



Palo Alto Networks Firewall

nShield® HSM Integration Guide

2024-10-21

Table of Contents

1. Introduction	1
1.1. Product configurations.....	1
1.2. Requirements	2
1.3. Considerations for keys.....	3
2. Procedures	5
2.1. Prepare the RFS and the HSM(s)	5
2.2. Set up connectivity between the Firewall, the HSM, and the RFS	6
2.3. Encrypt the master key using the HSM	11
2.4. Store the key used in SSL/TLS decryption	13
2.5. Adding more HSMs	18
3. Additional resources and related products	19
3.1. nShield Connect	19
3.2. nShield as a Service	19
3.3. Entrust products	19
3.4. nShield product documentation	19

Chapter 1. Introduction

This Integration Guide describes the deployment of a Palo Alto Networks Firewall with an nShield Connect hardware security module (HSM). The HSM securely generates and stores digital keys. It provides both logical and physical protection from non-authorized use and potential adversaries. The HSM-Firewall integration provides security by protecting the master keys. The HSM can also provide protection for the private keys used in SSL/TLS decryption, both in SSL forward proxy and SSL inbound inspection.

This guide assumes that there is no existing nShield Security World. For instructions to create a Security World, see the *User Guide* for your HSM. In situations in which a Security World already exists, parts of this integration guide can still be used for the generation and subsequent storage of keys.

The benefits of using an nShield HSM with the Palo Alto Networks Firewall include:

- Secure encryption and storage of the firewall master key and private keys.
- FIPS 140 Level 3 validated hardware.

1.1. Product configurations

Entrust has successfully tested nShield HSM integration with the Palo Alto Networks Firewall in the following configurations:

- PAN-OS v10.1, v10.2, v11.0 with Entrust Security World v12.40.2



Palo Alto does not support firewall master key protection when using Entrust nShield HSM firmware 12.72.1 and 13.2.2. In addition, firewall master key protection is not supported with the use of a FIPS 140 Level 3 enabled Security World. FIPS 140 Level 2 is required for this feature.

nShield Model	Security World Client	Connect Image	Firmware	Security World Version	Tested / Validated*
nShield 5c	12.40.2	13.3.2	13.2.2	v3	Not Supported
Connect XC	12.40.2	12.80.4	12.72.1 (FIPS 140-2 certified)	v2**	1,2,3 / 2,3

nShield Model	Security World Client	Connect Image	Firmware	Security World Version	Tested / Validated*
Connect XC	12.40.2	12.60.10	12.50.11 (FIPS 140-2 certified)	v2**	1,2,3 / 1,2,3

*Tested/Validated use cases:

1. Firewall Master Key Protection
2. SSL/TLS encrypt/decrypt (Inbound Inspection)
3. SSL/TLS Outbound encrypt/decrypt (Forward Proxy)

**Compatibility Pack 1.1.0 required to build v2 world.

1.2. Requirements

1.2.1. Before starting the integration process

Familiarize yourself with:

- *Installation Guide* and *User Guide* for your HSM.
- *nShield Remote Administration User Guide*.
- *Security World v12.40 Compatibility Package v1.1.0 Release Notes*
- [PAN-OS® 10.2 Administrator's Guide](#)
- [PAN-OS® 11.0 Administrator's Guide](#)

1.2.2. Before using Entrust hardware and software

The following preparations must be made before starting to use Entrust products:

- Each HSM uses a remote file system (RFS). You can configure the RFS on any computer running nShield Security World software.
- The RFS computer can also be used as a client to the HSM, to allow presentation of smart cards using nShield Remote Administration, an optional product. For information, see the *nShield Remote Administration User Guide*.
- A correct quorum for the Administrator Card Set (ACS).
 - For creating the Security World, determine who within the organization will act as

custodians of the ACS.

- Obtain enough blank smart cards to create the Administrator Card Set (ACS).
- Operator Card Set (OCS), Softcard, or Module-Only protection.
 - If OCS protection is to be used, a 1-of-N quorum must be used.
- Firewall configuration with usable ports:
 - 9004 for the HSM nfast server (hardserver).
 - 8200 for the Firewall.

Furthermore, the Security World parameters must be defined. For details of the security implications of the choices, see the *nShield Security Manual*:

- Whether your Security World must comply with FIPS 140 Level 3 standards.
 - If using FIPS 140 Level 3, it is advisable to create an OCS for FIPS authorization. The OCS can also provide key protection for the Firewall master key. For information about limitations on FIPS authorization, see the *Installation Guide* of the nShield HSM.



Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

- Whether to instantiate the Security World as recoverable or not.

1.2.3. Before using the Palo Alto Networks Firewall

The following preparations must be made before starting to use the Palo Alto Networks Firewall:

- Obtain a Palo Alto Networks customer support account. This account requires access to the latest software releases.
- Procure a Palo Alto Networks Firewall appliance, or set up the Firewall in a bare-metal computer. A virtual machine (VM) can also be used. This guide was tested using a VMWare ESXi virtual machine.
- Upgrade the Firewall installation software with the latest package to be tested.
- The nShield RFS version must be compatible with the Palo Alto Networks Firewall, see [Product configurations](#).

1.3. Considerations for keys

1024-bit and 2048-bit RSA keys are supported but it is recommended to use 2048-bit

keys. Security Worlds that meet FIPS 140 Level 3 standards require 2048-bit keys.

Chapter 2. Procedures

The high-level procedure to install and configure a Palo Alto Network Firewall with an nShield HSM is as follows:

1. Set up the HSM and the Security World.
2. Configure the Firewall to authenticate with the HSM(s).
3. Encrypt the master key on a Firewall and store it in the HSM.
4. Store the keys used for SSL forward proxy or SSL inbound inspection decryption.
5. Perform attestation that:
 - The master key is encrypted on the HSM.
 - The certificate use in SSL/TLS forward proxy is successfully imported into the Firewall.

2.1. Prepare the RFS and the HSM(s)

Each nShield HSM must have a remote file system (RFS) configured. The RFS includes master copies of all the files that the HSM requires, see the *User Guide* for your HSM.

If more than one HSM is used, they must be in the same, v2, Security World.

2.1.1. Upgrade the RFS software

To upgrade the RFS software:

1. Check the software version of the RFS by running the `ncversions` command.
2. If the software is older than **v12.60.11**, upgrade it. For instructions, see the *User Guide* for your HSM.

2.1.2. Install the Security World v12.40 Compatibility Package on the RFS

The v12.40 Compatibility Package must be installed on the RFS. For instructions, see the *Security World v12.40 Compatibility Package v1.1.0 Release Notes*.

2.1.3. Create a v2 Security World on the RFS

At the RFS command prompt, run `new-world-1240`.

For information on this command, see the *Security World v12.40 Compatibility Package v1.1.0 Release Notes*.

2.2. Set up connectivity between the Firewall, the HSM, and the RFS

To set up connectivity between the Firewall, the HSM, and the RFS:

1. [Define connection settings for each HSM](#)
2. [Configure a service route to the HSM](#)
3. [Register the Firewall as an HSM client](#)
4. [Configure the RFS to accept connections from the Firewall and the HSM](#)
5. [Authenticate the Firewall to the HSM](#)
6. [Synchronize the Firewall with the RFS](#)
7. [Verify Firewall connectivity and authentication with the HSM](#)

2.2.1. Define connection settings for each HSM

The HSM authenticates the Firewalls based on their IP addresses. Therefore, you must configure the Firewalls to use static IP addresses. Dynamic addresses, assigned through DHCP, cannot be used.

If you want to set up connectivity to more than one HSM for high-availability, do it at this point. If more than one HSM is being used, the HSMs must share the same v2 security world. For steps on loading an existing security world onto an HSM, see the *nShield Connect User Guide*. Adding more HSMs after the master key has been encrypted and stored in an HSM (see [Encrypt the master key using the HSM](#)) is only possible by first removing the master key from the HSM. The master key is required to perform the removal. Then encrypt and store the master key again in the HSM after adding new HSM to the list above.

1. Sign in to the Palo Alto Networks Firewall web interface and select **Device > Setup > HSM**.
2. Edit the **Hardware Security Module Provider** settings and set the **Provider Configured** to **nCipher nShield Connect**.
3. Add each HSM as follows. A high-availability HSM configuration requires at least two HSMs.
 - a. Enter a module name for the HSM. This can be any ASCII string of up to 31 characters.

- b. Enter an IPv4 address for the HSM.
- c. Repeat the first two steps for all HSMs.

4. Enter an IPv4 address for the RFS.
5. Select **OK**.
6. Select the **Commit** icon, shown with a red arrow in the following picture.



2.2.2. Configure a service route to the HSM

Perform these optional steps if you do not want the Firewall to connect through the default management interface. If you are connecting through the default management interface, go to [Register the Firewall as an HSM client](#).

1. Select **Device > Setup > Services > Service Route Configuration**.
2. Select **Customize a service route**.

The IPv4 tab is active by default.

3. For **Service**, select **HSM**.
4. Select a **Source Interface** for the HSM.
5. Select **OK**.
6. Select the **Commit** icon.

2.2.3. Register the Firewall as an HSM client

This can be done from the front panel of the HSM or from the RFS. These steps describe

3. Configure or disable the RFS firewall:

```
service firewalld stop
```



The RFS firewall is independent of the Palo Alto Networks Firewall.



An RFS reboot re-enables the RFS firewall.

4. Verify that the RFS firewall stopped:

```
service firewalld status
```

5. Set up the RFS. The following command must be run for each HSM being added to your high-availability configuration:

```
rfs-setup --force <HSM_IP_address> $(anonkneti <HSM_IP_address>)
```

6. Run the following command to permit HSM client submissions on the RFS:

```
rfs-setup --gang-client --write-noauth <Firewall-IP-address>
```

You can use the following commands to configure the RFS to accept connections from the client Firewall. **rfs-setup** is run on the RFS. **rfs-sync** is run on the client.

```
RFS    rfs-setup --gang-client --write-noauth --force <client_IP_address>
Client rfs-sync --setup --no-authenticate <RFS_IP_Address>
       rfs-sync --update
       rfs-sync --commit
```

For security reasons, the Firewall has a protected command-line interface that does not allow direct access to **rfs-setup** and **rfs-sync** in its built-in nfast server. Instead, equivalent commands are available in the protected Palo Alto Networks Firewall command-line interface and can be useful for debugging.


nShield Command	Palo Alto Networks Command
/opt/nfast/bin/rfs-sync --setup --no-authenticate <RFS_IP_Address>	request hsm rfs-setup
/opt/nfast/bin/rfs-sync --update	request hsm rfs-sync
/opt/nfast/bin/rfs-sync --commit	
/opt/nfast/bin/enquiry	show hsm info

2.2.5. Authenticate the Firewall to the HSM

To authenticate the Firewall to the HSM:

1. In the Palo Alto Networks Firewall web interface, select **Device > Setup > HSM > Setup Hardware Security Module**.
2. Select **OK**.

The Firewall authenticates to the HSM and displays a completion message:

	Type	Response	Status
	Enroll Hardware Security Module	Enrolled with server nShield successfully	success

OK

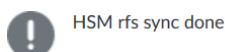
3. Select **OK**.

2.2.6. Synchronize the Firewall with the RFS

To synchronize the Firewall with the RFS:

1. In the Palo Alto Networks Firewall web interface, select **Device > Setup > HSM > Synchronize with Remote Filesystem**.

The Firewall synchronizes with the RFS and displays a completion message:



OK

2. Select **OK**.

2.2.7. Verify Firewall connectivity and authentication with the HSM

To verify Firewall connectivity and authentication with the HSM:

1. In the Palo Alto Networks Firewall web interface, select **Device > Setup > HSM**.
2. Check the **Hardware Security Module Status**. It should show **Authenticated**.
 - **Name** - The name of the HSM.
 - **IP address** - The IP address of the HSM.
 - **Module State** - The current state of the HSM connection: **Authenticated** or **NotAuthenticated**.

Hardware Security Module Status		
NAME	IP ADDRESS	MODULE STATE
nShield ConnectXC		Authenticated
nShield ConnectPlus		Authenticated

3. Check the connection status:

- **Green** - The Firewall is successfully authenticated and connected to the HSM.
- **Red** - The Firewall failed to authenticate to the HSM, or network connectivity to the HSM is down.



A left-over **rfs-sync** lock from a failed attempt could cause red status. Launch a command-line interface on the RFS, remove the **/opt/nfast/kmdata/local/.nft-lock** file, then re-run the instructions in [Synchronize the Firewall with the RFS](#).

2.3. Encrypt the master key using the HSM

A master key encrypts all private keys and passwords on the Palo Alto Networks Firewall. Every time the Firewall is required to decrypt a password or private key, it requests the HSM to decrypt the master key.

The HSM encrypts the master key using a wrapping key. To maintain security, you must occasionally change (refresh) this wrapping key.



Firewall master key protection is not supported with the use of a FIPS 140 Level 3 enabled Security World. FIPS 140 Level 2 is required for this feature.

2.3.1. Encrypt the master key

Use this procedure for first time encryption of a key, or if you define a new master key and you want to encrypt it.

1. In the Palo Alto Networks Firewall web interface, select **Device > Master Key and Diagnostics**.
2. Select the gear icon next to **Master Key**.
3. Select the **Master Key** check box.
4. For **Current Master Key**, enter the key that is currently used to encrypt all of the private keys and passwords on the Firewall (if applicable).
5. Select the **Stored on HSM** check box.
6. Enter the new master key and confirm.

7. Enter the following information:

- **Life Time** - The number of days and hours after which the master key expires (1-18250 days).
- **Time for Reminder** - The number of days and hours before expiration when the user is notified of the impending expiration (1-365 days).

8. Select **OK** and then select **Commit**.

The **Master Key** information is updated.

The new key is also visible in **Device > Setup > HSM > Hardware Security Module Details**.

2.3.2. Refresh the master key encryption

Refresh the master key encryption by rotating the wrapping key that encrypts it. The wrapping key resides on the HSM.

1. Sign in to the Palo Alto Networks Firewall command-line interface.
2. Use the following command to rotate the wrapping key for the master key on an HSM:

```
request hsm mkey-wrapping-key-rotation
```

For example:

```
admin@PA-VM> request hsm mkey-wrapping-key-rotation
Mkey wrapping key rotation succeeded.
New key handle 1119.
admin@PA-VM>
```

The **mkey-wrapping-key-rotation** command does not delete the old wrapping key.

- If the master key is encrypted on the HSM, the command generates a new wrapping key on the HSM and encrypts the master key with the new wrapping key.
- If the master key is not encrypted on the HSM, the command generates a new wrapping key on the HSM for future use.

2.4. Store the key used in SSL/TLS decryption

The HSM can be used to securely store the private keys used in SSL/TLS decryption for:

- **SSL forward proxy** - Store the private key of the Forward Trust certificate that signs certificates in SSL/TLS forward proxy operations. The Firewall will then send the certificates that it generates during such operations to the HSM for signing before forwarding these to the clients.
- **SSL inbound inspection** - Store the private keys for the internal servers for which it is performing SSL/TLS inbound inspection.

To store the key used in SSL/TLS decryption:

1. [Generate a self-signed certificate and key](#)
2. [Synchronize the key data from the RFS to the Firewall](#)
3. [Import the certificate that corresponds to the HSM-stored key into the Firewall](#)
4. [Enable the certificate for use in SSL/TLS forward proxy](#)
5. [Verify the certificate import into the Firewall](#)

2.4.1. Generate a self-signed certificate and key

This section describes a method to generate a self-signed certificate and key for purposes of this guide using the HSM. This is the preferred method to generate such key and certificate. For information about importing existing keys and certificates, see the *User Guide* for your HSM.

The HSM **generatekey** command generates a key file with the same syntax as an RSA private key file, but contains the key identifier rather than the key itself, which remains protected in the HSM.

1. Sign in to the RFS.
2. Assume root privileges by running the **su** command:

```
su
```

3. Run the **generatekey** command:

```
cd /opt/nfast/kmdata/local
generatekey pkcs11 selfcert=yes
```

For example, with Softcard protection:

```
[root@red_hat_8_rfs local]# generatekey pkcs11 selfcert=yes
module: Module to use? (1, 2) [1] >
protect: Protected by? (token, softcard, module) [token] > softcard
recovery: Key recovery? (yes/no) [yes] >
type: Key type? (DES3, DH, DHEX, DSA, HMACSHA1, HMACSHA256, HMACSHA384,
HMACSHA512, RSA, DES2, AES, Rijndael, Ed25519, X25519) [RSA]
>
size: Key size? (bits, minimum 1024) [2048] >
OPTIONAL: pubexp: Public exponent for RSA key (hex)? []
>
plainname: Key name? [] > paloaltoss1
x509country: Country code? [] > US
x509province: State or province? [] > FL
x509locality: City or locality? [] > Sunrise
x509org: Organization? [] > SWTesting
x509orgunit: Organization unit? [] > InterOp
x509dnscommon: Domain name? [] > paloaltofirewall
x509email: Email address? [] > test@test.com
nvrn: Blob in NVRAM (needs ACS)? (yes/no) [no] > no
digest: Digest to sign cert req with? (md5, sha1, sha256, sha384, sha512)
[default sha256] >
key generation parameters:
operation      Operation to perform      generate
application    Application              pkcs11
module         Module to use            1
protect        Protected by            softcard
softcard       Soft card to protect key <softcard-name>
recovery       Key recovery            yes
verify         Verify security of key   yes
type           Key type                RSA
size           Key size                2048
pubexp         Public exponent for RSA key (hex)
plainname      Key name                HSMKey
x509country    Country code            US
x509province   State or province       FL
x509locality   City or locality        Sunrise
x509org        Organization             SWTesting
x509orgunit    Organization unit       InterOp
x509dnscommon  Domain name             paloaltofirewall
x509email      Email address            test@test.com
nvrn           Blob in NVRAM (needs ACS) no
digest         Digest to sign cert req with sha256
```



```
Please enter the pass phrase for softcard '<softcard-name>':
```

```
Please wait.....
```

```
Key successfully generated.
```

```
Path to key: /opt/nfast/kmdata/local/key_pkcs11_ua5efdb72cb623c41d6ec9baeacc1eac95be8ada2b
```

```
Path to self-cert: /opt/nfast/kmdata/local/pkcs11_ua5efdb72cb623c41d6ec9baeacc1eac95be8ada2b_selfcert
```

```
[root@red_hat_8_rfs local]#
```

- a. If you selected **token** for OCS protection, you must provide the OCS 1/N quorum for **fips-auth**. If you provide the ACS quorum, the **generatekey** command will fail.
 - b. If you selected **module** for module protection, you must provide either the ACS or OCS 1/N quorum to provide **fips-auth** for this HSM operation.
4. Two files are created. The key file has the same syntax as an RSA private key file, but actually contains the key identifier rather than the key itself, which remains protected. The file type and naming are:

File Type	Naming
Key file (key identifier rather than the key itself)	key_pkcs11_...
Self-signed certificate	pkcs11_..._selfcert

5. You can view the content of the certificate created above by viewing the self-signed certificate (**.crt**):

```
openssl x509 -text -noout  
-in /opt/nfast/kmdata/local/pkcs11_ua5efdb72cb623c41d6ec9baeacc1eac95be8ada2b_selfcert
```

2.4.2. Synchronize the key data from the RFS to the Firewall

To synchronize the key data from the RFS to the Firewall:

1. In the Palo Alto Networks Firewall web interface and select **Device > Setup > HSM**.
2. In the **Hardware Security Operations** settings, select **Synchronize with Remote Filesystem**.

The Firewall confirms when the synchronization is complete.

2.4.3. Import the certificate that corresponds to the HSM-stored key into the Firewall

To import the certificate that corresponds to the HSM-stored key into the Firewall:

1. Sign in to the Palo Alto Networks Firewall web interface from the RFS.

2. Launch the browser from the RFS to be able to upload files from the RFS files system to the Palo Alto Networks Firewall.
3. Select **Device > Certificate Management > Certificates > Device Certificates**
4. Select **Import**.
5. For **Certificate Type**, select the **Local** option.
6. Enter the **Certificate Name**.
7. Browse to the Certificate File on the RFS. This is the file ending in **_selfcert** from the certificate generated in the previous step.

```
/opt/nfast/kmdata/local/pkcs11_ua5efdb72cb623c41d6ec9baeacc1eac95be8ada2b_selfcert
```

8. From the **File Format** list, select **Base64 Encoded Certificate (PEM)**.
9. Select the **Private key resides on Hardware Security Module** check box.

The 'Import Certificate' dialog box is shown with the following fields and options:

- Certificate Type:** Local (selected), SCEP
- Certificate Name:** HSMKey
- Certificate File:** C:\fakepath\pkcs11_ua5efdb72cb623c41d6ec9baeacc1eac95b (with a 'Browse...' button)
- File Format:** Base64 Encoded Certificate (PEM) (selected from a dropdown)
- Private key resides on Hardware Security Module:** ☒ (checked)
- Import Private Key:** ☐ (unchecked)
- Block Private Key Export:** ☐ (unchecked)
- Key File:** (empty field with a 'Browse...' button)
- Passphrase:** (empty field)
- Confirm Passphrase:** (empty field)
- Buttons:** OK (blue), Cancel (grey)

10. Select **OK**.
11. Select the **Commit** icon and close the dialog.

A new certificate has been imported:

The 'Certificate information' dialog box displays the following details:

- Name:** HSMKey
- Subject:** /C=US/ST=FL/L=Sunrise/O=SETest/OU=InterOp/CN=interop/emailAddress=test@test.com
- Issuer:** /C=US/ST=FL/L=Sunrise/O=SETest/OU=InterOp/CN=interop/emailAddress=test@test.com
- Not Valid Before:** Jun 1 23:45:44 2020 GMT
- Not Valid After:** Jul 1 23:45:44 2020 GMT
- Algorithm:** RSA
- Certificate Authority:** ☒ (checked)
- Forward Trust Certificate:** ☐ (unchecked)
- Forward Untrust Certificate:** ☐ (unchecked)
- Trusted Root CA:** ☐ (unchecked)
- Buttons:** Revoke (grey), OK (blue), Cancel (grey)

2.4.4. Enable the certificate for use in SSL/TLS forward proxy

To enable the certificate for use in SSL/TLS forward proxy:

1. In the Firewall web interface, open the certificate that you have imported: select **Device > Certificate Management > Certificates > Device Certificates**.
2. Select the certificate to open it.
3. Select the **Forward Trust Certificate** check box.

Certificate information ⓘ

Name	HSMKey
Subject	/C=US/ST=FL/L=Sunrise/O=SETest/OU=InterOp/CN=interop/emailAddress=test@test.com
Issuer	/C=US/ST=FL/L=Sunrise/O=SETest/OU=InterOp/CN=interop/emailAddress=test@test.com
Not Valid Before	Jun 1 23:45:44 2020 GMT
Not Valid After	Jul 1 23:45:44 2020 GMT
Algorithm	RSA
<input checked="" type="checkbox"/> Certificate Authority	
<input checked="" type="checkbox"/> Forward Trust Certificate	
<input type="checkbox"/> Forward Untrust Certificate	
<input type="checkbox"/> Trusted Root CA	

Revoke OK Cancel

4. Select **OK**.
5. Commit your changes.

The **USAGE** column now shows **Forward Trust Certificate**.

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

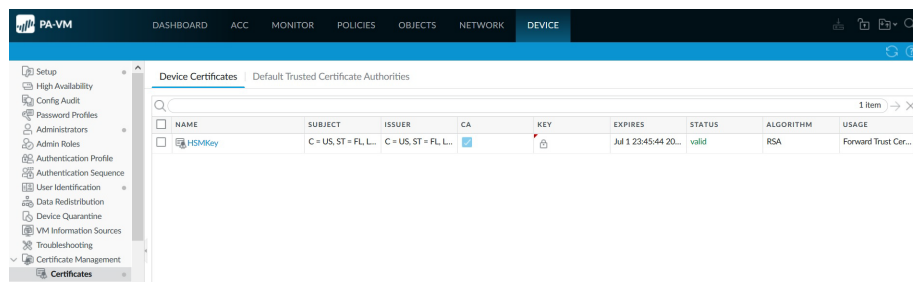
Device Certificates | Default Trusted Certificate Authorities

NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
HSMKey	C = US, ST = FL, L...	C = US, ST = FL, L...	<input checked="" type="checkbox"/>		Jul 1 23:45:44 20...	valid	RSA	Forward Trust Cer...

2.4.5. Verify the certificate import into the Firewall

To verify the certificate import into the Firewall:

1. Locate the certificate that you imported.



2. Check the icon in the **KEY** column:

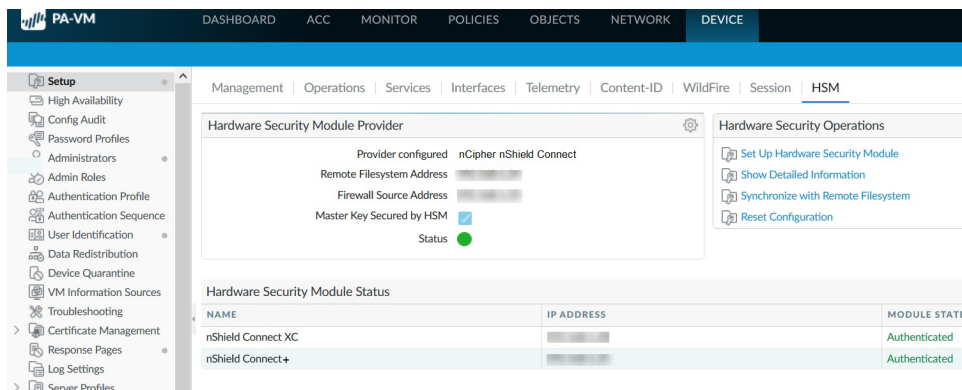
- **Lock icon** — The private key for the certificate is on the HSM.
- **Error icon** — The private key is not on the HSM or the HSM is not properly authenticated or connected.

3. Check the **USAGE** column. It should show **Forward Trust Certificate**.

2.5. Adding more HSMs

Adding more HSMs after the master key has been encrypted and stored in an HSM (see [Encrypt the master key using the HSM](#)) is only possible by first removing the master key from the HSM. The master key is required to perform the removal. Then encrypt and store the master key again in the HSM after adding a new HSM. Any new HSMs that are added must share the same v2 security world being used.

Two HSMs are shown in the **Hardware Security Module Status** pane:



Chapter 3. Additional resources and related products

3.1. nShield Connect

3.2. nShield as a Service

3.3. Entrust products

3.4. nShield product documentation