CHAPTER 7

Using Hardware Keystores and Security Worlds

This chapter describes how to set up hardware keystores and nCipher security worlds that use them. It covers these topics:

Setting Up a Keystore

The nForce device from nCipher is an optional, factory-installed hardware upgrade module for the ACE XML Gateway.

Note In addition to providing hardware keystores, the nCipher card provides encryption/decryption acceleration. For information on enabling this functionality, see "Enabling SSL Acceleration" section on page 9-61.

If you have nCipher hardware-based key storage devices, you can use them by adding the appliance to a new or existing nCipher security world. A "security world" is a set of appliances configured to use the hardware-backed keys that nCipher security modules provide. These appliances share secure key information, as well as the set of configuration files and smart cards associated with the keys. When you create the security world, you can set options such as the number of smart cards in the set, whether keys protected by the security world can be recovered.

Each appliance that is to use the hardware-backed keys must have an nCipher card pre-installed. The smart cards fit into an nCipher card reader that attaches physically to a port on the appliance. Because smart cards are used only for nCipher administration tasks, such as setting up security worlds or adding appliances to existing security worlds, the card reader does not need to remain attached to the appliance after nCipher administration tasks are complete. Therefore, you can use a single card reader to configure the nCipher functions of multiple appliances.

To use a hardware keystore in a clustered environment, you must set up a hardware keystore and a security world that uses it on each appliance in the cluster.

Because the initialization process involves changing the settings of hardware switches, you must have physical access to the appliances that house the keystore hardware. You'll also need the administrative privileges required to run the terminal-based nCipher software tools that reconfigure the keystore.

Because proper operation of the smart cards is vital to the accessibility of the keystore and security world, it is recommended that you create a backup set of smart cards and keep the backup cards in an off-site location. Accordingly, the examples in this chapter create a set of four cards, any two of which can be used to edit the security world, thus allowing the other two cards to be stored in a safe location.

This guide provides complete, step-by-step descriptions of all tasks related to using nCipher modules with the Cisco ACE XML Gateway. However, you should review the nCipher documentation that accompanied your nCipher-equipped appliance for more information about the nCipher system.

Creating a New Security World

This section describes how to create a new nCipher security world and add a Gateway to it. Subsequently, you can add more Gateways to this security world by following the steps in "Joining an Existing Security World" section on page 7-40.

When configuring a new security world, you must specify the number of smart cards to configure (n), and the number of cards that must be physically present (k) to add a new appliance to the security world. In the instructions in this section, the assumption is n=4 and k=2. That is, the security world has four administrator cards, and any two of them must be present to add new modules to the security world.

Note Before executing any nCipher commands, determine requirements for your IT environment's security world and see the nCipher documentation for further explanation of the security world options available to you.

Before You Begin

Before configuring the security world, be sure you have the following:

- Physical access to the appliance and its nCipher card reader.
- The root password for the appliance.
- Four nCipher smart cards, numbered and labeled. Feel free to use any labeling scheme that is convenient for you.

Creating the New Security World

Take the following steps to create a simple security world having four administrator cards:

Step 1 On the appliance, access the `bash` shell as `root` user (from the main menu, choose **Advanced Options > Run bash**).

For details, see "Accessing the bash Shell" section on page 4-17.

Step 2 On the appliance chassis, move the switch on the nCipher module to the "I" position. (The card may be either on the front or back panel, depending on the appliance model.)

This action indicates to the nCipher module that you intend to put it into "pre-initialization" mode. However, you will see no additional feedback other than the changed position of the switch. Simply moving the switch does not change the module's mode; you must reset the module to put it into a new mode.

Note In the next step, you initialize the nCipher keystore. Doing so destroys stored private keys and the hardware password that protects them. If those keys are important, you should make sure that you have a way to recover them before initializing a previously used keystore. **There is no way to recover the hardware password for the keystore if you lose it or if you erase it by reinitializing the keystore.** Be extremely careful with the hardware password and with keys stored in the keystore.

Step 3 Reset the module by taking one of the following actions:

- Press the reset button next to the mode switch. (You may need to use a pen, straight pin, or paper clip to reach the reset button.)

or:

- As the `root` user in a terminal session on the appliance, execute the following command:

  ```
  /opt/nfast/bin/nopclearfail -ca
  ```

  The `-ca` option specifies that the `nopclearfail` command is to initialize all available nCipher modules. To initialize a particular module specified by its number, use the `-m` and `-c` options instead, as in the following example:

  ```
  /opt/nfast/bin/nopclearfail -c -m 1
  ```

  The `-c` option indicates that the `nopclearfail` command is to clear the nCipher module that the `-m` option specifies. In this example, the options specify that the command is to clear module #1.

The shell indicates successful reset by printing to standard output a line similar to the following:

```
module 1, command , clearunit: OK
```

Also, the blue LED on the nCipher module blinks in single, short flashes. (The nCipher light is next to the three-position, M, I, O, switch on the nCipher card itself.) This feedback occurs whether you use the command line or the hardware reset switch to change the module's mode.

Step 4 To confirm the module's current operating mode, execute the following command from the command line

```
/opt/nfast/bin/enquiry
```

The `enquiry` command summarizes the status of each available nCipher module. If you've switched successfully to pre-initialization mode, a value of `pre-initialization` appears in the `mode` field of the summary for each module you reset.

Step 5 Plug the nCipher card reader into the nCipher PCI card interface on the appliance.

An LED lights on the card reader to indicate that it is connected. The LED is red if no card is present or the card cannot be read, or green if a valid smart card is present. Do not put a card in the reader yet.

On older nCipher card readers and appliances in which the card is on the back panel, the plug may be too short to reach beyond the lip that extends over the chassis' back panel. If the plug on the nCipher card reader is too short to seat firmly, attach both the male and female gender changers to the plug to extend it.

Step 6 To create the new security world, execute the command:

```
/opt/nfast/bin/new-world -i -Q cardsReqd/cardsInSet -m moduleNum
```

where:

- *cardsReqd* specifies the number of smart cards that must be physically present in order to edit the security world.
- *cardsInSet* specifies the total number of smart cards in the set.

- *moduleNum* specifies the nCipher module to initialize.

Your new-world command must specify values that describe your particular installation. For example, to initialize four smart cards and require that two be present to edit the security world, you would specify `2` as the *`cardsReqd`* value and `4` as the *`cardsInSet`* value, as the following example:

```
/opt/nfast/bin/new-world -i -Q 2/4 -m 1
```

To initialize two smart cards and require only one to be present when editing the security world, substitute `1/2` for the `2/4` value in the example.

The `new-world` utility initializes a single nCipher module at a time. To initialize multiple nCipher modules, run the `new-world` utility once for each module, using the `-m` option to indicate the module that `new-world` is to initialize.

For example, in the preceding command, the `-m 1` argument indicates that `new-world` is to initialize module # 1. For more information, see the nCipher documentation that accompanied your nCipher-equipped appliance.

After a few moments, the shell prompts you to insert the first smart card in the set.

Step 7 Insert the card into the card reader, with the chip side up, pushing gently but firmly until the card clicks into place.

The light on the card reader turns green and the shell prompts you to initialize the card or set its password.

Step 8 If the **Module 1 slot contains an unrecognized card. Overwrite it?** prompt appears, type **yes** and press the **Enter** key.

The appliance prompts you to set a new password for the card.

If the unrecognized card prompt does not appear, go on to the next step.

Step 9 Enter the new password for the card and, when prompted, confirm the password. If the second password does not match the first exactly, you are prompted to set the password again.

Note Do not lose smart card passwords. You'll need them to add other modules to the security world.

The appliance prompts you to remove the card.

Step 10 Remove the card from the reader.

Step 11 Repeat the preceding steps as prompted to set passwords for the remaining cards in the set.

When you've set passwords for all cards in the set, the console displays the **security world created** message followed by the command-line prompt.

Step 12 To confirm the existence of the new security world, execute the following command line:

```
ls -la /opt/nfast/kmdata/local
```

The shell lists the contents of the specified directory. If the security world was created successfully, the directory contains one world file and at least one module_*X* file, as in the example listing:

```
# ls -la /opt/nfast/kmdata/local
total 32
drwxrwsr-x 2 nfast nfast 4096 Jan 24 00:16 .
drwxrwsr-x 8 nfast nfast 4096 Jan 23 23:09 ..
-rw-r--r-- 1 root nfast 856 Jan 24 00:16
                    module_XXXX-XXXX-XXXX
-rw-r--r-- 1 root nfast 16472 Jan 24 00:16
                    world
```

Step 13 Disconnect the card reader from the nCipher PCI card.

Step 14 Move the switch on the nCipher module to the "O" position.

This action indicates to the nCipher module that you intend to put it into "operational" mode.

Step 15 Reset the module by taking one of the following actions:

- Press the reset button next to the mode switch. (You may need to use a pen, straight pin, or paper clip to reach the reset button.)
- Alternatively, as the `root` user in a terminal session on the appliance, execute the following command:

  ```
  /opt/nfast/bin/nopclearfail -ca
  ```

  The shell indicates successful reset by printing to standard output a line similar to the following:

  ```
  module 1, command , clearunit: OK
  ```

  The `-ca` option specifies that the `nopclearfail` command is to initialize all available nCipher modules. To initialize a particular module specified by its number, use the `-m` and `-c` options instead, as in the following example:

  ```
  /opt/nfast/bin/nopclearfail -c -m 1
  ```

  The `-c` option indicates that the `nopclearfail` command is to clear the nCipher module that the `-m` option specifies. In this example, the options specify that the command is to clear module #1.

When you have reset the nCipher module to enter operational mode, the blue LED on the nCipher module blinks in long flashes.

Step 16 Verify that the module is now operational by executing the following command line:

```
/opt/nfast/bin/enquiry
```

The `enquiry` command summarizes the status of each available nCipher module. If you've switched successfully to operational mode, a value of `operational` appears in the `mode` field of the summary for each module you reset.

Step 17 Exit the `bash` shell.

Step 18 In the **Advanced Options** menu, choose the **SSL Engine Configuration** item.

Step 19 Choose **chil** to enable the nCipher CHIL device.

Step 20 In the **Advanced Options** menu appears, choose the **Return to Main Menu** item.

Step 21 Choose the **Manage Gateway Processes** item.

Step 22 Choose **Restart All Services**.

The shell attempts to restart the appliance, and displays a status screen upon completion of this task.

After the appliance restarts in the new configuration, the nCipher module is ready for use with the private keys created in this security world. For more information, see the nCipher documentation that accompanied your appliance.

The public/private keypair can now be applied to secure communication between the appliances. To apply the keypair to service traffic, create a resource object in the policy for the keypair in the Manager web console.

Joining an Existing Security World

This section describes how to add a Gateway to an existing nCipher security world. For general information on security worlds and instructions for creating a security world, see "Creating a New Security World" section on page 7-36. Also, see the nCipher documentation that accompanied your appliance.

Before You Begin

Before you add another appliance to a security world, be sure you have the following:

- An appliance on which the security world has already been initialized. For more information, see "Creating a New Security World" section on page 7-36. The instructions in this section refer to this appliance as the source system.
- A copy of the security world files. This is a directory of files that define security world configuration information. Typically, these files reside in the `/opt/nfast/kmdata` directory of the source system.
- Administrator cards from the existing security world. The number of cards you need from the set depends on how the security world was configured when it was created.
- Physical access to the appliance to be added to the security world. The instructions in this section refer to this appliance as the destination system.
- An nCipher card reader attached to the destination system.
- The root passwords for the source and destination systems.

Adding an Appliance to the Security World

Adding an appliance to an existing nCipher security world involves using files copied from the source appliance to initialize the nCipher card on the destination system, as follows:

Step 1 On the destination system, run the `bash` shell as the `root` user.

Step 2 Move the switch on the nCipher module to the "I" position.

Step 3 Reset the module by taking one of the following actions:

- Press the reset button next to the mode switch.

  You may need to use a pen, straight pin, or paper clip to reach the reset button.

or:

- Execute the following command line on the destination system:

  ```
  /opt/nfast/bin/nopclearfail -ca
  ```

  The shell indicates successful reset by printing to standard output a line similar to the following:

  ```
  module 1, command , clearunit: OK
  ```

  The `-ca` option specifies that the `nopclearfail` command is to initialize all available nCipher modules. To initialize a particular module specified by its number, use the `-m` and `-c` options instead, as in the following example:

  ```
  /opt/nfast/bin/nopclearfail -c -m 1
  ```

The `-c` option indicates that the `nopclearfail` command is to clear the nCipher module that the `-m` option specifies. In this example, the options specify that the command is to clear module #1.

When you have reset the nCipher module to enter pre-initialization mode, the blue LED on the nCipher module blinks in short flashes.

Step 4 To confirm the module's current operating mode, execute the following command on the destination system:

```
/opt/nfast/bin/enquiry
```

The `enquiry` command summarizes the status of each available nCipher module. If you've switched successfully to pre-initialization mode, a value of `pre-initialization` appears in the `mode` field of the summary for each module you reset.

Step 5 Plug the nCipher card reader into the nCipher PCI card interface.

An LED lights on the card reader to indicate that it is connected. The LED is red if no card is present or the card cannot be read. The LED is green if a valid smart card is present. **Do not put a card in the reader yet.**

On older nCipher card readers and appliance chassis in which the card is on the back panel, the plug may be too short to reach beyond the lip that extends over the back of the appliance chassis. If the plug on the nCipher card reader is too short to seat firmly, attach both the male and female gender changers to the plug to extend it.

Step 6 On the source system, run `bash` as the `root` user.

For more information, see "Accessing the bash Shell" section on page 4-17.

Step 7 Copy the existing security world files from the source system's `/opt/nfast/kmdata` directory into the same directory path on the destination system.

You may need to use the `scp` program to copy the data onto the destination system.

For the files to work properly on the destination system, their ownership properties must be retained during the transer. Execute the following commands to move the files while preserving their ownership attributes:

- on the source gateway

  ```
  cd /opt/nfast/kmdata
  ```

  ```
  tar -cvf archive.tar ./*
  ```

  ```
  scp /opt/nfast/kmdata/archive.tar <targetHost>:/opt/nfast/kmdata/
  ```

  Where `<targetHost>` is the hostname or IP address of the system to which you are moving the file.

- on the destination gateway

  ```
  cd /opt/nfast/kmdata
  ```

  ```
  tar -xvf archive.tar
  ```

Note After copying the files, you should ensure that their ownership has been maintained by checking their ownership manually. The files should be owned by the user "agateway".

Step 8 On the destination system, execute the following command line to add the destination system to the security world:

```
/opt/nfast/bin/new-world -l -s 0 -m 1
```

You are prompted for passwords and smart cards from the administrator card set. Enter passwords and insert cards as directed.

Note The arguments to the `new-world` command can be customized. For more information, see the nCipher documentation that accompanied your nCipher-equipped appliance.

Step 9 Disconnect the card reader from the nCipher PCI card.

Step 10 Move the switch on the nCipher module to the "O" position.

This action indicates to the nCipher module that you intend to put it into operational mode. At this point, the blue light on the back of the nCipher card still blinks in short flashes to indicate that the card is still in pre-initialization mode. Simply moving the switch does not change the module's mode; you must reset the module to put it into a new mode.

Step 11 Reset the module by taking one of the following actions:

- Press the reset button next to the mode switch. (You may need a pen, straight pin, or paper clip to reach the reset button.)
- Alternatively, as the `root` user in a terminal session on the appliance, execute the following command:

  ```
  /opt/nfast/bin/nopclearfail -ca
  ```

  The shell indicates successful reset by printing to standard output a line similar to the following:

  ```
  module 1, command , clearunit: OK
  ```

  The `-ca` option specifies that the `nopclearfail` command is to initialize all available nCipher modules. To initialize a particular module specified by its number, you can use the `-m` and `-c` options instead, as in the following example:

  ```
  /opt/nfast/bin/nopclearfail -c -m 1
  ```

  The `-c` option indicates that the `nopclearfail` command is to clear the nCipher module that the `-m` option specifies. In this example, the options specify that the command is to clear module #1.

When you have reset the nCipher module to enter operational mode, the blue LED on the nCipher module blinks in long flashes.

Step 12 Verify that the module is now operational by executing the following command line:

```
/opt/nfast/bin/enquiry
```

The `enquiry` command summarizes the status of each available nCipher module. If you've switched successfully to operational mode, a value of `operational` appears in the `mode` field of the summary for each module you reset.

Step 13 Exit the `bash` shell.

Step 14 In the **Advanced Options** menu, choose the **SSL Engine Configuration** item.

The **SSL Engine** screen appears.

Step 15 Choose **chil** to enable the nCipher CHIL device.

The **Advanced Options** menu appears.

Step 16 Choose the **Return to Main Menu** item.

Step 17 In the **Main Menu** menu, choose the **Manage Gateway Processes** item.

The **Manage Gateway Processes** menu appears.

Step 18 Choose the **Restart All Services** item.

The shell attempts to restart the appliance in the currently-specified configuration, and displays a status screen upon completion of this task.

After the appliance restarts, its nCipher module is ready for use with the private keys the existing security world provides. For more information, see the nCipher documentation that accompanied your appliance.