

STORMSHIELD



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

Produits concernés : SNS 4.3.37 LTSB et 4.3 LTSB supérieures, SNS 4.8.7 et versions supérieures Dernière mise à jour du document : 10 juin 2025 Référence : sns-fr-TPM protection note technique



# Table des matières

Historique des modifications	4
Avant de commencer	6
Prérequis	7
Posséder un firewall SNS disposant d'un module TPM	7
Avoir active la fonctionnalite Secure Boot du firewall SNS Disposer d'un droit d'accès au module TPM	
Pouvoir accéder à la console CLI du firewall SNS	7
Fonctionnement	8
Liste des certificats dont la clé privée peut être protégée par le module TPM Mot de passe d'administration du module TPM Clé symétrique	8 8 9
Principe	9
Registres PCR	9
Principe Valeurs des empreintes des PCR et accès au module TPM	9 10
Cas nécessitant de sceller de nouveau le module TPM	10
Initialiser le module TPM d'un firewall SNS	11
Depuis l'interface Web d'administration	11
Versions SNS 4.8.7 et superieures Versions SNS 4.3.37 LTSB et 4.3 LTSB supérieures	11
Depuis la console CLI	13
Le module TPM n'est pas encore initialisé sur les deux firewalls du cluster	13
Le module TPM est déjà initialisé sur le futur firewall actif du cluster	13
Gérer le module TPM d'un firewall SNS	14
Vérifier l'état du module TPM Modifier le mot de passe d'administration du module du TPM	14
Sceller le module TPM	
Désactiver le module TPM	17
Gérer la protection de la clé privée des certificats d'un firewall SNS	18
Gerer la protection de la cle privee d'un certificat deja present Ajouter un certificat et protéger sa clé privée	18 19
Importer un certificat et protéger sa clé privée	19
Verifier si la cle privee d'un certificat est protegee Cas d'un parc de firewalls géré par un serveur SMC	20
Gérer la protection de la clé privée du certificat utilisé pour communiquer avec le serveur SMC	21
Gérer la protection de la clé privée des certificats du firewall SNS depuis le serveur SMC	22
Utiliser des certificats dont la clé privée est protégée par le module TPM	. 23
VPN SSL	23 24
VPN IPsec	24
	25





# **SNS - NOTE TECHNIQUE** STORMSHIELD CONFIGURER LE MODULE TPM ET PROTÉGER LES CLÉS PRIVÉES DE CERTIFICATS DU FIREWALL SNS

LDAP interne	25
Envois de logs vers un serveur Syslog TLS	26
Précisions sur les cas d'utilisation une fois le module TPM initialisé	28
Sauvegarde de configuration	28
Restauration d'une sauvegarde de configuration	28
Procédure de configuration initiale par clé USB	29
Calcul du facteur de qualité de la haute disponibilité (HA)	29
Résoudre les problèmes	30
Perte du mot de passe d'administration du module TPM	30
Accès à l'interface Web d'administration du firewall SNS et certificat de secours	30
Des fonctionnalités ne sont plus opérationnelles	31
Après la mise à jour logicielle du firewall SNS	31
Après avoir inséré un périphérique de stockage et redémarré le firewall SNS	31
Après la bascule du firewall passif en actif (haute disponibilité)	31
Pour aller plus loin	32
Annexe : points d'attention pour une mise à jour d'un firewall SNS avec le module TP	М
initialisé	33
Contexte	
Versions paliers à prendre en compte	
Recommandations à suivre pour mettre à jour un firewall SNS avec le module TPM	
initialisé	34



# Historique des modifications

Date	Description
10 juin 2025	<ul> <li>Ajout de précisions concernant la clé symétrique et les registres PCR dans la section "Fonctionnement"</li> </ul>
	<ul> <li>Ajout de précisions concernant le mécanisme de dérivation de la clé symétrique sur les versions SNS 4.3 LTSB dans les sections "Fonctionnement" et "Initialiser le module TPM d'un firewall SNS"</li> </ul>
	<ul> <li>Ajout de précisions concernant la suppression de la protection d'une clé privée et le cas d'un parc de firewalls SNS géré par un serveur SMC dans la section "Gérer la protection de la clé privée des certificats d'un firewall SNS"</li> </ul>
	<ul> <li>Ajout de précisions concernant l'utilisation d'un certificat dont la clé privée est protégée pour les services VPN du firewall SNS dans la section "Utiliser des certificats dont la clé privée est protégée par le module TPM"</li> </ul>
	<ul> <li>Ajout d'une nouvelle section "Annexe : points d'attention pour une mise à jour d'un firewall SNS avec le module TPM initialisé"</li> </ul>
6 mai 2025	<ul> <li>Ajout d'un nouveau prérequis concernant l'activation de la fonctionnalité Secure Boot dans la section "Prérequis"</li> </ul>
	<ul> <li>Ajout d'informations concernant le mot de passe d'administration du module TPM, la clé symétrique, les registres PCR et le scellement du module TPM dans la section "Fonctionnement"</li> </ul>
	<ul> <li>Le contenu lié à l'initialisation du module TPM a été mis à jour et dispose à présent de sa propre section distincte dans le document</li> </ul>
	<ul> <li>Ajout d'informations concernant la vérification de l'état du module TPM et le scellement du module TPM dans la section "Gérer le module TPM d'un firewall SNS"</li> </ul>
	<ul> <li>Précision ajoutée concernant la vérification de la protection d'une clé privée d'un certificat dans la section "Protéger les clés privées de certificats d'un firewall SNS"</li> </ul>
	<ul> <li>Ajout de précisions concernant l'utilisation d'un certificat de secours pour l'interface Web d'administration dans la section "Utiliser des certificats dont la clé privée est protégée par le module TPM"</li> </ul>
	<ul> <li>Ajout de précisions concernant le calcul du facteur de qualité de la haute disponibilité lorsque la fonctionnalité Secure Boot est activée dans la section "Précisions sur les cas d'utilisation une fois le module TPM initialisé"</li> </ul>
	Le contenu de la section "Résoudre les problèmes" a été enrichi
13 décembre 2024	<ul> <li>Ajout de précisions concernant l'initialisation du TPM dans le cas d'un cluster en haute disponibilité</li> </ul>





13 février 2024	<ul> <li>Ajout de précisions concernant les PCR dans la section "Protection de la clé privée des certificats du firewall grâce à la clé symétrique"</li> </ul>
	<ul> <li>Modification de la description de l'état du TPM en orange dans la section "Vérifier si le module TPM est initialisé"</li> </ul>
	<ul> <li>Ajout de précisions concernant la réinitialisation du TPM dans la section "Si vous avez oublié le mot de passe du TPM"</li> </ul>
	<ul> <li>Reformulation de l'explication du jeton force=on dans la section "Désactiver le module TPM"</li> </ul>
	<ul> <li>Modification de l'exemple &lt;<i>CN</i>&gt; par &lt;<i>CERTNAME</i>&gt; 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"</li> </ul>
	<ul> <li>Reformulation de l'information concernant l'autorité de certification dans la section "VPN SSL"</li> </ul>
	<ul> <li>Ajout d'une information importante concernant l'utilisation d'une clé privée protégée dans la section "Communications avec le serveur SMC"</li> </ul>
	<ul> <li>Ajout de précisions concernant la protection par mot de passe du fichier de sauvegarde dans la section "Sauvegarde de configuration"</li> </ul>
18 janvier 2024	Nouveau document



# Avant de commencer

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

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

Cette note technique présente :

- Des informations sur le fonctionnement du module TPM,
- L'initialisation et la configuration du module TPM d'un firewall SNS,
- La gestion de la protection de la clé privée des certificats d'un firewall SNS,
- L'utilisation dans la configuration d'un firewall SNS des certificats dont la clé privée est protégée,
- Des informations importantes dans le cas d'une mise à jour d'un firewall SNS avec le module TPM initialisé.

## 🚺 NOTE

Pour mettre à jour la version d'un module TPM d'un firewall SNS, reportez-vous à la note technique Mettre à jour la version du module TPM des firewalls SNS.





# Prérequis

Cette section présente les prérequis nécessaires pour initialiser et configurer le module TPM d'un firewall SNS.

# Posséder un firewall SNS disposant d'un module TPM

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

# Avoir activé la fonctionnalité Secure Boot du firewall SNS

Sur les versions SNS 4.8.7 et supérieures, l'intégrité du firewall SNS et de son module TPM est compromise si la fonctionnalité Secure Boot n'est pas activée. Il est recommandé de l'activer avant d'initialiser le module TPM ou de sceller de nouveau le module TPM. Notez qu'un avertissement s'affiche dans le **Tableau de bord** du firewall SNS si la fonctionnalité Secure Boot est désactivée et que le module TPM est initialisé.

Sur les versions SNS 4.3.37 LTSB et 4.3 LTSB supérieures, même si ce n'est pas obligatoire, il est recommandé d'activer la fonctionnalité Secure Boot sur le firewall SNS.

# 🚺 NOTE

La fonctionnalité Secure Boot est activée par défaut sur certains modèles de firewalls SNS. Pour plus d'informations sur les modèles concernés et sur l'activation de la fonctionnalité Secure Boot, reportez-vous à la note technique Gérer Secure Boot dans l'UEFI des firewalls SNS.

# Disposer d'un droit d'accès au module TPM

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

# Pouvoir accéder à la console CLI du firewall SNS

Si vous souhaitez effectuer des actions mentionnées dans cette note technique depuis la console CLI du firewall SNS, rendez-vous dans **Configuration > Système > Console CLI** depuis l'interface Web d'administration du firewall SNS. Pour plus d'informations, reportez-vous à la section **Console CLI** du *Manuel utilisateur SNS* v4.8 ou v4.3 LTSB selon la version utilisée.



# Fonctionnement

Cette section présente la liste des certificats dont la clé privée peut être protégée par le module TPM, le mot de passe d'administration du TPM, la clé symétrique et son mécanisme de dérivation, les registres PCR et l'importance de disposer d'un accès au module TPM.

# Liste des certificats dont la clé privée peut être protégée par le module TPM

La protection par le module TPM s'applique à certains certificats selon la version SNS installée.

Cartificata utiliada dana las ses suivents et dant la	Versions SNS compatibles			
clé privée peut être protégée par le module TPM	4.3.37 LTSB et versions 4.3 LTSB supérieures	4.8.7 et versions supérieures		
VPN IPsec	0	0		
VPN SSL	-	0		
Déchiffrement SSL/TLS (interface Web d'administration et portail captif)	-	0		
Communications avec le serveur SMC	-	0		
Envois de logs vers un serveur syslog	-	0		
LDAP interne	-	0		

# Mot de passe d'administration du module TPM

Vous devez définir un mot de passe d'administration du module TPM lors de son initialisation. Dans cette note technique, il est nommé "*mot de passe du TPM*".

Ce mot de passe vous sera demandé lors de certaines opérations de maintenance, lors de la modification du BIOS, après certaines mises à jour logicielles ou après un changement de la partition de démarrage du firewall SNS.

Concernant le mot de passe du TPM :

- Il doit respecter la politique de mots de passe définie sur le firewall SNS,
- Sur les versions SNS 4.8.7 et supérieures, il est recommandé de le générer aléatoirement avec une longueur d'au moins 64 caractères. Sur les versions SNS 4.3.37 LTSB et 4.3 LTSB supérieures, en raison d'une limitation, sa longueur ne doit pas excéder 32 caractères.
- Il doit être conservé dans un espace sécurisé et sauvegardé.

#### 🕒 IMPORTANT

En cas de perte du mot de passe du TPM, il n'est pas possible de le réinitialiser et Stormshield n'est pas en mesure de le retrouver. Ce cas est décrit dans la section Résoudre les problèmes.



# Clé symétrique

## **Principe**

Une clé symétrique est définie lors de l'initialisation du module TPM et est stockée sur ce dernier. Lorsqu'une clé privée d'un certificat est protégée par le module TPM, elle est chiffrée grâce à la clé symétrique.

#### Seule la clé symétrique permet de chiffrer et de déchiffrer la clé privée d'un certificat.

La clé symétrique est scellée dans le module TPM et son accès est strictement protégé par le mot de passe du TPM, ainsi que par une mesure fiable de l'état du système : les registres PCR (*Platform Configuration Registers*).

## Mécanisme de dérivation de la clé symétrique

Un mécanisme de dérivation de la clé symétrique (appelé *derivekey*) permet, lors de l'initialisation du module TPM d'un firewall SNS, de générer à partir du mot de passe du TPM la clé symétrique.

Dans le cas d'un cluster de firewalls en haute disponibilité, 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.

Pour assurer la continuité du service en cas de bascule des firewalls SNS du cluster, il est indispensable que la clé symétrique stockée sur le firewall actif soit identique à celle stockée sur le firewall passif. Lors de l'initialisation du module TPM des deux firewalls du cluster, le mécanisme de dérivation est automatiquement utilisé, ce qui permet de générer à partir du mot de passe du TPM la même clé symétrique. Ainsi, en cas de bascule, chaque firewall SNS est capable de déchiffrer les clés privées.

Ce mécanisme est également utile dans le cas d'un échange de firewall SNS (RMA) pour restaurer une sauvegarde de configuration contenant des clés privées protégées. Du fait que seule la clé symétrique permet de chiffrer et de déchiffrer les clés privées protégées, il est indispensable que la clé symétrique stockée sur le nouveau firewall soit identique à celle qui était stockée sur le firewall retourné.

# **Registres PCR**

#### **Principe**

Le scellement du module TPM par les registres PCR est basé sur une série d'empreintes. Leur valeur est définie par un ensemble de mesures prises lors du démarrage du firewall SNS :

- Version et options du BIOS,
- Binaires UEFI lancés (PCR 4),
- Table de partitions,
- Système d'exploitation,
- Modules matériels branchés (comme les modules réseaux et les périphériques USB),
- etc.





#### Valeurs des empreintes des PCR et accès au module TPM

Dans le cas où la valeur des empreintes des PCR change, l'accès au module TPM peut être refusé.

- Sur les versions SNS 4.8.7 et supérieures, l'accès au module TPM est refusé si la valeur des empreintes des PCR 0 à 3 et 5 à 7 change. L'empreinte du PCR 4 liée à la séquence de démarrage du firewall SNS n'est pas prise en compte dans la politique de scellement du module TPM. La fonctionnalité Secure Boot contrôle l'intégrité des binaires UEFI de cette séquence de démarrage.
- Sur les versions SNS 4.3.37 LTSB et 4.3 LTSB supérieures, l'accès au module TPM est refusé si la valeur des empreintes des PCR 0 à 7 change, ce qui inclut l'empreinte du PCR 4 liée à la séquence de démarrage du firewall SNS. Cette empreinte peut être modifiée après une mise à jour de version apportant des changements dans la séquence de démarrage du firewall SNS.

Lorsque l'accès au module TPM est refusé, la clé symétrique ne peut plus être récupérée et les clés privées protégées ne peuvent plus être déchiffrées sans saisir le mot de passe du TPM.

Pour rétablir l'accès au module TPM, vous devez au préalable vous assurer que le changement rencontré est légitime. Vous devez ensuite sceller de nouveau le module TPM pour actualiser la valeur des empreintes des PCR. Cette procédure est décrite dans la section Sceller le module TPM.

#### IMPORTANT

Si l'accès au module TPM est refusé, les fonctionnalités du firewall SNS qui utilisent des certificats dont la clé privée est protégée (VPN, administration par un serveur SMC, etc.) ne sont plus opérationnelles tant que l'accès au module TPM n'est pas rétabli. Ces blocages peuvent notamment survenir après la mise à jour d'un firewall SNS. Ce cas est décrit dans la section Annexe : points d'attention pour une mise à jour d'un firewall SNS avec le module TPM initialisé.

#### Cas nécessitant de sceller de nouveau le module TPM

Les cas suivants nécessitent de sceller de nouveau le module TPM :

- La politique de scellement du module TPM a été modifiée après une mise à jour de version. Dans ce cas, une information dans les Notes de version SNS est présente.
- Une option du BIOS a été modifiée, par exemple si la fonctionnalité Secure Boot du firewall SNS a été activée ou désactivée.
- Une opération de maintenance physique a été effectuée, par exemple si un périphérique USB a été branché ou débranché, ou si un module réseau a été changé.
- La partition de démarrage a été modifiée et que le firewall SNS a été démarré sur celle-ci. À noter que si la partition a été sélectionnée en mode console lors du choix interactif proposé au démarrage du firewall SNS, vous devrez sceller de nouveau le module TPM après un second redémarrage.





# Initialiser le module TPM d'un firewall SNS

Cette section explique comment initialiser le module TPM d'un firewall SNS ou les modules TPM d'un cluster de firewalls SNS en haute disponibilité.

# Depuis l'interface Web d'administration

La procédure d'initialisation est différente selon la version installée sur le firewall SNS.

## Versions SNS 4.8.7 et supérieures

- 1. Rendez-vous dans Configuration > Objets > Certificats et PKI.
- 2. Cliquez sur Init. TPM.

SOBJECTS / CERTIFICATES AND	) PKI		
🔍 Enter a filter 🛛 📽 Filter: all	-	🗚 🦨   🕂 Add 👻 X Revoke 🛛 Actions 👻   🖺 Download 👻	🛱 Init. TPM
In sslvpn-full-default-authority     In SSL proxy default authority	م م	Choose a certificate or filter the list using the search bar.	

 Si la fonctionnalité Secure Boot n'est pas activée, un avertissement s'affiche. Il est recommandé d'activer Secure Boot avant d'initialiser le module TPM, mais vous pouvez le faire plus tard.

# 🕒 IMPORTANT

Pour rappel, l'intégrité du firewall SNS et de son module TPM est compromise si la **fonctionnalité Secure Boot** n'est pas activée.

 Dans la fenêtre Définir le mot de passe, définissez le mot de passe d'administration du module TPM en respectant les recommandations de la section Mot de passe d'administration du module TPM, puis cliquez sur Continuer.

INITIALIZE TPM - SET F	ASSWORD (1/2)
The trusted platform certificates stored o <u>TPM and protect key</u> A Keep the TPM protect You will be aske modifying the B	n module (TPM) provides hardware storage allowing stronger protection of n the firewall. For more information, refer to the technical note: <u>Configure the</u> <u>(s on the firewall</u> . assword in a safe and protected location d to provide the TPM password for certain maintenance operations, when IOS after a firmware update or after a boot partition is changed. Without
modifying the B the TPM passwo Password (min. 64 chars recommended) Confirm password	IOS, after a firmware update, or after a boot partition is changed. Without rd, all private keys of protected certificates will be lost.
	Password strength
	- douring a druga
	X CANCEL





5. Sélectionnez les fonctionnalités pour lesquelles vous souhaitez protéger la clé privée du certificat utilisé. Les fonctionnalités qui n'utilisent pas de certificat dans leur configuration ne peuvent pas être sélectionnées. Vous pouvez également laisser toutes les cases décochées et protéger les clés privées de certificats du firewall SNS plus tard.

INITIALIZE TPM - OPTIONAL (2/2)				
Select the features for which the private keys of the certificates used will be protected:				
IPsec VPN				
SSL VPN				
SSL/TLS decryption on the captive portal web page				
Communication with SMC				
Syslog server				
□ Internal LDAP directory				
Disabled: features cannot be protected when no certificates are used in their configuration.				
× CANCEL ≪ PREVIOUS ✓ FINISH				

6. Cliquez sur Terminer.

Le module TPM est initialisé et le mécanisme de dérivation de la clé symétrique est utilisé pour générer la clé symétrique, que le firewall SNS soit membre d'un cluster en haute disponibilité ou non. Si le firewall SNS est membre d'un cluster en haute disponibilité, le module TPM du firewall passif est initialisé automatiquement.

# Versions SNS 4.3.37 LTSB et 4.3 LTSB supérieures

- 1. Rendez-vous dans Configuration > Objets > Certificats et PKI.
- 2. Dans la fenêtre d'initialisation du module TPM, définissez le mot de passe d'administration du module TPM en respectant les recommandations de la section Mot de passe d'administration du module TPM. Si la fenêtre ne s'affiche pas automatiquement, vérifiez si le module TPM n'est pas délà initialisé ou initialisez-le depuis la console CLI.

INITIALIZE TPM		
Specify a pass You will need t	word to initialize to enter this passv	the built-in TPM (Trusted Platform Module) on the firewall. word in order to manage the TPM and the keys that it protects.
Passphrase (8	chars min.):	
Confirm passv	vord:	
		Password strength
	× CANCEL	X DO NOT ASK ME AGAIN

3. Cliquez sur Appliquer.

Le module TPM est initialisé et le mécanisme de dérivation de la clé symétrique est utilisé pour générer la clé symétrique, que le firewall SNS soit membre d'un cluster en haute disponibilité ou non. Si le firewall SNS est membre d'un cluster en haute disponibilité, le module TPM du firewall passif est initialisé automatiquement.

Vous devez ensuite protéger les clés privées de certificats du firewall SNS.





# Depuis la console CLI

- 1. Initialisez le module TPM du firewall SNS avec la commande : SYSTEM TPM INIT tpmpassword=<password> derivekey=<on|off>
  - Remplacez <password> par le mot de passe d'administration du module TPM souhaité en respectant les recommandations de la section Mot de passe d'administration du module TPM,
  - Si le firewall SNS est membre d'un cluster en haute disponibilité, renseignez derivekey=on pour utiliser le mécanisme de dérivation de la clé symétrique.
- Si le firewall SNS est membre d'un cluster en haute disponibilité, initialisez le module TPM du firewall passif avec la commande :

HA TPMSYNC tpmpassword=<password>

Vous devez ensuite protéger les clés privées de certificats du firewall SNS.

# Cas d'un cluster de firewalls en haute disponibilité pas encore créé

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

- 1. Configurez le cluster (création du cluster et intégration du second firewall SNS).
- 2. Reportez-vous aux procédures ci-dessus pour initialiser le module TPM des firewalls SNS.

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

#### Versions SNS 4.8.7 et supérieures

- 1. Configurez le cluster (création du cluster et intégration du second firewall SNS).
- 2. Déconnectez-vous de l'interface Web d'administration du firewall SNS et reconnectez-vous.
- 3. Une fenêtre s'affiche automatiquement vous invitant à initialiser le module TPM du firewall passif. Renseignez le mot de passe du TPM dans le champ correspondant.
- 4. Cliquez sur **OK**.

#### Versions SNS 4.3.37 LTSB et 4.3 LTSB supérieures

- 1. Dans une console CLI, renouvelez la clé symétrique du firewall actif avec la commande : SYSTEM TPM RENEW tpmpassword=<password> derivekey=on
  - Remplacez <password> par le mot de passe du TPM,
  - Comme le firewall est membre d'un cluster en haute disponibilité, renseignez derivekey=on pour utiliser le mécanisme de dérivation de la clé symétrique.

Toutes les clés privées protégées par le module TPM sont déchiffrées puis de nouveau chiffrées avec la nouvelle clé symétrique générée à partir du mot de passe du TPM.

2. Initialisez le module TPM du firewall passif avec la commande : HA TPMSYNC tpmpassword=<password>





# Gérer le module TPM d'un firewall SNS

Cette section explique comment vérifier l'état du module TPM, modifier son mot de passe d'administration, le sceller, et comment le désactiver.

# Vérifier l'état du module TPM

#### **Depuis l'interface Web d'administration**

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

1. Rendez-vous dans Monitoring > Tableau de bord, widget Indicateurs de santé.

HEALTH INDICA	TORS				
	POWER	FAN	CPU	MEMORY	
RAID			трм	SD-WAN	

2. Vérifiez la couleur de l'icône de l'indicateur de santé "TPM" pour connaître son état.





# **Depuis la console CLI**

- 1. Affichez les informations de la supervision du module TPM avec la commande : MONITOR TPM
- 2. Vérifiez le résultat.

Jeton	Valeurs / Description
ondisk_init	<ul> <li>1 : le module TPM est initialisé,</li> <li>0 : le module TPM n'est pas initialisé.</li> </ul>
	<b>1 NOTE</b> Sur les versions SNS 4.3.37 LTSB et 4.3 LTSB supérieures, les autres jetons ci-dessous n'existent pas.
secure_boot_enabled	<ul> <li>1 : la fonctionnalité Secure Boot est activée,</li> <li>0 : la fonctionnalité Secure Boot est désactivée.</li> </ul>
ondisk_pkeys_present	<ul> <li>1 : le module TPM protège au moins une clé privée,</li> <li>0 : aucune clé privée n'est protégée par le module TPM.</li> </ul>
pcr_access_status	<ul> <li>Good : l'accès au module TPM est fonctionnel, aucune action nécessaire.</li> <li>Legacy : la politique de scellement du module TPM a été modifiée. Pour l'appliquer, vous devez sceller de nouveau le module TPM en suivant la procédure Sceller le module TPM. Un message confirme cet état.</li> <li>N0 : l'accès au module TPM n'est plus possible car la valeur des empreintes des PCR a été modifiée. Pour les actualiser, vous devez</li> </ul>
	sceller de nouveau le module TPM en suivant la procédure Sceller le module TPM. Un message confirme cet état.
message	Si nécessaire, précise des informations sur l'état du module TPM.

# Modifier le mot de passe d'administration du module du TPM

Dans une console CLI, modifiez le mot de passe d'administration du module du TPM avec la commande :

SYSTEM TPM CHANGE currentpassword=<password> newpassword=<new password>

- Remplacez <password> par l'actuel mot de passe du TPM, •
- Remplacez <new password> par le nouveau mot de passe du TPM en respectant les • recommandations de la section Mot de passe d'administration du module TPM.

Si vous avez oublié le mot de passe du TPM, reportez-vous à la section Résoudre les problèmes.

# Sceller le module TPM

Vous devez sceller le module TPM dans les cas suivants :

- L'accès au module TPM n'est plus possible,
- Une nouvelle politique de scellement du module TPM est disponible et vous souhaitez en bénéficier.





L'état du module TPM permet d'identifier si le module TPM doit être de nouveau scellé. Lorsque vous scellez le module TPM, la valeur des empreintes des PCR est recalculée.

#### **Depuis l'interface Web d'administration**

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

#### IMPORTANT

Pour rappel, l'intégrité du firewall SNS et de son module TPM est compromise si la fonctionnalité Secure Boot n'est pas activée. Il est recommandé de l'activer avant de sceller de nouveau le module TPM.

1. Connectez-vous à l'interface Web d'administration du firewall SNS. Une fenêtre s'affiche automatiquement si un scellement du module TPM est requis. Dans une configuration en haute disponibilité, une fenêtre s'affiche également si un scellement

du module TPM du firewall passif est requis. Si les deux membres du cluster sont concernés, deux fenêtres s'affichent l'une après l'autre.		
CONFIGURATION (1/1): TPM REHASH	×	

CONFIGURATION (1/1): TPM REHASH	×
The trusted platform module (TPM) provides hardware storage that increases the security of certificates stored on the firewall. The TPM password must be entered to update the TPM hash	
Enter the TPM administration password:	
TPM password	
The trusted platform module (TPM) provides hardware storage that increases the security of certificates stored on the firewall. The TPM password must be entered to update the TPM hash Enter the TPM administration password: TPM password K IGNORE V OK	

- 2. Renseignez le mot de passe du TPM dans le champ correspondant.
- 3. Cliquez sur OK.

#### Depuis la console CLI

1. Scellez le module TPM du firewall SNS avec la commande : SYSTEM TPM PCRSEAL tpmpassword=<password>

Remplacez <password> par le mot de passe du TPM.

2. Si le firewall SNS est membre d'un cluster en haute disponibilité, scellez le module TPM du firewall passif avec la commande :

#### SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive

#### Depuis la console SSH

L'accès SSH doit être autorisé sur le firewall. Seul le compte admin peut effectuer cette action.

Scellez le module TPM du firewall SNS avec la commande :

tpmctl -svp <tpmpassword>

Remplacez <password> par le mot de passe du TPM.



# Désactiver le module TPM

Dans une console CLI, désactivez le module TPM avec la commande :

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 module TPM et que vous souhaitez tout de même forcer sa désactivation. Les clés privées protégées seront alors déchiffrées.





# Gérer la protection de la clé privée des certificats d'un firewall SNS

Cette section explique comment protéger la clé privée des certificats d'un firewall SNS par le module TPM, comment vérifier si une clé privée est protégée et comment supprimer cette protection si nécessaire.

# Gérer la protection de la clé privée d'un certificat déjà présent

#### Depuis l'interface Web d'administration

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

- 1. Rendez-vous dans Configuration > Objets > Certificats et PKI.
- 2. Sélectionnez le certificat (identité) concerné.
- 3. Pour protéger la clé privée du certificat, cliquez sur **Actions > Protéger avec le TPM**. Pour supprimer sa protection, reportez-vous à la section **Depuis la console CLI**.
- 4. Cliquez sur **OK**.



#### Depuis la console CLI

- 1. Affichez les autorités de certification avec la commande :
  - PKI CA LIST

Si besoin, vous pouvez afficher la liste des autorités de certification intermédiaires signées par l'autorité racine concernée en ajoutant CANAME=<RootCA> à la commande.

- 2. Affichez les certificats issus de l'autorité de certification (<CA>) avec la commande : PKI CERT LIST CANAME=<CA>
- 3. Selon l'action que vous souhaitez effectuer sur le certificat (<CERTNAME>) concerné :
  - Pour protéger sa clé privée, exécutez la commande : PKI CERT PROTECT CANAME=<CA> NAME=<CERTNAME> tpm=ondisk
  - Pour supprimer sa protection, exécutez la commande : PKI CERT PROTECT CANAME=<CA> NAME=<CERTNAME> tpm=none tpmpassword=<password>

Remplacez <password> par le mot de passe du TPM.

4. Activez la nouvelle configuration avec la commande : PKI ACTIVATE





# Ajouter un certificat et protéger sa clé privée

Depuis l'interface Web d'administration

- 1. Rendez-vous dans Configuration > Objets > Certificats et PKI.
- 2. Cliquez sur Ajouter et sélectionnez le certificat (identité) concerné.
- 3. Complétez les informations demandées. Cochez la case **Protéger cette identité à l'aide du TPM** pendant les étapes.
- 4. Cliquez sur Terminer.

Pour plus d'informations, reportez-vous à la section **Certificats et PKI** du *Manuel utilisateur SNS* v4.8 ou v4.3 LTSB selon la version utilisée.

CREATE A SERVER IDENTITY			
IDENTITY OPTIONS - CREATION WIZAR	D		
Validity (days)	365	÷	
Key type	SECP	-	
Key size (bits)	256	-	
Protect this identity with the TPM	1		
	× CANCEL	≪ PREVIOUS	» NEXT

#### Depuis la console CLI

- 1. Ajoutez un nouveau certificat avec la commande : PKI CERT CREATE Utilisez le jeton tpm=ondisk pour protéger la clé privée du certificat. Si besoin, affichez l'aide de la commande avec : PKI CERT CREATE HELP
- 2. Activez la nouvelle configuration avec la commande : PKI ACTIVATE

# Importer un certificat et protéger sa clé privée

#### **Depuis l'interface Web d'administration**

- 1. Rendez-vous dans Configuration > Objets > Certificats et PKI.
- 2. Cliquez sur Ajouter > Importer un fichier.
- 3. Complétez les informations demandées. Cochez la case **Protéger cette identité à l'aide du TPM** pendant les étapes.
- 4. Cliquez sur Terminer.





Pour plus d'informations, reportez-vous à la section **Certificats et PKI** du *Manuel utilisateur SNS* v4.8 ou v4.3 LTSB selon la version utilisée.

IMPORT FILE			
File to import:			
File format:	P12		•
File password:			
What to import:	All		*
Overwrite existing conten	nt: 🗆		
Protect this identity with TPM:	the 🗹		
	× CANCEL	✓ IMPORT	

#### **Depuis la console CLI**

1. Importez un certificat avec la commande :

```
PKI IMPORT type=<req|cert|pkey|crl|ca|all> format=<p12|pem|der>
password=<pass> force=<0|1> tpm=ondisk < /tmp/monfichier.p12</pre>
```

- · Personnalisez les jetons de configuration,
- Dans l'exemple ci-dessus, le fichier *monfichier.p12*, préalablement téléversé sur le firewall SNS dans le répertoire /tpm/, sera importé.

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

PKI IMPORT HELP

2. Activez la nouvelle configuration avec la commande : PKI ACTIVATE

# Vérifier si la clé privée d'un certificat est protégée

#### **Depuis l'interface Web d'administration**

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

Rendez-vous dans Configuration > Objets > Certificats et PKI.

 L'icône A indique que la clé privée du certificat est protégée par le module TPM. Cette information est également disponible dans l'onglet Détails du certificat ou dans l'info-bulle qui s'affiche en survolant le certificat.

OBJECTS / CERTIFIC	ATES AND PKI			
<b>Q</b> Enter a filter	* Filter: all	* x <sup>2</sup> x <sup>3</sup>	+ Add - × Re	voke 🗮 Actions 🔹   📮 Download 🔹
🗄 🗈 sslvpn-full-default-author	ity 👂	DETAILO	REVOCATION (CRI.)	
🕀 🖪 Stormshield	P	DETAILS	REVOCATION (CRL)	CERTIFICATE PROFILES
🗆 🗇 Doc Stormshield	P	Usage		
bapt.dub	14			
b doc.stormshield.eu	🗱 P	Usage:		This certificate is not yet in use
b doc.preprod.stormshi	eld.eu 👂	This portifie	ate is protected by the T	DM
SSL proxy default author	ity 👂	This certific	cate is protected by the Ti	





 L'icône O indique que le certificat est utilisé dans la configuration du firewall SNS mais sa clé privée n'est pas protégée par le module TPM. Cette information est également disponible dans l'info-bulle qui s'affiche en survolant le certificat.

👔 🙆 nternal.st	ormshield.eu		۶	Issued
SSL proxy default	authority		٩	
	Name	h internal.stormshield	d.eu	
		_		
	Usage	Directories configuratio	n	
	Warning	this certificate's private	key is not TPM-protected	
	Statue	This certificate is not p	rotected by the TDM	
	Status	rins certificate is not p	rotected by the TFM	

#### Depuis la console CLI

- Pour vérifier les certificats actuellement utilisés dans la configuration du firewall SNS, exécutez la commande :
  - MONITOR CERT

Dans le résultat, tpm=Used indique que la clé privée est protégée par le module TPM.

• Pour vérifier un certificat en particulier, exécutez la commande : PKI CERT SHOW CANAME=<CA> NAME=<CERTNAME>

Dans le résultat, tpm=ondisk indique que la clé privée est protégée par le module TPM.

- Pour vérifier les certificats d'une autorité de certification du firewall SNS :
  - 1. Affichez les autorités de certification avec la commande :
    - PKI CA LIST

Si besoin, vous pouvez afficher la liste des autorités de certification intermédiaires signées par l'autorité racine concernée en ajoutant CANAME=<RootCA> à la commande.

2. Affichez les certificats issus de l'autorité de certification (<CA>) avec la commande : PKI CERT LIST CANAME=<CA>

Dans le résultat, tpm=ondisk indique que la clé privée est protégée par le module TPM.

# Cas d'un parc de firewalls géré par un serveur SMC

# Gérer la protection de la clé privée du certificat utilisé pour communiquer avec le serveur SMC

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

- 1. Rendez-vous dans Configuration > Système > Management Center.
- Dans le cadre TPM, pour protéger la clé privée du certificat utilisé pour communiquer avec le serveur SMC, cliquez sur Protéger l'agent SMC. Pour supprimer sa protection, cliquez sur Déprotéger l'agent SMC.
- 3. Confirmez la modification.

# IMPORTANT

Si la clé privée du certificat utilisé pour communiquer avec le serveur SMC est protégée et que l'accès au module TPM est refusé dans le futur, les communications avec le serveur SMC ne seront plus possibles tant que le module TPM n'aura pas été de nouveau scellé. Pendant ce laps de temps, il ne sera plus possible d'administrer le firewall SNS via le serveur SMC.





<ul> <li>Connection settings</li> </ul>		
Connection:	Connected	
connection.	Connected	
IPv4 address and port:	1000000000	
<ul> <li>Advanced properties</li> </ul>		
TPM		
Protecting the SMC agent:	The agent is not protected by the TPM	
	Protect the SMC agent	
	· · · · · · · · · · · · · · · · · · ·	

Vous pouvez également réaliser ces opérations depuis la console CLI avec ces commandes :

- Pour protéger la clé privée du certificat : CONFIG FWADMIN PROTECT tpm=ondisk
- Pour supprimer la protection de la clé privée du certificat : CONFIG FWADMIN PROTECT tpm=none tpmpassword=<password>

Remplacez <password> par le mot de passe du TPM du firewall SNS.

Vous pouvez exécuter ces commandes sur un parc de firewalls SNS depuis le serveur SMC. Pour plus d'informations, reportez-vous à la section Exécuter des commandes CLI SNS sur un parc de firewalls du *Guide d'administration SMC*.

#### Gérer la protection de la clé privée des certificats du firewall SNS depuis le serveur SMC

Pour plus d'informations sur la protection de la clé privée des certificats du firewall SNS depuis le serveur SMC, reportez-vous aux sections suivantes du *Guide d'administration SMC* :

- Activer la protection par TPM d'une clé privée déjà existante,
- Importer ou déclarer un certificat pour un firewall,
- Savoir si une clé privée est protégée par TPM.

# 🚺 NOTE

Lorsque le module TPM est initialisé, la clé privée des certificats déclarés sur le firewall SNS par le serveur SMC est par défaut protégée par le module TPM. Pour modifier ce comportement, reportez-vous à la section Désactiver la protection de la clé privée par TPM du *Guide d'administration SMC*.

Page 22/35



sns-fr-TPM\_protection\_note\_technique - 10/06/2025



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

Cette section explique comment utiliser dans la configuration d'un firewall SNS des certificats dont la clé privée est protégée par le module TPM.

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

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

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

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 鄰 indique les certificats dont la clé privée est protégée par le module TPM.
- Appliquez la modification.
   La connexion à l'interface Web d'administration est perdue. En retournant sur la page d'authentification, un avertissement peut s'afficher. Vous pouvez continuer vers le site.

# 🚺 NOTE

Un certificat de secours est utilisé pour maintenir l'accès à l'interface Web d'administration si la clé privée du certificat sélectionné est protégée et que l'accès au module TPM est refusé.

- Sur les versions SNS 4.8.7 et 4.8.x supérieures en configuration d'usine, il s'agit d'un certificat correspondant au numéro de série du firewall SNS.
- Sur les versions 5 en configuration d'usine, il s'agit d'un certificat auto-généré pour cet accès.

USERS / AUTHENTIC	ATION						
AVAILABLE METHODS AUTHENTICATION POLICY CAPTIVE PORTAL CAPTIVE PORTAL PROFILES Captive portal AUTHENTICATION PROFILE AND INTERFACE MATCH + Add × Delete							
Captive portal							
AUTHENTICATION PROFILE AND INTERFACE MATCH							
+ Add × Delete							
Interface	Profile	Default method or directory					
m out	e openypnserver		۶				
in in	www.stormshield.eu		P				
	doc.stormshield.eu		۶				
	b doc.preprod.stormshie	ld.eu	P				
SSL server	b Doc Stormshield Interr	al FW	<b>1</b>				
Certificate (private key):	Select a certificate			<b>▼</b> ×			



# **VPN SSL**

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

La clé privée du certificat présenté par le service VPN SSL du firewall SNS peut être protégée par le module TPM.

# 🕒 IMPORTANT

Si la clé privée du certificat sélectionné est protégée et que l'accès au module TPM est refusé dans le futur, vous ne pourrez plus établir de tunnels VPN SSL avec le firewall SNS tant que le module TPM n'aura pas été de nouveau scellé.

Pour vérifier / modifier le certificat utilisé :

- Rendez-vous dans Configuration > VPN > VPN SSL, zone Configuration avancée, cadre Certificats.
- Dans le champ Certificat serveur, sélectionnez le certificat souhaité. L'icône indique les certificats dont la clé privée est protégée par le module TPM. Le certificat sélectionné doit être issu de la même autorité de certification que celle du certificat client.
- 3. Dans le champ **Certificat client**, vous ne pouvez pas sélectionner un certificat dont la clé privée est protégée par le module TPM. En effet, la clé privée de ce certificat doit être disponible en clair (non chiffrée) dans la configuration VPN distribuée aux clients VPN.
- 4. Appliquez la modification.

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 importer de nouveau la configuration VPN (fichier *.ovpn*). Pour plus d'informations, reportez-vous à la note technique Configurer et utiliser le VPN SSL des firewalls SNS.

Used certificates				
Server certificate:	openvpnserver		-	×
Client certificate:	b openvpnserver	٩	-	×
	www.stormshield.eu	P		
	doc.stormshield.eu	P		
Configuration	Doc Stormshield Internal FW	10 P		
	VPN_Server	1 P		

# **VPN IPsec**

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

# 🕕 IMPORTANT

Si la clé privée du certificat sélectionné est protégée et que l'accès au module TPM est refusé dans le futur, vous ne pourrez plus établir de tunnels VPN IPsec avec le firewall SNS tant que le module TPM n'aura pas été de nouveau scellé.

Pour vérifier / modifier le certificat utilisé :

- 1. Rendez-vous dans Configuration > VPN > VPN IPsec, onglet Correspondants.
- 2. Sélectionnez dans la grille le correspondant utilisé dans la configuration VPN.



Dans le cadre Identification, champ Certificat, sélectionnez le certificat souhaité. L'icône indique les certificats dont la clé privée est protégée par le module TPM.



4. Appliquez la modification.

ENCRYPTION POLICY - TUNNELS PEERS	IDENTIFICATION	ENCRYPTION PROFILES	
O Local			
Q Enter a filter     + Add → ≡ Actions	• SITE_TEST		
Remote gateways (1) Site test	- General -		
	Comment	t internet	
	Remote g	ateway: 🗈 SSL proxy default authority	▼ 5.
	Local add	Iress:	-
	IKE profile	e: El Stormshield	-
	IKE versio	Doc Stormshield	-
	INE VEISIO	🚯 bapt.dub 🏥 👂	
		🕼 doc.stormshield.eu 🖉	
	Identificat	tion 🕼 Doc Stormshield Internal FW 🛛 🗱 👂	
		🚯 VPN_Server 🗱 👂	
	Authentic	ation method: VPN_Client P	•
	Certificate	e: Doc Stormshield:VPN_Server	* X

# **Communications avec le serveur SMC**

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

La clé privée du certificat utilisé pour communiquer avec le serveur SMC peut être protégée par le module TPM.

#### 🕕 IMPORTANT

Pour rappel, si la clé privée du certificat utilisé pour communiquer avec le serveur SMC est protégée et que l'accès au module TPM est refusé dans le futur, les communications avec le serveur SMC ne seront plus possibles tant que le module TPM n'aura pas été de nouveau scellé.

Pour plus d'informations, reportez-vous à la section Cas d'un parc de firewalls géré par un serveur SMC.

#### LDAP interne

Ce cas concerne exclusivement les versions SNS 4.8.7 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.





- 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.

LUSERS / DIRECTORIES CONFIGURA	TION				
CONFIGURED DIRECTORIES (MAXIMUM 5)					
+ Add a directory $\equiv$ Action •	Configuration				
Domain name	oomgalaton				
E stormshield.com	Enable user directory				
	Organization:	stormshield			
	Domain:	com			
	ID:	cn=NetasqAdmin			
	Password:				
	Confirm:				
		Password strength			
		b openvpnserver		8	
		www.stormshield.eu		8	
	Access to the Internal LDAP	doc.stormshield.eu		٩	
	Enable unencrypted acc	Doc Stormshield Internal FW	4	٩	
		VPN_Server		۶	
	Enable SSL access	b LDAPS Doc Stormshield		P	
	SSL certificate issued by the server:	LDAPS Doc Stormshield 💌 🗙		_	

# Envois de logs vers un serveur Syslog TLS

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

La clé privée du certificat présenté par le firewall SNS pour s'authentifier auprès du serveur Syslog peut être protégée par le module TPM.

Pour vérifier / modifier le certificat utilisé :

- 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. Les détails du profil s'affichent à droite.
- Dans le champ Autorité de certification, sélectionnez l'autorité de certification (CA) ayant signé les certificats que présenteront le firewall SNS et le serveur Syslog pour s'authentifier mutuellement.
- 4. Dans le champ **Certificat serveur**, sélectionnez le certificat que doit présenter le serveur Syslog pour s'authentifier auprès du firewall SNS. Vous ne pouvez pas sélectionner un certificat dont la clé privée est protégée par le module TPM.
- Dans le champ Certificat client, sélectionnez le certificat que doit présenter le firewall SNS pour s'authentifier auprès du serveur Syslog. L'icône indique les certificats dont la clé privée est protégée par le TPM.
- 6. Appliquez la modification.
- 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.







LOCAL STOR	AGE SYSLOG	IPFIX					
SYSLOG PROF	ILES		Details				
Status	Name						
C Enabled	Syslog Server		Name:	Syslog Server			
CD Disabled	Syslog Profile 1		Comments:				
CD Disabled	Syslog Profile 2		Syslog server:	syslog-tis-server	-	5	
C Disabled	Syslog Profile 3		Protocol:	TLS		-	
			Port:	syslog-tis	Ŧ	8+	
			Certification authority:	Doc Stormshield	Ŧ	×	
			Server certificate:	Syslog TLS Doc Server	-	×	
			Client certificate:	Syslog Doc Client		×	
			Format:	openvpnclient			٦
			Advanced properties	VPN_Client			P
			- • Auvanced properties	Syslog Doc Client			4 P



sns-fr-TPM\_protection\_note\_technique - 10/06/2025



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

Cette section apporte des précisions sur la sauvegarde et la restauration d'une configuration, sur la procédure de configuration initiale par clé USB et sur le calcul du facteur de qualité de la haute disponibilité, une fois le module TPM initialisé.

# Sauvegarde de configuration

Vous pouvez sauvegarder manuellement ou automatiquement la configuration du firewall SNS depuis l'interface Web d'administration, la console CLI ou depuis le serveur SMC.

Selon la méthode utilisée, des spécificités existent concernant la présence des clés privées protégées dans le fichier de sauvegarde, ainsi que sur leur état de chiffrement.

Sauvegarde manuelle			Sauvegarde automatique	
Interface SNS	Console CLI SNS	SMC (Script CLI)	Interface SNS	Interface SMC
Clés privées incluses (protégées par le module TPM ou non)				😢 Clés privées exclues
Les clés privées protégées sont déchiffrées	Les clés privées protégées sont déchiffrées Il est possible de les conserver chiffrées avec le jeton <i>ondiskprotect=1</i>		Les clés privées protégées restent chiffrées	N/A

Pour plus d'informations sur la réalisation d'une sauvegarde de configuration, reportez-vous :

- Pour l'interface Web d'administration du firewall SNS, à la section Maintenance > Onglet Sauvegarder du Manuel utilisateur SNS v4.8 ou v4.3 LTSB selon la version utilisée.
- Pour la console CLI du firewall SNS, à l'aide de la commande CONFIG BACKUP : CONFIG BACKUP HELP
- Pour le serveur SMC, à la section Sauvegarder la configuration des firewalls du Guide d'administration SMC.

#### \rm Important

Le serveur SMC permet de sauvegarder automatiquement la configuration des firewalls SNS. Lorsque le module TPM est initialisé, <u>toutes</u> les clés privées de certificats, protégées par le module TPM ou non, sont <u>exclues</u> des sauvegardes automatiques.

#### Restauration d'une sauvegarde de configuration

Une sauvegarde contenant des clés privées chiffrées ne peut être restaurée **<u>que</u>** sur le firewall d'origine. Sur un autre firewall SNS, les clés privées chiffrées ne peuvent pas être déchiffrées car la clé symétrique est supposément différente.

Quelques exceptions existent dans les cas suivants :

• Si le mécanisme de dérivation de la clé symétrique a été utilisé pour générer la clé symétrique à partir du mot de passe du TPM, et que ce dernier est le même sur les deux firewalls SNS. Dans ce cas, la clé symétrique est la même sur les deux firewalls SNS.





• 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 (authentification nécessaire - anglais uniquement).

# Procédure de configuration initiale par clé USB

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

- L'opération initTPM permet d'initialiser le module TPM du firewall SNS. Si le firewall SNS est membre d'un cluster en haute disponibilité, le mécanisme de dérivation de la clé symétrique est automatiquement utilisé.
- L'opération p12import permet d'importer des fichiers PKCS#12 au format .p12 et de protéger par le module TPM la clé privée contenue dans le fichier. L'opération initTPM doit être réalisée avant l'opération p12import.

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)

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.

Sur les versions SNS 4.8.7 et supérieures, l'état du module TPM n'est pas pris en compte dans le calcul du facteur de qualité de la haute disponibilité si la fonctionnalité Secure Boot est désactivée.

#### IMPORTANT

Pour rappel, l'intégrité du firewall SNS et de son module TPM est compromise si la fonctionnalité Secure Boot n'est pas activée.

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.

Page 29/35



sns-fr-TPM protection note technique - 10/06/2025



# Résoudre les problèmes

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

## 💡 astuce

Pour effectuer un diagnostic du module TPM, exécutez dans une console SSH cette commande : tpmctl -a -v

L'accès SSH doit être autorisé sur le firewall SNS.

## Perte du mot de passe d'administration du module TPM

Situation : Le mot de passe du TPM est requis pour réaliser une opération, mais il a été perdu.

Cause : Le mot de passe n'a pas été conservé ni sauvegardé dans un endroit sécurisé.

*Solution* : Il n'est pas possible de réinitialiser le mot de passe du TPM, et Stormshield n'est pas en mesure de le retrouver.

En dernier recours, si vous ne le retrouvez pas, vous pouvez réinitialiser le module TPM en vous reportant aux instructions de l'article l have lost my TPM password, how can l reset it? de la Base de connaissances Stormshield (authentification nécessaire - anglais uniquement).

#### IMPORTANT

Réinitialiser le module TPM <u>ne permet pas</u> de retrouver l'usage des clés privées qu'il protège. Vous devrez importer de nouveau les certificats concernés et protéger leur clé privée.

# Accès à l'interface Web d'administration du firewall SNS et certificat de secours

*Situation* : L'accès à l'interface Web d'administration est toujours possible sur un firewall SNS en version 4.8.7 ou supérieure dont la clé privée du certificat présenté par l'interface Web d'administration est protégée par le module TPM, alors que l'état du module TPM indique qu'il doit être scellé de nouveau.

*Cause* : Des caractéristiques techniques du système ont été modifiées. L'accès au module TPM n'est alors plus possible car la valeur des empreintes des PCR a été modifiée, ce qui rend impossible le déchiffrement de la clé privée protégée du certificat présenté par l'interface Web d'administration.

Cependant, un certificat de secours est utilisé pour maintenir l'accès à l'interface Web d'administration :

- Sur les versions SNS 4.8.7 et 4.8.x supérieures, il s'agit du certificat par défaut en configuration d'usine, correspondant au numéro de série du firewall SNS,
- Sur les versions SNS 5 en configuration d'usine, il s'agit d'un certificat auto-généré pour cet accès.

*Solution* : Même si l'accès à l'interface Web d'administration est toujours possible grâce au certificat de secours, toutes les clés privées protégées par le module TPM ne peuvent plus être déchiffrées. Pour résoudre ce problème, vérifiez d'abord que le changement des caractéristiques techniques est légitime, puis scellez le module TPM en suivant la procédure **Sceller le module TPM**.





sns-fr-TPM\_protection\_note\_technique - 10/06/2025



# Des fonctionnalités ne sont plus opérationnelles

#### Après la mise à jour logicielle du firewall SNS

*Situation* : Après la mise à jour logicielle d'un firewall SNS ou d'un cluster de firewalls SNS en version 4.3 LTSB ou supérieure, les fonctionnalités utilisant un certificat dont la clé privée est protégée ne sont plus opérationnelles.

*Cause* : Des caractéristiques techniques du système ont été modifiées à la suite de la mise à jour du firewall SNS. L'accès au module TPM n'est alors plus possible car la valeur des empreintes des PCR a été modifiée, ce qui rend impossible le déchiffrement des clés privées protégées. L'état du module TPM indique qu'il doit être scellé de nouveau.

Solution : Scellez le module TPM en suivant la procédure Sceller le module TPM.

#### Après avoir inséré un périphérique de stockage et redémarré le firewall SNS

*Situation* : Après avoir inséré un périphérique de stockage et redémarré le firewall SNS, les fonctionnalités utilisant un certificat dont la clé privée est protégée ne sont plus opérationnelles.

*Cause* : Des caractéristiques techniques du système ont été modifiées au démarrage du firewall SNS car un nouveau périphérique de stockage a été détecté. L'accès au module TPM n'est alors plus possible car la valeur des empreintes des PCR a été modifiée, ce qui rend impossible le déchiffrement des clés privées protégées. L'état du module TPM indique qu'il doit être scellé de nouveau.

*Solution* : Si la présence du périphérique de stockage est légitime, scellez le module TPM en suivant la procédure Sceller le module TPM.

#### Après la bascule du firewall passif en actif (haute disponibilité)

*Situation* : Après la bascule d'un firewall passif en actif, les fonctionnalités utilisant un certificat dont la clé privée est protégée ne sont plus opérationnelles.

 Cause 1 : Le mécanisme de dérivation de la clé symétrique n'a pas été activé sur le cluster de firewalls SNS. Vous pouvez le vérifier en exécutant cette commande CLI : SYSTEM TPM STATUS tpmpassword=<password>

*Solution* : Activez le mécanisme de dérivation de la clé symétrique sur le cluster et renouvelez la clé symétrique en exécutant les commandes CLI suivantes :

SYSTEM TPM RENEW tpmpassword=<password> derivekey=on

HA TPMSYNC tpmpassword=<password>

- Remplacez <password> par le mot de passe du TPM,
- Comme le firewall est membre d'un cluster en haute disponibilité, renseignez derivekey=on.
- Cause 2 : Les deux firewalls SNS du cluster ont été mis à jour dernièrement en version SNS 4.3 LTSB ou supérieure. Après la bascule, l'accès au module TPM n'est alors plus possible car la valeur des empreintes des PCR a été modifiée, ce qui rend impossible le déchiffrement des clés privées protégées. L'état du module TPM indique qu'il doit être scellé de nouveau.

Solution : Scellez le module TPM en suivant la procédure Sceller le module TPM.





# Pour aller plus loin

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

Pour mettre à jour la version d'un module TPM d'un firewall SNS, reportez-vous à la note technique Mettre à jour la version du module TPM des firewalls SNS.





sns-fr-TPM\_protection\_note\_technique - 10/06/2025



# Annexe : points d'attention pour une mise à jour d'un firewall SNS avec le module TPM initialisé

Cette section présente des informations importantes sur la mise à jour d'un firewall SNS avec le module TPM initialisé.

## Contexte

Si une information dans les *Notes de version SNS* indique que le module TPM devra être scellé de nouveau à l'issue d'une mise à jour, il est fortement recommandé de prendre connaissance des informations de cette section avant de mettre à jour le firewall SNS.

Selon les modifications apportées à la nouvelle version SNS, la valeur des empreintes des PCR peut changer à l'issue de la mise à jour, et l'accès au module TPM peut alors être refusé.

Si l'accès au module TPM est refusé, les fonctionnalités du firewall SNS qui utilisent des certificats dont la clé privée est protégée ne seront plus opérationnelles à l'issue de la mise à jour, et cela tant que l'accès au module TPM ne sera pas rétabli. Par exemple, vous pourriez ne plus pouvoir établir de tunnels VPN avec le firewall SNS ou ne plus pouvoir administrer ce dernier via un serveur SMC.

Pour plus d'informations sur les registres PCR et l'accès au module TPM, reportez-vous à la section **Registres PCR**.

## Versions paliers à prendre en compte

Ce tableau résume les versions paliers à prendre en compte dans le cas d'une **mise à jour vers une version 4.8 ou supérieure depuis la dernière version 4.3 LTSB disponible**. En cas de saut de version, le contenu des versions intermédiaires s'applique.

Version	Description			
4.8.0	Accès au module TPM refusé. Vous devez sceller de nouveau le module TPM.			
4.8.3	Accès au module TPM refusé. Vous devez sceller de nouveau le module TPM.			
4.8.7	A Si la clé privée des certificats utilisés pour les services VPN SSL et lPsec est protégée, vous devez sceller de nouveau le module TPM. Ce problème a été corrigé en version 4.8.9.			
	40 Accès au module TPM toujours possible, mais sa politique de scellement est modifiée.			
	<ul> <li>Vous devez sceller de nouveau le module TPM pour bénéficier de la nouvelle politique de scellement. En vous connectant à l'interface Web d'administration du firewall SNS, une fenêtre vous invite à le faire.</li> </ul>			
	<ul> <li>Avec la nouvelle politique de scellement, l'intégrité du firewall SNS et de son module TPM est compromise si la fonctionnalité Secure Boot n'est pas activée. Il est recommandé de l'activer avant de sceller de nouveau le module TPM.</li> </ul>			
À partir de la version 4.8.9	<ul> <li>Mise à jour bloquée si ces trois conditions sont remplies :</li> <li>Le firewall SNS est administré par un serveur SMC,</li> </ul>			
	<ul> <li>La clé privée du certificat utilisé pour communiquer avec le serveur SMC est protégée,</li> <li>La politique de scellement du module TPM sera modifiée à l'issue de la mise à jour.</li> </ul>			



# Recommandations à suivre pour mettre à jour un firewall SNS avec le module TPM initialisé

- 1. Si vous n'êtes pas sûr que le module TPM est initialisé sur votre firewall SNS, vérifiez-le en vous reportant à la section Vérifier l'état du module TPM.
- 2. Vérifiez si la version que vous souhaitez installer nécessite de sceller de nouveau le module TPM. Pour cela, reportez-vous à la section ci-dessus *Versions paliers à prendre en compte* et aux informations des *Notes de version SNS*.
- 3. Si le module TPM est initialisé et qu'il nécessite d'être scellé à l'issue de la mise à jour, vérifiez que la clé privée du certificat utilisé pour communiquer avec le serveur SMC ou celle du certificat présenté par les services VPN du firewall SNS <u>n'est pas protégée</u>. Pour le serveur SMC, reportez-vous à la section Cas d'un parc de firewalls géré par un serveur SMC. Pour les services VPN, reportez-vous à la section Utiliser des certificats dont la clé privée est protégée par le module TPM.
- 4. Si la clé privée de ces certificats est protégée, vous devez supprimer cette protection <u>avant</u> de mettre à jour le firewall SNS. Pour le serveur SMC, reportez-vous à la section Cas d'un parc de firewalls géré par un serveur SMC. Pour les services VPN, reportez-vous à la section Gérer la protection de la clé privée d'un certificat déjà présent.
- 5. Dès lors que ces clés privées ne sont plus protégées, vous pouvez mettre à jour le firewall SNS.
- 6. Une fois le firewall SNS à jour, vous devez sceller de nouveau le module TPM. En vous connectant à l'interface Web d'administration du firewall SNS, une fenêtre vous invite à le faire. Si besoin, reportez-vous à la procédure Sceller le module TPM.
- 7. Une fois le module TPM scellé, vous pouvez protéger de nouveau les clés privées dont la protection a été supprimée précédemment. Pour le serveur SMC, reportez-vous à la section Cas d'un parc de firewalls géré par un serveur SMC. Pour les services VPN, reportez-vous à la section Gérer la protection de la clé privée d'un certificat déjà présent.

Page 34/35





documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2025. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.

