Basic Settings

This chapter describes how to configure basic settings on the ASA that are typically required for a functioning configuration.

- Set the Hostname, Domain Name, and the Enable and Telnet Passwords, page 14-1
- Recover Enable and Telnet Passwords, page 14-3
- Set the Date and Time, page 14-7
- Configure the Master Passphrase, page 14-10
- Configure the DNS Server, page 14-14
- Monitoring the DNS Cache, page 14-16
- History for Basic Settings, page 14-17

Set the Hostname, Domain Name, and the Enable and Telnet Passwords

This section describes how to configure the hostname, domain name, and the enable and Telnet passwords.

Before You Begin

- In multiple context mode, you can configure the hostname and domain name in both the system and context execution spaces.
- For the enable and Telnet passwords, set them in each context; they are not available in the system. When you session to the ASASM from the switch in multiple context mode, the ASASM uses the login password you set in the admin context.
- To change from the system to a context configuration, enter the changeto context name command.

To set the hostname, domain name, and the enable and Telnet passwords, perform the following steps.

Procedure

Step 1 Specify the hostname for the ASA or for a context. The default hostname is “asa.”

hostname name
Example:
ciscoasa(config)# hostname myhostnameexample12345

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.

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.

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.

**Step 2** Specify the domain name for the ASA. The default domain name is `default.domain.invalid`.

domain-name name

Example:
ciscoasa(config)# domain-name example.com

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.”

**Step 3** Change the enable password. By default, the enable password is blank.

The enable password lets you enter privileged EXEC mode if you do not configure enable authentication. The enable password also lets you log into ASDM with a blank username if you do not configure HTTP authentication.

`enable password password`

Example:
ciscoasa(config)# enable passwd Pa$$w0rd

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.

**Step 4** Set the login password for Telnet access. There is no default password.

The login password is used for Telnet access when you do not configure Telnet authentication. You also use this password when accessing the ASASM from the switch with the `session` command.

`{passwd | password} password [encrypted]`

Example:
ciscoasa(config)# password cisco12345

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.

---

**Recover Enable and Telnet Passwords**

If you forget the enable or Telnet passwords, you can recover them. The procedure differs by device type. You must perform the task using the CLI.

**Recover Passwords on the ASA**

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

**Procedure**

- **Step 1** Connect to the ASA console port.
- **Step 2** Power off the ASA, 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
  ```
Recover Enable and Telnet Passwords

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. See the command reference for more information about the configuration register.

Step 17 Save the new passwords to the startup configuration by entering the following command:
```
ciscoasa(config)# copy running-config startup-config
```

Recover Passwords on the ASA 5506-X

To recover passwords for the ASA 5506-X, perform the following steps:

**Procedure**

Step 1 Connect to the ASA console port.

Step 2 Power off the ASA, 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
```
You must reset or power cycle for new config to take effect.

The ASA displays the current configuration register value and a list of configuration options. Record the current configuration register value, so you can restore it later.

Configuration Register: 0x00000041
Recover Enable and Telnet Passwords

Configuration Summary
- [0] password recovery
- [1] display break prompt
- [2] ignore system configuration
- [3] auto-boot image in disks
- [4] console baud: 9600

Step 5
Reload the ASA by entering the following command:

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

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

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

Step 6
Access the privileged EXEC mode by entering the following command:
```
ciscoasa# enable
```

Step 7
When prompted for the password, press Enter.
The password is blank.

Step 8
Load the startup configuration by entering the following command:
```
ciscoasa# copy startup-config running-config
```

Step 9
Access the global configuration mode by entering the following command:
```
ciscoasa# configure terminal
```

Step 10
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 11
Load the default configuration by entering the following command:
```
ciscoasa(config)# no config-register
```

The default configuration register value is 0x1. See the command reference for more information about the configuration register.

Step 12
Save the new passwords to the startup configuration by entering the following command:
```
ciscoasa(config)# copy running-config startup-config
```

Recover Passwords or Images on the ASAv

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

Procedure

Step 1
Copy the running configuration to a backup file on the ASAv:
```
copy running-config filename
```
Example:
ciscoasa# copy running-config backup.cfg

**Step 2** Restart the ASAv:
```
reload
```

**Step 3** 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. Then load the selected boot image.

```
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
```

**Step 4** Copy the backup configuration file to the running configuration.
```
copy filename running-config
```

Example:
ciscoasa (config)# copy backup.cfg running-config

**Step 5** Reset the password.
```
enable password
```

Example:
ciscoasa(config)# enable password cisco123

**Step 6** Save the new configuration.
```
write memory
```

Example:
ciscoasa(config)# write memory

---

**Disable Password Recovery**

**Note** You cannot disable password recovery on the ASAv.

To disable password recovery to ensure that unauthorized users cannot use the password recovery mechanism to compromise the ASA, perform the following steps.

**Before You Begin**

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. You cannot enter ROMMON mode without first performing this erasure. If you choose not to erase the Flash file system, the ASA reboots. 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.

**Procedure**

**Step 1** Disable password recovery.

```
no service password-recovery
```

Example:

```
ciscoasa (config)# no service password-recovery
```

---

### Set the Date and Time

**Note**

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

### Set the Time Zone and Daylight Savings Dates

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

**Procedure**

**Step 1** Set 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.

```
clock timezone zone [-]hours [minutes]
```

Example:

```
ciscoasa(config)# clock timezone PST -8
```

The `zone` argument 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.
Set the Date and Time

Step 2

Enter one of the following commands to change the date range for daylight saving time from the default. 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.

- Set 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.

  \[\text{clock summer-time zone date } \{\text{day month | month day}\} \text{ year hh:mm (day month | month day)} \text{ year hh:mm [offset]}\]

  Example:
  
  \[\text{ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60}\]

  The \text{zone} value specifies the time zone as a string, for example, PDT for Pacific Daylight Time.

  The \text{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 \text{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 \text{year} value sets the year using four digits, for example, 2004. The year range is 1993 to 2035.

  The \text{hh:mm} value sets the hour and minutes in 24-hour time.

  The \text{offset} value sets the number of minutes to change the time for daylight saving time. By default, the value is 60 minutes.

- Specify 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.

  \[\text{clock summer-time zone recurring [week weekday month hh:mm week weekday month hh:mm]}\]

  Example:
  
  \[\text{ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60}\]

  The \text{zone} value specifies the time zone as a string, for example, PDT for Pacific Daylight Time.

  The \text{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 \text{weekday} value specifies the day of the week: Monday, Tuesday, Wednesday, and so on.

  The \text{month} value sets the month as a string.

  The \text{hh:mm} value sets the hour and minutes in 24-hour time.

  The \text{offset} value sets the number of minutes to change the time for daylight savings time. By default, the value is 60 minutes.

Set the Date and Time Using an NTP Server

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The ASA chooses the server with the lowest stratum—a measure of how reliable the data is.

Time derived from an NTP server overrides any time set manually.
Before You Begin

In multiple context mode, you can set the time in the system configuration only.

To set the date and time using an NTP server, perform the following steps:

Procedure

**Step 1**
Enable authentication with an NTP server.

```
ntp authenticate
```

Example:
```
ciscoasa(config)# ntp authenticate
```

**Step 2**
Specify an authentication key ID to be a trusted key, which is required for authentication with an NTP server.

```
ntp trusted-key key_id
```

Example:
```
ciscoasa(config)# ntp trusted-key 1
```

The `key_id` argument is a value between 1 and 4294967295. You can enter multiple trusted keys for use with multiple servers.

**Step 3**
Set a key to authenticate with an NTP server.

```
ntp authentication-key key_id md5 key
```

Example:
```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
```

The `key_id` argument is the ID that 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**
Identify an NTP server.

```
ntp server ip_address [key key_id] [source interface_name] [prefer]
```

Example:
```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
```

The `key_id` argument is the ID that you set 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.
Set the Date and Time Manually

This section describes how to set the date and time manually.

Before You Begin

In multiple context mode, you can set the time in the system configuration only.

To set the date and time manually, perform the following steps:

Procedure

Step 1

Set the date time manually.

```
clock set hh:mm:ss (month day | day month) year
```

Example:

```
ciscoasa# clock set 20:54:00 april 1 2004
```

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.

Configure 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
Configure the Master Passphrase

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.

Add or Change the Master Passphrase

This section describes how to add or change the master passphrase.

Before You Begin
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:

Procedure

Step 1
Set 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.

```
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
```

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 may use the `no` form of this command when downgrading to a software version that does not support password encryption.

Step 2
Enable password encryption.

```
password encryption aes
```

Example:
```
ciscoasa(config)# password encryption aes
```

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.
Configure the Master Passphrase

Step 3  
Save the runtime value of the master passphrase and the resulting configuration.

`write memory`

Example:

```
ciscoasa(config)# write memory
```

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:

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

The following example shows that a key already exists:

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

In the following example, you enter the command without parameters so that you will be prompted for keys. Because a key already exists, you are prompted for it.

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

In the following example, there is no existing key, so you are not prompted to supply it.

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

Disable 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.

Before You Begin

- You must know the current master passphrase to disable it. See Remove the Master Passphrase, page 14-13 if you do not know the passphrase.
- 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:
Configure the Master Passphrase

**Procedure**

**Step 1** Remove the master passphrase. If you do not enter the passphrase in the command, you are prompted for it.

```plaintext
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

**Step 2** Save the runtime value of the master passphrase and the resulting configuration.

```plaintext
write memory
```

Example:

```
ciscoasa(config)# write memory
```

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 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.

---

**Remove the Master Passphrase**

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

**Procedure**

**Step 1** Remove the master key and the configuration that includes the encrypted passwords.

```plaintext
write erase
```

Example:

```
ciscoasa(config)# write erase
```

**Step 2** Reload the ASA with the startup configuration, without any master key or encrypted passwords.

```plaintext
reload
```

Example:

```
ciscoasa(config)# reload
```
Configure the DNS Server

You need to configure DNS servers so that the ASA can resolve host names to IP addresses. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

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.

Before You Begin
Make sure that you configure the appropriate routing and access rules for any interface on which you enable DNS domain lookup so you can reach the DNS server.

To configure the DNS server, perform the following steps:

Procedure

**Step 1**
Enable the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.

dns domain-lookup interface_name

Example:
ciscoasa(config)# dns domain-lookup inside

**Step 2**
Specify the DNS server group that the ASA uses for outgoing requests.

dns server-group DefaultDNS

Example:
ciscoasa(config)# dns server-group DefaultDNS

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**
Specify one or more DNS servers. You may 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.

name-server ip_address [ip_address2] [...] [ip_address6]

Example:
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
Adjust ASP (Accelerated Security Path) Performance and Behavior

The ASP is an implementation layer that puts your policies and configurations into action. It is not of direct interest except during troubleshooting with the Cisco Technical Assistance Center. However, there are a few behaviors related to performance and reliability that you can adjust.

- Choose a Rule Engine Transactional Commit Model, page 14-15
- Enable ASP Load Balancing, page 14-16

Choose 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 with 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 also searches uncompiled rules when evaluating a connection attempt so that new rules can be applied; because 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. With the transactional model, performance should not drop during the rule compilation. The following table clarifies the behavioral difference.

<table>
<thead>
<tr>
<th>Model</th>
<th>Before Compilation</th>
<th>During Compilation</th>
<th>After Compilation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(The rate for connections per second decreases.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(The rate for connections per second is unaffected.)</td>
<td></td>
</tr>
</tbody>
</table>

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 feature reduces the chances that acceptable connections may be dropped during the operation.

Tip

If you enable the transactional model for a rule type, syslogs to mark the beginning and the end of the compilation are generated. These syslogs are numbered 780001 through 780004.

To enable the transactional commit model for the rule engine, use the following command:

```
asp rule-engine transactional-commit option
```

Where the options are:

- access-group—Access rules applied globally or to interfaces.
**Monitoring the 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.

See the following command for monitoring the DNS cache:

- **show dns-hosts**

  This command shows 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.
## History for Basic Settings

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Passphrase</td>
<td>8.3(1)</td>
<td>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: <code>key config-key password-encryption</code>, <code>password encryption aes</code>, <code>configure password encryption aes</code>, <code>show running-config password encryption aes</code>, <code>show password encryption</code>.</td>
</tr>
<tr>
<td>Password Encryption Visibility</td>
<td>8.4(1)</td>
<td>We modified the <code>show password encryption</code> command.</td>
</tr>
</tbody>
</table>
| 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).  
Previously, 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`. |
| ASP Load Balancing                | 9.3(2)            | We introduced this feature. The ASP load balancing mechanism reduces packet drop and improves throughput by allowing multiple cores of the CPU to receive packets from an interface receive ring and work on them independently.  
We introduced the following command: `asp load-balance per-packet-auto`. |