NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

CONFIGURER LE MODULE TPM ET PROTÉGER LES CLÉS PRIVÉES DE CERTIFICATS DU FIREWALL SNS

Produits concernés : SNS 3.11 LTSB, SNS 4.3 LTSB, SNS 4.7 et versions supérieures

Dernière mise à jour du document : 13 février 2024

Référence : sns-fr-TPM_protection_note_technique

Table des matières

Historique des modifications

Date	Description
13 février 2024	- Ajout de précisions concernant les PCR dans la section "Protection de la clé privée des certificats du firewall grâce à la clé symétrique". - Modification de la description de l'état du TPM en orange dans la section "Vérifier si le module TPM est initialisé". - Précisions ajoutées concernant la réinitialisation du TPM dans la section "Si vous avez oublié le mot de passe du TPM". - Reformulation de l'explication du jeton `force=on` dans la section "Désactiver le module TPM". - Modification de l'exemple *<CN>* par *<CERTNAME>* dans les sections "Protéger la clé privée d'un certificat déjà ajouté" et "Vérifier si la clé privée d'un certificat du firewall SNS est protégée". - Reformulation de l'information concernant l'autorité de certification dans la section "VPN SSL". - Ajout d'une information importante concernant l'utilisation d'une clé privée protégée dans la section "Communications avec le serveur SMC". - Ajout de précisions concernant la protection par mot de passe du fichier de sauvegarde dans la section "Sauvegarde de configuration".
18 janvier 2024	Nouveau document

Avant de commencer

Le module TPM (*Trusted Platform Module*) présent sur certains firewalls SNS offre un stockage matériel renforçant le niveau de sécurité des certificats stockés sur le firewall.

Ce mécanisme de sécurisation par le module TPM s'applique à certains certificats selon la version SNS installée sur le firewall.

Cette note technique présente l'initialisation et la configuration du module TPM d'un firewall SNS, ainsi que la protection par le TPM de la clé privée des certificats du firewall jusqu'à la configuration de ces certificats dans les modules du firewall.

Prérequis

Posséder un firewall SNS disposant d'un module TPM

Tous les modèles récents depuis le SNi20 disposent d'un module TPM.

Retrouvez les modèles concernés sur la page Nos firewalls Stormshield Network Security du site de Stormshield.

Avoir installé une version SNS compatible

Le mécanisme de sécurisation par le module TPM s'applique à certains certificats selon la version SNS installée sur le firewall.

Certificats utilisés dans les cas suivants et dont la clé privée peut être protégée	Versions SNS compatibles		
	3.11 LTSB	4.3 LTSB	4.7 et supérieures
VPN IPsec	✓	✓	✓
VPN SSL	-	-	✓
Déchiffrement SSL/TLS (interface Web d'administration et portail captif)	-	-	✓
Communications avec le serveur SMC	-	-	✓
Envois de logs vers un serveur syslog	-	-	✓
LDAP interne	-	-	✓

Disposer d'un droit d'accès au module TPM

Pour initialiser et utiliser le module TPM, l'administrateur doit posséder le droit **Accès au TPM (E)**. Seul le compte *admin* peut attribuer ce droit dans l'interface Web d'administration du firewall dans **Configuration > Système > Administrateurs**, onglet **Administrateurs**, bouton **Passer en vue avancée**.

Pouvoir accéder à la console CLI du firewall SNS

Selon la version SNS installée sur le firewall, certaines actions ou toutes les actions liées au TPM doivent être réalisées dans une console CLI avec des commandes.

Pour accéder à la console CLI, rendez-vous par exemple dans l'interface Web d'administration du firewall dans **Configuration > Système > Console CLI**.

Fonctionnement

Certificats dont la clé privée peut être protégée par le module TPM

Retrouvez les certificats concernés et les versions SNS compatibles dans le chapitre Prérequis.

Mot de passe d'administration du module TPM

Lors de l'initialisation du module TPM sur le firewall SNS, un mot de passe d'administration du TPM doit être défini. Ce dernier est indispensable pour réaliser certaines actions sur le module TPM, comme arrêter de protéger la clé privée d'un certificat ou désactiver le module TPM.

Dans cette note technique, le mot de passe d'administration du module TPM est nommé "*mot de passe du TPM*".

IMPORTANT
Conservez le mot de passe du TPM dans un espace sécurisé et sauvegardé. En cas de perte, Stormshield n'est pas en mesure de retrouver ce mot de passe.

Protection de la clé privée des certificats du firewall grâce à la clé symétrique

Quand la clé privée d'un certificat est protégée par le TPM, celle-ci est chiffrée grâce à une clé symétrique. **Seule la clé symétrique permet de chiffrer et de déchiffrer la clé privée du certificat.**

La clé symétrique est définie lors de l'initialisation du module TPM et est stockée sur le TPM. L'accès à cette clé est strictement protégé, notamment par une mesure fiable de l'état du système : les registres PCR (*Platform Configuration Registers*).

Lorsqu'une clé privée doit être déchiffrée, le firewall doit récupérer la clé symétrique du TPM. Cette opération ne peut aboutir que si l'état du firewall est reconnu comme fiable par les PCR.

Dans le cas où les PCR changent, par exemple après une mise à jour de version SNS impliquant des modifications dans la séquence de démarrage du produit, le firewall ne peut plus récupérer la clé symétrique et les clés privées protégées ne peuvent plus être déchiffrées. Seul le mot de passe du TPM permet de mettre à jour la politique d'accès et ainsi de retrouver l'usage de ces clés (ce cas est décrit dans le chapitre Résoudre les problèmes).

Mécanisme de dérivation de la clé symétrique pour un cluster de firewalls

Dans le cas d'un cluster de firewalls en haute disponibilité (HA), chaque firewall dispose de son propre module TPM. Deux clés symétriques existent donc :

- Une première clé symétrique stockée sur le module TPM du firewall actif,
- Une seconde clé symétrique stockée sur le module TPM du firewall passif.

Un mécanisme de dérivation de la clé symétrique (appelé *derivekey*) permet de définir sur les deux firewalls du cluster la même clé symétrique. Ainsi, en cas de bascule du firewall passif en actif, les clés privées de certificats protégées par le TPM peuvent toujours être déchiffrées car les clés symétriques sont les mêmes.

Configurer le module TPM du firewall SNS

Ce chapitre explique comment configurer le module TPM d'un firewall SNS.

Initialiser le module TPM

Cette section contient les procédures d'initialisation du module TPM d'un firewall SNS ou des modules TPM d'un cluster de firewalls en haute disponibilité (HA).

> **NOTE**
> L'initialisation du module TPM n'entraîne pas automatiquement la protection des clés privées de certificats du firewall. Pour les protéger, reportez-vous au chapitre Protéger les clés privées de certificats du firewall SNS.

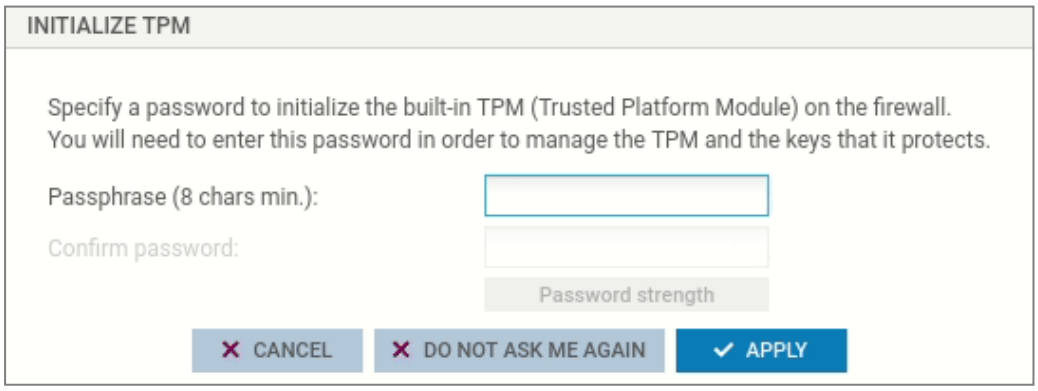
Initialiser le module TPM d'un firewall SNS

Depuis l'interface Web d'administration

Ce cas concerne exclusivement les versions SNS 4.3 LTSB et SNS 4.7 et supérieures.

1. Rendez-vous dans **Configuration > Objets > Certificats et PKI**.
2. Dans la fenêtre d'initialisation du TPM, définissez un mot de passe d'administration du TPM. Il doit respecter la politique de mots de passe définie sur le firewall. **Conservez le mot de passe du TPM dans un espace sécurisé et sauvegardé**.
   Si la fenêtre n'apparaît pas, vérifiez si le module TPM n'est pas déjà initialisé. Si nécessaire, initialisez le module TPM depuis la console CLI.
3. Cliquez sur **Appliquer**.

Si le firewall est membre d'un cluster en haute disponibilité, le mécanisme de dérivation de la clé symétrique est automatiquement activé.



Depuis la console CLI

Exécutez la commande suivante :

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

- Remplacez `<password>` par le mot de passe d'administration du TPM souhaité. Il doit respecter la politique de mots de passe définie sur le firewall. **Conservez le mot de passe du TPM dans un espace sécurisé et sauvegardé**,
- Si le firewall est membre d'un cluster en haute disponibilité, renseignez `derivekey=on`.

Initialiser les modules TPM d'un cluster de firewalls en haute disponibilité (HA)

Si le cluster est déjà créé

Initialisez le TPM du firewall actif afin de déclencher automatiquement l'initialisation du TPM du firewall passif. Reportez-vous aux procédures ci-dessus.

Si le cluster n'est pas encore créé

Deux possibilités existent selon si le TPM est déjà initialisé ou non sur les firewalls du cluster.

Le TPM n'est pas encore initialisé sur les firewalls du cluster

1. Configurez le cluster (création du cluster et intégration du second firewall).
2. Initialisez le TPM du firewall actif afin de déclencher automatiquement l'initialisation du TPM du firewall passif. Reportez-vous aux procédures ci-dessus.

Le TPM est déjà initialisé sur le futur firewall actif du cluster

1. Configurez le cluster (création du cluster et intégration du second firewall).
2. Renouvelez la clé symétrique du firewall actif en exécutant la commande suivante dans une console CLI :

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

   - Remplacez `<password>` par le mot de passe du TPM,
   - Comme le firewall est membre d'un cluster, renseignez `derivekey=on`.

   Toutes les clés privées de certificats protégées par le TPM sont déchiffrées puis re-chiffrées avec la nouvelle clé symétrique (dérivée du mot de passe du TPM).
3. Initialisez le module TPM du firewall passif en exécutant la commande suivante :

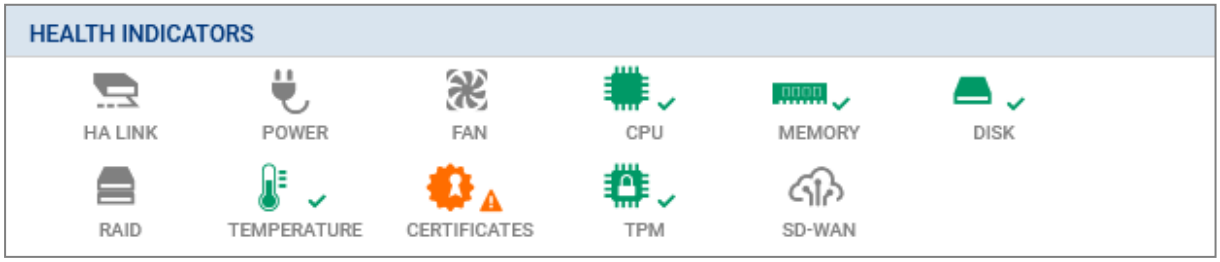
   ```
   HA TPMSYNC tpmpassword=<password>
   ```

Vérifier si le module TPM est initialisé

Depuis l'interface Web d'administration

Ce cas concerne exclusivement les versions SNS 4.7 et supérieures.

1. Rendez-vous dans **Monitoring > Tableau de bord**.
2. Dans le widget **Indicateurs de santé**, vérifiez l'état du module TPM :
   - Un état en vert indique que le TPM est initialisé et opérationnel,
   - Un état en orange indique que le TPM n'est pas initialisé ou que les sauvegardes automatiques de la configuration du firewall ne sont pas protégées par un mot de passe,
   - Un état en rouge indique que les tests sur le TPM ne sont pas fonctionnels (par exemple lorsque le module TPM ne répond plus),
   - Si l'état du TPM n'apparaît pas (icône non visible), c'est que le firewall n'est pas équipé d'un TPM.



Depuis la console CLI

Exécutez la commande suivante :

```
SYSTEM PROPERTY
```

`TpmInit=1` indique que le module TPM est initialisé.

Gérer le mot de passe du TPM

Modifier le mot de passe du TPM

Dans une console CLI, exécutez la commande suivante :

```
SYSTEM TPM CHANGE currentpassword=<current_password> newpassword=<new_password>
```

- Remplacez `<current_password>` par l'actuel mot de passe du TPM,
- Remplacez `<new_password>` par le nouveau mot de passe du TPM. Il doit respecter la politique de mots de passe définie sur le firewall. **Conservez le mot de passe du TPM dans un espace sécurisé et sauvegardé**.

Si vous avez oublié le mot de passe du TPM

Il n'est pas possible de réinitialiser le mot de passe du TPM. Si vous ne retrouvez pas le mot de passe du TPM, en dernier recours, vous pouvez réinitialiser le module TPM du firewall.

Notez que réinitialiser le module TPM **ne permet pas** de retrouver l'usage des clés privées de certificats chiffrées. Vous devrez ré-importer sur le firewall les certificats concernés et protéger de nouveau leur clé privée.

Pour réinitialiser le module TPM, reportez-vous aux instructions de l'article I've lost my TPM password, how can I reset it? de la Base de connaissances Stormshield (anglais uniquement).

Désactiver le module TPM

Dans une console CLI, exécutez la commande suivante :

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

- Remplacez `<password>` par le mot de passe du TPM,
- Renseignez `force=on` si des clés privées de certificats sont protégées par le TPM et que vous souhaitez tout de même forcer sa désactivation. Les clés privées protégées seront alors déchiffrées.

Protéger les clés privées de certificats du firewall SNS

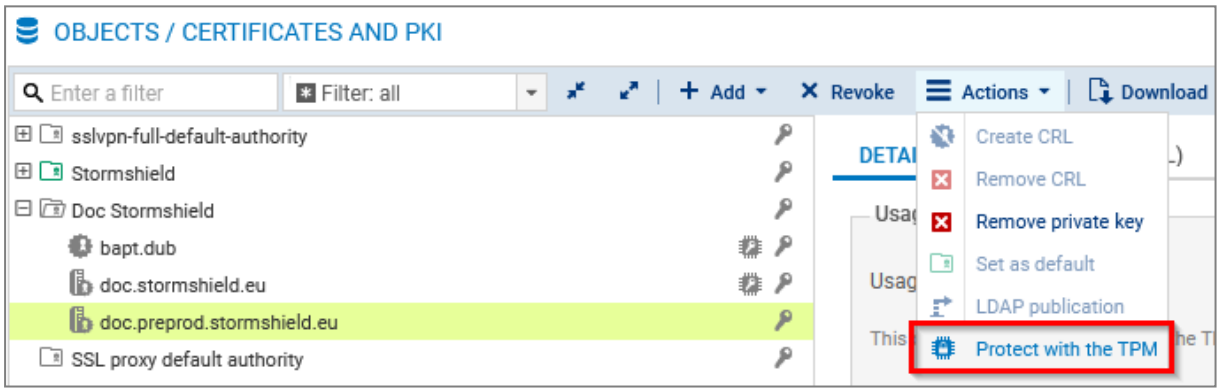
Ce chapitre explique comment protéger par le TPM la clé privée d'un certificat du firewall SNS.

Protéger la clé privée d'un certificat déjà ajouté

Depuis l'interface Web d'administration

Ce cas concerne exclusivement les versions SNS 4.7 et supérieures.

1. Dans **Configuration** > **Objets** > **Certificats et PKI**, sélectionnez le certificat (identité) concerné.
2. Cliquez sur **Actions** > **Protéger avec le TPM**.
3. Cliquez sur **OK**.



Depuis la console CLI

1. Exécutez la commande suivante pour afficher les autorités de certification :
   ```
   PKI CA LIST
   ```
2. Si nécessaire, affichez la liste des autorités de certification intermédiaires signées par l'autorité racine concernée (`<RootCA>` dans la commande) avec :
   ```
   PKI CA LIST CANAME=<RootCA>
   ```
3. Affichez les certificats issus de l'autorité de certification (`<CA>` dans la commande) avec :
   ```
   PKI CERT LIST CANAME=<CA>
   ```
4. Protégez la clé privée du certificat concerné (`<CERTNAME>` dans la commande) avec :
   ```
   PKI CERT PROTECT CANAME=<CA> NAME=<CERTNAME> tpm=ondisk
   ```
5. Activez le changement de configuration avec :
   ```
   PKI ACTIVATE
   ```

Depuis le serveur SMC

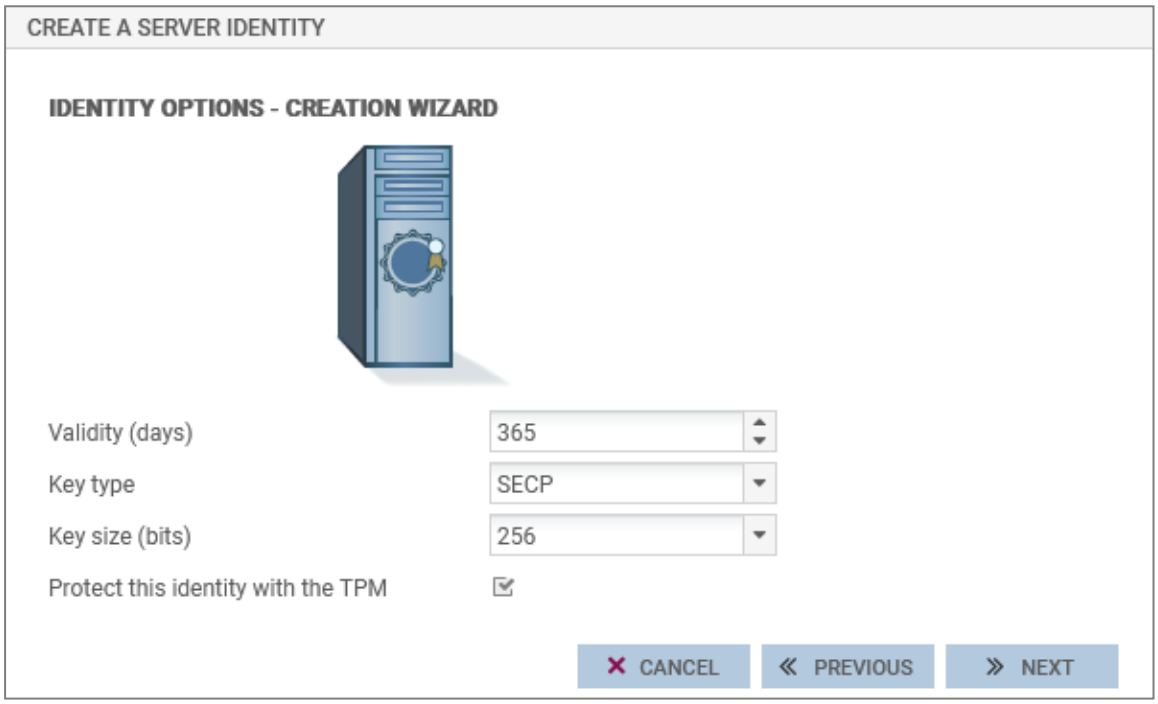
Pour plus d'informations, reportez-vous à la section Activer la protection par TPM d'une clé privée déjà existante du Guide d'administration SMC.

Ajouter un certificat et protéger sa clé privée

Depuis l'interface Web d'administration

1. Dans **Configuration > Objets > Certificats et PKI**, cliquez sur **Ajouter** et sélectionnez le certificat (identité) à ajouter.
2. Complétez les informations demandées. Pour les versions SNS 4.3 LTSB et SNS 4.7 et supérieures, cochez la case **Protéger cette identité à l'aide du TPM** pendant les étapes.
3. Cliquez sur **Terminer**.
4. Pour les versions SNS 3.11 LTSB, protégez la clé privée du certificat depuis la console CLI.

Pour plus d'informations, reportez-vous à la section *Certificats et PKI* du manuel utilisateur v4 ou v3 de la version SNS utilisée.



Depuis la console CLI

1. Exécutez la commande suivante en utilisant notamment le jeton `tpm=ondisk` :

```
PKI CERT CREATE
```

Si nécessaire, affichez l'aide de la commande avec :

```
PKI CERT CREATE HELP
```

2. Activez ensuite le changement de configuration avec :

```
PKI ACTIVATE
```

Depuis le serveur SMC

Vous pouvez importer des certificats (identités) sur le serveur SMC et les déclarer sur le firewall SNS. Pour plus d'informations, reportez-vous à la section Importer ou déclarer un certificat pour un firewall du Guide d'administration SMC.

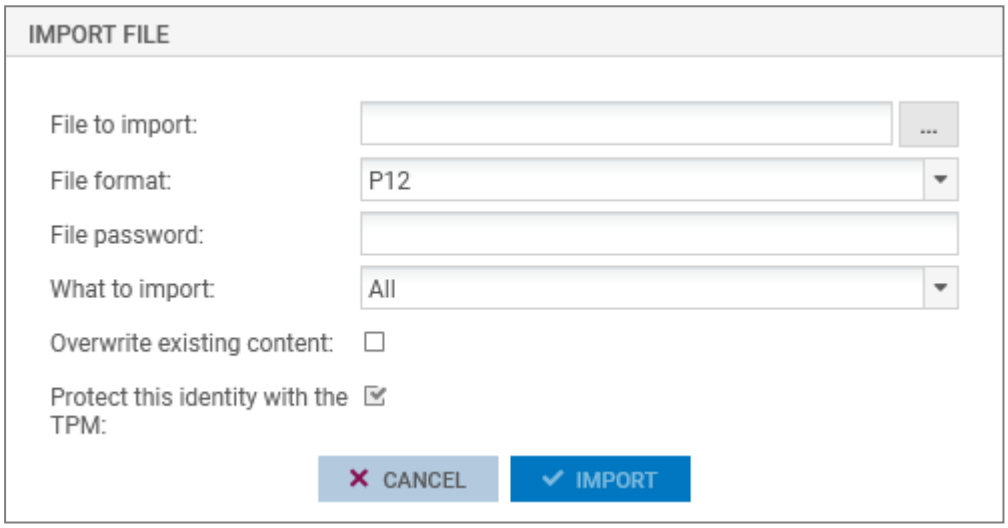
Par défaut, les clés privées des certificats déclarés sur le firewall SNS par le serveur SMC sont protégées par le TPM si ce dernier est initialisé. Pour modifier ce comportement, reportez-vous à la section Désactiver la protection de la clé privée par TPM du Guide d'administration SMC.

Importer un certificat et protéger sa clé privée

Depuis l'interface Web d'administration

1. Dans **Configuration > Objets > Certificats et PKI**, cliquez sur **Ajouter > Importer un fichier**.
2. Complétez les informations demandées. Pour les versions SNS 4.3 LTSB et SNS 4.7 et supérieures, cochez la case **Protéger cette identité à l'aide du TPM**.
3. Cliquez sur **Importer**.
4. Pour les versions SNS 3.11 LTSB, protégez la clé privée du certificat depuis la console CLI.

Pour plus d'informations, reportez-vous à la section *Certificats et PKI* du manuel utilisateur v4 ou v3 de la version SNS utilisée.



Depuis le serveur SMC

Vous pouvez importer des certificats (identités) sur le serveur SMC et les déclarer sur le firewall SNS. Pour plus d'informations, reportez-vous à la section Importer ou déclarer un certificat pour un firewall du Guide d'administration SMC.

Par défaut, les clés privées des certificats déclarés sur le firewall SNS par le serveur SMC sont protégées par le TPM si ce dernier est initialisé. Pour modifier ce comportement, reportez-vous à la section Désactiver la protection de la clé privée par TPM du Guide d'administration SMC.

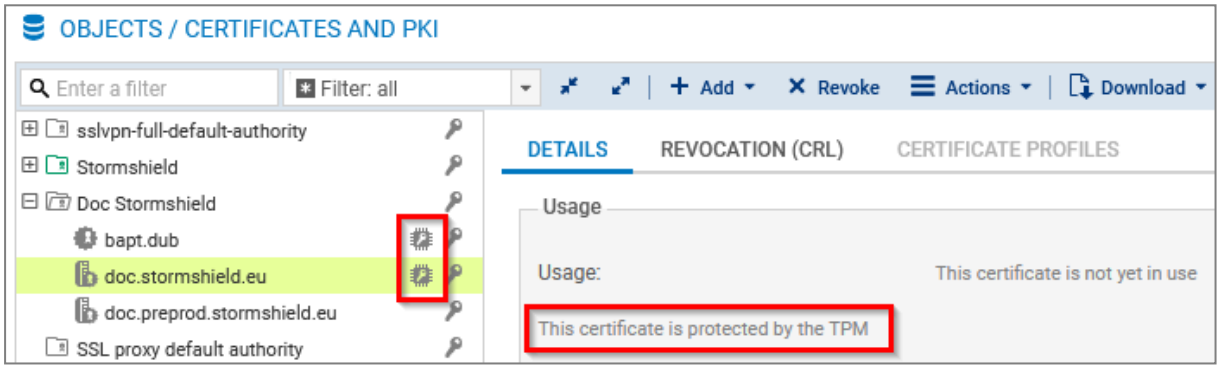
Vérifier si la clé privée d'un certificat du firewall SNS est protégée

Ce chapitre explique comment vérifier si la clé privée d'un certificat du firewall SNS est protégée par le module TPM.

Depuis l'interface Web d'administration

Ce cas concerne exclusivement les versions SNS 4.7 et supérieures.

Dans **Configuration > Objets > Certificats et PKI**, repérez le certificat (identité) concerné. Si l'icône apparaît, la clé privée du certificat est protégée par le TPM. L'information apparaît également dans l'onglet **Détails** en sélectionnant au préalable le certificat concerné.



Depuis la console CLI

Pour vérifier les certificats utilisés dans la configuration du firewall :

Exécutez la commande suivante :

```
MONITOR CERT
```

`tpm=Used` indique que la clé privée du certificat est protégée par le TPM.

Pour vérifier l'ensemble des certificats du firewall :

1. Exécutez la commande suivante pour afficher les autorités de certification :
   ```
   PKI CA LIST
   ```
2. Si nécessaire, affichez la liste des autorités de certification intermédiaires signées par l'autorité racine concernée (`<RootCA>` dans la commande) avec :
   ```
   PKI CA LIST CANAME=<RootCA>
   ```
3. Affichez les certificats issus de l'autorité de certification (`<CA>` dans la commande) avec :
   ```
   PKI CERT LIST CANAME=<CA>
   ```
   `tpm=ondisk` indique que la clé privée du certificat est protégée par le TPM.
4. Si nécessaire, affichez les informations d'un certificat (`<CERTNAME>` dans la commande) avec :
   ```
   PKI CERT SHOW CANAME=<CA> NAME=<CERTNAME>
   ```

Depuis le serveur SMC

Pour plus d'informations, reportez-vous à la section Savoir si une clé privée est protégée par TPM du Guide d'administration SMC.

Utiliser des certificats dont la clé privée est protégée par le TPM

Ce chapitre récapitule les cas où vous pouvez utiliser des certificats dont la clé privée est protégée par le TPM :

- Déchiffrement SSL/TLS (interface Web d'administration et portail captif),
- VPN SSL,
- VPN IPsec,
- LDAP interne,
- Communications avec le serveur SMC,
- Envois de logs vers un serveur Syslog TLS.

Déchiffrement SSL/TLS (interface Web d'administration et portail captif)

Ce cas concerne exclusivement les versions SNS 4.7 et supérieures.

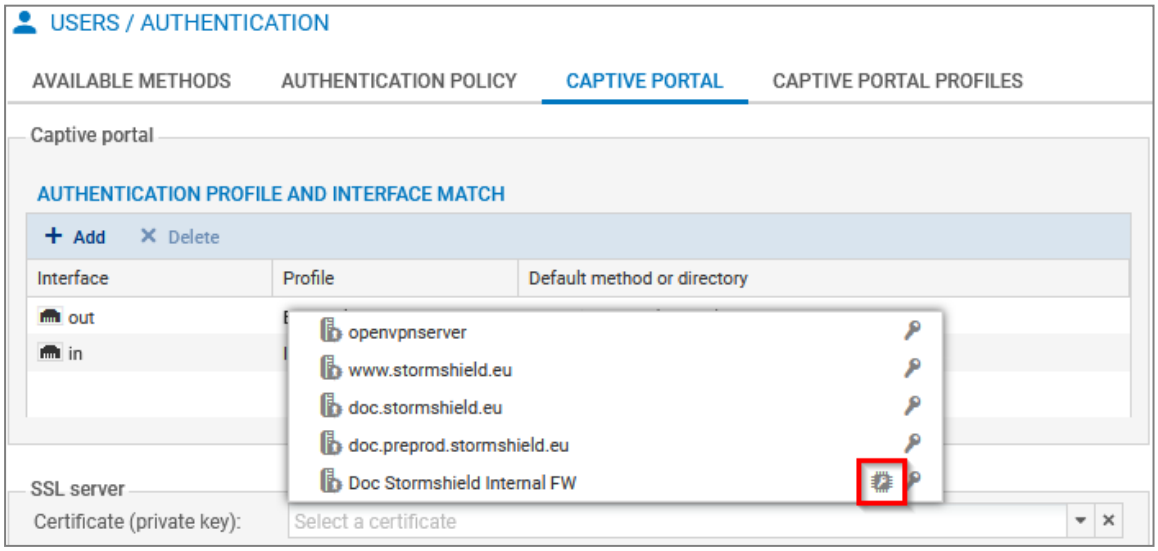
La clé privée du certificat présenté par l'interface Web d'administration du firewall et son portail captif peut être protégée par le module TPM.

IMPORTANT
Prenez en considération que l'accès à ces interfaces ne sera plus possible si la clé privée du certificat utilisé ne peut plus être déchiffrée.

Pour vérifier / modifier le certificat utilisé :

1. Rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Portail captif**, cadre **Serveur SSL**.
2. Dans le champ **Certificat (clé privée)**, sélectionnez le certificat souhaité. L'icône indique les certificats dont la clé privée est protégée par le TPM.
3. Appliquez la modification.

La connexion à l'interface Web d'administration est alors perdue. En retournant sur la page d'authentification, un avertissement peut apparaître en fonction du certificat utilisé. Vous pouvez continuer vers le site.



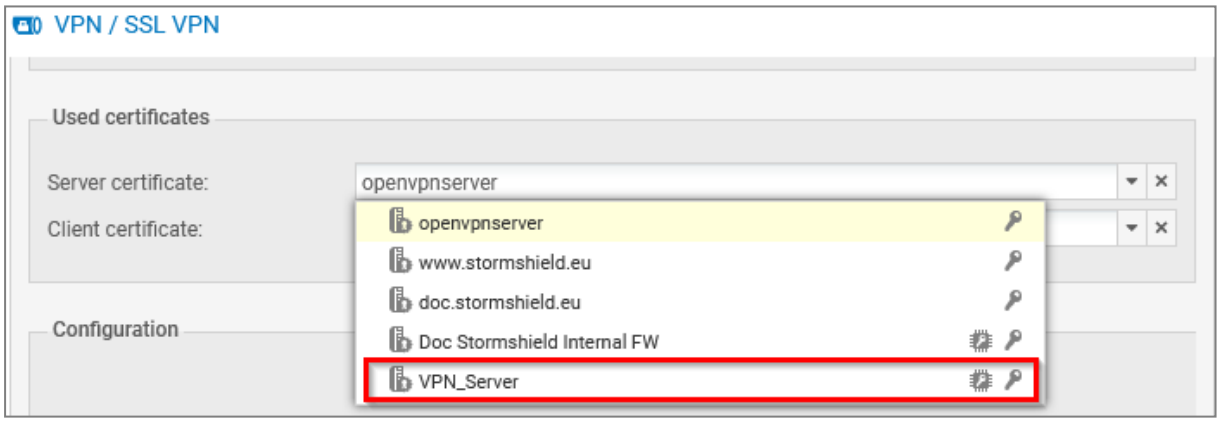
VPN SSL

Ce cas concerne exclusivement les versions SNS 4.7 et supérieures.

Le service VPN SSL du firewall SNS et le client VPN présentent des certificats (serveur et client) pour établir un tunnel.

Pour vérifier / modifier les certificats utilisés :

1. Rendez-vous dans **Configuration > VPN > VPN SSL**, zone **Configuration avancée**, cadre **Certificats utilisés**.
2. Sélectionnez les certificats souhaités dans les champs correspondants. Ils doivent être issus de la même autorité de certification.
   - Dans le champ **Certificat serveur**, l'icône indique les certificats dont la clé privée est protégée par le TPM,
   - Dans le champ **Certificat client**, vous ne pouvez pas sélectionner un certificat dont la clé privée est protégée par le TPM. En effet, la clé privée de ce certificat doit être disponible en clair (non chiffrée) dans la configuration VPN distribuée aux clients VPN.
3. Appliquez la modification.
4. Si vous utilisez le client VPN SSL Stormshield en mode automatique, la configuration VPN sera automatiquement récupérée à la prochaine connexion. Pour tous les autres cas, vous devez ré-importer manuellement la configuration (fichier *.ovpn*). Pour plus d'informations, reportez-vous à la note technique Configurer et utiliser le VPN SSL des firewalls SNS.



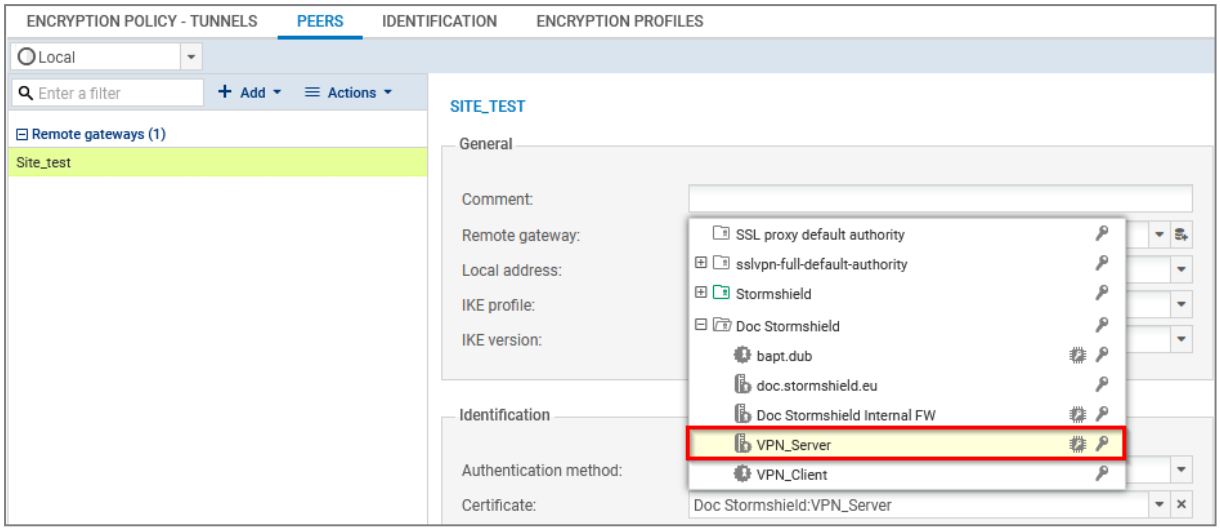
VPN IPsec

La clé privée du certificat présenté pour établir des tunnels IPsec avec authentification par certificat peut être protégée par le module TPM.

Pour vérifier / modifier le certificat utilisé :

1. Rendez-vous dans **Configuration > VPN > VPN IPsec**, onglet **Correspondants**.
2. Dans la grille, sélectionnez le correspondant utilisé dans la configuration VPN.
3. Dans le cadre **Identification**, champ **Certificat**, sélectionnez le certificat souhaité. L'icône indique les certificats dont la clé privée est protégée par le TPM.
   Pour des configurations utilisant le moteur de gestion des tunnels VPN IPsec IKEv1, les tunnels ne s'établiront plus si la clé privée du certificat utilisé est protégée par le TPM.
4. Appliquez la modification.

Vous pouvez également sélectionner le certificat lors de l'ajout d'un correspondant (passerelle distante ou correspondant mobile avec authentification par certificat).



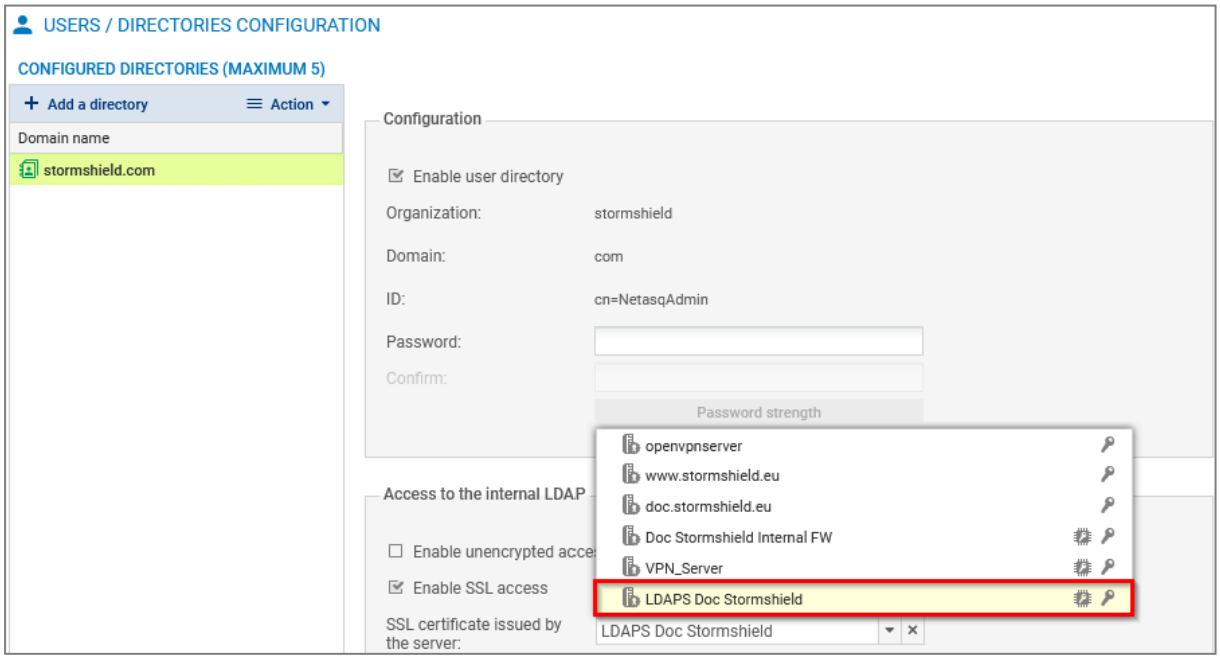
LDAP interne

Ce cas concerne exclusivement les versions SNS 4.7 et supérieures.

La clé privée du certificat utilisé pour l'authentification à l'annuaire LDAP interne peut être protégée par le module TPM.

Pour vérifier / modifier le certificat utilisé :

1. Rendez-vous dans **Configuration > Utilisateurs > Configuration des annuaires**.
2. Dans la grille, sélectionnez l'annuaire LDAP interne.
3. Dans le cadre **Accès au LDAP interne**, champ **Certificat SSL présenté par le serveur**, sélectionnez le certificat souhaité. L'icône indique les certificats dont la clé privée est protégée par le TPM.
4. Appliquez la modification.



Communications avec le serveur SMC

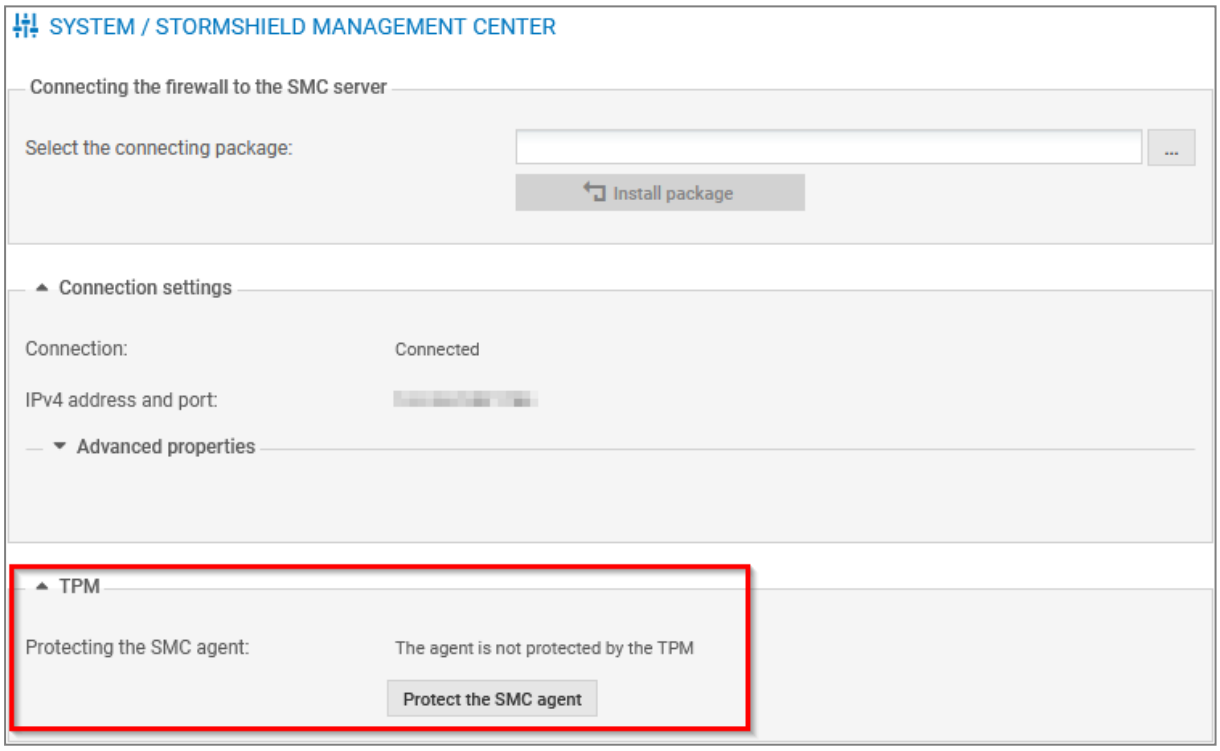
Ce cas concerne exclusivement les versions SNS 4.7 et supérieures.

La clé privée du certificat utilisé pour les communications avec le serveur SMC peut être protégée par le module TPM. À noter que si le firewall était déjà rattaché à un serveur SMC lors de l'initialisation du module TPM, la clé privée du certificat utilisé pour les communications avec le serveur SMC a été protégée automatiquement.

IMPORTANT
Prenez en considération que les communications avec le serveur SMC ne fonctionneront plus si la clé privée du certificat utilisé ne peut plus être déchiffrée.

Pour protéger la clé privée de ce certificat :

1. Rendez-vous dans **Configuration > Système > Management Center**.
2. Dans le cadre **TPM**, cliquez sur **Protéger l'agent SMC**.
   Si le bouton **Déprotéger l'agent SMC** apparaît, c'est que la clé privée est déjà protégée.
3. Confirmez la modification.



Envois de logs vers un serveur Syslog TLS

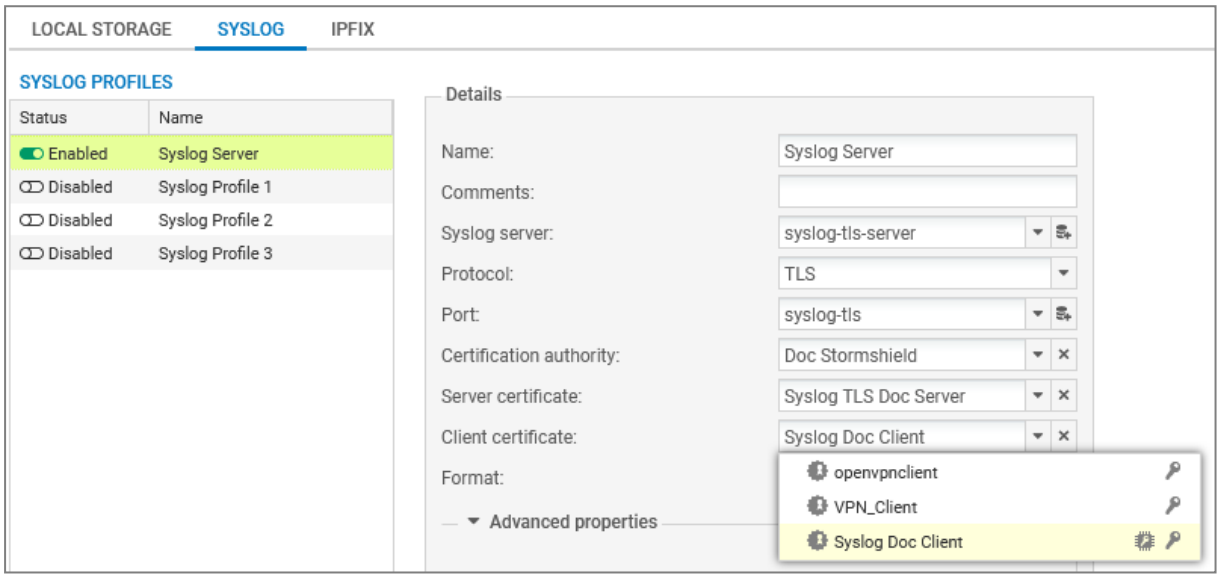
Ce cas concerne exclusivement les versions SNS 4.7 et supérieures.

La clé privée des certificats serveur et client utilisés pour l'authentification à un serveur Syslog TLS (protocole TLS) peut être protégée par le module TPM.

Pour vérifier / modifier les certificats utilisés :

1. Rendez-vous dans **Configuration > Notifications > Logs - Syslog - IPFIX**, onglet **Syslog**.
2. Dans la grille, sélectionnez le profil du serveur Syslog que vous souhaitez modifier.

3. Dans les détails du profil, sélectionnez l'autorité de certification signataire et les certificats souhaités dans les champs correspondants. L'icône indique les certificats dont la clé privée est protégée par le TPM.
   Si besoin, vous pouvez au préalable créer une identité client et une identité serveur protégées par le TPM dans **Configuration > Objets > Certificats et PKI** et les sélectionner ici.
4. Appliquez la modification.
5. Assurez-vous que le serveur Syslog dispose bien du certificat client sélectionné. Vous pouvez exporter le certificat au format P12 dans **Configuration > Objets > Certificats et PKI**.



Précisions sur les cas d'utilisation une fois le module TPM initialisé

Ce chapitre présente des précisions sur des cas d'utilisation une fois le module TPM initialisé :

- Sauvegarde de configuration,
- Restauration d'une sauvegarde de configuration,
- Procédure de configuration initiale par clé USB,
- Calcul du facteur de qualité de la haute disponibilité (HA).

Sauvegarde de configuration

Vous pouvez sauvegarder manuellement ou automatiquement la configuration d'un firewall SNS. Des spécificités existent selon la méthode utilisée.

> **NOTE**
> Il est recommandé de protéger le fichier de sauvegarde par un mot de passe lorsque cela est possible.

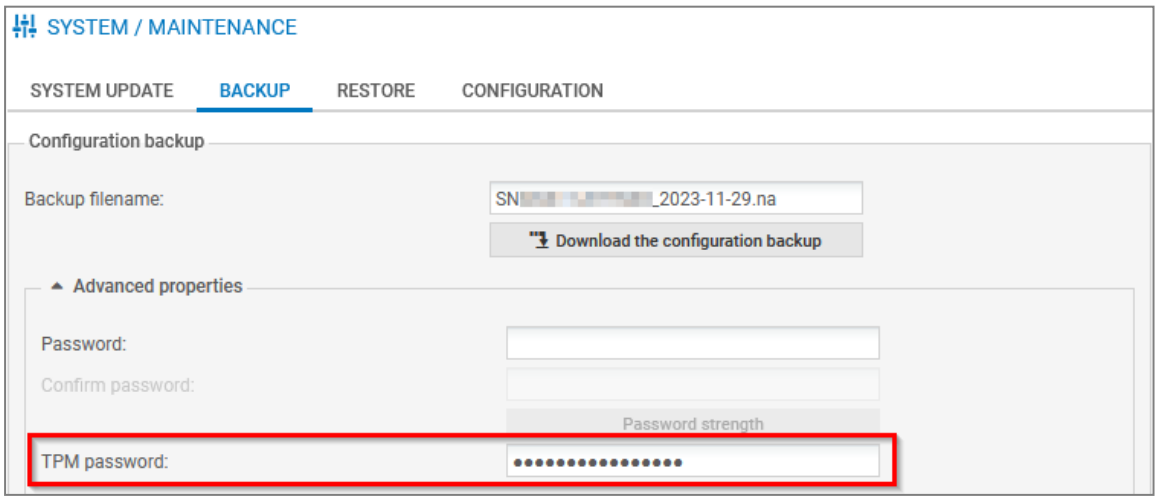
Sauvegarde manuelle

Depuis l'interface Web d'administration

Ce cas concerne exclusivement les versions SNS 4.3 LTSB et SNS 4.7 et supérieures. Pour les versions SNS 3.11 LTSB, vous devez réaliser la sauvegarde depuis la console CLI.

1. Rendez-vous dans **Configuration > Système > Maintenance**, onglet **Sauvegarder**.
2. Dans le cadre **Configuration avancée** :
   - Vous pouvez protéger par un mot de passe le fichier de sauvegarde en complétant le champ **Mot de passe**,
   - Renseignez le mot de passe du TPM dans le champ correspondant.
3. Cliquez sur **Télécharger la sauvegarde de configuration**.

La sauvegarde contient toutes les clés privées de certificats du firewall, mais **celles protégées par le TPM sont incluses déchiffrées**.



Depuis la console CLI

Exécutez la commande suivante :

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

- `password=<filepassword>` permet de protéger le fichier de sauvegarde par un mot de passe,
- `list=all` permet de sauvegarder tous les modules du firewall. Vous pouvez remplacer `all` par les modules à sauvegarder (`list=network,vpn-ssl`),
- Par défaut, la sauvegarde contient toutes les clés privées de certificats du firewall, mais celles protégées par le TPM sont incluses déchiffrées. Pour les conserver chiffrées, et si vous allez restaurer cette sauvegarde sur le même firewall, renseignez `ondiskprotect=1`,
- Si nécessaire, affichez l'aide de la commande avec :
  ```
  CONFIG BACKUP HELP
  ```

Pour récupérer la sauvegarde, connectez-vous au firewall avec un client SCP. L'accès SSH doit être autorisé sur le firewall et une règle de filtrage doit autoriser la connexion.

Depuis le serveur SMC

Vous pouvez sauvegarder manuellement la configuration d'un firewall SNS avec un script CLI. Pour inclure les clés privées de certificats du firewall (protégées par le TPM ou non), le script doit contenir le mot de passe du TPM en clair.

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

Pour plus d'informations sur les jetons de configuration de la commande, reportez-vous à la section ci-dessus Depuis la console CLI.

Pour plus d'informations sur la mise en œuvre de cette sauvegarde, reportez-vous à la section Sauvegarder la configuration des firewalls du Guide d'administration SMC.

Sauvegarde automatique

Depuis l'interface Web d'administration

1. Rendez-vous dans **Configuration > Système > Maintenance**, onglet **Sauvegarder**.
2. Dans le cadre **Sauvegarde automatique de configuration**, activez la sauvegarde automatique et complétez les informations. Vous pouvez protéger par un mot de passe le fichier de sauvegarde en complétant le champ **Mot de passe du fichier de sauvegarde**.
3. Appliquez la configuration.

La sauvegarde contient toutes les clés privées de certificats du firewall, et celles protégées par le TPM sont incluses chiffrées.

Depuis le serveur SMC

Le serveur SMC permet de sauvegarder automatiquement la configuration des firewalls SNS. **Lorsque le TPM est initialisé sur le firewall SNS, toutes les clés privées de certificats du firewall (protégés par le TPM ou non) sont exclues des sauvegardes automatiques.**

Pour plus d'informations, reportez-vous à la section Sauvegarder la configuration des firewalls du Guide d'administration SMC.

Tableau récapitulatif

Sauvegarde manuelle			Sauvegarde automatique	
Interface Web SNS	Console CLI	SMC (Script CLI)	Interface Web SNS	SMC
Toutes les privées sont incluses Celles protégées par le TPM sont déchiffrées	Toutes les clés privées sont incluses en renseignant le jeton *tpmpassword* Celles protégées par le TPM sont déchiffrées, sauf en renseignant le jeton *ondiskprotect=1*		Toutes les privées sont incluses Celles protégées par le TPM restent chiffrées	-

Restauration d'une sauvegarde de configuration

Une sauvegarde contenant des clés privées chiffrées de certificats protégées par le TPM ne peut être restaurée que sur le firewall source. Sur un autre firewall, les clés privées chiffrées ne pourront plus être déchiffrées car la clé symétrique sera différente.

Quelques exceptions existent dans les cas suivants :

- Lorsque le mécanisme de dérivation de la clé symétrique est activé et que le mot de passe du TPM est le même sur l'autre firewall,
- À la suite d'un échange de firewall (RMA) configuré en haute disponibilité. Pour plus d'informations, reportez-vous aux instructions de l'article Following an RMA, how can I synchronize the configuration and the content of the TPM? de la Base de connaissances Stormshield (anglais uniquement).

Procédure de configuration initiale par clé USB

Lors d'une configuration initiale d'un firewall par clé USB, des opérations permettent d'interagir avec le module TPM du firewall SNS :

- L'opération `inittpm` permet d'initialiser le module TPM. Son format est le suivant :
  ```
  "serial | any", inittpm, "tpmpassword"
  ```
  - Le mécanisme de dérivation de la clé symétrique est activé par défaut,
  - Cette opération doit être réalisée avant de protéger par le TPM une clé privée.
- L'opération `p12import` permet d'importer des fichiers PKCS#12 au format *.p12* et de protéger par le TPM la clé privée contenue dans le fichier. Son format est le suivant :
  ```
  "serial | any", p12import, none|ondisk, "p12file", "p12password"
  ```

Pour plus d'informations sur la mise en œuvre de cette procédure et sur les opérations possibles, reportez-vous à la note technique Configuration initiale par clé USB.

Calcul du facteur de qualité de la haute disponibilité (HA)

Ce cas concerne exclusivement les versions SNS 4.3 LTSB et SNS 4.7 et supérieures.

L'état du module TPM peut être pris en compte dans le calcul du facteur de qualité de la haute disponibilité (HA). Le jeton de configuration `TPMQualityIncluded=1` présent dans la section *[Global]* du fichier de configuration *ConfigFiles/HA/highavailability* indique que l'état du module TPM est pris en compte.

Pour plus d'informations sur le calcul du facteur de qualité de la haute disponibilité (HA), reportez-vous à la note technique Haute disponibilité sur SNS.

Résoudre les problèmes

Ce chapitre liste certains problèmes fréquemment rencontrés lors de l'utilisation du TPM. Si celui que vous rencontrez ne se trouve pas dans ce chapitre, nous vous recommandons de consulter la Base de connaissances Stormshield.

ASTUCE
Vous pouvez effectuer un diagnostic du TPM en exécutant dans une console SSH la commande : `tpmctl -a -v`. L'accès SSH doit être autorisé sur le firewall.

Certains modules ne sont plus opérationnels après la mise à jour logicielle d'un firewall

Situation : Après la mise à jour logicielle d'un firewall ou d'un cluster de firewalls en version SNS 4.3 LTSB ou supérieures, les modules utilisant un certificat dont la clé privée est protégée ne sont plus opérationnels (par exemple : les tunnels VPN ne s'établissent plus).

Cause : Des caractéristiques techniques du système ont été modifiées suite à la mise à jour du firewall. Ces nouvelles caractéristiques ne permettent plus aux registres PCR d'accéder au TPM. Il n'est donc plus possible de déchiffrer les clés privées protégées par le TPM.

Solution : Actualisez les valeurs des registres PCR.

1. Exécutez dans une console CLI la commande suivante :
```
SYSTEM TPM PCRSEAL tpmpassword=<password>
```
2. Si le firewall est membre d'un cluster en haute disponibilité, exécutez la commande suivante pour effectuer la manipulation sur le firewall passif :
```
SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive
```
Pour plus d'informations, reportez-vous à la section Mise à jour logicielle d'un cluster de la note technique *Haute disponibilité sur SNS*.

Certains modules ne sont plus opérationnels après avoir inséré un périphérique de stockage et redémarré le firewall

Situation : Après avoir inséré un périphérique de stockage et redémarré le firewall SNS, les modules utilisant un certificat dont la clé privée est protégée ne sont plus opérationnels (par exemple : les tunnels VPN ne s'établissent plus).

Cause : Des caractéristiques techniques du système ont été modifiées au démarrage du firewall car un nouveau périphérique de stockage a été détecté. Ces nouvelles caractéristiques ne permettent plus aux registres PCR d'accéder au TPM. Il n'est donc plus possible de déchiffrer les clés privées protégées par le TPM.

Solution : Actualisez les valeurs des registres PCR.

- Pour les versions SNS 4.3 LTSB et SNS 4.7 et supérieures :
  1. Exécutez dans une console CLI la commande suivante :
```
SYSTEM TPM PCRSEAL tpmpassword=<password>
```
  2. Si le firewall est membre d'un cluster en haute disponibilité, actualisez les valeurs des registres PCR du firewall passif en exécutant la commande suivante :
```
SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive
```

- Pour les versions SNS 3.11 LTSB, exécutez dans une console SSH la commande suivante :
  ```
  tpmctl -svp <tpmpassword>
  ```
  L'accès SSH doit être autorisé sur le firewall. Seul le compte *admin* peut effectuer cette action.

Certains modules ne sont plus opérationnels après la bascule d'un firewall passif en actif (haute disponibilité)

Situation : Après la bascule d'un firewall passif en actif, les modules utilisant un certificat dont la clé privée est protégée ne sont plus opérationnels (par exemple : les tunnels VPN ne s'établissent plus).

Cause 1 : Il n'est plus possible de déchiffrer les clés privées protégées par le TPM car le mécanisme de dérivation de la clé symétrique n'est pas activé sur le cluster de firewalls.

Solution 1 :

1. Vérifiez si le mécanisme de dérivation de la clé symétrique a été activé en exécutant la commande suivante :
   ```
   SYSTEM TPM STATUS tpmpassword=<password>
   ```
2. Activez le mécanisme de dérivation de la clé symétrique sur le cluster et renouvelez la clé symétrique en exécutant dans une console CLI les commandes suivantes :
   ```
   SYSTEM TPM RENEW tpmpassword=<password> derivekey=on
   HA TPMSYNC tpmpassword=<password>
   ```

Cause 2 : Il n'est plus possible de déchiffrer les clés privées protégées par le TPM car les deux firewalls du cluster ont été mis à jour dernièrement en version SNS 4.3 LTSB ou supérieure et les valeurs des registres PCR du firewall passif n'ont pas été actualisées.

Solution 2 : Actualisez les valeurs des registres PCR du nouveau firewall actif.

- Exécutez dans une console CLI la commande suivante :
  ```
  SYSTEM TPM PCRSEAL tpmpassword=<password>
  ```
  Pour plus d'informations, reportez-vous à la section Mise à jour logicielle d'un cluster de la note technique *Haute disponibilité sur SNS*.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions peuvent être disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu