NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

CONFIGURATION INITIALE PAR CLÉ USB

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

Date : 09 décembre 2019

Référence : sns-fr-configuration_initiale_par_cle_usb_note_technique

Table des matières

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

Depuis la version 3.9, des améliorations existent quant aux possibilités de configuration initiale d'un firewall SNS via une clé USB : import de certificats au format PKCS#12, import du mot de passe du compte *admin*, exécution de commandes de configuration additionnelle (fichiers au format CSV) permettant, entre autres, de construire un cluster Haute Disponibilité.

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

1. Licence (extension ".licence").
2. Mise à jour de firmware (extension ".maj").
   Redémarrage du firewall.
3. Fichier de sauvegarde de configuration (extension ".na").
4. Package de rattachement à un serveur SMC (extension ".pack").
5. Certificats (extension ".p12").
6. Mot de passe du compte *admin* (extension ".pwd").
7. Fichiers de configuration additionnelle (extension ".csv").

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

Préparer les fichiers

Une seule clé USB pouvant être utilisée pour la configuration initiale de plusieurs firewalls, plusieurs fichiers d'une même catégorie peuvent ainsi être présents sur cette clé.

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

Licences

Chaque firewall dispose d'un fichier de licence qui lui est propre. Ces fichiers sont disponibles dans votre espace client MyStormshield, menu **Produit** > **Gestion des Produits**.

Un fichier licence destiné à une installation via clé USB est obligatoirement nommé *Firewall_Serial_Number*.licence.

Exemple : SN310A00000000Z.licence.

Mises à jour logicielle

Les fichiers de mise à jour logicielle sont disponibles dans votre espace client MyStormshield, menu **Téléchargements** > **Stormshield Network Security** > **Firmware** > **4.X** > **Stormshield Network Security - Firmware - V 4.0.0** (ou version supérieure).

Ces fichiers portent l'extension ".maj".

Exemple : fwupd-4.0.0-SNS-armv6-S.maj

Lorsque plusieurs firewalls doivent être configurés à l'aide d'une même clé USB, plusieurs fichiers de mise à jour logicielle peuvent être nécessaires (architectures firewalls différentes, versions logicielles préchargées différentes...).

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

Les fichiers de sauvegardes de configuration peuvent être créés depuis le module **Configuration** > **Système** > **Maintenance**, sur l'onglet *Sauvegarder* de l'Interface Web d'Administration d'un firewall en activité.

Si la configuration destinée à être chargée sur les firewalls est générique, le fichier de sauvegarde peut être nommé *default.na*. S'il est différent pour les firewalls à configurer via la clé USB, chaque fichier de sauvegarde doit être nommé : *Firewall_Serial_Number.licence*.

Exemple : SN310A00000000Z.licence, SN310B00000000Z.na.

Packages de rattachement SMC

Si le firewall est destiné à être administré depuis un serveur Stormshield Management Center, un package de rattachement doit être généré depuis le serveur SMC.

Vérifiez avant l'export que le package de rattachement du firewall n'inclut pas de configuration réseau si vous ne souhaitez pas écraser une configuration réseau précédemment restaurée à l'aide d'un fichier .na.

Les packs de rattachement sont nommés *Firewall_Serial_Number.pack*.

Exemple : SN310A00000000Z.pack, SN310B00000000Z.pack.

Pour utiliser un seul package de rattachement pour plusieurs firewalls, ce fichier doit être nommé *default.pack*.

Certificats

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.

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".

Exemple : SN310A00000000Z.p12., SN310A00000000Z_cert1.p12., SN310A00000000Z_cert2.p12, SN310B00000000Z.p12.

Mots de passe du compte *admin*

Il s'agit d'un fichier texte contenant une seule chaîne, non chiffrée, et au format UTF-8 : le mot de passe du compte *admin* à déployer sur le firewall.

La taille du mot de passe doit être comprise entre 5 et 128 caractères. Le mot de passe doit également respecter les caractères autorisés / interdits pour les mots de passe : dans le cas contraire, la connexion au firewall avec le compte *admin* ne fonctionnera pas.

Si le mot de passe précisé dans le fichier ne respecte pas la politique de mots de passe qui aurait été restaurée à l'aide d'un fichier de sauvegarde de configuration, ce mot de passe n'est pas pris en compte.

Si ce mot de passe est identique pour tous les firewalls à configurer via la clé USB, le fichier le contenant doit être nommé *default.pwd*. Si le mot de passe du compte *admin* diffère d'un firewall à l'autre, le nom de chaque fichier contenant le mot de passe est alors composé du numéro de série du firewall avec l'extension .pwd.

Exemple : SN310A00000000Z.pwd, SN310B00000000Z.pwd.

Fichiers de configuration additionnelle

Des commandes de configuration complémentaire peuvent être exécutées via un ou plusieurs fichiers au format CSV (champs séparés par des virgules) au format UTF-8.

Ces fichiers permettent notamment de construire un cluster de firewalls opérationnel.

Il est important de noter que **tous** les fichiers CSV présents sur la clé USB seront exécutés lors de la configuration du firewall.

Les opérations autorisées et la structure du fichier de configuration additionnelle sont détaillées ci-après.

Structure générale d'une opération

Dans un fichier de configuration additionnelle au format CSV, une ligne d'opération est définie selon la nomenclature suivante :

"serial | any" ,"operation" [, "paramètre 1", ...]

Avec :

- serial : le N° de série du firewall auquel s'applique la ligne de configuration,
- any : indique que l'opération doit être appliquée quel que soit le firewall.

Des lignes de commentaires, commençant par le caractère "#", peuvent être insérées dans ce fichier.

Opération *setconf*

L'opération *setconf* peut être utilisée pour :

- Fixer la valeur d'un champ présent dans une section particulière d'un fichier de configuration,
- A partir de la version SNS 3.10.0 : 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 parenthèses.

Fixer la valeur d'un champ

Format

"serial | any", setconf, "fichier", "section", "champ", "valeur"

Exemples

any, setconf, network, ethernet0, Protected, 0

any, setconf, object, Host, gateway, "192.168.0.254, resolve=static"

Ajouter une ligne complète (à partir de la version SNS 3.10.0)

Format

"serial | any", setconf, "fichier", "section", "ligne"

Exemple

any, setconf, Global/VPN/03, StaticRoutes, "global_nmc_ntp,M2P3->global_taira02_gw1"

Opération *delconf*

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

Format

"serial | any", delconf, "fichier", "section", "champ"

"serial | any", delconf, "fichier", "section"

Exemples

SN310A000000000Z, delconf, wiki, Global, Schedule

any, delconf, dns, client

Opération *setglobal*

L'opération *setglobal* fixe 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", "champ", "valeur"

Exemples

SN310A000000000Z, setglobal, ASQ, BridgeLimit, 9

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"

Avec :

- "IP_HA_master" : adresse IP affectée à l'interface "interface_name" (interface 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),
- "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

SN310A000000000Z, createHA, 192.168.192.5, 255.255.255.248, HA, *PasswordValue*

SN310A000000000Z, 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 existant :

- Le cluster doit avoir été initialisé auparavant,
- Les interfaces réseau dédiées à la Haute Disponibilité doivent être physiquement connectées (firewalls actif et passif).

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"

Avec :

- "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",
- "interface_name_backup" : nom donné à l'interface dédiée au lien HA de secours.

Exemples

SN310B000000000Z, joinHA, 192.168.192.4, 192.168.192.5, 192.168.192.6, 255.255.255.248, HA, PasswordValue

SN310B000000000Z, 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

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 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.

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 Généralités.
   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 son interface Web d'Administration 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*.

documentation@stormshield.eu