TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

CONFIGURING WEB SERVICES ON SNS FIREWALLS

Product concerned: SNS 4.5 and higher versions

Document last updated: February 27, 2024

Reference: sns-en-configuring_web_services_technical_note

Table of contents

Change log

Date	Description
February 27, 2024	- Added new firewalls regarding the number of lines allowed in an import file to the section "Import file: format, structure and limitations"
November 3, 2022	- New document

Getting started

The SNS firewall can identify the services associated with certain web traffic. Such services are called web services on the firewall. By identifying them, you can:

- Set for each web service granular SD-WAN SLA (Service Level Agreement), Quality of Service (QoS) and routing policies to provide optimal connectivity for high-priority web traffic,
- Allow traffic from certain web services to avoid the proxy, in order to free up space on the proxy for other traffic,
- Block or allow traffic from certain web services.

This technical note explains how to manage web services on the SNS firewall and provides illustrations with the most common scenarios in which web services are used with the SNS firewall.

Requirements and operation

Compatible SNS versions with web services

- SNS 4.5 and higher versions

DNS traffic in plaintext

The SNS firewall must be able to view in plaintext (unencrypted) the DNS traffic that passes through it, as FQDN recognition is the basis for identifying web services. If this is not the case, the SNS firewall will not be able to identify web services based on FQDNs.

DNS protocol analysis must be enabled on DNS traffic (IPS or IDS inspection level).

Blocking DoH and DoT protocols

By default, the SNS firewall blocks the encrypted DNS protocols DoH and DoT to force a fallback to the standard DNS protocol with the purpose of viewing DNS traffic in plaintext.

This fallback occurs only if it is allowed on the web browser used, and after a certain number of successive tries, which may cause latency until the requested web page appears. Do note that the number of tries and duration of latency depend on the web browser and cannot be configured on the SNS firewall.

DoH and DoT can be blocked on the SNS firewall by using context-based signature detection (**Configuration > Application protection > Applications and protections**). DoT can also be blocked when it is detected in the ALPN extension of TLS (**Configuration > Application protection > Protocols > SSL**, **IPS** tab, **Application-Layer Protocol Negotiation (ALPN)** section).

IMPORTANT
These protocols must remain blocked so that web services can be correctly identified.

Using public IP addresses

Only public IP addresses can be used in the databases of official and custom web services. Private IP addresses cannot be used.

Dependency of web services

Some web services may be dependent on other web services, for example, when a provider hosts its service with another provider, or when a provider offers several services.

When web services are used in the SNS firewall's configuration, and to avoid mistakenly blocking or allowing certain web traffic, we recommend that you first check whether a web service is dependent on any other, or whether any web services depend on it. Known dependencies are listed on the Stormshield Security Portal.

Managing web services

Web services are divided into two databases on the SNS firewall:

- **Official web service database**: created and maintained by Stormshield using information that providers communicate,
- **Custom web service database**: manually imported by an administrator on the SNS firewall.

Since web services are used in the configuration of the SNS firewall, by managing them, you will have access to all the web services needed to create the desired configurations, and can keep them up to date over time.

Looking up the database of official web services and checking whether it is up to date

This section explains how to look up the database of official web services and how to check whether it is up to date.

Looking up the official web service database

From the Stormshield Security Portal

1. Go to https://security.stormshield.eu/index.php/webservices/.
2. Look up the official web services in the table. For each web service, you will see the number of IP addresses and FQDNs that it contains, as well as any of its known dependencies on other web services.

From the SNS firewall's administration interface

1. Go to **Configuration > Objects > Web services**, **List of web services** tab.
2. Official web services appear. Scroll over one to show its properties:
   - **Name**: name of the official web service,
   - **Description**: short description of what the web service contains,
   - **Read only**: official web services are always in read-only mode,
   - **Revision number** and **Revised on**: these items change as soon as the SNS firewall retrieves a new version of information about the web service,
   - **URL**: list of URLs where information about the web service can be looked up with the provider.

Checking whether the database of official web services is up to date

The database of official web services is regularly and automatically updated with the firewall's Active Update module. To check whether the official web service database is up to date:

1. In the SNS firewall's administration interface, go to **Monitoring > Monitoring > System**, **Active Update** section.
2. Ensure that the status **Up to date** appears in the **Geolocation/reputation & web services** and **Application icons and web services** modules.
   If the status **Disabled** or **Failure** appears, check in **Configuration > System > Active Update** that automatic updates are enabled on the modules in question, and that the SNS firewall can contact the update servers found in the **Advanced properties** area.

Requesting Stormshield to add web services to the official database

1. Log in to your MyStormshield personal area.
2. Go to **Technical support > Request for webservice detection**.
3. Fill out the requested information. The **Web service name** and **Web service URL** fields are mandatory. The provider must provide information about the web service in question (IP addresses and FQDNs) at a public URL. Without it, Stormshield will not be able to add the web service to the official database.
4. Click on **Send**.

You will receive a reply as soon as possible at the e-mail address associated with your MyStormshield account. In the meantime, you can add the web service to your SNS firewall's custom database (refer to the chapter Looking up and managing the custom web service database). If the web service is eventually added to the official database, don't forget to delete it from the custom database.

Looking up and managing the custom web service database

This section explains how to look up and manage (import, export and delete) the custom web service database.

IMPORTANT
The custom database always has priority over the official database. By using a custom database, searches in databases stop once a match is found in the custom database, so ensure that you keep it up to date.

Looking up the custom web service database

1. In the SNS firewall's administration interface, go to **Configuration > Objects > Web services**, **List of web services** tab.
2. Custom web services appear below official web services. Scroll over one to show its properties, which are taken from the last import.
3. You can look up the IP addresses and FQDNs of custom web services by exporting the database. To do so, click on **Export custom database**, accept the download of the CSV file, then locate the desired information in the file.

If no custom web services appear, or if you wish to add, modify or remove a web service from the existing database, you must import a new custom database.

Importing a custom web service database

Before proceeding with any import, take note of the following points:

- You can have only one custom database on the SNS firewall,
- Databases are imported with a CSV file containing information about web services,
- When a custom database is successfully imported, it **deletes and replaces** the existing custom database. When this occurs, ensure that the import file used contains all the custom web services that you wish to keep, otherwise they will be lost,
- You can download the existing database by clicking on **Export custom database** to use it as a template to create the new import file.

Import file: format, structure and limitations

- The file must be in CSV format,
- Each line of the file is made up of several fields, all separated by commas,
- Empty optional fields will be included between two commas,
- The file must contain a blank line after the last entry.

```
#name,#ip/fqdn,#date,#revision,#comment
```

Field	Description
Service name (mandatory)	Text string meeting the following criteria: • Maximum 20 alphanumeric characters, • Case insensitive; the name will always be considered in lowercase. Uppercase characters are not kept on the SNS firewall during import.
IP address or FQDN (mandatory)	Public IPv4/IPv6 address or FQDN. An FQDN can contain **only one** wildcard ***** at the beginning or middle of its name. If a web service relies on several IP addresses or several FQDNs, the line that describes it must be duplicated as many times as the number of addresses IP or FQDNs that the service web contains. Only the optional information from the first line will be kept.
Date of revision (optional)	Date and time of revision in **YYYY/MM/DD** or **YYYY/MM/DD hh:mm** format (e.g., *2022/10/15 10:30*).
Revision number (optional)	Revision number that may contain up to 3 digits: **major.minor.patch** (e.g., *10.2*).
Comments (optional)	Free-form text string that can be placed between quotes if it contains commas.

```
name1,1.1.1.1,2021/09/21 11:00,1.1.1,Simple case
name2,2.2.2.2,2021/12/31,2,"Comment, with comma"
name2,domain.tld,2022/01/01,3,"Date, revision and comment are discarded"
name3,*.newdomain.tld,,,No date and revision
```

There are limits as to the number of lines allowed in the import file:

Physical SNS firewalls

SN160(W)	5 000
SN210(W), SN310	10 000
SN-S-Series-220, SN-S-Series-320, SN510, SN710, SNi20, SNi40	100 000
SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100	1 000 000

Elastic Virtual Appliances (EVA)

EVA with 1 GB of RAM	10 000
EVA with 2 GB to 6 GB of RAM	100 000
EVA with 8 GB to 64 GB of RAM	1 000 000

There is a limit to the possible number of lines containing an FQDN with a wildcard * in the middle: 10% of the number of lines allowed in the import file.

Importing the CSV file

1. In the SNS firewall's administration interface, go to **Configuration > Objects > Web services**, **List of web services** tab.
2. If a custom database already exists, we recommend that you download a copy of it by clicking on **Export custom database**.
3. In the **Import custom services** tab, **Import** section, select the import file. If a custom database already exists, the file must contain the web services that you wish to keep, otherwise they will be deleted. Ensure that the web services you are about to delete are no longer used in the configuration of the SNS firewall (filter policy rules, web service groups, etc.).
4. Click on **Import database**. The import can be canceled at any time before its completion. If an error appears, take note of it and check your import file. Use a text editor rather than Excel to check the file.

A message will inform you that the import completed successfully. If a custom database already existed, it will be deleted and replaced with the new one.

TIP
You can ask Stormshield to add a web service to the official database.

Deleting the custom web service database

1. In the SNS firewall's administration interface, ensure that the custom web services are no longer used in the configuration of the SNS firewall (filter policy rules, web service groups, etc.).
2. Go to **Configuration > Objects > Web services**, **List of web services** tab.
3. We recommend that you download a copy of the custom database before deleting it by clicking on **Export custom database**.
4. Click on **Delete custom database** and confirm.

Managing web service groups

This section explains how to look up and manage (add, delete and change members) web service groups.

The operations in this section must be performed in administration interface of the SNS firewall in **Configuration > Objects > Web services**, **Groups** tab.

Looking up web service groups and their members

Available groups appear in the **List of groups** grid. Two types are available:

- **Predefined groups**: created and maintained by Stormshield, containing only official web services. These groups are always in read-only mode;
- **Custom groups**: created and managed by an administrator on the SNS firewall and may contain both official and custom web services.

For each group, you will see the number of members it contains. Double-click on a group to display its members in the **Members of the group** grid on the right.

Adding a web service group

1. In the **List of groups** grid, click on **Add**.
2. Assign a name to the web service group. Enter comments if necessary.
3. Click on **Apply**.

The group will be created without any members. The **Members of the group** grid appears on the right, allowing you to add members.

Managing members of a web service group

1. In the **List of groups** grid, double-click on the group in question.
2. In the **Members of the group** grid on the right:
   - To add members: click on **Add** and select the official and custom web services to add,
   - To delete members: select the web services in the grid, then click on **Delete** (several can be selected by holding down the **[Ctrl]** key).

Changes are applied immediately after each action.

Deleting a web service group

1. Before deleting a group, ensure that it is no longer used in the configuration of the SNS firewall (in filter policy rules, for example).
2. In the **List of groups** grid, click on the group in question.
3. Click on **Remove**.

Using web services with an SD-WAN or QoS

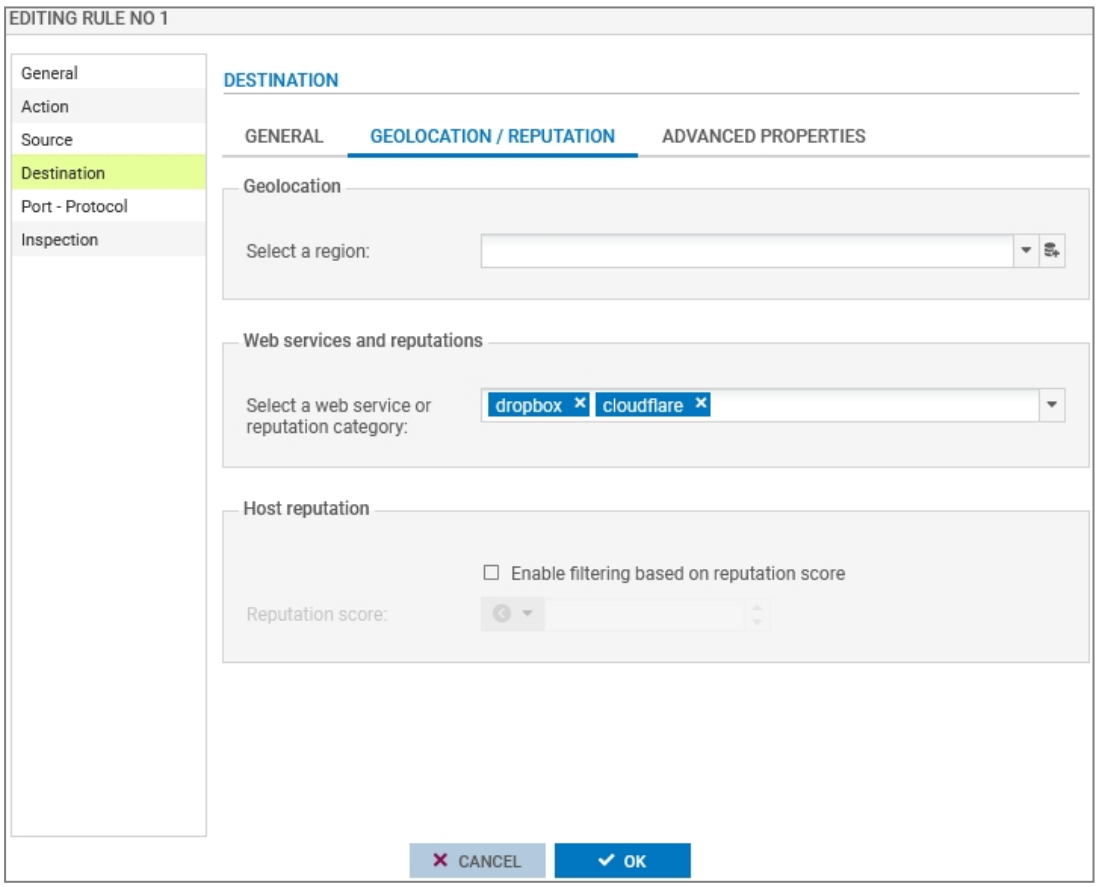
If you have configured on your SNS firewall a Quality of Service (QoS) policy or SD-WAN SLA, you can specify web services as destination criteria in the relevant filter rules.

With QoS, you can reserve or restrict bandwidth for each web service to ensure optimal connectivity for high-priority web traffic. For further information, refer to the technical note on Configuring QoS on SNS firewalls.

With SD-WAN, for each web service, you can set the network links to take automatically and transparently, based on their associated performance constraints, such as accepted latency availability rate, etc.). For further information, refer to the Technical note on SD-WAN - Selecting the best the network link.

As a general rule, to add a web service as a destination criterion in an existing filter rule:

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Double-click on the number of the rule in question.
3. In the window to edit rules, go to the **Destination** tab on the left, then the **Geolocation/Reputation** sub-tab, **Web services and reputations** section, and select the web services in question (official, custom or groups). Remember, you can check the dependencies of official web services on the Stormshield Security Portal.
4. Click on **OK**.



Configuring web service traffic to avoid the proxy

Web services can be configured in such a way to let their traffic avoid the proxy, in order to free up space on the proxy for other traffic. However, this operation should only be applied to web services that you fully trust.

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > Single rule**.
3. Double-click on the number of the new rule.
4. In the window to edit rules, fill out the following information:
   - **General** tab, **Status** field: select *On*,
   - **Action** tab, **Action** field: select *pass*,
   - **Source** tab, **Source hosts** field: select *Network_in*,
   - **Destination** tab:
     - **General** sub-tab, **Destination hosts** field: select *Any*,
     - **Geolocation/Reputation** sub-tab, **Web services and reputations** section: select the web service in question. Remember, to avoid mistakenly allowing certain streams of web traffic, check the dependencies of the web service in question on the Stormshield Security Portal first.
5. Click on **OK**.
6. Place the rule at the top of the filter policy, above any rules that use the SNS firewall's proxy.

Blocking or allowing traffic from a web service

You can block or allow traffic from a web service by adding a rule in the SNS firewall's filter policy.

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > Single rule**.
3. Double-click on the number of the new rule.
4. In the window to edit rules, fill out the following information:
   - **General** tab, **Status** field: select *On*,
   - **Action** tab, **Action** field: select *pass* or *block*,
   - **Source** tab, **Source hosts** field: select the desired objects (e.g., *Network_in*),
   - **Destination** tab:
     - **General** sub-tab, **Destination hosts** field: select the desired objects (e.g., *Any*),
     - **Geolocation/Reputation** sub-tab, **Web services and reputations** section: select the web service in question. Remember, to avoid mistakenly blocking or allowing certain streams of web traffic, check the dependencies of the web service in question on the Stormshield Security Portal first.
5. Click on **OK**.
6. Place rules that allow web service traffic above block rules due to the fact that rules are read in the order of their numbering.

Tracking web service activity

This chapter explains how to track the activity of web services in the SNS firewall's administration interface. These explanations will allow you to adjust your configurations based on the activity of web services that you observe.

In firewall monitoring

Monitoring allows you to view in real time, for each monitored web service:

- The number of connections set up,
- Incoming bandwidth consumed,
- Outgoing bandwidth consumed.

To monitor a web service:

1. Go to **Configuration > Notifications > Monitoring configuration**, **Web service configuration** tab.
2. Click on **Add** and select a web service. You can add up to 10 services.
3. Click on **Apply**.

To look up the curves of monitored web services:

1. Go to **Monitoring > Monitoring > Web services**.
2. Click on the tab of the data that you want to view.

In firewall reports

Reports allow you to view the top 10 web services over a specific time range (last hour, last day, last 7 days and last 30 days) for which:

- There was the most traffic in terms of volume of data exchanged,
- The highest number of connections was recorded.

To look up reports:

1. In **Configuration > Notifications > Report configuration,** ensure that **Static reports** and **Web service** reports are enabled.
2. Go to **Monitoring > Reports > Web services** and click on the report that you want to view.
3. On the report, change the time range if necessary. If you have just enabled the reports, wait for a few minutes while the SNS firewall retrieves enough data to create reports.

In the firewall's audit logs

Some logs may show the source or destination web service. To look up a log, go to **Monitoring > Logs - Audit logs** and select the log in question.

Some information can be accessed if the user has been granted permissions to look up private data. If you hold this permission or a code to access private data, click on **Logs: restricted access** in the upper banner. For further information, refer to the Technical note Complying with privacy regulations.

Further reading

You can find additional information and answers to your questions at the following links:

- Technical note on Configuring QoS on SNS firewalls.
- Technical note on SD-WAN - Selecting the best network access.
- Stormshield knowledge base (authentication required).

documentation@stormshield.eu