NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SN3100 - METTRE À JOUR LE BIOS EN VERSION R2.30

Produits concernés : SN3100

Dernière mise à jour du document : 6 août 2025

Référence : sns-fr-SN3100_mettre_a_jour_BIOS_note_technique

Table des matières

Historique des modifications

Date	Description
6 août 2025	Ajout de précisions concernant la gestion du mot de passe d'accès au panneau de configuration de l'UEFI, de Secure Boot et du module TPM.
22 juillet 2025	Nouveau document

Avant de commencer

Ce document décrit la procédure permettant de mettre à jour le BIOS d'un firewall modèle SN3100 depuis la version R1.06 vers la version R2.30.

INFORMATION
La version de BIOS R2.30 est indispensable pour embarquer l'ensemble des correctifs remédiant aux problèmes d'instabilité rencontrés par le jeu de puces (chipset) et le CPU Intel® du firewall modèle SN3100.

À l'issue de la mise à jour du BIOS, les fonctionnalités suivantes devront être configurées à nouveau :

- **Mot de passe d'accès au panneau de configuration de l'UEFI** : si vous l'aviez défini préalablement sur le firewall, il sera supprimé lors de la mise à jour du BIOS. Vous devrez le paramétrer à nouveau.
- **Secure Boot** : cette fonctionnalité est désactivée par défaut sur le firewall modèle SN3100. Si vous l'avez activée sur votre firewall, vous devrez la désactiver au cours de la procédure de mise à jour du BIOS. Vous pourrez la réactiver après la mise à jour.
- **Module TPM** : s'il avait été initialisé sur le firewall, il ne sera plus scellé après la procédure de mise à jour du BIOS. Vous devrez le sceller à nouveau.

Ces procédures sont décrites dans la section Actions à mener à l'issue de la mise à jour du BIOS de cette note technique.

Équipement nécessaire

Cette section décrit l'équipement nécessaire pour mettre à jour la version du BIOS sur un firewall SN3100.

- Un moniteur disposant d'un port HDMI ainsi qu'un cordon HDMI / HDMI,
- Un clavier USB,
- Une clé USB vierge et formatée avec le système de fichiers FAT32,
- Un firewall modèle SN3100 disposant du BIOS version R1.06.

Vous pouvez également effectuer cette manipulation avec l'équipement suivant :

- Un ordinateur équipé d'un émulateur de terminal installé (PuTTY par exemple, avec un baud rate de 115200),
- Un câble série RJ45 vers DB9F (fourni avec le firewall) et un câble RS232 vers USB-A,
- Une clé USB vierge et formatée avec le système de fichiers FAT32,
- Un firewall modèle SN3100 disposant du BIOS version R1.06.

Préparer la clé USB

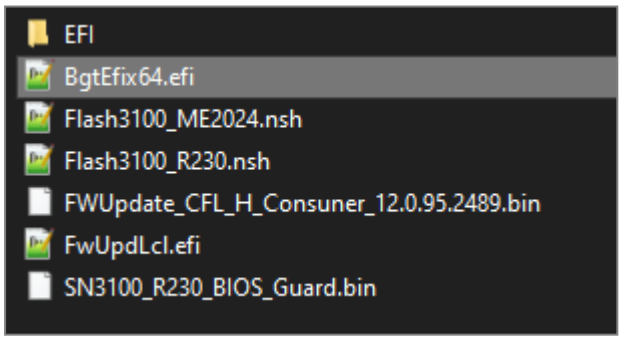
Cette section décrit la procédure de préparation de la clé USB utilisée pendant la mise à jour. Assurez-vous que votre clé USB soit vierge et formatée avec le système de fichiers FAT32.

Copier l'utilitaire de mise à jour sur la clé USB

1. Téléchargez la dernière version de l'utilitaire *Aptio V AMI Firmware Update Utility* de mise à jour AMI Firmware Update (AFU) disponible en suivant le lien : https://www.ami.com/bios-uefi-utilities/#aptiov
2. Décompressez l'archive *Aptio_V_AMI_Firmware_Update_Utility.zip*.
3. Décompressez l'archive *BgtEfi64.zip* présente dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility/bgt/bgtefi/64/5.03*.
4. Copiez le fichier *BgtEfix64.efi* présent dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility/bgt/bgtefi/64/5.03/BgtEfi64/BgtEfi64* **vers la racine** de votre clé USB.

Télécharger la version R2.30 du BIOS

1. Depuis votre espace personnel MyStormshield, rendez-vous dans **Téléchargements** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY-TOOLS** > **SN3100 BIOS R230** pour télécharger le fichier *SN3100_BIOS_R230.zip*.
2. Contrôlez l'intégrité du fichier téléchargé à l'aide de son empreinte SHA256 : 14fb5675c619ccba4342807530fc9f90c8a82e954df024fb64449d7efd4aab5a.
3. Décompressez l'archive *SN3100_BIOS_R230.zip* **à la racine** de votre clé USB.
4. Vérifiez la racine de votre clé USB. Vous devez y trouver les fichiers et répertoires suivants :



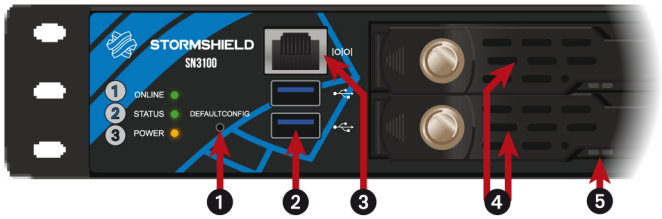
5. Contrôlez l'intégrité du binaire *SN3100_R230_BIOS_Guard.bin* à l'aide de son empreinte SHA 256 : 036113e77edaf0f6eda51ba7edbb733bbd1cfc7167110fbeda9fad2ef4967f57.
6. Contrôlez également l'intégrité du binaire *FWUpdate_CFL_H_Consuner_12.0.95.2489.bin* à l'aide de son empreinte SHA 256 : 00319e0bf2b9078f3c41b1b7c799e87b27335fe551e3eb37aad37c0270220f4f.

Votre clé USB de mise à jour du BIOS vers la version R2.30 est prête.

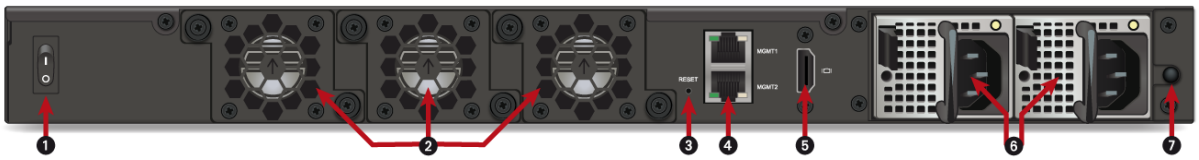
Mettre à jour le BIOS (SN3100)

Cette section présente la connectique du firewall SN3100 ainsi que les étapes successives à suivre dans cet ordre pour mettre à jour le BIOS en version R2.30.

L'essentiel de la connectique de ces firewalls se situe en façade, sauf le port HDMI, situé à l'arrière du firewall.



1 : Bouton de mise en configuration usine (defaultconfig).
2 : Ports USB 3.0.
3 : Port série RJ45 en mode console.
4 : Racks des SSD pour le stockage des traces.
5 : Voyants des racks SSD.



1 : Bouton d'alimentation.
2 : Ventilateurs.
3 : Bouton Reset : reset électrique.
4 : Ports dédiés au management du produit (MGMT1 et MGMT2).
5 : Port HDMI : branchement de l'écran.
6 : Embases secteur pour la redondance d'alimentation.
7 : Bouton Alarm off.

Connecter les périphériques sur le firewall

1. Raccordez l'écran sur le port HDMI à l'arrière du firewall.
2. Raccordez le clavier sur un port USB du firewall.
3. Insérez la clé USB dans le deuxième port USB.

NOTE
Vous pouvez également effectuer cette manipulation en mode console.
Dans ce cas, reliez votre firewall à un ordinateur équipé d'un émulateur de terminal installé (PuTTY par exemple, avec un baud rate de 115200) à l'aide du câble série RJ45 vers DB9F (fourni avec le firewall) et d'un câble RS232 vers USB-A.

Vérifier la version de BIOS du firewall

1. Connectez-vous en console au système du firewall.
2. Authentifiez-vous à l'aide du compte *admin* du système du firewall.
3. Tapez la commande : `dmidecode -s bios-version`.
   Le firewall affiche la version de BIOS : cette version doit être R1.06.

Mettre à jour le BIOS du firewall

La fonctionnalité Secure Boot est désactivée par défaut sur le firewall modèle SN3100. Si vous l'aviez activée sur votre firewall, vous devez la désactiver avant de suivre les étapes ci-dessous. Vous pourrez réactiver Secure Boot à l'issue de la mise à jour. Pour plus d'information, reportez-vous à la note technique Gérer Secure Boot dans l'UEFI des firewalls SNS.

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

1. Le firewall SN3100 dispose de deux alimentations internes pour la redondance, assurez-vous d'avoir branché les deux alimentations au réseau électrique.
2. Vérifiez que la clé USB préparée précédemment soit insérée dans un port USB.
3. Redémarrez le firewall à l'aide de la commande `reboot`.
4. Depuis l'invite de commandes, tapez `fs0:` ou `fs1:` pour atteindre la clé USB et vérifier son contenu. Repérez l'exécutable `Flash3100_R230.nsh`.
   Si l'emplacement de la clé USB n'est pas connu, tapez la commande `ls` pour chacun d'eux et vérifiez le contenu.
5. Lancez l'exécutable `Flash3100_R230.nsh`. Le processus de mise à jour démarre :

```
FS0:\SN3100_BIOS_R2.30\> Flash3100_R230.nsh
FS0:\SN3100_BIOS_R2.30\> BgtEfix64_2.efi SN3100_R230_BIOS_Guard.bin /BIOSALL
+-------------------------------------------------------------------------+
|               AMI BIOS Guard Firmware Update Tool  v5.03.03.0022        |
|      Copyright (C)2018 American Megatrends Inc. All Rights Reserved.    |
+-------------------------------------------------------------------------+
 BIOS_FV_NVRAM.bin ................. (100%)
 BIOS_FV_NVRAM_BACKUP.bin .......... (100%)
 BIOS_FV_OA.bin .................... (100%)
 BIOS_FV_MAIN.bin_00 ............... ( 20%)
 BIOS_FV_MAIN.bin_01 ............... ( 40%)
 BIOS_FV_MAIN.bin_02 ............... ( 60%)
 BIOS_FV_MAIN.bin_03 ............... ( 80%)
 BIOS_FV_MAIN.bin_04 ............... (100%)
 BIOS_FV_DATA.bin_00 ............... ( 50%)
 BIOS_FV_DATA.bin_01 ............... (100%)
 BIOS_FV_AfterBB.bin ............... (100%)
 BIOS_FV_FSPS.bin .................. (100%)
 BIOS_FV_FSPTM.bin ................. (100%)
 BIOS_FV_BB.bin .................... (100%)
```

6. Lorsque le processus de mise à jour est terminé, exécutez la commande `reset` pour redémarrer le firewall. Il démarre automatiquement sur la clé USB.

Mettre à jour le firmware de Intel® Management Engine

Suite à la mise à jour du BIOS, vous devez également mettre à jour le firmware de Intel® Management Engine.

1. Depuis l'invite de commande, lancez l'exécutable `Flash3100_ME2024.nsh` :

```
fs1:\> Flash3100_ME2024.nsh
Flash3100_ME2024.nsh> FwUpdLcl.efi -F FWUpdate_CFL_H_Consuner_12.0.95.2489.bin
Intel (R) Firmware Update Utility Version: 12.0.95.2495
Copyright (C) 2005 - 2024, Intel Corporation. All rights reserved.

Checking firmware parameters...

Warning: Do not exit the process or power off the machine before the firmware update process ends.
Sending the update image to FW for verification:  [ COMPLETE ]



FW Update:  [ 100% (-)] Do not Interrupt
FW Update completed successfully and a reboot will run the new FW.
```

2. Lorsque le processus de mise à jour est terminé, éteignez le firewall en utilisant la commande `reset -s`.
3. Déconnectez les deux alimentations électriques de votre firewall.
4. Débranchez la clé USB de votre firewall.
5. Patientez cinq minutes et rebranchez les deux cordons d'alimentation.
6. Démarrez votre firewall en pressant le bouton d'alimentation situé à l'arrière du firewall.

Vérifier la version de BIOS et du firmware de Intel® Management Engine du firewall après la mise à jour

1. Appuyez plusieurs fois sur la touche **[Suppr]** du clavier pour interrompre la séquence de démarrage et atteindre le BIOS.
2. Rendez-vous dans l'onglet **Main** et vérifiez la version de BIOS qui doit être égale à R2.30.
3. Rendez-vous dans l'onglet **Advanced** > **PCH-FW** et vérifiez la version du Intel® Management Engine (ME Firmware Version) qui doit être égale à 12.0.95.2489.
4. Appuyez sur la touche **[Échap]** du clavier.

Actions à mener à l'issue de la mise à jour du BIOS

À l'issue de la mise à jour du BIOS, vous devez mener les actions ci-dessous, dans cet ordre.

Paramétrer le mot de passe d'accès au panneau de configuration de l'UEFI

Si vous aviez défini un mot de passe d'accès au panneau de configuration de l'UEFI avant la mise à jour du BIOS, celui-ci est supprimé. Vous devez le paramétrer à nouveau en suivant la procédure de la note technique **Protéger l'accès au panneau de configuration de l'UEFI des firewalls SNS**.

Activer Secure Boot

La fonctionnalité Secure Boot est désactivée par défaut sur le firewall modèle SN3100. Si vous l'aviez activée sur votre firewall avant la mise à jour du BIOS, vous devez la réactiver en suivant la procédure de la section **Activer Secure Boot dans l'UEFI du Firewall SNS** de la note technique *Gérer Secure Boot dans l'UEFI des firewalls SNS*.

Sceller le module TPM

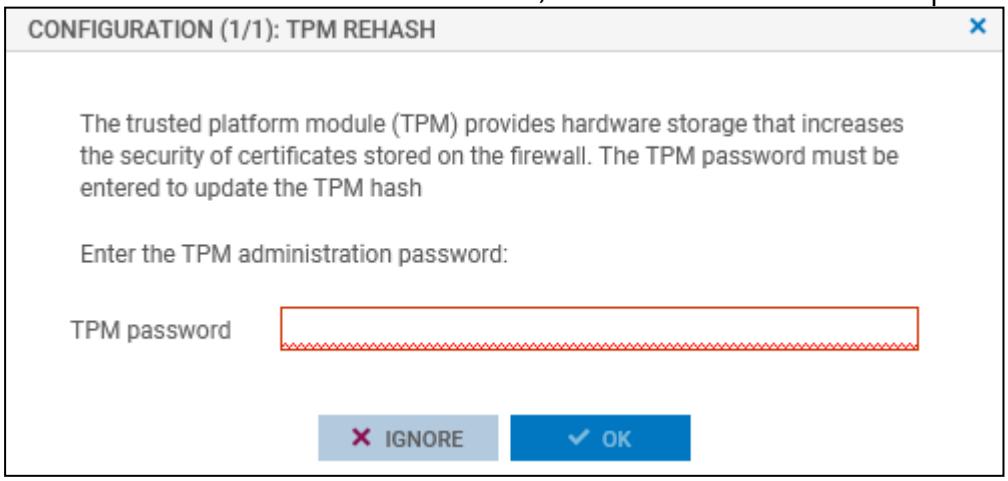
Si le module TPM avait été initialisé sur le firewall avant la mise à jour du BIOS, vous devez le sceller à nouveau. En effet, à l'issue de la mise à jour du BIOS, la valeur des empreintes de confiance a été modifiée, ce qui rend impossible le déchiffrement des clés privées protégées.

Pour sceller à nouveau le module TPM, suivez l'une des procédures ci-dessous.

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 s'affiche automatiquement. 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.



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
   ```

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