CHAPTER 7

Configuring Basic Settings

This chapter describes how to configure basic settings on your adaptive security appliance that are typically required for a functioning configuration. This chapter includes the following sections:

Configuring the Hostname, Domain Name, and Passwords

This section describes how to change the device name and passwords, and includes the following topics:

Changing the Login Password

The login password is used for Telnet and SSH connections. By default, the login password is “cisco.” To change the password, enter the following command:

Command	Purpose
{**passwd** | **password**} *password*	Changes the 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. Use the no password command to restore the password to the default setting.

Changing the Enable Password

The enable password lets you enter privileged EXEC mode. By default, the enable password is blank. To change the enable password, enter the following command:

Command	Purpose
enable password *password*	Changes the enable 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. This command changes the password for the highest privilege level. If you configure local command authorization, you can set enable passwords for each privilege level from 0 to 15. 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 adaptive security appliance, 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. The default hostname depends on your platform.

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.

Command	Purpose

hostname *name*
 	
Example:
 	
`hostname(config)# hostname farscape`
`farscape(config)#`
	Specifies the hostname for the adaptive security appliance or for a context.
	
	This name can be up to 63 characters. A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.

Setting the Domain Name

The adaptive security appliance 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 security appliance qualifies the name to "jupiter.example.com."

The default domain name is default.domain.invalid.

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

Command	Purpose
domain-name *name* **Example:** hostname(config)# **domain-name example.com**	Specifies the domain name for the adaptive security appliance. For example, to set the domain as example.com.

Setting the Date and Time

This section describes how to set the date and time, either manually or dynamically using an NTP server. Time derived from an NTP server overrides any time set manually. This section also describes how to set the time zone and daylight saving time date range.

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

This section includes the following topics:

Setting the Time Zone and Daylight Saving Time Date Range

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

	Command	Purpose
Step 1	**clock timezone** *zone* [**-**]*hours* [*minutes*]	Sets the time zone. 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	Do one of the following 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:	
	clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]	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**, for example, 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*]	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 lets you set a recurring date range that you do not need to alter 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 saving 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**	Enables authentication with an NTP server.
Step 2	**ntp trusted-key** *key_id*	Specifies an authentication key ID to be a trusted key, which is required for authentication with an NTP server. Where the *key_id* is between 1 and 4294967295. You can enter multiple trusted keys for use with multiple servers.
Step 3	**ntp authentication-key** *key_id* **md5** *key*	Sets a key to authenticate with an NTP server. Where *key_id* is the ID you set in Step 2 using the **ntp trusted-key** command, and key is a string up to 32 characters in length.
Step 4	**ntp server** *ip_address* [**key** *key_id*] [source interface_name] [**prefer**]	Identifies an NTP server. Where the *key_id* is the ID you set in Step 2 using the **ntp trusted-key** command. The **source** *interface_name* 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 adaptive security appliance uses the more accurate one. For example, the adaptive security appliance uses a server of stratum 2 over a server of stratum 3 that is preferred. You can identify multiple servers; the adaptive security appliance uses the most accurate server.

Setting the Date and Time Manually

Command	Purpose
clock set *hh:mm:ss {month day | day month} year*	Sets the date time manually. Where *hh*:*mm*:*ss* sets the hour, minutes, and seconds in 24-hour time. For example, set **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 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 for the **clock set** command.

Configuring the Master Passphrase

This section describes how to configure the master passphrase. This section includes the following topics:

Information About the Master Passphrase

The master passphrase feature allows you to securely store plain text passwords in encrypted format. The master passphrase provides a key that is used to universally encrypt or mask all passwords, without changing any functionality. Passwords that take advantage of this feature include:

- OSPF

- EIGRP
- VPN load balancing
- VPN (remote access and site-to-site)
- Failover
- AAA servers
- Logging
- Shared licenses
- And many more...

Licensing Requirements for the Master Passphrase

Model	License Requirement
All 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.

Adding or Changing the Master Passphrase

This section describes how to configure the master passphrase feature.

Prerequisites

- If failover is enabled but no failover shared key is set, then changing the master passphrase displays an error message, informing you that a failover shared key must be entered to protect the master passphrase changes from being sent as plain text.
- This procedure will only be accepted in a secure session, for example by console, SSH or ASDM via HTTPS.

Detailed Steps

	Command	Purpose

Step 1	**key config-key password-encryption** [*new_passphrase* [*old_passphrase*]]
	
	Example:
	`hostname(config)# key config-key password-encryption`
	`Old key: bumblebee`
	`New key: haverford`
	`Confirm key: haverford`
		Sets the passphrase used for generating the encryption key, between 8 and 128 characters in length. All characters except back space and double quote are accepted for the passphrase.
		
		If you do not enter the new passphrase in the command, you are prompted for it.
		
		When you want to change the passphrase, you also have to enter the old passphrase.
		
		See the "Examples" section on page 7-9 for examples of the interactive prompts.
		
		Note It is advised to use the interactive prompts to enter passwords, to avoid the passwords being logged in the command history buffer.
		
		Use the **no key config-key password-encrypt** command with caution as it will turn 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:** `hostname(config)# password encryption aes`	Enables password encryption. As soon as password encryption is turned on and 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 of enabling password encryption, the command will succeed in anticipation that the passphrase will be available in 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:** `hostname(config)# write memory`	Saves the run time value of the master passphrase and the resultant configuration. Unless that is done, passwords in startup configuration may still be visible if they were not saved with encryption before. Further, 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. Alternately, use the **write memory all** command in system context to save all configuration.

Examples

In the following configuration example, no previous key is present:

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

In the following configuration example, no previous key is present:

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

In the following configuration example, a key already exists:

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

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

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

In the following example, the user wants to key in interactively, but no key is present. The New key and Confirm key prompts will 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.

Prerequisites

- You must know the current master passphrase to disable it. If you do not know the passphrase, see the "Recovering the Master Passphrase" section on page 7-10.
- This procedure will only be accepted in a secure session, for example by console, SSH or ASDM via HTTPS.

Detailed Steps

	Command	Purpose

Step 1	**no key config-key password-encryption** [*old_passphrase*]]
	
	Example:
	`hostname(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:** `hostname(config)# write memory`	Saves the run time value of the master passphrase and the resultant configuration. The non-volatile memory containing the passphrase will be erased and overwritten with 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. Alternately, use the **write memory all** command in system context to save all configuration.

Recovering the Master Passphrase

You cannot recover the master passphrase.

If the master passphrase is lost or unknown, it could be removed by using the **write erase** command followed by the **reload** command. This removes the master key along with the configuration containing the encrypted passwords.

Feature History for the Master Passphrase

Table 7-2 lists each feature change and the platform release in which it was implemented.

Table 1 Feature History for the Master Passphrase

Feature Name	Platform Releases	Feature Information
Master Passphrase	8.3(1)	This feature was introduced. The following commands were introduced: **key config-key password-encryption**, **password encryption aes**, **clear configure password encryption aes**, **show running-config password encryption aes**.

Configuring the DNS Server

Some adaptive security appliance 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 for traceroute, and the adaptive security appliance can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names.

Note The adaptive security appliance 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 the "Configuring DDNS" section on page 9-2.

Prerequisites

Make sure you configure the appropriate routing for any interface on which you enable DNS domain lookup so you can reach the DNS server. See the "Information About Routing" section on page 19-1 for more information about routing.

Detailed Steps

	Command	Purpose
Step 1	**dns domain-lookup** *interface_name* **Example:** `hostname(config)# dns domain-lookup inside`	Enables the adaptive security appliance 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 adaptive security appliance uses for from-the-box requests. Other DNS server groups can be configured for VPN tunnel groups. See the **tunnel-group** command in the *Cisco ASA 5500 Series 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 6 IP addresses in the same command, separated by spaces, or you can enter each command separately. The security appliance tries each DNS server in order until it receives a response.

Setting the Management IP Address for a Transparent Firewall

This section describes how to configure the management IP address for transparent firewall mode, and includes the following topics:

Information About the Management IP Address

A transparent firewall does not participate in IP routing. The only IP configuration required for the adaptive security appliance is to set the management IP address. This address is required because the adaptive security appliance uses this address as the source address for traffic originating on the adaptive security appliance, such as system messages or communications with AAA servers. You can also use this address for remote management access.

For IPv4 traffic, the management IP address is required to pass any traffic. For IPv6 traffic, you must, at a minimum, configure the link-local addresses to pass traffic, but a global management address is recommended for full functionality, including remote management and other management operations.

Note In addition to the management IP address for the device, you can configure an IP address for the Management 0/0 or 0/1 management-only interface. This IP address can be on a separate subnet from the main management IP address. See the "Configuring General Interface Parameters" section on page 8-24.

Although you do not configure IPv4 or global IPv6 addresses for other interfaces, you still need to configure the security level and interface name according to the "Configuring General Interface Parameters" section on page 8-24.

Licensing Requirements for the Management IP Address for a Transparent Firewall

Model	License Requirement
All 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. For multiple context mode, set the management IP address within each context.

Firewall Mode Guidelines

Supported in transparent firewall mode. For routed mode, set the IP address for each interface according to the "Configuring General Interface Parameters" section on page 8-24.

IPv6 Guidelines

- Supports IPv6.
- The following IPv6 address-related commands are not supported in transparent mode, because they require router capabilities:
  - **ipv6 address autoconfig**
  - **ipv6 nd suppress-ra**

  For a complete list of IPv6 commands that are not supported in transparent mode, see the "IPv6-Enabled Commands" section on page 19-10.
- No support for IPv6 anycast addresses.
- You can configure both IPv6 and IPv4 addresses.

Additional Guidelines and Limitations

- In addition to the management IP address for the device, you can configure an IP address for the Management 0/0 or 0/1 management-only interface. This IP address can be on a separate subnet from the main management IP address. See the "Configuring General Interface Parameters" section on page 8-24.
- Although you do not configure IP addresses for other interfaces, you still need to configure the security level and interface name according to the "Configuring General Interface Parameters" section on page 8-24.

Configuring the IPv4 Address

This section tells how to configure the IPv4 address.

Detailed Steps

Command	Purpose
ip address *ip_address* [*mask*] [**standby** *ip_address*] **Example:** hostname(config)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2	This address must be on the same subnet as the upstream and downstream routers. You cannot set the subnet to a host subnet (255.255.255.255). The **standby** keyword and address is used for failover. See the "Configuring Active/Standby Failover" section on page 59-7 or the "Configuring Active/Active Failover" section on page 58-8 for more information.

Configuring the IPv6 Address

When you configure a global address, a link-local addresses is automatically configured on each interface, so you do not also need to specifically configure a link-local address.

Note If you want to only configure the link-local addresses, see the **ipv6 enable** or **ipv6 address link-local** command in the *Cisco ASA 5500 Series Command Reference*.

Detailed Steps

Command	Purpose
ipv6 address *ipv6-prefix/prefix-length* **Example:** hostname(config)# ipv6 address 2001:0DB8::BA98:0:3210/48	Assigns a global address. When you assign a global address, link-local addresses are automatically created for each interface. **Note** The **eui** keyword, which is available in routed mode, is not available in transparent mode. The EUI address ties the unicast address to the adaptive security appliance interface MAC address; but because the transparent mode IP address is not tied to an interface, an interface MAC address cannot be used. See the "IPv6 Addresses" section on page A-5 for more information about IPv6 addressing.

Configuration Examples for the Management IP Address for a Transparent Firewall

The following example sets the IPv4 and IPv6 global management IP addresses, and configures the inside, outside, and management interfaces:

```
hostname(config)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config)# ipv6 address 2001:0DB8::BA98:0:3210/48

hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# nameif inside
```

```
hostname(config-if)# security-level 100
hostname(config-if)# no shutdown

hostname(config-if)# interface gigabitethernet 0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# no shutdown

hostname(config-if)# interface management 0/0
hostname(config-if)# nameif management
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# ipv6 address 2001:0DB8::BA98:0:3211/48
hostname(config-if)# no shutdown
```

Feature History for the Management IP Address for a Transparent Firewall

Table 7-2 lists the release history for this feature.

Table 7-2 Feature History for Transparent Mode Management Address

Feature Name	Releases	Feature Information
IPv6 support	8.2(1)	IPv6 support was introduced for transparent firewall mode.