PAN-OS Integration with SafeNet Luna SA HSM

Tech Note

PAN-OS 6.0

Secure Keys with a SafeNet Luna Hardware Security Module

A hardware security module (HSM) is a physical device that manages digital keys. An HSM provides secure storage and generation of digital keys. It provides both logical and physical protection of these materials from non-authorized use and potential adversaries.

The SafeNet HSM client integrated with Palo Alto Networks PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7050, and VM-Series firewalls and on Panorama (virtual appliance and M-100 appliance) for use with SafeNet Luna SA 5.2.1 or later. HSM integration enables enhanced security for the private keys used in SSL/TLS decryption (both SSL forward proxy and SSL inbound inspection). In addition, you can use the HSM to encrypt device master keys.

The following topics describe how to integrate an Luna SafeNet HSM with Palo Alto Networks devices:

- Set up Connectivity with a SafeNet Luna HSM
- Encrypt a Master Key Using an HSM
- Store Private Keys on an HSM
- Manage the HSM Deployment

Set up Connectivity with a SafeNet Luna HSM

To set up connectivity between the Palo Alto Networks device and a SafeNet Luna SA HSM, you must specify the address of the HSM server and the password for connecting to it in the firewall configuration. In addition, you must register the firewall with the HSM server. Prior to beginning the configuration, make sure you have created a partition for the Palo Alto Networks devices on the HSM server.

HSM configuration is not synced between high availability firewall peers. Consequently, you must configure the HSM module separately on each of the peers.

In Active-Passive HA deployments, you must manually perform one failover to configure and authenticate each HA peer individually to the HSM. After this manual failover has been performed, user interaction is not required for the failover function.

Set up a Connectivity with a SafeNet Luna SA HSM		

Step 1	Register the firewall (the HSM client) with the HSM and assign it to a partition on the HSM.
	Note If the HSM already has a firewall with the same `<cl-name>` registered, you must remove the duplicate registration using the following command before registration will succeed:
	`client delete -client <cl-name>`
	where `<cl-name>` is the name of the client (firewall) registration you want to delete.
		1. Log in to the HSM from a remote system.
		2. Register the firewall using the following command:
		`client register -c <cl-name> -ip <fw-ip-addr>`
		where `<cl-name>` is a name that you assign to the firewall for use on the HSM and `<fw-ip-addr>` is the IP address of the firewall that is being configured as an HSM client.
		3. Assign a partition to the firewall using the following command:
		`client assignpartition -c <cl-name> -p <partition-name>`
		where `<cl-name>` is the name assigned to the firewall in the `client register` command and `<partition-name>` is the name of a previously configured partition that you want to assign to the firewall.

Step 2	Configure the firewall to communicate with the SafeNet Luna SA HSM.	1. Log in to the firewall web interface and select **Device > Setup > HSM**. 2. Edit the Hardware Security Module Provider section and select **Safenet Luna SA** as the **Provider Configured**. 3. Click **Add** and enter a **Module Name**. This can be any ASCII string up to 31 characters in length. 4. Enter the IPv4 address of the HSM module as the **Server Address**. If you are configuring a high availability HSM configuration, enter module names and IP addresses for the additional HSM devices. 5. (Optional) If configuring a high availability HSM configuration, select the **High Availability** check box and add the following: a value for **Auto Recovery Retry** and a **High Availability Group Name**. If two HSM servers are configured, you should configure high availability. Otherwise the second HSM server is not used. 6. Click **OK** and **Commit.**
Step 3	(Optional) Configure a service route to enable the firewall to connect to the HSM. By default, the firewall uses the Management Interface to communicate with the HSM. To use a different interface, you must configure a service route.	1. Select **Device > Setup > Services.** 2. Select **Service Route Configuration** from the Services Features area. 3. Select **Customize** from the Service Route Configuration area. 4. Select the **IPv4** tab. 5. Select **HSM** from the **Service** column. 6. Select an interface to use for HSM from the **Source Interface** drop-down. **Note** If you select a dataplane connected port for HSM, issuing the `clear session all` CLI command, will clear all existing HSM sessions causing all HSM states to be brought down and then up. During the several seconds required for HSM to recover, all SSL/TLS operations will fail. 7. Click **OK** and **Commit.**

Set up a Connectivity with a SafeNet Luna SA HSM (Continued)		
Step 4	Configure the firewall to authenticate to the HSM.	1. Select **Device > Setup > HSM**. 2. Select **Setup Hardware Security Module** in the Hardware Security Operations area. 3. Select the HSM **Server Name** from the drop-down. 4. Enter the **Administrator Password** to authenticate the firewall to the HSM. 5. Click **OK.** The firewall attempts to perform an authentication with the HSM and displays a status message. 6. Click **OK.**
Step 5	Configure the firewall to connect to the HSM partition.	1. Select **Device > Setup > HSM**. 2. Click the **Refresh** icon. 3. Select the **Setup HSM Partition** in the Hardware Security Operations area. 4. Enter the **Partition Password** to authenticate the firewall to the partition on the HSM. 5. Click **OK**.
Step 6	(Optional) Configure an additional HSM for high availability (HA).	1. Follow Step 2 through Step 5 to add an additional HSM for high availability (HA). This process adds a new HSM to the existing HA group. 2. If you remove an HSM from your configuration, repeat Step 5. This will remove the deleted HSM from the HA group.
Step 7	Verify connectivity with the HSM.	1. Select **Device > Setup > HSM**. 2. Check the **Status** of the HSM connection: Green = HSM is authenticated and connected Red = HSM was not authenticated or network connectivity to the HSM is down. 3. View the following columns in Hardware Security Module Status area to determine authentication status: **Serial Number** —The serial number of the HSM partition if the HSM was successfully authenticated. **Partition—**The partition name on the HSM that was assigned on the firewall. **Module State**—The current operating state of the HSM. It always has the value Authenticated if the HSM is displayed in this table.

Encrypt a Master Key Using an HSM

A master key is configured on a Palo Alto Networks firewall to encrypt all private keys and passwords. If you have security requirements to store your private keys in a secure location, you can encrypt the master key using an encryption key that is stored on an HSM. The firewall then requests the HSM to decrypt the master key whenever it is required to decrypt a password or private key on the firewall. Typically, the HSM is located in a highly secure location that is separate from the firewall for greater security.

The HSM encrypts the master key using a wrapping key. To maintain security, this encryption key must occasionally be changed. For this reason, a command is provided on the firewall to rotate the wrapping key which changes the master key encryption. The frequency of this wrapping key rotation depends on your application.

Master key encryption using an HSM is not supported on firewalls configured in FIPS of CC mode.

The following procedures show how to encrypt the master key initially and how to refresh the encryption:

- Encrypt the Master Key
- Refresh the Master Key Encryption

Encrypt the Master Key

If you have not previously encrypted the master key on a device, use the following procedure to encrypt it. Use this procedure for first time encryption of a key, or if you define a new master key and you want to encrypt it. If you want to refresh the encryption on a previously encrypted key, see Refresh the Master Key Encryption.

Encrypt a Master Key Using an HSM	
1.	Select **Device > Master Key and Diagnostics.**
Step 8	Specify the key that is currently used to encrypt all of the private keys and passwords on the firewall in the **Master Key** field.
Step 9	If changing the master key, enter the new master key and confirm.
Step 10	Select the **HSM** check box. **Life Time:** The number of days and hours after which the master key expires (range 1-730 days). **Time for Reminder:** The number of days and hours before expiration when the user is notified of the impending expiration (range 1-365 days).
Step 11	Click **OK**.

Refresh the Master Key Encryption

As a best practice, refresh the master key encryption on a regular basis by rotating the master key wrapping key on the HSM.

Refresh the Master Key Encryption
1. Use the following CLI command to rotate the wrapping key for the master key on an HSM: `> request hsm mkey-wrapping-key-rotation` If the master key is encrypted on the HSM, the CLI command will generate a new wrapping key on the HSM and encrypt the master key with the new wrapping key. If the master key is not encrypted on the HSM, the CLI command will generate new wrapping key on the HSM for future use. The old wrapping key is not deleted by this command.

Store Private Keys on an HSM

For added security, the private keys used to enable SSL/TLS decryption—both SSL forward proxy and SSL inbound inspection—can be secured with an HSM as follows:

- **SSL forward proxy**—The private key in the CA certificate that is used to sign certificates in SSL/TLS forward proxy operations can be stored on the HSM. The firewall will then send the certificates it generates during SSL/TLS forward proxy operations to the HSM for signing before forwarding them on to the client.
- **SSL inbound inspection**—The private keys for the internal servers for which you are doing SSL/TLS inbound inspection can be stored on the HSM.

For instructions on importing the private keys onto the HSM, refer to the Luna SafeNet documentation. After the required keys are on the HSM, you can configure the firewall to locate the keys as follows:

Store Private Keys on an HSM		
Step 1	Import the private keys used in your SSL forward proxy and/or SSL inbound inspection deployments onto the HSM.	For instructions on importing the private keys onto the HSM, refer to the documentation from your HSM provider.
Step 2	Import the certificate(s) that correspond to the private key(s) you are storing on the HSM onto the firewall.	1. From the firewall web interface, select **Device > Certificate Management > Certificates > Device Certificates**. 2. Click **Import**. 3. Enter the **Certificate Name**. 4. Enter filename of the **Certificate File** you imported to the HSM. 5. Select the appropriate **File Format** from the drop-down. 6. Select the **Private Key resides on Hardware Security Module** check box. 7. Click **OK** and **Commit**.

Store Private Keys on an HSM (Continued)		
Step 3	(Forward trust certificates only) Enable the certificate for use in SSL/TLS Forward Proxy.	1. Select the **Device > Certificate Management > Certificates > Device Certificates**. 2. Locate the certificate you imported in Step 2. 3. Select the **Forward Trust Certificate** check box. 4. Click **OK** and **Commit**.
Step 4	Verify that the certificate has been successfully imported to the firewall.	1. Select **Device > Certificate Management > Certificates > Device Certificates**. 2. Locate the certificate you imported in Step 2. 3. In the Key column notice the following: If a Lock icon is displayed, the private key for the certificate can be found on the HSM. If an Error icon is displayed, the private key is not imported to the HSM or the HSM is not properly authenticated or connected.

Manage the HSM Deployment

Manage HSM	
• View the HSM configuration settings.	Select **Device > Setup > HSM**.
• Display detailed HSM information.	Select **Show Detailed Information** from the Hardware Security Operations section. Information regarding the HSM servers, HSM HA status, and HSM hardware is displayed.
• Export Support file	Select **Export Support File** from the Hardware Security Operations section. A test file is created to help customer support when addressing a problem with an HSM configuration on the firewall.
• Reset HSM configuration.	Select **Reset HSM Configuration** from the Hardware Security Operations section. Selecting this option removes all HSM connections. All authentication procedures must be repeated after using this option.