



CONFIGURATIONS DE BASE EN INTERFACE LIGNE DE COMMANDE (CLI)

Produits concernés: SNS 3.x, SNS 4.x

Dernière mise à jour du document : 13 janvier 2021

Référence : sns-fr-configuration_de_base_cli_note_technique



Table des matières

Avant de commencer	4
Utiliser l'interface en ligne de commande	4
Administration du firewall	5
Afficher l'aide des commandes et de leurs arguments	
Récupérer les droits d'écriture	
·	
Restaurer la configuration usine Injecter une licence	
,	
Syntaxe console	
Syntaxe script	
Sauvegarder toute la configuration	
Syntaxe console	
Syntaxe script Postauror touto la configuration	
Restaurer toute la configuration	
Syntaxe console	
Syntaxe script Mettre à jour le firewall	
Syntaxe console	
Syntaxe script Activer l'accès SSH avec utilisation de mot de passe	
Désactiver l'accès SSH	c
Autoriser une adresse IP publique d'accès à l'interface web	
Advoliser dire adresse ir publique d'acces à l'interface web	U
Gestion des objets réseaux	7
Objet Machine	7
Créer un objet Machine	
Supprimer un objet Machine	7
Objet Réseau	7
Créer un objet Réseau	7
Supprimer un objet Réseau	7
Objet Plage d'adresses IP	8
Créer un objet Plage d'adresses IP	
Supprimer un objet Plage d'adresses IP	8
Objet Port	
Créer un objet Port	8
Supprimer un objet Port	
Objet Plage de ports	
Créer un objet Plage de ports	
Supprimer un objet Plage de ports	
Objet Routeur	
Créer un objet Routeur	
Supprimer un objet Routeur	
Objet Groupe	
Créer un objet Groupe	
Ajouter un objet au groupe	
Supprimer un objet Groupe	
Objet Protocole IP	
Créer un objet Protocole IP	
Supprimer un objet Protocole IP	
Objet Groupe de ports	10

Page 2/20



Créer un objet Groupe de ports	
Ajouter un objet au groupe	
Supprimer un objet Groupe de ports	
Objet Groupe de régions	
Créer un objet Groupe de régions	
Ajouter un objet au groupe	
Supprimer un objet Groupe de régions Objet Temps	
Créer un objet Temps	
Supprimer un objet Temps	
Configuration réseau	
Configurer une interface Ethernet	
Adresse IP statique	
Adresse IP dynamique	
Créer un bridge	
Adresse IP statique	
Adresse IP dynamique	
Modifier un bridge	
Supprimer un bridge	
Configurer up a route statisme	
Configurer une route statique Créer une route statique	
Supprimer une route statique	
Configurer les serveurs DNS utilisés par le firewall	
Ajouter un serveur DNS	
Supprimer un serveur DNS	
Règles de filtrage	
Activer une politique de filtrage ou de NAT	
Ajouter une règle de filtrage	
Modifier une règle filtrage	
Désactiver une règle de filtrage	
Supprimer une règle de filtrage	15
Règles de translation	16
Ajouter une règle de translation	16
Translation dynamique	16
Translation statique par port	
Translation statique	
Modifier une règle de translation	
Désactiver une règle de translation	
Supprimer une règle de translation	17
Gestion des utilisateurs dans la base LDAP interne	18
Créer une base LDAP interne	18
Créer un utilisateur	
Supprimer un utilisateur	
Créer un groupe d'utilisateurs	
Ajouter un utilisateur à un groupe	
Pour aller plus loin	19

Page 3/20



Avant de commencer

Les firewalls Stormshield Network Security embarquent une interface en ligne de commandes (CLI) constituée d'un jeu de commandes propriétaire. Les commandes sont accessibles via un shell et elles permettent de configurer et de superviser toutes les fonctionnalités du firewall.

Ce document présente les commandes CLI nécessaires pour configurer les fonctionnalités de base d'un firewall. L'ensemble des commandes et de leurs arguments est détaillé dans le document Stormshield Network Security - CLI Serverd Commands Reference Guide.

Utiliser l'interface en ligne de commande

L'accès au shell CLI se fait via un protocole sécurisé NSRPC (NETASQ Secure Remote Procedure Call) :

- En local sur le firewall (ligne de commande et interface web),
- A distance à partir d'une machine en utilisant des exécutables dédiés sous Windows et Linux.

Les commandes CLI peuvent être regroupées dans un fichier texte pour former un script CLI qui peut être, à son tour, exécuté en local ou à distance.



Pour consulter toutes les méthodes d'accès au shell CLI et la procédure à suivre pour l'écriture et l'exécution des scripts, veuillez vous référer au module E-learning CLI ACCESS & SCRIPTS.





Administration du firewall

Afficher l'aide des commandes et de leurs arguments

HELP

Utilisez la commande HELP comme argument d'une commande pour afficher de l'aide sur les arguments de la commande.

Récupérer les droits d'écriture

MODIFY ON FORCE

Restaurer la configuration usine

SYSTEM DEFAULTCONFIG

Cette commande ne réinitialise pas le mot de passe de l'utilisateur admin.

Injecter une licence

Syntaxe console

SYSTEM LICENCE UPLOAD < U70SXA02J2681A7.licence

Syntaxe script

SYSTEM LICENCE UPLOAD \$FROM DATA FILE ("U70SXA02J2681A7.licence")

Sauvegarder toute la configuration

Syntaxe console

CONFIG BACKUP list=all [password=mot de passe] > mybackup.na

Syntaxe script

CONFIG BACKUP list=all [password=mot_de_passe] \$SAVE_TO_DATA_FILE
("mybackup.na")





Restaurer toute la configuration

Syntaxe console

```
CONFIG RESTORE list=all [password=mot de passe] < mybackup.na
```

Syntaxe script

```
CONFIG RESTORE list=all [password=mot de passe] $FROM DATA FILE
("mybackup.na")
```

Mettre à jour le firewall

Syntaxe console

```
SYSTEM UPDATE UPLOAD < fwupd-2.2.0-NETASQ-amd64-M-VM-NETASQ.maj
SYSTEM UPDATE ACTIVATE
```

Syntaxe script

```
SYSTEM UPDATE UPLOAD $FROM DATA FILE("fwupd-2.2.0-NETASQ-amd64-M-VM-
NETASQ.maj")
SYSTEM UPDATE ACTIVATE
```

Activer l'accès SSH avec utilisation de mot de passe

```
CONFIG CONSOLE SSH state=1 userpass=1 port=ssh
CONFIG CONSOLE ACTIVATE
```

Désactiver l'accès SSH

```
CONFIG CONSOLE SSH state=0
CONFIG CONSOLE ACTIVATE
```

Autoriser une adresse IP publique d'accès à l'interface web

```
CONFIG WEBADMIN ACCESS ADD PUBLIC IP
CONFIG WEBADMIN ACTIVATE
```

PUBLIC IP est un objet machine mais il peut être un objet réseau, une plage d'adresses IP, ou l'objet any.





Gestion des objets réseaux

Cette section décrit comment créer ou supprimer des objets.

Pour modifier un objet, utilisez les mêmes commandes que pour sa création et ajoutez le paramètre *update=1* :

Exemple pour modifier un objet Machine :

```
CONFIG OBJECT HOST NEW name=DNS_SRV comment="DNS Server" ip="192.168.250.152" resolve=static mac="" update=1 CONFIG OBJECT ACTIVATE
```

Objet Machine

Créer un objet Machine

• Nom : DNS SRV,

Commentaire: DNS Server,
Adresse IP: 192.168.250.150,
Adresse MAC: 0A:00:27:00:00:28.

CONFIG OBJECT HOST NEW name=DNS_SRV comment="DNS Server" ip="192.168.250.150" resolve=static mac="0A:00:27:00:00:28" CONFIG OBJECT ACTIVATE

Supprimer un objet Machine

```
CONFIG OBJECT HOST DELETE name=DNS_SRV force=1
```

Objet Réseau

Créer un objet Réseau

Nom: VPN NET,

Commentaire : VPN Network,Adresse réseau : 192.168.1.0/24.

CONFIG OBJECT NETWORK NEW name=VPN_NET comment="VPN Network" ip=192.168.1.0 mask=255.255.255.0 CONFIG OBJECT ACTIVATE

Supprimer un objet Réseau

CONFIG OBJECT NETWORK DELETE name=VPN NET force=1





Objet Plage d'adresses IP

Créer un objet Plage d'adresses IP

• Nom: DHCP LAN RANGE,

· Commentaire: DHCP LAN RANGE,

Début : 192.168.250.100,Fin : 192.168.250.200.

CONFIG OBJECT HOST NEW name=DHCP_LAN_RANGE comment="DHCP LAN RANGE"

begin=192.168.250.100 end=192.16 $\overline{8}$.25 $\overline{0}$.200

CONFIG OBJECT ACTIVATE

Supprimer un objet Plage d'adresses IP

CONFIG OBJECT HOST DELETE name=DHCP LAN RANGE force=1

Objet Port

Créer un objet Port

Nom: SRV_PORT,

· Pas de commentaire,

Numéro de port : 2500,

· Protocole: TCP.

CONFIG OBJECT SERVICE NEW name=SRV_PORT comment="" port=2500 proto=TCP CONFIG OBJECT ACTIVATE

Supprimer un objet Port

CONFIG OBJECT SERVICE DELETE name=SRV_PORT force=1

Objet Plage de ports

Créer un objet Plage de ports

Nom: PORT RANGE,

· Commentaire: PORT RANGE,

Début : 20000,Fin : 20500,Protocole : Any.

CONFIG OBJECT SERVICE NEW name=PORT_RANGE comment="PORT RANGE" port=20000 toport=20500 proto=ANY CONFIG OBJECT ACTIVATE





Supprimer un objet Plage de ports

CONFIG OBJECT SERVICE DELETE name=PORT RANGE force=1

Objet Routeur

Créer un objet Routeur

- Nom : DEFAULT ROUTER,
- Pas de commentaire,
- Répartition de charge : par connexion,
- Activation des passerelles de secours lorsque toutes les passerelles sont injoignables,
- Ne pas activer toutes les passerelles de secours,
- Si aucune passerelle n'est disponible appliquer le routage par défaut.

Passerelles principales 1:

- Objet machine: MAIN GW1
- Test de la disponibilité : dns1.google.com
- Poids: 1

Passerelle principale 2:

- Objet machine: MAIN GW2
- Test de la disponibilité : dns1.google.com
- Poids: 1

Passerelle de secours :

- Objet machine: BACKUP GW
- Test de la disponibilité : dns1.google.com
- Poids: 1

CONFIG OBJECT ROUTER NEW name=DEFAULT_ROUTER comment="" tries=3 wait=2 frequency=15 onfailpolicy=Pass gatewaythreshold=1 activateallbackup=Off loadbalancing=connhash

CONFIG OBJECT ROUTER GATEWAY ADD type=principalgateway name=DEFAULT_ROUTER host=MAIN_GW1 check="dns1.google.com" weight=1 monitor=icmp comment=""

CONFIG OBJECT ROUTER GATEWAY ADD type=backupgateway name=DEFAULT_ROUTER host=BACKUP_GW check="dns1.google.com" weight=1 monitor=icmp comment=""

CONFIG OBJECT ACTIVATE

Supprimer un objet Routeur

CONFIG OBJECT ROUTER DELETE name=DEFAULT ROUTER force=1





Objet Groupe

Créer un objet Groupe

• Nom: SRV GRP,

• Commentaire: Server Group.

```
CONFIG OBJECT GROUP NEW name=SRV_GRP comment="Server Group" CONFIG OBJECT ACTIVATE
```

Ajouter un objet au groupe

• Ajouter au groupe SRV GRP l'objet machine srv web.

```
CONFIG OBJECT GROUP ADDTO group=SRV_GRP node=srv_web CONFIG OBJECT ACTIVATE
```

Supprimer un objet Groupe

```
CONFIG OBJECT GROUP DELETE name=SRV GRP force=1
```

Objet Protocole IP

Créer un objet Protocole IP

• Nom: IP PROTO,

• Commentaire: OWNER IP PROTOCOLE,

Numéro du protocole : 200.

```
CONFIG OBJECT PROTOCOL NEW name=IP_PROTO comment="OWNER IP PROTOCOLE" protonumber=200 CONFIG OBJECT ACTIVATE
```

Supprimer un objet Protocole IP

```
CONFIG OBJECT PROTOCOL DELETE name=IP_PROTO force=1
```

Objet Groupe de ports

Créer un objet Groupe de ports

• Nom: WEB PORT,

· Commentaire: WEB PORT.

```
CONFIG OBJECT SERVICEGROUP NEW name=WEB_PORT comment="WEB PORT" CONFIG OBJECT ACTIVATE
```







Ajouter un objet au groupe

· Ajouter au groupe WEB PORT l'objet protocole https.

```
CONFIG OBJECT SERVICEGROUP ADDTO group=WEB_PORT node=https CONFIG OBJECT ACTIVATE
```

Supprimer un objet Groupe de ports

```
CONFIG OBJECT SERVICEGROUP DELETE name=WEB PORT force=1
```

Objet Groupe de régions

Créer un objet Groupe de régions

• Nom: PART LOC,

Commentaire: Partners Location.

```
CONFIG OBJECT GEOGROUP NEW name=PART_LOC comment="Partners Location" CONFIG OBJECT ACTIVATE
```

Ajouter un objet au groupe

• Ajouter au group PART LOC le pays eu :it.

```
CONFIG OBJECT GEOGROUP ADDTO group=PART_LOC node=eu:it CONFIG OBJECT ACTIVATE
```

Supprimer un objet Groupe de régions

```
CONFIG OBJECT GEOGROUP DELETE name=PART LOC force=1
```

Objet Temps

Créer un objet Temps

Nom : Working Time,

· Commentaire: Working Time,

• Jours de la semaine : lundi, mardi, mercredi, jeudi et vendredi,

Plage horaire: 09:00 à 18:00.

```
CONFIG OBJECT TIME NEW name=working_time comment="Working Time" time=09:00-18:00 weekday=1;2;3;4;5 yearday= date= CONFIG OBJECT ACTIVATE
```

Supprimer un objet Temps

```
CONFIG OBJECT TIME DELETE name=working_time force=1
```





Configuration réseau

Configurer une interface Ethernet

Les noms des interfaces sont :

Ethernet0 : out
Ethernet1 : in
Ethernet2 : dmz1
Ethernet3 : dmz2

Adresse IP statique

• Configurer l'interface in avec l'adresse IP statique 192.168.1.254/24.

CONFIG NETWORK INTERFACE ADDRESS ADD ifname=ethernet1 address=192.168.1.254 mask=24 addressComment= CONFIG NETWORK INTERFACE ACTIVATE

Adresse IP dynamique

• Configurer l'interface out en DHCP.

CONFIG NETWORK INTERFACE ADDRESS ADD ifname=ethernet0 address=DHCP dhcpLeaseTime=0 requestDns=1 CONFIG NETWORK INTERFACE ACTIVATE

Créer un bridge

Adresse IP statique

• Créer un bridge BRIDGE_LAN qui contiendra les interfaces in et dmz1 et qui sera configuré avec l'adresse IP statique 192.168.5.254/24.

CONFIG NETWORK INTERFACE CREATE mtu=1500 name=BRIGE_LAN interfaces=ethernet2,ethernet1 ifname=bridge1 address=192.168.5.254 mask=255.255.255.0 addressComment= CONFIG NETWORK INTERFACE ACTIVATE

Adresse IP dynamique

 Créer un bridge BRIDGE_LAN qui contiendra les interfaces in et dmz1 et qui sera configuré en DHCP.

CONFIG NETWORK INTERFACE CREATE mtu=1500 name=BRIDGE_LAN interfaces=ethernet1,ethernet2 ifname=bridge1 address=DHCP dhcpLeaseTime=3600 dhcpHostname= CONFIG NETWORK INTERFACE ACTIVATE





Modifier un bridge

CONFIG NETWORK INTERFACE ADDRESS UPDATE ifname=bridge1 address=192.168.5.250 mask=255.255.255.0 addrnb=0 addressComment= CONFIG NETWORK INTERFACE ACTIVATE

Supprimer un bridge

Avant de supprimer un bridge, il faut retirer d'abord les interfaces appartenant au bridge.

```
CONFIG NETWORK INTERFACE ADDRESS ADD ifname=ethernet1 address=DHCP dhcpLeaseTime=0 requestDns=0

CONFIG NETWORK INTERFACE ADDRESS ADD ifname=ethernet2 address=DHCP dhcpLeaseTime=0 requestDns=0

CONFIG NETWORK INTERFACE REMOVE ifname=bridge1

CONFIG NETWORK INTERFACE ACTIVATE
```

Configurer la passerelle par défaut

• Configurer l'objet machine (ou routeur) DEFAULT_GW comme passerelle par défaut.

```
CONFIG NETWORK DEFAULTROUTE SET type=ipv4 name=DEFAULT_GW

CONFIG NETWORK DEFAULTROUTE ACTIVATE
```

Configurer une route statique

• Créer la route statique suivante :



Créer une route statique

CONFIG NETWORK ROUTE ADD State=1 Remote=NET_A Interface=dmz2 Gateway=FW_A Color=333399 CONFIG NETWORK ROUTE ACTIVATE

Supprimer une route statique

```
CONFIG NETWORK ROUTE REMOVE Remote=NET_A
CONFIG NETWORK ROUTE ACTIVATE
```





Configurer les serveurs DNS utilisés par le firewall

Ajouter un serveur DNS

 Ajouter le serveur DNS_SRV à la liste des serveurs DNS du firewall dans le menu Configuration > Système > Configuration > Onglet Paramètres réseaux > Zone Résolution DNS.

```
CONFIG DNS SERVER ADD DNS_SRV
CONFIG DNS ACTIVATE
```

Supprimer un serveur DNS

```
CONFIG DNS SERVER REMOVE DNS_SRV

CONFIG DNS ACTIVATE
```





Règles de filtrage

Activer une politique de filtrage ou de NAT

• Activer la politique de filtrage ou de NAT numéro 5.

CONFIG SLOT ACTIVATE type=filter slot=5

Ajouter une règle de filtrage

• Créer la règle de filtrage suivante en première position de la politique de Filtrage - NAT numéro 9 :

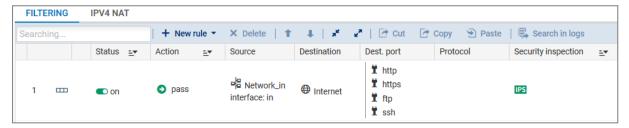


CONFIG FILTER RULE INSERT index=9 type=filter state=on action=pass srctarget=Network_internals dsttarget=internet dstport=http position=1 loglevel=minor

CONFIG FILTER ACTIVATE

Modifier une règle filtrage

Modifier la règle précédente comme suit :



CONFIG FILTER RULE UPDATE srctarget=Network_in srcif=in dstport=http,https,ftp,ssh index=9 global=0 type=filter position=1CONFIG FILTER ACTIVATE

Désactiver une règle de filtrage

CONFIG FILTER RULE UPDATE state=off index=9 global=0 type=filter position=1 CONFIG FILTER ACTIVATE

Supprimer une règle de filtrage

CONFIG FILTER RULE REMOVE index=9 global=0 type=filter position=1 CONFIG FILTER ACTIVATE



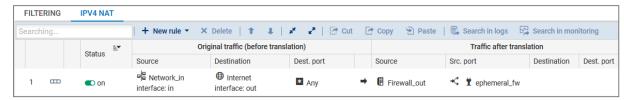


Règles de translation

Ajouter une règle de translation

Translation dynamique

• Créer la règle de translation dynamique suivante :



CONFIG FILTER RULE INSERT index=9 type=nat state=on action=nat srctarget=Network_in srcif=in dsttarget=internet dstif=out natsrctarget=Firewall_out natsrcport=ephemeral_fw natsrcportlb=random position=1 CONFIG FILTER ACTIVATE

Translation statique par port

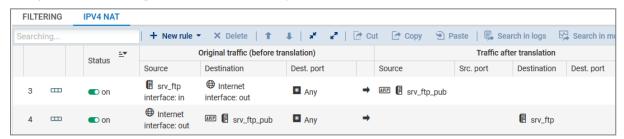
Créer la règle de translation statique par port suivante :



CONFIG FILTER RULE INSERT index=9 type=nat state=on action=nat srctarget=internet srcif=out dsttarget=Firewall_out dstport=http natdsttarget=web_srv natdstport=http position=2 loglevel=minor CONFIG FILTER ACTIVATE

Translation statique

• Ajouter les deux règles de translation statique suivantes :



CONFIG FILTER RULE INSERT index=9 type=nat state=on action=nat srctarget=srv_ftp srcif=in dsttarget=internet dstif=out natsrctarget=srv_ftp_pub natsrcarp=on natsrcport=any position=3

CONFIG FILTER RULE INSERT index=9 type=nat state=on action=nat srctarget=internet srcif=out dsttarget=srv ftp pub natdstarp=on

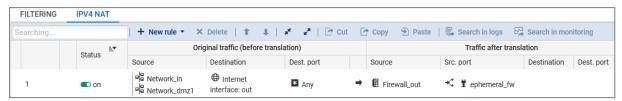




dstport=any natdsttarget=srv_ftp natdstport=any position=4 loglevel=minor CONFIG FILTER ACTIVATE

Modifier une règle de translation

• Modifier la règle de translation dynamique comme suit :



CONFIG FILTER RULE update srctarget=Network_in,Network_dmz2 srcif=any index=9 global=0 type=nat position=1

CONFIG FILTER ACTIVATE

Désactiver une règle de translation

CONFIG FILTER RULE UPDATE state=off index=9 type=nat global=0 position=1 CONFIG FILTER ACTIVATE

Supprimer une règle de translation

CONFIG FILTER RULE REMOVE index=9 global=0 type=nat position=1

CONFIG FILTER ACTIVATE





Gestion des utilisateurs dans la base LDAP interne

Créer une base LDAP interne

Créer une base LDAP interne,

· Nom de l'annuaire : institute.com,

· Organisation: institute,

· Domaine: com,

• Mot de passe de l'annuaire : P@ssw0rd.

CONFIG LDAP INITIALIZE domainname=institute.com o=institute dc=com password=P@ssw0rd CONFIG LDAP ACTIVATE

Créer un utilisateur

• Créer l'utilisateur Jean Doe dans l'annuaire avec le mot de passe adminadmin.

USER CREATE uid=jdoe name=doe gname=jean
USER PASSWORD dn=jdoe password=adminadmin

Supprimer un utilisateur

USER REMOVE "cn=jean doe,ou=users,o=institute,dc=madrid.institute.com"

Créer un groupe d'utilisateurs

• Créer le groupe d'utilisateurs Marketing

USER GROUP CREATE "Marketing"

Ajouter un utilisateur à un groupe

• Ajouter au groupe Marketing l'utilisateur Jean Doe.

USER GROUP ADDUSER "cn=test,ou=groups,o=institute,dc=madrid.institute.com" "jdoe"





Pour aller plus loin

Base de connaissances Stormshield

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





documentation@stormshield.eu

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

Copyright © Stormshield 2023. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.

