TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

MIGRATING CONFIGURATION FROM ONE FIREWALL MODEL TO ANOTHER

Product concerned: SN160, SN210(W), SN310, SN-S-Series-220, SN-S-Series320

Document last updated: February 22, 2024

Reference: sns-en-migrating_configuration_from_one_firewall_model_to_another-technical_note

Table of contents

Getting started ... 3

Requirements and operation ... 4

An administrator account with the Maintenance permission ... 4
Important information regarding Wi-Fi ... 4
Overview of a configuration migration ... 4

SN160(W) to SN-S-Series ... 5

Ports and interfaces on SN160(W) and SN-S-Series firewalls ... 5
Backing up the configuration on the source SN160(W) firewall ... 5
Restoring the configuration backup on the SN-S-Series firewall ... 6
Scenario no. 1: Only one port on the LAN/in interface was used on the SN160(W) firewall ... 6
If a Wi-Fi interface was configured on the SN160(W) firewall ... 6
Scenario no. 2: Multiple ports on the LAN/in interface were used on the SN160(W) firewall 7
Option 1: Connect a network switch to the SN-S-Series firewall ... 7
Option 2: Adapt the configuration of the SN-S-Series firewall ... 7

SN210(W) to SN-S-Series ... 11

Ports and interfaces on SN210(W) and SN-S-Series firewalls ... 11
Backing up the configuration on the source SN210(W) firewall ... 11
Restoring the configuration backup on the SN-S-Series firewall ... 12
Scenario no. 1: Only one port on the LAN/in interface was used on the SN210(W) firewall . 12
If a Wi-Fi interface was configured on the SN210W firewall ... 12
Scenario no. 2: Multiple ports on the LAN/in interface were used on the SN210(W) firewall 13
Option 1: Connect a network switch to the SN-S-Series firewall ... 13
Option 2: Adapt the configuration of the SN-S-Series firewall ... 13

SN310 to SN-S-Series ... 17

Ports and interfaces on SN310 and SN-S-Series firewalls ... 17
Backing up the configuration of the source SN310 firewall ... 17
Restoring the configuration backup on the SN-S-Series firewall ... 18
One or more ports were used on the SN310 firewall ... 18
18
18
If the SN310 firewall was configured in high availability ... 19

Getting started

SN-S-Series-220, SN-S-Series-320 and SN-M-Series-520 model firewalls are set to replace older firewall models by offering higher performance.

This document sets out the steps involved in migrating the configuration on an older firewall model to a new model in the equivalent range.

The following migration scenarios are covered:

- SN160(W) to SN-S-Series,
- SN210(W) to SN-S-Series,
- SN310 to SN-S-Series.

Requirements and operation

An administrator account with the Maintenance permission

> **NOTE**
> Some operations require access to the web administration interface of the firewalls in question using an administration account that has at least permissions to perform/restore backups (administrator with the **Maintenance** permission).

Find out more on creating administrator accounts with specific permissions.

Important information regarding Wi-Fi

Do note that if your source firewall had an internal Wi-Fi access point (AP) built into its configuration (SN160W/SN210W model firewalls), you will need to configure and connect an external Wi-Fi access point to your destination model when you migrate the configuration.

Overview of a configuration migration

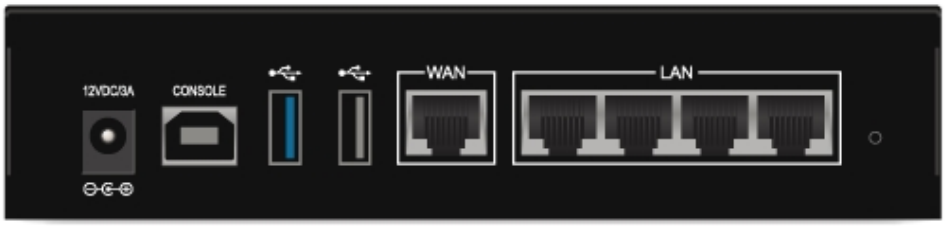
The following steps are required in the migration of a configuration:

1. Backing up the configuration of the source firewall.
2. Restoring the configuration backup on the destination firewall.
3. Adapting cable connections and the configuration on the destination firewall.

SN160(W) to SN-S-Series

Ports and interfaces on SN160(W) and SN-S-Series firewalls

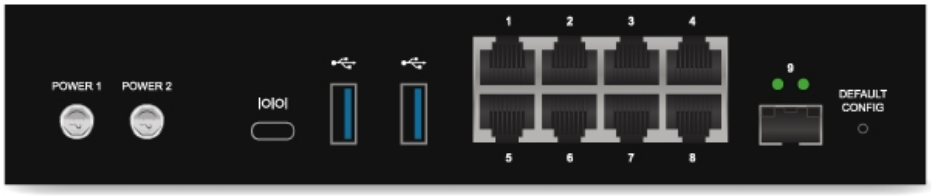
SN160(W) firewalls



Port no.	1	2	3	4	5
Interface	WAN/out	LAN/in			

SN160(W) firewalls treat ports 2 to 5 (LAN/in interface) as a single interface, as they behave in the same way as a 4-port Gigabit Ethernet network switch.

SN-S-Series firewalls



Port no.	1	2	3	4	
Interface	WAN/out	LAN/in	dmz1	dmz2	
Port no.	5	6	7	8	9 (fiber)
Interface	dmz3	dmz4	dmz5	dmz6	dmz7

Only port 2 corresponds to the LAN/in interface: there is no longer any internal switch that groups ports 2 to 8 as a single interface.

Backing up the configuration on the source SN160(W) firewall

1. Log in to the web administration interface of the SN160(W) firewall using an administrator account that has at least the **Maintenance**permission.
2. Go to **Configuration** > **System** > **Maintenance** > **Backup** tab.
3. You can:

- Customizing the name of the backup file,
- Protect the configuration backup file with a password (recommended) by entering and confirming the password in the **Advanced properties** section.

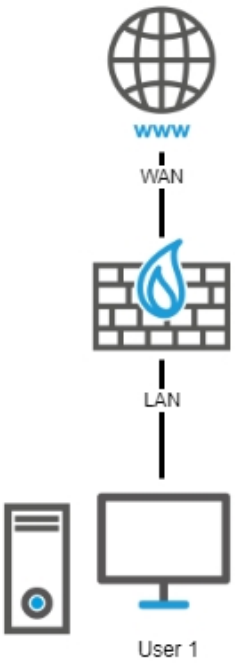
4. Click on **Download the configuration backup.**
5. Save this backup file with a "*.na*" extension on your workstation.

Restoring the configuration backup on the SN-S-Series firewall

1. Log in to the web administration interface of the SN-S-Series firewall using an administrator account that has at least the **Maintenance**permission.
2. Go to **Configuration** > **System** > **Maintenance** > **Restore** tab.
3. Select the file **Backup to restore**.
4. If you have protected your backup file with a password, click on **Advanced properties** and enter the **Backup password**.
5. Click on **Restore the configuration from the file**.
6. Once the backup has been restored, restart your SN-S-Series firewall.

Scenario no. 1: Only one port on the LAN/in interface was used on the SN160(W) firewall

Plug in the cable that was on one of the ports from 2 to 5 (LAN/in interface) on the SN160(W) firewall to port 2 (LAN/in interface) on the SN-S-Series firewall:



If a Wi-Fi interface was configured on the SN160(W) firewall

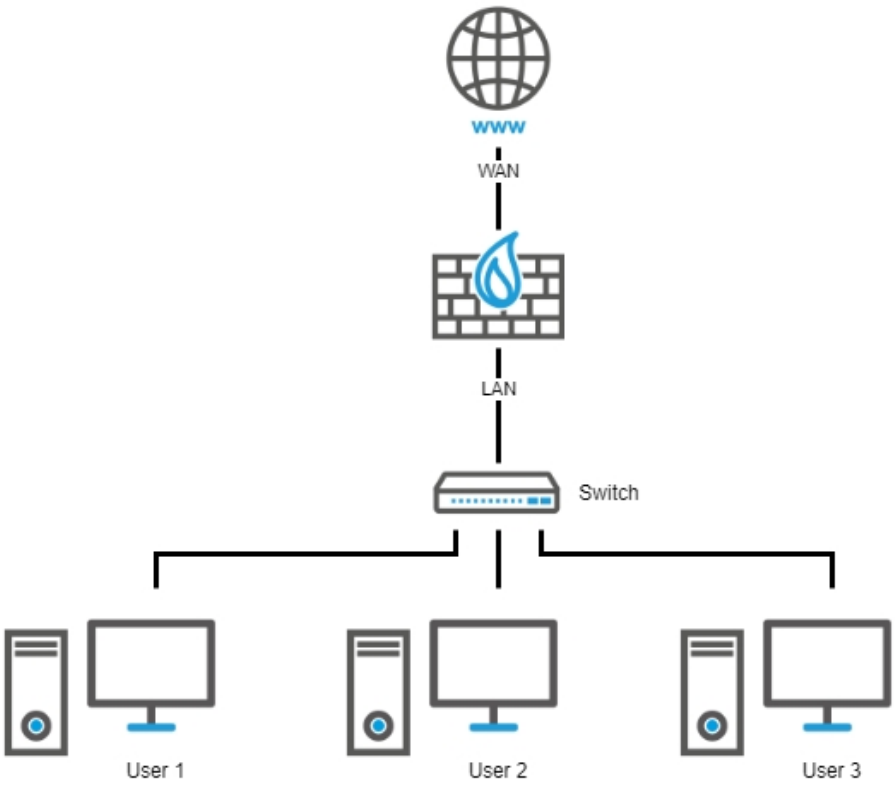
Configure a Wi-Fi access point (not provided by Stormshield) in the same way that the Wi-Fi interface was configured on the SN160(W) firewall and connect it to one of the free ports on the SN-S-Series firewall (port 3/dmz1, port 4/dmz2, port 5/dmz3, port 6/dmz4, port 7/dmz5 or port 8/dmz6).

NOTE
On the SN-S-Series firewall, you need to check/adapt the filter policy relating to traffic from the access point that passes through the firewall, in order to apply the address range of the access point and the interface to which the access point is connected.

Scenario no. 2: Multiple ports on the LAN/in interface were used on the SN160(W) firewall

Option 1: Connect a network switch to the SN-S-Series firewall

This option does not require any changes to be made to the configuration. It consists of connecting a network switch (not provided by Stormshield) to port 2 (LAN/in interface) on the SN-S-Series firewall and then connecting users to this switch:

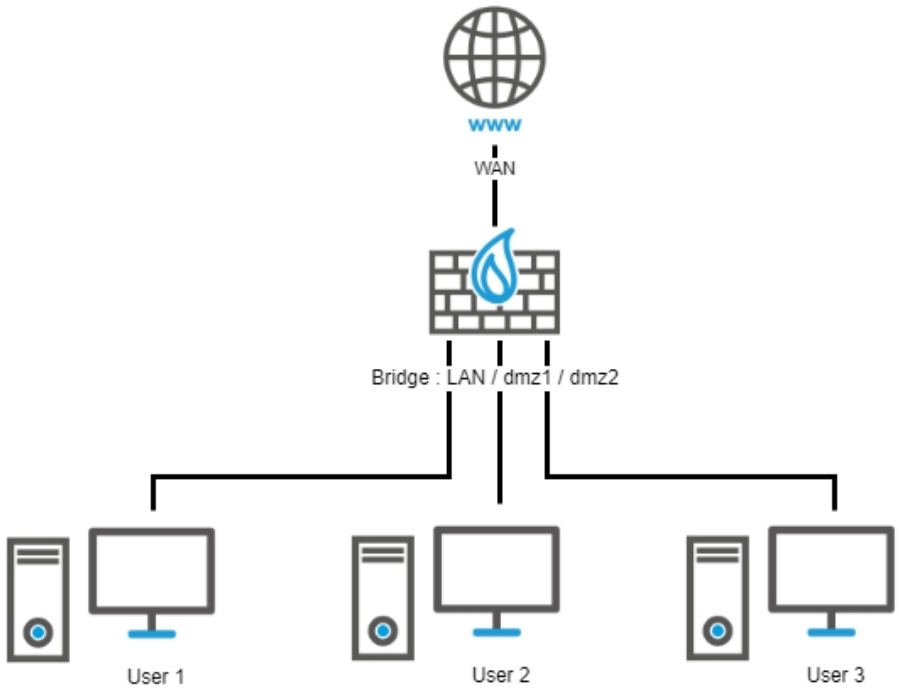


Option 2: Adapt the configuration of the SN-S-Series firewall

If you choose not to connect a switch to port 2 (LAN/in interface) on the SN-S-Series firewall, you will need to change the configuration on the firewall by creating a bridge that groups all necessary ports on the SN-S-Series firewall, and by transferring the cable connections of ports on the SN160(W) firewall to ports on the new SN-S-Series firewall bridge.

EXAMPLE

- Cable for port 2 (LAN/in interface) on the SN160(W) firewall to port 2 (LAN/in interface) on the SN-S-Series firewall,
- Cable for port 3 (LAN/in interface) on the SN160(W) firewall to port 3 (dmz1 interface) on the SN-S-Series firewall,
- Cable for port 4 (LAN/in interface) on the SN160(W) firewall to port 4 (dmz2 interface) on the SN-S-Series firewall.



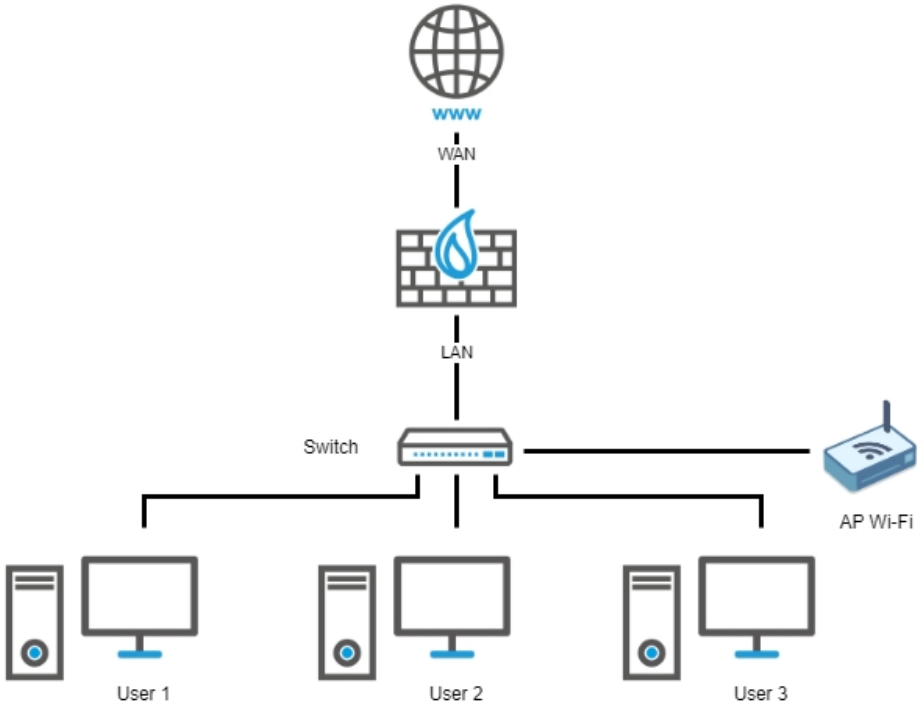
For more information on creating bridges, refer to the section Bridge interface in the SNS v4 user guide.

NOTE
The firewall behavior with this bridge will be similar to the configuration on the SN160(W) firewall, but not identical. Even with a *pass all* policy, traffic that passes through the bridge will be filtered and inspected. Traffic from a host placed on a port on the bridge to another host on another port on the bridge will be inspected by the intrusion prevention engine in this case.

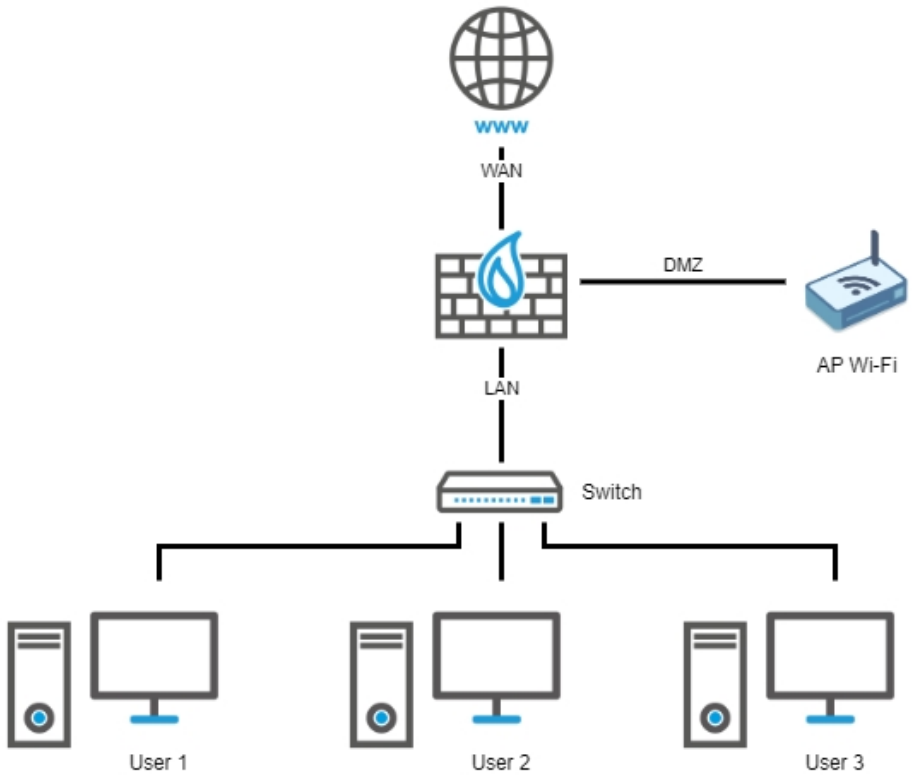
If a Wi-Fi interface was configured on the SN160W firewall

Configure a Wi-Fi access point (not provided by Stormshield) in the same way that the Wi-Fi interface was configured on the SN160W firewall and connect it to:

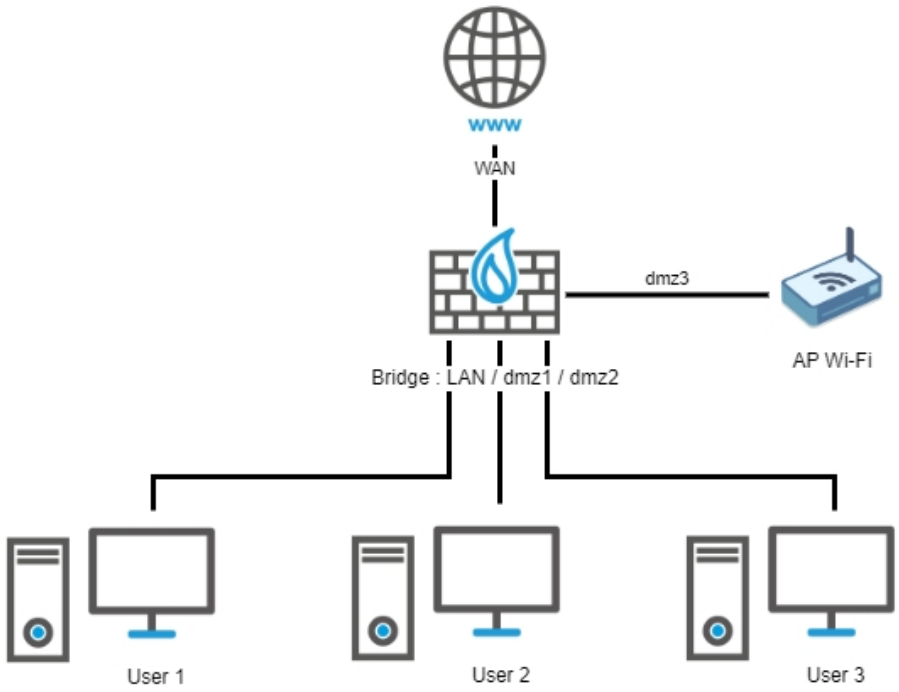
- The network switch that was connected to port 2 (LAN/in interface) if Option 1: Connect a network switch to the SN-S-Series firewall is chosen.
  Example:



- One of the free ports on the SN-S-Series firewall (port 3/dmz1, port 4/dmz2, port 5/dmz3, port 6/dmz4, port 7/dmz5 or port 8/dmz6) if Option 2: Adapt the configuration of the SN-S-Series firewall is chosen.
  Example:



- One of the free ports on the SN-S-Series firewall (port 3/dmz1, port 4/dmz2, port 5/dmz3, port 6/dmz4, port 7/dmz5 or port 8/dmz6) if Option 2: Adapt the configuration of the SN-S-Series firewall is chosen. Example:



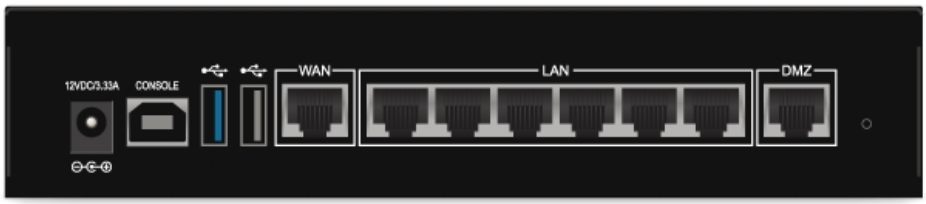
NOTE

Regardless of the option chosen, on the SN-S-Series firewall, you need to check/adapt the filter policy relating to traffic from the access point that passes through the firewall, in order to apply the address range of the access point and the interface to which the access point is connected.

SN210(W) to SN-S-Series

Ports and interfaces on SN210(W) and SN-S-Series firewalls

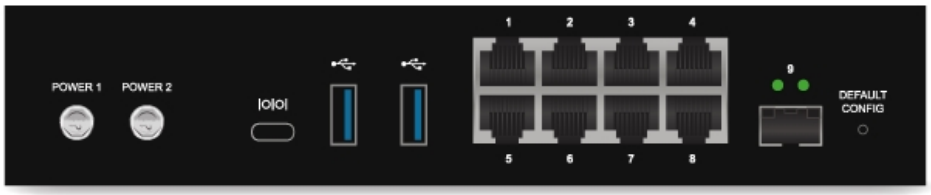
SN210(W) firewalls



Port no.	1	2	3	4	5	6	7	8
Interface	WAN/out	LAN/in						DMZ/dmz1

SN210(W) firewalls treat ports 2 to 7 (LAN/in interface) as a single interface, as they behave in the same way as a 6-port Gigabit Ethernet network switch.

SN-S-Series firewalls



Port no.	1	2	3	4	
Interface	WAN/out	LAN/in	dmz1	dmz2	
Port no.	5	6	7	8	9 (fiber)
Interface	dmz3	dmz4	dmz5	dmz6	dmz7

Only port 2 corresponds to the LAN/in interface: there is no longer any internal switch that groups ports 2 to 8 as a single interface.

Backing up the configuration on the source SN210(W) firewall

1. Log in to the web administration interface of the SN210(W) firewall using an administrator account that has at least the **Maintenance**permission.
2. Go to **Configuration** > **System** > **Maintenance** > **Backup** tab.
3. You can:

- Customizing the name of the backup file,
- Protect the configuration backup file with a password (recommended) by entering and confirming the password in the **Advanced properties** section.

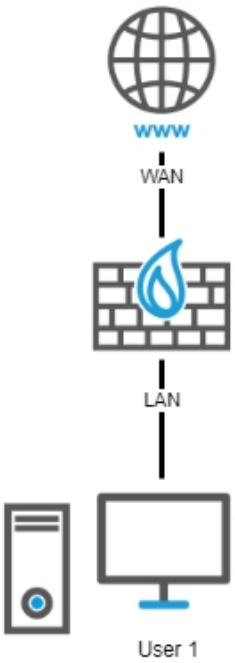
4. Click on **Download the configuration backup.**
5. Save this backup file with a "*.na*" extension on your workstation.

Restoring the configuration backup on the SN-S-Series firewall

1. Log in to the web administration interface of the SN-S-Series firewall using an administrator account that has at least the **Maintenance**permission.
2. Go to **Configuration** > **System** > **Maintenance** > **Restore** tab.
3. Select the file **Backup to restore**.
4. If you have protected your backup file with a password, click on **Advanced properties** and enter the **Backup password**.
5. Click on **Restore the configuration from the file**.
6. Once the backup has been restored, restart your SN-S-Series firewall.

Scenario no. 1: Only one port on the LAN/in interface was used on the SN210(W) firewall

Plug in the cable that was on one of the ports from 2 to 7 (LAN/in interface) on the SN210(W) firewall to port 2 (LAN/in interface) on the SN-S-Series firewall:



If a Wi-Fi interface was configured on the SN210W firewall

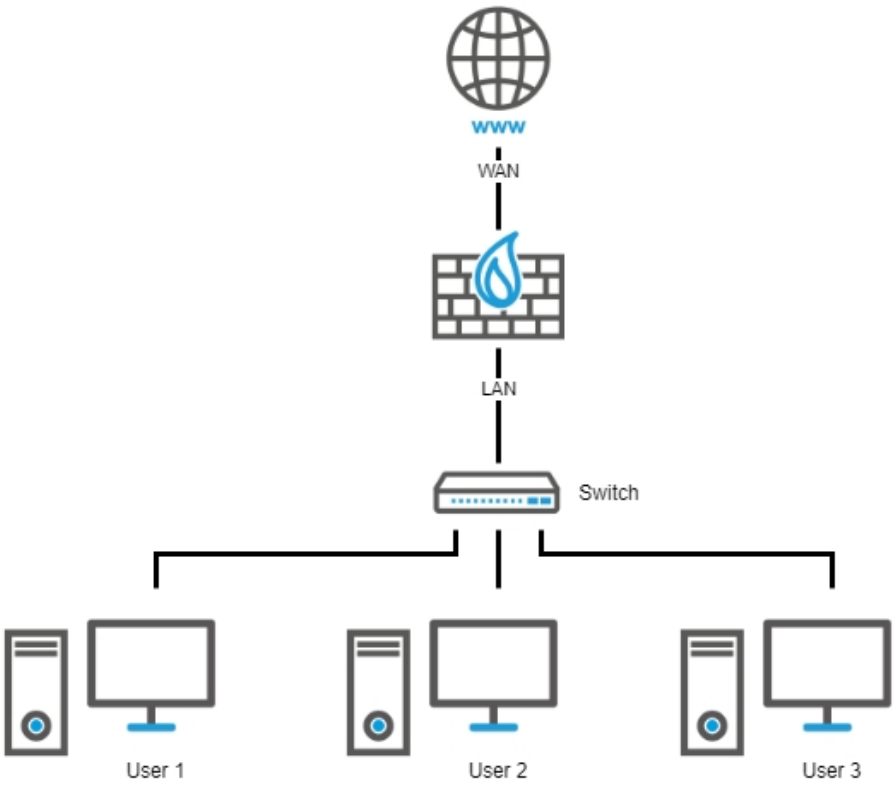
Configure a Wi-Fi access point (not provided by Stormshield) in the same way that the Wi-Fi interface was configured on the SN210W firewall and connect it to one of the free ports on the SN-S-Series firewall (port 3/dmz1, port 4/dmz2, port 5/dmz3, port 6/dmz4, port 7/dmz5 or port 8/dmz6).

NOTE
On the SN-S-Series firewall, you need to check/adapt the filter policy relating to traffic from the access point that passes through the firewall, in order to apply the address range of the access point and the interface to which the access point is connected.

Scenario no. 2: Multiple ports on the LAN/in interface were used on the SN210(W) firewall

Option 1: Connect a network switch to the SN-S-Series firewall

This option does not require any changes to be made to the configuration. It consists of connecting a network switch (not provided by Stormshield) to port 2 (LAN/in interface) on the SN-S-Series firewall and then connecting users to this switch:



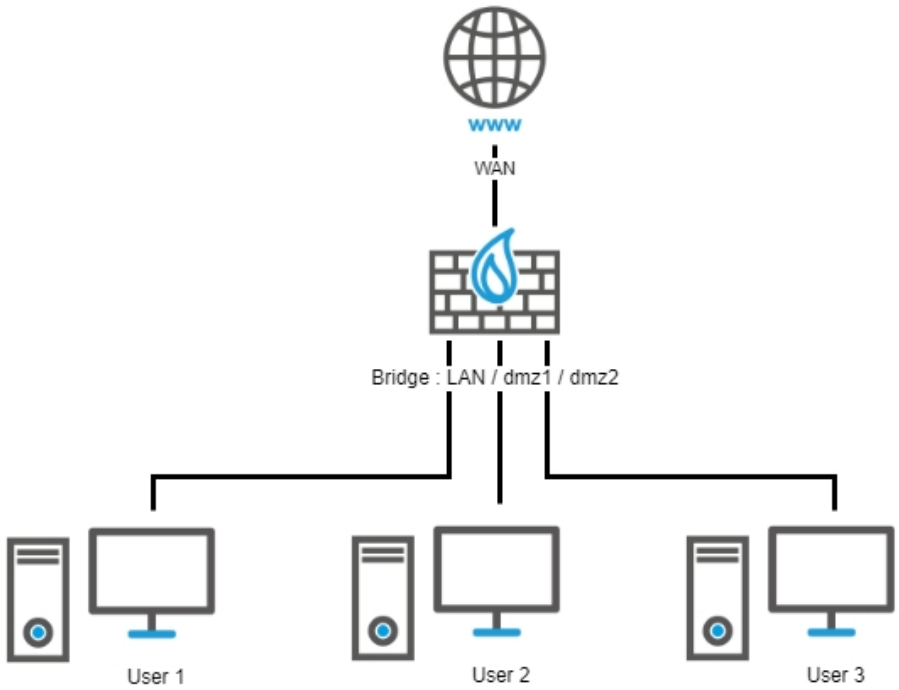
Option 2: Adapt the configuration of the SN-S-Series firewall

If you choose not to connect a switch to port 2 (LAN/in interface) on the SN-S-Series firewall, you will need to change the configuration on the firewall by creating a bridge that groups all necessary ports on the SN-S-Series firewall, and by transferring the cable connections of ports on the SN210(W) firewall to ports on the new SN-S-Series firewall bridge.

IMPORTANT
If ports 2 to 7 (LAN/in interface) were used on the SN210(W) firewall, and you wish to include ports 2 to 7 on the SN-S-Series firewall in this new bridge, the configuration on port 3 (DMZ/dmz1) of the SN210(W) firewall has to be transferred to port 8 (dmz6) on the SN-S-Series firewall **before** this bridge is created.

EXAMPLE

- Cable for port 2 (LAN/in interface) on the SN210(W) firewall to port 2 (LAN/in interface) on the SN-S-Series firewall,
- Cable for port 3 (LAN/in interface) on the SN210(W) firewall to port 3 (dmz1 interface) on the SN-S-Series firewall,
- Cable for port 4 (LAN/in interface) on the SN210(W) firewall to port 4 (dmz2 interface) on the SN-S-Series firewall.



For more information on creating bridges, refer to the section Bridge interface in the SNS v4 user guide.

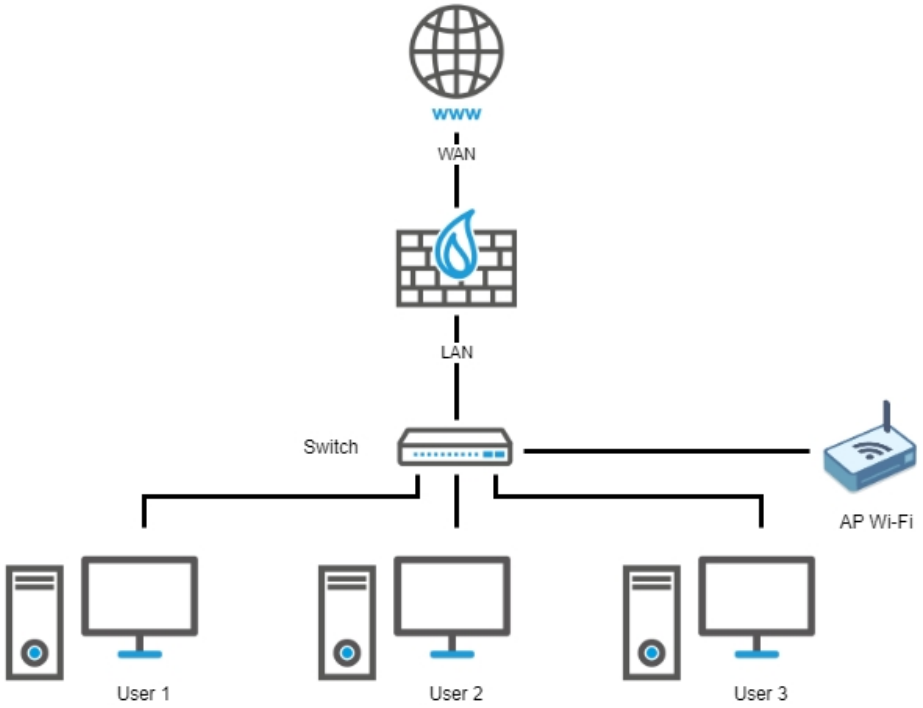
NOTE

The firewall behavior with this bridge will be similar to the configuration on the SN210(W) firewall, but not identical. Even with a *pass all* policy, traffic that passes through the bridge will be filtered and inspected. Traffic from a host placed on a port on the bridge to another host on another port on the bridge will be inspected by the intrusion prevention engine in this case.

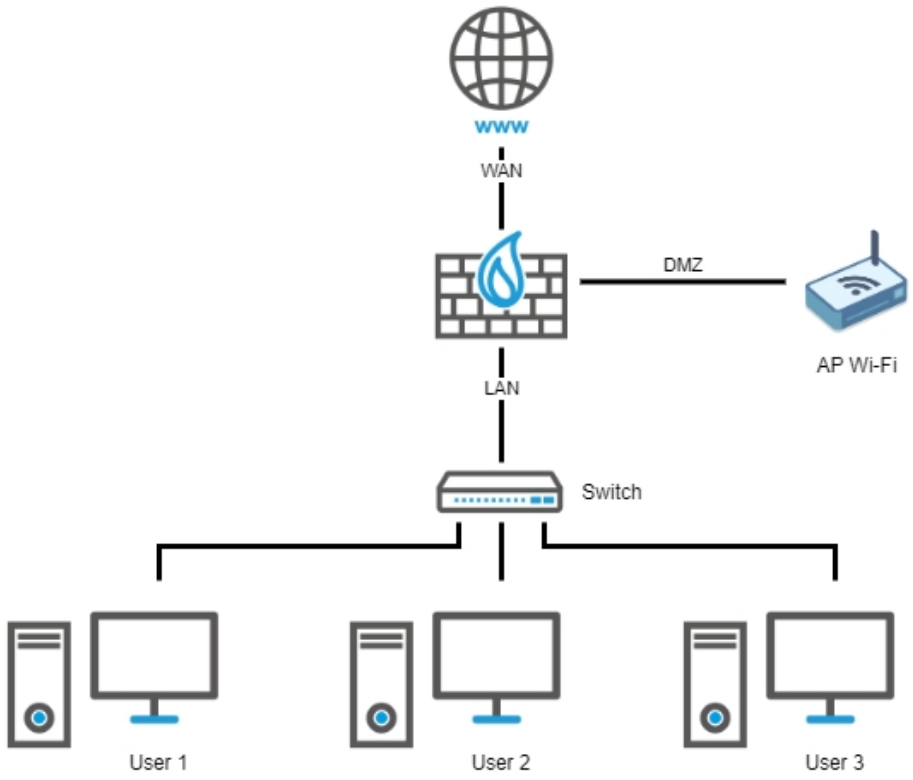
If a Wi-Fi interface was configured on the SN210(W) firewall

Configure a Wi-Fi access point (not provided by Stormshield) in the same way that the Wi-Fi interface was configured on the SN210(W) firewall and connect it to:

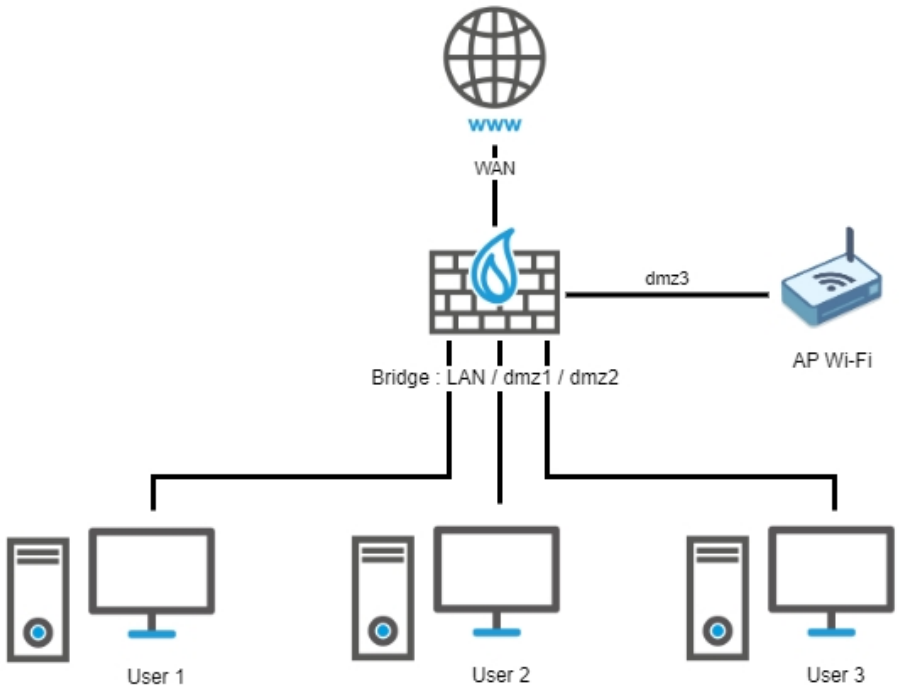
- The network switch that was connected to port 2 (LAN/in interface) if Option 1: Connect a network switch to the SN-S-Series firewall is chosen.
  Example:



- One of the free ports on the SN-S-Series firewall (port 3/dmz1, port 4/dmz2, port 5/dmz3, port 6/dmz4, port 7/dmz5 or port 8/dmz6) if Option 2: Adapt the configuration of the SN-S-Series firewall is chosen.
  Example:



- One of the free ports on the SN-S-Series firewall (port 3/dmz1, port 4/dmz2, port 5/dmz3, port 6/dmz4, port 7/dmz5 or port 8/dmz6) if Option 2: Adapt the configuration of the SN-S-Series firewall is chosen.
  Example:



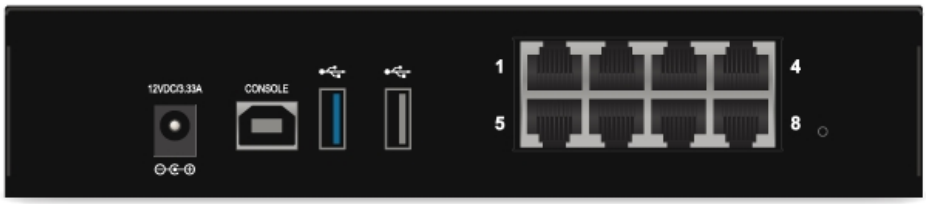
NOTE

Regardless of the option chosen, on the SN-S-Series firewall, you need to check/adapt the filter policy relating to traffic from the access point that passes through the firewall, in order to apply the address range of the access point and the interface to which the access point is connected.

SN310 to SN-S-Series

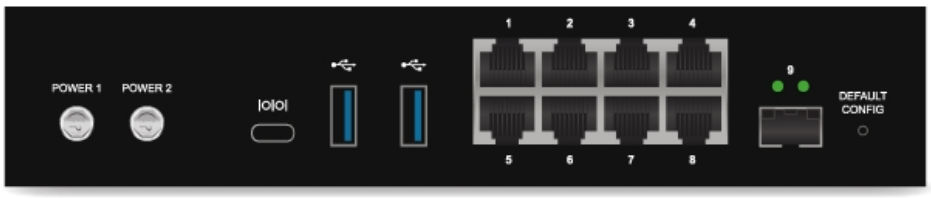
Ports and interfaces on SN310 and SN-S-Series firewalls

SN310 firewalls



Port no.	1	2	3	4
Interface	WAN/out	LAN/in	dmz1	dmz2
Port no.	5	6	7	8
Interface	dmz3	dmz4	dmz5	dmz6

SN-S-Series firewalls



Port no.	1	2	3	4	
Interface	WAN/out	LAN/in	dmz1	dmz2	
Port no.	5	6	7	8	9 (fiber)
Interface	dmz3	dmz4	dmz5	dmz6	dmz7

Backing up the configuration of the source SN310 firewall

1. Log in to the web administration interface of the SN310 firewall using an administrator account that has at least the **Maintenance**permission.
2. Go to **Configuration** > **System** > **Maintenance** > **Backup** tab.
3. You can:

- Customizing the name of the backup file,
- Protect the configuration backup file with a password (recommended) by entering and confirming the password in the **Advanced properties** section.

4. Click on **Download the configuration backup.**
5. Save this backup file with a "*.na*" extension on your workstation.

Restoring the configuration backup on the SN-S-Series firewall

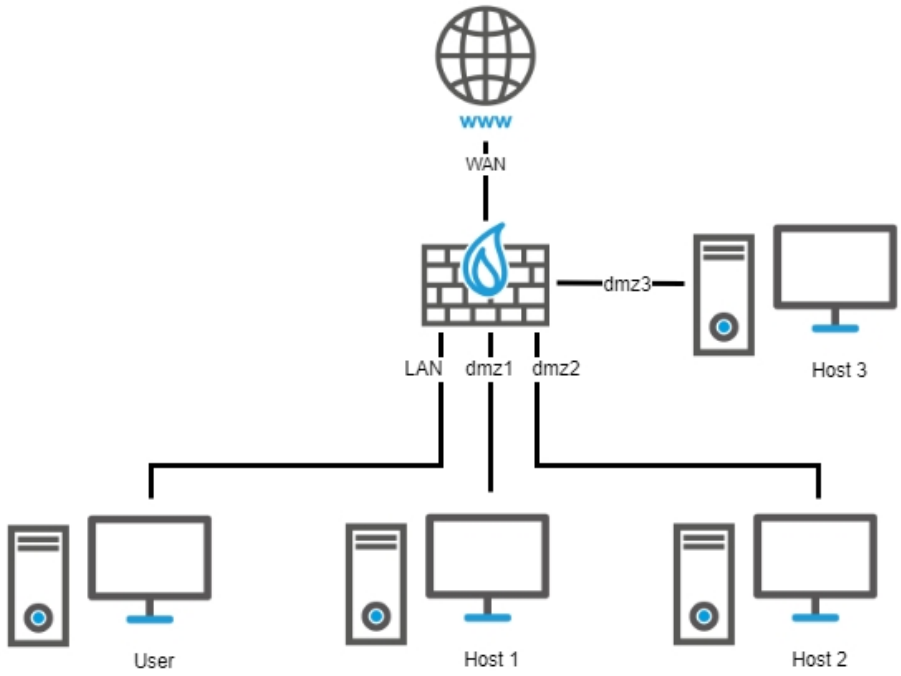
1. Log in to the web administration interface of the SN-S-Series firewall using an administrator account that has at least the **Maintenance**permission.
2. Go to **Configuration** > **System** > **Maintenance** > **Restore** tab.
3. Select the file **Backup to restore**.
4. If you have protected your backup file with a password, click on **Advanced properties** and enter the **Backup password**.
5. Click on **Restore the configuration from the file**.
6. Once the backup has been restored, restart your SN-S-Series firewall.

One or more ports were used on the SN310 firewall

Plug in the cables to the same ports on the SN310 as on the SN-S-Series firewall.

EXAMPLE

- Cable for port 2 (LAN/in interface) on the SN310 firewall to port 2 (LAN/in interface) on the SN-S-Series firewall,
- Cable for port 3 (dmz1 interface) on the SN310 firewall to port 3 (dmz1 interface) on the SN-S-Series firewall,
- Cable for port 4 (dmz2 interface) on the SN310 firewall to port 4 (dmz2 interface) on the SN-S-Series firewall,
- Cable for port 5 (dmz3 interface) on the SN310 firewall to port 5 (dmz3 interface) on the SN-S-Series firewall,



If the SN310 firewall was configured in high availability

After you have transferred the configuration to the SN-S-Series firewall:

1. Create the cluster on the firewall.
2. Configure the second SN-S-Series firewall.
3. Attach it to the cluster by following the procedure described in the section **Configuring HA** in the technical note High availability on SNS.

documentation@stormshield.eu