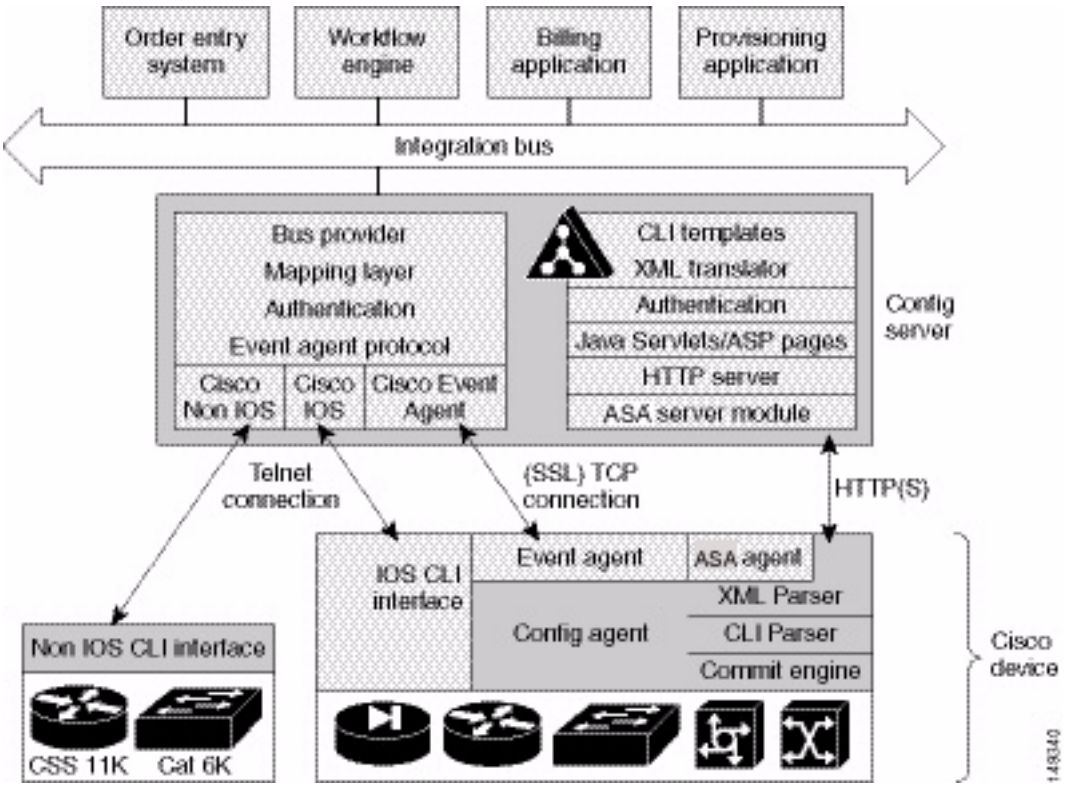
ASA Firewall Device Support

Cisco Configuration Engine provides configuration management and image service to Cisco Adaptive Security Appliance devices (ASA device). Figure 22-1 shows a functional block diagram of Cisco Configuration Engine including the ASA device interface module.

Figure 22-1 ASA-Compatible Configuration Engine Module Interaction



Note Encryption must be enabled during setup for ASA devices to supported by Cisco Configuration Engine.

ASA Device Polls for Updates

The ASA device contacts the ASA module in the Cisco Configuration Engine to report information about itself. This occurs when the ASA starts, when any of the reported information changes, and whenever the ASA wants to check for updates. ASA sends the **DeviceDetails** message to the server. The **DeviceDetails** provides the Cisco Configuration Engine with an update on the version of the software that the device is currently running. The information received in the **DeviceDetails** message is logged into the log file (*asa.log*) for reference.

The server responds with the **UpdateInfo** message. This message contains (optionally):

- Checksum and URL for the configuration file the ASA should be running
- Checksum and URL for the ASA image
- Checksum and URL for the ASA Device Manager (ASDM) image
- URL for reporting any errors

The ASA compares the checksum in the message with the current checksum of the component concerned. In the case of configuration, it also calculates the cryptochecksum of the running configuration and compares that with the one calculated last time when the configuration was updated from the Cisco Configuration Engine. An update is required if the checksum (or cryptochecksum) differs.

If a software/configuration update is required, the ASA sends requests on the respective URLs.

Configuration Processing

For any configuration update that is required, the ASA sends an HTTPS GET request to the returned URL. The configuration file is completely read into a local buffer before being applied. This message is used to prevent a connection error from leaving the ASA in a partially configured state. If there are no errors (or the *errors* attribute of the **config-data** message is *continue*) while applying the configuration commands, the running configuration is copied to flash with the write memory command. All configuration files work in the *replace* mode.

Completion of configuration download by a ASA device results in a log file entry indicating the same in *asa.log*.

Note The log entry does not mean that the configuration is successfully applied on a ASA device. It only means that the ASA device has downloaded the configuration file.

Image Processing

The **DeviceDetails** XML message sent along with the initial HTTPS POST optionally has information regarding the ASA image, its version, and checksum. Cisco Configuration Engine returns with the UpdateInfo XML containing image URLs and checksums based on the entries in the directory. The ASA downloads and applies images one after the other (and reloads itself if required). Any error is processed as mentioned next.

Note There is no notification for the successful image download because the image distribution can be external to Cisco Configuration Engine and hence, the ASA server cannot keep track of the same. Also, the ASA device does not provide any image upgrade successful indication.

Error Processing

All errors are reported by way of HTTPS POST to the error URL using the **ErrorList** message.

Each configuration error report (type=error, warning or info) is logged by the Cisco Configuration Engine into *asa.log*. The log file is cyclic to limit disk space usage.

Note An error occurring during configuration does not mean that the downloaded configuration is not applied on the ASA entirely. It only means that the error mentioned in the log file has happened with respect to this particular device.

Any error or notification (type= warning, notification, informational, debugging, emergency, alert, critical, and error) that occurs while retrieving the data at one of the URLs received from the Cisco Configuration Engine results in log file entries.

If a failure is encountered during the processing of any of the URLs in the UpdateInfo response from the server, the error is reported to the Error URL. Also, processing of all URLs received in the current call home is discontinued. Any further processing is deferred till the ASA calls home again.

After all the updates are successfully completed, another **DeviceDetails** message is sent to the Cisco Configuration Engine by the ASA device. Cisco Configuration Engine again sends the **UpdateInfo** and checksum. The ASA device compares the checksums and finds that no further updates are required.

Processing a DeviceDetails Request from ASA Device

The sequence of processing a DeviceDetails request from a ASA device is as follows:

1. ASA device contacts the Cisco Configuration Engine with the **DeviceDetails** message as XML payload by means of an HTTPS post request.
2. New ASA Configuration servlet receives request, parses XML, and retrieves DeviceID.
3. Device is authenticated.
4. Template associated with this DeviceID is processed to generate a configuration file.
5. Configuration file is converted into XML format as per the ASA DTD and the file is saved (over-written in case a file is already present for this DeviceID).
6. Checksum of XML configuration file is calculated and URL noted.
7. URLs and checksums for ASA image and PDM images are retrieved from image object attached with the ASA device.
8. Checksums and URLs for configuration files and various images (if the corresponding checksum differs) and the Error URL are sent to the ASA device as an HTTP response with an XML payload (UpdateInfo).
9. Device now requests for configuration/image based on the content of the UpdateInfo response.
10. Errors are encountered, information is posted to error URL.

11. The error servlet logs the errors to *asa.log*.

ASA DeviceID

The following ASA CLI decides the value of the DeviceID sent by the ASA in the DeviceDetails request:

[no] auto-update device-id hardware-serial | hostname | ipaddress [*if-name***] | mac-address [***if-name***] | string text**

- **auto-update device-id** command specifies the device ID to send when polling the Management server.
- **no auto-update device-id** command resets the device ID to the default of hostname.
- **hardware-serial** option uses the ASA serial number.
- **hostname** option uses the ASA host name.
- **ipaddress** option uses the IP address of the interface with the name **if-name**.

  If the interface name is not specified, it uses the IP address of the interface used to communicate with the remote management server.
- **mac-address** option uses the MAC address of the interface with the name *if-name*.

  If the interface name is not specified, it uses the MAC address of the interface used to communicate with the remote management server.
- **string text** option uses the specified *text*.

  The text can not contain white space or the characters ‘, “, <, >, &, and ?.

Note Since the DeviceID provided by the ASA is internally mapped to ConfigID and EventID in the Cisco Configuration Engine, it only supports hyphen (-), underscore (_), period (.) and alphanumeric characters.

Security Considerations

Because ASA devices are firewall devices and the configuration information is vital, the information is transported securely by using SSL.

HTTPS is enforced as the transport protocol between ASA devices and Cisco Configuration Engine under all circumstances. **DeviceDetails**, **Update Info**, **ErrorInfo,** and configuration files are transported using only HTTPS. The authorization mechanism used in the Configuration Service is leveraged in the ASA server module. The URLs supplied by you toward the ASDM/ASA-image can use HTTP or HTTPS.

ASA Device Polling Setup

ASA devices can be configured to poll the Cisco Configuration Engine at regular intervals for configuration or image updates. This entry has to be made by you on the ASA device itself. Details are available from ASA device documentation. CLI format for the same is as follows:

Usage: auto-update device-id hardware-serial | hostname |

ipaddress [<if_name>] | mac-address [<if_name>] | string <text>

no auto-update device-id

auto-update poll-period <poll-period> [<retry-count>

[<retry-period>]]

no auto-update poll-period

auto-update server <url> [verify-certificate]

no auto-update server

auto-update timeout <period>

no auto-update timeout

Example:

```
auto-update device-id string myASADevice
auto-update poll-period 120
auto-update server https://********@cns-ie2100/cns/ASAConfig
```

The URI to be polled on the Cisco Configuration Engine is:

/cns/ASAConfig

The **auto-update poll-period** command specifies how often to poll the Management server for configuration or image updates. The *poll-period* parameter specifies how often (in minutes) to check for an update. The default is 720 (12 hours). The *retry-count* option specifies how many times to try re-connecting to the server if the first attempt fails. The default is 0. The *retry-period* option specifies how long to wait (in minutes) between retries. The default is 5.

The **no auto-update poll-period** command resets the poll period to the default.

Also, you must map the hostname of the server on the ASA device with its IP address. You can do this by using the *name* command as follows:

asafirewall# **conf t**

asafirewall(config)# **name <ip_address of the server> <hostname of the server>**

Configuration and Restrictions

The ASA compatibility module is set up along with Configuration Service during the initial setup of the system. You need not do anything specifically to enable ASA compatibility.

ASA devices with **software versions of 8.2 and higher** are supported by Cisco Configuration Engine (auto-update from the ASA device side was introduced in this version). All ASA hardware platforms that run software version 8.2 or higher will be supported.

The configuration files will be generated with options config-action= **replace** and errors=**revert**. No other options are supported.

Following are the different type of configuration-actions.

- Replace—Specifies that the current configuration should be cleared before applying the new configuration.
- Merge—Merges the current configuration with the new configuration file.

Following are the different type of error-actions.

- Continue—Continues with applying the new configuration, even if there is a configuration error.

- Revert—Reverts the old configuration from the flash without rebooting when there is a configuration error.
- Stop—Stops reading the rest of the configuration when a command causes an error.