TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

BASIC COMMAND LINE INTERFACE CONFIGURATIONS

Product concerned: SNS 3.x, SNS 4.x

Document last update: January 13, 2021

Reference: sns-en-basic_cli_configuration_technical_note

Table of contents

Getting started

Stormshield Network Security Firewalls provide a command line interface (CLI), composed of a proprietary set of commands. The commands are available via a shell and allows configuring and monitoring all firewall features.

This document describes the CLI commands required to configure the basic firewall features. For details about all commands and their arguments, refer to Stormshield Network Security - CLI Serverd commands reference guide.

Using the command line interface

The CLI shell is accessed via a secured protocol (NETASQ Secure Remote Procedure Call):

- Locally on the firewall (command line and web interface),
- From a remote host, using dedicated executables on Windows and Linux.

You can write several CLI commands in a text file to create a CLI script that will then be run either locally or remotely.

NOTE
For details on how to access the CLI shell and how to write and run scripts, refer to the E-learning module CLI ACCESS & SCRIPTS.

Firewall administration

Displaying help for commands and arguments

```
HELP
```

Use HELP as an argument for another command to display help about all its arguments.

Getting write access

```
MODIFY ON FORCE
```

Resetting factory settings

```
SYSTEM DEFAULTCONFIG
```

This command does not reset the password of the *admin* user.

Importing a license

Console syntax

```
SYSTEM LICENCE UPLOAD < U70SXA02J2681A7.licence
```

Script syntax

```
SYSTEM LICENCE UPLOAD $FROM_DATA_FILE ("U70SXA02J2681A7.licence")
```

Backing up the whole configuration

Console syntax

```
CONFIG BACKUP list=all [password=mot_de_passe]> mybackup.na
```

Script syntax

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

Restoring the whole configuration

Console syntax

```
CONFIG RESTORE list=all [password=mot_de_passe]< mybackup.na
```

Script syntax

```
CONFIG RESTORE list=all [password=mot_de_passe] $FROM_DATA_FILE
("mybackup.na")
```

Updating the firmware

Console syntax

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

Script syntax

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

Enabling SSH access using a password

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

Disabling SSH access

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

Allowing a public IP address to access the web interface

```
CONFIG WEBADMIN ACCESS ADD PUBLIC_IP
CONFIG WEBADMIN ACTIVATE
```

PUBLIC_IP is a Host object, but it can also be a Network object, an IP address range, or the *any* object.

Managing Network objects

This section describes how to create and remove objects.

To modify an object, use the same commands as to create it, and add the *update=1* parameter:

Example to modify a Host object:

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

Host object

Creating a Host object

- Name: DNS_SRV,
- Comment: DNS Server,
- IP Address: 192.168.250.150,
- MAC Address: 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
```

Removing a Host object

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

Network object

Creating a Host object

- Name: VPN_NET,
- Comment: VPN Network,
- Network address: 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
```

Removing a Host object

```
CONFIG OBJECT NETWORK DELETE name=VPN_NET force=1
```

IP address range object

Creating an IP address range object

- Name: DHCP_LAN_RANGE,
- Comment: DHCP LAN RANGE,
- Start: 192.168.250.100,
- End: 192.168.250.200.

```
CONFIG OBJECT HOST NEW name=DHCP_LAN_RANGE comment="DHCP LAN RANGE"
begin=192.168.250.100 end=192.168.250.200
CONFIG OBJECT ACTIVATE
```

Removing an IP address range object

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

Port object

Creating a Port object

- Name: SRV_PORT,
- No comment,
- Port number: 2500,
- Protocol: TCP.

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

Removing a Port object

```
CONFIG OBJECT SERVICE DELETE name=SRV_PORT force=1
```

Port range object

Creating a port range object

- Name: PORT_RANGE,
- Comment: PORT RANGE,
- Start: 20000,
- End: 20500,
- Protocol: Any.

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

Removing a port range object

```
CONFIG OBJECT SERVICE DELETE name=PORT_RANGE force=1
```

Router Object

Creating a Router object

- Name: DEFAULT_ROUTER,
- No comment,
- Load balancing: By connection,
- Enable backup gateways when all gateways cannot be reached,
- Not all backup gateways are enabled,
- If no gateways are available, apply the Default route.

Main gateway 1:

- Host object: MAIN_GW1
- Device for testing availability: dns1.google.com
- Weight: 1

Main gateway 2:

- Host object: MAIN_GW2
- Device for testing availability: dns1.google.com
- Weight: 1

Backup gateway:

- Host object: BACKUP_GW
- Device for testing availability: dns1.google.com
- Weight: 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
```

Removing a Router object

```
CONFIG OBJECT ROUTER DELETE name=DEFAULT_ROUTER force=1
```

Group object

Creating a Group object

- Name: SRV_GRP,
- Comment: Server Group.

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

Adding an object to the group

- Add the *srv_web* Host object to the *SRV_GRP* group.

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

Removing a Group object

```
CONFIG OBJECT GROUP DELETE name=SRV_GRP force=1
```

IP protocol object

Creating an IP protocol object

- Name: IP_PROTO,
- Comment: OWNER IP PROTOCOLE,
- Protocol number: 200.

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

Removing an IP protocol object

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

Port group object

Creating a port group object

- Name: WEB_PORT,
- Comment: WEB PORT.

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

Adding an object to the group

- Add the https protocol object to the WEB_PORT group.

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

Removing a port group object

```
CONFIG OBJECT SERVICEGROUP DELETE name=WEB_PORT force=1
```

Region group object

Create a Region group object

- Name: PART_LOC,
- Comment: Partners Location.

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

Adding an object to the group

- Adding the *eu:it* country to the *PART_LOC* group.

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

Removing a Region group object

```
CONFIG OBJECT GEOGROUP DELETE name=PART_LOC force=1
```

Time object

Creating a Time object

- Name: Working_Time,
- Comment: Working Time,
- Week days: Monday, Tuesday, Wednesday, Thursday, and Friday,
- Time slot: 09:00 to 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
```

Removing a Time object

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

Network configuration

Configuring an Ethernet interface

The names of the interfaces are:

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

Static IP address

- Configure the *in* interface with static IP address 192.168.1.254/24.

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

Dynamic IP address

- Configure the *out* interface via DHCP.

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

Creating a bridge

Static IP address

- Create a *BRIDGE_LAN* bridge containing the *in* and *dmz1* interfaces, and configured with the static IP address 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
```

Dynamic IP address

- Create a *BRIDGE_LAN* bridge containing the *in* and *dmz1* interfaces, and configured via DHCP.

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

Modifying a 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
```

Removing a bridge

- Before removing a bridge, you must first remove the interfaces belonging to the 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
```

Configuring the default gateway

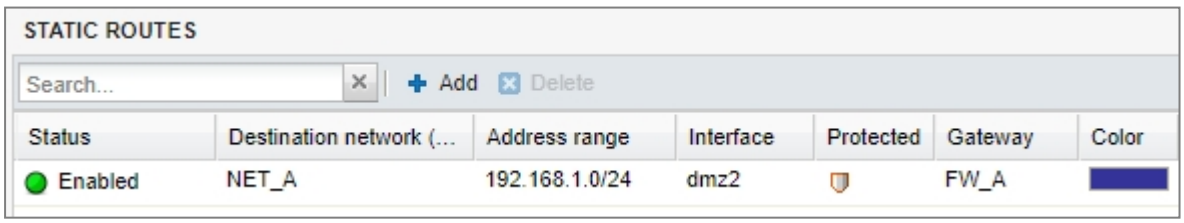
- Configure the Host (or Router) object *DEFAULT_GW* as the default gateway.

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

CONFIG NETWORK DEFAULTROUTE ACTIVATE
```

Configuring a static route

- Create the following static route:



Creating a static route

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

Removing a static route

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

Configuring the DNS servers used by the firewall

Adding a DNS server

- Add the *DNS_SRV* server to the list of the firewall DNS servers in the menu **Configuration > System > Configuration > Network Settings tab > DNS resolution**.

```
CONFIG DNS SERVER ADD DNS_SRV

CONFIG DNS ACTIVATE
```

Removing a DNS server

```
CONFIG DNS SERVER REMOVE DNS_SRV

CONFIG DNS ACTIVATE
```

Filter rules

Enable a filter or NAT policy

- Enable the filter or NAT policy #5.

```
CONFIG SLOT ACTIVATE type=filter slot=5
```

Adding a filter rule

- Create the following filter rule at the top of the Filter-NAT policy #9:

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	Network_internals	Internet	http		IPS

```
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
```

Modifying a filter rule

- Modify the preceding rule as follows:

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	Network_in interface: in	Internet	http https ftp ssh		IPS

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

CONFIG FILTER ACTIVATE
```

Disabling a filter rule

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

CONFIG FILTER ACTIVATE
```

Removing a filter rule

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

CONFIG FILTER ACTIVATE
```

Translation rules

Adding a translation rule

Dynamic translation

- Create the following dynamic translation rule:

	Status	Original traffic (before translation)				Traffic after translation			
		Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1	on	Network_in interface: in	Internet interface: out	Any	→	Firewall_out	ephemera		

```
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
```

Static translation by port

- Create the following static translation rule by port:

	Status	Original traffic (before translation)				Traffic after translation			
		Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
2	on	Internet interface: out	Firewall_out	http	→			web_srv	http

```
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
```

Static translation

- Add the two following static translation rules:

	Status	Original traffic (before translation)				Traffic after translation			
		Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
3	on	srv_ftp interface: in	Internet interface: out	Any	→	srv_ftp_pub			
4	on	Internet interface: out	srv_ftp_pub	Any	→			srv_ftp	

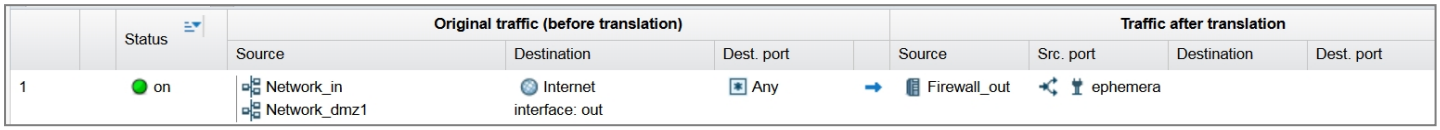
```
CONFIG FILTER RULE INSERT index=9 type=nat state=on action=nat
srctarget=srv_ftp srcif=in dsttarget=internet dstif=out natsrctarget=srv_
ftp_pub natsrcarp=on natsrcport=any position=3

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
```

Modifying a translation rule

- Modify the dynamic translation rule as follows:



		Status	Original traffic (before translation)				Traffic after translation			
			Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1		on	Network_in Network_dmz1	Internet interface: out	Any	→	Firewall_out	ephemera		

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

CONFIG FILTER ACTIVATE
```

Disabling a translation rule

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

CONFIG FILTER ACTIVATE
```

Removing a translation rule

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

CONFIG FILTER ACTIVATE
```

Managing users in the internal LDAP database

Creating an internal LDAP database

- Create an internal LDAP database,
- Directory name: institute.com,
- Organization: institute,
- Domain: com,
- Directory password: P@ssw0rd.

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

Creating a user

- Create the *Jean Doe* user with the *adminadmin* password in the directory.

```
USER CREATE uid=jdoe name=doe gname=jean

USER PASSWORD dn=jdoe password=adminadmin
```

Removing a user

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

Creating a user group

- Create the *Marketing* user group.

```
USER GROUP CREATE "Marketing"
```

Adding a user to a group

- Add the *Jean Doe* user to the *Marketing* group.

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

documentation@stormshield.eu