How To Enable FIPS

https://campus.barracuda.com/doc/9011852/

The Hardware Security Module (HSM) is available only on Barracuda Web Application Firewall Model 963 (End-of-Sales).

Overview

The Federal Information Processing Standards (FIPS) 140-2 Publication, issued by US National Institute of Standards and Technology (NIST), specifies the Security Requirements for Cryptographic Modules to protect sensitive data in the security appliances. The Barracuda Web Application Firewall integrates with Cavium Networks' Hardware Security Module (HSM) to meet these standards, thus enhancing the security of web applications, and accelerating performance.

The intended audience for this document is a Barracuda Web Application Firewall system administrator responsible for managing the HSM, who is assumed to have basic knowledge of the following:

- Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules
- SSL/TLS protocols and its terminology
- Cryptography
- Public Key Infrastructure (PKI)

This document covers HSM supported cryptographic functions, authentication and user roles, cloning an HSM masking secret, and sharing of keys between multiple HSMs.

HSM Functionality

The Cavium Networks' NITROX XL CN16xx-NFBE card, a cryptographic HSM, is integrated with the Barracuda Web Application Firewall at the device level via the Peripheral Component Interconnect (PCI) interface. It provides FIPS 140-2 level 3 certified cryptographic functions to the appliance, as well as strong authentication, and physical tamper resistance. The HSM manages cryptographic keys and provides accelerated cryptographic functions with keys including:

- Cryptographic key generation
- Secure storage of PKI Information
- Cryptographic algorithm processing

- Complex SSL/TLS protocol processing

FIPS 140-2 level 2 capabilities have been exposed even though the system supports FIPS 140-2 level 3 specifications.

Authentication and User Roles

The Barracuda Web Application Firewall authenticates users, challenging them for a username and password, before allowing access to the HSM or execution of its cryptographic functions. The HSM supports two distinct roles: Crypto-Officer and Crypto-User. The Crypto-Officer can install and initialize the HSM, and perform security administration tasks including Crypto-User (CU) creation, configuration of the HSM, and configuration of the security policy. The Crypto-User is an operational role which has access to all cryptographic operations provided by the HSM. There can be only one Crypto-Officer and one Crypto-User, with only one of them logged in at a time within a single application.

Protecting Keys with Secure Key Management

When a certificate is created or imported, the private keys are stored securely on the HSM, while certificates are stored on the Barracuda Web Application Firewall. The HSM authenticates users before allowing access to keys stored in the HSM, and any attempt to tamper with the card results in immediate destruction of all private key data on the HSM.

Certificate Management and Generation of Keys

Private cryptographic keys can be created on the Barracuda Web Application Firewall, or can be uploaded to it. In each case, the private key is stored securely in the HSM.

When you create a self-signed certificate, the private key is generated and securely stored in the HSM, while a Certificate Signing Request (CSR) is generated and saved on the Barracuda Web Application Firewall and can be viewed using the **BASIC > Certificates > Saved Certificates** section.

Private keys are imported to the HSM when any Certificate Authority certificate is uploaded to the Barracuda Web Application Firewall. For more information on how to create a certificate, see How to Add an SSL Certificate.

Initial Setup

Use the **ADVANCED > System Configuration > Hardware Security Module (HSM): Initial Setup** section to enable Hardware Security Module (HSM) support on the appliance, and perform initial settings. This section is visible only in the expert mode. To enable expert mode, the administrator is
required to add "*&expert=1*" at the end of the URL. For example:
`http://192.168.132.45:8000//cgimod/index.cgi?&user=admin&password=21f1c62f6&et=1304924640&auth_type=Local&locale=en_US&primary_tab=ADVANCED&secondary_tab=advanced_system&expert=1`

To perform Hardware Security Module (HSM) Initial Setup:

1. Go to the **ADVANCED > System Configuration** page.
2. In the **Hardware Security Module (HSM): Initial Setup** section, specify values for the following fields:
    1. **Security Domain** - Enter a name for security domain. This is used during the cloning process. It is recommended that the administrators change the default value to something specific to their organization. Note that the source HSM and target HSM(s) should share the same Security domain for cloning.
    2. **Login Fail Count** - Set the maximum number of failed login attempts for HSM. If the user does not successfully login within the specified value, the HSM automatically zeroize (erases all the data stored in the HSM) itself, and resets to factory-default state
    3. **HSM Cloning Supported** - Select **Yes** to enable HSM cloning. Note that if HSM cloning is disabled, High Availability will not work. Also, if you intend to restore the backup of this HSM to another Barracuda Web Application Firewall which is not cloned by this HSM does not work.
3. Click **Save Changes** to save the above settings.

Any changes made to these parameter values will result in HSM being reinitialized followed by a system **REBOOT**. The reinitialization process removes all the information stored in HSM.

Hardware Security Module (HSM): Backup / Restore

The **ADVANCED > System Configuration > Hardware Security Module (HSM): Backup / Restore** section enables you to backup the current private key data stored in the HSM of an appliance. The file is used for backup purpose in case of HSM hardware failure, and can also be uploaded to another HSM enabled Barracuda Web Application Firewall.

It is possible to export the private keys from one Barracuda Web Application Firewall and then restore it either on the same appliance or another Barracuda Web Application Firewall which has a cloned HSM.

> An HSM internally generates its own masking key, which is used to encrypt exported private keys and decrypt imported private keys. The masking key is known as a Key-Wrapping-Key or Key-Encryption-Key.

Backup

To backup the current private key data in the HSM to your local machine:

1. Go to the **ADVANCED > System Configuration** page.
2. In the **Hardware Security Module (HSM): Backup / Restore** section, click **Backup**.
3. Save "*hsm_masked_objects.tar.gz*" (gzip) file to the desired location.

Restoring the Keys

To restore the backup file onto the HSM enabled Barracuda Web Application Firewall:

1. Click the **Browse** button.
2. Locate the backup file, and click the **Upload** button to begin restoration.

Restoring Keys on the same HSM enabled Barracuda Web Application Firewall

Importing the exported private keys to the same appliance does not require the Key-Encryption-Key or security domain parameter, as the device is same and Key-Encryption-key will match during the import time.

Restoring Keys on the different HSM enabled Barracuda Web Application Firewall

If you intend to export the private keys from one appliance and import to another, then the following conditions should be met:

- All HSM domain members should share the same **Security Domain** i.e. the unit from which the backup is taken and the unit on which it is going to be restored.
- Key-Encryption-Key of HSM enabled Barracuda Web Application Firewalls must be synchronized. This can be performed using **Hardware Security Module (HSM): Cloning** section.

Cloning the Masking Key

A Hardware Security Module (HSM) internally generates its own masking key, or secret, which is used to encrypt exported private keys and decrypt imported private keys. The masking key is known as a Key-Wrapping-Key or Key-Encryption-Key. Cloning the masking key copies the internal masking secret from one HSM to another, allowing keys that have been masked by an HSM to be unmasked using the clone of the masking key. This allows for recovery of private key data in the event of HSM hardware failure. Cloning requires the source HSM and target HSM(s) to share the same **Security Domain**, a parameter configured while initializing the HSM.

Cloning of HSM includes four steps:

1. Export source public key (Key-Encryption-Key) from the source HSM:
    1. On the source appliance, select **Source** as the **System Role**.
    2. In the **Cloning Step** parameter, select **Export Source Public Key** and click **Save Changes**.
    3. Click **Download** to **Export Source Public Key** from the source HSM.
2. Transfer source public key to the target HSM:
    1. On the target appliance, select **Target** as the **System Role**.
    2. In the **Cloning Step** parameter, select **Import Source Public Key** and click **Save Changes**.
    3. Click **Browse** and **Import Source Public Key** exported from the source HSM.
    4. Click **Upload**.
    5. In this step, the target HSM accepts the source public key and returns target public key.
    6. Click **Download** to export the target public key.
3. Transfer target public key to the source HSM:
    1. On the source appliance, ensure the **System Role** is set to **Source**.
    2. In the **Cloning Step** parameter, select **Import Target Public Key** and click **Save Changes**.
    3. Click **Browse** and **Import Target Public Key** exported from the target HSM.
    4. Click **Upload**.
    5. The source HSM accepts the target public key and returns masking key (Key-Wrapping-Key/Key-Encryption-Key).
    6. Click **Download** to download the masking key. This needs to be imported to the target HSM to complete the cloning process.
4. Clone Key-Encryption-Key on target HSM:
    1. On the target appliance, select **Import Source Masking Key** as the **Cloning Step** and click **Save Changes**.
    2. Click **Browse** and **Import Masking Key** downloaded from the source HSM.
    3. Click **Upload**. This completes the cloning process.

Now, the source appliance and target appliance share the same Key-Encryption-Key. Either of the appliances can be used as the source appliance for subsequent cloning operations.

- You should create a clone of any HSM that is currently in use to allow for recovery of all previously masked data in case of HSM hardware failure.
- To start a fresh configuration on the Barracuda Web Application Firewall, use **Clear Configuration** from the **ADVANCED > Troubleshooting > Support Diagnostics** section. This operation restores the Barracuda Web Application Firewall to its initial configuration, and deletes all private keys on the HSM.

High Availability (HA) in FIPS Environment

The **ADVANCED > High Availability** page allows you to configure a second HSM enabled Barracuda Web Application Firewall to act as a backup to the primary. Both systems must be on the same network. If the primary unit is down for any reason, the backup unit assumes ownership of the configured services and inherits the work of the primary unit, providing continuous availability. For more information, see How to Set Up a High Availability Environment with Two Barracuda Web Application Firewalls.

Before configuring HA in FIPS environment, ensure the following conditions are met:

1. Both units (primary and secondary) should share the same Security Domain name.
2. Both units should have the same masking key (Key-Encryption-Key), which can be achieved by:
    1. Cloning the HSM on the secondary unit with the HSM of the primary.
    2. Or, alternatively both primary and secondary cloned from some master HSM.

Once the above configuration is done, the Barracuda Web Application Firewall synchronizes HSM configuration internally.