text, there are two input fields: 'Connection Profile Name:' with a text box containing 'Anyconnect-VPN', and 'VPN Access Interface:' with a dropdown menu showing 'outside'.

## Step.2 Select which protocol u want to use to protect the data either IPsec or SSL and select the device certificate if any



The screenshot shows the 'VPN Protocols' step of the AnyConnect VPN Connection Setup Wizard. On the left, a 'Steps' sidebar lists steps 1 through 9, with '3. VPN Protocols' highlighted. The main area contains the following text: 'AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.' Below this are two checkboxes: 'SSL' (checked) and 'IPsec' (unchecked). A 'Device Certificate' section follows, with a text box containing 'Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.' At the bottom, there is a dropdown menu for 'Device Certificate' set to '-- None --' and a 'Manage...' button.

## Step.3 Allow ASA to automatically upload the latest AnyConnect package to the client



The screenshot shows the 'Client Images' step of the AnyConnect VPN Connection Setup Wizard. The 'Steps' sidebar on the left highlights '4. Client Images'. The main area contains the text: 'ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network. A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.' Below this is a toolbar with 'Add', 'Replace', 'Delete', and arrow icons. A table lists client images with columns for 'Image' and 'Regular expression to match user-agent'. One entry is 'disk0:/anyconnect-win-4.2.02075-k9.pkg'. An 'Add AnyConnect Client Image' dialog box is open, showing the 'AnyConnect Image' field with the same path and a 'Browse Flash...' button. A red checkmark is next to the 'Add' button in the main window, and another red checkmark is next to the 'Browse Flash...' button in the dialog box. At the bottom of the main window, there is a link: 'You can download AnyConnect Client packages from [Cisco](#) by searching 'AnyConnect VPN Client' or [click here](#).'

## Step-4 Create the authentication method either with a AAA server or use LOCAL and create account if is local

**AnyConnect VPN Connection Setup Wizard**

**Steps**

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
- 5. Authentication Methods**
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

**Authentication Methods**

This step lets you specify the location of the authentication server. You can click on the "New..." button to create a new server group.

AAA Server Group: LOCAL

**Local User Database Details**

User to be Added

Username: admin-user1

Password: ●●●●

Confirm Password: ●●●●

admin  
admin-user1

The screenshot shows the 'Authentication Methods' step of the AnyConnect VPN Connection Setup Wizard. The 'AAA Server Group' is set to 'LOCAL', and the 'New...' button is highlighted with a red checkmark. In the 'Local User Database Details' section, the 'User to be Added' form has 'admin-user1' entered in the 'Username' field, and both the 'Password' and 'Confirm Password' fields are filled with dots. The 'Add >>' button is highlighted with a red checkmark, and the 'Delete' button is also highlighted with a red checkmark. A list box on the right shows the current users in the database: 'admin' and 'admin-user1', with a red checkmark next to 'admin-user1'.

## Step.5 Create DHCP pool for the remote vpn client

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
- 6. Client Address Assignment**
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

### Client Address Assignment

This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyC will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

IP v4 Address Pool | IP v6 Address Pool

Address Pool:

Details of the selected address pool

Starting IP Address:  ...

Ending IP Address:  ...

Subnet Mask:  ▾

## Step.6 Add your dns server info (should be corporate info)

The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window. On the left, a 'Steps' sidebar lists: 1. Introduction, 2. Connection Profile Identification, 3. VPN Protocols, 4. Client Images, 5. Authentication Methods, and 6. Client Address Assignme. The main area is titled 'Network Name Resolution Servers' and contains the following text: 'This step lets you specify how domain names are resolved for the remote user when accessing the internal network.' Below this text are three input fields: 'DNS Servers:' with the value '10.10.0.40', 'WINS Servers:' with the value '10.10.0.40', and 'Domain Name:' with the value 'nptc.com'.

## Step.7 Exempt NAT from vpn traffic if NAT is enable on this ASA

The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window. On the left, the 'Steps' sidebar is updated to include: 7. Network Name Resolutio Servers, 8. NAT Exempt (highlighted in bold), 9. AnyConnect Client Deployment, and 10. Summary. The main area is titled 'NAT Exempt' and contains the following text: 'If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.' Below this text is a checked checkbox labeled 'Exempt VPN traffic from network address translation'. Underneath, there are two sections: 'Inside Interface is the interface directly connected to your internal network.' with a dropdown menu showing 'inside', and 'Local Network is the network address(es) of the internal network that client can access.' with a text input field containing 'any4' and a search icon. At the bottom, a note states: 'The traffic between AnyConnect client and internal network will be exempt from network address translation.'

AnyConnect VPN Connection Setup Wizard

**Steps**

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt

**AnyConnect Client Deployment**

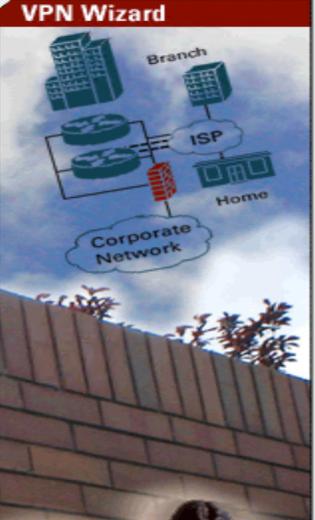
AnyConnect client program can be installed to a client device by one of the following two methods:

- 1) Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed;
- 2) Pre-deployment - Manually install the AnyConnect client package.

## Step.8 Go through the Summary of the configuration before clicking finish

AnyConnect VPN Connection Setup Wizard

**VPN Wizard**



**Summary**

Here is the summary of the configuration.

Name	Value
<input type="checkbox"/> Summary	
Name/Alias of the Connection Profile	Anyconnect-VPN
VPN Access Interface	outside
Device Digital Certificate	-- none --
VPN Protocols Enabled	SSL only
AnyConnect Client Images	1 package
Authentication Server Group	LOCAL
Address Pool for the Client	192.168.50.50 - 192.168.50.200
DNS	Server: Domain Name:
Network Address Translation	The protected traffic is not subjected to network address translation

## Step.9 Ensure all this are check with your connection profile

[Configuration](#) > [Remote Access VPN](#) > [Network \(Client\) Access](#) > [AnyConnect Connection Profiles](#)

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment is performed on the interfaces selected in the table below.

Access Interfaces

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

Allow user to select connection profile on the login page. [i](#)

Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificates to connection profiles.

[+](#) Add [✎](#) Edit [🗑](#) Delete Find:  [▼](#) [▲](#)  Match Case

Name	SSL Enabled	IPsec Enabled
DefaultRAGroup	<input type="checkbox"/>	
DefaultWEBVPNGroup	<input type="checkbox"/>	
Sales-con-profile	<input type="checkbox"/>	
ipsec1-group	<input type="checkbox"/>	
Anyconnect-VPN	<input checked="" type="checkbox"/>	

## Split Tunnel

By default all traffic will be sent through the tunnel once the remote user is connected. If you want to allow remote users to access the Internet once they are connected then you need to configure split tunneling. We will configure an access-list that specifies what networks we want to reach through the tunnel.

So let now configure the split tunnel

[Configuration > Remote Access VPN > Network \(Client\) Access > AnyConnect Connection Profiles](#)

Click on the connection profile > edit

The screenshot shows the 'Edit AnyConnect Connection Profile: Anyconnect-VPN' configuration window. The window is divided into several sections:

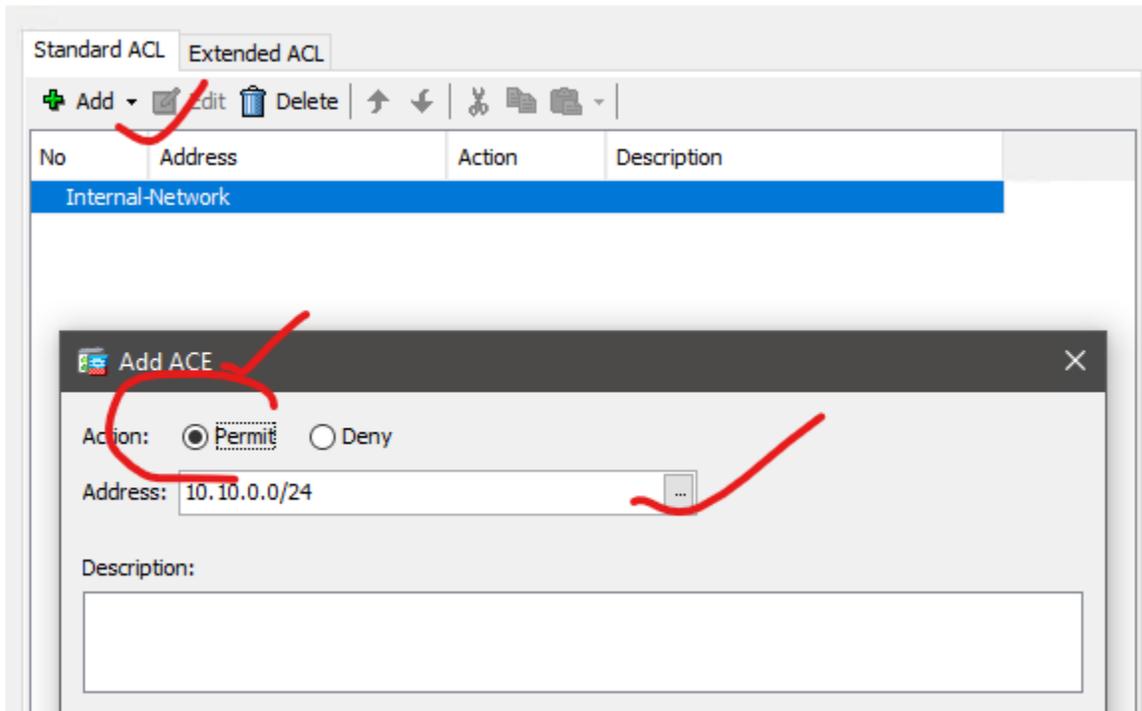
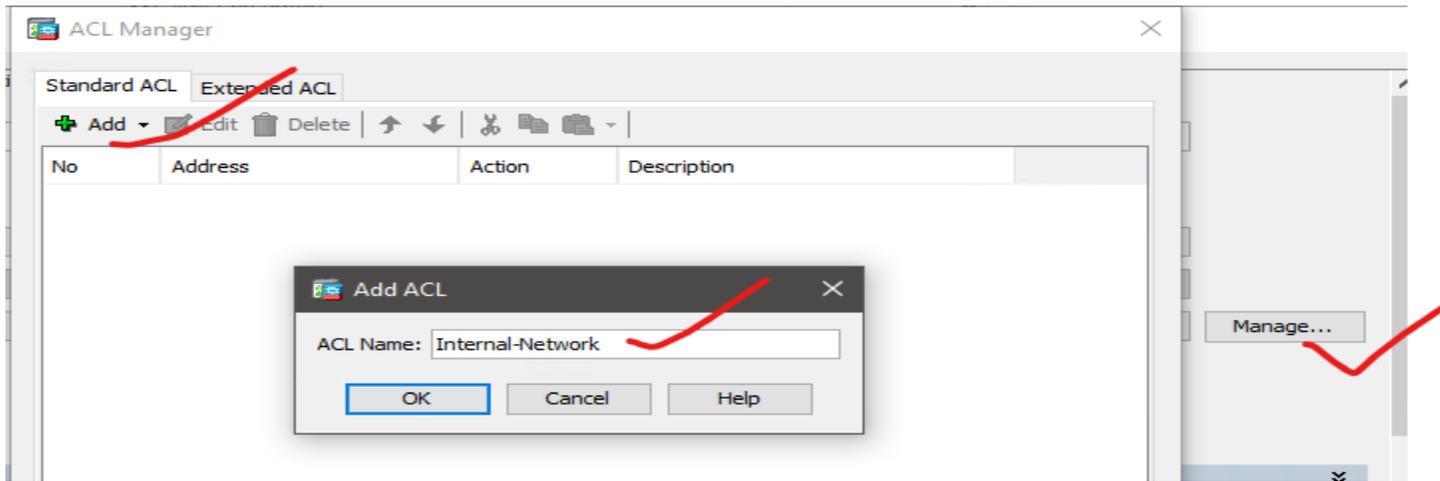
- Name:** Anyconnect-VPN
- Aliases:** Anyconnect-VPN
- Authentication:**
  - Method:  AAA  Certificate  AAA and Certificate  Saml
  - AAA Server Group: LOCAL (dropdown menu) [Manage...]
  - Use LOCAL if Server Group fails
- Client Address Assignment:**
  - DHCP Servers: [Empty text box]
  - None  DHCP Link  DHCP Subnet
  - Client Address Pools: Anyconnect-Pool [Select...]
  - Client IPv6 Address Pools: [Empty text box] [Select...]
- Default Group Policy:**
  - Group Policy: GroupPolicy\_Anyconnect-VPN (dropdown menu) [Manage...]
  - (Following fields are linked to attribute of the group policy selected above.)
  - Enable SSL VPN client protocol
  - Enable IPsec(IKEv2) client protocol
  - DNS Servers: 10.10.0.40
  - WINS Servers: 10.10.0.40
  - Domain Name: nptc.com

## Click on manage under default

The image shows two overlapping windows from a network management interface. The left window, titled "Edit AnyConnect Connection Profile: Anyconnect-VPN", has the "Advanced" tab selected. It contains fields for Name, Aliases, Authentication Method (AAA selected), AAA Server Group (LOCAL), Client Address Assignment (DHCP Servers, Client Address Pools, Client IPv6 Address Pools), and Default Group Policy (GroupPolicy\_Anyconnect-VPN). A red checkmark is next to the "Manage..." button for the Default Group Policy. The right window, titled "Configure Group Policies", shows a table of policies. A red checkmark is next to the "Edit" button. The table lists policies with columns for Name, Type, Tunneling Protocol, and Connection Profiles/Users Assigned To.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
ipsec1-group	Internal	ikev1	ipsec1-group;ipsecuser 1
GroupPolicy_A...	Internal	ssl-client	Anyconnect-VPN
DfltGrpPolicy (...)	Internal	ikev1;ikev2;ssl-clientless;I2...	DefaultRAGroup;DefaultL2LGroup...
Sales-Group	Internal	ssl-clientless	Sales-con-profile;user 1;user

The image shows the "Edit Internal Group Policy: GroupPolicy\_SSL-VPN-Con-Profile" window. The "Advanced" tab is selected, and the "Split Tunneling" section is highlighted in the left sidebar. The main area contains settings for DNS Names, Send All DNS Lookups Through Tunnel, Policy, IPv6 Policy, and Network List. Red checkmarks are placed next to the "Inherit" checkboxes for DNS Names, Send All DNS Lookups Through Tunnel, IPv6 Policy, and Network List. A red checkmark is also next to the "Manage..." button. A red checkmark is also next to the "Split Tunneling" section in the sidebar.



The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' fields.

DNS Names:  Inherit

Send All DNS Lookups Through Tunnel:  Inherit  Yes  No

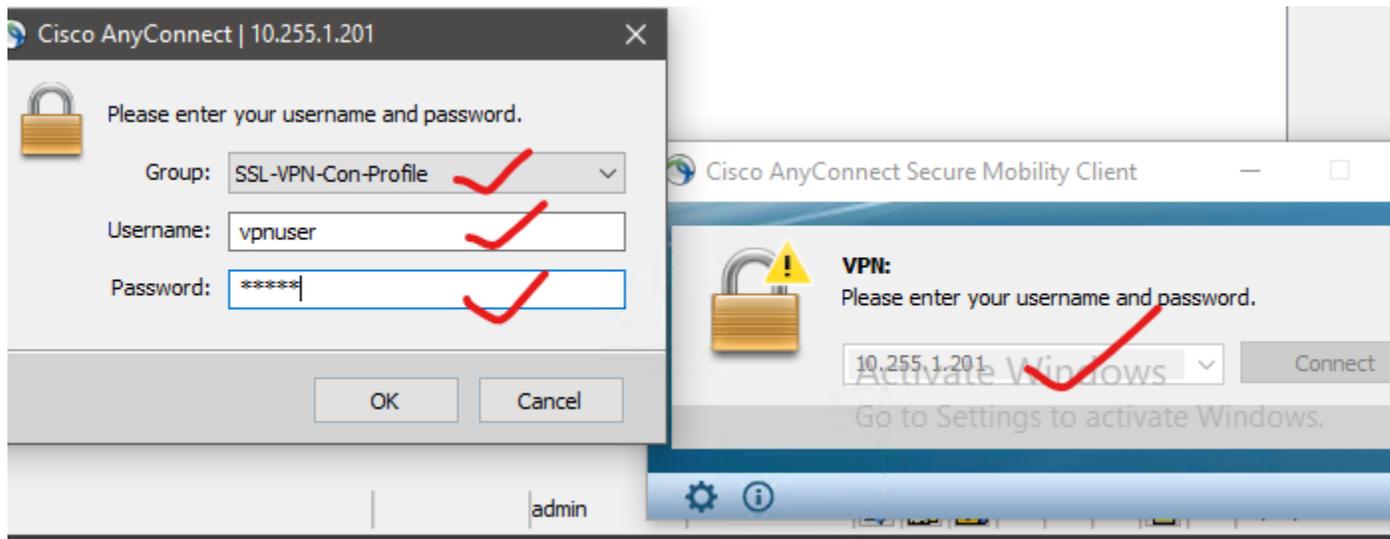
Policy:  Inherit  ✓

IPv6 Policy:  Inherit

Network List:  Inherit  ✓

Pressing this button to set up split exclusion for Web Security proxies.

## Now we can test our vpn



Now you can connect as local user but not with rdp so use anydesk for testing purpose

The screenshot displays the Cisco AnyConnect Secure Mobility Client interface. The title bar reads "Cisco AnyConnect Secure Mobility Client". The main header features the Cisco logo and the text "AnyConnect Secure Mobility Client". Below this, the section "Virtual Private Network (VPN)" is active, with tabs for "Preferences", "Statistics", "Route Details", "Firewall", and "Message History".

The "Statistics" tab is selected, showing the following data:

Connection Information	
State:	Connected
Tunnel Mode (IPv4):	Split Include
Tunnel Mode (IPv6):	Drop All Traffic
Duration:	00:04:30

Address Information	
Client (IPv4):	192.168.10.50
Client (IPv6):	Not Available
Server:	10.255.1.201

Bytes	
Sent:	12099
Received:	27495

Frames	
--------	--

Red checkmarks are drawn over the "Connected" state, the "Client (IPv4)" address, and the "Server" address.



## Virtual Private Network (VPN)

Preferences Statistics Route Details Firewall Message History

05:30:09 AnyConnect was not able to establish a connection to the specified secure gateway. Please try connecting again. ^

05:30:09 VPN session ended.

05:36:08 Contacting 10.255.1.201. ✓

05:36:21 User credentials entered.

05:36:21 Establishing VPN session...

05:36:21 The AnyConnect Downloader is performing update checks...

05:36:21 Checking for profile updates...

05:36:27 Downloading AnyConnect VPN Profile - 100% ✓

05:36:27 Checking for product updates...

05:36:27 Checking for customization updates...

05:36:28 Performing any required updates...

05:36:28 The AnyConnect Downloader updates have been completed.

05:36:32 Establishing VPN session...

05:36:32 Establishing VPN - Initiating connection...

05:36:32 Establishing VPN - Examining system...

05:36:32 Establishing VPN - Activating VPN adapter... ✓

05:36:36 Establishing VPN - Configuring system... ✓

05:36:37 Establishing VPN...

05:36:37 Connected to 10.255.1.201. ✓

▼

```
ciscoasa# show vpn-sessiondb summary
```

```
-----  
----  
VPN Session Summary  
-----  
----
```

```
Active : Cumulative : Peak Concur : Inac  
tive  
-----  
----  
AnyConnect Client : 1 : 4 : 1 :  
0  
SSL/TLS/DTLS : 1 : 4 : 1 :  
0
```

## Implementing clientless VPN on Cisco ASA

Cisco clientless SSL VPNs allow organizations to provide secure remote access to protected network resources in the headquarters, even when the remote user device is not managed or has no VPN client installed.

In other words, it provides the simplest way for users to access mainly web-based (and some non-web-based) applications over a web browser.

The VPN gateway that acts as a proxy between the remote user and protected resources is responsible for the overall VPN permissions, such as services allowed, bookmarks available

Keep in mind that the Cisco Firepower NGFW firewall doesn't support clientless VPN deployment.

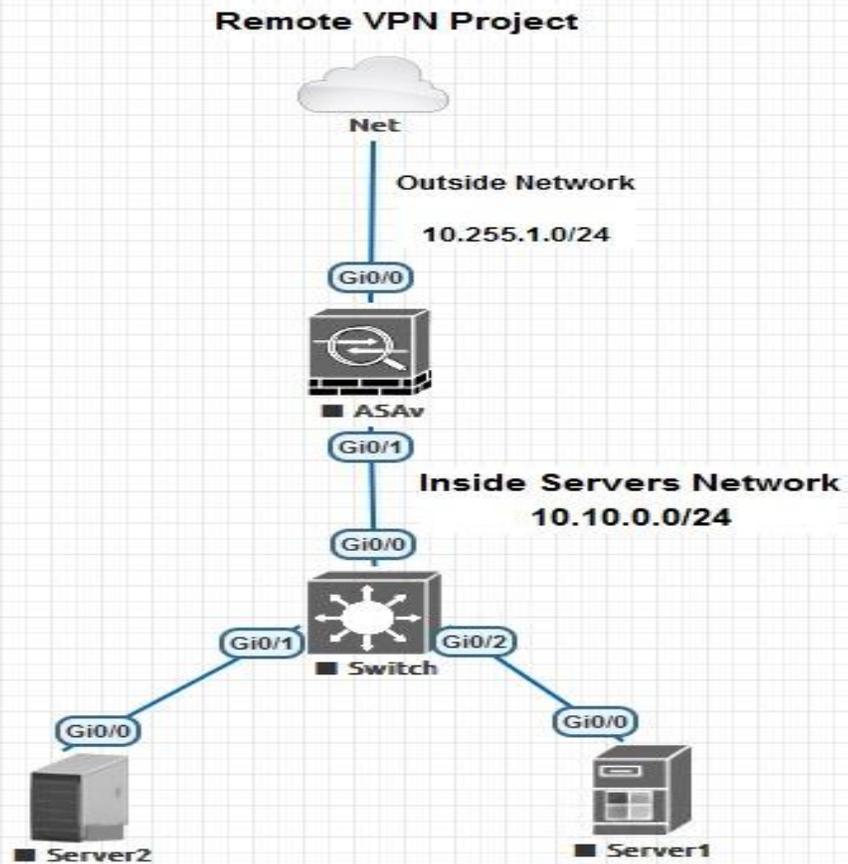
Typical use cases include **internet kiosks, on demand** and **business partners** that require access only to a specific set of services and resources in general, which works perfectly with the clientless VPN limitation.

However, the clientless TLS VPN solution has some limitations. Because everything is done through the web portal, it may require user training so that users can learn how to use the navigation portal before they begin using it.

Furthermore, due to its proxying nature, real-time applications often experience latency and delay, which makes them unusable at times.

Finally, since this VPN solution doesn't support all IP applications, sometimes you have to choose a different option

## Clientless SSL VPN on ASA Project



## SSL Clientless Project Task

Project requirement is to create clientless VPN where any random machines on the internet can connect to internal sales server for corporate work

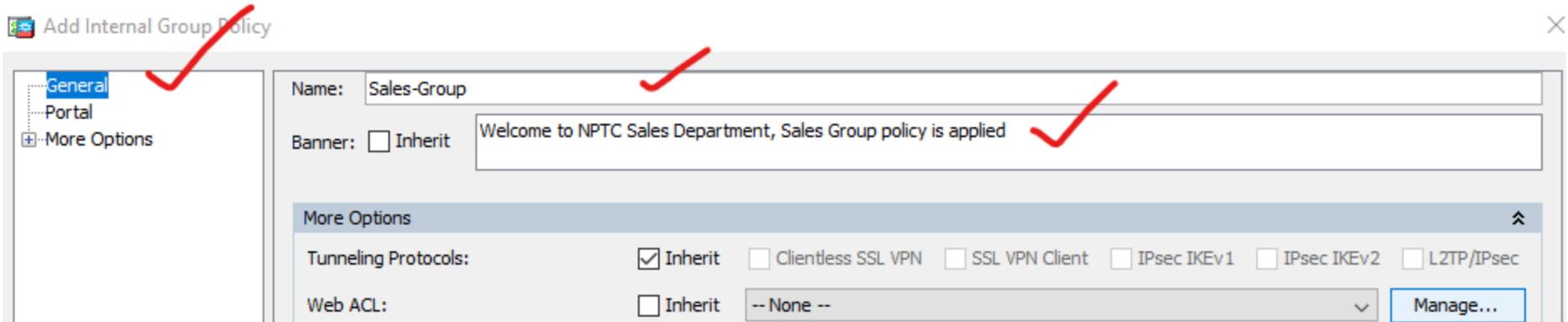
The **clientless WebVPN** method does not require a VPN client to be installed on the user's computer. You just open your web browser, enter the IP address of the ASA and you will get access through a web portal. You only have limited access to a number of applications, for example:

- Internal websites (HTTP and HTTPS)
- Web applications
- Windows file shares
- Email servers (POP3, IMAP, SMTP)
- Microsoft Outlook Web Access

There is **no full network access** when you use clientless WebVPN

**Step1. Create a new vpn policies for sales users**

**Configuration ▶ Remote Access ▶ Clientless SSL VPN Access ▶ Group Policies ▶ Add**

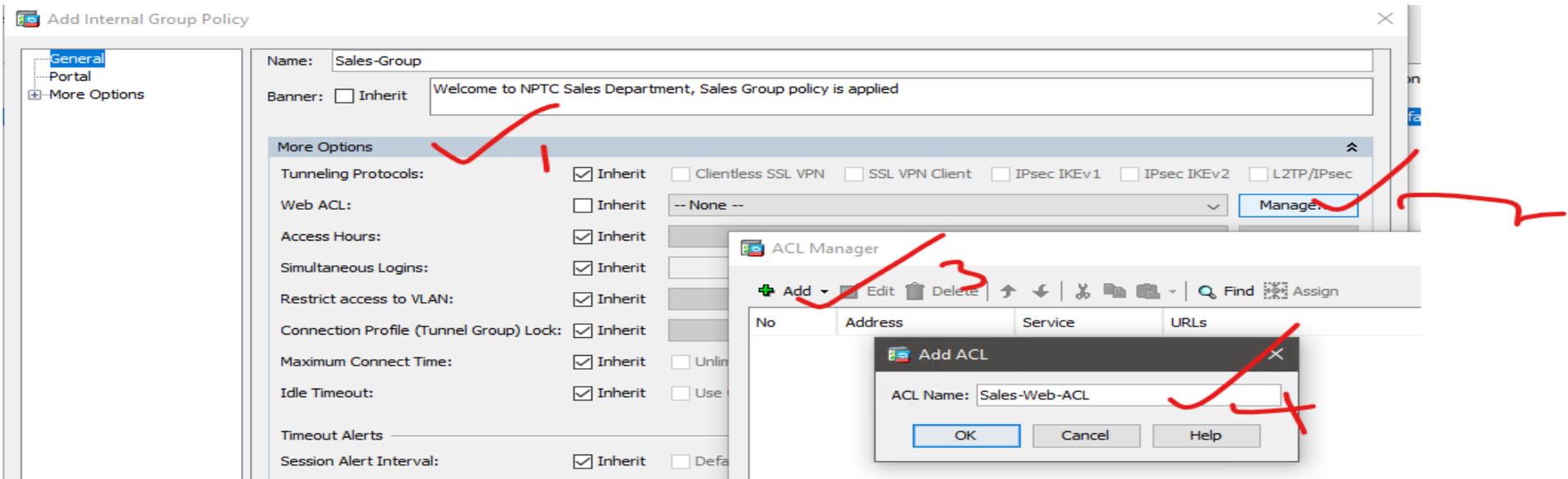


**Step2. Apply web type ACL to prevent sales users from accessing certain services (Optional)**

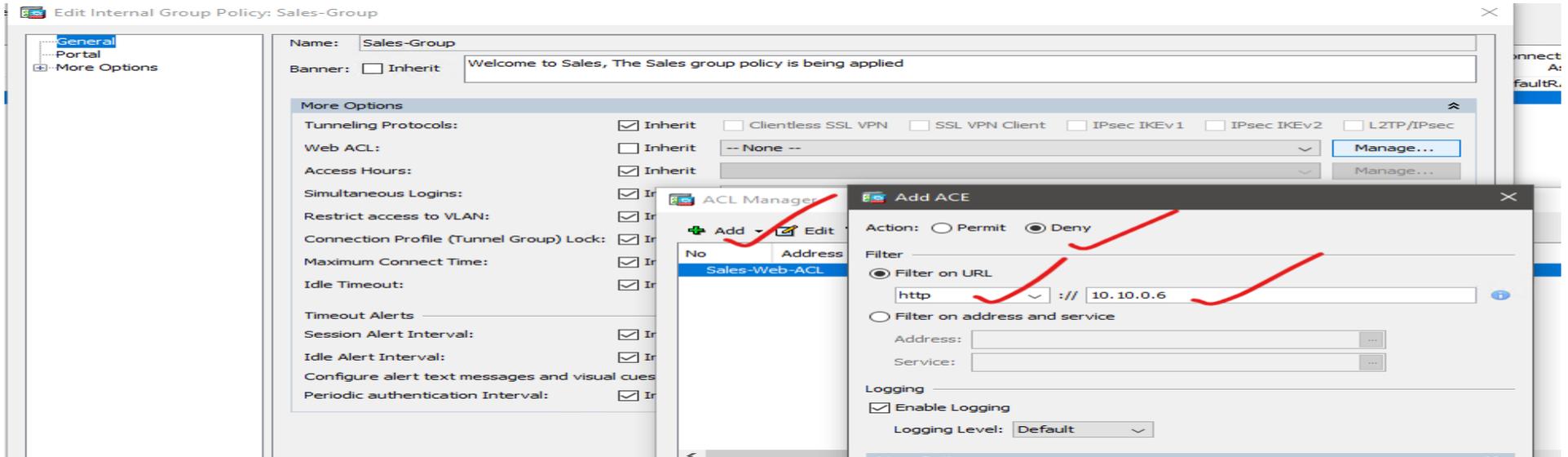
1. First is to create web acl

2. Second Create ACE – Access Control Entry

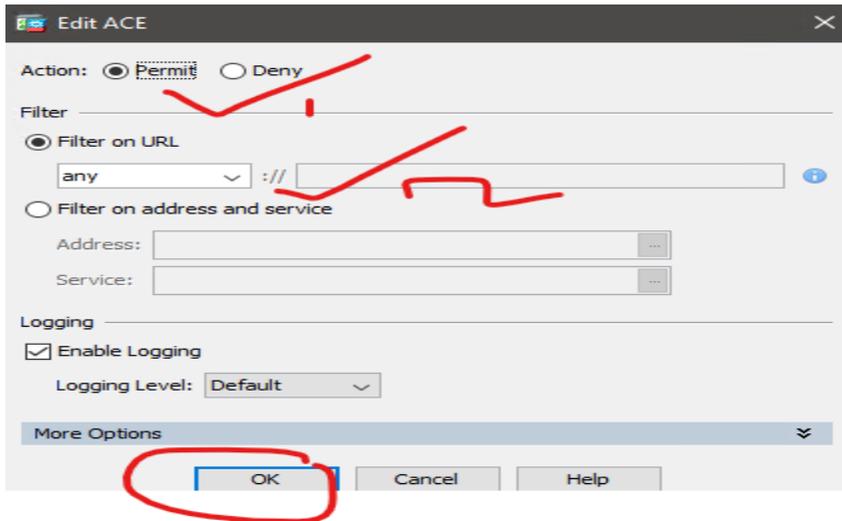
1. First is to create web acl



## Second Create ACE – Access Control Entry



Now permit all other traffic without this everything will be drop



ACL Manager

No	Address	Service	URLs	Action	Time
Sales-Web-ACL					
1			http://10.10.0.6	Deny	
2			any	Permit	

Last step for the ACL is to select it on the drop menu

Edit Internal Group Policy: Sales-Group

Name: Sales-Group

Banner:  Inherit

More Options

Tunneling Protocols:  Inherit  Clientless SSL VPN  SSL VPN Client  IPsec IKEv1  IPsec IKEv2  LTP/IPsec

Web ACL:  Inherit

Access Hours:  Inherit

Simultaneous Logins:  Inherit

Restrict access to VLAN:  Inherit

### Step-3 Create the bookmark list

#### Add internal Group Policy ► Portal ► un-chick Bookmark list ► Manage ► Add

**Edit Internal Group Policy: Sales-Group**

**General** | **Portal** | More Options

Bookmark List:  Inherit -- None -- Manage...

URL Entry:  Inherit  Enable  Disable

**File Access Control**

File Server Entry:  Inherit

File Server Browsing:  Inherit

Hidden Share Access:  Inherit

**Port Forwarding Control**

Port Forwarding List:  Inherit

Applet Name:  Inherit

**Smart Tunnel**

Smart Tunnel Policy:  Inherit

Smart Tunnel Application:  Inherit

Auto Sign-on Server:  Inherit

ActiveX Relay:  Inherit  Enable  Disable

**Configure GUI Customization Objects**

Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.

This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on [Assign](#) button to assign the selected one to them.

Add  Edit  Delete  Import

Bookmarks	Group Policies/DA
Template	

Find:

**Add Bookmark List**

Bookmark List Name: Book-for-Sales

Bookmark Title	URL
----------------	-----

**Select Bookmark Type**

Select an option to use for bookmark creation:

- URL with GET or POST method  
This is the traditional bookmark using the GET method, or the POST method with parameters.
- Predefined application templates (Microsoft OWA, SharePoint, Citrix XenApp/XenDesktop, Lotus Domino)  
This option simplifies bookmark creation with users selecting a predefined ASDM template that contains the pre-filled necessary values for certain well-defined applications like Microsoft OWA 2010 and Citrix XenApp.
- HTML form auto-submit  
This option lets you create bookmark for any complex auto sign-on application. It will require two steps:  
1- Define the bookmark with some basic initial data and without the post parameters. Save and assign the bookmark to use in a group policy or user.

Bookmark Title: Server 1

URL: http://10.10.0.5

Preload Page (Optional)

Preload URL: http://

Wait Time: (seconds)

Other Settings (Optional)

Subtitle: This server is a web server

Thumbnail: -- None -- Manage

Place this bookmark on the VPN home page

Enable Smart Tunnel

Creating another Bookmark starting item 6 as reference

Add Bookmark

Bookmark Title: Sales File Application

URL: http://10.10.0.8 Assistant...

Preload Page (Optional)

Preload URL: http://

Wait Time: (seconds)

Other Settings (Optional)

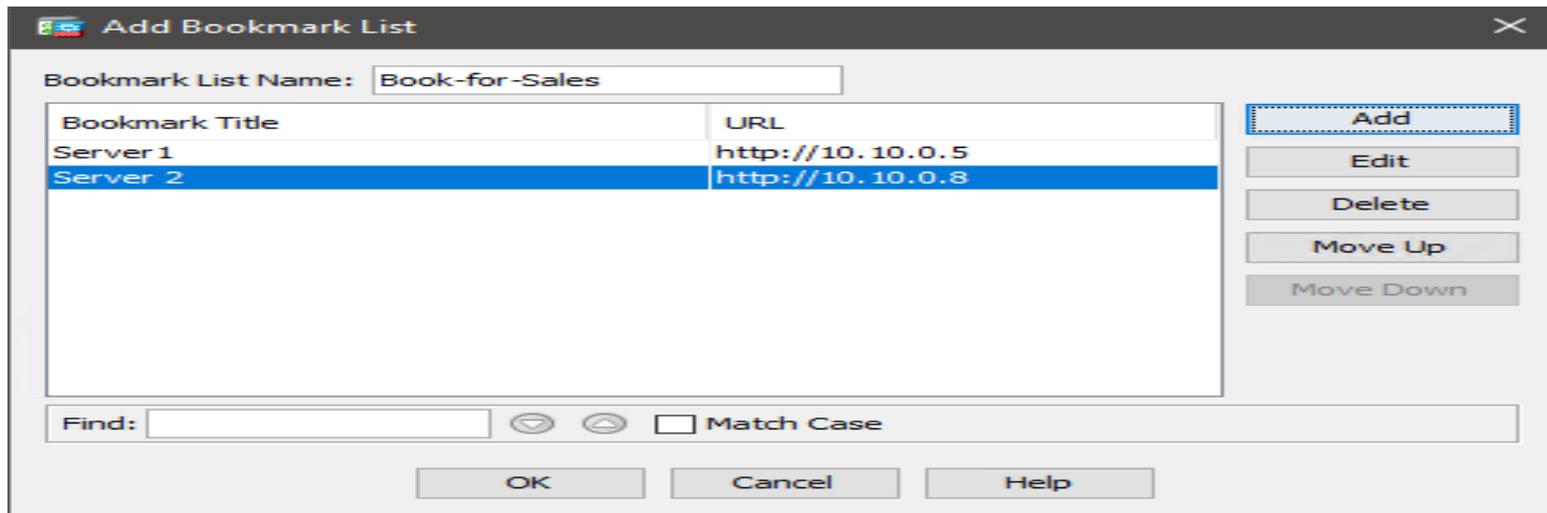
Subtitle: File Server

Thumbnail: -- None -- Manage

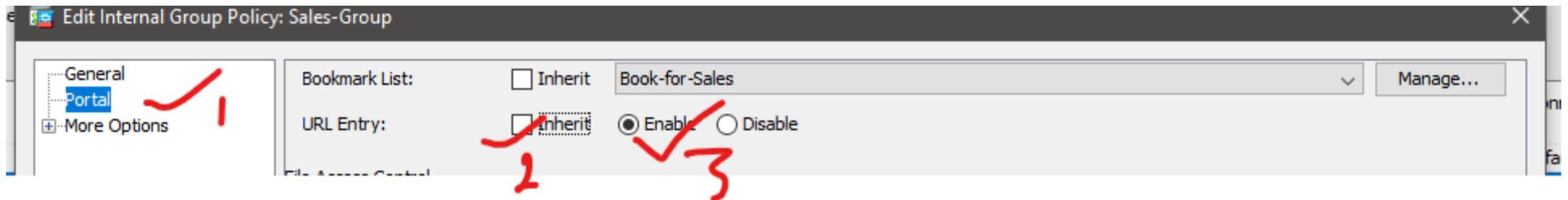
Place this bookmark on the VPN home page

Enable Smart Tunnel

Advanced Options



Enable the URL Entry on the ASA under the Portal



Final Step is to click Apply for all the group policy configuration to take effect

Step 4 Create the Connection profiles to be use for this group

Configuration ► Remote Access ► Clientless SSL VPN ► Connection Profile ► Add

The screenshot displays the Cisco VPN configuration interface. The breadcrumb navigation at the top reads: Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles. The left sidebar shows a tree view with 'Connection Profiles' selected under 'Clientless SSL VPN Access'. The main content area is divided into three sections:

- Access Interfaces:** Contains a table for enabling interfaces for clientless SSL VPN access. The table has two columns: 'Interface' and 'Allow Access'. The 'outside' and 'inside' interfaces are listed, both with 'Allow Access' checkboxes that are currently unchecked. Below the table is a checked checkbox for 'Bypass interface access lists for inbound VPN sessions' and a note: 'Access lists from group policy and user policy always apply to the traffic.'
- Login Page Setting:** Contains three unchecked checkboxes: 'Allow user to select connection profile on the login page.', 'Allow user to enter internal password on the login page.', and 'Shutdown portal login page.'
- Connection Profiles:** Contains a text description: 'Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).' Below this is a toolbar with 'Add', 'Edit', and 'Delete' buttons. The 'Add' button is circled in red. To the right of the toolbar is a search box labeled 'Find:' and a 'Match Case' checkbox.

Additional UI elements include a top navigation bar with 'Home', 'Configuration', 'Monitoring', 'Save', 'Refresh', 'Back', 'Forward', and 'Help'. A 'Device List' sidebar on the left shows IP addresses 10.255.1.201 and 10.255.1.202. The 'Connection Profiles' section also includes 'Device Certificate ...' and 'Port Setting ...' buttons.

Add Clientless SSL VPN Connection Profile

Basic ✓  
Advanced

Name: sales-con-profile ✓  
Aliases: sale-con-alias ✓

Authentication  
Method:  AAA  Certificate  AAA and Certificate  Saml  
AAA Server Group: LOCAL ✓  ✓  
 Use LOCAL if Server Group fails

DNS  
Server Group: DefaultDNS ✓   
(Following fields are attributes of the DNS server group selected above.)  
Servers: 10.10.0.40 ✓  
Domain Name: nptc.com ✓

Default Group Policy  
Group Policy: Sales-Group ✓  ✓  
(Following field is an attribute of the group policy selected above.)  
 Enable clientless SSL VPN protocol

SAML Identity Provider  
SAML Server : --- None ---

## Now Create the URL the users are going to connect with

The screenshot shows the 'Edit Clientless SSL VPN Connection Profile: sales-con-profile' window. The left sidebar has 'Clientless SSL VPN' selected. The main panel shows 'Login and Logout Page Customization' set to 'DfltCustomization'. Under 'Connection Aliases', a table lists an alias 'sale-con-alias' which is enabled. An 'Add Group URL' dialog box is open, showing a URL of 'https://10.255.1.201/sales' and the 'Enabled' checkbox checked.

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Login and Logout Page Customization: DfltCustomization Manage...

Enable the display of Radius Reject-Message on the login screen when authentication is rejected

Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

+ Add ✎ Delete (The table is in-line editable.) ⓘ

Alias	Enabled
sale-con-alias	<input checked="" type="checkbox"/>

Group URL

This SSL VPN access method will present a list of group URLs configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

+ Add ✎ Delete (The table is in-line editable.) ⓘ

URL

without the need for user selection.

URL: https://10.255.1.201/sales

Enabled

OK Cancel Help

Enable clientless SSL VPN traffic termination on Cisco ASA's interface where the remote sessions will arrive.

The screenshot shows the Cisco ASA configuration interface. The breadcrumb navigation is: Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles. The main content area is titled "Access Interfaces" and contains the following text: "Enable interfaces for clientless SSL VPN access." Below this is a table with two columns: "Interface" and "Allow Access". The "outside" interface is selected and has its "Allow Access" checkbox checked, with a red checkmark next to it. The "inside" interface has its "Allow Access" checkbox unchecked. To the right of the table are two buttons: "Device Certificate ..." and "Port Setting ...". Below the table is a checked checkbox labeled "Bypass interface access lists for inbound VPN sessions", also with a red checkmark. Below this is the text: "Access lists from group policy and user policy always apply to the traffic." The "Login Page Setting" section contains three unchecked checkboxes: "Allow user to select connection profile on the login page.", "Allow user to enter internal password on the login page.", and "Shutdown portal login page." The left sidebar shows the "Remote Access VPN" tree with "Clientless SSL VPN Access" expanded to "Connection Profiles". The "Device List" pane shows two devices: 10.255.1.201 and 10.255.1.202.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>

Final stage is to click Apply for the configuration to take effect

Let's create users who can access this VPN by using cisco as password

[Configuration](#) > [Remote Access VPN](#) > [AAA/Local Users](#) > [Local Users](#)

Configuration must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

### Add User Account

- Identity
- Public Key Authentication
- Public Key Using PKF
- + VPN Policy

Username:

Password:

Confirm Password:

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.  
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)  
Privilege level is used with command authorization.  
Privilege Level:

CLI login prompt for SSH, Telnet and console (no ASDM access)  
This setting is effective only if "aaa authentication http console LOCAL" command is configured.

No ASDM, SSH, Telnet or Console access  
This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are configured.

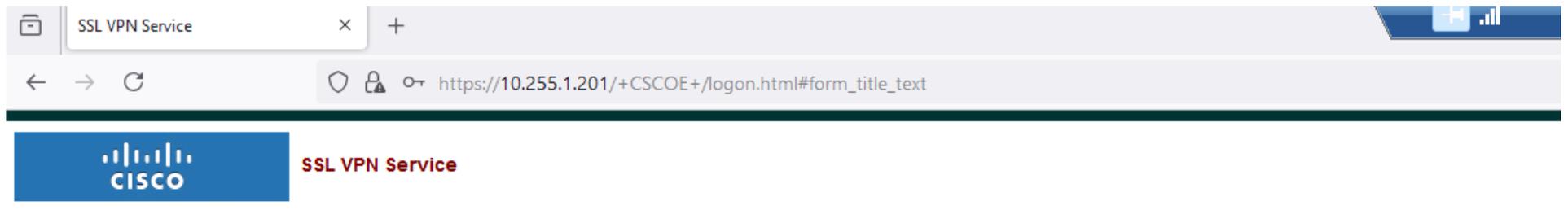
## Add the User to the right vpn policy group and connection profile group

The screenshot shows the 'Edit User Account' window with the following settings:

- Identity:** VPN Policy (checked)
- Group Policy:**  Inherit, Sales-Group (checked)
- Tunneling Protocols:**  Inherit, Clientless SSL VPN, SSL VPN Client, IPsec IKEv1, IPsec IKEv2, L2TP/IPsec
- Filter:**  Inherit
- Connection Profile (Tunnel Group) Lock:**  Inherit, Sales-Connection-Profile (checked)
- Store Password on Client System:**  Inherit, Yes, No (selected)
- Security Group Tag (SGT):**  Inherit, None, (2 - 65519)
- Connection Settings:**
  - Access Hours:**  Inherit
  - Simultaneous Logins:**  Inherit
  - Maximum Connect Time:**  Inherit, Unlimited, Minutes

Buttons on the right: Add, Edit (checked), Delete.

## Let's verify



 Login

Please enter your username and password.

USERNAME:

PASSWORD:



SSL VPN Service

Welcome to NPTC Sales Department, Sales Group policy is applied



https://10.255.1.201/+CSCOE+/portal.html



## SSL VPN Service



http://



Home



Web Applications



Browse Networks

Web Bookmarks

Server1



This server is a web server

Server2



This Server is a file Server

