



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SN-S-SERIES - METTRE À JOUR LE BIOS EN VERSION R1.03

Produits concernés : SN-S-Series-220 et SN-S-Series-320

Dernière mise à jour du document : 23 avril 2026

Référence : sns-fr-SN-S-Series_mettre_a_jour_BIOS_note_technique



Table des matières

Historique des modifications	3
Avant de commencer	4
Liste des versions de BIOS du firewall SN-S-Series	4
Mettre à jour le BIOS depuis l'interface Web d'administration	5
Équipements nécessaires	5
Informations importantes concernant certaines fonctionnalités du firewall SNS	5
Télécharger le fichier de mise à jour du BIOS	5
Mettre à jour le BIOS et le firmware de Intel Management Engine	5
Vérifier la version de BIOS actuelle	5
Mettre à jour le BIOS et le firmware de Intel Management Engine	6
Action à mener à l'issue de la mise à jour	7
Pour aller plus loin	8



Historique des modifications

Date	Description
23 avril 2026	Nouveau document



Avant de commencer

Ce document décrit la procédure de mise à jour du BIOS d'un firewall SN-S-Series en version R1.03 depuis la version R1.02.

La mise à jour du BIOS ne peut être réalisée que depuis l'interface Web d'administration du firewall SNS.

Liste des versions de BIOS du firewall SN-S-Series

Version	Peut être installée sur la version	Notes de version
R1.03	R1.02	- Correction d'un problème lié au changement de PCR.



Mettre à jour le BIOS depuis l'interface Web d'administration

Cette section décrit la procédure de mise à jour du BIOS d'un firewall SN-S-Series (SN-S-Series-220 et SN-S-Series-320) en version R1.03 depuis la version R1.02. Cette mise à jour ne peut être réalisée que depuis l'interface Web d'administration du firewall SNS.

Équipements nécessaires

- Un ordinateur avec un accès à l'interface Web d'administration du firewall SN-S-Series via un navigateur Web compatible.

Informations importantes concernant certaines fonctionnalités du firewall SNS

- **Module TPM** : si vous avez initialisé le module TPM, les fonctionnalités qui utilisent des certificats dont la clé privée est protégée par le module TPM (VPN, firewall SNS administré par un serveur SMC, etc.) ne seront plus opérationnelles. Vous devrez sceller de nouveau le module TPM pour rétablir les fonctionnalités concernées.

Cette procédure est décrite dans la section [Action à mener à l'issue de la mise à jour](#).

Télécharger le fichier de mise à jour du BIOS

1. Depuis votre espace [MyStormshield](#), rendez-vous dans **Téléchargements > STORMSHIELD NETWORK SECURITY > TOOLS > STORMSHIELD NETWORK SECURITY - TOOLS**.
2. Téléchargez le fichier **.maj SN-S-Series_BIOS_R103_remote_update** en cliquant sur son nom.
3. Contrôlez l'intégrité du fichier téléchargé à l'aide de son empreinte SHA256 :

```
d3224163e34c32a67b7ebe523ce632cdb34ab75a8f26f21beb52c029cfddf919
```

Le fichier .maj téléchargé contient la mise à jour du BIOS et du firmware de Intel Management Engine.

Mettre à jour le BIOS et le firmware de Intel Management Engine

Vérifier la version de BIOS actuelle

Depuis les versions SNS 4.8.13 LTSB et 4.3.41 LTSB, vous pouvez vérifier la version de BIOS en console CLI :

1. Depuis l'interface Web d'administration du firewall SNS, rendez-vous dans **Configuration > Système > Console CLI**.
2. Tapez la commande :

```
SYSTEM PROPERTY
```

Le jeton de configuration **BIOSVersion** doit afficher la version R1.02.

Pour les versions SNS antérieures, vous devez faire cette vérification en console ou en SSH :

1. Connectez-vous en console ou en SSH au système du firewall SNS.
2. Authentifiez-vous à l'aide du compte *admin* du système du firewall SNS.



3. Tapez la commande :

```
dmidecode -s bios-version
```

Le firewall SNS doit afficher la version R1.02.

Mettre à jour le BIOS et le firmware de Intel Management Engine

! IMPORTANT

Le processus de mise à jour est automatique et dure environ cinq minutes. Une fois lancé, ce processus **ne doit jamais** être interrompu et le firewall SNS **ne doit pas** être déconnecté du réseau électrique. Ceci aurait pour conséquence de rendre le firewall SNS totalement inopérant.

1. Depuis l'interface Web d'administration du firewall SNS, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Mise à jour du système**.
2. Sélectionnez le fichier de mise à jour *[.maj]* téléchargé précédemment.
3. Dépliez le cadre **Configuration avancée** et décochez **Sauvegarder la partition active sur la partition de sauvegarde avant de mettre à jour le Firewall**.
4. Cliquez sur **Mettre à jour le firewall**.

SYSTEM UPDATE BACKUP RESTORE CONFIGURATION

Available updates

No update available

Check for new updates

System update

Select the update

Update firmware

Advanced properties

Save the active partition on the backup partition before updating the firewall

5. Patientez pendant la mise à jour. Une fenêtre pop-up indique l'état d'avancement. Pendant la mise à jour, le firewall SNS redémarre à plusieurs reprises. Ce comportement est normal.

RECONNECT AUTOMATICALLY TO: [IP address]

Do not power off your appliance. Firmware update installation pending. Please wait, we will connect you as soon as possible

Estimated remaining time: 2m 48s

Le retour à la page de connexion de l'interface Web d'administration du firewall SNS indique que la mise à jour est terminée.



Action à mener à l'issue de la mise à jour

Sceller de nouveau le module TPM

Si vous aviez initialisé le module TPM, les fonctionnalités qui utilisent des certificats dont la clé privée est protégée par le module TPM (VPN, firewall SNS administré par un serveur SMC, etc.) ne sont plus opérationnelles. Pour rétablir les fonctionnalités concernées, suivez l'une des procédures ci-dessous pour sceller de nouveau le module TPM.

Depuis l'interface Web d'administration

Ce cas concerne exclusivement les versions SNS 4.8.7 et supérieures.

1. Connectez-vous à l'interface Web d'administration du firewall SNS. Une fenêtre vous invite à sceller le module TPM du firewall SNS.

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

2. Renseignez le mot de passe d'administration du module TPM dans le champ correspondant.
3. Cliquez sur **OK**.
4. Si le firewall SNS est membre d'un cluster en haute disponibilité, une deuxième fenêtre vous invite à sceller le module TPM du firewall passif. Renseignez le mot de passe d'administration du module TPM et 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 d'administration du module 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
```



Pour aller plus loin

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



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2026. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.