# CCNA Security 2.0 Study Material – Chapter 9: Implementing the Cisco Adaptive Security Appliance

itexamanswers.net/ccna-security-2-0-study-material-chapter-9-implementing-cisco-adaptive-security-appliance.html

October 9, 2017

## Chapter Outline:



## Section 9.1: Introduction to the ASA

### Upon completion of this section, you should be able to:

- Compare ASA solutions to other routing firewall technologies.
- Explain ASA 5505 operation with the default configuration.

### Topic 9.1.1: ASA Solutions

#### ASA Firewall Models

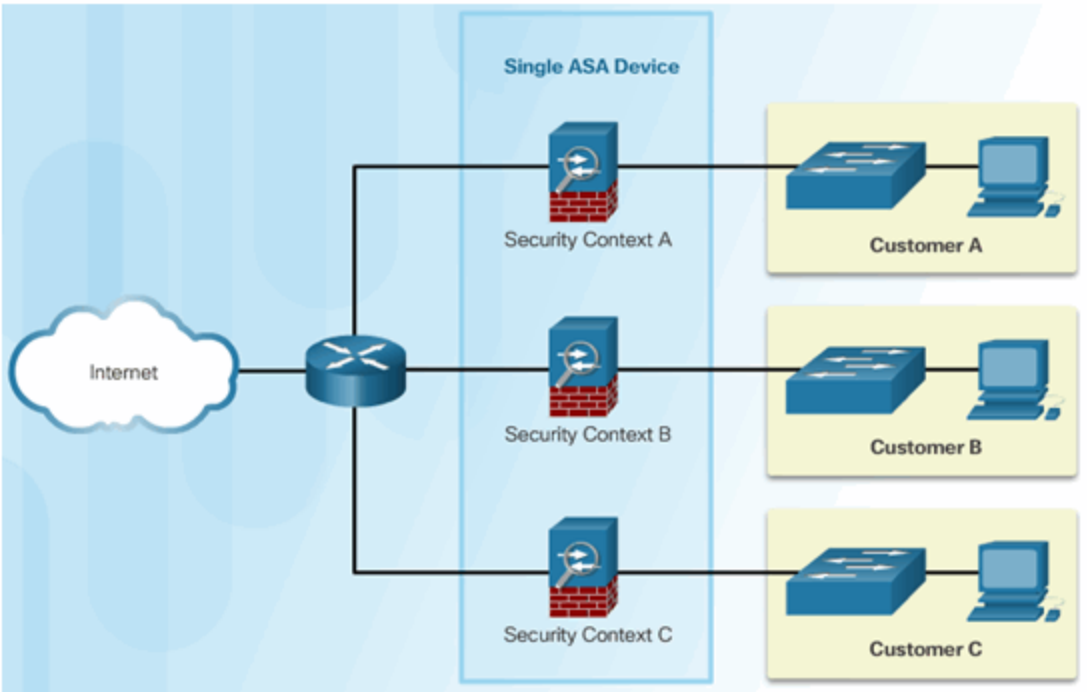
Small Office and Branch Office ASA Models


Internet Edge Models

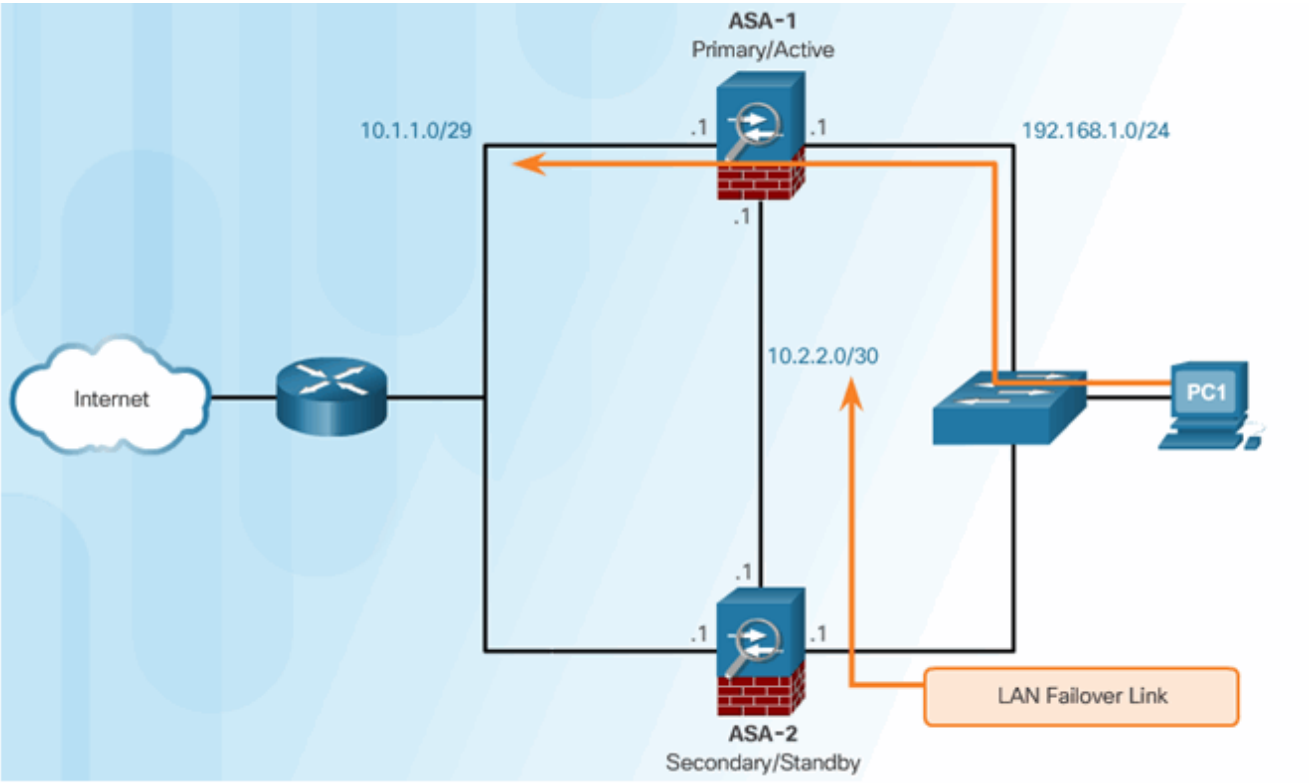

Enterprise Data Center Models


## Advanced ASA Firewall Feature

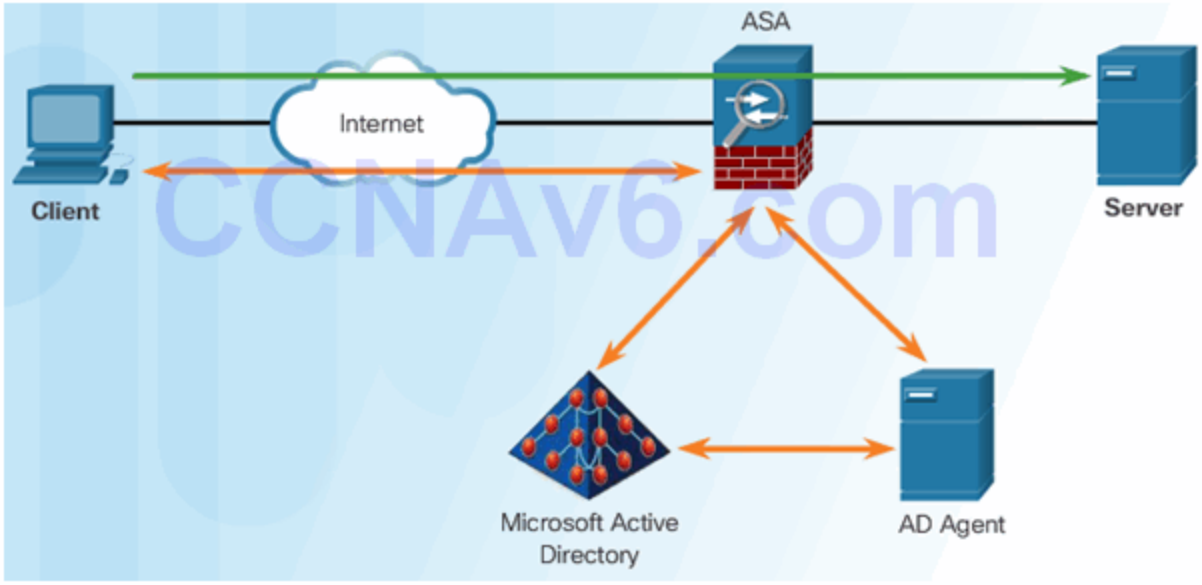
ASA Virtualization



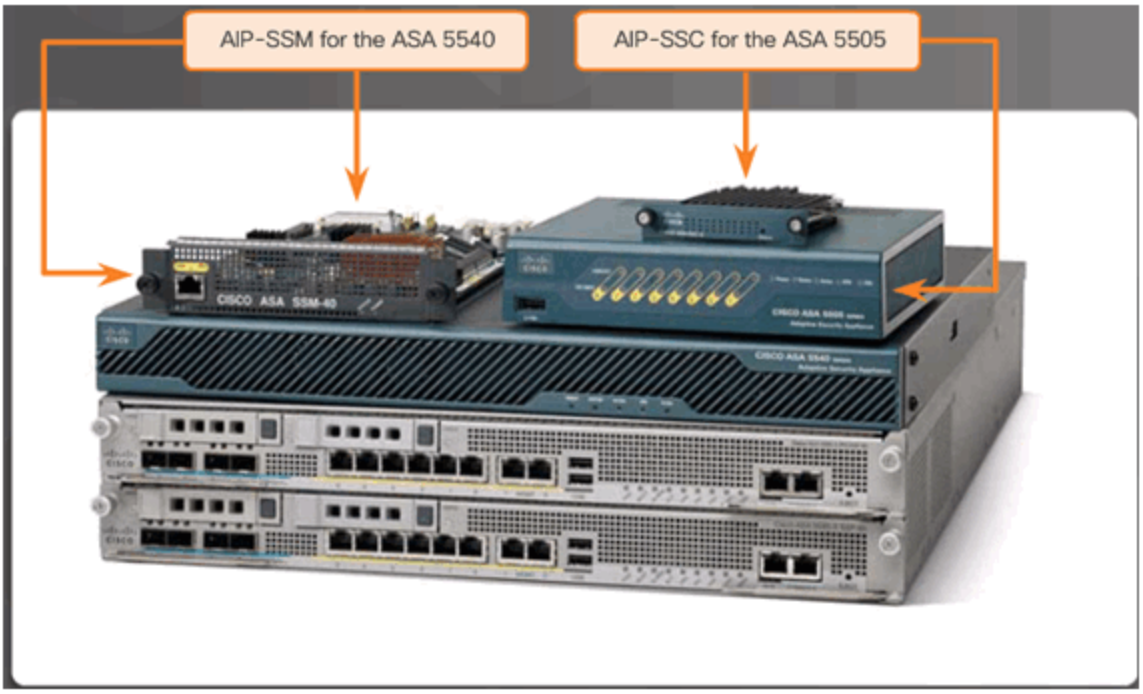

High Availability




Identity Firewall

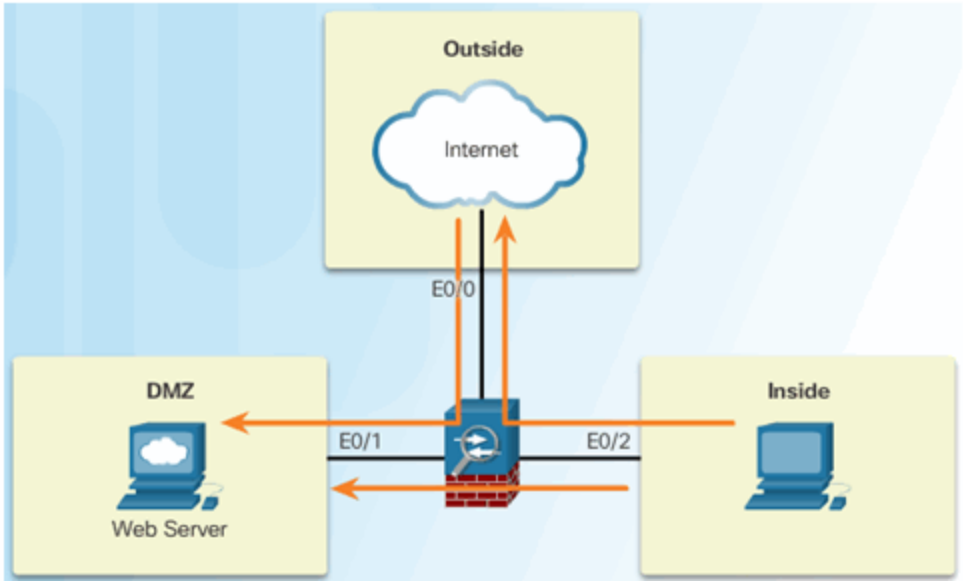



ASA Threat Control

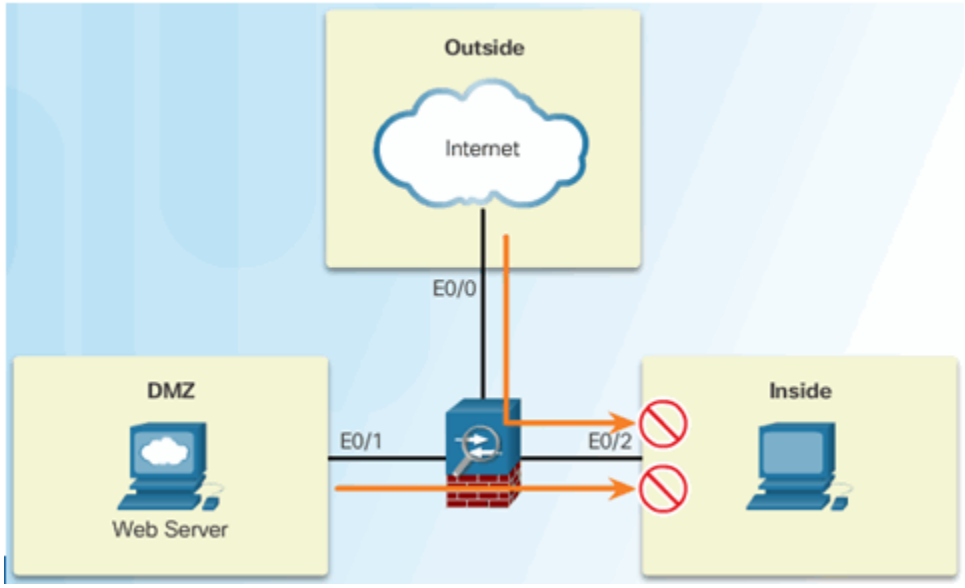



## Review of Firewalls in Network Design

Permitted Traffic



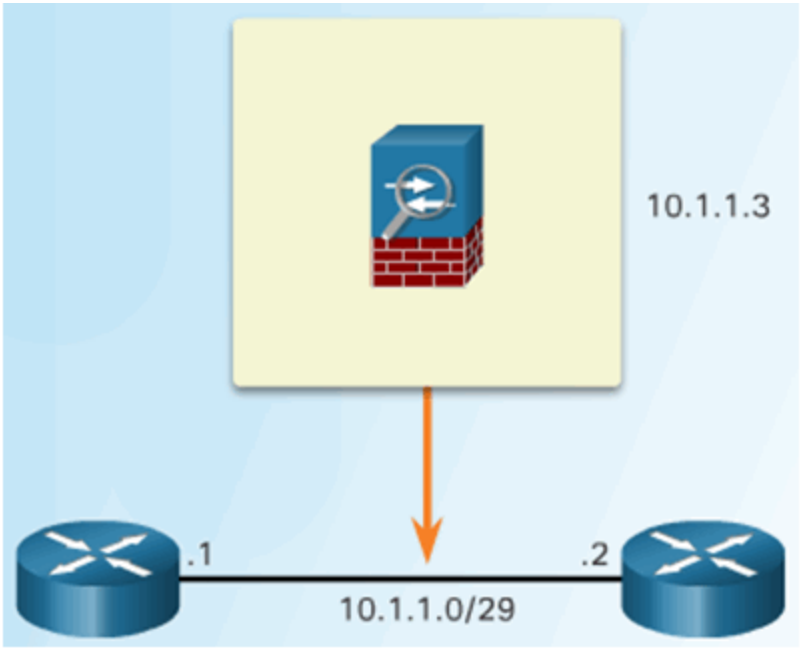

DeniedTraffic




## ASA Firewall Modes of Operation

Routed Mode

Transparent Mode




## ASA Licensing Requirements

Base License Specifics

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

Security Plus License Specifics

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

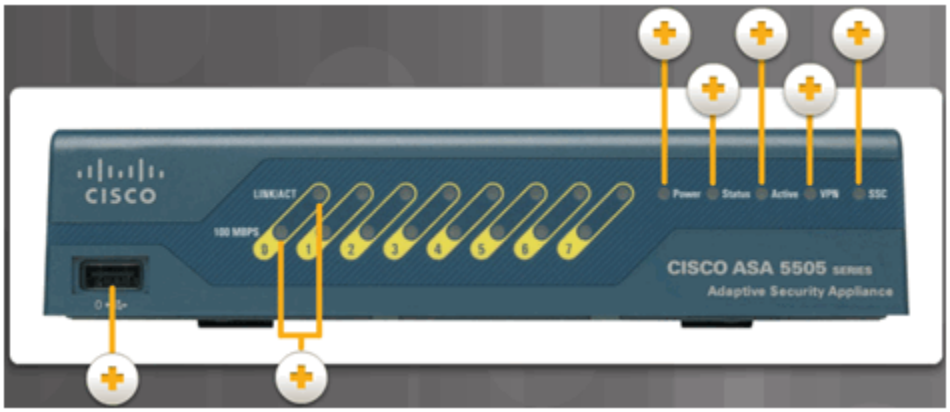
show version Command Output

```
CCNAS-ASA# 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
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 10             perpetual
Total VPN Peers                   : 12             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
Cluster                           : Disabled       perpetual

This platform has a Base license.
```

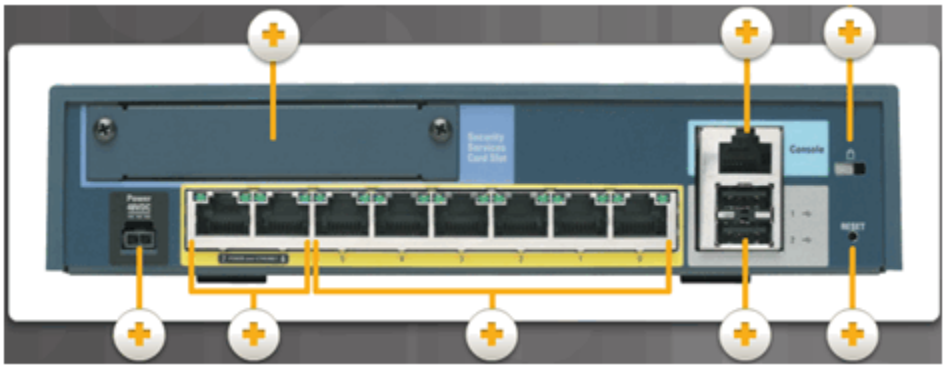
## Topic 9.1.2: Basic ASA Configuration

### Overview of ASA 5505

ASA 5505 Back Panel



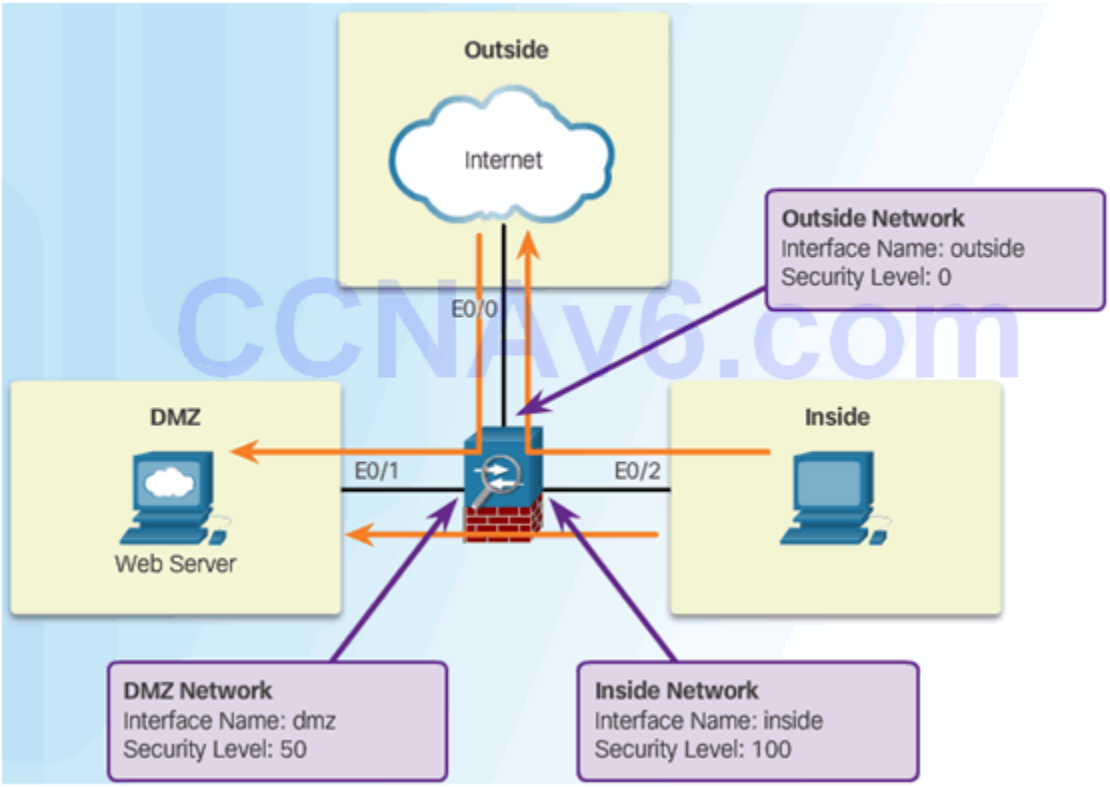

ASA 5505 Front Panel



## ASA Security Levels

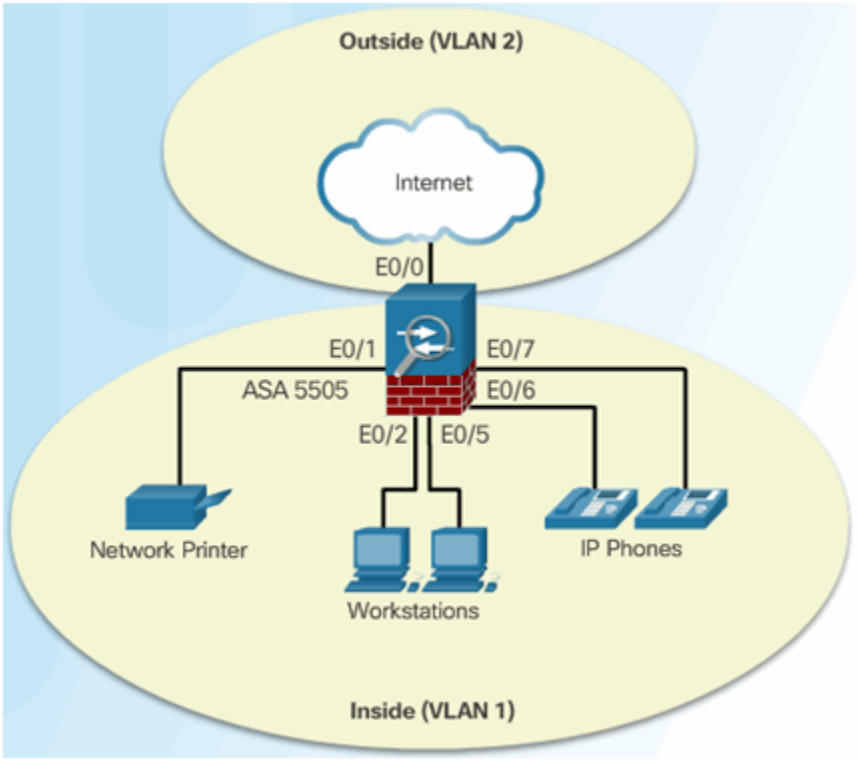
Security Level Control:

- Network Access
- Inspection Engines
- Application Filtering

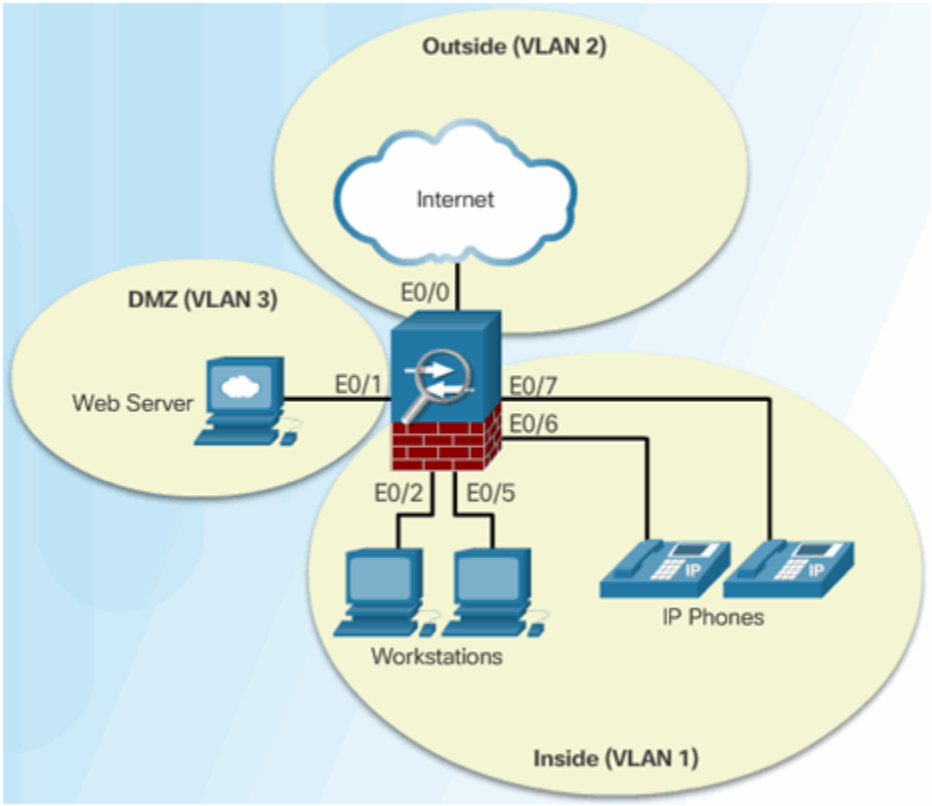



## ASA 5505 Deployment Scenarios

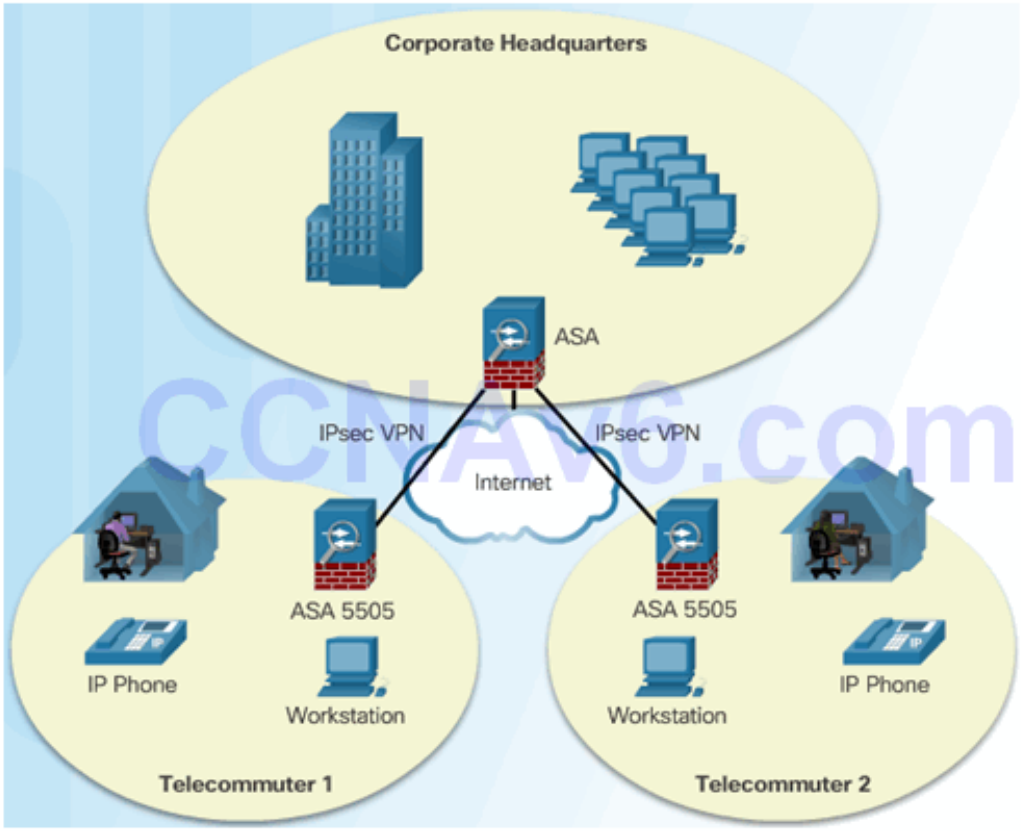
ASA Deployment in a Small Branch




ASA Deployment in a Small Business




ASA Deployment in an Enterprise




## Section 9.2: ASA Firewall Configuration

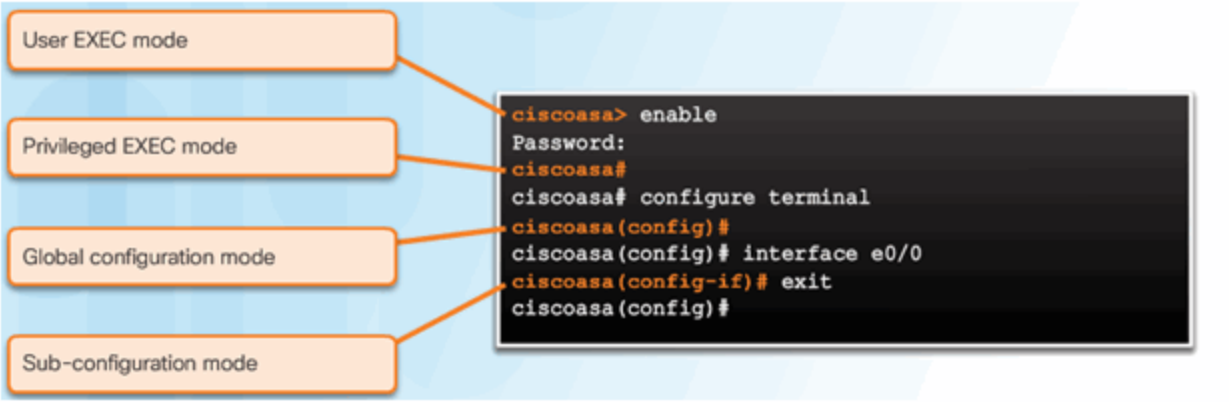
**Upon completion of this section, you should be able to:**

- Explain what ASA firewall services are enabled using the default configuration.
- Configure an ASA to provide basic firewall services.
- Configure object groups on an ASA.
- Configure access lists with object groups on an ASA.
- Configure an ASA to provide NAT services.
- Configure access control using the local database and AAA server.
- Explain how the Cisco Modular Framework (MPF) is used to configure ASA policies.

## Topic 9.2.1: The ASA Firewall Configuration

### Introduce Basic ASA Settings

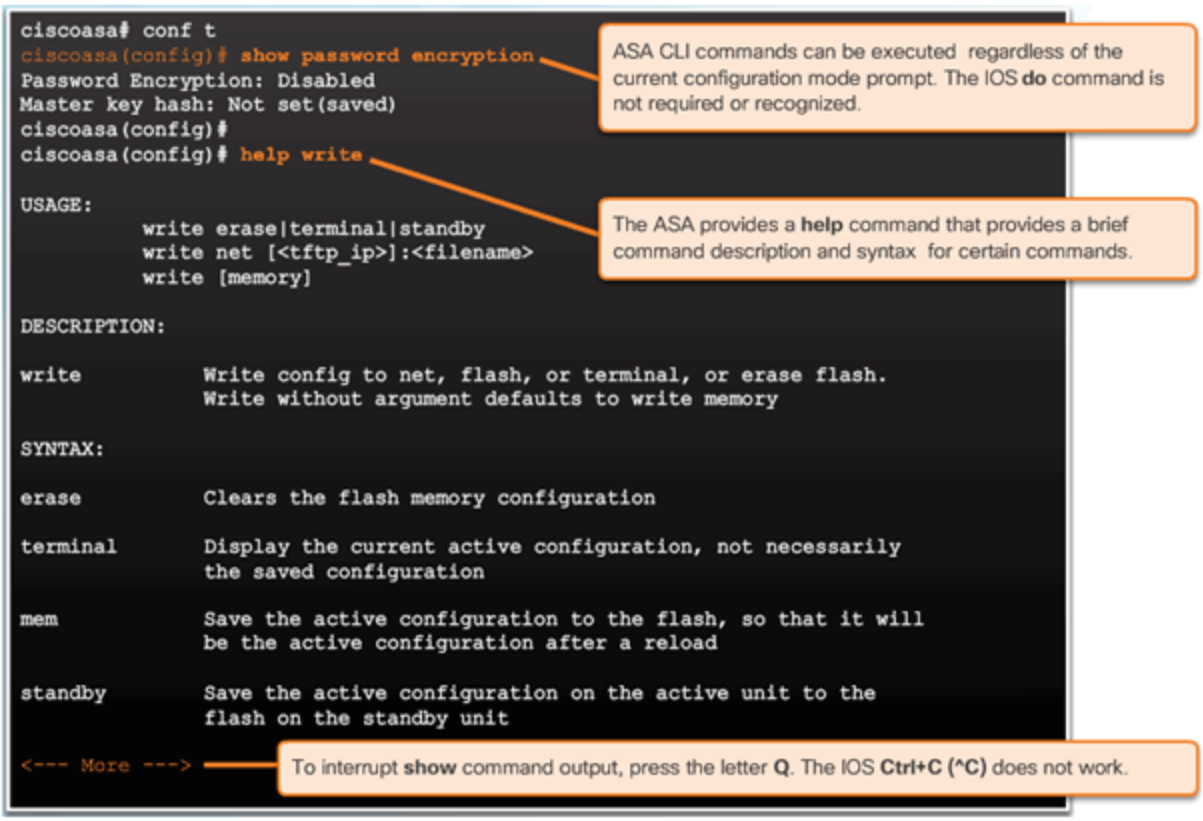
Base License Specifics




Security Plus License Specifics

| IOS Router Command | Equivalent ASA Command |
|---|---|
| `enable secret` *password* | `enable password` *password* |
| `line vty 0 - 4`<br>`password` *password*<br>`login` | `passwd` *password* |
| `ip route` | `route outside` |
| `show ip interfaces brief` | `show interfaces 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` |

show version Command Output




## ASA Default Configuration

ASA 5505 Default Configuration Overview.

### ASA Interactive Setup Initialization Wizard

Entering the ASA 5505 Setup Initialization Wizard


## Topic 9.2.2: Configuring Management Settings and Services

### Enter Global Configuration Mode

Entering Global Configuration Mode Example

```
ciscoasa> enable
Password:
ciscoasa#
ciscoasa# clock set 12:00:00 1 April 2015
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)#

*************************** NOTICE ***************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: A
You will be reminded again in 7 days.

If you would like to enable this feature, issue the command
"call-home reporting anonymous".

Please remember to save your configuration.

ciscoasa(config)#
```

## Configuring Basic Settings

ASA Basic Configuration Commands

| ASA Command | Description |
|---|---|
| **hostname** *name* | • Specifies a hostname up to 63 characters.<br>• A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen. |
| **domain-name** *name* | • Sets the default domain name |
| **enable password** *password* | • Sets the enable password for privileged EXEC mode.<br>• Sets the password as a case-sensitive string of 3 to 32 alphanumeric and special characters (not including a question mark or a space). |
| **banner motd** *message* | • Provides legal notification and configures the system to display a message-of-the-day banner when connecting to the ASA |
| **key config-key password-encryption** [ *new-pass* [ *old-pass* ] ] | • Sets the passphrase between 8 and 128 character long.<br>• Used for generation the encryption key. |
| **password encryption aes** | • Enables password encryption and encrypts all user passwords. |

Configuring Basic Settings

```
ciscoasa(config)# hostname CCNAS-ASA
CCNAS-ASA(config)# domain-name ccnasecurity.com
CCNAS-ASA(config)# enable password class
CCNAS-ASA(config)#
CCNAS-ASA(config)# banner motd ------------------------------------------------
CCNAS-ASA(config)# banner motd     Authorized access only!
CCNAS-ASA(config)# banner motd     You have logged into a secure device.
CCNAS-ASA(config)# banner motd ------------------------------------------------
CCNAS-ASA(config)# banner motd
CCNAS-ASA(config)# exit
CCNAS-ASA# exit

Logoff

------------------------------------------------------------
    Authorized access only!
    You have logged into a secure device.
------------------------------------------------------------


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

Enabling AES Encryption Example

```
CCNAS-ASA# show password encryption
Password Encryption: Disabled
Master key hash: Not set(saved)
CCNAS-ASA#
CCNAS-ASA# conf t
CCNAS-ASA(config)# key config-key password-encryption cisco123
CCNAS-ASA(config)# password encryption aes
CCNAS-ASA(config)# exit
CCNAS-ASA#
CCNAS-ASA# show password encryption
Password Encryption: Enabled
Master key hash: 0x45ebef8e 0x77a0f287 0x90247f80 0x2a184246 0xe85cbcc4(not saved)
CCNAS-ASA#
CCNAS-ASA# write
Building configuration...
Cryptochecksum: 99934042 e6c6b12b 607a9920 89d8a181

2359 bytes copied in 1.340 secs (2359 bytes/sec)
[OK]
CCNAS-ASA#
```

## Configuring Logical VLAN Interfaces

Local VLAN Interface Commands

| ASA Command | Description |
|---|---|
| `interface vlan` *vlan-number* | • Enters VLAN interface configuration mode. |
| `nameif` *if_name* | • Names the interface using a text string of up to 48 characters.<br>• The name is not case-sensitive.<br>• You can change the name by re-entering this command with a new value.<br>• Do not enter the no form, because that command causes all commands that refer to that name to be deleted. |
| `security-level` *value* | • Sets the security level, where number is an integer between 0 (lowest) and 100 (highest). |



Configuring IP Addresses on VLAN Interfaces

| To Configure | ASA Command | Description |
|---|---|---|
| Manually | `ip address` *ip-address netmask* | • Assigns an IP address to the interface. |
| Using DHCP | `ip address dhcp` | • Used to have the interface request an IP address configuration from the upstream device. |
| | `ip address dhcp setroute` | • Used to have the interface request and install a default route to the upstream device. |
| Using PPPOE | `ip address pppoe` | • Interface configuration mode command that requests an IP address from the upstream device. |
| | `ip address pppoe setroute` | • Same command but it also requests and installs a default route to the upstream device. |

Configuring VLAN Interfaces Example

```
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)#
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)#
```

## Assigning Layer 2 Ports to VLANs

Configuring Layer 2 Ports Example

```
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)#
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)#
```

Verifying VLAN Port Assignment Example

```
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#
```

Verifying Interfaces Example

```
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  up                    up
Ethernet0/3                unassigned      YES unset  up                    up
Ethernet0/4                unassigned      YES unset  down                  down
Ethernet0/5                unassigned      YES unset  down                  down
Ethernet0/6                unassigned      YES unset  down                  down
Ethernet0/7                unassigned      YES unset  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                      209.165.200.226 YES manual up                    up
Virtual0                   127.1.0.1       YES unset  up                    up
CCNAS-ASA#
```

Verifying IP Addresses Example

```
CCNAS-ASA# show ip address
System IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   manual
Vlan2                  outside             209.165.200.226 255.255.255.248 manual
Current IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   manual
Vlan2                  outside             209.165.200.226 255.255.255.248 manual
CCNAS-ASA#
```

## Configuring a Default Static Route

```
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNAS-ASA(config)#
CCNAS-ASA(config)# show route | begin Gateway
Gateway of last resort is 209.165.200.225 to network 0.0.0.0

S*    0.0.0.0 0.0.0.0 [1/0] via 209.165.200.225, outside
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
C        209.165.200.224 255.255.255.248 is directly connected, outside
L        209.165.200.226 255.255.255.255 is directly connected, outside

CCNAS-ASA(config)#
```

## Configuring Remote Access Services

Telnet Configuration Commands

| ASA Command | Description |
|---|---|
| `{passwd \| password}` *password* | • Sets the login password up to 80 characters in length for Telnet. |
| `telnet` {*ipv4_address mask* \| *ipv6_address/prefix*} *if_name* | • Identifies which inside host or network can Telnet to the ASA interface.<br>• Use the `clear configure telnet` command to remove the Telnet connection. |
| `telnet timeout` *minutes* | • By default, Telnet sessions left idle for five minutes are closed by the ASA.<br>• The command alters the default exec timeout of five minutes. |
| `aaa authentication telnet console LOCAL` | • Configures Telnet to refer to the local database for authentication.<br>• The `LOCAL` keyword is case sensitive and is a predefined server tag. |
| `clear configure telnet` | • Removes the Telnet connection from the configuration. |



Telnet Configuration Commands Example

```
CCNAS-ASA(config)# password cisco
CCNAS-ASA(config)# telnet 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# telnet timeout 3
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run telnet
telnet 192.168.1.3 255.255.255.255 inside
telnet timeout 3
CCNAS-ASA(config)#
```

SSH Configuration Commands

| ASA Command | Description |
|---|---|
| `username` *name* `password` *password* | • Creates a local database entry. |
| `aaa authentication ssh console LOCAL` | • Configures SSH to refer to the local database for authentication.<br>• The `LOCAL` keyword is case sensitive and is a predefined server tag. |
| `crypto key generate rsa modulus` *modulus_size* | • Generates the RSA key required for SSH encryption.<br>• The `modulus_size` (in bits) can be 512, 768, 1024, or 2048.<br>• A value of 2048 is recommended. |
| `ssh` {*ip_address mask* \| *ipv6_address/prefix*} *if_name* | • Identifies which inside host or network can SSH to the ASA interface.<br>• Multiple commands can be in the configuration.<br>• If the `if_name` is not specified, SSH is enabled on all interfaces except the outside interface.<br>• Use the clear configure ssh command to remove the SSH connection. |
| `ssh version` *version_number* | • (Optional) By default, the ASA allows both SSH Version 1 (less secure) and Version 2 (more secure).<br>• Enter this command in order to restrict the connections to a specific version. |
| `ssh timeout` *minutes* | • Alters the default exec timeout of five minutes. |



Configuring SSH Access Example

```
CCNAS-ASA(config)# username ADMIN password class
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
CCNAS-ASA(config)#
CCNAS-ASA(config)# crypto key generate rsa modulus 2048
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)#
CCNAS-ASA(config)# ssh 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# ssh 192.168.1.4 255.255.255.255 inside
CCNAS-ASA(config)# ssh 172.16.1.3 255.255.255.255 outside
CCNAS-ASA(config)#
CCNAS-ASA(config)# ssh version 2
CCNAS-ASA(config)#
CCNAS-ASA(config)# show ssh
Timeout: 5 minutes
Version allowed: 2
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
172.16.1.3 255.255.255.255 outside
CCNAS-ASA(config)#
```

### Configuring Network Time Protocol Services

NTP Authentication Commands

| ASA Command | Description |
|---|---|
| `ntp authenticate` | • Enables authentication with an NTP server. |
| `ntp trusted-key` *key_id* | • Specifies an authentication key ID to be a trusted key, which is required for authentication with an NTP server. |
| `ntp authentication-key` *key_id* `md5` *key* | • Sets a key to authenticate with an NTP server. |
| `ntp server` *ip_address* [`key` *key_id*] | • Identifies an NTP server. |

Configuring NTP Example

```
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.100
ERROR: % Incomplete command
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 lease 1800
CCNAS-ASA(config)#
```

## Topic 9.2.3: Object Groups

### Introduction to Objects and Object Groups

```
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)#
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)#
```

## Configuring Network Objects

Network Object Commands

| ASA Command | Description |
|---|---|
| **host** *ip-addr* | • Assigns an IP address to the named object. |
| **subnet** *net-address net-mask* | • Assigns a network subnet to the named object. |
| **range** *ip-addr-1 ip-addr-n* | • Assigns IP addresses in a range |



Configuring a Network Object Example

```
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.3
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object network EXAMPLE-1
 host 192.168.1.3
CCNAS-ASA(config)#
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 Service Objects

Service Object Options Example

```
CCNAS-ASA(config)# object service EXAMPLE-2
CCNAS-ASA(config-service-object)#
CCNAS-ASA(config-service-object)# service ?

service-object mode commands/options:
  <0-255>  Enter protocol number (0 - 255)
  ah
  eigrp
  esp
  gre
  icmp
  icmp6
  igmp
  igrp
  ip
  ipinip
  ipsec
  nos
  ospf
  pcp
  pim
  pptp
  snp
  tcp
  udp

configure mode commands/options:
  call-home          Enable or disable Smart Call-Home
```

Common Service Object Commands

| ASA Command | Description |
|---|---|
| **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 Example

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

## Object Groups


## Configuring Common Object Groups

Network Object Group Example

```
CCNAS-ASA(config)# object-group network ADMIN-HOST
CCNAS-ASA(config-network-object-group)# description Administrative hosts
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)# description All inside 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)#
```

ICMP-type Object Group Example

```
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)#
```

Services Object Group Example

```
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 tcp destination eq pop3
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 www
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)#
```

## Topic 9.2.4: ACLS

### ASA ACLs

ASA ACL and IOS ACL Similarities

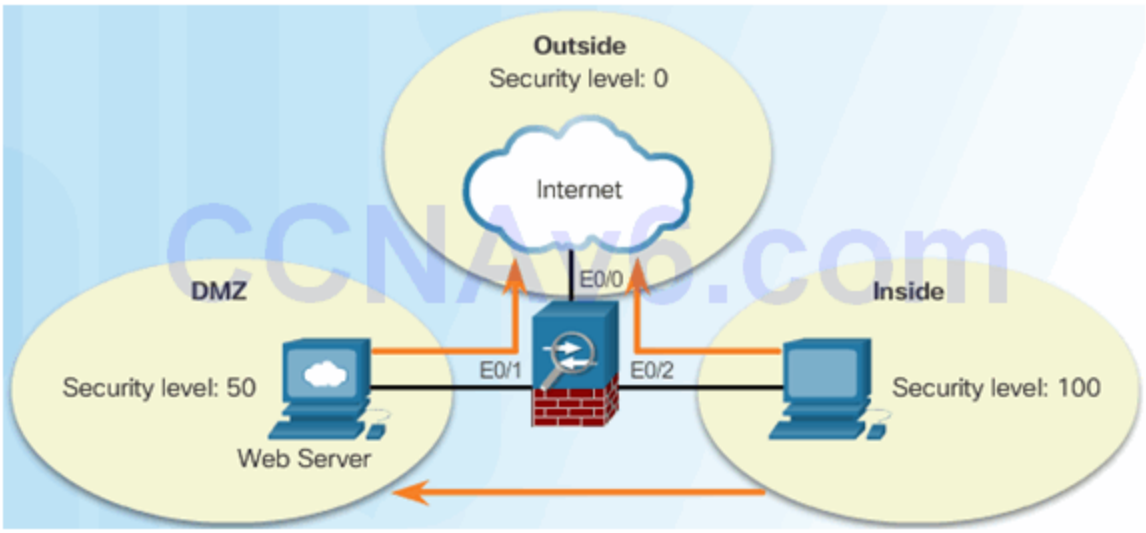
- ACLs are made up of one or more ACEs. An ACE is a single entry in an access list that specifies a permit or deny rule (to forward or drop the packet) and is applied to a protocol, to a source and destination IP address or network, and, optionally, to the source and destination ports.
- ACLs are processed sequentially from top down.
- A criteria match will cause the ACL to be exited.
- There is an implicit deny all at the bottom.
- Remarks can be added per ACE or ACL.
- Only apply one access list per interface, per protocol, per direction.
- ACLs can be enabled/disabled based on time ranges.

ASA ACL and IOS ACL Similarities

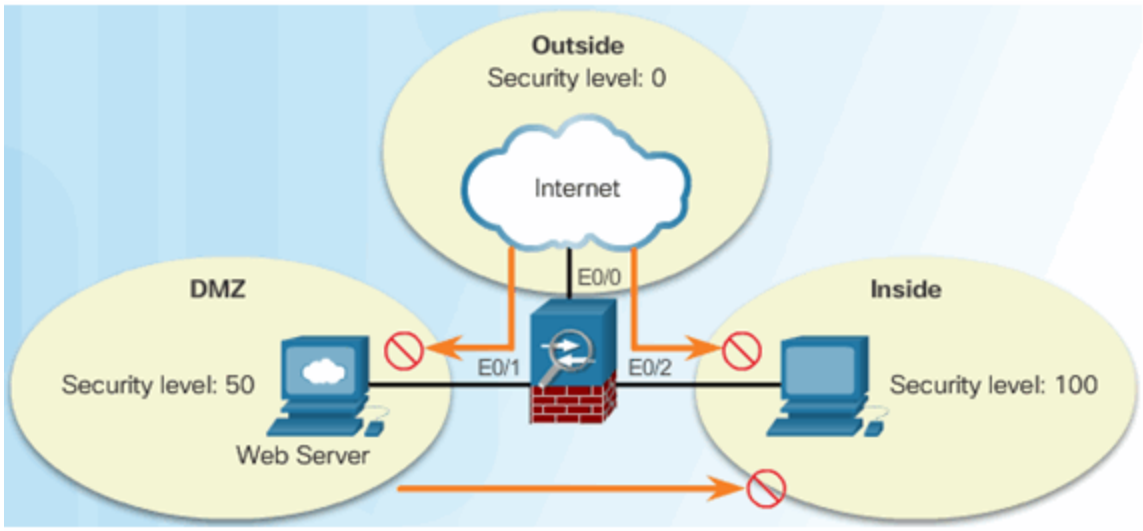
- The ASA uses a network mask (e.g., 255.255.255.0) and not a wildcard mask (e.g. 0.0.0.255).
- ACLs are always named instead of numbered.
- By default, interface security levels apply access control without an ACL configured.

## Types of ASA ACL Filtering

Higher Levels Allowed To Lower Levels




Lower Levels Denied To Higher Levels




## Types of ASA ACLs

Extended ACL Examples

| ACL Use | Description |
| --- | --- |
| Control network access for IP traffic | • The ASA does not allow any traffic from a lower security interface to a higher security interface unless it is explicitly permitted by an extended access list. |
| Identify traffic for AAA rules | • AAA rules use access lists to identify traffic. |
| Identify addresses for NAT | • Policy NAT lets you identify local traffic for address translation by specifying the source and destination addresses in an extended access list. |
| Establish VPN access | • Extended access list can be used in VPN commands. |
| Identify traffic for Modular Policy Framework (MPF) | • Access lists can be used to identify traffic in a class map, which is used for features that support MPF.<br>• Features that support Modular Policy Framework include TCP and general connection settings, and inspection. |

Standard ACL Example

| ACL Use | Description |
| --- | --- |
| Identify OSPF destination network | • Standard access lists include only the destination address.<br>• It can be used to control the redistribution of OSPF routes. |

IPv6 ACL Example

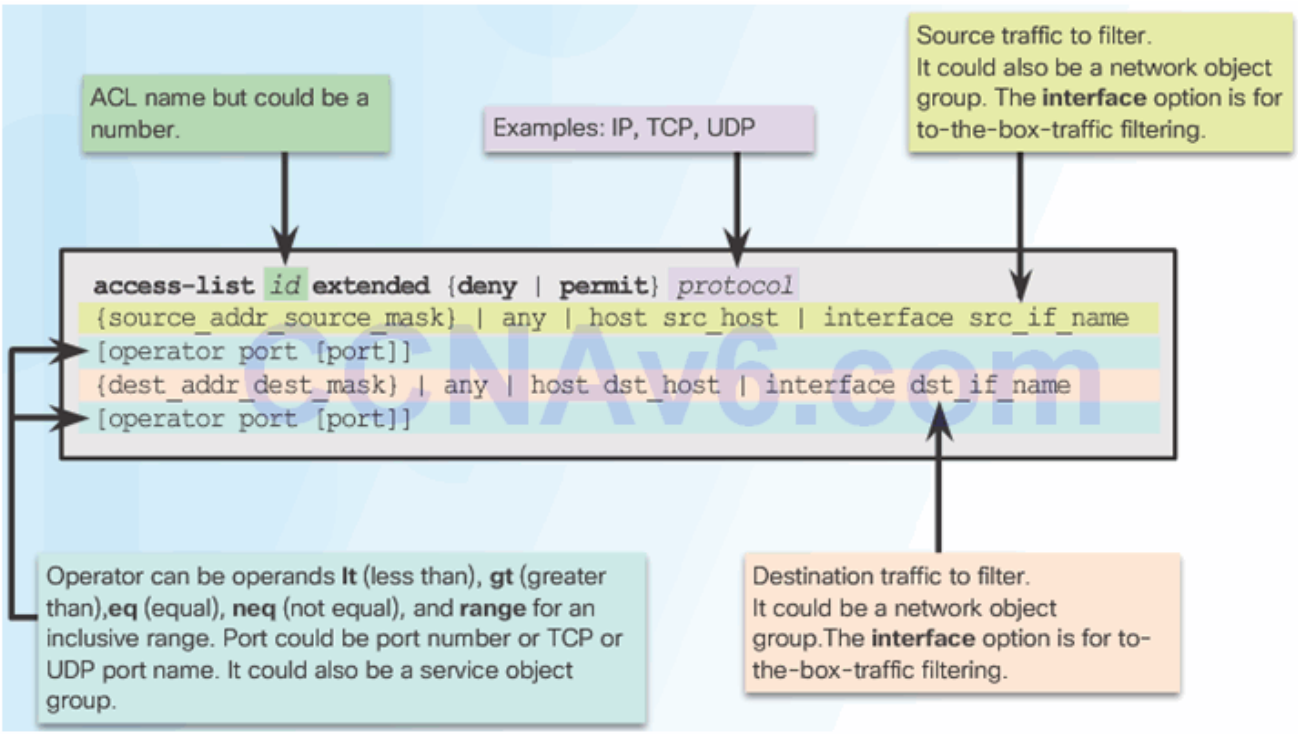
| ACL Use | Description |
| --- | --- |
| Control network access for IPv6 networks | • Can be used to add and apply access lists to control traffic in IPv6 networks. |

## Configuring ACLs

ACL Command Parameters

```
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>]
                      [security-group {name <sgname> | tag <sgt>} |
                          object-group-security <security_obj_grp_id>]
                      {host <sip> | <sip> <smask> | <sip-prefix> |
                      interface <ifc> | any | any4 | any6
                      object-group <network_obj_grp_id> |
                      object <network_obj_name>}
                      [<operator> <port> [<port>] |
                      object-group <service_obj_grp_id>]
                      [security-group {name <sgname> | tag <sgt>} |
                          object-group-security <security_obj_grp_id>]
                      {host <dip> | <dip> <dmask> | <dip-prefix> |
                      interface <ifc> | any | any4 |any6
<--- More --->
```

Condensed Extended ACL Syntax




ASA ACL Elements

| Element | Description |
| --- | --- |
| **ACL id** | • The name of the ACL. It can be any alphanumeric name up to 241 characters. |
| **Action** | • Can be **permit** or **deny**. |
| **Protocol number - Source** | • Can be **ip** for all traffic, or the name / IP protocol number (0-250) including **icmp** (**1**), **tcp** (**6**), **udp** (**17**), or a protocol object-group. |
| **Source** | • Identifies the source and can be **any**, a **host**, a network, or a network object group.<br>• For to-the-box-traffic filtering, the **interface** keyword is used to specify the source interface of the ASA. |
| **Source port operator** | • (Optional) Operand is used in conjunction with the source port.<br>• Valid operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** for an inclusive range. |
| **Source port** | • (Optional) Can be the actual TCP or UDP port number, select port name, or service object group. |
| **Destination** | • Identifies the destination and like the source, it can be **any**, a **host**, a network, or a network object group.<br>• For to-the-box-traffic filtering, the **interface** keyword is used to specify the destination interface of the ASA. |
| **Destination port operator** | • (Optional) Operand is used in conjunction with the destination port.<br>• Valid operands are the same as the source port operands. |
| **Destination port** | • (Optional) Can be the actual TCP or UDP port number, select port name, or service object group. |
| **Log** | • Can set elements for syslog including severity level and log interval. |
| **Time range** | • (Optional) Specify a time range for this ACE. |

## Applying ACLs

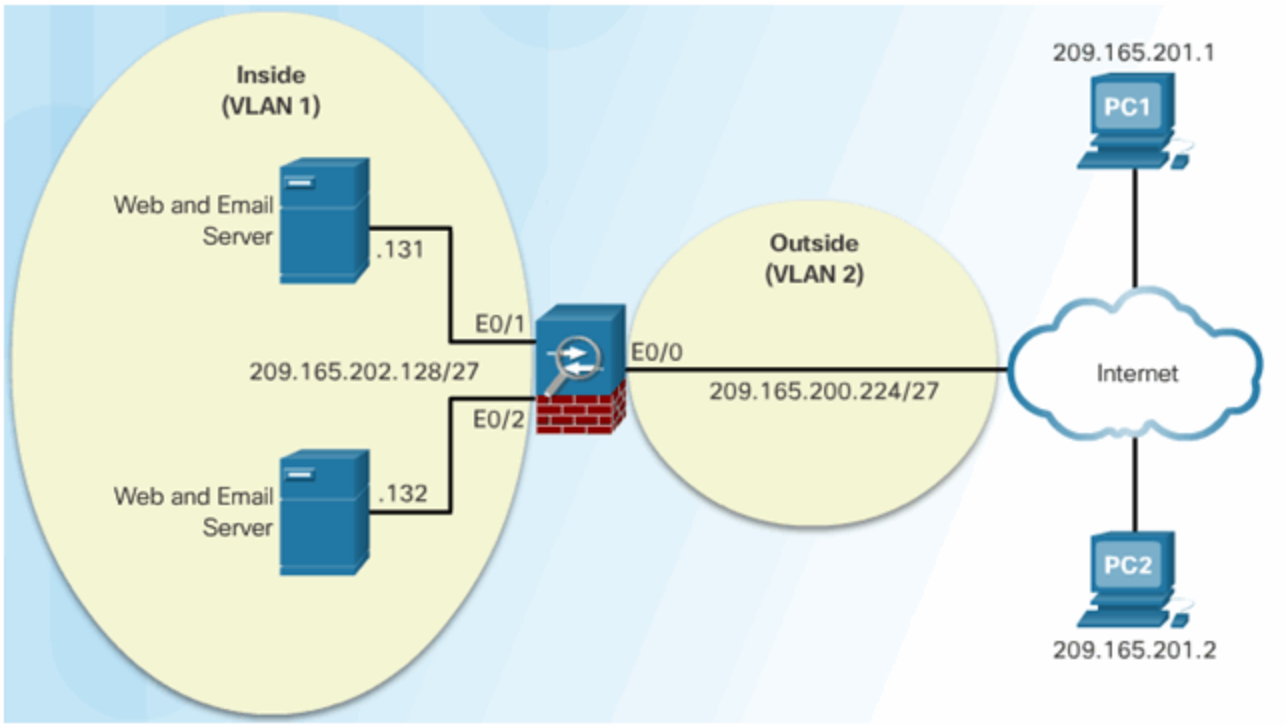
access-group Command Syntax

```
access-group id { in | out } interface if_name [ per-user-override | control-plane ]
```

| Syntax | Description |
|---|---|
| **access-group** | Keyword used to apply an ACL to an interface. |
| *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. |
| *if_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** | Keyword to specify whether the applied ACL analyzes traffic destined to ASA for management purposes. |

## ACLs and Object Groups

ACL Reference Topology




Extended ACL Configuration Example

```
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-1 -> 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-1 -> 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-2 -> 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-2 -> 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)#
```

Verifying the ACL

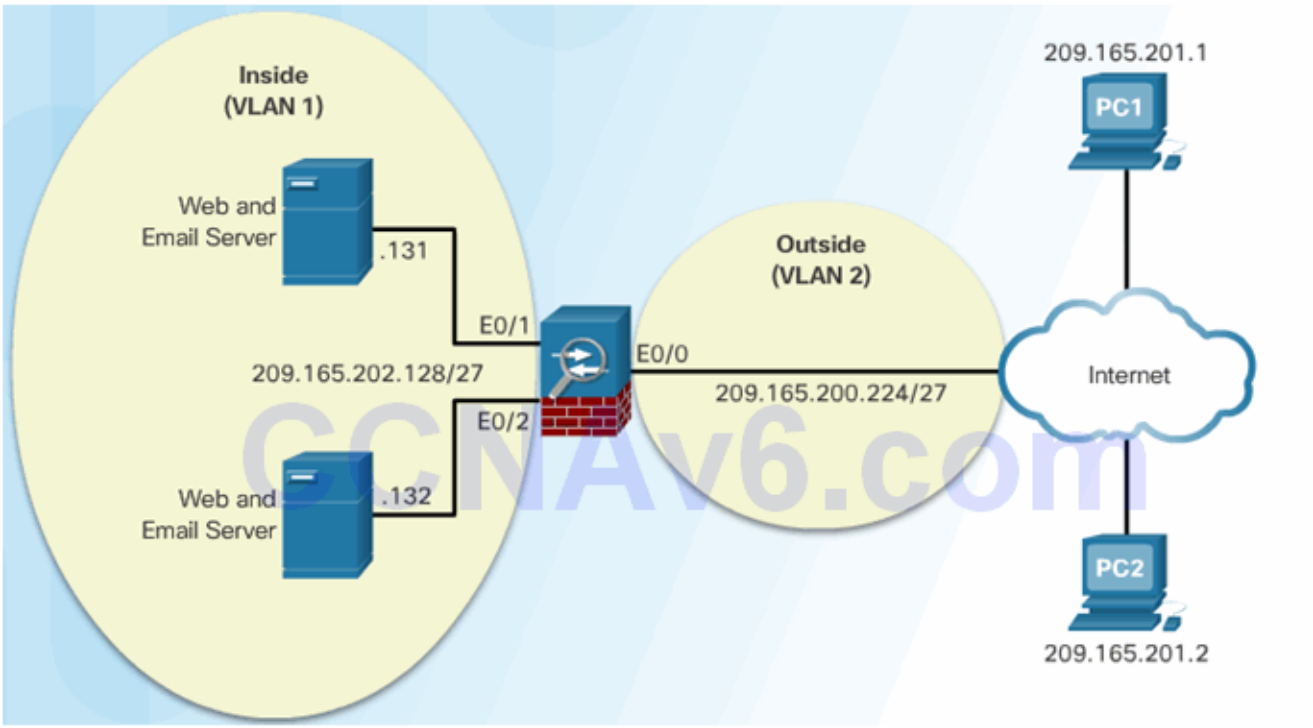
```
CCNAS-ASA(config)# show running-config access-list
access-list ACL-IN remark Permit PC-1 -> Server A for HTTP / SMTP
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq www
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq smtp
access-list ACL-IN remark Permit PC-1 -> 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-2 -> 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-2 -> 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 Using Object Groups Examples

Condensed Extended ACL Syntax with Object Groups

```
access-list id extended { deny | permit } protocol object-group
network-obj-grp-id object-group network-obj-grp-id object-group
service-obj-grp-id
```

ACL Reference Topology




ACL and Object Group Configuration Example

```
CCNAS-ASA(config)# object-group network NET-HOSTS
CCNAS-ASA(config-network-object-group)# description OG matches PC-A and PC-B
CCNAS-ASA(config-network-object-group)# network-object host 209.165.201.1
CCNAS-ASA(config-network-object-group)# network-object host 209.165.201.2
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group network SERVERS
CCNAS-ASA(config-network-object-group)# description OG matches Web / Email Servers
CCNAS-ASA(config-network-object-group)# network-object host 209.165.202.131
CCNAS-ASA(config-network-object-group)# network-object host 209.165.202.132
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service HTTP-SMTP tcp
CCNAS-ASA(config-service-object-group)# description OG matches SMTP / WEB traffic
CCNAS-ASA(config-service-object-group)# port-object eq smtp
CCNAS-ASA(config-service-object-group)# port-object eq www
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-list ACL-IN remark Only permit PC-A / PC-B -> Internal Servers
CCNAS-ASA(config)#  access-list ACL-IN extended permit tcp object-group NET-HOSTS
object-group SERVERS object-group HTTP-SMTP
```

Verifying the ACL and Object Group Configuration Example

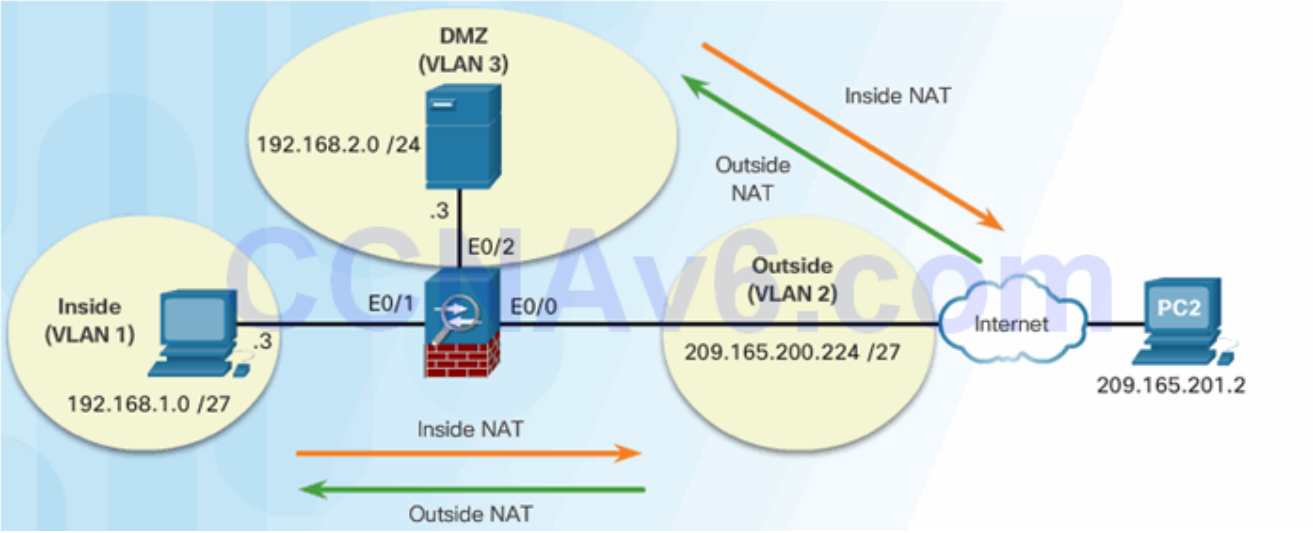
```
CCNAS-ASA(config)# show running-config access-list
access-list ACL-IN remark Only permit PC-A / PC-B -> Internal Servers
access-list ACL-IN extended permit tcp object-group NET-HOSTS object-group SERVERS
object-group HTTP-SMTP
CCNAS-ASA(config)#
```

## Topic 9.2.5: NAT Services on an ASA

### ASA NAT Overview

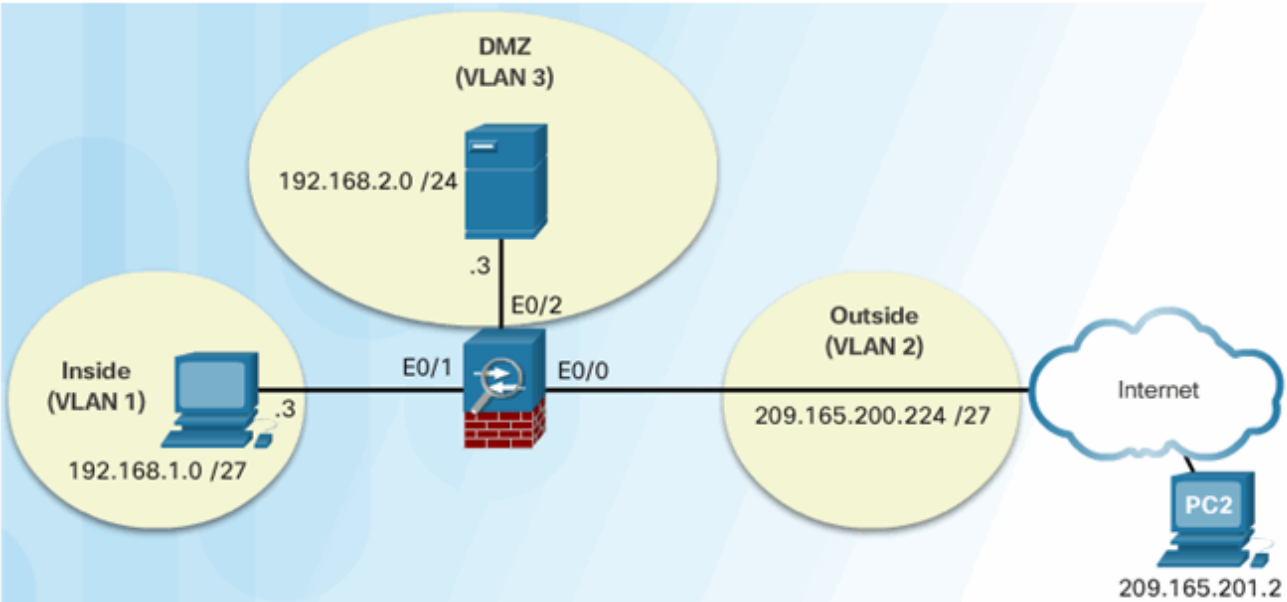
Types of NAT Deployments:

- Inside NAT
- Outside NAT
- Bidirectional NAT




### Configuring Dynamic NAT

Dynamic NAT Reference Topology




Dynamic NAT Configuration Example

```
CCNAS-ASA(config)# object network PUBLIC
CCNAS-ASA(config-network-object)# range 209.165.200.240 209.165.200.248
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network DYNAMIC-NAT
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic PUBLIC
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

Enable Return Traffic Example

```
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-cmap)# access-list ICMPACL extended permit icmp any any
CCNAS-ASA(config)# access-group ICMPACL in interface outside
CCNAS-ASA(config)#
```

Verifying the Dynamic NAT Configuration Example

```
CCNAS-ASA(config)# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

NAT from inside:192.168.1.3 to outside:209.165.200.242 flags i idle 0:00:02 timeout 3:00:00
CCNAS-ASA(config)#
CCNAS-ASA(config)# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic DYNAMIC-NAT PUBLIC
    translate_hits = 1, untranslate_hits = 1
CCNAS-ASA(config)#
CCNAS-ASA(config)# show nat detail

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic DYNAMIC-NAT PUBLIC
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.1.0/27, Translated: 209.165.200.240-209.165.200.248
CCNAS-ASA(config)#
```

## Configuring Dynamic PAT

Dynamic PAT Configuration 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#
```

Verifying the Dynamic PAT Configuration Example

```
CCNAS-ASA# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

ICMP PAT from inside:192.168.1.3/1 to outside:209.165.200.226/1 flags ri idle
 0:00:02 timeout 0:00:30
CCNAS-ASA#
```

## Configuring Static NAT

Configure the DMZ Interface Example

```
CCNAS-ASA(config)# interface Vlan3
CCNAS-ASA(config-if)# no forward interface Vlan1
CCNAS-ASA(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
CCNAS-ASA(config-if)# security-level 70
CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# interface Ethernet0/2
CCNAS-ASA(config-if)# switchport access vlan 3
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
```

Static NAT Configuration Example

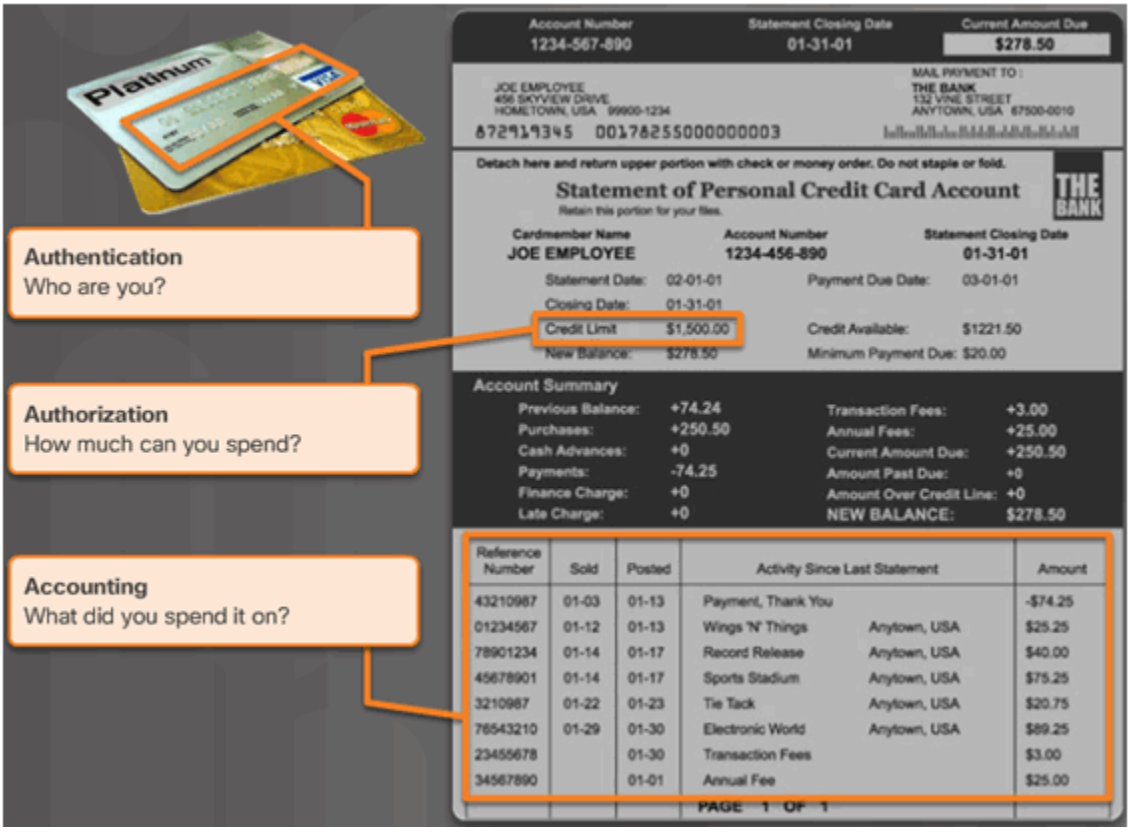
```
CCNAS-ASA(config)# object network DMZ-SERVER
CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# access-list ICMPACL extended permit icmp any any
CCNAS-ASA(config)# access-group ICMPACL in interface dmz
CCNAS-ASA(config)#
```

Verifying the Static NAT Configuration Example

```
CCNAS-ASA(config)# show xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:192.168.2.3 to outside:209.165.200.227
    flags s idle 0:00:21 timeout 0:00:00

NAT from inside:192.168.1.3 to outside:209.165.200.242 flags i idle 0:09:06 timeout
 3:00:00
CCNAS-ASA(config)#
CCNAS-ASA(config)# show nat detail

Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static DMZ-SERVER 209.165.200.227
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.2.3/32, Translated: 209.165.200.227/32
2 (inside) to (outside) source dynamic DYNAMIC-NAT PUBLIC
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.1.0/27, Translated: 209.165.200.240-209.165.200.248
CCNAS-ASA(config)#
```

## Topic 9.2.6: AAA

### AAA Review




### Local Database and Servers

RADIUS and TACACS+ Server Commands

| ASA Command | Description |
| --- | --- |
| `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* ] | • Configures a AAA server as part of a AAA server group.<br>• Also configures AAA server parameters that are host-specific. |



Sample AAA TACACS+ Server Configuration

```
CCNAS-ASA(config)# username Admin password class privilege 15
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run username
username Admin password obYXcKAuUW.jT5NE encrypted 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 192.168.2.3
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)#
```

## AAA Configuration

```
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)# 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>
```

## Topic 9.2.7: Service Policies on an ASA

### Overview of MPF


### Configuring Class Maps

```
CCNAS-ASA(config)# access-list UDP permit udp any any
CCNAS-ASA(config)# access-list TCP permit tcp any any
CCNAS-ASA(config)# access-list SERVER permit ip any host 10.1.1.1
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-TCP
CCNAS-ASA(config-cmap)# description "This class-map matches all TCP traffic"
CCNAS-ASA(config-cmap)# match access-list TCP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-UDP
CCNAS-ASA(config-cmap)# description "This class-map matches all UDP traffic"
CCNAS-ASA(config-cmap)# match access-list UDP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-HTTP
CCNAS-ASA(config-cmap)# description "This class-map matches all HTTP traffic"
CCNAS-ASA(config-cmap)# match port TCP eq http
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map TO-SERVER
CCNAS-ASA(config-cmap)# description "Class map matches traffic    10.1.1.1"
CCNAS-ASA(config-cmap)# match access-list SERVER
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
```

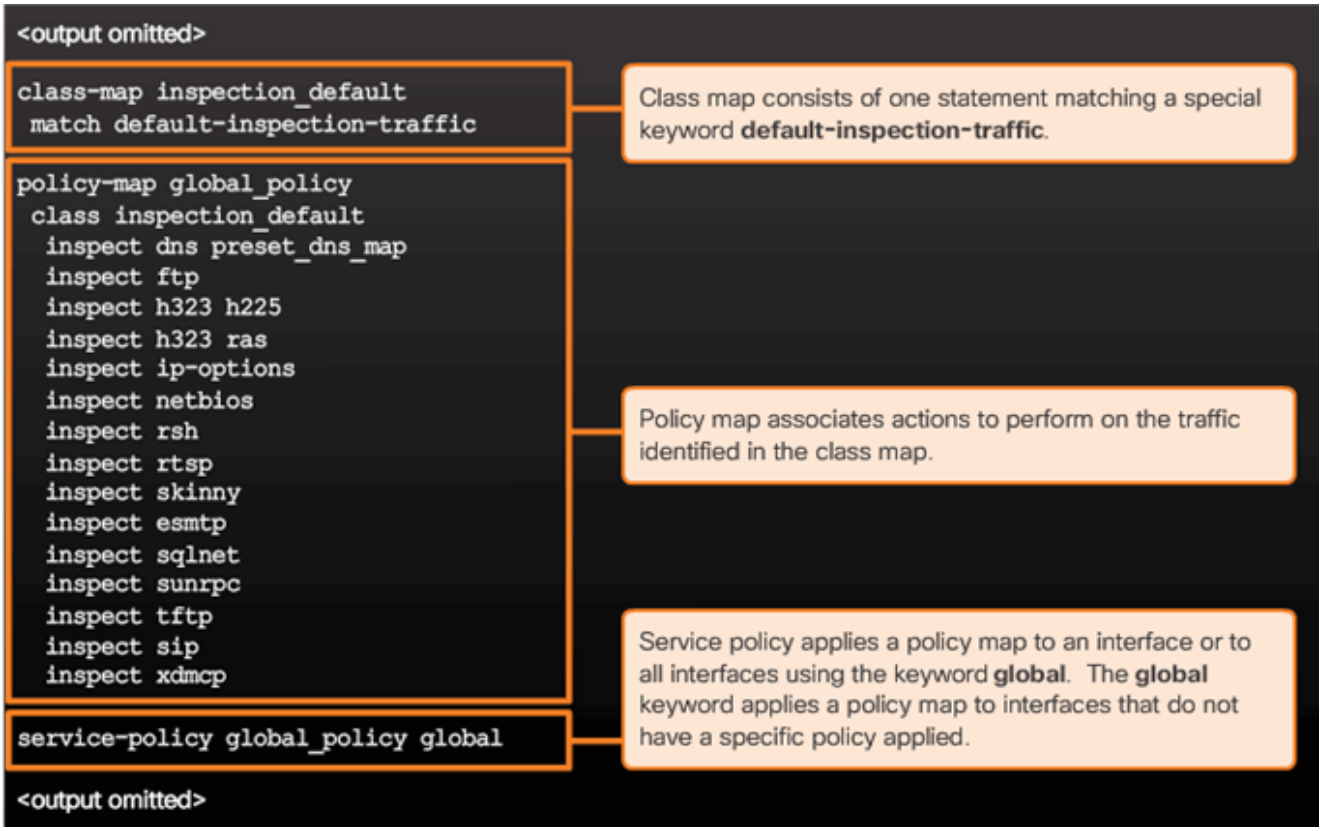
### Define and Activate a Policy

Implementing Modular Policy Framework

```
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)#
```

### ASA Default Policy

Default Service Policy Configuration




## Section 9.3: Summary

### Chapter Objectives:

- Explain how the ASA operates as an advanced stateful firewall.
- Implement an ASA firewall configuration.

## Download Slide PowerPoint (pptx):

[sociallocker id=”54558″]


**CCNASv2_InstructorPPT_CH9.pptx** 6.76 MB 2933 downloads

...

Download

[/sociallocker]