NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SN-L-SERIES - METTRE À JOUR LE BIOS EN VERSION R1.05

Produits concernés : SN-L-Series 2200, SN-L-Series 3200

Dernière mise à jour du document : 12 juin 2025

Référence : sns-fr-SN-L-Series_mettre_a_jour_BIOS_note_technique

Table des matières

Historique des modifications

Date	Description
12 juin 2025	Nouveau document

Avant de commencer

Ce document décrit la procédure permettant de mettre à jour le BIOS d'un firewall SNS SN-L-Series (SN-L-Series-2200 et SN-L-Series-3200) depuis la version R1.02 vers la version R1.05.

INFORMATION
La version de BIOS R1.05 est indispensable pour corriger les problèmes d'instabilité rencontrés par les processeurs Intel® de ces firewalls.

À l'issue de la mise à jour du BIOS :

- Le mot de passe d'accès au panneau de configuration de l'UEFI sera supprimé. Vous devrez le paramétrer à nouveau.
- La fonctionnalité Secure Boot sera désactivée. Vous devrez la réactiver.
- Le module TPM ne sera plus scellé. 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 TNO.

Équipement nécessaire

Cette section décrit l'équipement nécessaire pour mettre à jour la version du BIOS sur un firewall SN-L-Series (SN-L-Series-2200 et SN-L-Series-3200).

- Un ordinateur avec un émulateur de terminal installé (PuTTY par exemple, avec un baud rate de 115200) et le pilote PL23XX USB-to-Serial installé si la connexion côté firewall s'effectue sur un port USB-C,
- Une clé USB vierge et formatée avec le système de fichiers FAT32,
- Un câble USB-A vers USB-C ou un câble série RJ45 vers DB9 (RS232),
- Un firewall modèle SN-L-Series disposant du BIOS version R1.02.

NOTE
Vous pouvez également effectuer cette manipulation directement sur un écran à l'aide d'un câble HDMI / HDMI.
Dans ce cas, branchez également un clavier USB au firewall SNS.

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 version la plus récente de l'utilitaire *AMI Firmware Update Tool* (AFU) disponible en suivant le lien : https://www.ami.com/static-downloads/Aptio_V_AMI_Firmware_Update_Utility.zip
2. Décompressez l'archive *Aptio_V_AMI_Firmware_Update_Utility.zip*.
   Les fichiers décompressés sont placés dans un répertoire nommé *Aptio_V_AMI_Firmware_Update_Utility*.
3. Décompressez l'archive *Afu£fi64.zip* présente dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility/afu/afuefi/64*.
4. Copiez le fichier *Afu£fix64.efi* présent dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility/afu/afuefi/64/Afu£fi64* **vers la racine** de votre clé USB.

Télécharger la version R1.05 du BIOS

1. Téléchargez le fichier *SN-L-Series_BIOS_R105.zip* depuis votre espace personnel MyStormshield (**Téléchargements** > **STORMSHIELD NETWORK SECURITY** > **TOOLS** > **STORMSHIELD NETWORK SECURITY-TOOLS** > **SN-L-Series BIOS R105**).
2. Contrôlez l'intégrité du fichier téléchargé à l'aide de son empreinte SHA256 :
   ?c64d14d?dcd68c649bd4?41931f6c04d80da539bddce?58376e?6fac1?28a6b.
3. Décompressez l'archive *SN-L-Series_BIOS_R105.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 :

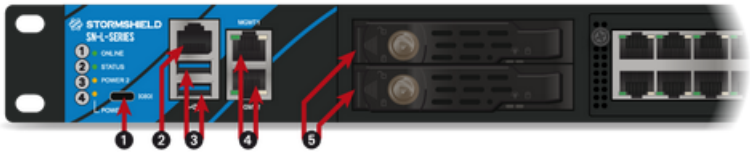
5. Contrôlez l'intégrité du binaire *SN-L-Series_R105_BIOS_Guard.bin* à l'aide de son empreinte SHA 256 :
   67c47695800c1a?3e8cfb430173c84ba61dcbfad5b99902a41d3ea?0a612e31c.
6. Contrôlez également l'intégrité du binaire *ADL_S_Corporate_DDR5_Prod_FWUpdate.bin* à l'aide de son empreinte SHA 256 :
   97d1d80d5fa60a86df36d456629ab?75bd8b139b913?41dc5306f37e0b83abe9.

Votre clé USB de mise à jour du BIOS vers la version R1.05 est prête.

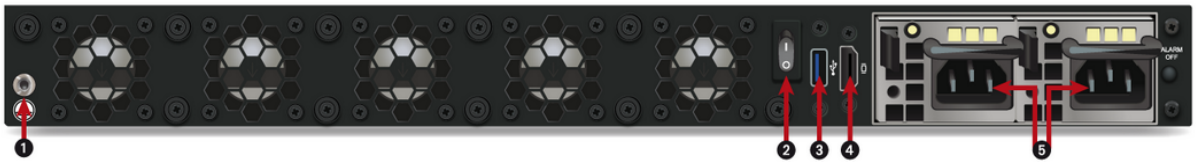
Mettre à jour le BIOS (SN-L-Series)

Cette section présente la connectique du firewall SN-L-Series (SN-L-Series 2200 et SN-L-Series 3200) ainsi que les étapes successives à suivre dans cet ordre pour mettre à jour le BIOS en version R1.05.

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



1 : Port série USB-C en mode console
2 : Port série RJ45 en mode console
3 : Ports USB 3.0
4 : Ports dédiés au management du produit (MGMT1 et MGMT2)
5 : Racks des SSD pour le stockage des traces



1 : Branchement de mise à la terre
2 : Bouton d'alimentation
3 : Port USB 3.0
4 : Port HDMI : branchement de l'écran
5 : Embases secteur pour la redondance d'alimentation.

Connecter les périphériques sur le firewall

- Raccordez l'ordinateur équipé d'un émulateur de terminal au firewall à l'aide du câble USB-A vers USB-C côté firewall (cette connexion sur un port USB-C nécessite l'installation du pilote PL23XX USB-to-Serial) ou du câble série RJ45 vers DB9.
- Vous pouvez également connecter directement le firewall sur un écran à l'aide d'un câble HDMI / HDMI.
  Dans ce cas, branchez également un clavier au firewall SNS.

Vérifier la version de BIOS du firewall

1. Connectez-vous en console ou en SSH (à l'aide d'un logiciel de type *PuTTY*) 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 R1.02.

Désactiver Secure Boot

La mise à jour du BIOS nécessite la désactivation de Secure Boot afin de permettre le démarrage du firewall sur la clé USB précédemment préparée. Pour désactiver Secure Boot, reportez-vous à la section **Désactiver Secure Boot dans l'UEFI du Firewall SNS** de la note technique *Gérer Secure Boot dans l'UEFI des firewalls SNS*.

Mettre à jour le BIOS du firewall

IMPORTANT
Le processus de mise à jour est entièrement automatique et dure environ 5 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. Le firewall SN-L-Series dispose de deux alimentations internes pour la redondance, assurez-vous d'avoir branché les deux alimentations au réseau électrique.

1. Insérez la clé USB préparée précédemment dans un port USB.
2. Redémarrez le firewall à l'aide de la commande `reboot`.
3. Depuis l'invite de commande, lancez l'exécutable `Flash_SNL_R105.nsh`. Le processus de mise à jour démarre :

```
Flash_SNL_R105.nsh> AfuEfix64.efi SN-L-Series_R105_BIOS_Guard.BIN /BIOSALL
+-------------------------------------------------------------------------------+
|                AMI Firmware Update Utility v5.16.04.0135                      |
|      Copyright (c) 1985-2024, American Megatrends International LLC.         |
|         All rights reserved. Subject to AMI licensing agreement.              |
+-------------------------------------------------------------------------------+
 - System BIOS Guard Support ........ Enabled
 Reading flash ..................... Done
 - ME Data Size Checking ............ Pass
 - System Secure Flash .............. Enabled
 - FFS Checksums .................... Pass
 Loading BIOS Guard File To Memory .. Done
 FV_BB1_BACKUP ..................... (100%)
 FV_BB_AFTER_MEMORY_BACKUP ......... (100%)
 FV_FSP_S_BACKUP ................... (100%)
 FV_FSP_M_BACKUP_00 ................ ( 50%)
 FV_FSP_M_BACKUP_01 ................ (100%)
 FV_FSP_T_BACKUP ................... (100%)
 FV_BB_BACKUP ...................... (100%)
```

4. 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 `Flash_ME_SNL.nsh` :

```
FS0:\> Flash_ME_SNL.nsh
FS0:\> FWUpdLcl.efi ADL_S_Corporate_DDR5_Prod_FWUpdate.bin

Intel (R) FW Update Sample Application

Loading file into memory...

FW type is: Corporate.
PCH SKU is: H.

Executing Full FW Update.

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 5 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 R1.05.
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 16.1.35.2557.
4. Appuyez sur la touche **[Échap]** du clavier.

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

Suite à la mise à jour du BIOS, vous devez mener les actions suivantes, dans cet ordre :

1. Paramétrer le mot de passe d'accès au panneau de configuration de l'UEFI du firewall en suivant la procédure de la note technique **Protéger l'accès au panneau de configuration de l'UEFI des firewalls SNS**.
2. Activer la fonctionnalité Secure Boot en suivant la section **Activer Secure Boot dans l'UEFI du Firewall SNS** de la note technique *Gérer Secure Boot dans l'UEFI des firewalls SNS*.
3. Si le module TPM avait été initialisé sur le firewall, sceller le module TPM. En effet, suite à 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 le module TPM, reportez-vous à la section **Sceller le module TPM** de la note technique *Configurer le module TPM et protéger les clés privées de certificats du firewall SNS*.
   Pour plus d'informations sur le module TPM et le registre PCR, reportez-vous à la section **Fonctionnement** de la note technique *Configurer le module TPM et protéger les clés privées de certificats du firewall 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