Implementing the Cisco Adaptive Security Appliance (ASA)

IOS Firewall Solution

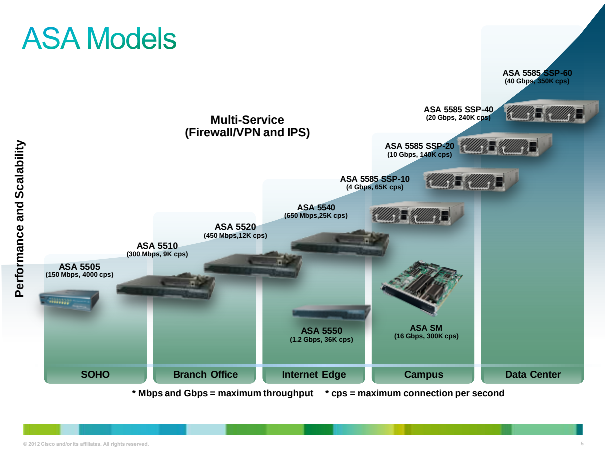
- An IOS router firewall solution is appropriate for small branch deployments and for administrators who are experienced with Cisco IOS.
- However, an IOS firewall solution does not scale well and typically cannot meet the needs of a large enterprise.

ASA 5500 Firewall Solution

- The ASA 5500 firewall appliance is a multi-service standalone appliance that is a primary component of the Cisco SecureX architecture.
- ASA 5500 appliances incorporate:
  - Proven firewall technology.
  - High-performance VPNs and always-on remote-access.
  - Comprehensive, highly effective intrusion prevention system (IPS) with Cisco Global Correlation and guaranteed coverage.
  - Failover feature for fault tolerance.

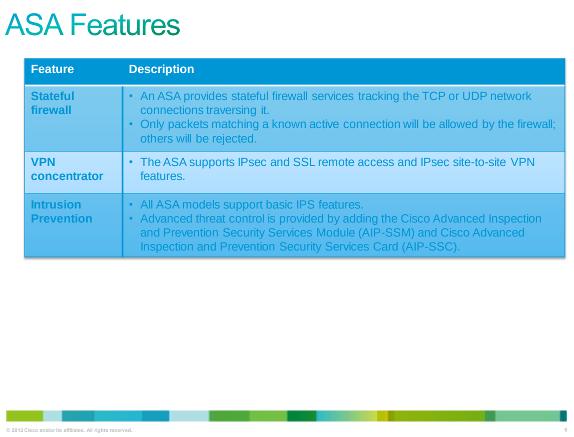
ASA Models

- Cisco ASA devices scale to meet a range of requirements and network sizes.
- There are six ASA models, ranging from the basic 5505 branch office model to the 5585 data center version.
  - All provide advanced stateful firewall features and VPN functionality.
- The biggest difference between models is the:
  - Maximum traffic throughput handled by the device.
  - The types and the number of interfaces on the device.
- The choice of ASA model will depend on an organization's requirements, such as:
  - Maximum throughput
  - Maximum connections per second
  - Available budget



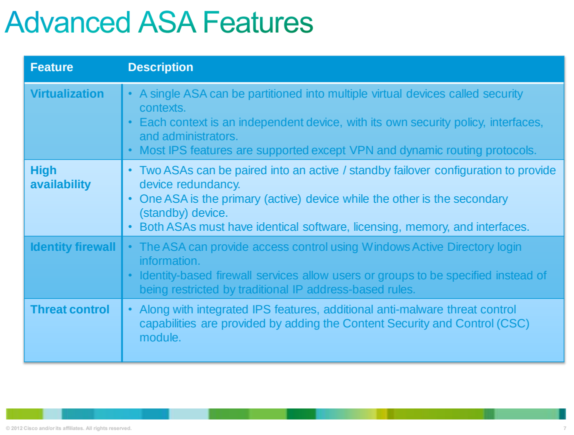
ASA Models

* Mbps and Gbps = maximum throughput   * cps = maximum connection per second



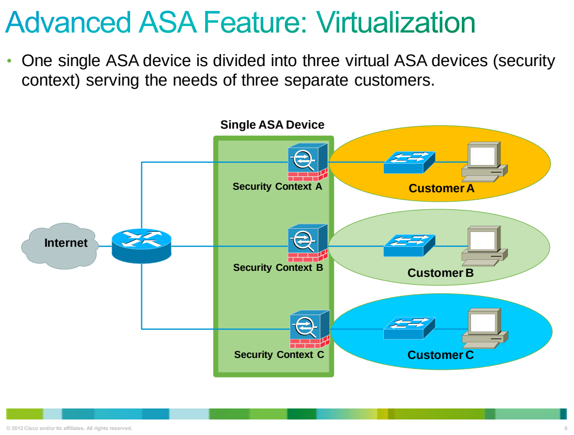
ASA Features

Feature	Description
Stateful firewall	• An ASA provides stateful firewall services tracking the TCP or UDP network connections traversing it. • Only packets matching a known active connection will be allowed by the firewall; others will be rejected.
VPN concentrator	• The ASA supports IPsec and SSL remote access and IPsec site-to-site VPN features.
Intrusion Prevention	• All ASA models support basic IPS features. • Advanced threat control is provided by adding the Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM) and Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC).



Advanced ASA Features

Feature	Description
Virtualization	• A single ASA can be partitioned into multiple virtual devices called security contexts. • Each context is an independent device, with its own security policy, interfaces, and administrators. • Most IPS features are supported except VPN and dynamic routing protocols.
High availability	• Two ASAs can be paired into an active / standby failover configuration to provide device redundancy. • One ASA is the primary (active) device while the other is the secondary (standby) device. • Both ASAs must have identical software, licensing, memory, and interfaces.
Identity firewall	• The ASA can provide access control using Windows Active Directory login information. • Identity-based firewall services allow users or groups to be specified instead of being restricted by traditional IP address-based rules.
Threat control	• Along with integrated IPS features, additional anti-malware threat control capabilities are provided by adding the Content Security and Control (CSC) module.

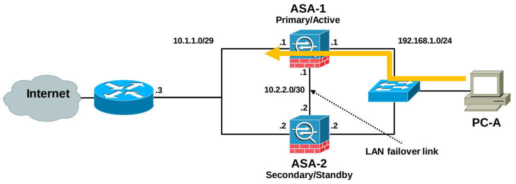


Advanced ASA Feature: Virtualization

- One single ASA device is divided into three virtual ASA devices (security context) serving the needs of three separate customers.

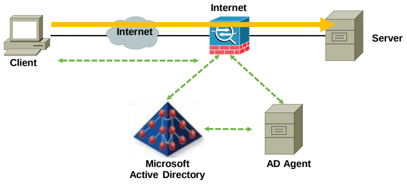
Advanced ASA Feature: High Availability

- Traffic leaving PC-A takes the preferred path using ASA-1.
- ASA-1 and ASA-2 are identical ASA devices configured for failover and each device monitors the other device over the LAN failover link.
- If ASA-2 detects that ASA-1 has failed, then ASA-2 would become the Primary/Active firewall gateway and traffic from PC-A would take the preferred path using ASA-2.



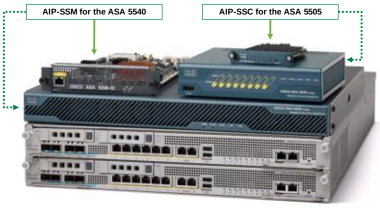
Advanced ASA Feature: Identity Firewall

- A Client attempting to access Server resources must first be authenticated using the Microsoft Active Directory.



Advanced ASA Feature: Identity Firewall

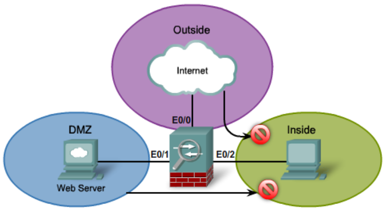
- Full IPS features are provided by integrating special hardware modules with the ASA architecture.
  - The Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM) is for the ASA 5540 device.
  - The Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC) is for the ASA 5505 device.



Networks on a Firewall

- Inside network
  - Network that is protected and behind the firewall.
- DMZ
  - Demilitarized zone, while protected by the firewall, limited access is allowed to outside users.
- Outside network
  - Network that is outside the protection of the firewall.

Networks on a Firewall



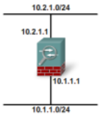
- Traffic originating from the Outside network going to the Inside network is denied.
- Traffic originating from the DMZ network going to the Inside network is denied.

Routed vs. Transparent Mode

- An ASA device can operate in one of two modes:

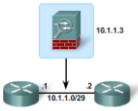
Routed Mode

- Is the traditional firewall deployment mode.
- Separates two Layer 3 domains.
- Provides a NAT boundary.
- Applies policy to flows as they transit the firewall.



Transparent Mode

- Operates at Layer 2.
- Integrates with existing networks without the need for re-addressing.
- Simplifies internal firewalling and network segmentation.

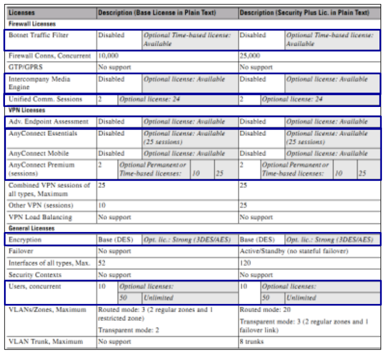


- NOTE:
  - The focus of this chapter is on Routed Mode.

ASA Licenses

- ASA appliances come pre-installed with either a:
  - Base license
  - Security Plus license
- Additional time-based and optional licenses can be purchased.
- Combining additional licenses to the pre-installed licenses creates a permanent license.
  - The permanent license is activated by installing a permanent activation key using the **`activation-key`** command.
  - Only one permanent license key can be installed and once it is installed, it is referred to as the running license.
- To verify the license information on an ASA device, use the commands:
  - **`show version`**
  - **`show activation-key`**

ASA 5505 Base License



Licenses	Description (Base License in Plain Text)		Description (Security Plus Lic. in Plain Text)	
Firewall Licenses				
Botnet Traffic Filter	Disabled	*Optional Time-based license: Available*	Disabled	*Optional Time-based license: Available*
Firewall Conns, Concurrent	10,000		25,000	
GTP/GPRS	No support		No support	
Intercompany Media Engine	Disabled	*Optional license: Available*	Disabled	*Optional license: Available*
Unified Comm. Sessions	2	*Optional license: 24*	2	*Optional license: 24*
VPN Licenses				
Adv. Endpoint Assessment	Disabled	*Optional license: Available*	Disabled	*Optional license: Available*
AnyConnect Essentials	Disabled	*Optional license: Available (25 sessions)*	Disabled	*Optional license: Available (25 sessions)*
AnyConnect Mobile	Disabled	*Optional license: Available*	Disabled	*Optional license: Available*
AnyConnect Premium (sessions)	2	*Optional Permanent or Time-based licenses:* *10* *25*	2	*Optional Permanent or Time-based licenses:* *10* *25*
Combined VPN sessions of all types, Maximum	25		25	
Other VPN (sessions)	10		25	
VPN Load Balancing	No support		No support	
General Licenses				
Encryption	Base (DES)	*Opt. lic.: Strong (3DES/AES)*	Base (DES)	*Opt. lic.: Strong (3DES/AES)*
Failover	No support		Active/Standby (no stateful failover)	
Interfaces of all types, Max.	52		120	
Security Contexts	No support		No support	
Users, concurrent	10	*Optional licenses:* *50* *Unlimited*	10	*Optional licenses:* *50* *Unlimited*
VLANs/Zones, Maximum	Routed mode: 3 (2 regular zones and 1 restricted zone) Transparent mode: 2		Routed mode: 20 Transparent mode: 3 (2 regular zones and 1 failover link)	
VLAN Trunk, Maximum	No support		8 trunks	

ASA 5505 Base License

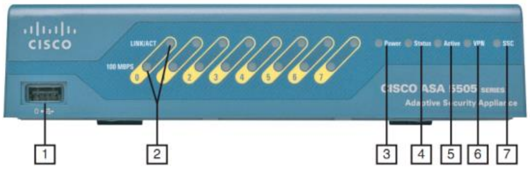
```
ciscoasa# show version

<Output omitted>

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 3              DMZ Restricted
Dual ISPs                         : Disabled       perpetual
VLAN Trunk Ports                  : 0              perpetual
Inside Hosts                      : 10             perpetual
Failover                          : Disabled       perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 10             perpetual
Total VPN Peers                   : 25             perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

Serial Number: JMX15364077
Running Permanent Activation Key: 0x970bc671 0x305fc569 0x70d21158 0xb6ec2ca8 0x8a003fb9
Configuration register is 0x41 (will be 0x1 at next reload)
Configuration last modified by enable_15 at 10:03:12.749 UTC Fri Sep 23 2011
ciscoasa#
```

Basic ASA Configuration

ASA 5505

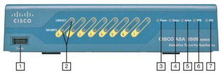
- The Cisco ASA 5505 is a full-featured security appliance for small businesses, branch offices, and enterprise teleworker environments.
- It delivers a high-performance firewall, SSL VPN, IPsec VPN, and rich networking services in a modular, plug-and-play appliance.

ASA 5505 Front Panel



1	USB 2.0 interface	5	Active LED
2	Speed and Link Activity LEDs	6	VPN LED
3	Power LED	7	Security Service Card (SSC) LED
4	Status LED		

ASA 5505 Front Panel



2 Speed and link activity LEDs

- Solid green speed indicator LED indicates 100 Mb/s; no LED indicates 10 Mb/s.
- Green link activity indicator LED indicates that a network link is established.
- Blinking link activity indicator indicates network activity.

4 Status LED

- Flashing green indicates that the system is booting and performing POST.
- Solid green indicates that the system tests passed and the system is operational.
- Amber solid indicates that the system tests failed.

5 Active LED

- Solid green LED indicates that this Cisco ASA is configured for failover.

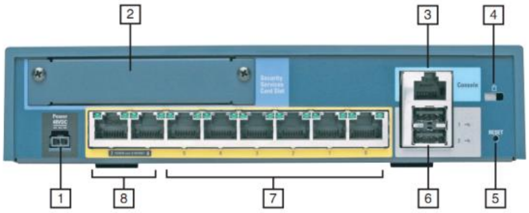
6 VPN LED

- Solid green indicates that one or more VPN tunnels are active.

7 Security Services Card (SSC) LED

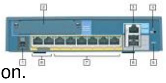
- Solid green indicates that an SSC card is present in the SSC slot.

ASA 5505 Back Panel



1	Power connector (48 VDC)	5	Reset button
2	SSC slot	6	Two USB 2.0 ports
3	Serial console port	7	10/100 Ethernet switch (ports 0 – 5)
4	Lock slot	8	10/100 Power over Ethernet (PoE) switch ports (ports 6 and 7)

ASA 5505 Back Panel



2 One Security Service Card (SSC) slot for expansion.

- The slot can be used to add the Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC) to provide intrusion prevention services.

6 USB ports (front and back) can be used to enable additional services and capabilities.

7 Consists of an 8-port 10/100 Fast Ethernet switch.

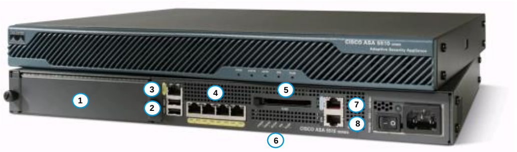
- Each port can be dynamically grouped to create up to three separate VLANs or zones to support network segmentation and security.

8 Ports 6 and 7 are Power over Ethernet (PoE) ports to simplify the deployment of Cisco IP phones and external wireless access points.

NOTE:

- The default DRAM memory is 256 MB (upgradable to 512 MB) and the default internal flash memory is 128 MB for the Cisco ASA 5505.

ASA 5510 Back Panel

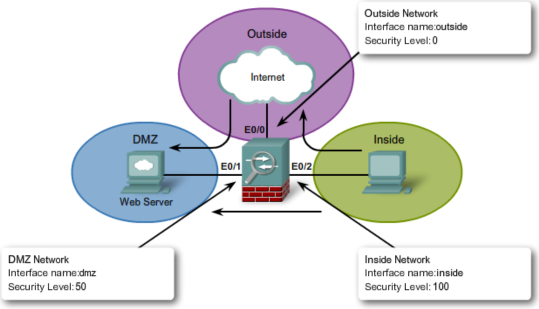


1	Security Services Module (SSM) slot	5	Flash card slot
2	Two USB 2.0 ports	6	Power, status, active, VPN, and flash LED indicators
3	Out of band (OOB) management interface	7	Serial console port
4	4 Fast Ethernet interfaces		Auxiliary port

Security Levels

- The ASA assigns security levels to distinguish between inside and outside networks.
- Security levels define the level of trustworthiness of an interface.
  - The higher the level, the more trusted the interface.
  - Security levels range between 0 (untrustworthy) to 100 (very trustworthy).
- Each operational interface must have:
  - A name.
  - A security level from 0 (lowest) to 100 (highest) assigned.
  - An IP address (routed mode).

Security Levels



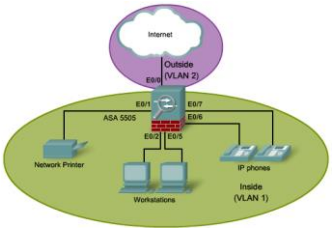
Outside Network
Interface name:outside
Security Level:0

DMZ Network
Interface name:dmz
Security Level:50

Inside Network
Interface name:inside
Security Level:100

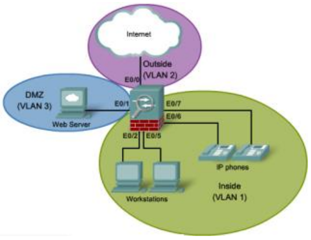
ASA 5505 Deployment - Small Branch

- In a small branch deployment, a common deployment would include:
  - An inside network (VLAN 1) with security level 100.
  - An outside network (VLAN 2) with security level 0.



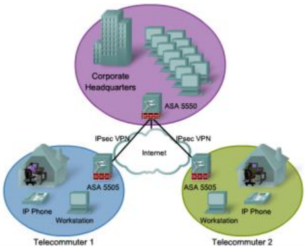
ASA 5505 Deployment - Small Business

- In a small business, the ASA 5505 can be deployed with two different protected network segments:
  - The inside network (VLAN 1) to connect workstations and IP phones.
  - The outside interface (VLAN 2) is used to connect to the Internet.
  - The DMZ (VLAN 3) to connect a company web server.



ASA 5505 Deployment - Enterprise

- In an enterprise deployment, the ASA 5505 can be used by telecommuters and home users to connect to a centralized location using a VPN.



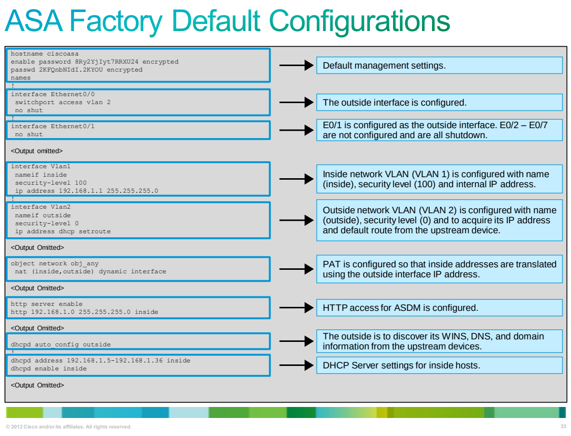
Configure Basic Settings

ASA Command Line Interface (CLI)

- The ASA CLI is a proprietary OS which has a similar look and feel to the router IOS.
- Like a Cisco IOS router, the ASA recognizes the following:
  - Abbreviation of commands and keywords.
  - Using the Tab key to complete a partial command.
  - Using the help key (?) after a command to view additional syntax.
- Unlike an ISR, the ASA:
  - Can execute any ASA CLI command regardless of the current configuration mode prompt and does not require or recognize the **`do`** IOS CLI command.
  - Can provide additional help listing a brief command description and syntax by using the EXEC command **`help`** followed by the CLI command. (e.g., **`help reload`**)
  - Interrupts **`show`** command output by simply using the letter **`Q`**. (Unlike the **Ctrl+C** (**^C**) IOS CLI key sequence.)

Common IOS and Equivalent Commands

IOS Router Command	Equivalent ASA Command
enable secret *password*	**enable password** *password*
line con 0 **password** *password* **login**	**passwd** *password*
ip route	**route outside**
show ip interfaces brief	**show interface ip brief**
show ip route	**show route**
show vlan	**show switch vlan**
show ip nat translations	**show xlate**
copy running-config startup-config	**write** [**memory**]
erase startup-config	**write erase**



ASA Factory Default Configurations

```
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
```

Default management settings.

```
!
interface Ethernet0/0
 switchport access vlan 2
 no shut
```

The outside interface is configured.

```
!
interface Ethernet0/1
 no shut
```

E0/1 is configured as the outside interface. E0/2 – E0/7 are not configured and are all shutdown.

<Output omitted>

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

Inside network VLAN (VLAN 1) is configured with name (inside), security level (100) and internal IP address.

```
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
```

Outside network VLAN (VLAN 2) is configured with name (outside), security level (0) and to acquire its IP address and default route from the upstream device.

<Output Omitted>

```
object network obj_any
 nat (inside,outside) dynamic interface
```

PAT is configured so that inside addresses are translated using the outside interface IP address.

<Output Omitted>

```
http server enable
http 192.168.1.0 255.255.255.0 inside
```

HTTP access for ASDM is configured.

<Output Omitted>

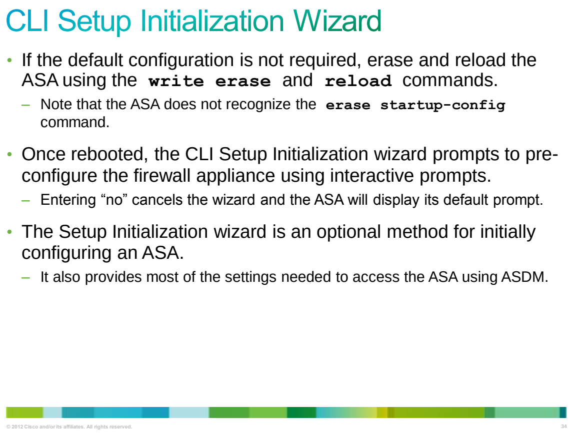
```
dhcpd auto_config outside
```

The outside is to discover its WINS, DNS, and domain information from the upstream devices.

```
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
```

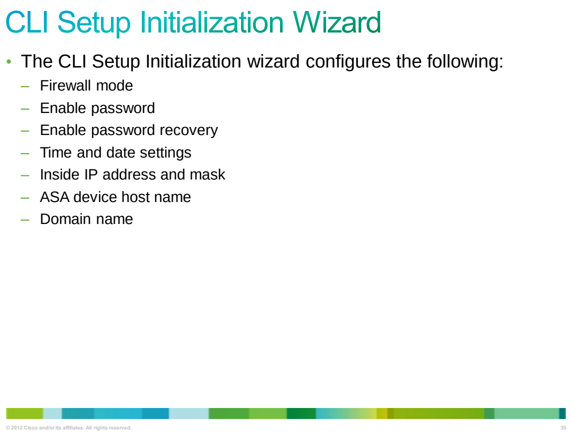
DHCP Server settings for inside hosts.

<Output Omitted>



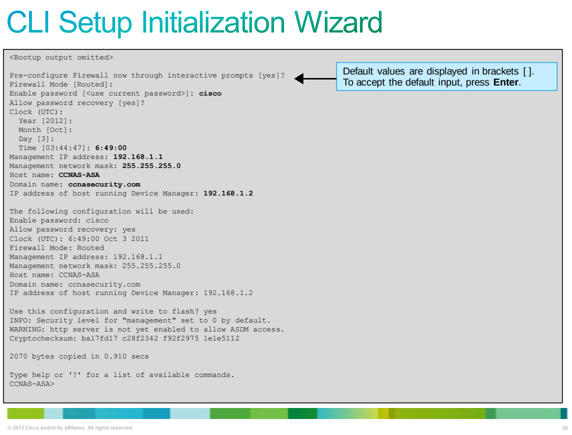
CLI Setup Initialization Wizard

- If the default configuration is not required, erase and reload the ASA using the **`write erase`** and **`reload`** commands.
  - Note that the ASA does not recognize the **`erase startup-config`** command.
- Once rebooted, the CLI Setup Initialization wizard prompts to pre-configure the firewall appliance using interactive prompts.
  - Entering “no” cancels the wizard and the ASA will display its default prompt.
- The Setup Initialization wizard is an optional method for initially configuring an ASA.
  - It also provides most of the settings needed to access the ASA using ASDM.



CLI Setup Initialization Wizard

- The CLI Setup Initialization wizard configures the following:
  - Firewall mode
  - Enable password
  - Enable password recovery
  - Time and date settings
  - Inside IP address and mask
  - ASA device host name
  - Domain name



CLI Setup Initialization Wizard

```
<Bootup output omitted>

Pre-configure Firewall now through interactive prompts [yes]?
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2012]:
  Month [Oct]:
  Day [3]:
  Time [03:44:47]: 6:49:00
Management IP address: 192.168.1.1
Management network mask: 255.255.255.0
Host name: CCNAS-ASA
Domain name: ccnasecurity.com
IP address of host running Device Manager: 192.168.1.2

The following configuration will be used:
Enable password: cisco
Allow password recovery: yes
Clock (UTC): 6:49:00 Oct 3 2011
Firewall Mode: Routed
Management IP address: 192.168.1.1
Management network mask: 255.255.255.0
Host name: CCNAS-ASA
Domain name: ccnasecurity.com
IP address of host running Device Manager: 192.168.1.2

Use this configuration and write to flash? yes
INFO: Security level for "management" set to 0 by default.
WARNING: http server is not yet enabled to allow ASDM access.
Cryptochecksum: ba17fd17 c28f2342 f92f2975 1e1e5112

2070 bytes copied in 0.910 secs

Type help or '?' for a list of available commands.
CCNAS-ASA>
```

Default values are displayed in brackets [ ].
To accept the default input, press **Enter**.

Configure Basic Settings

- Basic management settings are configured in global configuration mode.

NOTE:

- The first time global configuration mode is accessed, a message prompting you to enable the Smart Call Home feature appears.
  - This feature offers proactive diagnostics and real-time alerts on select Cisco devices, which provides higher network availability and increased operational efficiency.
  - To participate, a CCO ID is required and the ASA device must be registered under a Cisco SMARTnet Service contract.

Steps to Configure Basic Settings

1. Configure basic management settings.
   - (i.e., hostname, domain name, and enable password.)
2. Enable the master passphrase.
3. Configure the Inside and Outside SVIs (on an ASA 5505).
4. Assign Layer 2 ports to VLANs (on an ASA 5505).
5. Enable Telnet, SSH, and HTTPS access.
6. Configure time services.
7. Configure a default route.

1 - Configure Basic Management Settings

- In global configuration mode, configure the ASA host name, domain name, and privileged EXEC mode password using the following commands:
  - **hostname** *name* - Changes the name of the ASA.
  - **domain-name** *name* - Changes the domain name.
  - **enable password** *password* - Configures the privileged EXEC mode password.
    - Note that there is no secret option.
  - **passwd** *password* - Configures the Telnet / SSH password.

```
ciscoasa# conf t
ciscoasa(config)# hostname CCNAS-ASA
CCNAS-ASA(config)# domain-name ccnasecurity.com
CCNAS-ASA(config)# enable password class
CCNAS-ASA(config)# passwd cisco
CCNAS-ASA(config)#
```

2 - Enable the Master Passphrase

- A master passphrase securely stores plaintext passwords in encrypted format.
  - Similar to the IOS **service password-encryption** command.
- To configure a master passphrase, use the following commands:
  - **key config-key password-encryption** [*new-passphrase* [*old-passphrase*]]
    - Creates or changes an existing master passphrase (8 to 128 characters in length).
  - **password encryption aes**
    - Enables password encryption.

```
CCNAS-ASA(config)# key config-key password-encryption cisco123
CCNAS-ASA(config)# password encryption aes
CCNAS-ASA(config)#
```

3 - Configure Inside and Outside SVIs

- On ASA 5510 and higher, routed interfaces are configured with IP configurations.
- However, the ASA 5505 has an integrated 8 port Layer 2 switch and therefore IP configurations are accomplished by:
  - Configuring the inside and outside switched virtual interfaces (SVIs) by assigning interface names, security level, and IP address.
  - Assigning Layer 2 ports to the inside and outside SVI VLANs.

NOTE:

- Optionally, a third SVI (DMZ) could also be configured if required.
- However, ASA 5505 with a Base License can only support a limited SVI.

3 - Configure Inside and Outside SVIs

- Use the following commands to configure the inside and outside SVI VLAN interfaces:
  - **interface vlan** *vlan-number* - Creates a switch virtual interface (SVI).
  - **nameif** {**inside** | **outside** | *name*} - Assigns an interface name.
  - **security-level** *value* - Assigns a security level to the SVI interface.
    - By default, the inside interface is assigned 100 and the outside interface is 0.
  - **ip address** *ip-address netmask* – Manually configure an IP address.

```
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# security-level 0
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
```

3 - Configure Inside and Outside SVIs

- Optionally, instead of manually configuring an IP address, the interface could also be configured as a:
  - DHCP client using the **ip address dhcp** [**setroute**] command.
  - PPPoE client using the **ip address pppoe** [**setroute**] command.

NOTE:

- An ASA can also be configured as a DHCP server which is covered later.

3 - Configure Inside and Outside SVIs

- An ASA 5505 with the Security Plus License automatically supports the creation of additional VLANs to create other zones such as a DMZ zone.
- However, an ASA 5505 with a Basic License only supports a third “restricted" SVI.
  - This SVI is limited from initiating contact to another specified VLAN.
- The following command must be configured to support the third restricted VLAN SVI on an ASA 5505 with a Base License:
  - **no forward interface vlan** *vlan-id*
    - *vlan-id* specifies the VLAN to which this interface cannot initiate traffic.
  - Configure this command only once the inside and outside VLAN interfaces are configured.
- The new SVI must also be named, assigned a security level value, and IP address.

4 - Assign Layer 2 ports to VLANs

- The Layer 2 ports must be assigned to a VLAN.
  - By default, all ports are members of VLAN 1.
- Use the following commands to change the VLAN assignment:
  - **`interface`** *`interface number`* – Enter interface configuration mode.
  - **`switchport access vlan`** *`vlan-id`* – Change the VLAN assignment.
  - **`no shutdown`** – Enable the physical interface.
- To verify VLAN settings, use the **`show switch vlan`** command.

```
CCNAS-ASA(config-if)# interface e0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
```

Verify SVI and Interface Settings

```
CCNAS-ASA# show switch vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------------------------
1    inside                           up        Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          up        Et0/0
CCNAS-ASA#
CCNAS-ASA# show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES unset  up                    up
Ethernet0/1                unassigned      YES unset  up                    up
Ethernet0/2                unassigned      YES unset  administratively down up
Ethernet0/3                unassigned      YES unset  administratively down up
Ethernet0/4                unassigned      YES unset  administratively down down
Ethernet0/5                unassigned      YES unset  administratively down down
Ethernet0/6                unassigned      YES unset  administratively down down
Ethernet0/7                unassigned      YES unset  administratively down down
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Vlan1                      192.168.1.1     YES manual up                    up
Vlan2                      209.156.200.226 YES manual up                    up
Virtual0                   127.0.0.1       YES unset  up                    up
CCNAS-ASA#
```

5 - Enable Telnet, SSH, and HTTPS Access

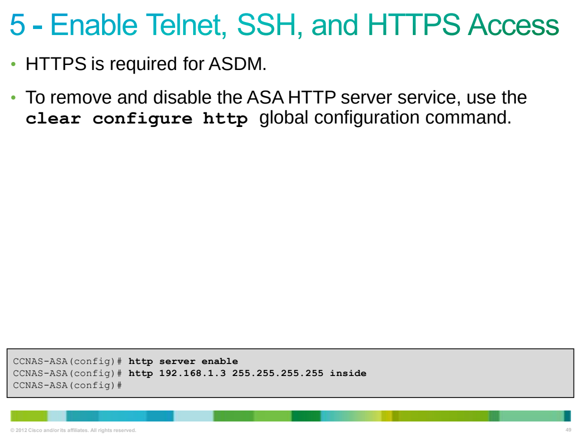
- Enable Telnet access (if required).
  - SSH is recommended instead of Telnet.
- Although simple authentication is provided using the **`passwd`** command, securing Telnet access using AAA authentication and the local database is recommended.
- Use the following commands to enable AAA authentication:
  - **`username`** *`name`* **`password`** *`password`*
  - **`aaa authentication`** {**`telnet`** | **`ssh`**} **`console`** {**`LOCAL`** | *`TACACS-server`* | *`RADIUS-server`*}
  - **`telnet`** *`host-ip host-mask`* **`inside`**
  - **`telnet timeout`** *`minutes`*

```
CCNAS-ASA(config)# username admin password class
CCNAS-ASA(config)# aaa authentication telnet console LOCAL
CCNAS-ASA(config)# telnet 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# telnet timeout 10
CCNAS-ASA(config)#
```

5 - Enable Telnet, SSH, and HTTPS Access

- Similarly configured as Telnet but requires:
  - AAA authentication to be enabled
  - RSA crypto key generated
- To verify the SSH configuration, use the **`show ssh`** command.

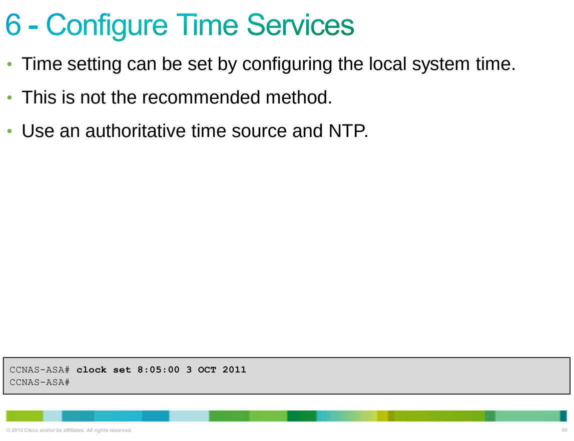
```
CCNAS-ASA(config)# username admin password class
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
CCNAS-ASA(config)# ssh 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# ssh timeout 10
CCNAS-ASA(config)# exit
CCNAS-ASA#
CCNAS-ASA# show ssh
Timeout: 5 minutes
Versions allowed: 1 and 2
192.168.1.3 255.255.255.255 inside
CCNAS-ASA#
```



5 - Enable Telnet, SSH, and HTTPS Access

- HTTPS is required for ASDM.
- To remove and disable the ASA HTTP server service, use the **`clear configure http`** global configuration command.

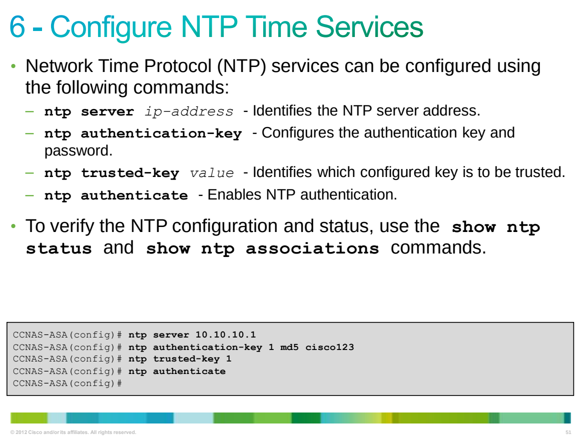
```
CCNAS-ASA(config)# http server enable
CCNAS-ASA(config)# http 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)#
```



6 - Configure Time Services

- Time setting can be set by configuring the local system time.
- This is not the recommended method.
- Use an authoritative time source and NTP.

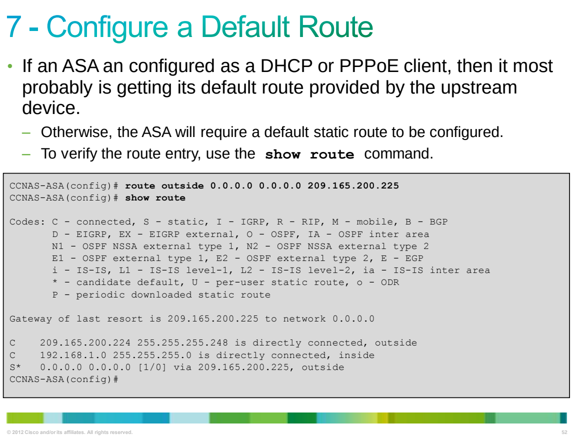
```
CCNAS-ASA# clock set 8:05:00 3 OCT 2011
CCNAS-ASA#
```



6 - Configure NTP Time Services

- Network Time Protocol (NTP) services can be configured using the following commands:
  - **`ntp server`** *`ip-address`* - Identifies the NTP server address.
  - **`ntp authentication-key`** - Configures the authentication key and password.
  - **`ntp trusted-key`** *`value`* - Identifies which configured key is to be trusted.
  - **`ntp authenticate`** - Enables NTP authentication.
- To verify the NTP configuration and status, use the **`show ntp status`** and **`show ntp associations`** commands.

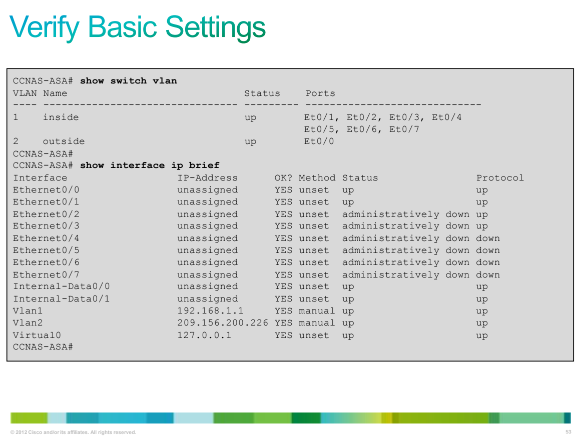
```
CCNAS-ASA(config)# ntp server 10.10.10.1
CCNAS-ASA(config)# ntp authentication-key 1 md5 cisco123
CCNAS-ASA(config)# ntp trusted-key 1
CCNAS-ASA(config)# ntp authenticate
CCNAS-ASA(config)#
```



7 - Configure a Default Route

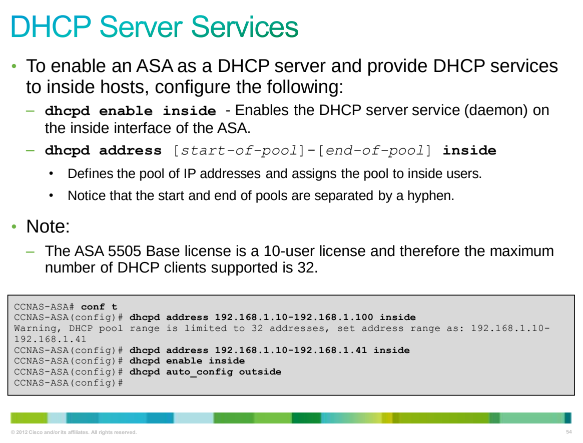
- If an ASA an configured as a DHCP or PPPoE client, then it most probably is getting its default route provided by the upstream device.
  - Otherwise, the ASA will require a default static route to be configured.
  - To verify the route entry, use the **`show route`** command.

```
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNAS-ASA(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

C    209.165.200.224 255.255.255.248 is directly connected, outside
C    192.168.1.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 209.165.200.225, outside
CCNAS-ASA(config)#
```



Verify Basic Settings

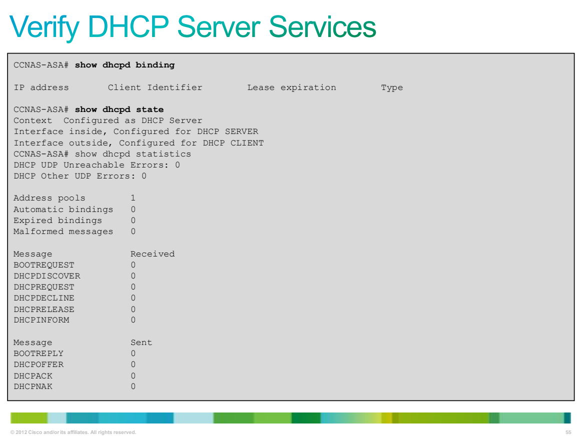
```
CCNAS-ASA# show switch vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------------------------
1    inside                           up        Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          up        Et0/0
CCNAS-ASA#
CCNAS-ASA# show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES unset  up                    up
Ethernet0/1                unassigned      YES unset  up                    up
Ethernet0/2                unassigned      YES unset  administratively down up
Ethernet0/3                unassigned      YES unset  administratively down up
Ethernet0/4                unassigned      YES unset  administratively down down
Ethernet0/5                unassigned      YES unset  administratively down down
Ethernet0/6                unassigned      YES unset  administratively down down
Ethernet0/7                unassigned      YES unset  administratively down down
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Vlan1                      192.168.1.1     YES manual up                    up
Vlan2                      209.156.200.226 YES manual up                    up
Virtual0                   127.0.0.1       YES unset  up                    up
CCNAS-ASA#
```



DHCP Server Services

- To enable an ASA as a DHCP server and provide DHCP services to inside hosts, configure the following:
  - **`dhcpd enable inside`** - Enables the DHCP server service (daemon) on the inside interface of the ASA.
  - **`dhcpd address`** `[`*`start-of-pool`*`]-[`*`end-of-pool`*`]` **`inside`**
    - Defines the pool of IP addresses and assigns the pool to inside users.
    - Notice that the start and end of pools are separated by a hyphen.
- Note:
  - The ASA 5505 Base license is a 10-user license and therefore the maximum number of DHCP clients supported is 32.

```
CCNAS-ASA# conf t
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.100 inside
Warning, DHCP pool range is limited to 32 addresses, set address range as: 192.168.1.10-
192.168.1.41
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.41 inside
CCNAS-ASA(config)# dhcpd enable inside
CCNAS-ASA(config)# dhcpd auto_config outside
CCNAS-ASA(config)#
```



Verify DHCP Server Services

```
CCNAS-ASA# show dhcpd binding

IP address       Client Identifier        Lease expiration        Type

CCNAS-ASA# show dhcpd state
Context  Configured as DHCP Server
Interface inside, Configured for DHCP SERVER
Interface outside, Configured for DHCP CLIENT
CCNAS-ASA# show dhcpd statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   0
Expired bindings     0
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         0
DHCPREQUEST          0
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            0
DHCPACK              0
DHCPNAK              0
```

Introduction to ASDM

Cisco ASDM

- Cisco ASA Security Device Manager (ASDM) is a Java-based GUI tool that facilitates the setup, configuration, monitoring, and troubleshooting of Cisco ASAs.
- ASDM is now preloaded in flash memory on any ASA running versions 7.0 and later.
- ASDM can be:
  - Run as a Java Web Start application that is dynamically downloaded from the ASA flash allowing an administrator to configure and monitor that ASA device.
  - Downloaded from flash and installed locally on a host as an application allowing an administrator to manage multiple ASA devices.

Starting ASDM

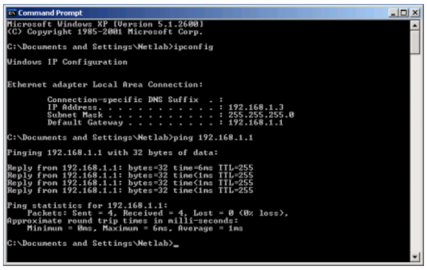
1. Verify connectivity to the ASA.
2. Open a browser and establish a HHTP connecting to the ASA.
3. Choose to:
   - Install ASDM Launcher and Run ASDM.
   - Run ASDM.
   - Run the Startup wizard.
4. Authenticate to ASDM.

NOTE:

- It is assumed that the ASA 5505 has been preconfigured with basic settings.

Starting ASDM

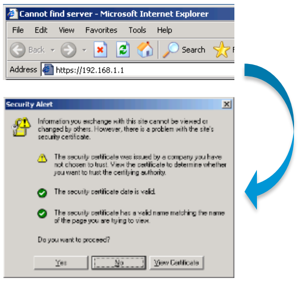
- Verify connectivity to the ASA.
  - You must be initiating the connecting from the identified trusted host in the HTTP basic settings.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Netlab>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Netlab>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=6ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\Documents and Settings\Netlab>_
```

Starting ASDM

- Open a browser and establish an SSL connection.
  - Click **Yes** to continue and open the ASDM Launch window.



https://192.168.1.1

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

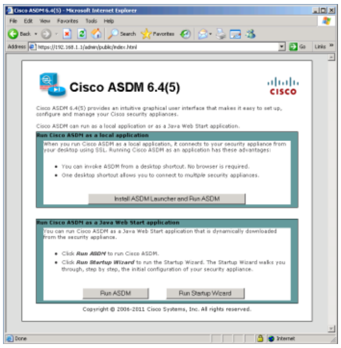
The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Starting ASDM

- **Install ASDM Launcher and Run ASDM:**
  - Install ASDM locally on the host.
  - The advantage is that ASDM can be used to manage several ASA devices.
- **Run ASDM:**
  - Run ASDM as a Java Web start application.
  - The advantage is that ASDM is not locally installed.
  - An Internet browser is required.
- **Run Startup Wizard:**
  - This choice is similar to the Setup Initialization wizard and provides step-by-step windows to help initially configure the ASA.


Cisco ASDM 6.4(5) - Microsoft Internet Explorer

Address: https://192.168.1.1/admin/public/index.html

Cisco ASDM 6.4(5)

Cisco ASDM 6.4(5) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

Run Cisco ASDM as a local application

When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

Install ASDM Launcher and Run ASDM

Run Cisco ASDM as a Java Web Start application

You can run Cisco ASDM as a Java Web Start application that is dynamically downloaded from the security appliance.

- Click ***Run ASDM*** to run Cisco ASDM.
- Click ***Run Startup Wizard*** to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

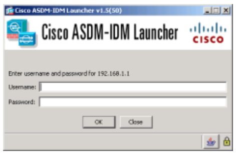
Run ASDM   Run Startup Wizard

Copyright © 2006-2011 Cisco Systems, Inc. All rights reserved.

Done   Internet

Starting ASDM

- After choosing **Run ASDM**, authenticate with the ASA.
  - When authentication is successful, the ASDM Home page will be displayed.


Cisco ASDM-IDM Launcher v1.5(50)

Cisco ASDM-IDM Launcher

Enter username and password for 192.168.1.1

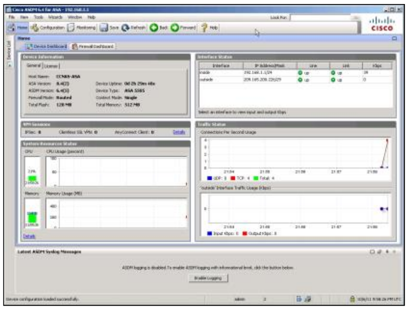
Username:

Password:

OK   Close

ASDM Device Dashboard

- The Cisco ASDM Home page displays provides a quick view of the operational status of ASA that is updated every 10 seconds.


File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device Dashboard
Firewall Dashboard
Device Information
Interface Status
VPN Sessions
Traffic Status
System Resources Status
Connections Per Second Usage
UDP: 0 TCP: 4 Total: 4
'outside' Interface Traffic Usage (Kbps)
Input Kbps: 0 Output Kbps: 0
CPU Usage (percent)
Memory Usage (MB)
Latest ASDM Syslog Messages

Host Name: CCNAS-ASA
ASA Version: 8.4(2)
ASDM Version: 6.4(5)
Firewall Mode: Routed
Total Flash: 128 MB
Device Uptime: 0d 2h 25m 48s
Device Type: ASA 5505
Context Mode: Single
Total Memory: 512 MB

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.1/24	up	up	0
outside	209.165.200.226/29	up	up	0

Select an interface to view input and output Kbps

IPSec: 0   Clientless SSL VPN: 0   AnyConnect Client: 0   Details

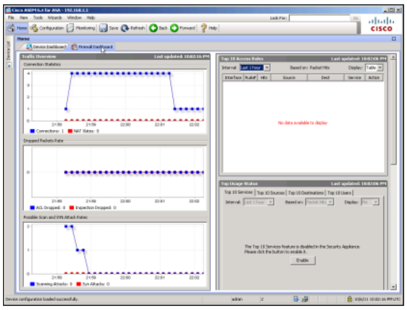
ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

Enable Logging

Device configuration loaded successfully.

ASDM Firewall Dashboard

- The Firewall Dashboard provides security related information about traffic that passes through the ASA.


File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device Dashboard
Firewall Dashboard
Traffic Overview
Connection Statistics
Connections: 1 NAT Xlates: 0
Dropped Packets Rate
ACL Dropped: 0 Inspection Dropped: 0
Possible Scan and SYN Attack Rates
Scanning Attacks: 0 Syn Attacks: 0
Top 10 Access Rules
Top Usage Status
Top 10 Services
Top 10 Sources
Top 10 Destinations
Top 10 Users

Interval: Last 1 hour   Based on: Packet Hits   Display: Table

Interface	Rule#	Hits	Source	Dest	Service	Action

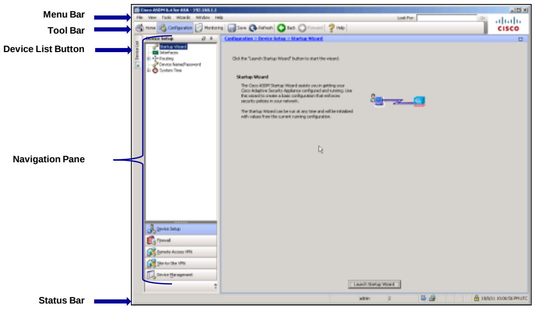
No data available to display

The Top 10 Services feature is disabled in the Security Appliance. Please click the button to enable it.

Enable

Device configuration loaded successfully.

ASDM Configuration View



Menu Bar

Tool Bar

Device List Button

Navigation Pane

Status Bar

Cisco ASDM 6.4 for ASA - 192.168.1.1

Configuration > Device Setup > Startup Wizard

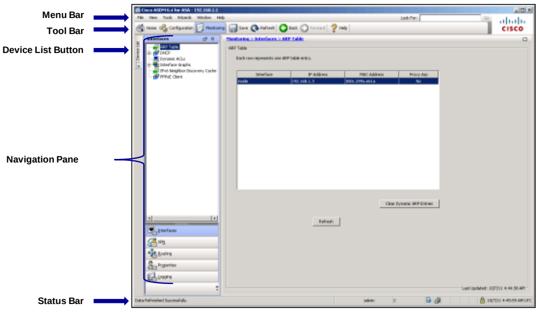
Click the "Launch Startup Wizard" button to start the wizard.

Startup Wizard

The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use the wizard to create a basic configuration that enforces security policies in your network.

The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.

ASDM Monitoring View



Menu Bar

Tool Bar

Device List Button

Navigation Pane

Status Bar

Cisco ASDM 6.4 for ASA - 192.168.1.1

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

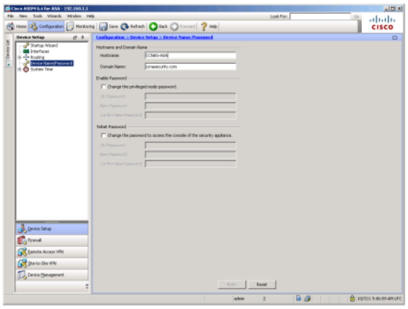
Interface	IP Address	MAC Address	Proxy Arp
inside	192.168.1.3	000c.29fa.e61a	No

Last Updated: 10/7/11 4:44:38 AM

Data Refreshed Successfully.

Configure Hostname and Passwords

- **Configuration** > **Device Setup** > **Device Name/Password**



Cisco ASDM 6.4 for ASA - 192.168.1.1

Configuration > Device Setup > Device Name/Password

Hostname and Domain Name

Hostname: CCNAS-ASA

Domain Name: ccnasecurity.com

Enable Password

☐ Change the privileged mode password.

Old Password:

New Password:

Confirm New Password:

Telnet Password

☐ Change the password to access the console of the security appliance.

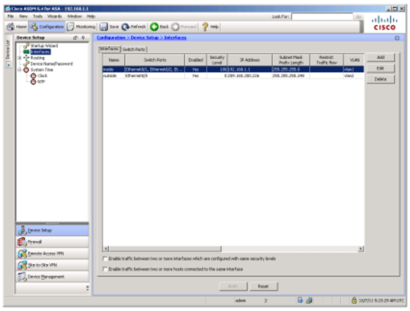
Old Password:

New Password:

Confirm New Password:

Interfaces

- **Configuration** > **Device Setup** > **Interfaces** > **Interfaces**



Cisco ASDM 6.4 for ASA - 192.168.1.1

Configuration > Device Setup > Interfaces

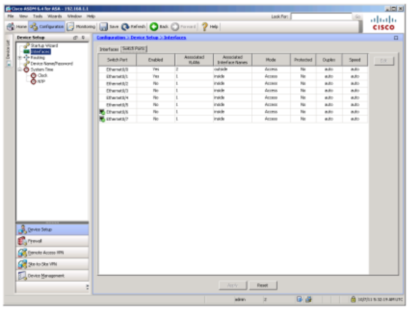
Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic Flow	VLAN
inside	Ethernet0/1, Ethernet0/2, E...	Yes	100	192.168.1.1	255.255.255.0		vlan1
outside	Ethernet0/0	Yes	0	209.165.200.226	255.255.255.248		vlan2

☐ 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

Layer 2 Switch Ports

- **Configuration** > **Device Setup** > **Interfaces** > **Switch Ports**

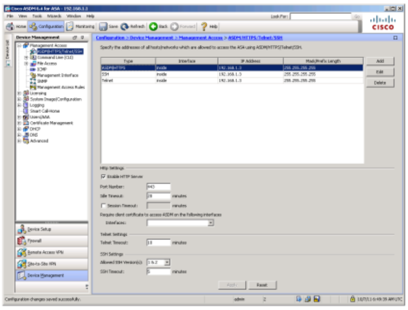


Configuration > Device Setup > Interfaces

Switch Port	Enabled	Associated VLANs	Associated Interface Names	Mode	Protected	Duplex	Speed
Ethernet0/0	Yes	2	outside	Access	No	auto	auto
Ethernet0/1	Yes	1	inside	Access	No	auto	auto
Ethernet0/2	No	1	inside	Access	No	auto	auto
Ethernet0/3	No	1	inside	Access	No	auto	auto
Ethernet0/4	No	1	inside	Access	No	auto	auto
Ethernet0/5	No	1	inside	Access	No	auto	auto
Ethernet0/6	No	1	inside	Access	No	auto	auto
Ethernet0/7	No	1	inside	Access	No	auto	auto

Configuring Telnet and SSH

- **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**



Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	inside	192.168.1.3	255.255.255.255
SSH	inside	192.168.1.3	255.255.255.255
Telnet	inside	192.168.1.3	255.255.255.255

Http Settings

☑ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 10 minutes

SSH Settings

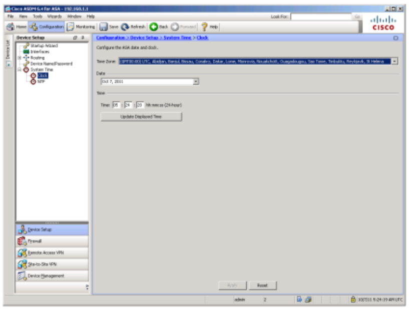
Allowed SSH Version(s): 1 & 2

SSH Timeout: 5 minutes

Configuration changes saved successfully.

System Time - Local Clock

- **Configuration** > **Device Setup** > **System Time > Clock**



Configuration > Device Setup > System Time > Clock

Configure the ASA date and clock.

Time Zone: (GMT00:00) UTC, Abidjan, Banjul, Bissau, Conakry, Dakar, Lome, Monrovia, Nouakchott, Ouagadougou, Sao Tome, Timbuktu, Reykjavik, St Helena

Date

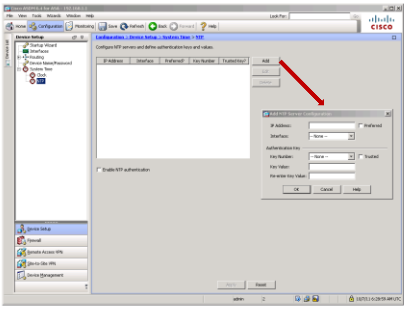
Oct 7, 2011

Time

Time: 05 : 24 : 20 hh:mm:ss (24-hour)

System Time - Configuring NTP

- **Configuration** > **Device Setup** > **System Time** > **NTP**



Configuration > Device Setup > System Time > NTP

Configure NTP servers and define authentication keys and values.

IP Address	Interface	Preferred?	Key Number	Trusted Key?

☐ Enable NTP authentication

Add NTP Server Configuration

IP Address: ☐ Preferred

Interface: -- None --

Authentication Key

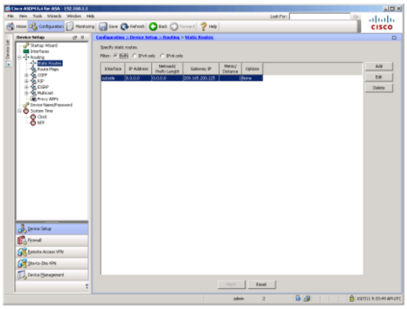
Key Number: -- None -- ☐ Trusted

Key Value:

Re-enter Key Value:

Default Static Route

- **Configuration** > **Device Setup** > **Routing** > **Static Routes**



Configuration > Device Setup > Routing > Static Routes

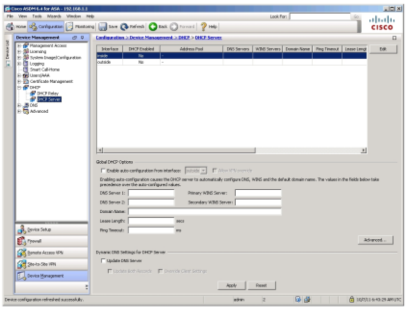
Specify static routes.

Filter: ● Both ○ IPv4 only ○ IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
outside	0.0.0.0	0.0.0.0	209.165.200.225	1	None

Configuring DHCP Server

- **Configuration** > **Device Management** > **DHCP** > **DHCP Server**



Configuration > Device Management > DHCP > DHCP Server

Interface	DHCP Enabled	Address Pool	DNS Servers	WINS Servers	Domain Name	Ping Timeout	Lease Length
inside	No	-					
outside	No	-					

Global DHCP Options

□ Enable auto-configuration from interface: outside □ Allow VPN override

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

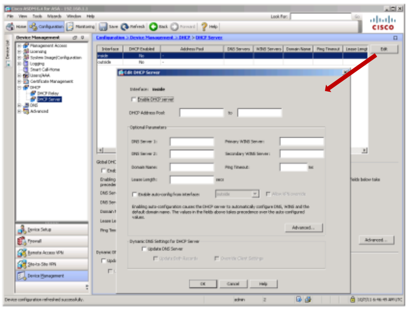
Dynamic DNS Settings for DHCP Server

□ Update DNS Server

Device configuration refreshed successfully.

Editing DHCP Server

- **Configuration** > **Device Management** > **DHCP** > **DHCP Server**



Edit DHCP Server

Interface: inside

□ Enable DHCP server

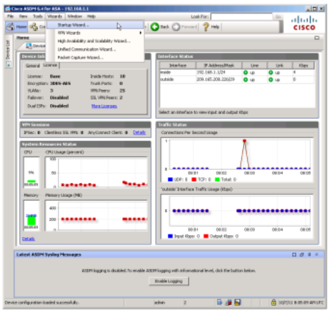
Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields above takes precedence over the auto-configured values.

Device configuration refreshed successfully.

ASDM Startup Wizard

ASDM Wizards

- ASDM has 5 wizards to choose from:
  - Startup Wizard
  - VPN Wizards
  - High-Availability and Scalability Wizard
  - Unified Communication Wizard
  - Packet Capture Wizard


Cisco ASDM 6.4 for ASA - 192.168.1.1
File
View
Tools
Wizards
Window
Help
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
Packet Capture Wizard...
Back
Forward
Help
CISCO

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

Enable Logging

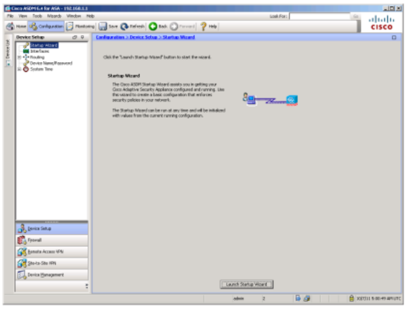
Device configuration loaded successfully.

ASDM Startup Wizard

- The Startup wizard is similar to the interactive Setup Initialization wizard and can be accessed:
  - When launching ASDM from a browser, choose **Run Startup Wizard**.
  - From the Tool bar, choose **Configuration** > **Device Setup** > **Startup Wizard**.
  - From the Menu bar, choose **Wizards** > **Startup Wizard**.

Configuration - Startup Wizard

- **Configuration** > **Device Setup** > **Startup Wizard**



Configuration > Device Setup > Startup Wizard

Click the "Launch Startup Wizard" button to start the wizard.

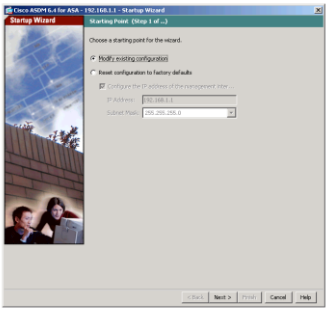
Startup Wizard

The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.

The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.

Startup Wizard - Step 1 of 9

- After the Startup wizard has been launched, the Starting Point window (also referred to as the Welcome window) is displayed.
- It provides a choice to:
  - **Modify existing configuration**
  - **Reset configuration to factory defaults**
- Select an option and click **Next** to continue.


Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Starting Point (Step 1 of ...)
< Back
Next >
Finish
Cancel
Help

Choose a starting point for the wizard.

● Modify existing configuration

○ Reset configuration to factory defaults

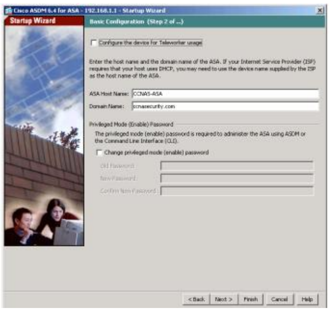
☑ Configure the IP address of the management inter...

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Startup Wizard - Step 2 of 9

- Complete the basic ASA management configuration consisting of:
  - A host name
  - Domain name
  - Privileged EXEC password
- Optionally, this step also allows the administrator to deploy the ASA for a remote worker.
- Complete the options and click **Next** to continue.



Basic Configuration (Step 2 of ...)

□ Configure the device for Teleworker usage

Enter the host name and the domain name of the ASA. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to use the device name supplied by the ISP as the host name of the ASA.

ASA Host Name: CCNAS-ASA

Domain Name: ccnasecurity.com

Privileged Mode (Enable) Password

The privileged mode (enable) password is required to administer the ASA using ASDM or the Command Line Interface (CLI).

□ Change privileged mode (enable) password

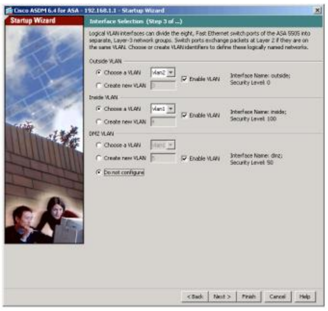
Old Password:

New Password:

Confirm New Password:

Startup Wizard - Step 3 of 9

- Create the VLAN switch interfaces.
- This step is specific to the ASA 5505 model.
- Complete the options and click **Next** to continue.



Interface Selection (Step 3 of ...)

Logical VLAN interfaces can divide the eight, Fast Ethernet switch ports of the ASA 5505 into separate, Layer-3 network groups. Switch ports exchange packets at Layer 2 if they are on the same VLAN. Choose or create VLAN identifiers to define these logically named networks.

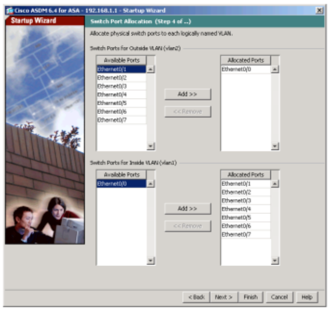
Outside VLAN
- ● Choose a VLAN: vlan2
- ○ Create new VLAN: 3
- ☑ Enable VLAN — Interface Name: outside; Security Level: 0

Inside VLAN
- ● Choose a VLAN: vlan1
- ○ Create new VLAN: 4
- ☑ Enable VLAN — Interface Name: inside; Security Level: 100

DMZ VLAN
- ○ Choose a VLAN: vlan3
- ○ Create new VLAN: 5
- ☑ Enable VLAN — Interface Name: dmz; Security Level: 50
- ● Do not configure

Startup Wizard - Step 4 of 9

- Map the physical Layer 2 switch ports to the logically named VLANs in the previous step.
- By default, all switch ports are assigned to VLAN 1 (Inside).
- Click **Next** to continue.



Switch Port Allocation (Step 4 of ...)

Allocate physical switch ports to each logically named VLAN.

Switch Ports for Outside VLAN (vlan2)

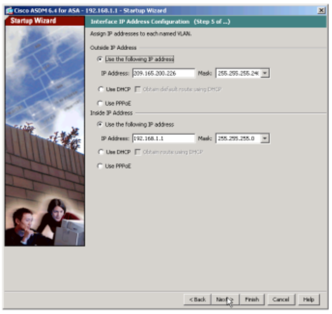
Available Ports	Allocated Ports
Ethernet0/1	Ethernet0/0
Ethernet0/2	
Ethernet0/3	
Ethernet0/4	
Ethernet0/5	
Ethernet0/6	
Ethernet0/7	

Switch Ports for Inside VLAN (vlan1)

Available Ports	Allocated Ports
Ethernet0/0	Ethernet0/1
	Ethernet0/2
	Ethernet0/3
	Ethernet0/4
	Ethernet0/5
	Ethernet0/6
	Ethernet0/7

Startup Wizard - Step 5 of 9

- Identify the inside and outside IP addresses for the defined VLANs.
- Note that these addresses could also be created using DHCP or PPPoE.
- Complete the options and click **Next** to continue.



Interface IP Address Configuration (Step 5 of ...)

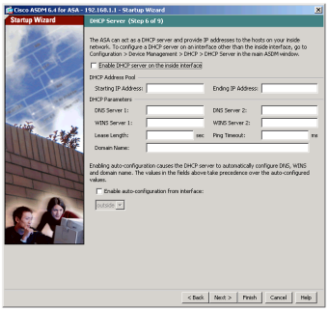
Assign IP addresses to each named VLAN.

Outside IP Address
- ● Use the following IP address
  - IP Address: 209.165.200.226 Mask: 255.255.255.24
- ○ Use DHCP □ Obtain default route using DHCP
- ○ Use PPPoE

Inside IP Address
- ● Use the following IP address
  - IP Address: 192.168.1.1 Mask: 255.255.255.0
- ○ Use DHCP □ Obtain route using DHCP
- ○ Use PPPoE

Startup Wizard - Step 6 of 9

- Enable the DHCP service for inside hosts.
- All DHCP related options are defined in this window.
- Complete the options and click **Next** to continue.



DHCP Server (Step 6 of 9)

The ASA can act as a DHCP server and provide IP addresses to the hosts on your inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.

☐ Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: Ending IP Address:

DHCP Parameters

DNS Server 1: DNS Server 2:

WINS Server 1: WINS Server 2:

Lease Length: sec Ping Timeout: ms

Domain Name:

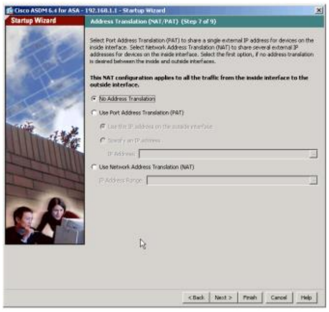
Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.

☐ Enable auto-configuration from interface:

outside

Startup Wizard - Step 7 of 9

- Enable PAT or NAT.
- Complete the options and click **Next** to continue.



Address Translation (NAT/PAT) (Step 7 of 9)

Select Port Address Translation (PAT) to share a single external IP address for devices on the inside interface. Select Network Address Translation (NAT) to share several external IP addresses for devices on the inside interface. Select the first option, if no address translation is desired between the inside and outside interfaces.

This NAT configuration applies to all the traffic from the inside interface to the outside interface.

● No Address Translation

○ Use Port Address Translation (PAT)

● Use the IP address on the outside interface

○ Specify an IP address

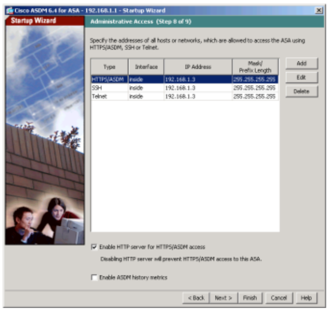
IP Address:

○ Use Network Address Translation (NAT)

IP Address Range:

Startup Wizard - Step 8 of 9

- Specify which host or hosts are allowed to access the ASA using either HTTPS/ASDM, SSH, or Telnet.
- Complete the options and click **Next** to continue.



Administrative Access (Step 8 of 9)

Specify the addresses of all hosts or networks, which are allowed to access the ASA using HTTPS/ASDM, SSH or Telnet.

Type	Interface	IP Address	Mask/ Prefix Length
HTTPS/ASDM	inside	192.168.1.3	255.255.255.255
SSH	inside	192.168.1.3	255.255.255.255
Telnet	inside	192.168.1.3	255.255.255.255

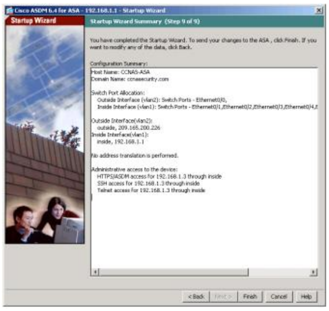
☑ Enable HTTP server for HTTPS/ASDM access

Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.

☐ Enable ASDM history metrics

Startup Wizard - Step 9 of 9

- Review the proposed configuration.
- Changes can be made by clicking the **Back** button or saved by clicking the **Finish** button.



Startup Wizard Summary (Step 9 of 9)

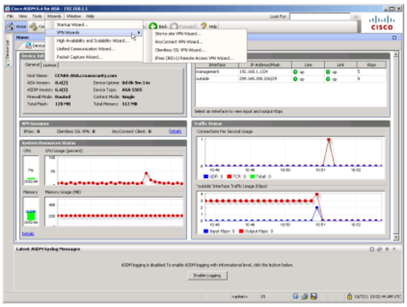
You have completed the Startup Wizard. To send your changes to the ASA , click Finish. If you want to modify any of the data, click Back.

Configuration Summary:

```
Host Name: CCNAS-ASA
Domain Name: ccnasecurity.com

Switch Port Allocation:
   Outside Interface (vlan2): Switch Ports - Ethernet0/0,
   Inside Interface (vlan1): Switch Ports - Ethernet0/1,Ethernet0/2,Ethernet0/3,Ethernet0/4,E

Outside Interface(vlan2):
   outside, 209.165.200.226
Inside Interface(vlan1):
   inside, 192.168.1.1

No address translation is performed.

Administrative access to the device:
   HTTPS/ASDM access for 192.168.1.3 through inside
   SSH access for 192.168.1.3 through inside
   Telnet access for 192.168.1.3 through inside
```

ASDM VPN Wizards

- Wizard to configure site-to-site and remote-access VPNs.



Cisco ASDM 6.4 for ASA - 192.168.1.1

File
View
Tools
Wizards
Window
Help
Look For:
Go
Home
Back
Forward
Help
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
AnyConnect VPN Wizard...
Clientless SSL VPN Wizard...
IPsec (IKEv1) Remote Access VPN Wizard...
General
License

Host Name: CCNAS-ASA.ccnasecurity.com
ASA Version: 8.4(2)
ASDM Version: 6.4(5)
Firewall Mode: Routed
Total Flash: 128 MB
Device Uptime: 0d 0h 5m 14s
Device Type: ASA 5505
Context Mode: Single
Total Memory: 512 MB

Interface	IP Address/Mask	Line	Link	Kbps
management	192.168.1.1/24	up	up	5
outside	209.165.200.226/29	up	up	0

Select an interface to view input and output Kbps

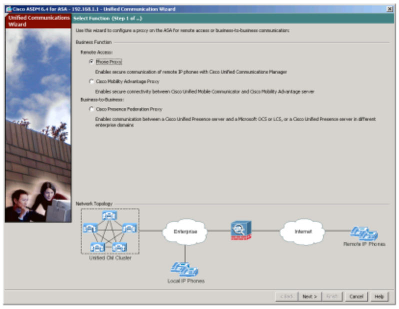
VPN Sessions
IPSec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 Details

Latest ASDM Syslog Messages

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

ASDM Unified Communication Wizard

- Configure the ASA to support the Cisco Unified Communications Proxy feature.



Cisco ASDM 6.4 for ASA - 192.168.1.1 - Unified Communication Wizard

Unified Communications Wizard

Select Function (Step 1 of ...)

Use this wizard to configure a proxy on the ASA for remote access or business-to-business communication:

Business Function

Remote Access:

● Phone Proxy

Enables secure communication of remote IP phones with Cisco Unified Communications Manager

○ Cisco Mobility Advantage Proxy

Enables secure connectivity between Cisco Unified Mobile Communicator and Cisco Mobility Advantage server

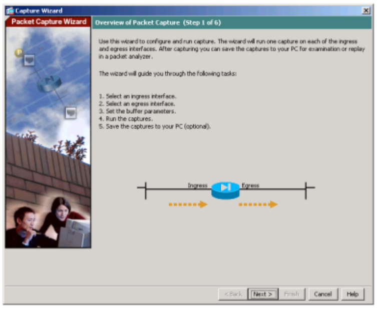
Business-to-Business:

○ Cisco Presence Federation Proxy

Enables communication between a Cisco Unified Presence server and a Microsoft OCS or LCS, or a Cisco Unified Presence server in different enterprise domains

ASDM Packet Capture Wizard

- Use the wizard for troubleshooting and testing purposes.



Capture Wizard

Packet Capture Wizard

Overview of Packet Capture (Step 1 of 6)

Use this wizard to configure and run capture. The wizard will run one capture on each of the ingress and egress interfaces. After capturing you can save the captures to your PC for examination or replay in a packet analyzer.

The wizard will guide you through the following tasks:

1. Select an ingress interface.
2. Select an egress interface.
3. Set the buffer parameters.
4. Run the captures.
5. Save the captures to your PC (optional).

Objects and Object Groups

Objects and Object Groups

- An object can be defined with a particular IP address and netmask pair or a protocol (and, optionally, a port) and it can be re-used in several configurations.
- The advantage is that when an object is modified, the change is automatically applied to all rules that use the specified object.
  - Therefore, objects make it easy to maintain configurations.
- Objects can be used in NAT, access lists, and object groups.

Objects

- The ASA supports two types of objects.
- **Network object:**
  - Contains a single IP address/mask pair.
  - Can be defined by host, subnet, or range of addresses.
- **Service object:**
  - Contains a protocol and optional source and/or destination port.

NOTE:

- A network object is required to configure NAT.

```
CCNAS-ASA(config)# object ?

configure mode commands/options:
  network  Specifies a host, subnet or range IP addresses
  service  Specifies a protocol/port
CCNAS-ASA(config)#
```

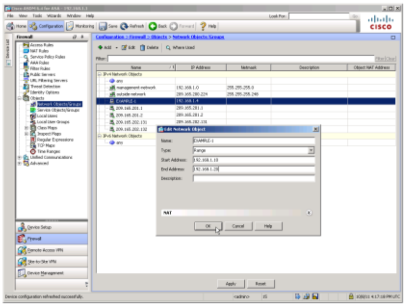
Configuring a Network Object

- To create a network object, use the **`object network`** *`object-name`* global configuration command.
  - The prompt will change to the network object configuration mode.
- A network object can contain only one IP address and mask pair.
  - Entering a second IP address/mask pair will replace the existing configuration.
- To erase all network objects, use the **`clear config object network`** command.
  - Note that this command clears all network objects.

```
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.4
CCNAS-ASA(config-network-object)# range 192.168.1.10 192.168.1.20
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object network EXAMPLE-1
 range 192.168.1.10 192.168.1.20
CCNAS-ASA(config)#
```

Configuring a Network Object using ASDM

- **Configurations** > **Firewall** > **Objects** > **Network Objects/Groups**



Edit Network Object

Name: EXAMPLE-1

Type: Range

Start Address: 192.168.1.10

End Address: 192.168.1.20

Description:

Configuring a Service Object

- To create a network object, use the **object service** *object-name* global configuration command.
  - The prompt will change to the network object configuration mode.
- A service object name can only be associated with one protocol and port (or ports).
  - If an existing service object is configured with a different protocol and port (or ports), the new configuration replaces the existing protocol and port (or ports) with the new ones.

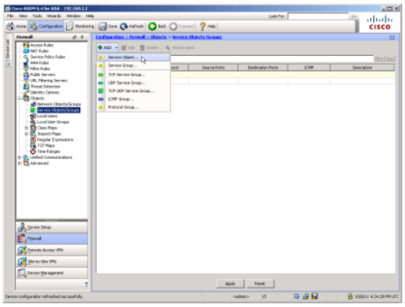
```
CCNAS-ASA(config)# object service SERV-1
CCNAS-ASA(config-service-object)# service tcp destination eq ftp
CCNAS-ASA(config-service-object)# service tcp destination eq www
CCNAS-ASA(config-service-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object service SERV-1
 service tcp destination eq www
CCNAS-ASA(config)#
```

Service Objects

- There are five service options:
  - **service** *protocol* [**source** [*operator port*]] [**destination** [*operator port*]]
    - Specifies an IP protocol name or number.
  - **service tcp** [**source** [*operator port*]] [**destination** [*operator port*]]
    - Specifies that the service object is for the TCP protocol.
  - **service udp** [**source** [*operator port*]] [**destination** [*operator port*]]
    - Specifies that the service object is for the UDP protocol.
  - **service icmp** *icmp-type*
    - Specifies that the service object is for the ICMP protocol.
  - **service icmp6** *icmp6-type*
    - Specifies that the service object is for the ICMPv6 protocol.

Configuring a Service Object using ASDM

- **Configurations** > **Firewall** > **Objects** > **Service Objects/Groups**



Object Groups

- Object groups are used to group objects.
  - Objects can be attached or detached from multiple object groups.
- Objects can be attached or detached from one or more object groups when needed, ensuring that the objects are not duplicated but can be re-used wherever needed.
- You can create network, protocol, and ICMP-type objects groups created using the **object-group** {**network** | **protocol** | **icmp-type**} *group-name* command.
- You can also create service objects groups by using **object-group service** *group-name* [**tcp** | **udp** | **tcp-udp**].

Object Groups

- There are four types of group objects.

Object-Group	Description
Network	• Specifies a list of IP host, subnet, or network addresses.
Protocol	• Combines IP protocols (such as TCP, UDP, and ICMP) into one object. • For example, to add both TCP and UDP services of DNS, create an object group and add TCP and UDP protocols into that group.
ICMP	• The ICMP protocol uses unique types to send control messages (RFC 792). • The ICMP-type object group can group the necessary types for security needs.
Service	• Used to group TCP, UDP, or TCP and UDP ports into an object. • It can contain a mix of TCP services, UDP services, ICMP-type services, and any protocol such as ESP, GRE, and TCP.

```
CCNAS-ASA(config)# object-group ?

configure mode commands/options:
  icmp-type  Specifies a group of ICMP types, such as echo
  network    Specifies a group of host or subnet IP addresses
  protocol   Specifies a group of protocols, such as TCP, etc
  service    Specifies a group of TCP/UDP ports/services
  user       Specifies single user, local or import user group
CCNAS-ASA(config)# object-group
```

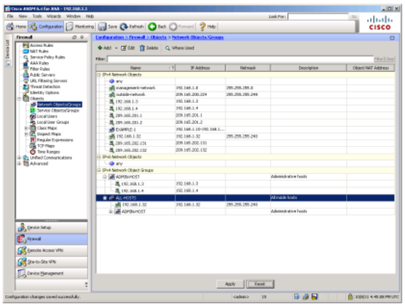
Network Object Group

- To configure a network object group, use the **`object-group network`** *`grp-name`* global configuration command.
- Add network objects to the network group using the commands:
  - **`network-object`**
  - **`group-object`**

```
CCNAS-ASA(config)# object-group network ADMIN-HOST
CCNAS-ASA(config-network-object-group)# network-object host 192.168.1.3
CCNAS-ASA(config-network-object-group)# network-object host 192.168.1.4
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)# object-group network ALL-HOSTS
CCNAS-ASA(config-network-object-group)# network-object 192.168.1.32 255.255.255.240
CCNAS-ASA(config-network-object-group)# group-object ADMIN-HOST
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)# show run object-group
object-group network ADMIN-HOST
 description Administrative host IP addresses
 network-object host 192.168.1.3
 network-object host 192.168.1.4
object-group network ALL-HOSTS
 network-object 192.168.1.32 255.255.255.240
 group-object ADMIN-HOST
CCNAS-ASA(config)#
```

Network Object Group using ASDM

- **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**



Name	IP Address	Netmask	Description	Object NAT Address
IPv4 Network Objects				
any				
management-network	192.168.1.0	255.255.255.0		
outside-network	209.165.200.224	255.255.255.240		
192.168.1.3	192.168.1.3			
192.168.1.4	192.168.1.4			
209.165.201.1	209.165.201.1			
209.165.201.2	209.165.201.2			
EXAMPLE-1	192.168.1.10-192.168.1...			
192.168.1.32	192.168.1.32	255.255.255.240		
209.165.202.131	209.165.202.131			
209.165.202.132	209.165.202.132			
IPv6 Network Objects				
any				
IPv4 Network Object Groups				
ADMIN-HOST			Administrative hosts	
192.168.1.3	192.168.1.3			
192.168.1.4	192.168.1.4			
ALL-HOSTS			All inside hosts	
192.168.1.32	192.168.1.32	255.255.255.240		
ADMIN-HOST			Administrative hosts	

Protocol Object Group

- To configure a protocol object group, use the **`object-group protocol`** *`grp-name`* global configuration command.
- Add network objects to the protocol group using the commands:
  - **`protocol-object`**
  - **`group-object`**

```
CCNAS-ASA(config)# object-group protocol PROTO-1
CCNAS-ASA(config-protocol-object-group)# protocol-object udp
CCNAS-ASA(config-protocol-object-group)# protocol-object ipsec
CCNAS-ASA(config-protocol-object-group)# exit
CCNAS-ASA(config)# object-group protocol PROTO-2
CCNAS-ASA(config-protocol-object-group)# protocol-object tcp
CCNAS-ASA(config-protocol-object-group)# group-object PROTO-1
CCNAS-ASA(config-protocol-object-group)# exit
CCNAS-ASA(config)# show running-config object-group protocol
object-group protocol PROTO-1
 protocol-object udp
 protocol-object esp
object-group protocol PROTO-2
 protocol-object tcp
 group-object PROTO-1
CCNAS-ASA(config)#
```

ICMP Object Group

- To configure an ICMP object group, use the **`object-group icmp-type`** *`grp-name`* global configuration command.
- Add ICMP objects to the protocol group using the commands:
  - **`icmp-object`**
  - **`group-object`**

```
CCNAS-ASA(config)# object-group icmp-type ICMP-ALLOWED
CCNAS-ASA(config-icmp-object-group)# icmp-object echo
CCNAS-ASA(config-icmp-object-group)# icmp-object time-exceeded
CCNAS-ASA(config-icmp-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object-group id ICMP-ALLOWED
object-group icmp-type ICMP-ALLOWED
 icmp-object echo
 icmp-object time-exceeded
CCNAS-ASA(config)#
```

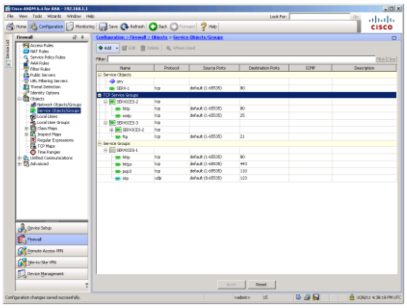
Service Object Group

- To configure a service object group, use the **`object-group service`** *`grp-name`* global configuration command.
- Add service objects to the protocol group using the commands:
  - **`service-object`**
  - **`group-object`**

```
CCNAS-ASA(config)# object-group service SERVICES-1
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq www
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq https
CCNAS-ASA(config-service-object-group)# service-object udp destination eq ntp
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service SERVICES-2 tcp
CCNAS-ASA(config-service-object-group)# port-object eq pop3
CCNAS-ASA(config-service-object-group)# port-object eq smtp
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service SERVICES-3 tcp
CCNAS-ASA(config-service-object-group)# group-object SERVICES-2
CCNAS-ASA(config-service-object-group)# port-object eq ftp
CCNAS-ASA(config-service-object-group)# port-object range 2000 2005
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
```

Services Object Group

- **Configuration** > **Firewall** > **Objects** > **Service Objects/Groups**



Name	Protocol	Source Ports	Destination Ports	ICMP	Description
Service Objects					
any					
SERV-1	tcp	default (1-65535)	80		
TCP Service Groups					
SERVICES-2	tcp				
http	tcp	default (1-65535)	80		
smtp	tcp	default (1-65535)	25		
SERVICES-3	tcp				
SERVICES-2	tcp				
ftp	tcp	default (1-65535)	21		
Service Groups					
SERVICES-1					
http	tcp	default (1-65535)	80		
https	tcp	default (1-65535)	443		
pop3	tcp	default (1-65535)	110		
ntp	udp	default (0-65535)	123		

Configuration changes saved successfully. <admin> 15 10/8/11 4:38:18 PM UTC

CISCO

ACLs

Similarities Between ASA and IOS ACLs

- Both ACLs are made up of one or more access control entries (ACEs).
- Both ACLs are processed sequentially from top down.
- Both follow the 1st ACE match will cause the ACL to be exited.
- Both have the implicit deny all at the bottom.
- Both support remarks added per ACE or ACL.
- Both follow the one access list per interface, per protocol, per direction rule.
- Both ACLs can be enabled/disabled based on time ranges.

Differences Between ASA and IOS ACLs

- The ASA ACL uses a network mask (e.g., 255.255.255.0).
  - The IOS ACL uses the wildcard mask (e.g., 0.0.0.255).
- ACLs are always named instead of numbered.
  - ASA ACLs can be numbered but unlike IOS ACL the numbers have no significance other than naming the ACL.
- By default, security levels apply access control without an ACL configured.

ACL Function

- ACLs on a security appliance can be used:
  - Through-traffic packet filtering:
    - Traffic is passing through the appliance from one interface to another interface.
    - The configuration requires an ACL to be defined and then applied to an interface.
  - To-the-box-traffic packet filtering:
    - Also known as a management access rule, traffic (e.g., Telnet, SSH, SNMP) is destined for the appliance.
    - Introduced to filter traffic destined to the control plane of the ASA.
    - It is completed in one step but requires an additional set of rules to implement access control.

Five Types of ASA ACL Types

- The ASA supports five types of ACLs.

ACL Type	Description
Extended	• Most popular type of ASA ACL. • Filters on source/destination port and protocol.
Standard	• Used for routing protocols, not firewall rules. • Cannot be applied to interfaces to control traffic.
IPv6	• Used to support IPv6 addressing.
Webtype	• Used for clientless SSL VPN.
Ethertype	• Specifies network layer protocol. • Only used with transparent mode.

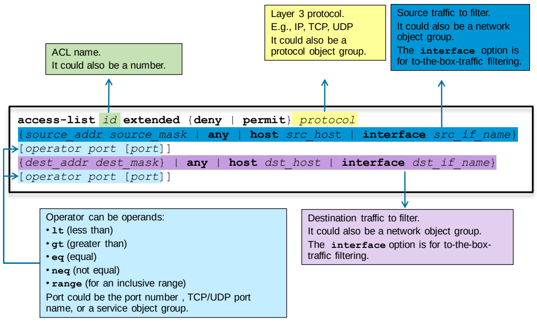
ACL Applications

ACL Use	ACL Type	Description
Provide through-traffic network access	Extended	• By default, the ASA does not allow lower security traffic to a higher security interface unless it is explicitly permitted.
Identify traffic for AAA rules	Extended	• Used in AAA access lists to identify traffic.
Identify addresses for NAT	Extended	• Policy NAT lets you identify local traffic for address translation by specifying the source and destination addresses.
Establish VPN access	Extended	• Used in VPN commands.
Identify traffic Modular Policy Framework (MPF)	Extended	• Used to identify traffic in a class map, which is used for features that support MPF.
Identify OSPF route redistribution	Standard	• Standard access lists include only the destination address. • Used to control the redistribution of OSPF routes.
Control network access for IPV6 networks	IPv6	• Used for control traffic in IPv6 networks.

Extended ACL Command Syntax

```
CCNAS-ASA(config)# help access-list

USAGE:


Extended access list:
          Use this to configure policy for IP traffic through the firewall

[no] access-list <id> [line <line_num>] [extended] {deny | permit}
                    {<protocol> | object-group {<service_obj_grp_id> |
                    <protocol_obj_grp_id>} | object <service_object_name>}
                    [user-group [<domain_nickname>\\]<user_group_name> |
                     user [<domain_nickname>\]<user_name> |
                     object-group-user < object_group_user_name>]
                    {host <sip> | <sip> <smask> | interface <ifc> | any |
                    object-group <network_obj_grp_id> |
                    object <network_obj_name>}
                    [<operator> <port> [<port>] |
                    object-group <service_obj_grp_id>]
                    {host <dip> | <dip> <dmask> | interface <ifc> | any |
                    object-group <network_obj_grp_id> |
                    object <network_obj_name>}
                    [<operator> <port> [<port>] |
                    object-group <service_obj_grp_id>]
                    [log [disable] | [<level>] | [default] [interval <secs>]]

<Output omitted>
```

Condensed ACL



ACL name.
It could also be a number.

Layer 3 protocol.
E.g., IP, TCP, UDP
It could also be a protocol object group.

Source traffic to filter.
It could also be a network object group.
The **interface** option is for to-the-box-traffic filtering.

```
access-list id extended {deny | permit} protocol
{source_addr source_mask | any | host src_host | interface src_if_name}
[operator port [port]]
{dest_addr dest_mask} | any | host dst_host | interface dst_if_name}
[operator port [port]]
```

Operator can be operands:
- **lt** (less than)
- **gt** (greater than)
- **eq** (equal)
- **neq** (not equal)
- **range** (for an inclusive range)

Port could be the port number , TCP/UDP port name, or a service object group.

Destination traffic to filter.
It could also be a network object group.
The **interface** option is for to-the-box-traffic filtering.

Access-group Syntax

- To provide through-traffic network access, the ACL must be applied to an interface.
  - **access-group** *acl-id* {**in** | **out**} **interface** *interface-name* [**per-user-override** | **control-plane**]

Syntax	Description
access-group	Keyword used to apply an ACL to an interface.
acl-id	The name of the actual ACL to be applied to an interface.
in	The ACL will filter inbound packets.
out	The ACL will filter outbound packets.
interface	Keyword to specify the interface to which to apply the ACL.
interface_name	The name of the interface to which to apply an ACL.
per-user-override	Option that allows downloadable ACLs to override the entries on the interface ACL.
control-plane	Specifies if the rule is for to-the-box traffic.

ACL Examples

ACL Examples

Allowing Same Security Level Communication

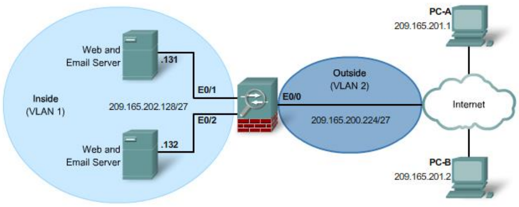
- By default, interfaces on the same security level:
  - Cannot communicate with each other.
  - Packets cannot enter and exit the same interface.
    - Useful for VPN traffic that enters an interface, but is then routed out the same interface.
- Use the **`same-security-traffic permit inter-interface`** enables interfaces on the same security level so that they can communicate with each other.
- Use the **`same-security-traffic permit intra-interface`** command to enable communication between hosts connected to the same interface.

Verifying ACLs

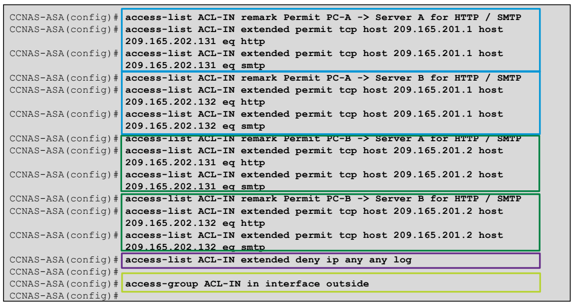
- To verify the ACL syntax, use the following commands:
  - **`show running-config access-list`**
  - **`show access-list`**

ACL - Example 1

- PC-A and PC-B are external hosts that require access to the two internal servers.
  - Each server provides Web and email services.



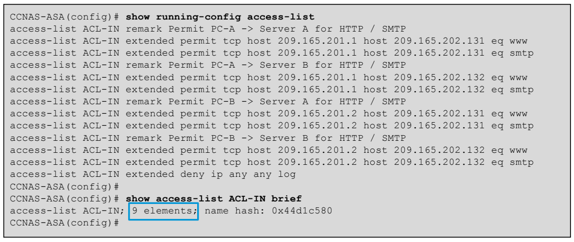
ACL - Example 1



```
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-A -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host
                   209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host
                   209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-A -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host
                   209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host
                   209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-B -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host
                   209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host
                   209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-B -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host
                   209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host
                   209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN extended deny ip any any log
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-group ACL-IN in interface outside
CCNAS-ASA(config)#
```

ACL - Example 1

- Verify the configuration.
- Notice that there are 9 elements (9 ACEs), excluding the remarks, that must be processed by the ASA.



```
CCNAS-ASA(config)# show running-config access-list
access-list ACL-IN remark Permit PC-A -> Server A for HTTP / SMTP
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq www
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq smtp
access-list ACL-IN remark Permit PC-A -> Server B for HTTP / SMTP
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq www
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq smtp
access-list ACL-IN remark Permit PC-B -> Server A for HTTP / SMTP
access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq www
access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq smtp
access-list ACL-IN remark Permit PC-B -> Server B for HTTP / SMTP
access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq www
access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq smtp
access-list ACL-IN extended deny ip any any log
CCNAS-ASA(config)#
CCNAS-ASA(config)# show access-list ACL-IN brief
access-list ACL-IN; 9 elements; name hash: 0x44d1c580
CCNAS-ASA(config)#
```

ACL with Object Groups - Example 2

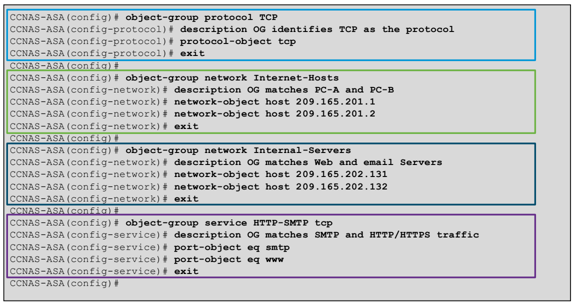
- This example achieves the same result as Example 1 except it uses object groups to simplify and modularize the configuration.
- The following object groups are created:
  - **TCP:** Protocol object group.
  - **Internet-Hosts:** Network object group identifying the two external hosts.
  - **Internal-Servers:** Network object group identifying the two internal servers.
  - **HTTP-SMTP:** Service object group identifying HTTP and SMTP protocols.
- These object groups are then specified in one ACL-IN ACE.
- All remaining traffic will be denied and logged.

NOTE:

- Although there will only be two ACEs in ACL-IN, the total number of elements will remain at 9.

ACL with OGs - Example 2

- Create Object groups.



```
CCNAS-ASA(config)# object-group protocol TCP
CCNAS-ASA(config-protocol)# description OG identifies TCP as the protocol
CCNAS-ASA(config-protocol)# protocol-object tcp
CCNAS-ASA(config-protocol)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group network Internet-Hosts
CCNAS-ASA(config-network)# description OG matches PC-A and PC-B
CCNAS-ASA(config-network)# network-object host 209.165.201.1
CCNAS-ASA(config-network)# network-object host 209.165.201.2
CCNAS-ASA(config-network)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group network Internal-Servers
CCNAS-ASA(config-network)# description OG matches Web and email Servers
CCNAS-ASA(config-network)# network-object host 209.165.202.131
CCNAS-ASA(config-network)# network-object host 209.165.202.132
CCNAS-ASA(config-network)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service HTTP-SMTP tcp
CCNAS-ASA(config-service)# description OG matches SMTP and HTTP/HTTPS traffic
CCNAS-ASA(config-service)# port-object eq smtp
CCNAS-ASA(config-service)# port-object eq www
CCNAS-ASA(config-service)# exit
CCNAS-ASA(config)#
```

ACL with OGs - Example 2

- Create the ACL and apply it.

```
CCNAS-ASA(config)# access-list ACL-IN remark Only permit PC-A / PC-B -> servers
CCNAS-ASA(config)# access-list ACL-IN extended permit object-group TCP
object-group Internet-Hosts object-group Internal-Servers object-group HTTP-SMTP
CCNAS-ASA(config)# access-list ACL-IN extended deny ip any any log
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-group ACL-IN in interface outside
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config access-list
access-list ACL-IN remark Only permit PC-A / PC-B -> servers
access-list ACL-IN extended permit object-group TCP object-group Internet-Hosts object-
group Internal-Servers object-group HTTP-SMTP
CCNAS-ASA(config)#
CCNAS-ASA(config)# show access-list ACL-IN brief
access-list ACL-IN; 9 elements; name hash: 0x44d1c580
CCNAS-ASA(config)#
```

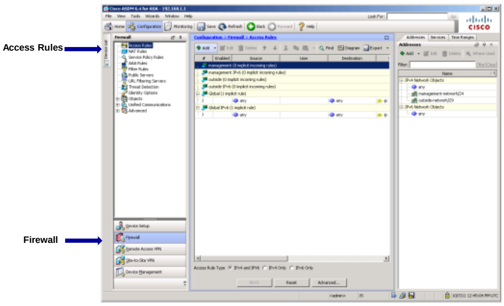
ACL with OGs - Example 2

- Display the content of ACL-IN.

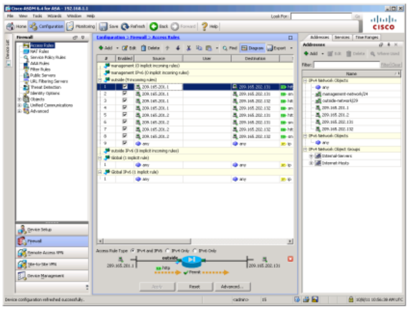
```
CCNAS-ASA(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list ACL-IN; 9 elements; name hash: 0x44d1c580
access-list ACL-IN line 1 remark Only permit PC-A / PC-B -> servers
access-list ACL-IN line 2 extended permit object-group TCP object-group Internet-Hosts
object-group Internal-Servers object-group HTTP-SMTP 0xbd5ed7a7
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.1 host 209.165.202.131 eq
smtp (hitcnt=0) 0x3f0a0233
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.1 host 209.165.202.131 eq
www (hitcnt=0) 0xab920b7c
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.1 host 209.165.202.132 eq
smtp (hitcnt=0) 0x92b62c8c
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.1 host 209.165.202.132 eq
www (hitcnt=0) 0x52206d23
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.2 host 209.165.202.131 eq
smtp (hitcnt=0) 0x68a43a2d
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.2 host 209.165.202.131 eq
www (hitcnt=0) 0x46270b1a
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.2 host 209.165.202.132 eq
smtp (hitcnt=0) 0x9fe1ca85
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.2 host 209.165.202.132 eq
www (hitcnt=0) 0x598855e6
access-list ACL-IN line 4 extended deny ip any any log informational interval 300
(hitcnt=0) 0x4d6e3bb6
CCNAS-ASA(config)#
```

Access Rule Pane

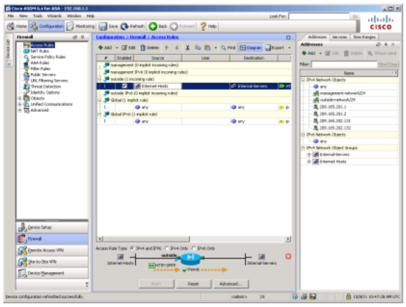
- **Configuration** > **Firewall** > **Access Rules**



ACL Example



ACL with Object Group Example



Cisco ASDM 6.4 for ASA - 192.168.1.1

Configuration > Firewall > Access Rules

#	Enabled	Source	User	Destination
management (0 implicit incoming rules)				
management IPv6 (0 implicit incoming rules)				
outside (1 incoming rule)				
1	☑	Internet-Hosts		Internal-Servers
outside IPv6 (0 implicit incoming rules)				
Global (1 implicit rule)				
1		any		any
Global IPv6 (1 implicit rule)				
1		any		any

Addresses

- IPv4 Network Objects
  - any
  - management-network/24
  - outside-network/29
  - 209.165.201.1
  - 209.165.201.2
  - 209.165.202.131
  - 209.165.202.132
- IPv6 Network Objects
  - any
- IPv4 Network Object Groups
  - Internal-Servers
  - Internet-Hosts

Access Rule Type ● IPv4 and IPv6 ○ IPv4 Only ○ IPv6 Only

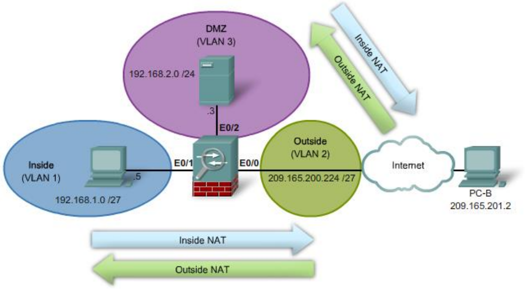
Device configuration refreshed successfully.

NAT

ASA NAT Services

- Like IOS routers, the ASA supports the following NAT and PAT deployment methods:
- **Inside NAT**
  - Typical NAT deployment method when the ASA translates the internal host address to a global address.
  - The ASA restores return traffic the original inside IP address.
- **Outside NAT**
  - Deployment method used when traffic from a lower-security interface is destined for a higher-security interface.
  - This method may be useful to make a host on the outside appear as one from a known internal IP address.
- **Bidirectional NAT**
  - Both inside NAT and outside NAT are used together.

NAT Deployment Methods



Auto NAT

- Introduced in ASA version 8.3, the Auto NAT feature has simplified the NAT configuration as follows:
  1. Create a network object.
  2. Identify host(s) network to be translated.
  3. Define the **`nat`** command parameters.

NOTE:

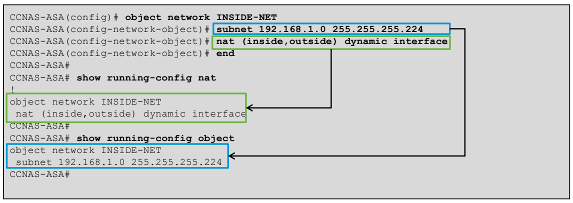
- Prior to ASA version 8.3, NAT was configured using the **`nat`**, **`global`**, and **`static`** commands.
- The **`global`** and **`static`** commands are no longer recognized.

Configuring NAT

- The ASA divides the NAT configuration into two sections:
  - The first section defines the network to be translated using a network object.
  - The second section defines the actual **`nat`** command parameters.
- These appear in two different places in the running-config.

NOTE:

- This actual configuration is for PAT.



```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
CCNAS-ASA# show running-config nat
!
object network INSIDE-NET
 nat (inside,outside) dynamic interface
CCNAS-ASA#
CCNAS-ASA# show running-config object
object network INSIDE-NET
 subnet 192.168.1.0 255.255.255.224
CCNAS-ASA#
```

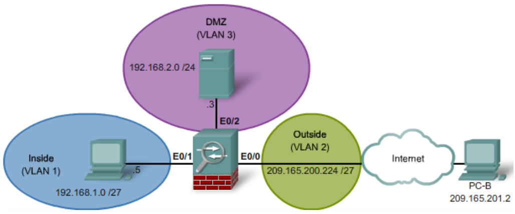
Types of NAT Configurations

- **Dynamic NAT**
  - Many-to-many translation.
  - Typically deployed using inside NAT.
- **Dynamic PAT**
  - Many-to-one translation.
  - Usually an inside pool of private addresses overloading an outside interface or outside address.
  - Typically deployed using inside NAT.
- **Static NAT**
  - A one-to-one translation.
  - Usually an outside address mapping to an internal server.
  - Typically deployed using outside NAT.
- **Twice-NAT**
  - ASA version 8.3 NAT feature that identifies both the source and destination address in a single rule (nat command).
  - Used when configuring remote-access IPsec and SSL VPNs.

Configuring Dynamic NAT

- To configure dynamic NAT, two network objects are required.
- The first network object identifies the pool of public IP addresses that internal addresses will be translated to.
  - **`object network`** *`mapped-obj`*
    - Names the network object that identifies the pool of public addresses.
  - **`range`** *`ip-addr-1 ip-addr-n`*
    - Assigns the public pool IP addresses in a range.
- The second network object binds the two objects together.
  - **`object network`** *`nat-object-name`*
    - Names the NAT object to bind the inside subnet with the public pool network object.
  - **`subnet`** *`net-address net-mask`*
    - Identifies the inside network subnet to the named object.
  - **`nat (`***`real-ifc,mapped-ifc`***`) dynamic`** *`mapped-obj`*
    - Traffic going from the *`real-ifc`* and going to the *`mapped-ifc`* will be dynamically assigned addresses from the public pool of addresses.

Configuring Dynamic NAT Example

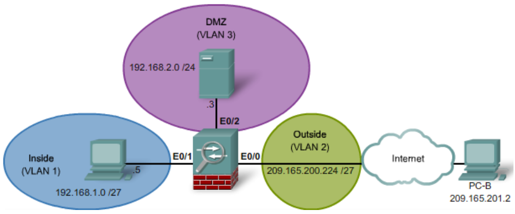


```
CCNAS-ASA(config)# object network PUBLIC-IP
CCNAS-ASA(config-network-object)# range 209.165.200.240 255.255.255.240
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic PUBLIC-IP
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

Configuring Dynamic PAT

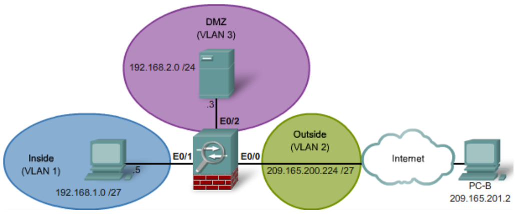
- Dynamic PAT is when the outside interface IP address or another specified IP address is overloaded.
- Only one network object is required to configure dynamic PAT:
  - **object network** *nat-object-name*
    - Names the static NAT object.
  - **subnet** *net-address net-mask*
    - Identifies the inside network subnet as the network object.
  - **nat (***real-ifc*,*mapped-ifc***) dynamic** [**interface** | *ip-address*]
    - Traffic going from the *real-ifc* interface to the *mapped-ifc* interface will be dynamically the IP address of the outside interface or a specified outside IP address.
    - The parentheses and comma **(,)** are required.

Configuring Dynamic PAT Example



```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

Configuring Dynamic PAT Example



```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic 209.165.200.229
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

- As an alternative, you can specify an outside IP address.

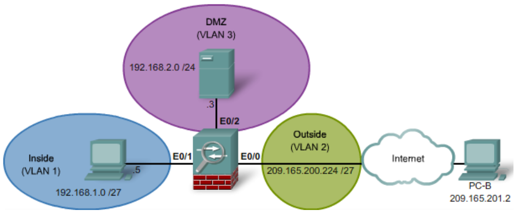
Configuring Static NAT

- Static NAT maps an inside IP address to an outside address.
  - To access Web servers by outside hosts.
- To configure static NAT:
  - **`object network`** *`nat-object-name`*
    - Names the static NAT object.
  - **`host`** *`ip-addr`*
    - Identifies the inside host IP address.
  - **`nat (`***`real-ifc`*`,` *`mapped-ifc`***`) static`** *`mapped-ip-addr`*
    - Statically maps an inside address to an identified outside IP address.
    - The parentheses and comma **`(,)`** are required.
    - Note that the **`any`** keyword could be used instead of the interface names to allow the translation of an object between multiple interfaces using one CLI command.

NOTE:

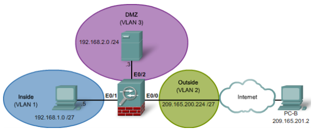
- Static NAT also requires that an ACE be added to the outside interface ACL.

Static NAT Example



```
CCNAS-ASA(config)# object network DMZ-SERVER
CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.200.165.227
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit ip any host 192.168.2.3
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside
CCNAS-ASA(config)#
```

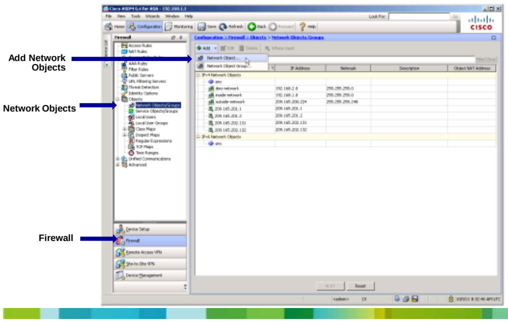
Verifying Static NAT



```
CCNAS-ASA# show nat

Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static DMZ-SERVER 209.165.200.227
    translate_hits = 0, untranslate_hits = 4

2 (inside) to (outside) source dynamic inside-net interface
    translate_hits = 4, untranslate_hits = 0

CCNAS-ASA# show xlate
1 in use, 3 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from dmz:192.168.2.3 to outside:209.165.200.227 flags s idle 0:22:58 timeout 0:00:00
CCNAS-ASA#
```

Add Network Object

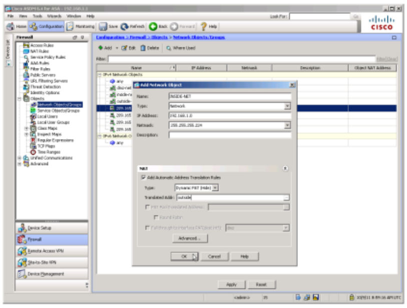
- **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**



	IP Address	Netmask	Description	Object NAT Address
IPv4 Network Objects				
any				
dmz-network	192.168.2.0	255.255.255.0		
inside-network	192.168.1.0	255.255.255.0		
outside-network	209.165.200.224	255.255.255.248		
209.165.201.1	209.165.201.1			
209.165.201.2	209.165.201.2			
209.165.202.131	209.165.202.131			
209.165.202.132	209.165.202.132			
IPv6 Network Objects				
any				

Dynamic PAT

- **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**

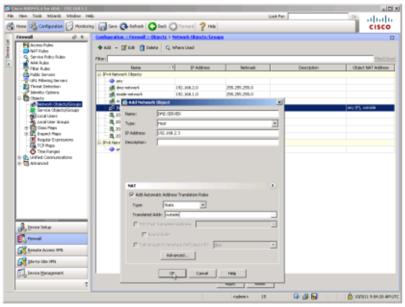


Name: INSIDE-NET
Type: Network
IP Address: 192.168.1.0
Netmask: 255.255.255.224
Description:

NAT
☑ Add Automatic Address Translation Rules
Type: Dynamic PAT (Hide)
Translated Addr: outside

Static NAT

- **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**



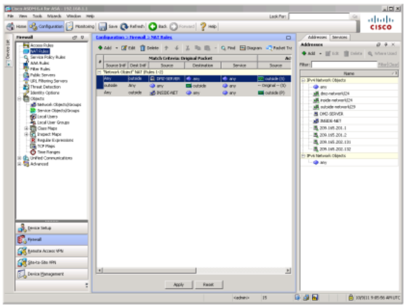
Name	IP Address	Netmask	Description	Object NAT Address
IPv4 Network Objects				
any				
dmz-network	192.168.2.0	255.255.255.0		
inside-network	192.168.1.0	255.255.255.0		

Name: DMZ-SERVER
Type: Host
IP Address: 192.168.2.3
Description:

NAT
☑ Add Automatic Address Translation Rules
Type: Static
Translated Addr: outside

Verifying NAT

- **Configuration** > **Firewall** > **NAT Rules**


Cisco ASDM 6.4 for ASA - 192.168.1.1
Configuration > Firewall > NAT Rules
Add
Edit
Delete
Find
Diagram
Packet Trace
Addresses
Services
Apply
Reset

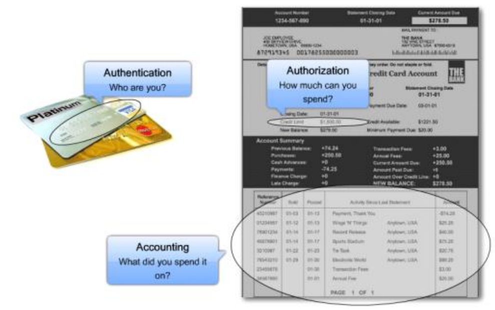
#	Match Criteria: Original Packet					Action
	Source Intf	Dest Intf	Source	Destination	Service	Source
"Network Object" NAT (Rules 1-2)						
	Any	outside	DMZ-SERVER	any	any	outside (S)
	outside	Any	any	outside	any	-- Original -- (S)
	Any	outside	INSIDE-NET	any	any	outside (P)

Addresses
- IPv4 Network Objects
  - any
  - dmz-network/24
  - inside-network/24
  - outside-network/29
  - DMZ-SERVER
  - INSIDE-NET
  - 209.165.201.1
  - 209.165.201.2
  - 209.165.202.131
  - 209.165.202.132
- IPv6 Network Objects
  - any

AAA

AAA

The AAA Concept is Similar to the Use of a Credit Card



ASA AAA

- Unlike the ISR, ASA devices do not support local authentication without using AAA.
- Cisco ASA can be configured to authenticate using:
  - A local user database
  - An external server for authentication
  - Both

Local Database AAA Authentication

- Local AAA uses a local database for authentication.
  - Users authenticate against the local database entries.
  - Local AAA is ideal for small networks that do not need a dedicated server.
- Use the **`username`** *`name`* **`password`** *`password`* `[`**`privilege`** *`priv-level`*`]` command to create local user accounts.
- Use the **`aaa authentication`** `{`**`enable`** `|` **`http`** `|` **`ssh`** `|` **`telnet`**`}` **`console`** `{`*`aaa-svr-name`* `|` **`LOCAL`**`}` command.

```
CCNAS-ASA(config)# username admin password cisco privilege 15
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa authentication enable console LOCAL
CCNAS-ASA(config)# aaa authentication http console LOCAL
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
CCNAS-ASA(config)# aaa authentication telnet console LOCAL
CCNAS-ASA(config)#
```

Server-Based AAA Authentication

- Server-based AAA authentication is a far more scalable solution.
- Server-based AAA authentication uses an external database server resource leveraging RADIUS or TACACS+ protocols.
- To configure a TACACS+ or RADIUS server, use the following commands:
  - **`aaa-server`** *`server-tag`* **`protocol`** *`protocol`*
    - Creates a TACACS+ or RADIUS AAA server group.
  - **`aaa-server`** *`server-tag`* `[(`*`interface-name`*`)]` **`host`** `{`*`server-ip`* `|` *`name`*`}` `[`**`key`** *`password`*`]`
    - Configures a AAA server as part of a AAA server group. Also configures AAA server parameters that are host-specific.
- Configure server based AAA authentication.
  - Use the **`aaa authentication`** `{`**`enable`** `|` **`http`** `|` **`ssh`** `|` **`telnet`**`}` **`console`** *`server-tag`* command.

Configuring AAA Authentication

- Configure AAA TACACS+ server and local AAA authentication.
  - The local database is used as a backup.

```
CCNAS-ASA(config)# username admin password cisco privilege 15
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa-server TACACS-SVR protocol tacacs+
CCNAS-ASA(config-aaa-server-group)# aaa-server TACACS-SVR (dmz) host 192.168.2 cisco123
CCNAS-ASA(config-aaa-server-host)#exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run aaa-server
aaa-server TACACS-SVR protocol tacacs+
aaa-server TACACS-SVR (dmz) host 192.168.2.3
 key *****
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa authentication http console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication enable console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication http console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication serial console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication ssh console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication telnet console TACACS-SVR LOCAL
CCNAS-ASA(config)#
CCNAS-ASA(config)#
```

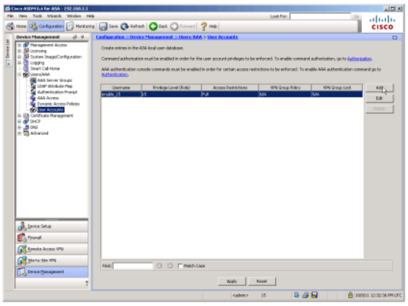
Verify the AAA Configuration

- Log out and log back in.
- Use the:
  - **show running-conf username** command to view all user accounts.
  - **show running-conf aaa** command to view the AAA configuration.
- Use the **clear config aaa** command to erase AAA.

```
CCNAS-ASA(config)# show run aaa
aaa authentication enable console TACACS-SVR LOCAL
aaa authentication http console TACACS-SVR LOCAL
aaa authentication serial console TACACS-SVR LOCAL
aaa authentication ssh console TACACS-SVR LOCAL
aaa authentication telnet console TACACS-SVR LOCAL
CCNAS-ASA(config)# exit
CCNAS-ASA# disable
CCNAS-ASA> exit

Logoff

Username: admin
Password: *****
Type help or '?' for a list of available commands.
CCNAS-ASA>
```

Add Local Database Entries

- **Configuration** > **Device Management** > **Users/AAA** > **User Accounts**



Configuration > Device Management > Users/AAA > User Accounts

Create entries in the ASA local user database.

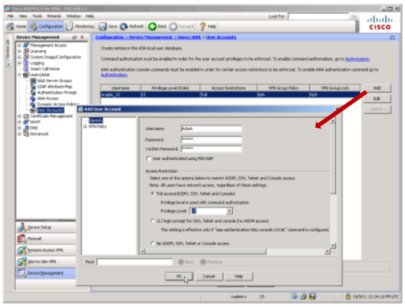
Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization.

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
enable_15	15	Full	N/A	N/A

Add a User

- Click on **Add** and enter the user detail.



Add User Account

Username: Admin

Password: *****

Confirm Password: *****

□ User authenticated using MSCHAP

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: [illegible]

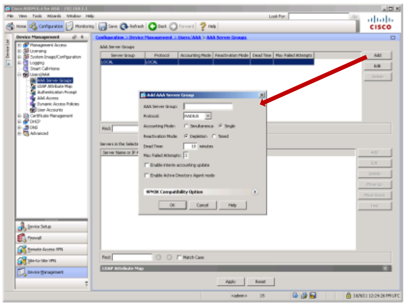
○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if "aaa authentication http console LOCAL" command is configured.

○ No ASDM, SSH, Telnet or Console access

Add AAA Server Group

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



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

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

Add AAA Server Group

AAA Server Group:

Protocol: RADIUS

Accounting Mode: ○ Simultaneous ● Single

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

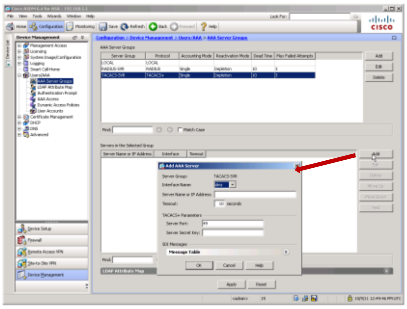
□ Enable interim accounting update

□ Enable Active Directory Agent mode

VPN3K Compatibility Option

Add TACACS Server to AAA Server Group

- Add a TACACS+ server to the configured server group.



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

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
RADIUS-SVR	RADIUS	Single	Depletion	10	3
TACACS-SVR	TACACS+	Single	Depletion	10	3

Add AAA Server

Server Group: TACACS-SVR

Interface Name: dmz

Server Name or IP Address:

Timeout: 10 seconds

TACACS+ Parameters

Server Port: 49

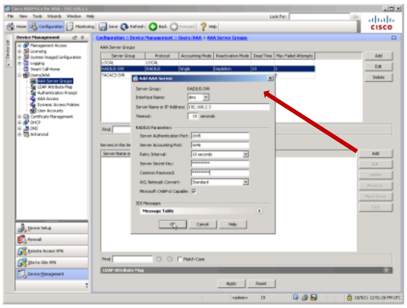
Server Secret Key:

SDI Messages

Message Table

Add RADIUS Server to AAA Server Group

- Add a RADIUS server to the configured server group.



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

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

Add AAA Server

Server Group: RADIUS-SVR

Interface Name: dmz

Server Name or IP Address: 192.168.2.3

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

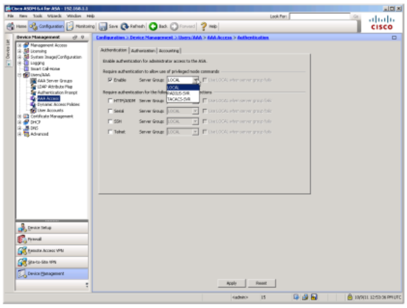
Microsoft CHAPv2 Capable: ☑

SDI Messages

Message Table

Enable AAA Authentication

- **Configuration** > **Firewall** > **Users/AAA** > **AAA Access** > **Authentication**



Configuration > Device Management > Users/AAA > AAA Access > Authentication

Authentication | Authorization | Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

☑ Enable Server Group: LOCAL □ Use LOCAL when server group fails

LOCAL
RADIUS-SVR
TACACS-SVR

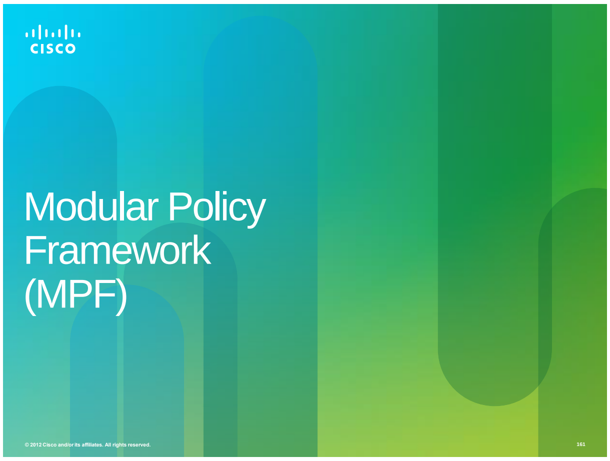
Require authentication for the following types of connections

□ HTTP/ASDM Server Group: □ Use LOCAL when server group fails

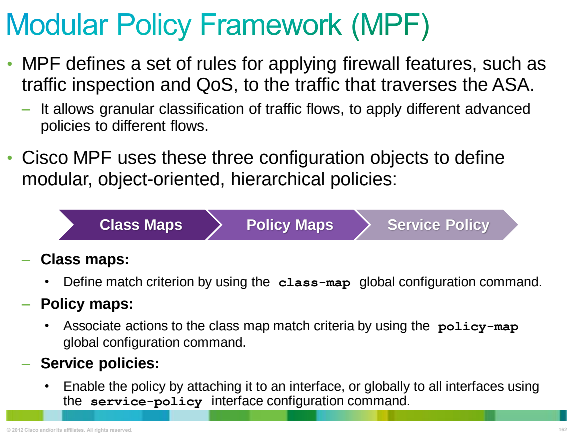
□ Serial Server Group: LOCAL □ Use LOCAL when server group fails

□ SSH Server Group: LOCAL □ Use LOCAL when server group fails

□ Telnet Server Group: LOCAL □ Use LOCAL when server group fails



Modular Policy Framework (MPF)



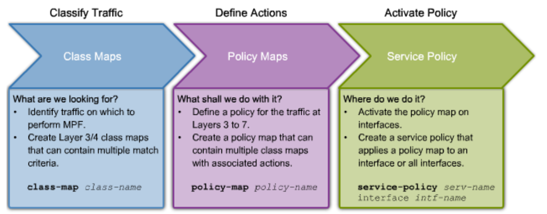
Modular Policy Framework (MPF)

- MPF defines a set of rules for applying firewall features, such as traffic inspection and QoS, to the traffic that traverses the ASA.
  - It allows granular classification of traffic flows, to apply different advanced policies to different flows.
- Cisco MPF uses these three configuration objects to define modular, object-oriented, hierarchical policies:

Class Maps → Policy Maps → Service Policy

  - **Class maps:**
    - Define match criterion by using the **`class-map`** global configuration command.
  - **Policy maps:**
    - Associate actions to the class map match criteria by using the **`policy-map`** global configuration command.
  - **Service policies:**
    - Enable the policy by attaching it to an interface, or globally to all interfaces using the **`service-policy`** interface configuration command.

Modular Policy Framework (MPF)



Classify Traffic

Class Maps

What are we looking for?
- Identify traffic on which to perform MPF.
- Create Layer 3/4 class maps that can contain multiple match criteria.

class-map *class-name*

Define Actions

Policy Maps

What shall we do with it?
- Define a policy for the traffic at Layers 3 to 7.
- Create a policy map that can contain multiple class maps with associated actions.

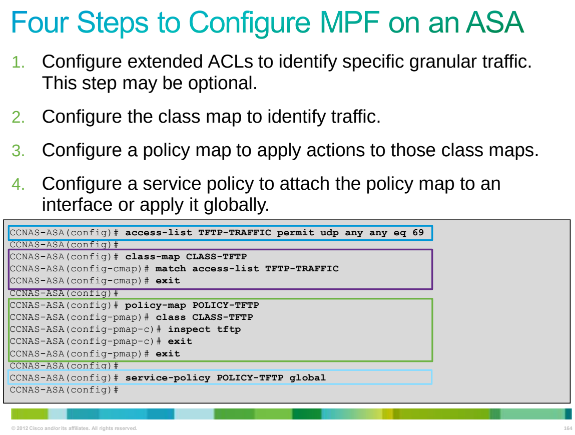
policy-map *policy-name*

Activate Policy

Service Policy

Where do we do it?
- Activate the policy map on interfaces.
- Create a service policy that applies a policy map to an interface or all interfaces.

service-policy *serv-name*
interface *intf-name*



Four Steps to Configure MPF on an ASA

1. Configure extended ACLs to identify specific granular traffic. This step may be optional.
2. Configure the class map to identify traffic.
3. Configure a policy map to apply actions to those class maps.
4. Configure a service policy to attach the policy map to an interface or apply it globally.

```
CCNAS-ASA(config)# access-list TFTP-TRAFFIC permit udp any any eq 69
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map CLASS-TFTP
CCNAS-ASA(config-cmap)# match access-list TFTP-TRAFFIC
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map POLICY-TFTP
CCNAS-ASA(config-pmap)# class CLASS-TFTP
CCNAS-ASA(config-pmap-c)# inspect tftp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# service-policy POLICY-TFTP global
CCNAS-ASA(config)#
```

Class Maps

- Class maps are configured to identify Layer 3/4 traffic.
- To create a class map and enter class-map configuration mode, use the **class-map** *class-map-name* global configuration command.
  - The names "**class-default**" and any name that begins with **"_internal**" or **"_default**" are reserved.
  - The class map name must be unique and can be up to 40 characters in length.
  - The name should also be descriptive.

NOTE:

- For management traffic destined to the ASA configure the **class-map type management** *class-map-name* command.

Class Map Configuration Mode

- In class-map configuration mode, define the traffic to include in the class by matching one of the following characteristics.
  - **description** - Add description text.
  - **match any** - Class map matches all traffic.
  - **match access-list** *access-list-name* - Class map matches traffic specified by an extended access list.
- To display information about the class map configuration, use the **show running-config class-map** command.

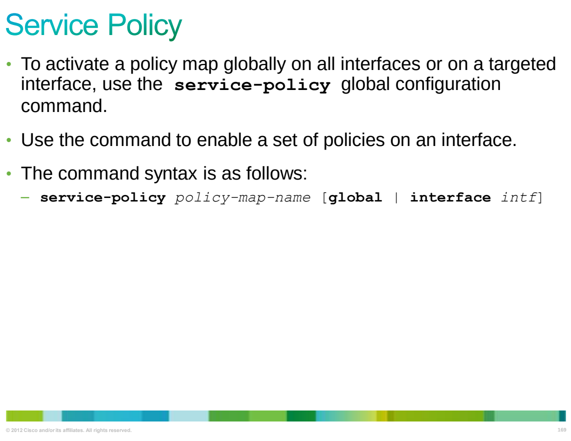
Policy Map

Policy maps are used to bind class maps with actions in 3 steps:

1. Use the **policy-map** *policy-map-name* global command.
   - The policy map name must be unique and up to 40 characters in length.
2. From policy-map configuration mode (config-pmap), configure:
   - **description** - Add description text.
   - **class** *class-map-name*
     - Identify a specific class map on which to perform actions.
     - Enter sub-configuration mode.
3. Assign actions for the class including:
   - **set connection** - sets connection values
   - **inspect** - provides protocol inspection servers
   - **police** - sets rate limits for traffic in this class

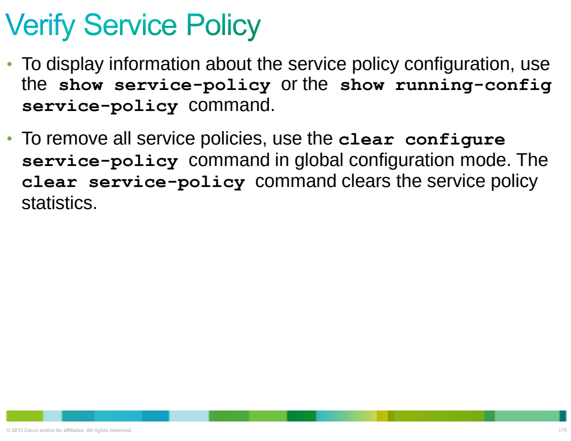
Verify Policy Map

- To display information about the policy map configuration, use the **show running-config policy-map** command.
- To remove all policy maps, use the **clear configure policy-map** command in global configuration mode.



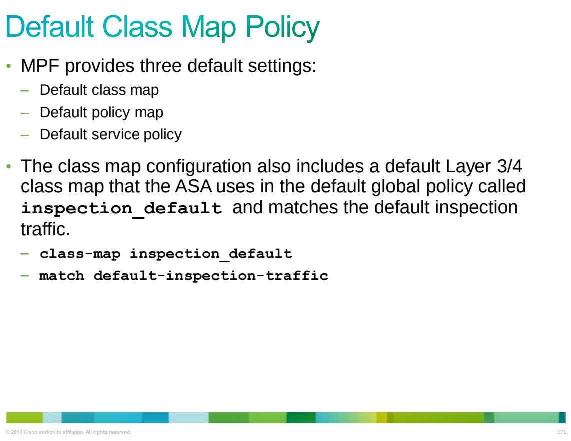
Service Policy

- To activate a policy map globally on all interfaces or on a targeted interface, use the **`service-policy`** global configuration command.
- Use the command to enable a set of policies on an interface.
- The command syntax is as follows:
  - **`service-policy`** *`policy-map-name`* `[`**`global`** `|` **`interface`** *`intf`*`]`



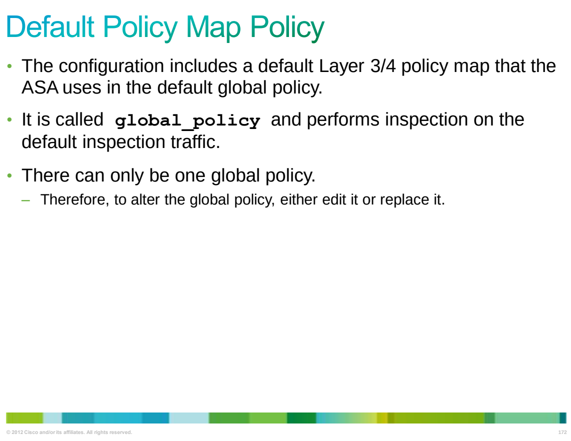
Verify Service Policy

- To display information about the service policy configuration, use the **`show service-policy`** or the **`show running-config service-policy`** command.
- To remove all service policies, use the **`clear configure service-policy`** command in global configuration mode. The **`clear service-policy`** command clears the service policy statistics.



Default Class Map Policy

- MPF provides three default settings:
  - Default class map
  - Default policy map
  - Default service policy
- The class map configuration also includes a default Layer 3/4 class map that the ASA uses in the default global policy called **`inspection_default`** and matches the default inspection traffic.
  - **`class-map inspection_default`**
  - **`match default-inspection-traffic`**



Default Policy Map Policy

- The configuration includes a default Layer 3/4 policy map that the ASA uses in the default global policy.
- It is called **`global_policy`** and performs inspection on the default inspection traffic.
- There can only be one global policy.
  - Therefore, to alter the global policy, either edit it or replace it.

ASA Default Policy

- The ASA default configuration includes a global service policy that matches all default application inspection traffic.
  - Otherwise, the service policy can be applied to an interface or globally.
  - Interface service policies take precedence over the global service policy for a given feature.
- To alter the global policy, an administrator needs to either edit the default policy, or disable the default policy and apply a new policy.

Default ASA MPF Policy

```
<Output omitted>

class-map inspection_default
 match default-inspection-traffic

policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp

service-policy global_policy global

<Output omitted>
```

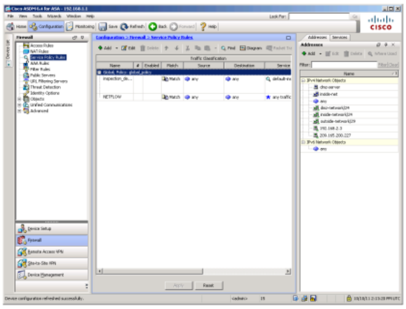
Class map statement matches the keyword "**`default-inspection-traffic`**."

Policy map associates actions to the traffic identified in the class map.

Service policy applies a policy map to an interface or as in this case, globally to all interfaces that do not have a specific policy.

ASDM Service Policies

- **Configuration** > **Firewall** > **Service Policy Rules** > **Add**



Cisco ASDM 6.4 for ASA - 192.168.1.1

Configuration > Firewall > Service Policy Rules

Name	#	Enabled	Match	Source	Destination	Service
Global; Policy: global_policy						
inspection_de...			Match	any	any	default-in
NETFLOW			Match	any	any	any traffic

Device configuration refreshed successfully.

ASA VPN Features

Remote Access VPNs

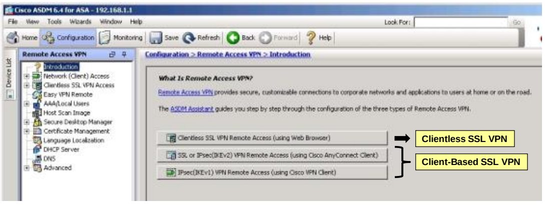
- Enterprise users are requesting support for their mobile devices including smart phones, tablets, notebooks, and a broader range of laptop manufacturers and operating systems.
- This shift has created a challenge for IT security.
- The solution is the use of SSL VPNs to secure access for all users, regardless of the endpoint from which they establish a connection.

IOS VPN versus ASA VPN

- Both Cisco ISR and ASA provide IPsec and SSL VPN capabilities.
  - ISRs are capable of supporting as many as 200 concurrent users.
  - ASA can support from 10 to 10,000 sessions per device.
- For this reason, the ASA is usually the choice when supporting a large remote networking deployment.

ASA Remote Access VPN Support

- The ASA supports three types of remote-access VPNs:
  - Clientless SSL VPN Remote Access (using a web browser)
  - SSL or IPsec (IKEv2) VPN Remote Access (using Cisco AnyConnect client)
  - IPsec (IKEv1) VPN Remote Access (using Cisco VPN client)


Cisco ASDM 6.4 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For:
Go
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Remote Access VPN
Introduction
Network (Client) Access
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Configuration > Remote Access VPN > Introduction

What Is Remote Access VPN?

Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road.

The ASDM Assistant guides you step by step through the configuration of the three types of Remote Access VPN.

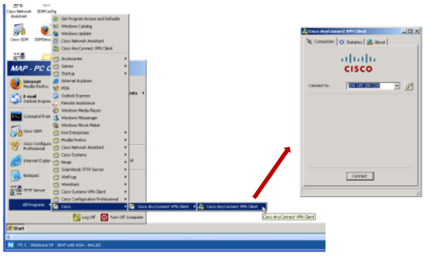
Clientless SSL VPN Remote Access (using Web Browser)
SSL or IPsec(IKEv2) VPN Remote Access (using Cisco AnyConnect Client)
IPsec(IKEv1) VPN Remote Access (using Cisco VPN Client)
Clientless SSL VPN
Client-Based SSL VPN

Clientless versus Client-Based SSL VPN

- **Clientless SSL VPN:**
  - Browser-based VPN that lets users establish a secure, remote-access VPN tunnel to the ASA using a web browser.
  - After authentication, users access a portal page and can access specific, supported internal resources.
- **Client-Based SSL VPN:**
  - Provides full tunnel SSL VPN connection but requires a VPN client application to be installed on the remote host.
  - Requires a client, such as the Cisco AnyConnect VPN client to be installed on the host.
- The AnyConnect client can be manually pre-installed on the host, or downloaded on-demand to a host via a browser.

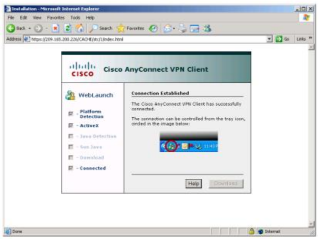
AnyConnect Previously Installed

- When the AnyConnect client is pre-installed on the host, the VPN connection can be initiated by starting the application.
  - Once the user authenticates, the ASA examines the revision of the client and upgrades it as necessary.



AnyConnect Downloaded and Installed

- Remote users can connect and authenticate to the ASA and then uploads the AnyConnect client to the host.
  - Host operating systems supported include Windows, Mac OS, and Linux.
  - The AnyConnect client then installs and configures itself and finally establishes an SSL VPN connection.



https://209.165.200.226/CACHE/stc/1/index.html

Connection Established

The Cisco AnyConnect VPN Client has successfully connected.

The connection can be controlled from the tray icon, circled in the image below:

Consumerization

- To support IT consumerization, the Cisco AnyConnect client is available for free for:
  - iOS devices (iPhone, iPad, and iPod Touch)
  - Android OS (select models)
  - BlackBerry
  - Windows Mobile 6.1
  - HP webOS
  - Nokia Symbian

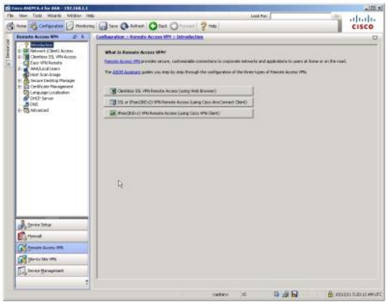
Status Connected
Server vpn.example.com
Time Connected 01:01:52
Client Address 10.81.8.44
Bytes Sent 135161
Bytes Received 3994025

CISCO

Clientless VPN Wizard

ASDM Assistant

- Clientless SSL VPN can be configured using the ASDM Assistant to guide an administrator through the SSL VPN configuration.


Cisco ASDM 6.4 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Introduction
Network (Client) Access
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access VPN > Introduction
Clientless SSL VPN Remote Access (using Web Browser)
SSL or IPsec(IKEv2) VPN Remote Access (using Cisco AnyConnect Client)
IPsec(IKEv1) VPN Remote Access (using Cisco VPN Client)
<admin> 15

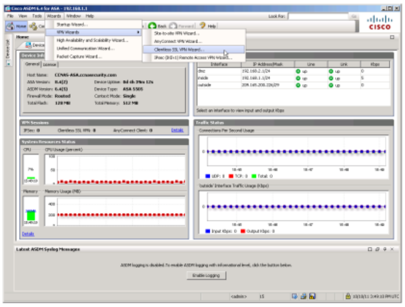
What Is Remote Access VPN?

Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road.

The ASDM Assistant guides you step-by-step through the configuration of the three types of Remote Access VPN.

Clientless SSL VPN Wizard

- Clientless SSL VPN can also be configured using the Menu Bar **Wizards** > **VPN Wizards** > **Clientless SSL VPN Wizard**.


Cisco ASDM 6.4 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For:
Home
Back Forward Help
CISCO
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
AnyConnect VPN Wizard...
Clientless SSL VPN Wizard...
IPsec (IKEv1) Remote Access VPN Wizard...
General License
VPN Sessions
System Resources Status
CPU
CPU Usage (percent)
Memory
Memory Usage (MB)
Details
Traffic Status
Connections Per Second Usage
UDP: 0 TCP: 0 Total: 0
'outside' Interface Traffic Usage (Kbps)
Input Kbps: 0 Output Kbps: 0
Latest ASDM Syslog Messages
Enable Logging
<admin> 15

Host Name: CCNAS-ASA.ccnasecurity.com
ASA Version: 8.4(2) Device Uptime: 0d 4h 39m 12s
ASDM Version: 6.4(5) Device Type: ASA 5505
Firewall Mode: Routed Context Mode: Single
Total Flash: 128 MB Total Memory: 512 MB

Interface	IP Address/Mask	Line	Link	Kbps
dmz	192.168.2.1/24	up	up	0
inside	192.168.1.1/24	up	up	5
outside	209.165.200.226/29	up	up	0

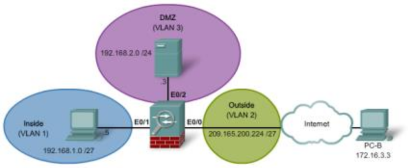
Select an interface to view input and output Kbps

IPSec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0

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

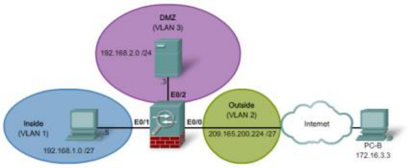
Clientless SSL VPN Wizard Example

- The topology in this example is as follows:
  - An inside network with security level 100
  - A DMZ with security level 50
  - An outside network with a security level of 0
- Access to the DMZ server is already provided using static NAT.



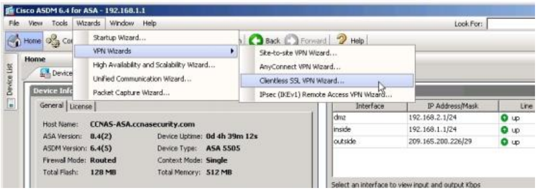
Clientless SSL VPN Wizard Example

- Assume the outside host requires access to specific applications which do not need a full tunnel SSL VPN.
- For this reason, the remote host will use a secure web browser connection to access select corporate resources.



Start the ASDM Clientless SSL VPN Wizard

- **Wizards** > **VPN Wizards** > **Clientless SSL VPN Wizard**

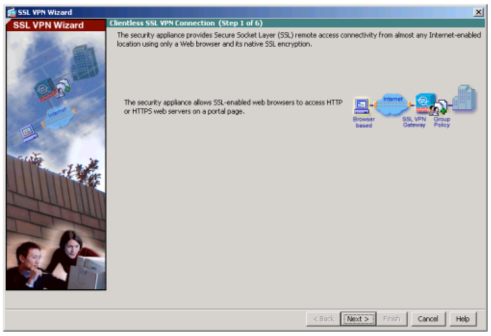

Cisco ASDM 6.4 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For:
Home Co
Back Forward Help
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
AnyConnect VPN Wizard...
Clientless SSL VPN Wizard...
IPsec (IKEv1) Remote Access VPN Wizard...
Device List
Home
Device
Device Info
General License

Host Name: **CCNAS-ASA.ccnasecurity.com**
ASA Version: **8.4(2)** Device Uptime: **0d 4h 39m 12s**
ASDM Version: **6.4(5)** Device Type: **ASA 5505**
Firewall Mode: **Routed** Context Mode: **Single**
Total Flash: **128 MB** Total Memory: **512 MB**

Interface	IP Address/Mask	Line
dmz	192.168.2.1/24	up
inside	192.168.1.1/24	up
outside	209.165.200.226/29	up

Select an interface to view input and output Kbps

1 - SSL VPN Welcome Window

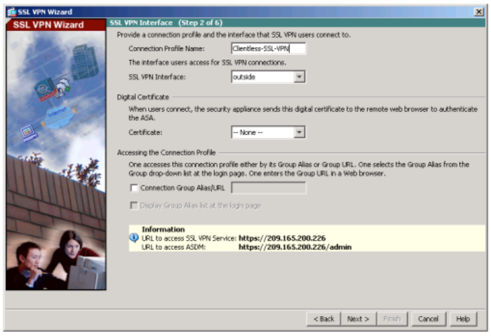


Clientless SSL VPN Connection (Step 1 of 6)

The security appliance provides Secure Socket Layer (SSL) remote access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption.

The security appliance allows SSL-enabled web browsers to access HTTP or HTTPS web servers on a portal page.

2 - SSL VPN Interface



SSL VPN Interface (Step 2 of 6)

Provide a connection profile and the interface that SSL VPN users connect to.

Connection Profile Name: Clientless-SSL-VPN

The interface users access for SSL VPN connections.

SSL VPN Interface: outside

Digital Certificate

When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.

Certificate: -- None --

Accessing the Connection Profile

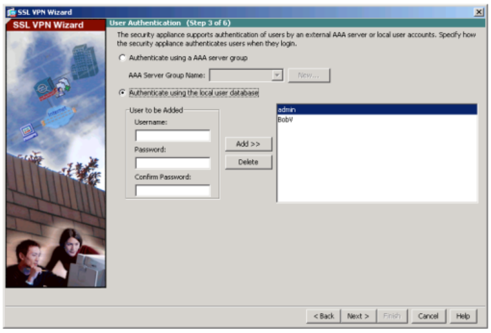
One accesses this connection profile either by its Group Alias or Group URL. One selects the Group Alias from the Group drop-down list at the login page. One enters the Group URL in a Web browser.

☐ Connection Group Alias/URL

☐ Display Group Alias list at the login page

Information
URL to access SSL VPN Service: **https://209.165.200.226**
URL to access ASDM: **https://209.165.200.226/admin**

3 - User Authentication



User Authentication (Step 3 of 6)

The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.

○ Authenticate using a AAA server group

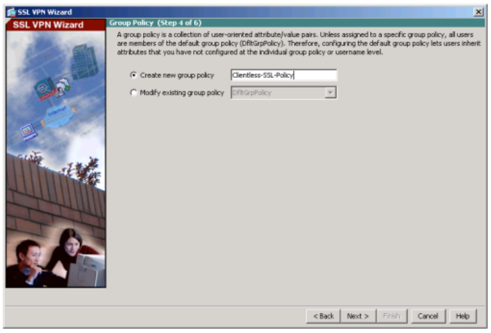
AAA Server Group Name:

● Authenticate using the local user database

User to be Added
Username:
Password:
Confirm Password:

admin
BobV

4 - Group Policy



SSL VPN Wizard

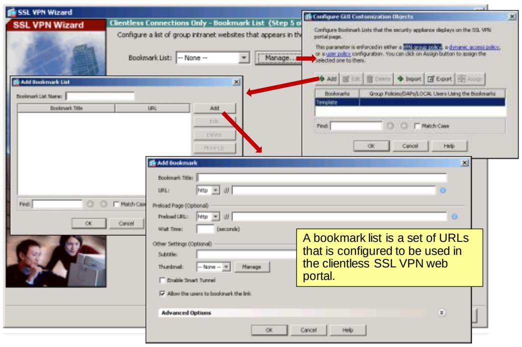
Group Policy (Step 4 of 6)

A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific group policy, all users are members of the default group policy (DfltGrpPolicy). Therefore, configuring the default group policy lets users inherit attributes that you have not configured at the individual group policy or username level.

● Create new group policy: Clientless-SSL-Policy

○ Modify existing group policy: DfltGrpPolicy

5 - Bookmark Lists



SSL VPN Wizard

Clientless Connections Only - Bookmark List (Step 5 o

Configure a list of group intranet websites that appears in th

Bookmark List: -- None --

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.

Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template	

Add Bookmark List

Bookmark List Name:

Bookmark Title	URL

Add Bookmark

Bookmark Title:

URL: http ://

Preload Page (Optional)

Preload URL: http ://

Wait Time: (seconds)

Other Settings (Optional)

Subtitle:

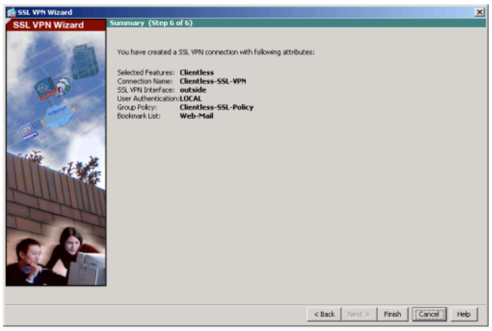
Thumbnail: -- None --

□ Enable Smart Tunnel

☑ Allow the users to bookmark the link

A bookmark list is a set of URLs that is configured to be used in the clientless SSL VPN web portal.

6 - Summary



SSL VPN Wizard

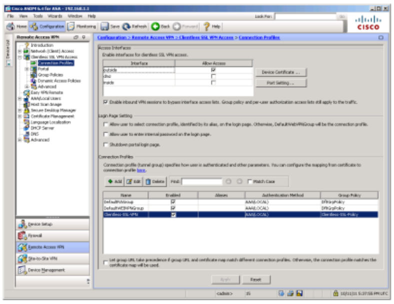
Summary (Step 6 of 6)

You have created a SSL VPN connection with following attributes:

Selected Features: **Clientless**
Connection Name: **Clientless-SSL-VPN**
SSL VPN Interface: **outside**
User Authentication: **LOCAL**
Group Policy: **Clientless-SSL-Policy**
Bookmark List: **Web-Mail**

Clientless SSL Connection Profiles Window

- **Configurations** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles**



Cisco ASDM 6.4 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	☑
dmz	□
inside	□

☑ Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Login Page Setting

□ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

□ Allow user to enter internal password on the login page.

□ Shutdown portal login page.

Connection Profiles

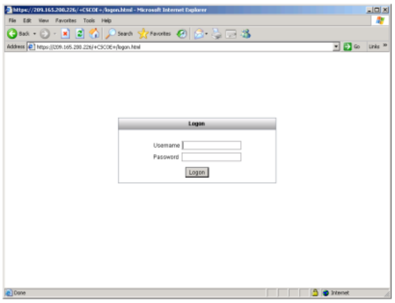
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	☑		AAA(LOCAL)	DfltGrpPolicy
Clientless-SSL-VPN	☑		AAA(LOCAL)	Clientless-SSL-Policy

□ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.

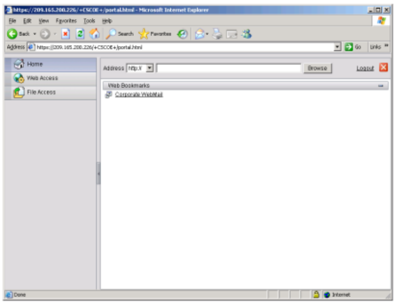
Login From the Remote Host

- From a web browser, enter the public address of the ASA device.
  - Be sure to use secure HTTP (HTTPS).


https://209.165.200.226/+CSCOE+/logon.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://209.165.200.226/+CSCOE+/logon.html
Go Links
Logon
Username
Password
Logon
Done
Internet

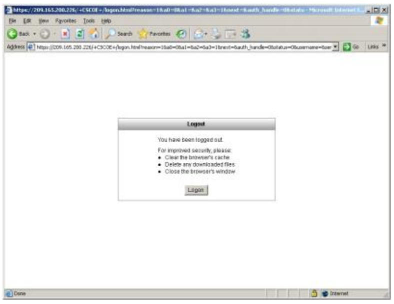
View Web Portal Bookmarks

- ASA SSL Web portal webpage will be displayed listing the various bookmarks previously assigned to the profile.


https://209.165.200.226/+CSCOE+/portal.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://209.165.200.226/+CSCOE+/portal.html
Go Links
Home
Web Access
File Access
Address http://
Browse
Logout
Web Bookmarks
Corporate WebMail
Done
Internet

Closing the Connection

- User either logs out or the connection timeouts.


https://209.165.200.226/+CSCOE+/logon.html?reason=1&a0=0&a1=&a2=&a3=1&next=&auth_handle=0&status= - Microsoft Internet E...
File Edit View Favorites Tools Help
Back Search Favorites
Address https://209.165.200.226/+CSCOE+/logon.html?reason=1&a0=0&a1=&a2=&a3=1&next=&auth_handle=0&status=0&username=&ser
Go Links
Logout
Logon
Done
Internet

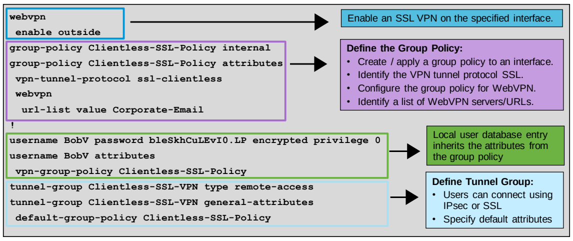
You have been logged out.

For improved security, please:

- Clear the browser's cache
- Delete any downloaded files
- Close the browser's window

Generated CLI Commands

- The clientless SSL VPN wizard generates configuration settings for the following:



```
webvpn
 enable outside
group-policy Clientless-SSL-Policy internal
group-policy Clientless-SSL-Policy attributes
 vpn-tunnel-protocol ssl-clientless
 webvpn
  url-list value Corporate-Email
!
username BobV password bleSkhCuLEvI0.LP encrypted privilege 0
username BobV attributes
 vpn-group-policy Clientless-SSL-Policy
tunnel-group Clientless-SSL-VPN type remote-access
tunnel-group Clientless-SSL-VPN general-attributes
 default-group-policy Clientless-SSL-Policy
```

Enable an SSL VPN on the specified interface.

Define the Group Policy:

- Create / apply a group policy to an interface.
- Identify the VPN tunnel protocol SSL.
- Configure the group policy for WebVPN.
- Identify a list of WebVPN servers/URLs.

Local user database entry inherits the attributes from the group policy

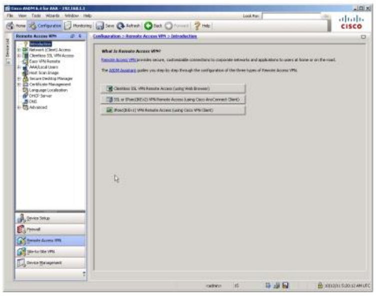
Define Tunnel Group:

- Users can connect using IPsec or SSL
- Specify default attributes

AnyConnect VPN Wizard

ASDM Assistant

- **Configurations** > **Remote-Access VPN** > **Introduction**
  - Click **SSL or IPsec(IKEv2) VPN Remote Access (using Cisco AnyConnect Client)**.


Cisco ASDM 6.4 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access VPN > Introduction
Clientless SSL VPN Remote Access (using Web Browser)
SSL or IPsec(IKEv2) VPN Remote Access (using Cisco AnyConnect Client)
IPsec(IKEv1) VPN Remote Access (using Cisco VPN Client)

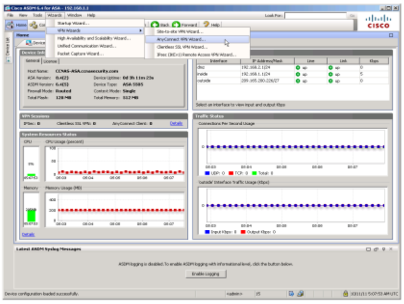
What Is Remote Access VPN?

Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road.

The ASDM Assistant guides you step by step through the configuration of the three types of Remote Access VPN.

AnyConnect VPN Wizard

- **Wizards** > **VPN Wizards** > **AnyConnect VPN Wizard**


Cisco ASDM 6.4 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For:
Home Back Forward Help
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
AnyConnect VPN Wizard...
Clientless SSL VPN Wizard...
IPsec (IKEv1) Remote Access VPN Wizard...
General License
VPN Sessions
System Resources Status
Traffic Status
CPU
CPU Usage (percent)
Memory
Memory Usage (MB)
Connections Per Second Usage
UDP: 0 TCP: 0 Total: 0
'outside' Interface Traffic Usage (Kbps)
Input Kbps: 0 Output Kbps: 0
Details
Latest ASDM Syslog Messages
Enable Logging

Host Name: CCNAS-ASA.ccnasecurity.com
ASA Version: 8.4(2)
ASDM Version: 6.4(5)
Firewall Mode: Routed
Total Flash: 128 MB
Device Uptime: 0d 3h 11m 23s
Device Type: ASA 5505
Context Mode: Single
Total Memory: 512 MB

Interface	IP Address/Mask	Line	Link	Kbps
dmz	192.168.2.1/24	up	up	0
inside	192.168.1.1/24	up	up	5
outside	209.165.200.226/27	up	up	0

Select an interface to view input and output Kbps

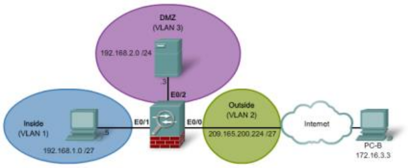
IPSec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0

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

Device configuration loaded successfully.

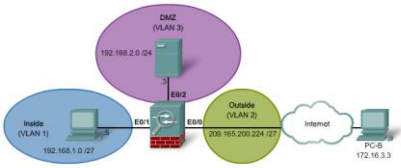
AnyConnect VPN Wizard Example

- The topology in this example is as follows:
  - An inside network with security level 100
  - A DMZ with security level 50
  - An outside network with a security level of 0
- Access to the DMZ server is already provided using static NAT.



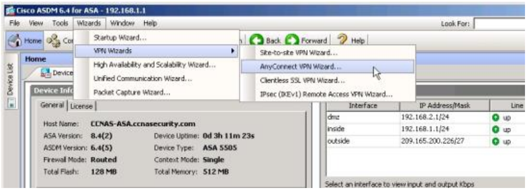
AnyConnect VPN Wizard Example

- The outside host does not have the Cisco AnyConnect client pre-installed.
  - Therefore, the remote user will have to initiate a clientless SSL VPN connection using a web browser, and then download and install the AnyConnect client on the remote host.
- Once installed, the host can exchange traffic with the ASA using a full tunnel SSL VPN connection.



Start the ASDM AnyConnect VPN Wizard

- **Wizards** > **VPN Wizards** > **AnyConnect VPN Wizard**

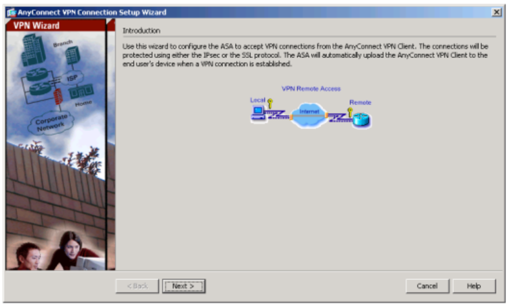

Cisco ASDM 6.4 for ASA - 192.168.1.1
File
View
Tools
Wizards
Window
Help
Look For:
Home
Back
Forward
Help
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
AnyConnect VPN Wizard...
Clientless SSL VPN Wizard...
IPsec (IKEv1) Remote Access VPN Wizard...
Device List
Device Info
General
License

Host Name: **CCNAS-ASA.ccnasecurity.com**
ASA Version: **8.4(2)** Device Uptime: **0d 3h 11m 23s**
ASDM Version: **6.4(5)** Device Type: **ASA 5505**
Firewall Mode: **Routed** Context Mode: **Single**
Total Flash: **128 MB** Total Memory: **512 MB**

Interface	IP Address/Mask	Line
dmz	192.168.2.1/24	up
inside	192.168.1.1/24	up
outside	209.165.200.226/27	up

Select an interface to view input and output Kbps

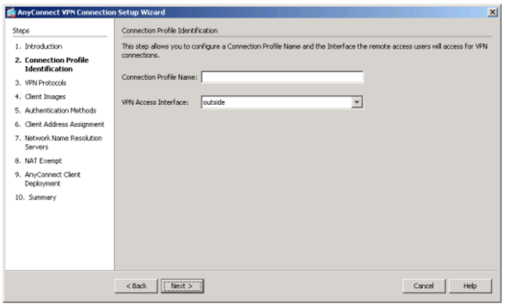
1 - SSL VPN Welcome Window



Introduction

Use this wizard to configure the ASA to accept VPN connections from the AnyConnect VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the AnyConnect VPN Client to the end user's device when a VPN connection is established.

2 - Connection Profile Identification



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

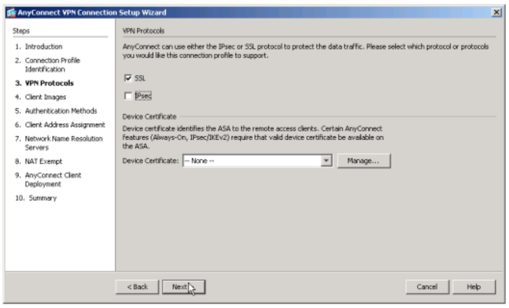
Connection Profile Identification

This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.

Connection Profile Name:

VPN Access Interface: outside

3 - VPN Protocols



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

VPN Protocols

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.

☑ SSL

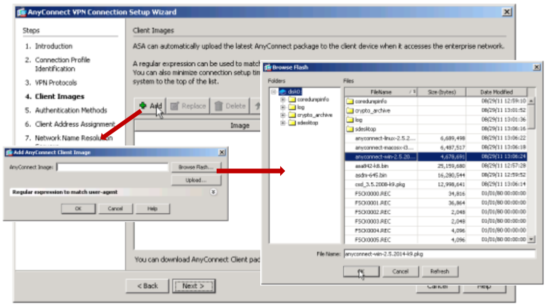
□ IPsec

Device Certificate

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.

Device Certificate: -- None --

4 - Client Images



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

Client Images

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 matc
You can also minimize connection setup tim
system to the top of the list.

You can download AnyConnect Client pac

Add AnyConnect Client Image

AnyConnect Image:

Regular expression to match user-agent

Browse Flash

Folders

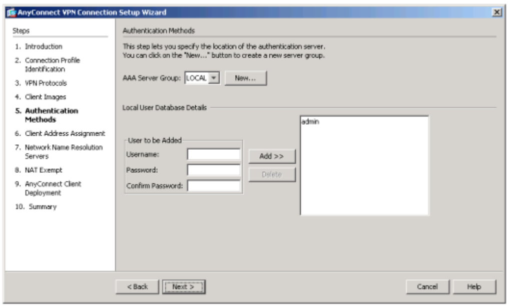
- disk0:
  - coredumpinfo
  - log
  - crypto_archive
  - sdesktop

Files

FileName	Size (bytes)	Date Modified
coredumpinfo		08/29/11 12:59:10
crypto_archive		08/29/11 13:01:52
log		08/29/11 13:01:36
sdesktop		08/29/11 13:06:16
anyconnect-linux-2.5.2...	6,689,498	08/29/11 13:06:22
anyconnect-macosx-i3...	6,487,517	08/29/11 13:06:18
anyconnect-win-2.5.20...	4,678,691	08/29/11 13:06:24
asa842-k8.bin	25,159,680	08/29/11 12:57:28
asdm-645.bin	16,280,544	08/29/11 12:59:52
csd_3.5.2008-k9.pkg	12,998,641	08/29/11 13:06:14
FSCK0000.REC	34,816	01/01/80 00:00:00
FSCK0001.REC	36,864	01/01/80 00:00:00
FSCK0002.REC	2,048	01/01/80 00:00:00
FSCK0003.REC	2,048	01/01/80 00:00:00
FSCK0004.REC	4,096	01/01/80 00:00:00
FSCK0005.REC	4,096	01/01/80 00:00:00

File Name: anyconnect-win-2.5.2014-k9.pkg

5 - Authentication Method



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

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

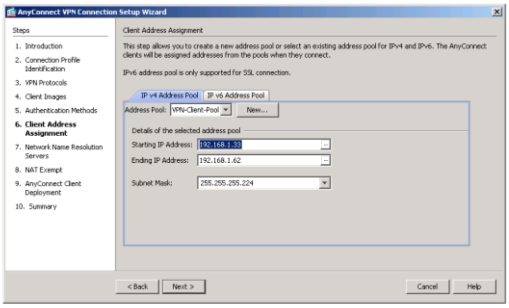
Username:

Password:

Confirm Password:

admin

6 - Client Address Assignment



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 AnyConnect clients will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

Address Pool: VPN-Client-Pool

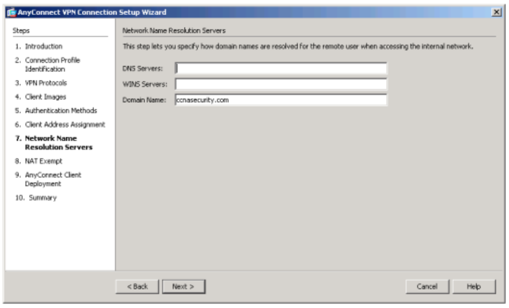
Details of the selected address pool

Starting IP Address: 192.168.1.33

Ending IP Address: 192.168.1.62

Subnet Mask: 255.255.255.224

7 - DNS Configuration


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
< Back
Next >
Cancel
Help

Network Name Resolution Servers

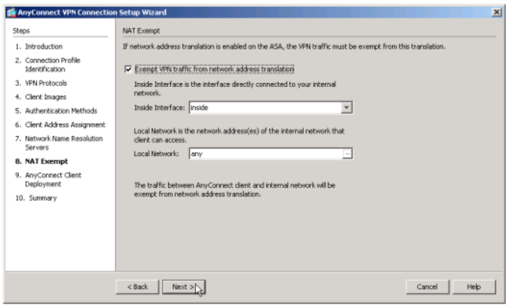
This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers:

WINS Servers:

Domain Name: ccnasecurity.com

8 - NAT Configuration


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
< Back
Next >
Cancel
Help

NAT Exempt

If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

☑ Exempt VPN traffic from network address translation

Inside Interface is the interface directly connected to your internal network.

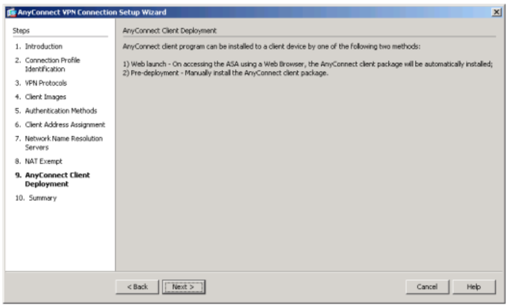
Inside Interface: inside

Local Network is the network address(es) of the internal network that client can access.

Local Network: any

The traffic between AnyConnect client and internal network will be exempt from network address translation.

9 - Client Deployment Message

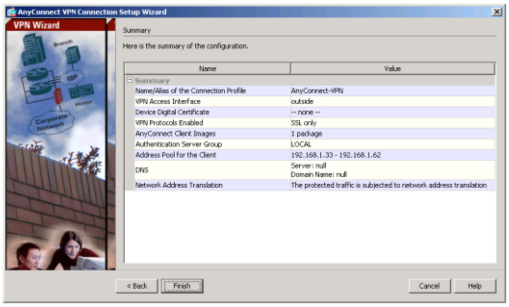

AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

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.

10 - Summary



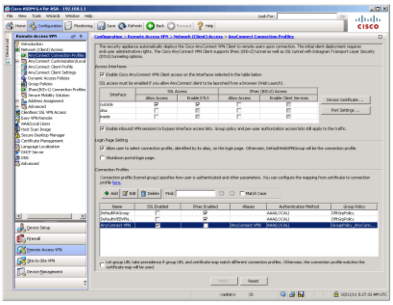
Summary

Here is the summary of the configuration.

Name	Value
⊟ 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	192.168.1.33 - 192.168.1.62
DNS	Server: null Domain Name: null
Network Address Translation	The protected traffic is subjected to network address translation

ASDM Network (Client) Access Window

- **Configurations** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles**



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 requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

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	☑	☑	☐	☐
dmz	☐	☐	☐	☐
inside	☐	☐	☐	☐

Device Certificate ... Port Settings ...

☑ Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

☐ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

Add Edit Delete Find: ☐ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☐	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPN...	☐	☑		AAA(LOCAL)	DfltGrpPolicy
AnyConnect-VPN	☑	☐	AnyConnect-VPN	AAA(LOCAL)	GroupPolicy_AnyConn...

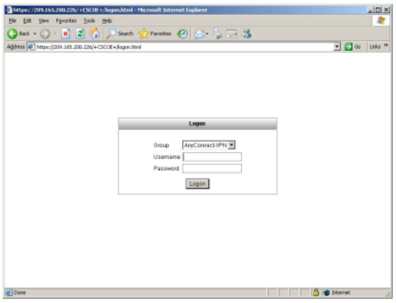
☐ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.

Apply Reset

<admin> 15 10/11/11 5:27:33 AM UTC

Login from the Remote Host

- Open web browser and enter the login URL for the SSL VPN into the address field.


https://209.165.200.226/+CSCOE+/logon.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://209.165.200.226/+CSCOE+/logon.html Go Links
Done Internet

Logon

Group AnyConnect-VPN

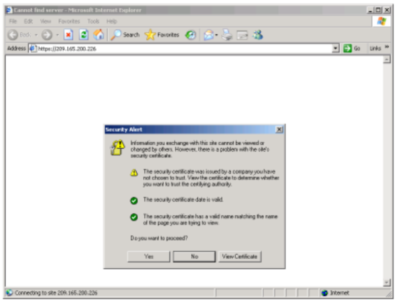
Username

Password

Logon

Accept the Security Certificate (if required)

- The ASA may request confirmation that this is a trusted site.
  - If requested, click **Yes** to proceed.


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://209.165.200.226 Go Links
Connecting to site 209.165.200.226
Internet

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

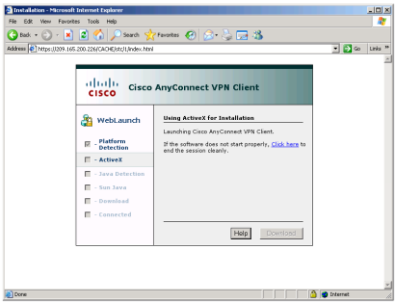
The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Yes No View Certificate

Platform Detection

- The ASA performs a series of compliance checks, platform detection, finally selects / downloads the software package.


Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://209.165.200.226/CACHE/stc/1/index.html Go Links
Done Internet

Cisco AnyConnect VPN Client

WebLaunch

☑ - Platform Detection

☐ - ActiveX

☐ - Java Detection

☐ - Sun Java

☐ - Download

☐ - Connected

Using ActiveX for Installation

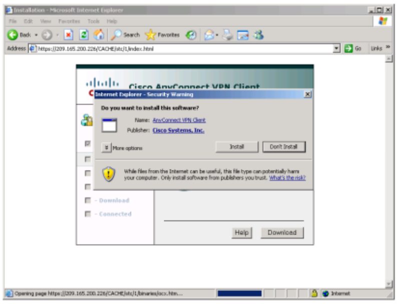
Launching Cisco AnyConnect VPN Client.

If the software does not start properly, Click here to end the session cleanly.

Help Download

Install AnyConnect (if required)

- A security warning will be displayed if AnyConnect must be installed.



Installation - Microsoft Internet Explorer

Address https://209.165.200.226/CACHE/stc/1/index.html

Internet Explorer - Security Warning

Do you want to install this software?

Name: AnyConnect VPN Client

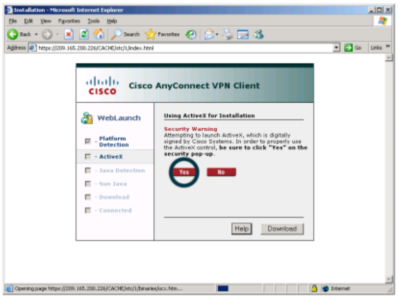
Publisher: Cisco Systems, Inc.

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Opening page https://209.165.200.226/CACHE/stc/1/binaries/ocx.htm...

Detect ActiveX (if required)

- If the AnyConnect client must be downloaded, then ActiveX must be installed and configured to trust the ASA.



Installation - Microsoft Internet Explorer

Address https://209.165.200.226/CACHE/stc/1/index.html

Using ActiveX for Installation

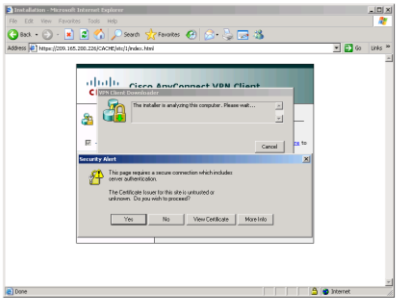
Security Warning

Attempting to launch ActiveX, which is digitally signed by Cisco Systems. In order to properly use the ActiveX control, **be sure to click "Yes" on the security pop-up.**

Opening page https://209.165.200.226/CACHE/stc/1/binaries/ocx.htm...

Add ASA as Trusted Site

- It is important that the security appliance is added as a trusted network site.



Installation - Microsoft Internet Explorer

Address https://209.165.200.226/CACHE/stc/1/index.html

VPN Client Downloader

The installer is analyzing this computer. Please wait...

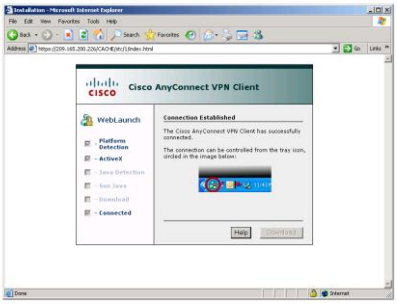
Security Alert

This page requires a secure connection which includes server authentication.

The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?

Auto-Download Complete

- After the client completes the auto-download, the web session will automatically launch the Cisco AnyConnect SSL VPN Client.



Installation - Microsoft Internet Explorer

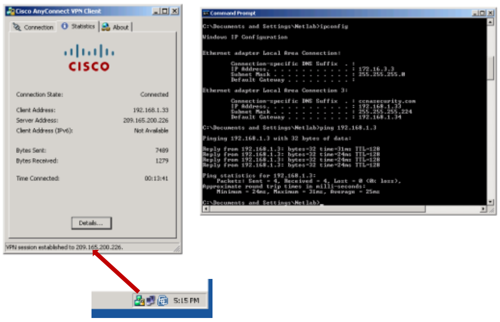
Address https://209.165.200.226/CACHE/stc/1/index.html

Connection Established

The Cisco AnyConnect VPN Client has successfully connected.

The connection can be controlled from the tray icon, circled in the image below:

Confirm Connectivity



Cisco AnyConnect VPN Client

Connection State: Connected
Client Address: 192.168.1.33
Server Address: 209.165.200.226
Client Address (IPv6): Not Available
Bytes Sent: 7489
Bytes Received: 1279
Time Connected: 00:13:41
VPN session established to 209.165.200.226.

Command Prompt

```
C:\Documents and Settings\Netlab>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.16.3.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection 3:

        Connection-specific DNS Suffix  . : ccnasecurity.com
        IP Address. . . . . . . . . . . . : 192.168.1.33
        Subnet Mask . . . . . . . . . . . : 255.255.255.224
        Default Gateway . . . . . . . . . : 192.168.1.34

C:\Documents and Settings\Netlab>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=31ms TTL=128
Reply from 192.168.1.3: bytes=32 time=24ms TTL=128
Reply from 192.168.1.3: bytes=32 time=24ms TTL=128
Reply from 192.168.1.3: bytes=32 time=24ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 31ms, Average = 25ms

C:\Documents and Settings\Netlab>_
```

AnyConnect Wizard Generated Output

- The generated output from the AnyConnect VPN Wizard.

```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK_OBJ_192.168.1.32_27 NETWORK_OBJ_192.168.1.32_27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```

AnyConnect Wizard Generated Output

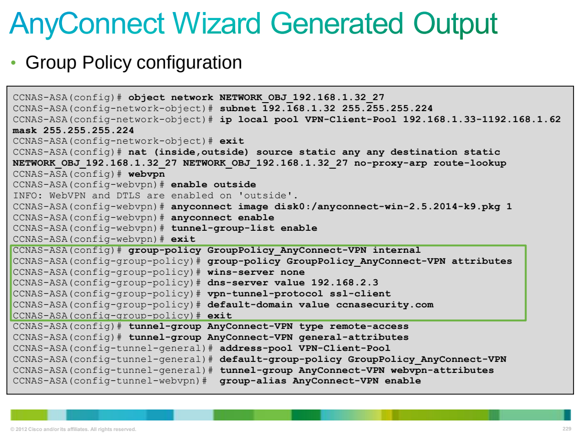
- NAT configuration

```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK_OBJ_192.168.1.32_27 NETWORK_OBJ_192.168.1.32_27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```

AnyConnect Wizard Generated Output

- WebVPN Configuration

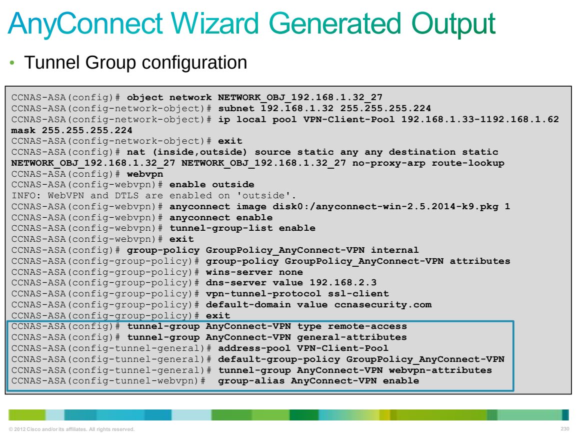
```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK_OBJ_192.168.1.32_27 NETWORK_OBJ_192.168.1.32_27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```



AnyConnect Wizard Generated Output

- Group Policy configuration

```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK_OBJ_192.168.1.32_27 NETWORK_OBJ_192.168.1.32_27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```



AnyConnect Wizard Generated Output

- Tunnel Group configuration

```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK_OBJ_192.168.1.32_27 NETWORK_OBJ_192.168.1.32_27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```