TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

INITIAL CONFIGURATION FROM USB KEY

Product concerned: SNS 3.9 and higher versions, SNS 4.x

Document last updated: April 10, 2024

Reference: sns-en-initial_configuration_from_usb_key_technical_note

Table of contents

Change log

Date	Description
April 10, 2024	- Corrects the name of the "initTPM" operation

Getting started

This technical note explains how SNS firewalls, either in their initial factory settings (new equipment) or reset to factory settings via the hardware reset button, can be updated and configured using a USB key.

Installation sequence

When the firewall starts up on a USB key, the files found on the key will be imported/installed/run automatically in the following sequence:

1. License (".licence" extension).
2. Firmware update (".maj" extension).
   The firewall will then be restarted.

   IMPORTANT
   The USB key must be removed when the firewall is restarting.
3. Configuration backup file (".na" extension).
4. SMC connecting package (".pack" extension).
5. Certificates (“.p12” extension), from SNS version 3.9.0 onwards.
6. Password of the *admin* account (".pwd" extension), from SNS version 3.9.0 onwards.
7. Dynamic routing configuration files (“.bird” and “.bird6” extensions), from SNS version 3.10.2 upwards or SNS version 4.1.1 upwards.
8. Additional configuration files (".csv" extension), from SNS version 3.9.0 onwards.

If any of the files in the list above is not on the key, the corresponding step will simply be skipped.

Preparing files

As only one USB key can be used for the initial configuration of several firewalls, there may be several files of the same category on the key.

This section specifies the format and designation of the various file types that can be imported.

Licenses

Every firewall has its own unique license file. These files can be found in your MyStormshield personal area, through the **Product** > **Product management** menu.

License files that will be installed via USB key must be named *Firewall_Serial_Number.licence*.

EXAMPLE
SN310A00000000Z.licence

Software updates

Software updates are available in your MyStormshield personal area, through the **Downloads** > **Stormshield Network Security** > **Firmware** > **3.X** > **Stormshield Network Security - Firmware - V 3.0.0** (or later versions) menu. The extension of these files is ".maj".

EXAMPLES
fwupd-3.0.0-SNS-armv6-S.maj
fwupd-4.0.0-SNS-armv6-S.maj

Whenever several firewalls need to be configured using the same USB key, you may need several software update files (different firewall architectures, different preloaded software versions, etc).

IMPORTANT
The USB key must be removed when the firewall is restarting.

If the increment between the major firmware version of the firewall in factory settings and the software versions found on the key is lower than 2 (e.g., firewall in version 3.9.0 and firmware 4.0.0 on the key), only the higher software version on the key will be installed. If this is not the case, an intermediate firmware version must be provided on the key so that an automatic update can be carried out in stages (e.g., firewall in version 2.14.0 and firmware versions 3.9.0 and 4.0.0 on the key).

Configuration backups

Configuration backup files can be created in the **Configuration** > **System** > **Maintenance** module, in the **Backup** tab in the web administration interface of a running firewall.

If a generic configuration will be loaded on the firewalls, the backup file may be named *default.na*. If various backup files are going to be used for the firewalls that will be configured via the USB key, each backup file must be named: *Firewall_Serial_Number.na*.

EXAMPLES
SN310A000000000Z.na
SN310B000000000Z.na

SMC connecting packages

If the firewall is going to be managed from a Stormshield Management Center server, a connecting package (.pack file) must be generated from the SMC server.

Before exporting the package, ensure that the **firewall's connecting package does not include the network configuration** if you do not wish to overwrite the network configuration restored earlier using a .na file.

Once you retrieve the SMC connecting packages (.pack files), rename them according to the format: *Firewall_Serial_Number.pack*.

EXAMPLES
SN310A000000000Z.pack
SN310B000000000Z.pack

Certificates

Certificates can be imported from SNS version 3.9.0 upwards.

Certificates must be in PKCS#12 format (encrypted file that contains the firewall's certificate and its private key). These files must be exported from the workstation that manages the organization's PKI.

NOTE
If your firewall is equipped with a trusted platform module (TPM) and you wish to protect the private key contained in a PKCS#12 file by sealing it to the TPM, see ***p12import* operation**.

The names of PKCS#12 files for a specific firewall consist of the firewall's serial number followed by an optional suffix, and the extension "p12".

EXAMPLES
SN310A000000000Z.p12
SN310A000000000Z_cert1.p12
SN310A000000000Z_cert2.p12
SN310B000000000Z.p12

admin account password

The password of the *admin* account can be deployed from SNS version 3.9.0 upwards.

It comes in the form of a text file containing a single unencrypted string in UTF-8.

The length of the password has to be between 8 and 128 characters. The password must also comply with rules on **allowed/prohibited characters for passwords for SNS v3** or

allowed/prohibited characters for passwords for SNS v4: otherwise, the *admin* account may not be able to connect to the firewall.

If the password specified in the file does not comply with the password policy that was restored through a configuration backup file, this password will not be applied.

If the password is the same for all the firewalls that will be configured via the USB key, the file containing it must be named *default.pwd*. If different passwords are used for each firewall's *admin* account, each file must be named *Firewall_Serial_Number*.pwd.

EXAMPLES
SN310A000000000Z.pwd
SN310B000000000Z.pwd

Dynamic routing configuration

Dynamic routing configuration files can be imported from SNS version 3.10.2 upwards or 4.1.1 upwards.

Every firewall that uses a dynamic routing configuration has a ".bird" file for IPv4 networks and routes, and a ".bird6" file for IPv6 networks and routes.

These files can be accessed via SSH on an active firewall in the folder */usr/Firewall/ConfigFiles/Bird/*.

This configuration can also be displayed from the web administration interface via **Configuration** > **Network** > **Routing**, in the *Dynamic routing* and *IPv6 dynamic routing* tabs.

Every file that will be installed via USB key must be named *Firewall_Serial_Number*.bird or *Firewall_Serial_Number*.bird6.

EXAMPLES
SN310A000000000Z.bird
SN310A000000000Z.bird6

To enable the use of the dynamic routing configuration and Bird files, both Bird and Bird6 modules must also be enabled on the firewall. This requires the use of an additional ".csv" configuration file that will make it possible to run a *setconf* operation. For more information, see Additional configuration files.

Additional configuration files

Additional configuration operations can be executed through one or several CSV files (fields separated by commas) in UTF-8, from SNS version 3.9.0 upwards.

These files make it possible to build an operational firewall cluster or change a value in a firewall configuration file.

Do note that **all** CSV files found on the USB key will be run during the configuration of the firewall.

The following section will set out allowed operations and the structure of the additional configuration file.

General structure of an operation

In an additional configuration file in CSV, each line in an operation is defined according to the following nomenclature:

```
"serial | any" ,"operation", ["parameter 1", etc.]
```

Where:

- serial: indicates that the line in the operation must be applied to the firewall associated with the serial number entered,
- any: indicates that the line in the operation must be applied regardless of the firewall involved.

Lines of comments beginning with the "#" character can be inserted in the file.

setconf operation

The *setconf* operation can be used to:

- Change the value of a field found in a particular section of a configuration file,
- As of version SNS 3.10.1: add a full line to a section of a configuration file.

When a comma is needed in any of the parameters in the command, the value of the parameter must be enclosed in quotation marks.

Setting the value of a field

Format

```
"serial | any", setconf, "file", "section", "field", "value"
```

EXAMPLES
any, setconf, network, ethernet0, Protected, 0
any, setconf, object, Host, gateway, "192.168.0.254, resolve=static"
any, setconf, Bird/global, bird, state, 1

Adding a full line (as of SNS version 3.10.1)

Format

```
"serial | any", setconf, "file", "section", "line"
```

EXAMPLE
any, setconf, route, StaticRoutes, "MyNetworkObject,my-if->MyGW"

delconf operation

The *delconf* operation deletes a field found in a particular section of a configuration file. If the field is not specified, the whole section will be deleted from the configuration file.

Format

```
"serial | any", delconf, "file", "section", "field"
```

```
"serial | any", delconf, "file", "section"
```

EXAMPLES
SN310A000000000Z, delconf, wiki, Global, Schedule
any, delconf, dns, client

setglobal operation

The *setglobal* operation changes the value of a field found in a particular section of a global configuration file (~/System/global.custom file).

Do note that the firewall must be manually restarted in order to apply any changes made to the configuration using the *setglobal* command.

Whenever this command is used, a warning will be recorded in the relevant log files.

Format

```
"serial | any", setglobal, "section", "field", "value"
```

EXAMPLE
SN310A000000000Z, setglobal, ASQ, BridgeLimit, 9

sethostname operation

This feature is available from SNS version 3.10.2 upwards or 4.1.1 upwards.

The *sethostname* operation changes the value of the following fields in the global configuration file (~/System/global file):

- SystemName: corresponds to the name of the firewall. When high availability (HA) is used, this field corresponds to the system name of the HA cluster.
- SystemNodeName: corresponds to the local name of the system node, so that it can be differentiated from the other nodes in the HA cluster.

Format

```
"serial | any", sethostname, "systemname"
```

```
"serial | any", sethostname, "systemname", "systemnodename"
```

EXAMPLE
any, sethostname, test_hostname, testnodename

createHA operation

This operation makes it possible to initialize a firewall cluster. To do so, the firewall to which the operation applies must have the HA license with the master option.

The network mask used for the HA link must accept at least three IP addresses (in CIDR notation: network mask strictly below 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"
```

Parameter	Description
IP_HA_master	IP address assigned to the interface "interface_name" (interface dedicated to the main HA link).
mask	Network mask of the interface "interface_name".
interface_name	Name given to the interface dedicated to the main HA link.
password	Pre-shared key to secure the connection between members of the cluster.
IP_HA_master_backup	IP address assigned to the interface "interface_name_backup" (interface dedicated to the backup HA link).
mask_backup	Network mask of the interface "interface_name_backup".
interface_name_backup	Name given to the interface dedicated to the backup HA link.

EXAMPLES
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

joinHA operation

This operation allows a firewall to join a cluster, which must already be initialized. The network interfaces dedicated to HA must be physically connected (active and passive firewalls)

In an RMA hardware return, the exchanged firewall must be removed from the cluster beforehand using the following CLI / serverd commands:

```
ha cluster remove serial="remote"
```

```
ha cluster activate
```

For more information on the syntax of these commands, refer to the CLI SERVERD Commands Reference Guide SNS v3 or CLI SERVERD Commands Reference Guide SNS v4.

The *joinHA* operation uses a third temporary IP address for the connection to the main firewall in the 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"
```

Parameter	Description
IP_HA_1	First remote IP address tested to reach the cluster.

IP_HA_2	Second remote IP address tested to reach the cluster if IP_HA_1 does not respond, or IP address assigned to the interface "interface_name" (interface dedicated to HA) if the main firewall could be reached via IP_HA_1.
IP_HA_join	IP address that the firewall temporarily uses to reach the cluster.
mask	Network mask of the interface "interface_name".
interface_name	Name given to the interface dedicated to the main HA link.
password	Pre-shared key to secure the connection between members of the cluster.
IP_HA_join_backup	IP address assigned to the interface "interface_name_backup" (interface dedicated to the backup HA link).
mask_backup	Network mask of the interface "interface_name_backup".
interface_name_backup	Name given to the interface dedicated to the backup HA link.

EXAMPLES
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

IMPORTANT
The USB key must be removed when the firewall joining the cluster restarts, during the configuration synchronization phase.

initTPM operation

This feature is available from SNS version 3.10.1 upwards or 4.0.1 upwards.

This operation initializes TPM chips by passing the password as an argument, and if the firewall is part of a cluster (high availability enabled), to derive the key from the TPM password so that both firewalls will obtain the exact same key.

The TPM password must comply with the password policy set in the configuration (file ~/ConfigFiles/serverd section PasswordPolicy).

This operation must be performed before attempting to protect any private keys with TPM.

Format

```
"serial | any", initTPM, "tpmpassword"
```

EXAMPLE
SN310A17B0023A7, initTPM, TpmPasswordValue

p12import operation

This feature is available from SNS version 3.10.1 upwards or 4.0.1 upwards.

It allows PKCS#12 files to be imported. File names must have a .p12 extension. If a PKCS#12 file is not protected by a password, the "p12password" field must remain empty. The "ondisk" parameter makes it possible to choose whether to protect the private key contained in a PKCS#12 file by sealing it to the TPM.

The TPM must to be initialized before it can be used to protect any private keys.

Format

```
"serial | any", p12import, none|ondisk, "p12file", "p12password"
```

EXAMPLES
SN310A17B0023A7, p12import, none, file1.p12, file1PwdValue
SN310A17B0023A7, p12import, none, file2.p12
SN310A17B0023A7, p12import, ondisk, file3.p12, file3PwdValue
SN310A17B0023A7, p12import, ondisk, file4.p12

Preparing the USB key

If you are using a USB key for a firewall's initial configuration, Stormshield strongly recommends encrypted USB keys such as Kingston Data Traveler, which are protected with a built-in PIN.

Formatting the USB key

The USB key must contain a single partition formatted to FAT32.

Copying the necessary files

Depending on the operations performed, copy the following files to the root folder of the USB key:

- Licenses (.licence),
- Software update(s) (.maj),
- Configuration backup(s) (.na),
- SMC connecting package(s) (.pack),
- PKCS#12 certificate(s) (.p12),
- Files containing the password to the *admin* account (.pwd),
- Files containing the dynamic routing configuration (.bird or .bird6),
- Additional configuration files (.csv).

Setting the initial configuration

No action is required from the operator during the initial configuration of a firewall via a USB key, except to:

- Unlock the USB key if it has been encrypted,
- Enter certificate passwords whenever certificates are imported during the configuration via USB key.

1. Check that the firewall is powered off.
2. If the firewall has been assigned to a cluster, ensure that all of its HA-dedicated network interfaces are connected to the master firewall.
3. Insert the key into the firewall's USB port.
4. Power up the firewall.
   The firewall will automatically run and install the prepared files in the sequence mentioned in Installation sequence.
   It will restart only after each software update.
5. If part of the configuration involved *setglobal* commands included in a CSV file, manually restart the firewall to apply changes.
6. Once all the steps in the configuration have been completed, the firewall will be operational. You can log in directly to its web administration interface (*https://firewall_IP_address/admin*) or via Stormshield Management Center if the firewall is connected to an SMC server.

Operations that were performed during the initial configuration of the firewall, except license imports and firmware updates, will be logged in a log file created in the root folder of the USB key named *<firewall_serial_number_staging>.log*.

Further reading

Additional information and responses to questions you may have are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu