NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

CONFIGURATION INITIALE PAR CLÉ USB

Produits concernés : SNS 3.9 et versions supérieures, SNS 4.x

Dernière mise à jour du document : 9 juillet 2024

Référence : sns-fr-configuration_initiale_par_cle_usb_note_technique

Table des matières

Historique des modifications

Date	Description
9 juillet 2024	- Sortie de SNS 4.8. - Ajout des opérations "*certimport*" et "*crlimport*".
10 avril 2024	- Correction du nom de l'opération "*initTPM*".

Avant de commencer

Cette Note Technique décrit comment mettre à jour et configurer avec une clé USB un ou plusieurs firewalls SNS initialement en configuration d'usine (matériel neuf) ou remis en configuration d'usine à l'aide du bouton de réinitialisation (*reset hardware*).

Séquence d'installation

Lors du démarrage du firewall SNS sur une clé USB, les fichiers présents sur la clé USB sont importés / installés / exécutés automatiquement selon la séquence suivante :

N°	Description de l'étape
1	Licence (extension ".licence")
2	Mise à jour de firmware (extension ".maj") Redémarrage du firewall **IMPORTANT** La clé USB doit être retirée lorsque le firewall redémarre.
3	Fichier de sauvegarde de configuration (extension ".na")
4	Package de rattachement à un serveur SMC (extension ".pack")
5	Certificats (extension ".p12"), à partir de la version SNS 3.9.0
6	Mot de passe du compte *admin* (extension ".pwd"), à partir de la version SNS 3.9.0
7	Fichiers de configuration de routage dynamique (extensions .bird et .bird6), à partir de la version SNS 3.10.2 ou de la version SNS 4.1.1
8	Fichiers de configuration additionnelle (extension ".csv"), à partir de la version SNS 3.9.0

Lorsque l'un des types de fichiers listés ci-dessus est absent de la clé, l'étape correspondante est simplement ignorée.

Préparer les fichiers

Cette section précise le format et la dénomination des fichiers pouvant être importés.

Vous pouvez utiliser une seule clé USB pour la configuration initiale de plusieurs firewalls. Ainsi, plusieurs fichiers au même format peuvent être présents sur une même clé USB.

Licences (*.licence*)

Chaque firewall dispose de son propre fichier de licence.

Vous pouvez récupérer les licences de vos firewalls SNS depuis votre espace MyStormhield dans **Produit > Gestion des produits**. Pour plus d'informations, reportez-vous à la section Télécharger le fichier de licence d'un produit du guide *Gérer des produits enregistrés*.

Dénomination

```
Firewall_Serial_Number.licence
```

EXEMPLES
SN320A000000000Z.licence
SN320B000000000Z.licence

Mises à jour logicielle (*.maj*)

Pour télécharger les fichiers de mise à jour logicielles des firewalls SNS :

1. Connectez-vous à votre espace MyStormhield.
2. Rendez-vous dans **Téléchargements > Stormshield Network Security > Firmware**. Si besoin, sélectionnez en plus une branche de version pour affiner la liste.
3. Repérez la ou les versions que vous souhaitez installer. Pour cela :
   - Consultez les notes de version pour connaître le contenu des versions SNS,
   - Assurez-vous que la version est compatible avec votre modèle de firewall. Si plusieurs firewalls sont configurés à l'aide d'une même clé USB, plusieurs fichiers de mise à jour logicielle peuvent être nécessaires (architectures des firewalls différentes, versions logicielles préchargées différentes, ...),
   - Si une version dispose de plusieurs versions correctives, privilégiez toujours la dernière afin de bénéficier des derniers correctifs fonctionnels et de vulnérabilités,
   - Utilisez des versions dont la date de fin de vie n'a pas été atteinte. Pour plus d'informations, reportez-vous au guide Cycle de vie produits Network Security & Tools.
4. Pour la version souhaitée, cliquez sur le nom correspondant au modèle de firewall pour télécharger le fichier de mise à jour logicielle (*.maj*).

Dénomination

EXEMPLES
fwupd-4.8.1-SNS-armv6-S.maj
fwupd-4.8.1-SNS-amd64-M.maj
fwupd-4.8.1-SNS-amd64-XL.maj

IMPORTANT
Pendant la séquence d'installation, la clé USB doit être retirée lorsque le firewall redémarre.

Si le différentiel entre la version majeure de firmware du firewall sorti d'usine et les versions logicielles présentes sur la clé est inférieur à 2 (exemple : firewall en version 3.9.0 et firmware 4.0.0 sur la clé), seule la version logicielle la plus élevée présente sur la clé est installée. Dans le cas contraire, une version intermédiaire de firmware doit être présente sur la clé afin de réaliser une mise à jour automatique par étapes (exemple : firewall en version 2.14.0 et firmwares 3.9.0 et 4.0.0 sur la clé).

Sauvegardes de configuration (*.na*)

Vous pouvez créer des fichiers de sauvegarde de configuration depuis l'interface Web d'administration du firewall en activité dans **Configuration > Système > Maintenance > Sauvegarder**.

Dénomination

Si la configuration est la même pour tous les firewalls :

```
default.na
```

En cas contraire :

```
Firewall_Serial_Number.na
```

EXEMPLES
SN310A000000000Z.na
SN310B000000000Z.na

Packages de rattachement SMC (*.pack*)

Si le firewall SNS est destiné à être administré depuis un serveur Stormshield Management Center, un package de rattachement (fichier *.pack*) doit être généré depuis le serveur SMC. Pour plus d'informations, reportez-vous à la section Rattacher un firewall en configuration d'usine au serveur du *Guide d'administration SMC*.

IMPORTANT
Vérifiez que le package de rattachement du firewall **n'inclut pas** de configuration réseau. Sinon, ce package écrasera la configuration réseau restaurée à l'aide du fichier *.na*.

Dénomination

```
Firewall_Serial_Number.pack
```

EXEMPLES
SN310A000000000Z.pack
SN310B000000000Z.pack

Certificats (*.p12*)

L'importation de certificats est disponible à partir de la version SNS 3.9.0.

Les certificats doivent être au format PKCS#12 (fichier chiffré regroupant le certificat du firewall et sa clé privée). Ces fichiers doivent être exportés depuis la machine gérant l'architecture à clés privées (PKI) de l'entreprise.

Si votre firewall est équipé d'un module TPM et que vous souhaitez protéger la clé privée contenue dans le fichier PKCS#12, reportez-vous à la section Opération *p12import*.

Dénomination

Les fichiers PKCS#12 destinés à un firewall ont un nom composé du numéro de série du firewall, suivi d'un éventuel suffixe (texte libre), et portent l'extension "p12".

```
FirewallSerialNumber.p12
FirewallSerialNumber_text.p12
```

EXEMPLES
SN310A000000000Z.p12
SN310A000000000Z_cert1.p12
SN310A000000000Z_cert2.p12
SN310B000000000Z.p12

Mot de passe du compte *admin* (*.pwd*)

Le déploiement du mot de passe du compte *admin* est disponible à partir de la version SNS 3.9.0.

Fichier

- Fichier texte contenant une seule chaîne, non chiffrée, et au format UTF-8.

Politique de mots de passe

- La taille du mot de passe doit être comprise entre 8 et 128 caractères,
- Le mot de passe doit respecter les caractères autorisés / interdits sur le firewall SNS, sinon, la connexion avec le compte *admin* ne fonctionnera pas. Pour plus d'informations, reportez-vous à la section Noms autorisés ou interdits du *manuel utilisateur SNS*,
- Le mot de passe doit respecter la politique de mots de passe restaurée à l'aide d'un fichier de sauvegarde de configuration, sinon, ce mot de passe ne sera pas pris en compte.

Dénomination

Pour un mot de passe différent d'un firewall SNS à un autre :

```
Firewall_Serial_Number.pwd
```

Pour un mot de passe identique sur tous les firewalls SNS (non recommandé) :

```
default.pwd
```

EXEMPLES
SN310A000000000Z.pwd
SN310B000000000Z.pwd

Configuration de routage dynamique (*.bird* et *.bird6*)

L'importation de fichiers de configuration de routage dynamique est disponible à partir de la version SNS 3.10.2 ou 4.1.1.

Chaque firewall utilisant une configuration de routage dynamique dispose :

- D'un fichier ".bird" pour les réseaux et routes IPv4,
- D'un fichier ".bird6" pour les réseaux et routes IPv6.

Vous pouvez récupérer ces fichiers via une connexion SSH sur un firewall en activité dans le répertoire */usr/Firewall/ConfigFiles/Bird/*.

Vous pouvez également afficher la configuration Bird dans l'interface d'administration du firewall SNS dans **Configuration** > **Réseau** > **Routage**, onglet *Routage dynamique*.

Dénomination

```
Firewall_Serial_Number.bird
Firewall_Serial_Number.bird6
```

EXEMPLES
SN310A000000000Z.bird
SN310A000000000Z.bird6

IMPORTANT
Pour que la configuration de routage dynamique soit utilisée, en plus des fichiers Bird, vous devez activer les modules Bird et Bird6 sur le firewall en utilisant un fichier de configuration additionnelle "*.csv*" permettant de lancer une opération *setconf*. Pour plus d'informations, reportez-vous à la section Fichiers de configuration additionnelle.

Fichiers de configuration additionnelle (*.csv*)

À partir de la version SNS 3.9.0, des opérations de configuration additionnelle peuvent être exécutées via un ou plusieurs fichiers CSV. Ces fichiers permettent notamment de construire un cluster de firewalls ou de modifier une valeur dans un fichier de configuration de firewall.

Les fichiers *.csv* doivent être au format UTF-8. **Tous** les fichiers *.csv* présents sur la clé USB seront exécutés lors de la séquence d'installation.

Structure générale d'un fichier de configuration additionnelle .csv

- Chaque ligne doit contenir une opération,
- Une ligne d'opération est définie selon la nomenclature suivante :
  ```
  "serial | any", "operation", ["parameter 1", ...]
  ```
  - serial : indique que l'opération doit être appliquée au firewall dont le numéro de série est renseigné,
  - any : indique que l'opération doit être appliquée quel que soit le firewall,
  - Tous les champs doivent être séparés par des virgules,
  - Les opérations et les paramètres sont détaillés ci-après.
- Des lignes de commentaires commençant par un "#" peuvent être insérées.

Opération *setconf*

L'opération *setconf* peut être utilisée pour :

- Modifier la valeur d'un champ présent dans une section particulière d'un fichier de configuration,
- A partir de la version SNS 3.10.1 : ajouter une ligne complète au sein d'une section d'un fichier de configuration.

Lorsqu'une virgule est nécessaire dans l'un des paramètres de la commande, la valeur du paramètre doit être encadrée par des guillemets.

Fixer la valeur d'un champ

Format

```
"serial | any", setconf, "file", "section", "field", "value"
```

EXEMPLES

```
any, setconf, network, ethernet0, Protected, 0
any, setconf, object, Host, gateway, "192.168.0.254, resolve=static"
any, setconf, Bird/global, bird, state, 1
```

Ajouter une ligne complète (à partir de la version SNS 3.10.1)

Format

```
"serial | any", setconf, "file", "section", "line"
```

EXEMPLE

```
any, setconf, route, StaticRoutes, "MyNetworkObject,my-if->MyGW"
```

Opération *delconf*

L'opération *delconf* supprime un champ présent dans une section particulière d'un fichier de configuration. Si le champ n'est pas précisé, la section complète est supprimée du fichier de configuration.

Format

```
"serial | any", delconf, "file", "section", "field"
"serial | any", delconf, "file", "section"
```

EXEMPLES

```
SN310A00000000Z, delconf, wiki, Global, Schedule
any, delconf, dns, client
```

Opération *setglobal*

L'opération *setglobal* modifie la valeur d'un champ présent dans une section particulière du fichier global de configuration (fichier ~/System/global.custom).

Notez que pour être prise en compte, une modification de configuration par la commande *setglobal* nécessite un redémarrage manuel du firewall.

L'utilisation de cette commande déclenche l'écriture d'un avertissement dans le fichier de logs.

Format

```
"serial | any", setglobal, "section", "field", "value"
```

EXEMPLE

```
SN310A00000000Z, setglobal, ASQ, BridgeLimit, 9
```

Opération *sethostname*

Cette opération est disponible à partir de la version SNS 3.10.2 ou 4.1.1.

L'opération *sethostname* modifie la valeur des champs suivants du fichier global de configuration (fichier ~/System/global) :

- SystemName : correspond au nom du firewall. En cas d'utilisation de la Haute Disponibilité (HA), correspond au nom système du cluster HA.
- SystemNodeName : correspond au nom local du nœud système, permettant de le distinguer parmi les autres nœuds du cluster HA.

Notez que pour être prise en compte, une modification de configuration par la commande *sethostname* nécessite un redémarrage manuel du firewall.

Format

```
"serial | any", sethostname, "systemname"
"serial | any", sethostname, "systemname", "systemnodename"
```

EXEMPLE

```
any, sethostname, test_hostname, testnodename
```

Opération *createHA*

Cette opération permet d'initialiser un cluster de firewalls. Elle requiert que le firewall auquel elle est appliquée dispose de la licence HA avec l'option Master.

Le masque réseau utilisé pour le lien HA doit accepter au moins trois adresses IP (en notation CIDR : masque réseau strictement inférieur à 30).

Format

```
"serial | any", createHA, "IP_HA_master", "mask", "interface_name",
"password"
"serial | any", createHA, "IP_HA_master", "mask", "interface_name",
"password", "IP_HA_master_backup", "mask_backup", "interface_name_backup"
```

Paramètre	Description
IP_HA_master	Adresse IP affectée à l'interface "interface_name" (dédiée au lien HA principal).
mask	Masque réseau de l'interface "interface_name".
interface_name	Nom donné à l'interface dédiée au lien HA principal.
password	Clé pré-partagée pour sécuriser la connexion entre les membres du cluster.
IP_HA_master_backup	Adresse IP affectée à l'interface "interface_name_backup" (interface dédiée au lien HA de secours).

Paramètre	Description
mask_backup	Masque réseau de l'interface "interface_name_backup".
interface_name_backup	Nom donné à l'interface dédiée au lien HA de secours.

EXEMPLES

```
SN310A00000000Z, createHA, 192.168.192.5, 255.255.255.248, HA,
PasswordValue
SN310A00000000Z, createHA, 192.168.192.5, 255.255.255.248, HA,
PasswordValue, 192.168.192.11, 255.255.255.248, HA2
```

Opération *joinHA*

Cette opération permet à un firewall de rejoindre un cluster. Elle requiert que ce cluster soit déjà initialisé et que les interfaces réseau dédiées à la HA soient physiquement connectées (firewalls actif et passif).

Dans le cadre d'un échange de matériel (RMA), le firewall échangé doit au préalable être retiré du cluster grâce aux commandes CLI / Serverd suivantes :

```
ha cluster remove serial="remote"
ha cluster activate
```

Pour plus d'informations concernant la syntaxe de ces commandes, veuillez vous référer au Guide de référence des commandes CLI / Serverd SNS v3 ou Guide de référence des commandes CLI / Serverd SNS v4.

L'opération *joinHA* utilise une troisième adresse IP, temporaire, pour la phase de connexion au firewall principal du cluster.

Format

```
"serial | any", joinHA, "IP_HA_1", "IP_HA_2", "IP_HA_join", "mask",
interface_name", "password"
"serial | any", joinHA, "IP_HA_1", "IP_HA_2", "IP_HA_join", "mask",
interface_name", "password", "IP_HA_join_backup", "mask_backup",
"interface_name_backup"
```

Paramètre	Description
IP_HA_1	Première adresse IP distante testée pour joindre le cluster.
IP_HA_2	Deuxième adresse IP distante testée pour joindre le cluster si IP_HA_1 n'a pas répondu, ou adresse IP affectée à l'interface "interface_name" (interface dédiée à la HA) si le firewall principal a pu être joint sur IP_HA_1.
IP_HA_join	Adresse IP utilisée temporairement par le firewall pour joindre le cluster.
mask	Masque réseau de l'interface "interface_name".
interface_name	Nom donné à l'interface dédiée au lien HA principal.
password	Clé pré-partagée pour sécuriser la connexion entre les membres du cluster.
IP_HA_join_backup	Adresse IP affectée à l'interface "interface_name_backup" (interface dédiée au lien HA de secours).
mask_backup	Masque réseau de l'interface "interface_name_backup".

Paramètre	Description
interface_name_backup	Nom donné à l'interface dédiée au lien HA de secours.

EXEMPLES

```
SN310B00000000Z, joinHA, 192.168.192.4, 192.168.192.5, 192.168.192.6,
255.255.255.248, HA, PasswordValue
SN310B00000000Z, joinHA, 192.168.192.4, 192.168.192.5, 192.168.192.6,
255.255.255.248, HA, PasswordValue, 192.168.192.12, 255.255.255.248, HA2
```

IMPORTANT

La clé USB doit être retirée au moment du redémarrage du firewall rejoignant le cluster (lors de la phase de synchronisation de configuration).

Opération *initTPM*

Cette opération est disponible à partir de la version SNS 3.10.1 ou 4.0.1.

Elle initialise le module matériel TPM en définissant son mot de passe dans un argument, et si le firewall est membre d'un cluster (Haute disponibilité activée), de dériver la clé depuis le mot de passe du TPM afin que les deux firewalls disposent d'une clé identique.

Le mot de passe du TPM doit respecter la politique de mots de passe paramétrée dans la configuration (fichier ~/ConfigFiles/serverd section PasswordPolicy).

Cette opération doit être réalisée avant d'essayer de protéger une clé privée sur le TPM.

Format

```
"serial | any", initTPM, "tpmpassword"
```

EXEMPLE

```
SN310A17B0023A7, initTPM, TpmPasswordValue
```

Opération *p12import*

Cette opération est disponible à partir de la version SNS 3.10.1 ou 4.0.1.

Elle permet d'importer des fichiers PKCS#12 au format .p12. Si un fichier n'est pas protégé par un mot de passe, le champ "p12password" doit rester vide. Le paramètre "ondisk" permet de choisir de protéger la clé privée contenue dans un fichier PKCS#12 en la stockant sur le TPM.

Le TPM doit être initialisé avant d'être utilisé pour protéger une clé privée.

Format

```
"serial | any", p12import, none|ondisk, "p12file", "p12password"
```

EXEMPLES

```
SN310A00000000Z, p12import, none, file1.p12, file1PwdValue
SN310A00000000Z, p12import, none, file2.p12
SN310A00000000Z, p12import, ondisk, file3.p12, file3PwdValue
SN310A00000000Z, p12import, ondisk, file4.p12
```

Opération *crlimport*

Cette opération est disponible à partir de la version SNS 4.8.0.

Cette opération permet d'importer sur le firewall une liste de révocation de certificats (CRL).

Le fichier contenant la CRL doit être au format :

- PEM (format ASCII - Encodage des données en Base64),
  - ou -
- DER (format binaire).

Format

```
"serial | any", crlimport, "filename", "pem | der"
```

EXEMPLES

```
any, crlimport, mycrl.pem, pem
SN310A00000000Z, crlimport, mycrl.der, der
```

Opération *certimport*

Cette opération est disponible à partir de la version SNS 4.8.0.

Cette opération permet d'importer sur le firewall un certificat ou une autorité de certification (CA).

Le fichier du certificat ou de l'autorité de certification doit être au format :

- PEM (format ASCII - Encodage des données en Base64),
  - ou -
- DER (format binaire).

Format

```
"serial | any", certimport, "filename", "pem | der"
```

EXEMPLES

```
any, certimport, myca.pem, pem
SN310A00000000Z, certimport, mycert.der, der
```

Préparer la clé USB

Pour la configuration initiale de firewalls à partir d'une clé USB, Stormshield vous recommande fortement d'utiliser des clés USB sécurisées (code PIN intégré à la clé pour la déverrouiller) de type Kingston Data Traveler.

Formater la clé

La clé USB doit contenir une partition unique, formatée selon le système de fichier FAT32.

Copier les fichiers nécessaires

Selon les opérations à réaliser, copiez les fichiers à la racine de la clé USB :

- Licences (.licence),
- Mise(s) à jour logicielle (.maj),
- Sauvegarde(s) de configuration (.na),
- Package(s) de rattachement SMC (.pack),
- Certificat(s) au format PKCS#12 (.p12),
- Fichiers contenant le mot de passe du compte *admin* (.pwd),
- Fichiers contenant la configuration de routage dynamique (.bird, .bird6),
- Fichiers de configuration additionnelle (.csv).

Réaliser la configuration initiale

La configuration initiale d'un firewall via une clé USB ne demande aucune intervention de l'opérateur sauf :

- Pour déverrouiller la clé USB si celle-ci est sécurisée,
- Pour saisir les mots de passe des certificats lorsque des certificats sont importés lors de la configuration via USB,
- Pour retirer la clé USB et la réinsérer lorsque cela est nécessaire.

Pour réaliser la configuration initiale :

1. Vérifiez que le firewall est hors tension.
2. Si le firewall est destiné à joindre un cluster, vérifiez que toutes ses interfaces réseau dédiées à la HA sont connectées au firewall Master.
3. Insérez la clé dans le port USB du firewall.
4. Mettez le firewall sous tension.
   Le firewall exécute et installe automatiquement les fichiers qui lui sont destinés selon la séquence décrite dans la section **Séquence d'installation**.
   Il redémarre uniquement après chaque mise à jour logicielle.
5. Si des opérations de configuration ont été réalisées à l'aide de commandes *setglobal* incluses dans un fichier CSV, redémarrez manuellement le firewall pour prendre en compte les modifications.
6. Lorsque toutes les étapes de configuration sont terminées, le firewall est opérationnel.
   - Vous pouvez-vous connecter à l'interface d'administration du firewall directement (*https://adresse_IP_firewall/admin*) ou via Stormshield Management Center si le firewall est rattaché à un serveur SMC,
   - Les opérations réalisées lors de la configuration initiale du firewall, sauf les éventuels imports de licences et mises à jour de firmware, sont enregistrées dans un fichier de log créé à la racine de la clé USB et nommé *<firewall_serial_number_staging>.log*.

Pour aller plus loin

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

documentation@stormshield.eu