TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

CONFIGURING THE TPM AND PROTECTING PRIVATE KEYS IN SNS FIREWALL CERTIFICATES

Product concerned: SNS 3.11 LTSB, SNS 4.3 LTSB, SNS 4.7 and higher versions

Document last updated: February 13, 2024

Reference: sns-en-TPM_protection_technical_note

Table of contents

Change log

Date	Description
February 13, 2024	- Explanations regarding PCRs added to the section "Protecting private keys in firewall certificates with symmetric keys". - Changes to the description of the TPM orange status in the section "Checking whether the TPM is initialized". - Explanations on resetting the TPM added to the section "If you have forgotten the TPM password". - Explanation on the `force=on` token reworded in the section "Disabling the TPM". - The example *<CN>* changed to *<CERTNAME>* in the sections "Protecting the private key of a certificate that has already been added" and "Checking whether the private key in the SNS firewall's certificate is protected". - Information regarding the certification authority reworded in the "SSL VPN" section. - Important information regarding the use of protected private keys added to the section "Communications with the SMC server". - Explanations on protecting the backup file with a password added to the section "Backing up a configuration".
January 18, 2024	New document

Getting started

The trusted platform module (TPM) found on some SNS firewalls offers hardware storage that increases the security of certificates stored on the firewall.

The TPM-based security mechanism applies to some certificates, depending on the SNS version installed on the firewall.

This technical note provides details on initializing and configuring the TPM on an SNS firewall, and protecting private keys in firewall certificates with the TPM, and includes the configuration of these certificates in the firewall's modules.

Requirements

An SNS firewall equipped with a TPM

All recent models as of SNi20 have a TPM.

See the list of the relevant firewall models on the Stormshield website at Our Stormshield Network Security firewalls.

A compatible SNS version installed

The TPM-based security mechanism applies to some certificates, depending on the SNS version installed on the firewall.

Certificates used in the following cases with a private key that can be protected	Compatible SNS versions		
	3.11 LTSB	4.3 LTSB	4.7 and higher
IPsec VPN	✓	✓	✓
SSL VPN	-	-	✓
SSL/TLS decryption (web administration interface and captive portal)	-	-	✓
Communications with the SMC server	-	-	✓
Sending of logs to a syslog server	-	-	✓
Internal LDAP	-	-	✓

Privilege to access the TPM

To initialize and use the TPM, the administrator must hold the **TPM (E)** privilege. Only the *admin* account can assign this privilege in the firewall's web administration interface in **Configuration > System > Administrators**, **Administrators** tab, **Switch to advanced view** button.

Ability to access the CLI console on the SNS firewall

Depending on the SNS version installed on the firewall, some or all operations relating to the TPM must be performed in a CLI console by using commands.

To access the CLI console, go to the firewall's web administration interface, for example, in **Configuration > System > CLI console**.

Operation

Certificates with private keys that can be protected by the TPM

See which certificates are concerned and which SNS versions are compatible in the chapter Requirements.

TPM administration password

When the TPM is initialized on the SNS firewall, a TPM administration password must be set. This password is required in order to perform certain operations on the TPM, such as removing protection from the private key of a certificate or disabling the TPM.

In this technical note, the TPM administration password is referred to as "*TPM password*".

IMPORTANT
Keep the TPM password in a safe and protected location. Do note that Stormshield will not be able to help you recover this password if you forget it.

Protecting private keys in firewall certificates with symmetric keys

When the private key of a certificate is protected by the TPM, the key will be encrypted with a symmetric key. **Only the symmetric key will enable the encryption and decryption of the certificate's private key.**

The symmetric key is set during the initialization of the TPM and stored on the TPM. Access to this key is strictly protected, notably through a feature that reliably measures the status of the system, known as PCRs (*platform configuration registers*).

When a private key needs to be decrypted, the firewall has to retrieve the TPM's symmetric key. This operation can only be completed if the PCRs confirm that the status of the firewall is reliable.

If PCRs change, for example after an SNS version update that involves changes to the startup sequence of the product, the firewall can no longer retrieve the symmetric key, and protected private keys can no longer be decrypted. Only the TPM password can be used to update the access policy and recover these keys (this scenario is described in Troubleshooting).

Symmetric key derivation mechanism on firewall clusters

Firewalls have their own TPMs in high availability (HA) clusters. Two symmetric keys are therefore generated:

- A first symmetric key stored on the active firewall's TPM,
- A second symmetric key stored on the passive firewall's TPM.

A symmetric key derivation mechanism (known as *derivekey*) makes it possible to set the same symmetric key on both firewalls in the cluster. As such, when the firewall switches from passive to active, TPM-protected private keys in certificates can always be decrypted because the symmetric keys are the same.

Configuring the TPM on SNS firewalls

This chapter explains the configuration of the TPM on an SNS firewall.

Initializing the TPM

This section includes procedures to initialize the TPM on an SNS firewall or TPMs in a high availability (HA) cluster.

> **NOTE**
> The initialization of the TPM does not automatically activate the protection of private keys in the firewall's certificates. To protect them, refer to the chapter Protecting private keys in SNS firewall certificates.

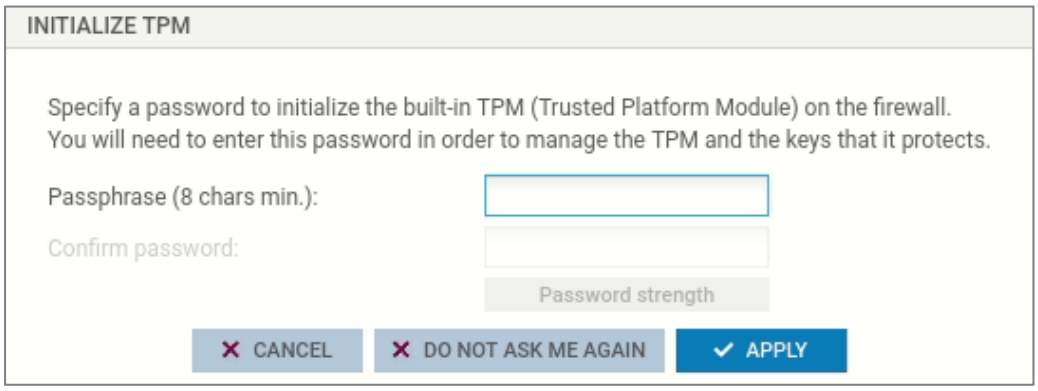
Initializing the TPM on SNS firewalls

From the web administration interface

This use case is exclusive to SNS 4.3 LTSB versions and SNS 4.7 and higher versions.

1. Go to **Configuration > Objects > Certificates and PKI**.
2. In the TPM initialization window, set a TPM administration password. The password must comply with the password policy set on the firewall. **Keep the TPM password in a safe and protected location**.
   If the window does not appear, check whether the TPM has already been initialized.
   Initialize the TPM from the CLI console if required.
3. Click on **Apply**.

If the firewall is part of a high availability cluster, the mechanism that derives the symmetric key will automatically be enabled.



From the CLI console

Run the following command:

```
SYSTEM TPM INIT tpmpassword=<password> derivekey=<on|off>
```

- Replace `<password>` with the desired TPM administration password. The password must comply with the password policy set on the firewall. **Keep the TPM password in a safe and protected location**,
- Enter `derivekey=on` if the firewall is part of a high availability cluster.

Initializing TPMs in a high availability (HA) cluster

If the cluster has already been created

Initialize the TPM on the active firewall to automatically activate the initialization of the TPM on the passive firewall Then refer to the procedures above.

If the cluster has not yet been created

There are two possibilities, depending on whether the TPM has already been initialized on the firewalls in the cluster.

The TPM has not yet been initialized on the firewalls in the cluster

1. Configure the cluster (create the cluster and integrate the second firewall).
2. Initialize the TPM on the active firewall to automatically activate the initialization of the TPM on the passive firewall Then refer to the procedures above.

The TPM is already initialized on the future active firewall in the cluster

1. Configure the cluster (create the cluster and integrate the second firewall).
2. Renew the symmetric key on the active firewall by running the following command in a CLI console:

```
SYSTEM TPM RENEW tpmpassword=<password> derivekey=on
```

   - Replace `<password>` with the TPM password,
   - As the firewall is part of a cluster, enter `derivekey=on`.

   All TPM-protected private keys of certificates are decrypted then re-encrypted with the new symmetric key derived from the TPM password.
3. Initialize the TPM on the passive firewall by running the following command:

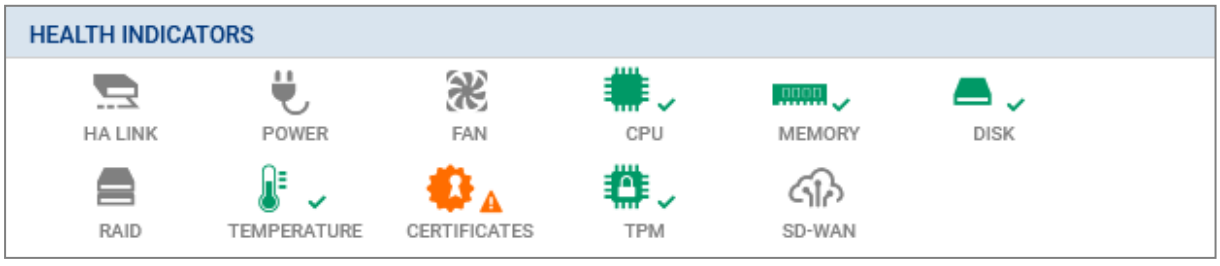
```
HA TPMSYNC tpmpassword=<password>
```

Checking whether the TPM is initialized

From the web administration interface

This use case is exclusive to SNS 4.7 and higher versions.

1. Go to **Monitoring > Dashboard**.
2. In the **Health indicators** widget, check the status of the TPM:
   - A status shown in green indicates that the TPM is initialized and functioning,
   - A status shown in orange indicates that either the TPM has not been initialized or automatic backups of the firewall configuration are not protected by a password,
   - A status shown in red indicates that pings to the TPM do not function (for example, when the TPM no longer responds),
   - If the status of the TPM does not appear (icon not displayed), this means that the firewall is not equipped with a TPM.



From the CLI console

Run the following command:

```
SYSTEM PROPERTY
```

`TpmInit=1` indicates that the TPM is initialized.

Managing the TPM password

Changing the TPM password

Run the following command in a CLI console:

```
SYSTEM TPM CHANGE currentpassword=<current_password> newpassword=<new_
password>
```

- Replace `<current_password>` with the current TPM password,
- Replace `<new_password>` with the new TPM password. The password must comply with the password policy set on the firewall. **Keep the TPM password in a safe and protected location**.

If you have forgotten the TPM password

You will not be able to reset the TPM password. If you cannot remember the TPM password, you can reset the TPM on the firewall as a last resort.

Do note that by resetting the TPM, you will **not be able** to recover the private keys of encrypted certificates. You will need to import the certificates in question again on the firewall and protect their private key again.

To reset the TPM, refer to the instructions in the Stormshield knowledge base article I've lost my TPM password, how can I reset it?.

Disabling the TPM

Run the following command in a CLI console:

```
SYSTEM TPM RESET tpmpassword=<password> force=<on|off>
```

- Replace `<password>` with the TPM password,
- Enter `force=on` if private keys in certificates are protected by the TPM and you wish to disable it by force anyway. The protected private keys will then be decrypted.

Protecting private keys in SNS firewall certificates

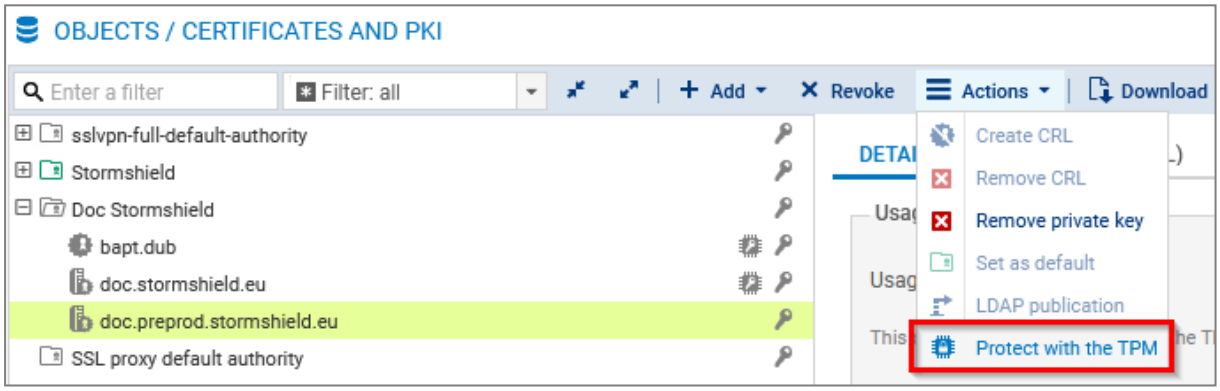
This chapter explains how to protect the private key in the SNS firewall's certificate with the TPM.

Protecting the private key of a certificate that has already been added

From the web administration interface

This use case is exclusive to SNS 4.7 and higher versions.

1. In **Configuration > Objects > Certificates and PKI**, select the certificate (identity) in question.
2. Click on **Actions > Protect with the TPM**.
3. Click on **OK**.



From the CLI console

1. Run the following command to show the certification authorities:
```
PKI CA LIST
```
2. If required, show the list of intermediate certification authorities that signed the root authority in question (`<RootCA>` in the command) with:
```
PKI CA LIST CANAME=<RootCA>
```
3. Show the certificates issued by the certification authority (`<CA>` in the command) with:
```
PKI CERT LIST CANAME=<CA>
```
4. Protect the private key of the certificate in question (`<CERTNAME>` in the command) with:
```
PKI CERT PROTECT CANAME=<CA> NAME=<CERTNAME> tpm=ondisk
```
5. Apply the new configuration with:
```
PKI ACTIVATE
```

From the SMC server

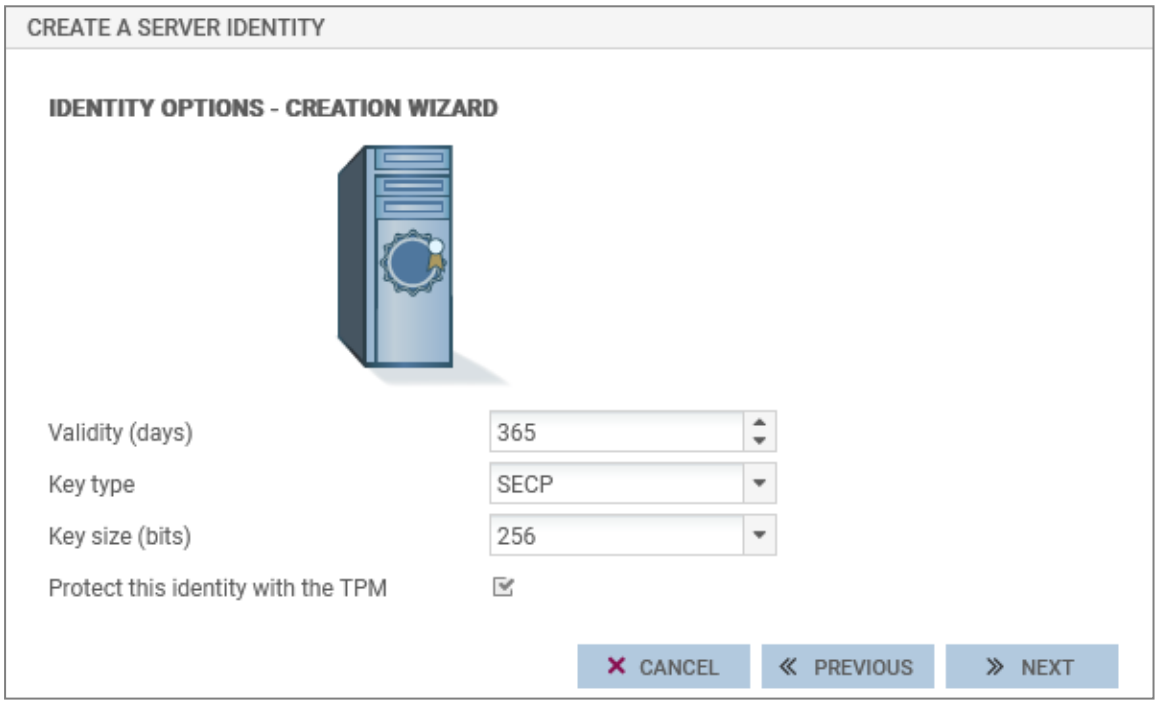
For further information, refer to the section Enabling TPM protection on existing private keys in the SMC administration guide..

Adding a certificate and protecting its private key

From the web administration interface

1. In **Configuration > Objects > Certificates and PKI**, click on **Add** and select the certificate (identity) to add.
2. Fill out the requested information. For SNS 4.3 LTSB versions and SNS 4.7 and higher versions, select the checkbox **Protect this identity with the TPM** during the relevant steps.
3. Click on **Finish**.
4. For SNS 3.11 LTSB versions, protect the private key of the certificate from the CLI console.

For more information, refer to the section on *Certificates and PKI* in the v4 or v3 user guide of the SNS version used.



From the CLI console

1. Run the following command, by using the `tpm=ondisk` token:

```
PKI CERT CREATE
```

If required, show command help with:

```
PKI CERT CREATE HELP
```

2. Next, apply the new configuration with:

```
PKI ACTIVATE
```

From the SMC server

You can import certificates (identities) on the SMC server and declare them on the SNS firewall. For more information, refer to the section Importing or declaring a certificate for a firewall in the SMC administration guide.

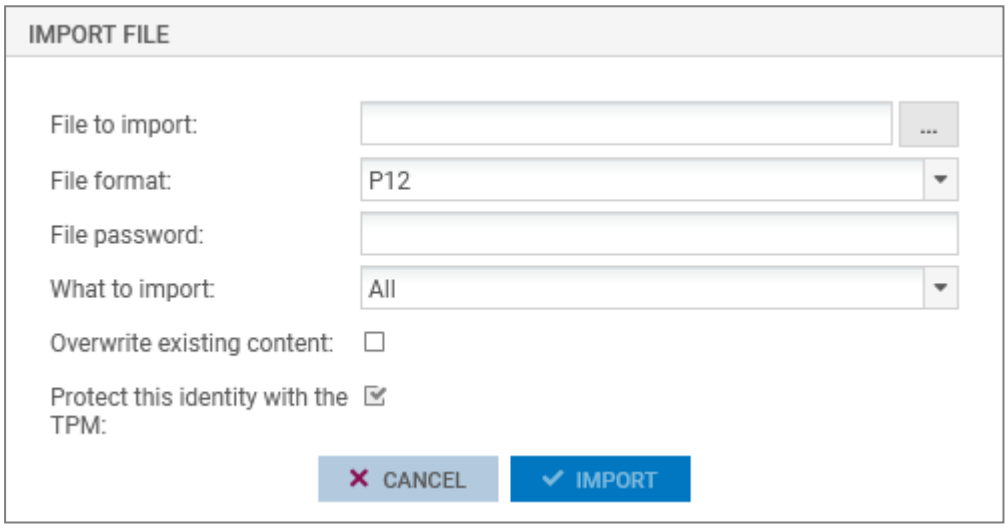
By default, the private keys of certificates that the SMC server declared on the SNS firewall are protected by the TPM if it has been initialized. To change the default setting, refer to the section Disabling TPM private key protection in the SMC administration guide..

Importing a certificate and protecting its private key

From the web administration interface

1. In **Configuration > Objects > Certificates and PKI**, click on **Add** > **Import a file**.
2. Fill out the requested information. For SNS 4.3 LTSB versions and SNS 4.7 and higher versions, select the checkbox **Protect this identity with the TPM**.
3. Click on **Import**.
4. For SNS 3.11 LTSB versions, protect the private key of the certificate from the CLI console.

For more information, refer to the section on *Certificates and PKI* in the v4 or v3 user guide of the SNS version used.



From the SMC server

You can import certificates (identities) on the SMC server and declare them on the SNS firewall. For more information, refer to the section Importing or declaring a certificate for a firewall in the SMC administration guide.

By default, the private keys of certificates that the SMC server declared on the SNS firewall are protected by the TPM if it has been initialized. To change the default setting, refer to the section Disabling TPM private key protection in the SMC administration guide..

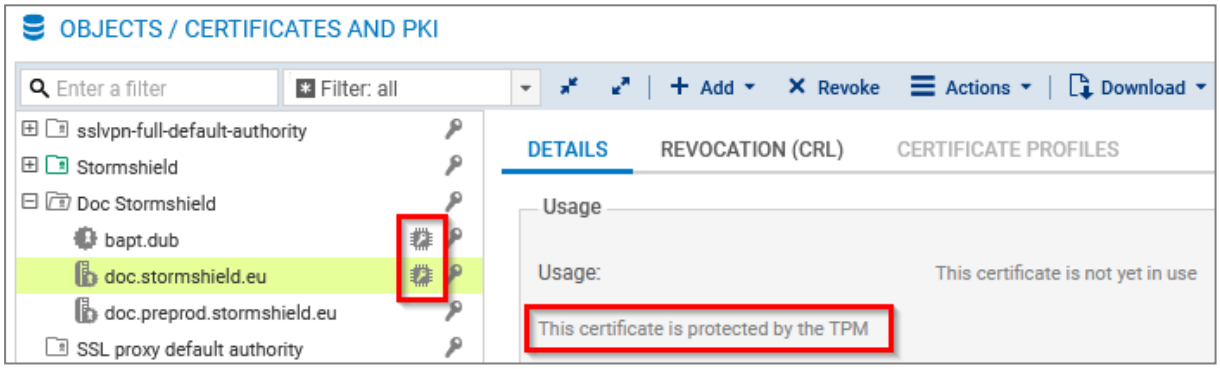
Checking whether the private key in the SNS firewall's certificate is protected

This chapter explains how to check whether the private key in the SNS firewall's certificate is protected by the TPM.

From the web administration interface

This use case is exclusive to SNS 4.7 and higher versions.

In **Configuration > Objects > Certificates and PKI**, locate the certificate (identity) in question. If the icon appears, this means that the private key of the certificate is protected by the TPM. This information also appears in the **Details** tab when the certificate in question is selected beforehand.



From the CLI console

To verify the certificates used in the firewall configuration:

Run the following command:

```
MONITOR CERT
```

`tpm=Used` indicates that the private key of the certificate is protected by the TPM.

To check all certificates on the firewall:

1. Run the following command to show the certification authorities:
   ```
   PKI CA LIST
   ```
2. If required, show the list of intermediate certification authorities that signed the root authority in question (`<RootCA>` in the command) with:
   ```
   PKI CA LIST CANAME=<RootCA>
   ```
3. Show the certificates issued by the certification authority (`<CA>` in the command) with:
   ```
   PKI CERT LIST CANAME=<CA>
   ```
   `tpm=ondisk` indicates that the private key of the certificate is protected by the TPM.
4. If required, show information about a certificate (`<CERTNAME>` in the command) with:
   ```
   PKI CERT SHOW CANAME=<CA> NAME=<CERTNAME>
   ```

From the SMC server

For more information, refer to the section Finding out whether a private key is TPM-protected in the SMC administration guide.

Using certificates with TPM-protected private keys

This chapter sums up the situations in which you can use certificates with TPM-protected private keys:

- SSL/TLS decryption (web administration interface and captive portal),
- SSL VPN,
- IPsec VPN,
- Internal LDAP,
- Communications with the SMC server,
- Sending of logs to a syslog server,.

SSL/TLS decryption (web administration interface and captive portal)

This use case is exclusive to SNS 4.7 and higher versions.

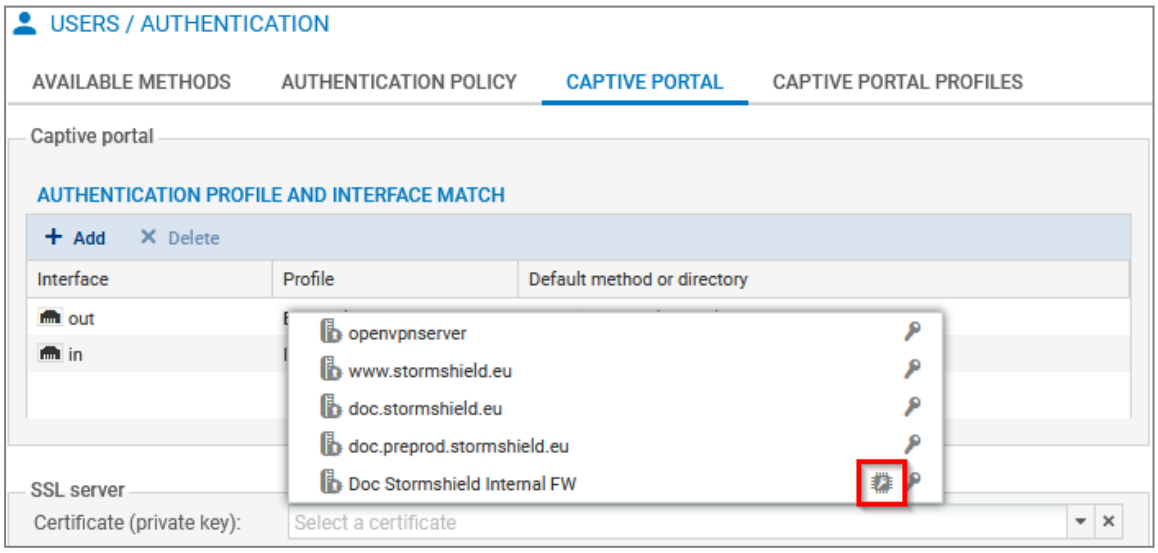
The private key in the certificate presented by the firewall's web administration interface and its captive portal can be protected by the TPM.

IMPORTANT
Keep in mind that you will no longer be able to access these interfaces if the private key in the certificate that is used can no longer be decrypted.

To check/change the certificate used:

1. Go to **Configuration > Users > Authentication**, **Captive portal** tab, **SSL server** section.
2. In the **Certificate (private key)** field, select the desired certificate. The icon indicates certificates with a TPM-protected private key.
3. Apply changes.

The connection to the web administration interface will then be lost. Depending on the certificate used, a warning message may appear when you go back to the authentication page You can proceed to the website.



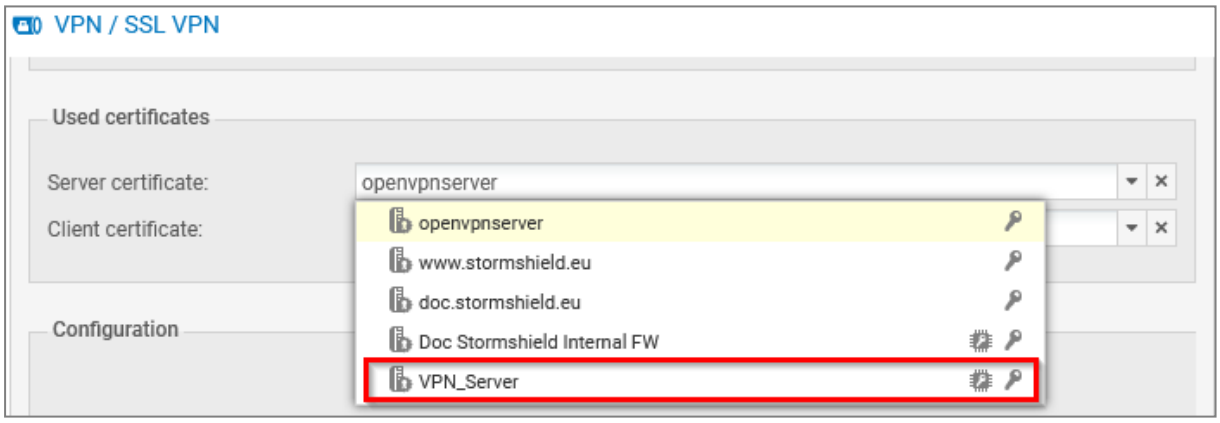
SSL VPN

This use case is exclusive to SNS 4.7 and higher versions.

The SSL VPN service on the SNS firewall and the VPN client present certificates (server and client) to set up tunnels.

To check/change the certificates used:

1. Go to **Configuration > VPN > SSL VPN**, **Advanced properties** area, **Used certificates** section.
2. Select the desired certificates in the relevant fields. They must be issued from the same certification authority.
   - In the **Server certificate** field, the icon indicates certificates with a TPM-protected private key.
   - In the **Client certificate** field, you cannot select certificates that have TPM-protected private keys. This is because the private keys of such certificates must be available in plaintext (unencrypted) in the VPN configuration that is distributed to VPN clients.
3. Apply changes.
4. If you are using the Stormshield VPN SSL client in automatic mode, the VPN configuration will automatically be retrieved at the next connection. For all other use cases, the configuration must be imported again manually (*.ovpn* file). For more information, refer to the technical note Configuring and using the SSL VPN on SNS firewalls.



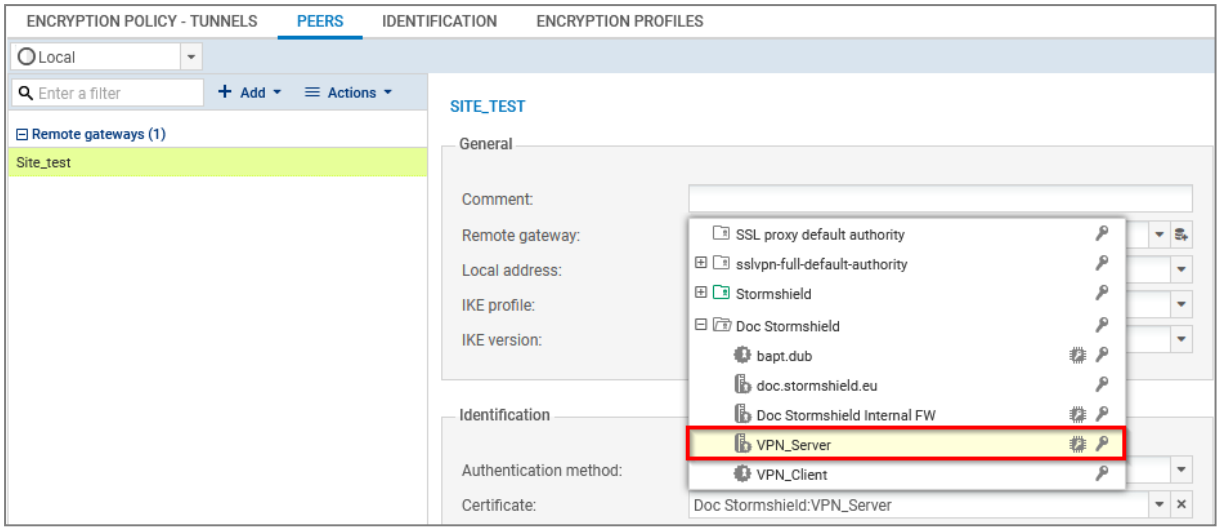
IPsec VPN

The private key of the certificate that is presented to set up IPsec tunnels in a certificate authentication can be protected by the TPM.

To check/change the certificate used:

1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Select the peer used in the VPN configuration from the grid.
3. In the **Identification** section, **Certificate** field, select the desired certificate. The icon indicates certificates with a TPM-protected private key.
   In configurations that use the IKEv1 IPsec VPN tunnel manager, tunnels will no longer be set up if the private key in the certificate used is protected by the TPM.
4. Apply changes.

You can also select the certificate when adding peers (remote gateway or mobile peer with certificate authentication).



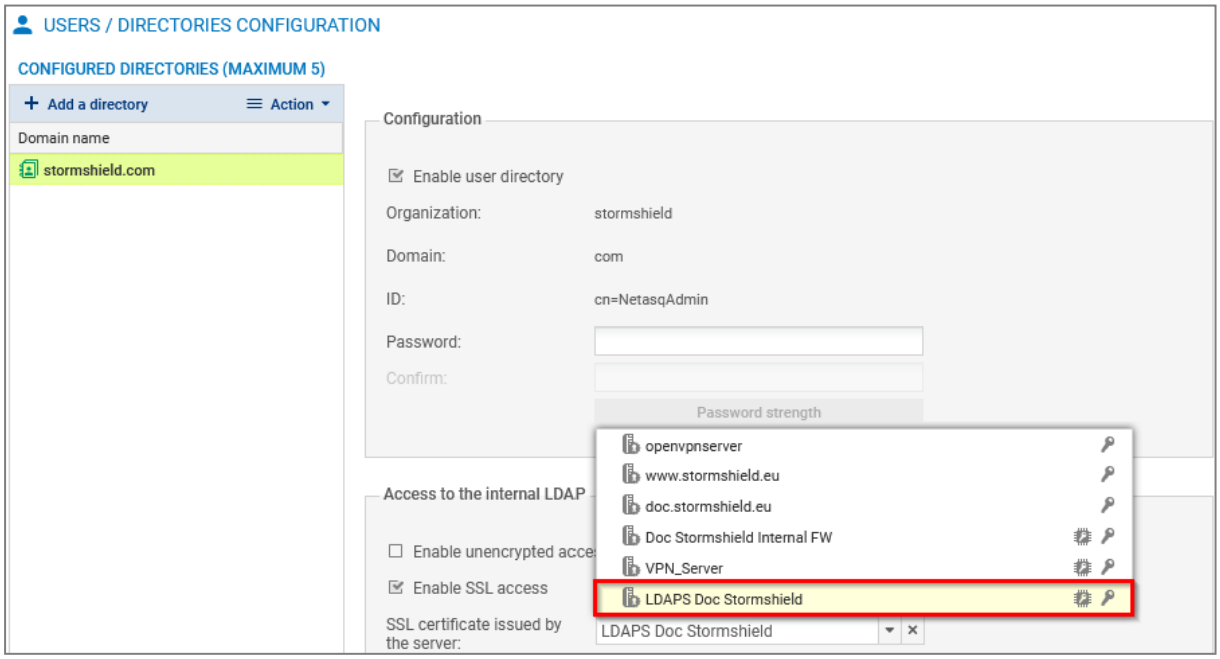
Internal LDAP

This use case is exclusive to SNS 4.7 and higher versions.

The private key of the certificate that is used for authentication to the internal LDAP directory can be protected by the TPM.

To check/change the certificate used:

1. Go to **Configuration** > **Users** > **Directory configuration**.
2. Select the internal LDAP directory from the grid.
3. In **Access to the internal LDAP**, **SSL certificate issued by the server** field, select the desired certificate. The icon indicates certificates with a TPM-protected private key.
4. Apply changes.



Communications with the SMC server

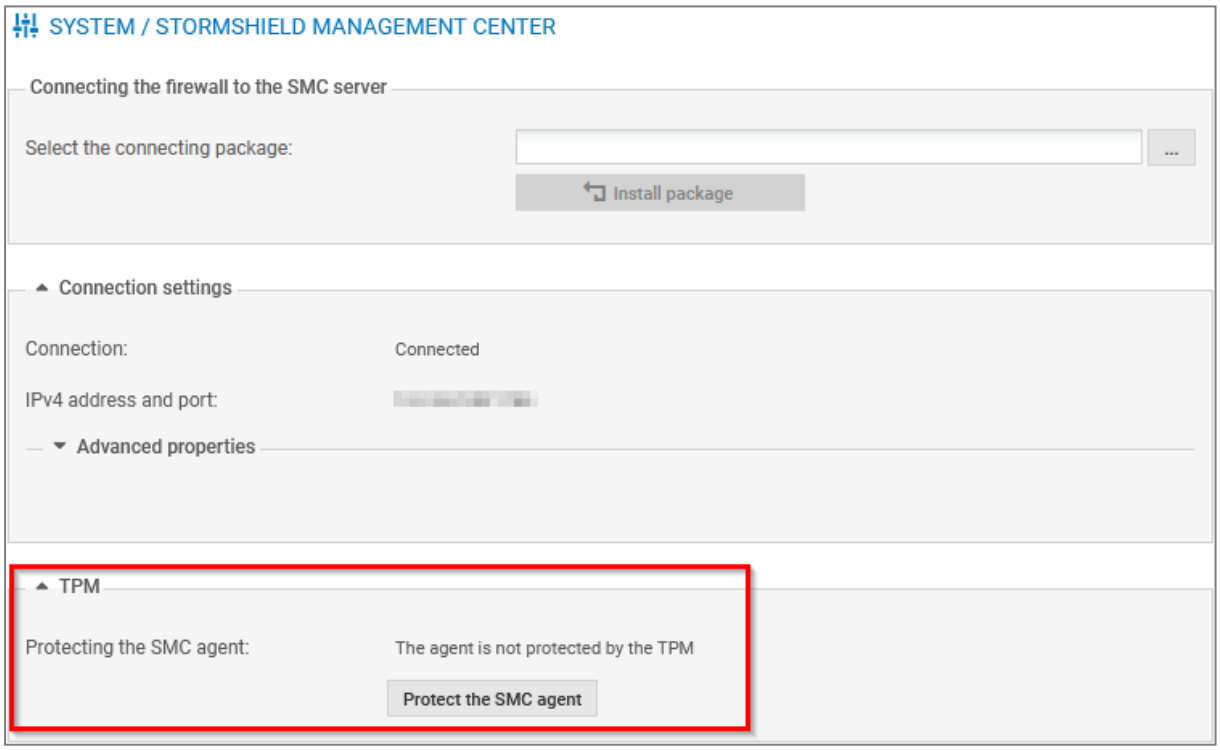
This use case is exclusive to SNS 4.7 and higher versions.

The private key of the certificate that is used for communications with the SMC server can be protected by the TPM. Do note that If the firewall is already connected to an SMC server when the TPM is initialized, the private key of the certificate that is used for communications with the SMC server will have been automatically protected.

IMPORTANT
Keep in mind that communications with the SMC server will no longer function if the private key in the certificate that is used can no longer be decrypted.

To protect the private key of this certificate:

1. Go to **Configuration > System > Management Center.**
2. Under **TPM**, click on **Protect the SMC agent.**
   If the button **Unprotect the SMC agent** appears, this means that the private key is already protected.
3. Confirm changes.



Sending logs to a TLS syslog server

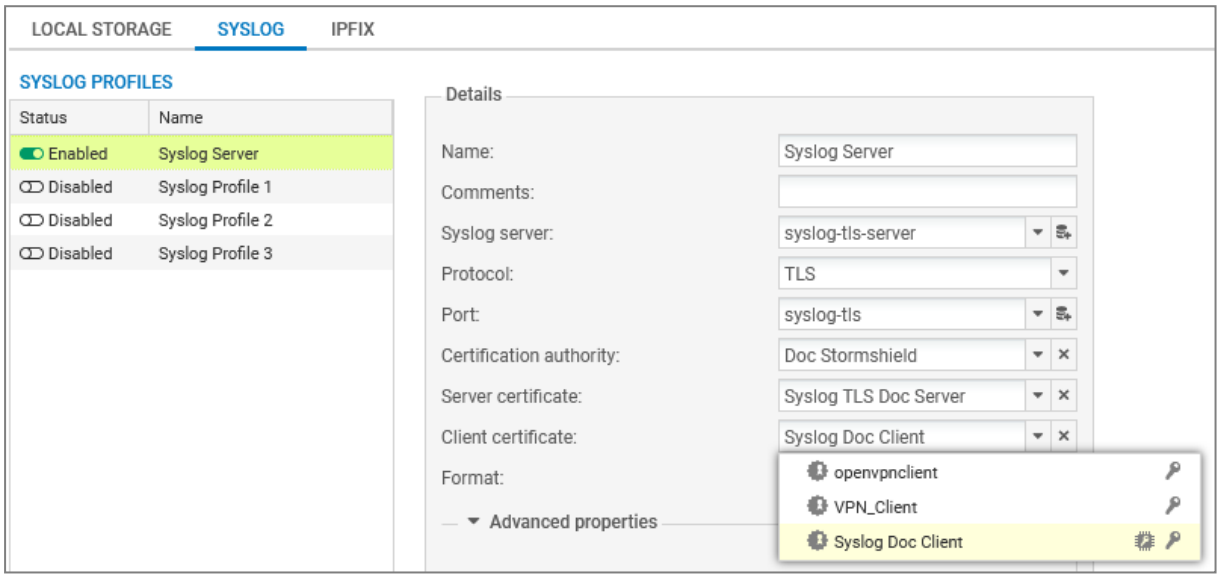
This use case is exclusive to SNS 4.7 and higher versions.

The private key in the server and client certificates that are used for authentication to a TLS syslog server (TLS protocol) can be protected by the TPM.

To check/change the certificates used:

1. Go to **Configuration > Notifications > Logs – Syslog - IPFIX, Syslog** tab.
2. Select the profile of the syslog server that you wish to modify from the grid.

3. In the profile details, select the signing certification authority and the desired certificates in the relevant fields. The icon indicates certificates with a TPM-protected private key.
   If required, you can create a TPM-protected client identity and server identity beforehand in **Configuration > Objects > Certificates and PKI** and select them here.
4. Apply changes.
5. Ensure that the syslog server has the selected client certificate. You can export the certificate as a P12 file in **Configuration > Objects > Certificates and PKI**.



Explanations on usage when the TPM is initialized

This chapter includes explanations on usage when the TPM is initialized:

- Backing up a configuration,
- Restoring a configuration backup,
- Initial configuration via USB key,
- Calculating the high availability (HA) quality factor.

Backing up a configuration

You can manually or automatically back up the configuration of an SNS firewall. Specific conditions apply, depending on the method used.

> **NOTE**
> You are advised to protect the backup file with a password whenever possible.

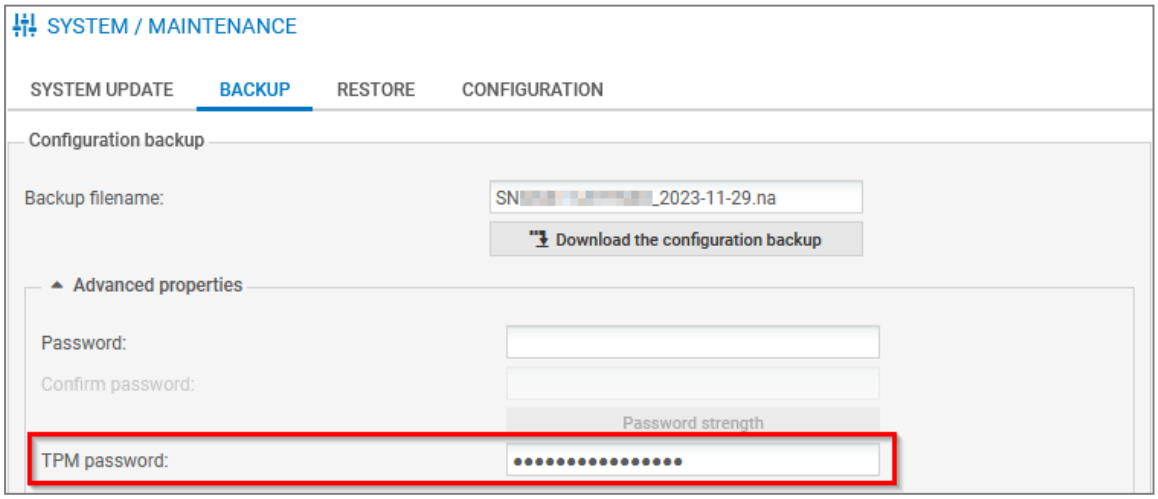
Manual backups

From the web administration interface

This use case is exclusive to SNS 4.3 LTSB versions and SNS 4.7 and higher versions. On SNS 3.11 LTSB versions, backups must be performed from the CLI console.

1. Go to **Configuration > System > Maintenance**, **Backup** tab.
2. In the **Advanced properties** section:
   - You can protect the backup file with a password by filling in the **Password** field,
   - Enter the TPM password in the relevant field.
3. Click on **Download the configuration backup**.

The backup will contain all private keys of certificates on the firewall, but the TPM-protected private keys that are included will be decrypted.



From the CLI console

Run the following command:

```
CONFIG BACKUP list=all password=<filepassword> tpmpassword=<tpmpassword> >
/tmp/backup.na
```

- `password=<filepassword>` makes it possible to protect the backup file with a password,
- `list=all` backs up all modules on the firewall. You can replace `all` with the modules that you wish to back up (`list=network,vpn-ssl`),
- By default, the backup will contain all private keys of certificates on the firewall, but the TPM-protected private keys that are included will be decrypted. To keep the keys encrypted, and if you intend to restore this backup on the same firewall, enter `ondiskprotect=1`,
- If required, show command help with:
  ```
  CONFIG BACKUP HELP
  ```

To retrieve the backup, connect to the firewall with an SCP client. SSH access must be allowed on the firewall, and a filter rule must allow the connection.

From the SMC server

You can manually back up the configuration on an SNS firewall with a CLI script. To include private keys of certificates on the firewall (either TPM-protected or not), the script must contain the TPM password in plaintext.

```
CONFIG BACKUP list=all password=<filepassword> tpmpassword=<password>
$SAVE_TO_DATA_FILE("Backup_with_decyphered_private_keys.na")
```

For more information on configuration tokens in the command, refer to the section From the CLI console above.

For more information on implementing the backup, see the section Backing up the configuration of firewalls in the SMC administration guide.

Automatic backup

From the web administration interface

1. Go to **Configuration > System > Maintenance**, **Backup** tab.
2. In the **Automatic configuration backup** section, enable automatic backups and fill in the required information. You can protect the backup file with a password by filling in the **Backup file password** field,
3. Apply the configuration.

The backup will contain all private keys of certificates on the firewall, and the TPM-protected private keys that are included will be encrypted.

From the SMC server

The SMC server makes it possible to automatically back up the configuration on SNS firewalls. **When the TPM is initialized on the SNS firewall, all private keys of certificates on the firewall (either TPM-protected or not) will be excluded from automatic backups.**

For more information, see the section Backing up the configuration of firewalls in the SMC administration guide.

Summary

Manual backups			Automatic backup	
SNS web interface	CLI console	SMC (CLI script)	SNS web interface	SMC
All private keys are included. TPM-protected private keys are decrypted.	All private keys are included when the *tpmpassword* token is entered. TPM-protected private keys are decrypted, unless the *ondiskprotect=1* token is entered.		All private keys are included. TPM-protected private keys remain encrypted.	-

Restoring a configuration backup

Backups containing TPM-protected private keys of certificates can only be restored on the source firewall. Encrypted private keys cannot be decrypted on another firewall as the symmetric key will be different.

There are a few exceptions in the following cases:

- When the mechanism that derives the symmetric key is enabled and the TPM password is the same on the other firewall,
- Following the exchange of a firewall (RMA) configured in high availability. For more information, refer to the instructions in the Stormshield knowledge base article Following an RMA, how can I synchronize the configuration and the content of the TPM?.

Initial configuration via USB key

During the initial configuration of a firewall via USB key, certain operations allow you to interact with the SNS firewall's TPM:

- The `inittpm` operation allows you to initialize the TPM. Its format is as follows:
  ```
  "serial | any", inittpm, "tpmpassword"
  ```
  - The mechanism that derives the symmetric key is enabled by default,
  - This operation must be performed before a private key is protected by the TPM.
- The `p12import` operation allows you to import PKCS#12 files in *.p12* format and protect the private key contained in the file with the TPM. Its format is as follows:
  ```
  "serial | any", p12import, none|ondisk, "p12file", "p12password"
  ```

For more information on implementing this procedure and other possible operations, refer to the technical note Initial configuration via USB key.

Calculating the high availability (HA) quality factor

This use case is exclusive to SNS 4.3 LTSB versions and SNS 4.7 and higher versions.

The status of the TPM can be applied to the calculation of the high availability (HA) quality factor. The configuration token `TPMQualityIncluded=1` found in the *[Global]* section of the configuration file *ConfigFiles/HA/highavailability* indicates that the status of the TPM has been applied.

For more information on calculating the high availability (HA) quality factor, refer to the technical note High availability on SNS.

Troubleshooting

In this chapter, you will see some of the issues that occur most frequently when using the TPM. If the issue you encounter cannot be found in this chapter, we recommend that you refer to the Stormshield knowledge base.

TIP
You can run a diagnostic on the TPM by executing this command in an SSH console: `tpmctl -a -v`. SSH access must be allowed on the firewall.

Some modules no longer function after a firewall software update

Situation: After the software on a firewall or firewall cluster is updated to SNS version 4.3 LTSB or higher, modules that use certificates with a protected private key no longer function (e.g., VPN tunnels can no longer be set up).

Cause: The system's technical characteristics have been modified following the update of the firewall. These new characteristics no longer allow platform configuration registers (PCRs) to access the TPM. As such, TPM-protected private keys can no longer be decrypted.

Solution: Refresh PCR values.

1. Run the following command in a CLI console:
   ```
   SYSTEM TPM PCRSEAL tpmpassword=<password>
   ```
2. If the firewall is part of a high availability cluster, run the following command to perform the operation on the passive firewall:
   ```
   SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive
   ```
   For more information, refer to the section Updating a cluster in the technical note *High availability on SNS.*

Some modules no longer function after inserting a storage medium and restarting the firewall

Situation: After having inserted a storage medium and restarted the SNS firewall, modules that use certificates with a protected private key no longer function (e.g., VPN tunnels can no longer be set up).

Cause: The system's technical characteristics were modified when the firewall started, as a new storage medium was detected. These new characteristics no longer allow platform configuration registers (PCRs) to access the TPM. As such, TPM-protected private keys can no longer be decrypted.

Solution: Refresh PCR values.

- In SNS 4.3 LTSB versions and SNS 4.7 and higher versions:
  1. Run the following command in a CLI console:
     ```
     SYSTEM TPM PCRSEAL tpmpassword=<password>
     ```
  2. If the firewall is part of a high availability cluster, refresh the PCR values on the passive firewall by running the following command:
     ```
     SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive
     ```

- On SNS 3.11 LTSB versions, run the following command in a SSH console:

```
tpmctl -svp <tpmpassword>
```

SSH access must be allowed on the firewall. Only the *admin* account can perform this operation.

Some modules no longer function after switching from a passive to an active firewall (high availability)

Situation: After having switched from a passive to an active firewall, modules that use certificates with a protected private key no longer function (e.g., VPN tunnels can no longer be set up).

Cause 1: TPM-protected private keys can no longer be decrypted as the mechanism that derives the symmetric key is no longer enabled on the firewall cluster.

Solution 1:

1. Check whether the symmetric key derivation mechanism has been enabled by executing the following command:

```
SYSTEM TPM STATUS tpmpassword=<password>
```

2. Enable the symmetric key derivation mechanism on the cluster and renew the symmetric key by running the following command in a CLI console:

```
SYSTEM TPM RENEW tpmpassword=<password> derivekey=on
HA TPMSYNC tpmpassword=<password>
```

Cause 2: TPM-protected private keys can no longer be decrypted as both firewalls in the cluster were recently updated to SNS version 4.3 LTSB or higher and the PCR values on the passive firewall were not refreshed.

Solution 2: Refresh the PCR values on the new active firewall.

- Run the following command in a CLI console:

```
SYSTEM TPM PCRSEAL tpmpassword=<password>
```

For more information, refer to the section Updating a cluster in the technical note *High availability on SNS*.

Further reading

Additional information and answers to some of your questions may be found in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu