



**STORMSHIELD**



TECHNICAL NOTE

**STORMSHIELD NETWORK SECURITY**

# SETTING UP A FILTERING RULE

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

Document last updated: December 9, 2019

Reference: [sns-en-setting\\_up\\_filtering\\_rule\\_Technical\\_Note](#)



# Table of contents

Getting started .....	3
Requirements .....	3
Creating network objects .....	4
Selecting a filtering policy .....	5
Adding a filtering rule .....	6
State .....	6
Action .....	6
Source .....	6
Destination .....	6
Destination port .....	6
Rule for administering the Firewall .....	7
Activating the filtering policy .....	8
Testing the Filter / NAT policy .....	9
Further reading .....	10



## Getting started

In this example, you wish to authorize HTTP access from a workstation on the internal network to an intranet server (located in a DMZ for example) through your Stormshield Network firewall.

### **i** NOTE

For connections to another type of application server, such as a database server for example, the procedure is the same except for the value of the destination port(s).

## Requirements

The client workstation and intranet server must be able to dialogue:

- Either by using the Firewall as the default gateway,
- Or by using a static route via the Firewall.



## Creating network objects

1. Click on **Configuration > Objects > Network objects**, then on **Add**.
2. In the wizard, ensure that the **Host** tab has been selected.
3. Fill in the **Object name** and **IP address** fields for the client workstation (**client\_desktop** object).
4. Validate by clicking on **Create and duplicate** to continue creating the object **intranet\_server** on the same model.
5. Once the last object has been defined, end the operation by clicking on **Create**.  
Network objects can also be created during the construction of the filter policy (during the stages of selecting sources and destinations).

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

IP address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name: client\_desktop

IPv4 address: 192.168.0.1

IPv6 address: No IP address defined

MAC address: 01:23:45:67:89:ab (optional)

Resolution

None (static IP)  Automatic

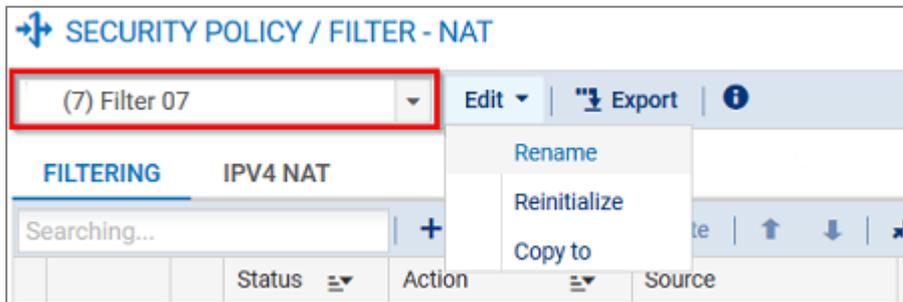
Comments:



## Selecting a filtering policy

In the **Configuration** menu:

1. Click on **Security policy > Filter – NAT**.
2. Select the filtering policy to modify.
3. You can rename this policy by clicking on **Edit > Rename**.





## Adding a filtering rule

1. In the **Filtering** tab, click on **New rule > Standard rule**.
2. A new rule, which is disabled by default, is created.

### State

1. Double-click on the value **off** in the **Status** column.
2. The status of the rule will change to **on**.

### Action

1. Double-click on the value **Block** in the **Action** column:
2. In the **Action** field, select **pass**,
3. In the **Log level** field, select **log** if you want traffic matching this rule to be reflected in the Firewall's filter logs.

### Source

1. Double-click on the value **Any** in the **Source** column.
2. In the **Source hosts** field, select the network object **client\_desktop**.

#### **i** NOTE

You can refine your filter rule by indicating in the **Incoming interface** field an interface on which your client workstation's network is connected.

### Destination

1. Double-click on the value **Any** in the **Destination** column.
2. In the **Destination hosts** field, select your network object **intranet\_server**.

#### **i** NOTE

You can refine your filter rule by indicating in the **Outgoing interface (Advanced properties tab)** field the network interface to which the intranet server is connected.

### Destination port

1. Double-click on the value **Any** in the **Destination port** column.
2. In this case for the **Destination port** field, select **HTTP**.



## Rule for administering the Firewall

Following the method described above, add a rule allowing the Firewall to be administered (rule 2):

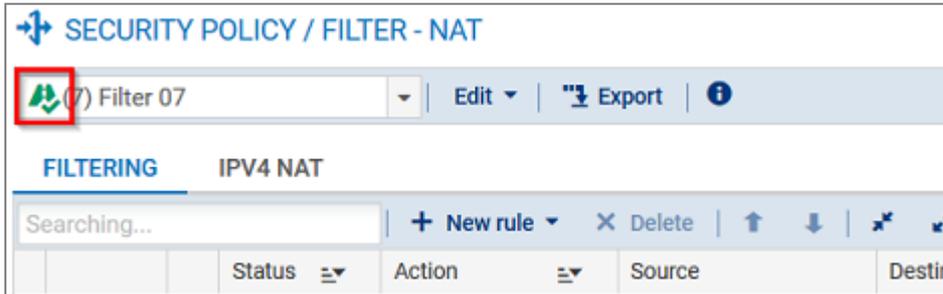
- Source: **Any** (or a group of authorized hosts)
- Destination: **Firewall\_Bridge** object
- Port: **Admin\_Srv** object

FILTERING		IPV4 NAT						
Searching...		+ New rule   X Delete   ↑ ↓   ✂ Cut   📄 Copy   📄 Paste   🔍 Search in logs   🔍 Search						
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	
1	on	pass	client_desktop	intranet_server	http		IPS	
2	on	pass	Any	Firewall_bridge	Admin_srv		IPS	



## Activating the filtering policy

1. At the bottom of the *Filter-NAT* window, click on **Save and apply**.
2. Confirm by clicking on **Yes, activate the policy**.
3. The active policy is recognizable by an icon.





## Testing the Filter / NAT policy

---

You have reached the end of the procedure, and your intranet must be accessible from your client workstation. In a web browser, type the server's URL, for example, "http://intranet\_server\_IP\_address".

If the intranet server's home page does not appear, check the following points:

- Have you activated your filter/NAT policy and the rules associated with it?
- Has routing between the client workstation and the server been defined (static routes, default gateway to the Firewall)?
- Is the web service running on the server?
- Is there a firewall blocking the connection on the workstation or the server?



## Further reading

---

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



**STORMSHIELD**

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)

*All images in this document are for representational purposes only, actual products may differ.*

*Copyright © Stormshield 2023. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.*