

Commandes utiles de console (ou en ssh) des Pare-feu SNS

Table des matières

I Réinitialiser le pare-feu (VM) avec la commande defaultconfig.....	1
II Principe de la modification de la configuration.....	1
III Divers.....	2

I Réinitialiser le pare-feu (VM) avec la commande defaultconfig

defaultconfig

Usage: [options]

- f: Force
- r: Reboot after defaultconfig
- D: Only Restore the data partition
- p: Reset password
- u: Check usb token boot restoration
- d: Dump root partition after defaultconfig
- k: Keep autoupdate data (Pattern, Pvm, Clamav, Kaspersky, URLFiltering), default SSL proxy authority, default sslvpn full authority and ssh host keys
- l: Keep network configuration file
- n: Do not mark firewall as having a defaultconfig configuration
- c: No backup files (.old)
- L: Remove logs
- s: Safe mode. Restore network configuration with only first interface enabled.
- t: Reset TPM (TPM password required)
- taper defaultconfig -f -r -p -c -L pour redémarrer en configuration usine.

II Principe de la modification de la configuration

La configuration du pare-feu se trouve dans le dossier ConfigFiles. Il est possible **d'intervenir directement dans les fichiers** (des exemples sont très souvent présents).

Une fois la modification réalisée, il est nécessaire de recharger la configuration. Là aussi, cela suit un même principe : la commande commence par « en », en saisissant ces 2 lettres et en « tabulant », on dispose de l'ensemble des commandes qui sont dans /usr/Firewall/sbin. Il faut bien sûr lancer la commande correspondante à la modification opérée.

Par exemple, pour modifier l'adresse IP d'une interface :

- vi ConfigFiles/network ⇒ Modification des paramètres souhaités à l'aide de vi. Définition des principaux paramètres sous le nom de section de l'interface ([ethernet0]) :
 - State = 1 ou 0 Connectivité de l'interface activée ou non
 - Media = 0 à 6 Définit la vitesse de média (0 = auto-négociation)
 - Protected = 1 ou 0 Interface protégée ou non (anti-spoofing sur des interfaces internes)
 - Address
 - Mask
 - Gateway

- Sauvegarder les modifications.

- Il suffit ensuite de recharger les configurations : **ennetwork**

Un ifconfig permet de valider la prise en compte des nouveaux paramètres.

Pour modifier la politique de filtrage

- vi ConfigFiles/Filter/num_politique ⇒ Modification souhaitée (par exemple suppression d'une règle ou désactivation d'une règle en mettant un «off » devant).
- Recharger la configuration : enfilter -u

À noter que

- **enfilter 10** permet de repasser sur la configuration par défaut pass all en cas de perte d'accès au pare-feu par exemple.

Pour désactiver le VPN : envpn 00

Remarque : envpn -u sans modification de l'emplacement ne fait RIEN.

III Divers

En cas de blocage d'une machine par le pare-feu

Si le pare-feu détecte une tentative d'usurpation d'adresse IP sur le bridge, il bloquera tout le trafic généré par la machine connectée sur l'interface **OUT**, **il est alors nécessaire de** modifier l'adresse IP de la machine cliente :

1) changer l'IP de la machine client

2) en mode console directe, purger l'IP de la machine pour la faire « oublier » de la table des hôtes :

sfctl -F state -H host=@IP

Pour voir les règles de pare-feu implicites générées (ACL) : sfctl -s filter