

Fiche 1 – Initialiser un pare-feu SNS

Table des matières

I Procédure de remise à zéro des pare-feu SNS.....	1
II Configuration initiale.....	2

I Procédure de remise à zéro des pare-feu SNS

Cette procédure ne doit évidemment être déroulée que sur un SNS qui aurait déjà été configuré.

Un RAZ du pare-feu peut être fait via la console (sur les VM ou les boîtiers physiques), ceci nécessite un redémarrage (reboot). **Sur les boîtiers physiques** : un appui sur le bouton *reset* pour les boîtiers physiques permet de restaurer la configuration d'usine et redémarrer en bridge sur toutes les interfaces.

Vous pouvez faire le choix de réinitialiser un boîtier physique via l'accès console. Pour cela, installer le driver du câble console sur Windows¹ : <https://ftdichip.com/drivers/vcp-drivers/>. Lancer un logiciel permettant l'accès console (Putty, Teraterm, minicom) et utilisant en débit **115200**.

```
ASQ Initialization...Done

Pattern checking...Done

Starting daemons... logd monitord hardware asqd userreqd modem service dns ldap
voucher filter network dialup ha snmp bird ipsec sl openvpn antivirus dhcp ntp
smcrouting event cad thind alived telemetryd hostapd.

SN210W16K0683A7: FW SN210W (S / EUROPE)
Firewall software version 4.0.2 RELEASE

port      name      NS-BSD  state  addressIPv4      addressIPv6
  1        out      mvneta0 no-link 10.0.0.254/8
  2        in      mvneta2 up      10.0.0.254/8
  3      dmz1      mvnetal no-link 10.0.0.254/8

System is now ready.

NS-BSD/arm (SN210W16K0683A7) (ttyu0)
```

Sur une VM :

- ☑️ démarrer (ou redémarrer) la machine virtuelle et s'authentifier pour accéder à la console en administrateur ;
- ☑️ saisir la commande **defaultconfig -f -r -p -c -L**.

Pour installer le pare-feu sur une KVM de Proxmox, suivre la fiche « Installer une VM SNS sur Proxmox » (fichier installerSNSsurProxmox.pdf).

Pour installer le pare-feu sur VirtualBox ou vmWare, suivre la documentation de Stormshield.

Sur une VM, faire en sorte qu'une des interfaces « in » se trouve connectée à un réseau logique sur lequel est également connecté (ou peut être connecté) un poste de travail permettant de procéder à la première configuration.

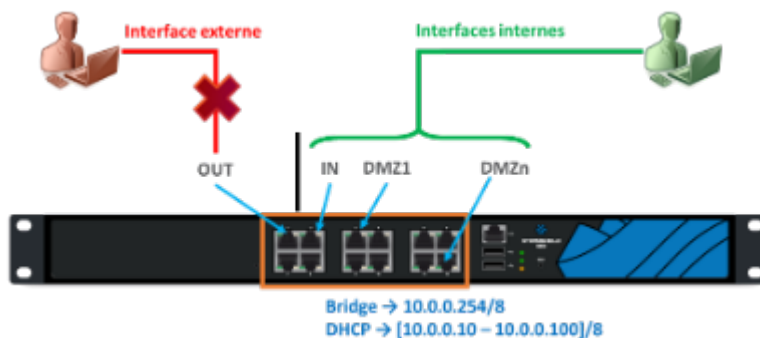
¹ https://documentation.stormshield.eu/SNS/v4/fr/Content/Software_Recovery_via_USB_key/SN150-SN160-SN160W-SN210-SN210W-SN310.htm

II Configuration initiale

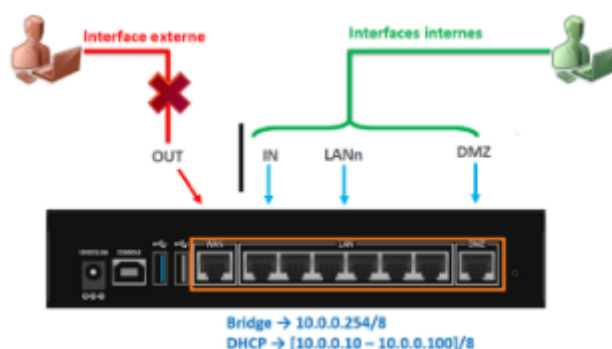
La configuration d'usine par défaut du *pare-feu* SNS (boîtier ou appliance VM laboratoire) est la suivante. Dans une configuration usine, notamment pour les machines virtuelles et les modèles SN310, la première interface **(1)** du pare-feu SNS physique est nommée « **OUT** », la seconde « **IN** » et le reste des interfaces « **DMZx** ». L'interface « **OUT** » est une interface **externe**, utilisée pour connecter le pare-feu SNS à internet et le reste des interfaces sont **internes** et servent principalement à connecter le pare-feu SNS à des réseaux locaux.



La distinction interne/externe pour les interfaces permet de se protéger contre les attaques d'usurpation d'adresse IP.



Le schéma présenté ci-dessous correspond, quant à lui, à un boîtier SN210. Comme vous pouvez le constater, l'organisation des interfaces est différente de celle des machines virtuelles ou des modèles SN310 et supérieur.



Pour initialiser le pare-feu, il faut se brancher sur l'interface « **IN** ».

En configuration usine, sur un **boîtier physique** de type SN210 ou SN310, **toutes les interfaces sont incluses dans un bridge** dont l'adresse est 10.0.0.254/8. Sur les **boîtiers physiques**, un serveur DHCP est actif sur toutes les interfaces du bridge et il distribue des adresses IP comprises entre 10.0.0.10 et 10.0.0.100. L'accès à l'interface web de configuration du pare-feu SNS se fait avec l'url : **https://10.0.0.254/admin**.

Sur le boîtier

Par défaut, seul le compte système **admin** (mot de passe par défaut **admin**), disposant de tous les privilèges sur le boîtier, existe et peut se connecter.

Sur une VM

La configuration usine lance un dialogue de pré-configuration qui demande de changer le mot de passe par défaut, de configurer vos interfaces, le clavier de la console, etc :

Un premier écran propose un choix qu'il n'est pas nécessaire de valider, le système continue automatiquement :

```
SeaBIOS (version rel-1.14.0)
Machine UUID 9c577cd1-57de-
Booting from Hard Disk...

>> FW
1) main
2) backup
choose:
```

Un premier redémarrage automatique est fait et la configuration continue :

```
Pattern checking...Done

Starting daemons... logd monitord hardwared asqd userreqd modem service dns ldap
voucher filter network dialup ha snmp bird ipsec sl openvpn antivirus dhcp ntp
smcrouting event cad thind alived telemetryd.
Setting boot partition to Main
No BACKUP partition found
mount_cd9660: /dev/cd0: No such file or directory

#####
## Configure keyboard mapping ##
#####

Current keyboard Mapping: us.iso

The available choices are:
  1 - ch
  2 - de
  3 - es
  4 - fr
  5 - it
  6 - pl
  7 - us
Select your keyboard mapping number: █
```

➤ Sélectionner 4 pour fr (sur le clavier le chiffre 4 sans utiliser la touche Maj).

```
New keyboard mapping is fr

#####
## Change SRP/SSH password for admin ##
#####
setting password for admin
enter password: █
```

➤ Saisir un mot de passe de 8 caractères minimum avec Maj/min/chiffre/caractères spéciaux. Pour éviter les soucis de clavier américain sur certaines consoles d'hyperviseur, utilisez par exemple Sio2022* puis confirmez.

```
#####
## Change SRP/SSH password for admin ##
#####
setting password for admin
enter password:
verify:
Modify SRP/SSH password of user 'admin' successful
```

Passons à la configuration des interfaces réseau :

```
Current network settings:
  1st interface (out): DHCP
  2nd interface (in): DHCP

Change 1st network interface (out) settings ? [y;N]:
```



Même si plusieurs interfaces ont été ajoutées sur l'hyperviseur (Proxmox, VirtualBox ou VmWare), seulement 2 sont modifiables via l'assistant du démarrage.

Les interfaces peuvent être laissées en DHCP ou être configurées via une adresse IP fixe.



Sachant qu'il est déconseillé d'administrer le pare-feu via l'interface OUT, l'idée est de configurer l'interface **IN** de manière à ce qu'elle se trouve connectée à un réseau logique sur lequel est également connecté (ou peut être connecté) un poste de travail permettant de procéder à l'administration du Stormshield.

Lors de cette configuration, le paramétrage pourra être, bien sûr, modifiée et, par exemple, une autre interface pourra être dédiée à l'administration.

Pour ce premier démarrage

- Laisser l'interface **OUT** en DHCP même si aucun serveur DHCP n'est relié au réseau ⇒ répondre « n » ou E
- Laisser l'interface **IN** en DHCP uniquement s'il y a un serveur DHCP sur le réseau sinon répondre « y » pour mettre une adresse IP accessible via le réseau. Par exemple :

```
#####
## Configure initial network connection ##
#####

Current network settings:
 1st interface (out): DHCP
 2nd interface (in): DHCP

Change 1st network interface (out) settings ? [y|N]: N
Change 2nd network interface (in) settings ? [y|N]: y
- IP addresses must be expressed in dotted-decimal notation
  (4 sets of numbers from 0 to 255 separated by dots).
- Netmask addresses must be expressed in dotted-decimal or CIDR notation
  (A number between 1 and 32 included).
- Example IP: 10.2.0.1 or DHCP
- Example Netmask: 255.255.0.0 or 16

IP address (without subnet): 192.168.90.230
Subnet mask: 255.255.255.0
```

Répondre « n » sur la dernière question, en effet il n'est pas recommandé d'autoriser l'administration sur votre interface **OUT**.

```
Will you configure your virtual appliance through its first interface (out) ?
[Y/n]: n
```

Votre système est installé avec les valeurs rappelées ci-dessus, vous pouvez tester que la configuration du clavier a bien été prise en compte en saisissant votre login/mdp.

```
UMSNSX00Z0000A0: FW EVA1 (XL / EUROPE)
Firewall software version 4.3.5
UM-RELEASE

port      name      NS-BSD   state  addressIPv4      addressIPv6
  1        out      vtnet0   up     169.254.240.103/16
  2        in       vtnet1   up     192.168.90.230/24

System is now ready.

NS-BSD/amd64 (UMSNSX00Z0000A0) (ttyv0)
login: █
```



L'interface d'administration est accessible à l'adresse <https://@IP-IN/admin/> à partir d'un poste sur le même réseau.



Basculer sur la fiche n°2 pour une première configuration du boîtier ou de la VM.