



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SNI20 - MISE À JOUR DU BIOS EN VERSION R1.06

Produits concernés : SNI20

Dernière mise à jour du document : 2 août 2022

Référence : sns-fr-SNi20_mettre_a_jour_BIOS_note_technique



Table des matières

Avant de commencer	3
Équipement nécessaire	3
Préparer la clé USB	3
Copier l'utilitaire de mise à jour sur la clé USB	3
Télécharger la version R1.06 du BIOS	3
Mettre à jour le BIOS (SNI20)	4
Connecter les périphériques sur le firewall	4
Vérifier la version de BIOS du firewall	4
Mettre à jour le BIOS du firewall	5
Vérifier la version de BIOS du firewall après mise à jour	6
Mettre à jour le registre PCR	6



Avant de commencer

Ce document décrit la procédure permettant de mettre à jour le BIOS d'un firewall modèle SNI20 depuis la version R1.03 vers la version R1.06.

Équipement nécessaire

- Un moniteur disposant d'un port HDMI ainsi qu'un cordon HDMI / Micro HDMI,
- Un clavier USB,
- Une clé USB vierge et formatée avec le système de fichier FAT32,
- Un firewall modèle SNI20 disposant du BIOS version R1.03.

Préparer la clé USB

Pour mettre à jour le BIOS, il est nécessaire de télécharger 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

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

1. 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*.
2. Décompressez l'archive *AfuEfi64.zip* présente dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility/afu/afuefi/64*.
3. Copiez le fichier *AfuEfi64.efi* présent dans le sous-répertoire *Aptio_V_AMI_Firmware_Update_Utility/afu/afuefi/64/AfuEfi64* **vers la racine** de votre clé USB.

Télécharger la version R1.06 du BIOS

1. Téléchargez le fichier *SNI20_BIOS_R106.zip* depuis votre espace personnel [Mystormshield](#) (**Téléchargements > STORMSHIELD NETWORK SECURITY > TOOLS > STORMSHIELD NETWORK SECURITY-TOOLS > SNI20 BIOS r1.03 to r1.06**).
2. Contrôlez l'intégrité du fichier téléchargé à l'aide de son empreinte SHA256 :
75CD8DE235E331494CDFC24E529EEAD06C5C3909EFE31745EE3F3A0C8462A7B7.
3. Décompressez l'archive *SNI20_BIOS_R106.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 :

EFI	06/01/2021 16:19
AfuEfi64.efi	09/03/2021 09:52
FlashR106.nsh	09/03/2021 11:28
fparts.txt	16/09/2016 11:38
SNI20_R106.bin	06/01/2021 16:19
startup.nsh	09/03/2021 11:38

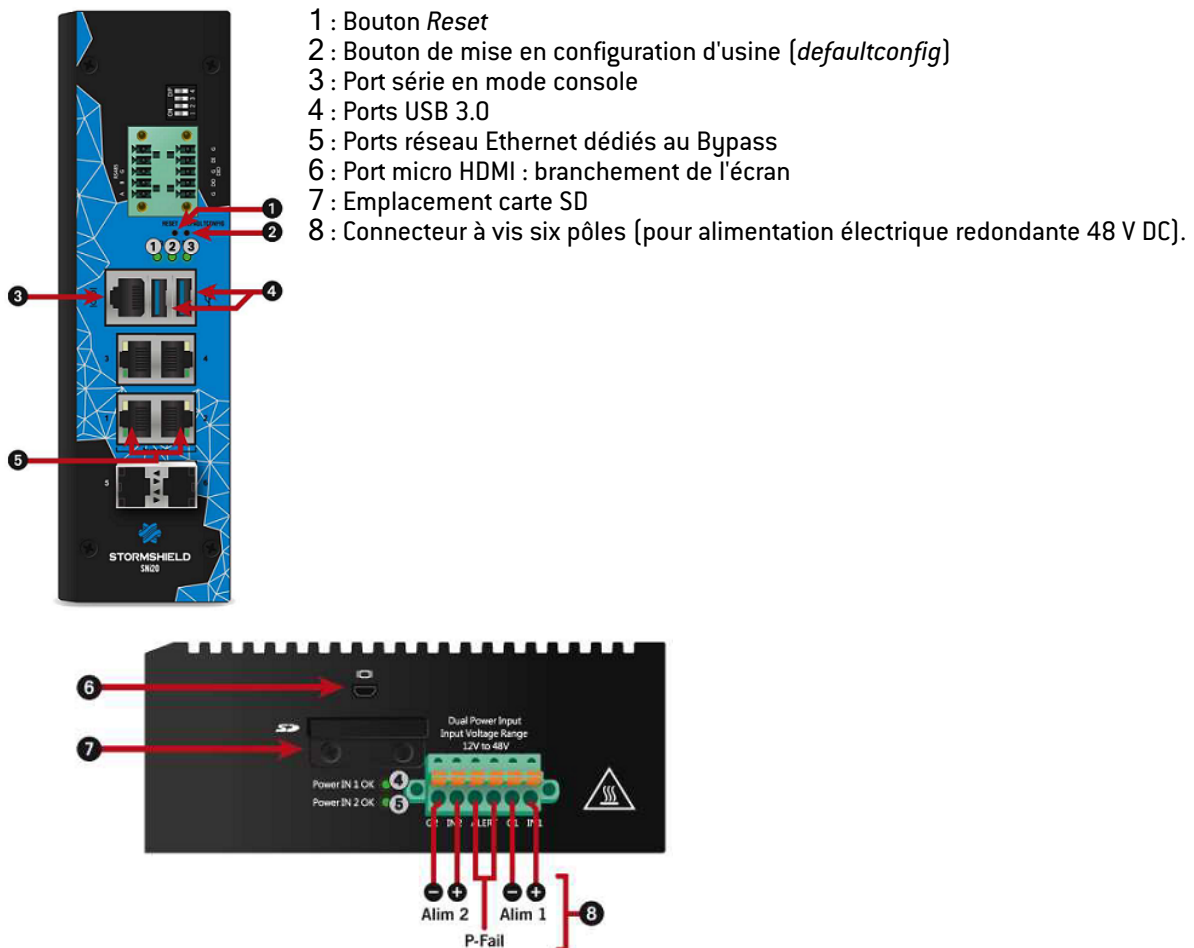
5. Contrôlez l'intégrité du binaire *SNI20_R106.bin* à l'aide de son empreinte SHA 256 :
20EA3191784AFD06BF9C504A60B5BFBF6F27AB3EFD6D3F648C9B5A0F67BA073E.



Votre clé USB de mise à jour du BIOS vers la version R1.06 est prête.

Mettre à jour le BIOS (SNI20)

L'essentiel de la connectique de ces firewalls se situe en façade, sauf pour le port micro HDMI situé sur le dessus du produit.



Connecter les périphériques sur le firewall

1. Raccordez l'écran sur le port micro HDMI [6] du firewall.
2. Raccordez le clavier sur un port USB [4] du firewall.
3. Insérez la clé USB dans le deuxième port USB (4).

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 firewall.
2. Authentifiez-vous à l'aide du compte *admin*.
3. Tapez la commande : `dmidecode -s bios-version`
Le firewall affiche la version du BIOS : cette version doit être R1.03.



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.

Si votre firewall dispose de modules d'alimentation redondants, assurez-vous d'avoir branché les deux modules au réseau électrique.

1. Lancez le redémarrage du firewall à l'aide de la commande `reboot`.
Le firewall démarre automatiquement sur la clé USB.
2. Depuis l'invite de commande, lancez l'exécutable *FlashR106.nsh* :

```
fsl:\> FlashR106.nsh
FlashR106.nsh> AfuEfix64.efi SNI20_R106.bin /P /N /REBOOT
+-----+
|               AMI Firmware Update Utility  v5.11.03.1778               |
|               APL FaultTolerance Mode                                     |
|               Copyright (C)2018 American Megatrends Inc. All Rights Reserved. |
+-----+
Reading flash ..... done
Secure Flash enabled, recalculate ROM size with signature... Enable.
- FFS checksums ..... ok
- Check RomLayout ..... ok.
Loading capsule to secure memory buffer ... done
- Fault Tolerance Flash Support Enable.
Fault Tolerant Backup..... done
Erasing AplFt Block ..... done
Updating AplFt Block ..... 0x00090000 (16%)
```

Lorsque le processus de mise à jour est terminé, le firewall redémarre automatiquement et affiche les informations suivantes :

```
EFI Shell version 2.50 [S.12]
Current running mode 1.1.2
Device mapping table
fs0 :HardDisk - Alias hdl2a65535a4 blk0
      PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(4,GPT,2828D30C-FD33-11EA-A45D-000DB41F8F92,0x401000,0x32000)
fs1 :Removable HardDisk - Alias hd2810b blk1
      PciRoot(0x0)/Pci(0x15,0x0)/USB(0x8,0x0)/HD(1,GPT,A69EC5D1-559F-11EB-AC1F-000DB41F38A0,0x800,0x394D000)
blk0 :HardDisk - Alias hdl2a65535a4 fs0
      PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(4,GPT,2828D30C-FD33-11EA-A45D-000DB41F8F92,0x401000,0x32000)
blk1 :Removable HardDisk - Alias hd2810b fs1
      PciRoot(0x0)/Pci(0x15,0x0)/USB(0x8,0x0)/HD(1,GPT,A69EC5D1-559F-11EB-AC1F-000DB41F38A0,0x800,0x394D000)
blk2 :HardDisk - Alias (null)
      PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(1,GPT,2801B648-FD33-11EA-A45D-000DB41F8F92,0x800,0x200000)
blk3 :HardDisk - Alias (null)
      PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(2,GPT,28110300-FD33-11EA-A45D-000DB41F8F92,0x200800,0x100)
blk4 :HardDisk - Alias (null)
      PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(3,GPT,28174D49-FD33-11EA-A45D-000DB41F8F92,0x201000,0x200000)
blk5 :HardDisk - Alias (null)
      PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)/HD(5,GPT,2838E1FC-FD33-11EA-A45D-000DB41F8F92,0x433000,0xAB9800)
blk6 :BlockDevice - Alias (null)
      PciRoot(0x0)/Pci(0x12,0x0)/Sata(0x0,0xFFFF,0x0)
blk7 :Removable BlockDevice - Alias (null)
      PciRoot(0x0)/Pci(0x15,0x0)/USB(0x8,0x0)

fsl:\> [C] in 1 seconds to skip startup.nsh, any other key to continue.
Found AfuEfix64 file on fsl:
```

3. Déconnectez l'alimentation électrique de votre firewall (ou les deux alimentations si votre firewall dispose de modules d'alimentation redondants).
4. Débranchez la clé USB de votre firewall.



Vérifier la version de BIOS du firewall après mise à jour

1. Branchez le(s) cordon(s) d'alimentation électrique au firewall SNI20.
Votre firewall démarre automatiquement.
2. Lorsque le système est entièrement redémarré après la mise à jour de BIOS (les 3 voyants *Online*, *Status* et *Power* sont actifs), appliquez de nouveau la procédure [Vérifier la version de BIOS du firewall](#).
Cette fois le firewall doit indiquer une version égale à R1.06.

Mettre à jour le registre PCR

Sur un firewall dont le TPM avait été initialisé en version R1.03 de BIOS, le registre PCR (Platform Configuration Register) doit être mis à jour.

Lorsque le système est entièrement redémarré après la mise à jour de BIOS (les 3 voyants *Online*, *Status* et *Power* sont actifs) :

1. Connectez-vous en SSH ou en console sur le firewall,
2. Tapez la commande :

```
tpmctl -v -s -p <tpm_password>
```



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2022. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.