Basic Settings

This chapter describes how to configure basic settings on the ASA that are typically required for a functioning configuration and includes the following sections:

- Configuring the Hostname, Domain Name, and Passwords, page 15-1
- Setting the Date and Time, page 15-5
- Configuring the Master Passphrase, page 15-8
- Configuring the DNS Server, page 15-13
- http://www.cisco.com/en/US/products/ps6121/products_tech_note09186a0080aaeff5.shtml, page 15-14
- Performing Password Recovery for the ASA, page 15-14
- Performing Password Recovery for the ASAv, page 15-16
- Monitoring DNS Cache, page 15-17
- Choosing a Rule Engine Transactional Commit Model, page 15-18

Configuring the Hostname, Domain Name, and Passwords

- Setting the Login Password, page 15-1
- Changing the Enable Password, page 15-2
- Setting the Hostname, page 15-3
- Setting the Domain Name, page 15-4
- Feature History for the Hostname, Domain Name, and Passwords, page 15-4

Setting the Login Password

The login password is used for Telnet access when you do not configure Telnet authentication (see Configuring Authentication for CLI and ASDM Access, page 43-20). You also use this password when accessing the ASASM from the switch with the **session** command.

Prerequisites

- Enable Telnet access according to the Configuring Telnet Access, page 43-3.

- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the **changeto context** *name* command. For the ASASM in multiple context mode, set the login password in the admin context for use when you session to the system execution space.

Detailed Steps

Command	Purpose
{**passwd** | **password**} *password* [**encrypted**]	Sets the login password. There is no default password. You can enter **passwd** or **password**. The *password* is a case-sensitive password of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another ASA but do not know the original password, you can enter the **passwd** command with the encrypted password and the **encrypted** keyword. Normally, you only see this keyword when you enter the **show running-config passwd** command.

Changing the Enable Password

The enable password lets you enter privileged EXEC mode if you do not configure enable authentication (see Configuring Authentication to Access Privileged EXEC Mode (the enable Command), page 43-21).

The enable password also lets you log into ASDM with a blank username if you do not configure HTTP authentication (see Configuring Authentication for CLI and ASDM Access, page 43-20.

Prerequisites

In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the **changeto context** *name* command.

Detailed Steps

Command	Purpose
enable password *password* **Example:** `hostname(config)# passwd Pa$$w0rd`	Changes the enable password. By default, the enable password is blank. The *password* argument is a case-sensitive password of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space. This command changes the password for the highest privilege level (15). If you configure local command authorization, you can set enable passwords for each privilege level from 0 to 15 using the following syntax: **enable password** *password* **level** *number* The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. Enter the **enable password** command without a password to set the password to the default, which is blank.

Setting the Hostname

When you set a hostname for the ASA, that name appears in the command line prompt. If you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands.

Guidelines

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts. The hostname that you optionally set within a context does not appear in the command line, but can be used by the **banner** command **$(hostname)** token.

Detailed Steps

Command	Purpose

hostname *name*
 	
Example:
`asa(config)# hostname farscape`
`farscape(config)#`
	Specifies the hostname for the ASA or for a context. The default hostname is “asa.”
	
	This name can be up to 63 characters. The hostname must start and end with a letter or digit, and have only letters, digits, or a hyphen.

Setting the Domain Name

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com” and specify a syslog server by the unqualified name of “jupiter,” then the ASA qualifies the name to “jupiter.example.com.”

Guidelines

For multiple context mode, you can set the domain name for each context, as well as within the system execution space.

Detailed Steps

Command	Purpose
domain-name *name* **Example:** `ciscoasa(config)# domain-name example.com`	Specifies the domain name for the ASA. The default domain name is default.domain.invalid.

Feature History for the Hostname, Domain Name, and Passwords

Table 15-1 lists each feature change and the platform release in which it was implemented.

Table 15-1 Feature History for the Master Passphrase

Feature Name	Platform Releases	Feature Information
Removal of the default Telnet password	9.0(2)/9.1(2)	To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. **Note**: The login password is only used for Telnet if you do not configure Telnet user authentication (the **aaa authentication telnet console** command). Formerly, when you cleared the password, the ASA restored the default of “cisco.” Now when you clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the ASASM (see the **session** command). For initial ASASM access, you must use the **service-module session** command, until you set a login password. We modified the following command: **passwd**.

Setting the Date and Time

Note Do not set the date and time for the ASASM; it receives these settings from the host switch.

This section includes the following topics:

- Setting the Time Zone and Daylight Saving Time Date Range, page 15-5
- Setting the Date and Time Using an NTP Server, page 15-6
- Setting the Date and Time Manually, page 15-8

Setting the Time Zone and Daylight Saving Time Date Range

To set the time zone and daylight saving time date range, perform the following steps:

	Command	Purpose
Step 1	**clock timezone** *zone* [**-**]*hours* [*minutes*] **Example:** `ciscoasa(config)# clock timezone PST -8`	Sets the time zone. By default, the time zone is UTC and the daylight saving time date range is from 2:00 a.m. on the first Sunday in April to 2:00 a.m. on the last Sunday in October. Where *zone* specifies the time zone as a string, for example, **PST** for Pacific Standard Time. The [**-**]*hours* value sets the number of hours of offset from UTC. For example, PST is **-8** hours. The *minutes* value sets the number of minutes of offset from UTC.
Step 2	To change the date range for daylight saving time from the default, enter one of the following commands. The default recurring date range is from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.	

Command	Purpose
clock summer-time *zone* **date** {*day month* | *month day*} *year hh:mm* {*day month* | *month day*} *year hh:mm* [*offset*] **Example:** `ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60`	Sets the start and end dates for daylight saving time as a specific date in a specific year. If you use this command, you need to reset the dates every year. The *zone* value specifies the time zone as a string, for example, **PDT** for Pacific Daylight Time. The *day* value sets the day of the month, from 1 to 31. You can enter the day and month as **April 1** or as **1 April**, for example, depending on your standard date format. The *month* value sets the month as a string. You can enter the day and month as **April 1** or as **1 April**, depending on your standard date format. The *year* value sets the year using four digits, for example, **2004**. The year range is 1993 to 2035. The *hh:mm* value sets the hour and minutes in 24-hour time. The *offset* value sets the number of minutes to change the time for daylight saving time. By default, the value is 60 minutes.
clock summer-time *zone* **recurring** [*week weekday month hh:mm week weekday month hh:mm*] [*offset*] **Example:** `ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60`	Specifies the start and end dates for daylight saving time, in the form of a day and time of the month, and not a specific date in a year. This command enables you to set a recurring date range that you do not need to change yearly. The *zone* value specifies the time zone as a string, for example, **PDT** for Pacific Daylight Time. The *week* value specifies the week of the month as an integer between 1 and 4 or as the words **first** or **last**. For example, if the day might fall in the partial fifth week, then specify **last**. The *weekday* value specifies the day of the week: **Monday**, **Tuesday**, **Wednesday**, and so on. The *month* value sets the month as a string. The *hh:mm* value sets the hour and minutes in 24-hour time. The *offset* value sets the number of minutes to change the time for daylight savings time. By default, the value is 60 minutes.

Setting the Date and Time Using an NTP Server

To obtain the date and time from an NTP server, perform the following steps :

Detailed Steps

	Command	Purpose
Step 1	**ntp authenticate** **Example:** `ciscoasa(config)# ntp authenticate`	Enables authentication with an NTP server.

Step 2	**ntp trusted-key** *key_id* **Example:** `ciscoasa(config)# ntp trusted-key 1`	Specifies an authentication key ID to be a trusted key, which is required for authentication with an NTP server. The *key_id* argument is a value between 1 and 4294967295. You can enter multiple trusted keys for use with multiple servers.
Step 3	**ntp authentication-key** *key_id* **md5** *key* **Example:** `hostname(config)# ntp authentication-key 1 md5 aNiceKey`	Sets a key to authenticate with an NTP server. The *key_id* argument is the ID you set in Step 2 using the **ntp trusted-key** command, and the *key* argument is a string up to 32 characters long.
Step 4	**ntp server** *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**] **Example:** `hostname(config)# ntp server 10.1.1.1 key 1 prefer`	Identifies an NTP server. The *key_id* argument is the ID you set in Step 2 using the **ntp trusted-key** command. The **source** *interface_name* keyword-argument pair identifies the outgoing interface for NTP packets if you do not want to use the default interface in the routing table. Because the system does not include any interfaces in multiple context mode, specify an interface name defined in the admin context. The **prefer** keyword sets this NTP server as the preferred server if multiple servers have similar accuracy. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If servers are of similar accuracy, then the **prefer** keyword specifies which of those servers to use. However, if a server is significantly more accurate than the preferred one, the ASA uses the more accurate one. For example, the ASA uses a server of stratum 2 over a server of stratum 3 that is preferred. You can identify multiple servers; the ASA uses the most accurate server. **Note** In multiple context mode, set the time in the system configuration only.

Setting the Date and Time Manually

To set the date and time manually, enter the following command:

Command	Purpose
clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year* **Example:** `hostname# clock set 20:54:00 april 1 2004`	Sets the date time manually. The *hh*:*mm*:*ss* argument sets the hour, minutes, and seconds in 24-hour time. For example, enter **20:54:00** for 8:54 pm. The *day* value sets the day of the month, from 1 to 31. You can enter the day and month as **april 1** or as **1 april**, for example, depending on your standard date format. The *month* value sets the month. Depending on your standard date format, you can enter the day and month as **april 1** or as **1 april**. The *year* value sets the year using four digits, for example, **2004**. The year range is from 1993 to 2035. The default time zone is UTC. If you change the time zone after you enter the **clock set** command using the **clock timezone** command, the time automatically adjusts to the new time zone. This command sets the time in the hardware chip, and does not save the time in the configuration file. This time endures reboots. Unlike the other **clock** commands, this command is a privileged EXEC command. To reset the clock, you need to set a new time with the **clock set** command.

Configuring the Master Passphrase

This section includes the following topics:

- Information About the Master Passphrase, page 15-8
- Licensing Requirements for the Master Passphrase, page 15-9
- Guidelines and Limitations, page 15-9
- Adding or Changing the Master Passphrase, page 15-9
- Disabling the Master Passphrase, page 15-11
- Recovering the Master Passphrase, page 15-12
- Feature History for the Master Passphrase, page 15-13

Information About the Master Passphrase

The master passphrase allows you to securely store plain text passwords in encrypted format and provides a key that is used to universally encrypt or mask all passwords, without changing any functionality. Features that use the master passphrase include the following:

- OSPF
- EIGRP
- VPN load balancing

- VPN (remote access and site-to-site)
- Failover
- AAA servers
- Logging
- Shared licenses

Licensing Requirements for the Master Passphrase

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Failover Guidelines

If failover is enabled but no failover shared key is set, an error message appears if you change the master passphrase, informing you that you must enter a failover shared key to protect the master passphrase changes from being sent as plain text.

Adding or Changing the Master Passphrase

This procedure will only be accepted in a secure session, for example by console, SSH, or ASDM via HTTPS.

To add or change the master passphrase, perform the following steps:

Detailed Steps

	Command	Purpose

Step 1	**key config-key password-encryption** [*new_passphrase* [*old_passphrase*]]
	
	Example:
	`ciscoasa(config)# key config-key password-encryption`
	`Old key: bumblebee`
	`New key: haverford`
	`Confirm key: haverford`
		Sets the passphrase used for generating the encryption key. The passphrase must be between 8 and 128 characters long. All characters except a backspace and double quotes are accepted for the passphrase.
		
		If you do not enter the new passphrase in the command, you are prompted for it.
		
		To change the passphrase, you must enter the old passphrase.
		
		see Examples, page 15-11 for examples of the interactive prompts.
		
		Note Use the interactive prompts to enter passwords to avoid having the passwords logged in the command history buffer.
		
		Use the **no key config-key password-encrypt** command with caution, because it changes the encrypted passwords into plain text passwords. You can use the **no** form of this command when downgrading to a software version that does not support password encryption.

Step 2	**password encryption aes** **Example:** `ciscoasa(config)# password encryption aes`	Enables password encryption. As soon as password encryption is enabled and the master passphrase is available, all the user passwords will be encrypted. The running configuration will show the passwords in the encrypted format. If the passphrase is not configured at the time that password encryption is enabled, the command will succeed in anticipation that the passphrase will be available in the future. If you later disable password encryption using the **no password encryption aes** command, all existing encrypted passwords are left unchanged, and as long as the master passphrase exists, the encrypted passwords will be decrypted, as required by the application.
Step 3	**write memory** **Example:** `ciscoasa(config)# write memory`	Saves the runtime value of the master passphrase and the resulting configuration. If you do not enter this command, passwords in startup configuration may still be visible if they were not saved with encryption previously. In addition, in multiple context mode the master passphrase is changed in the system context configuration. As a result, the passwords in all contexts will be affected. If the **write memory** command is not entered in the system context mode, but not in all user contexts, then the encrypted passwords in user contexts may be stale. Alternatively, use the **write memory all** command in the system context to save all configurations.

Examples

The following example shows that no previous key was present:

```
hostname (config)# key config-key password-encryption 12345678
```

The following example shows that a key already exists:

```
Hostname (config)# key config-key password-encryption 23456789
Old key: 12345678
hostname (config)#
```

In the following example, you want to key in interactively, but a key already exists. The Old key, New key, and Confirm key prompts appear on your screen if you enter the **key config-key password-encryption** command and press **Enter** to access interactive mode.

```
hostname (config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

In the following example, you want to key in interactively, but no key is present. The New key and Confirm key prompts appear on your screen if you are in interactive mode.

```
hostname (config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

Disabling the Master Passphrase

Disabling the master passphrase reverts encrypted passwords into plain text passwords. Removing the passphrase might be useful if you downgrade to a previous software version that does not support encrypted passwords.

You must know the current master passphrase to disable it. If you do not know the passphrase, see Recovering the Master Passphrase, page 15-12.

This procedure works only in a secure session; that is, by Telnet, SSH, or ASDM via HTTPS.

To disable the master passphrase, perform the following steps:

Detailed Steps

	Command	Purpose

Step 1	**no key config-key password-encryption** [*old_passphrase*]]
	
	Example:
	`ciscoasa(config)# no key config-key password-encryption`
	
	`Warning! You have chosen to revert the encrypted passwords to plain text. This operation will expose passwords in the configuration and therefore exercise caution while viewing, storing, and copying configuration.`
	
	`Old key: bumblebee`
		Removes the master passphrase.
		
		If you do not enter the passphrase in the command, you are prompted for it.

Step 2	**write memory** **Example:** `ciscoasa(config)# write memory`	Saves the runtime value of the master passphrase and the resulting configuration. The non-volatile memory containing the passphrase will be erased and overwritten with the 0xFF pattern. In multiple mode, the master passphrase is changed in the system context configuration. As a result, the passwords in all contexts will be affected. If the **write memory** command is not entered in the system context mode, but not in all user contexts, then the encrypted passwords in user contexts may be stale. Alternatively, use the **write memory all** command in the system context to save all configurations.

Recovering the Master Passphrase

You cannot recover the master passphrase. If the master passphrase is lost or unknown, you can remove it.

To remove the master passphrase, perform the following steps:

	Command	Purpose
Step 1	**write erase** **Example:** `ciscoasa(config)# write erase`	Removes the master key and the configuration that includes the encrypted passwords.
Step 2	**reload** **Example:** `ciscoasa(config)# reload`	Reloads the ASA with the startup configuration, without any master key or encrypted passwords.

Feature History for the Master Passphrase

Table 15-2 lists each feature change and the platform release in which it was implemented.

Table 15-2 Feature History for the Master Passphrase

Feature Name	Platform Releases	Feature Information
Master Passphrase	8.3(1)	We introduced this feature. The master passphrase allows you to securely store plain text passwords in encrypted format and provides a key that is used to universally encrypt or mask all passwords, without changing any functionality. We introduced the following commands: **key config-key password-encryption**, **password encryption aes**, **clear configure password encryption aes**, **show running-config password encryption aes, show password encryption**.
Password Encryption Visibility	8.4(1)	We modified the **show password encryption** command.

Configuring the DNS Server

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database. Other features, such as the **ping** or **traceroute** command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names.

Note The ASA has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the **name** command to associate a name with an IP address and enable use of the names using the **names** command.

For information about dynamic DNS, see Configuring DDNS, page 16-2.

Prerequisites

Make sure that you configure the appropriate routing for any interface on which you enable DNS domain lookup so you can reach the DNS server. see Information About Routing, page 26-1 for more information about routing.

To configure the DNS server, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**dns domain-lookup** *interface_name* **Example:** `hostname(config)# dns domain-lookup inside`	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
Step 2	**dns server-group DefaultDNS** **Example:** `hostname(config)# dns server-group DefaultDNS`	Specifies the DNS server group that the ASA uses for outgoing requests. Other DNS server groups can be configured for VPN tunnel groups. See the **tunnel-group** command in the command reference for more information.
Step 3	**name-server** *ip_address* [*ip_address2*] [...] [*ip_address6*] **Example:** `hostname(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6`	Specifies one or more DNS servers. You can enter all six IP addresses in the same command, separated by spaces, or you can enter each command separately. The ASA tries each DNS server in order until it receives a response.

http://www.cisco.com/en/US/products/ps6121/products_tech_note09186a0080aaeff5.shtml

Performing Password Recovery for the ASA

This section includes the following topics:

- Recovering Passwords for the ASA, page 15-14
- Disabling Password Recovery, page 15-16

Recovering Passwords for the ASA

To recover passwords for the ASA, perform the following steps:

Step 1 Connect to the ASA console port according to the instructions in Accessing the ASA Services Module Console, page 4-2 or the Accessing the Appliance Console, page 4-1.

Step 2 Power off the ASA, and then power it on.

Step 3 After startup, press the **Escape** key when you are prompted to enter ROMMON mode.

Step 4 To update the configuration register value, enter the following command:

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

Step 5 To set the ASA to ignore the startup configuration, enter the following command:

```
rommon #1> confreg
```

The ASA displays the current configuration register value, and asks whether you want to change it:

```
Current Configuration Register: 0x00000041
Configuration Summary:
  boot default image from Flash
  ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```

Step 6 Record the current configuration register value, so you can restore it later.

Step 7 At the prompt, enter **Y** to change the value.

The ASA prompts you for new values.

Step 8 Accept the default values for all settings, except for the "disable system configuration?" value.

Step 9 At the prompt, enter **Y**.

Step 10 Reload the ASA by entering the following command:

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

The ASA loads the default configuration instead of the startup configuration.

Step 11 Access the privileged EXEC mode by entering the following command:

```
ciscoasa# enable
```

Step 12 When prompted for the password, press **Enter**.

The password is blank.

Step 13 Load the startup configuration by entering the following command:

```
ciscoasa# copy startup-config running-config
```

Step 14 Access the global configuration mode by entering the following command:

```
ciscoasa# configure terminal
```

Step 15 Change the passwords, as required, in the default configuration by entering the following commands:

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

Step 16 Load the default configuration by entering the following command:

```
ciscoasa(config)# no config-register
```

The default configuration register value is 0x1. For more information about the configuration register, see the command reference.

Step 17 Save the new passwords to the startup configuration by entering the following command:

```
ciscoasa(config)# copy running-config startup-config
```

Disabling Password Recovery

To disable password recovery to ensure that unauthorized users cannot use the password recovery mechanism to compromise the ASA, enter the following command:

Command	Purpose
no service password-recovery **Example:** `ciscoasa (config)# no service password-recovery`	Disables password recovery.

On the ASA, the **no service password-recovery** command prevents you from entering ROMMON mode with the configuration intact. When you enter ROMMON mode, the ASA prompts you to erase all Flash file systems.Yyou cannot enter ROMMON mode without first performing this erasure. If you choose not to erase the Flash file system, the ASA reloads. Because password recovery depends on using ROMMON mode and maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to restore the system to an operating state, load a new image and a backup configuration file, if available.

The **service password-recovery** command appears in the configuration file for information only. When you enter the command at the CLI prompt, the setting is saved in NVRAM. The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If you disable password recovery when the ASA is configured to ignore the startup configuration at startup (in preparation for password recovery), then the ASA changes the setting to load the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, then the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit.

Performing Password Recovery for the ASAv

This section includes the following topics:

- Recovering Passwords or Images on the ASAv, page 15-17
- Disabling Password Recovery, page 15-16

Recovering Passwords or Images on the ASAv

To recover passwords or images on the ASAv, perform the following steps:

	Command	Purpose
Step 1	**copy running-config** *filename* **Example:** `ciscoasa# copy running-config backup.cfg`	Copies the running configuration to a backup file on the ASAv.
Step 2	**reload** **Example:** `ciscoasa# reload`	Restarts the ASAv.

Step 3	`GNU GRUB version 2.0(12)4`
	`bootflash:/asa100123-20-smp-k8.bin`
	bootflash: /asa100123-20-smp-k8.bin with no configuration load
	
	Example:
	`GNU GRUB version 2.0(12)4`
	bootflash: /asa100123-20-smp-k8.bin with no configuration load
		From the GNU GRUB menu, press the down arrow, choose the **<filename> with no configuration load** option, then press **Enter**. The filename is the default boot image filename on the ASAv. The default boot image is never automatically booted through the **fallback** command.
		
		Boots the selected boot image.

Step 4	**copy** *filename* **running-config** **Example:** `ciscoasa (config)# copy backup.cfg running-config`	Copies the backup configuration file to the running configuration.
Step 5	**enable password** **Example:** `ciscoasa (config)# enable password cisco123`	Resets the password.
Step 6	**write mem** **Example:** `ciscoasa (config)# write mem`	Saves the new configuration.

Disabling Password Recovery

You cannot disable password recovery on the ASAv.

Monitoring DNS Cache

The ASA provides a local cache of DNS information from external DNS queries that are sent for certain clientless SSL VPN and certificate commands. Each DNS translation request is first looked for in the local cache. If the local cache has the information, the resulting IP address is returned. If the local cache

can not resolve the request, a DNS query is sent to the various DNS servers that have been configured. If an external DNS server resolves the request, the resulting IP address is stored in the local cache with its corresponding hostname.

To monitor the DNS cache, enter the following command:

Command	Purpose
show dns-hosts	Show the DNS cache, which includes dynamically learned entries from a DNS server as well as manually entered name and IP addresses using the **name** command.

Choosing a Rule Engine Transactional Commit Model

By default, when you change a rule-based policy (such as access rules), the changes become effective immediately. However, this immediacy comes at a slight cost in performance. The performance cost is more noticeable for very large rule lists in a high connections-per-second environment, for example, when you change a policy with 25,000 rules while the ASA is handling 18,000 connections per second.

The performance is affected because the rule engine compiles rules to enable faster rule lookup. By default, the system will also search uncompiled rules when evaluating a connection attempt so that new rules can be applied; since the rules are not compiled, the search takes longer.

You can change this behavior so that the rule engine uses a transactional model when implementing rule changes, continuing to use the old rules until the new rules are compiled and ready for use. Using the transactional model, performance should not drop during the rule compilation. The following table clarifies the behavioral difference.

Model	Before Compilation	During Compilation	After Compilation
Default	Match old rules.	Match new rules. (Connections per second rate will decrease.)	Match new rules.
Transactional	Match old rules.	Match old rules. (Connections per second rate will be unaffected.)	Match new rules.

An additional benefit of the transactional model is that, when replacing an ACL on an interface, there is no gap between deleting the old ACL and applying the new one. This reduces the chances that acceptable connections will be dropped during the operation.

Tip If you enable the transactional model for a rule type, there are syslog messages to mark the beginning and the end of the compilation. These messages are numbered 780001 and following.

Detailed Steps

Command	Purpose
asp rule-engine transactional-commit *option* **Example:** `ciscoasa(config)# asp rule-engine transactional-commit access-group`	Enables the transactional commit model for the rule engine for the selected policies. Options include: • **access-group**—Access rules applied globally or to interfaces.