TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

EVA ON 3DS OUTSCALE

Product concerned: SNS 3.11.8 and higher versions, SNS 4.x

Document last updated: June 30, 2021

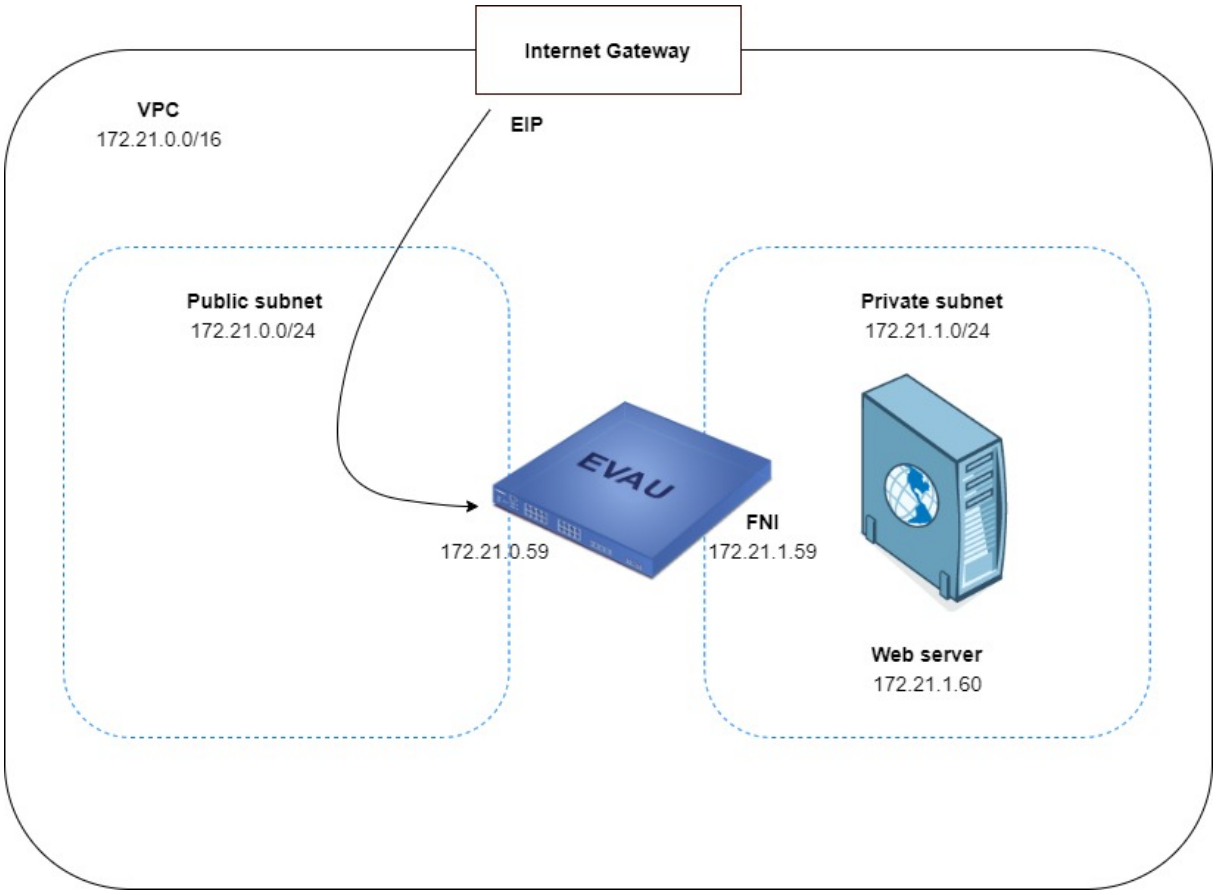
Reference: sns-en-eva_on_3DS_OUTSCALE_technical_note

Table of contents

Getting started

This technical note explains how to the hosting platform 3DS OUTSCALE can be used to deploy a Stormshield Network Security Elastic Virtual Appliance (EVA) firewall and a web server protected by this firewall.

The deployed firewall is equipped with two network interfaces - a public (unprotected) interface and a private (protected) interface.



Obtaining the firewall license

Once the deployment is complete, your EVA will require a software license in order to run.

Get in touch with your Stormshield distributor to order the license for your EVA. If you do not already have a Stormshield distributor, use our search engine to locate one close to where you are.

Deploying the SNS EVA firewall

Deploying an SNS EVA firewall on the Outscale platform involves a number of steps, all of which are completed from the Outscale administration console.

To deploy a firewall, log in to the COCKPIT 3DS OUTSCALE console.

The following steps are required in the configuration:

- Creating an SSH key (*Keypair),*
- Creating a Virtual Private Cloud (*VPC*),
- Creating an Internet gateway (*Gateway*),
- Creating a default route,
- Creating a security group for traffic with the outside,
- Creating a security group for traffic between protected hosts,
- Creating the SNS EVA firewall instance,
- Allocating an external IP address (EIP) to the SNS instance,
- Creating the private network interface of the SNS instance,
- Disabling the **Check Source and Destination** option,
- Creating a new route table and a default route for the private network,
- Enabling the SNS EVA firewall.

Creating an SSH key (*Keypair)*

This key makes it possible to authenticate via SSH on hosts (SNS firewall, web server, etc.) deployed on the Outscale platform.

Creating an SSH key

In the COCKPIT 3DS OUTSCALE console, under the **Network/Security** menu:

1. Select **Keypairs**.
2. Click on **Create**.
3. Enter a name for the new SSH key (e.g., *Documentation-keypair*) and click on **Create**.
   An SSH key will be generated and a dialog box opens to allow the key to be downloaded.
4. Download the SSH key and save it on your workstation.

Creating a VPC for instances to be deployed

The VPC (*Virtual Private Cloud*) is the virtual network in which the SNS EVA firewall, and the hosts that it protects, will be deployed. The VPC comprises two sub-networks:

- A public sub-network to which the public interface (out) of the SNS EVA firewall will be attached,
- A private sub-network to which the protected interface (in) of the SNS EVA firewall, and the interfaces of the protected hosts, will be attached.

Creating the VPC

In the COCKPIT 3DS OUTSCALE console, under the **VPC** menu:

1. Select **VPC**.
2. Click on **Create,** then **Expert mode**.
3. Enter a name for the VPC (e.g., *Documentation-VPC*) and the associated network in CIDR notation (e.g., *172.21.0.0/16*).
4. Confirm by clicking on **Create**.

Creating the public sub-network of the VPC

1. Click on the VPC created earlier to select it (*Documentation-VPC* in the example).
   Details about the VPC will appear in the lower section of the configuration window.
2. Click on **Create Subnet**.
3. Enter a name (e.g., *Documentation-VPC -Public*) and the associated network in CIDR notation (e.g., *172.21.0.0/24*).
   This sub-network must be part of the VPC's network.
4. Select the geographic area in which this sub-network is available (*eu-west-2a* in the example).
5. Confirm by clicking on **Create**.

Creating the private sub-network of the VPC

1. Click on **Create Subnet** again.
2. Enter a name (e.g., *Documentation-VPC -Private*) and the associated network in CIDR notation (e.g., *172.21.1.0/24*).
   This sub-network must be part of the VPC's network.
3. Select the geographic area in which this sub-network is available (*eu-west-2a* in the example).
4. Confirm by clicking on **Create**.

Creating an Internet gateway

This is the gateway through which the SNS EVA firewall and the hosts it protects access the Internet.

Creating the Internet gateway

In the COCKPIT 3DS OUTSCALE console, under the **VPC** menu:

1. Select **Internet gateways**.
2. Click on **Create**.
3. Confirm by clicking on **Create**.

Attaching the Internet gateway to the firewall's VPC

1. Select the gateway created in the previous step.
2. Click on **Attach.**
3. Select the firewall's VPC (*Documentation-VPC* in the example).
4. Confirm by clicking on **Attach**.

Creating a default route

The purpose of creating one is for all outbound traffic to take a default route to the Internet gateway.

Creating a default route in the route table of the VPC

In the COCKPIT 3DS OUTSCALE console, under the **Network/Security** menu:

1. Select **Route tables**.
2. Select the route table corresponding to the VPC created earlier (*Documentation-VPC* in the example).
   Details about the route table will appear in the lower section of the configuration window.
3. In the details of the route table, click on **Create Route**.
4. In the **Target** field, select your Internet gateway.
5. Click on **All IPs**.
   The value 0.0.0.0/0 will automatically be entered in the **Destination** field.
6. Confirm by clicking on **Create**.

Associating this route table with the public sub-network of the VPC

1. Select the route table corresponding to the VPC created earlier (*Documentation-VPC* in the example).
2. Click on **Attach.**
3. Select the public subnetwork of the VPC (*Documentation-VPC-Public* in the example).
4. Click on **Attach** to confirm the configuration.
   The **Explicit associations** column reflects this new status (switched from 0 to 1).

Creating a security group for traffic to and from the outside

This security group brings together rules for traffic allowed from external networks to the firewall and protected hosts, and from protected networks to the outside.
In this technical note, the following inbound traffic streams allowed :

- SSH: access to the firewall in console,
- SSH redirection port (e.g., TCP port 2222): access to the protected web server in console,
- HTTPS: access to the firewall's web administration interface,
- HTTP: access to the web server protected by the firewall.

Creating the security group

In the COCKPIT 3DS OUTSCALE console, under the **Network/Security** menu:

1. Select **Security groups**.
2. Click on **Create**.
3. Name the security group (e.g., *Documentation-Security-Group*).
4. Add a description (e.g., *SSH HTTPS HTTP Inbound access*).
5. Select the VPC (*Documentation-VPC* in the example).
6. Click on **Create**.

Creating security rules corresponding to traffic allowed with the outside

1. Select the security group created earlier (*Documentation-Security-Group* in the example). The list of rules attached to the security group appears in the lower section of the configuration window.
2. In the list of rules, click on **Create rule**.
3. Select **Inbound** mode.
4. Set **SSH** as the protocol.
5. Click on **All IPs**.
6. Click on the + symbol.
7. Repeat steps 3 to 6 with **HTTP** and **HTTPS**.
8. Repeat steps 3 to 6 with the values **Inbound**, **Custom, TCP**, **2222** and **All IPs**.
9. Confirm the rules by clicking on **Create**.

IMPORTANT
A rule allowing outbound traffic will automatically be created.
This rule must not be deleted because it allows outbound traffic that is necessary to get security updates for instances deployed in the VPC.

The list of rules regarding traffic allowed for the security group will then look like this:

Details for Documentation-Security-Group (sg-50df5ea2)

+ CREATE RULE | − DELETE RULE

Service	Type	Protocol	From Port	To Port	CIDR	Group
SSH	inbound	tcp	22	22	0.0.0.0/0	
HTTP	inbound	tcp	80	80	0.0.0.0/0	
HTTPS	inbound	tcp	443	443	0.0.0.0/0	
Custom	outbound	-1			0.0.0.0/0	

Creating a security group for traffic between protected hosts

This security group brings together rules for traffic allowed between protected hosts.

In this example, all protocols are allowed: traffic between protected hosts can in fact be filtered and inspected thoroughly on the SNS firewall.

Creating the security group

In the COCKPIT 3DS OUTSCALE console, under the **Network/Security** menu:

1. Select **Security groups**.
2. Click on **Create**.
3. Name the security group (*Documentation-Pass*-All in the example).
4. Add a description (*Pass all* in the example).
5. Select the VPC (*Documentation-VPC* in the example).
6. Click on **Create**.

Creating security rules corresponding to traffic between protected hosts

1. Select the security group created earlier (*Documentation-Pass-All* in the example).
   The list of rules from the security group appears in the lower section of the configuration window.
2. In the list of rules, click on **Create rule**.
3. Select **Inbound** mode.
4. Set **Custom** as the protocol.
5. Select **All** as the port.
6. Click on **All IPs**.
7. Click on the + symbol.
8. Confirm by clicking on **Create**.

IMPORTANT
A rule allowing outbound traffic will automatically be created.
This rule must not be deleted.

The list of rules regarding traffic allowed for the security group assigned to protected hosts will then look like this:

Details for Documentation-Pass-All (sg-989d15dc)

+ CREATE RULE | − DELETE RULE

Service	Type	Protocol	From Port	To Port	CIDR	Group
Custom	inbound	-1			0.0.0.0/0	
Custom	outbound	-1			0.0.0.0/0	

Creating the SNS EVA firewall instance

The deployed instance of the SNS EVA firewall is attached to the VPC, security group for traffic with the outside, SSH key and public network created earlier.

Creating the firewall instance

In the COCKPIT 3DS OUTSCALE console, under the **Compute** menu:

1. Select **Instances**.
2. Click on **Create,** then **Expert mode**.
3. Name the instance (e.g., *Documentation-SNS-EVA*) and click on **Next**.
4. Enter **SNS** in the search field, then select the desired firewall model.
5. Click on **Next**.
6. Define the properties of your instance, according to the properties chosen when you acquired your EVA license from Stormshield (cf. Stormshield Network Security Elastic Virtual Appliances – EVA datasheet):
   - The **CPU Generation**,
   - The desired **Performance** level (3DS OUTSCALE parameter),
   - The number of **Cores**,
   - The amount of **Memory** (GB) allocated to the virtual machine.

IMPORTANT
For optimal performance, ensure that these properties match those in your EVA license.

7. Click on **Next**.
8. Select the **VPC** (*Documentation-VPC* in the example).
9. Select the public sub-network of the VPC (*Documentation-VPC-Public* in the example).
10. Enter the IP address to associate with the firewall's public interface.
    This address (172.21.0.59 in the example) must belong to the sub-network selected in step 9.
11. Select the geographic area in which this sub-network is available (*eu-west-2a* in the example).
12. Click on **Next**.
13. Select the security group for traffic with the outside (*Documentation- Security-Group* in the example).
14. Click on **Next**.
15. Select the SSH key created at the start of the process (*Documentation-Keypair* in the example).
16. Click twice on **Next**.
    You will be shown a summary of the instance.
17. Confirm the creation of the instance by clicking on **Create**.

NOTE
The *admin* account password is the instance ID;
With this *admin* account, the user can connect:

- In SSH to the firewall's public IP address using a tool such as *PuTTY*.
- In HTTPS to the firewall's web administration interface (https://firewall_public_ip_address/admin).

This password must be changed for security reasons during the initial connection to the firewall.

Allocating an external IP address (EIP) to the SNS instance

Creating the external IP address

In the COCKPIT 3DS OUTSCALE console, under the **Network/Security** menu:

1. Select **External IPs**.
2. Click on **Allocate**.
3. Name the external IP address (e.g., *Documentation-Public-IP*).
4. Confirm by clicking on **Allocate**.
   An external IP address is created.

Allocating the address to the instance

1. Select the external IP address created earlier (*Documentation-Public-IP* in the example)
2. Click on **Associate instance**.

3. Select your SNS EVA instance (*Documentation-SNS-EVA* in the example).
4. Confirm by clicking on **Associate**.

Creating the private interface of the SNS instance

Here, a second network interface (located in the private network) is created for the SNS instance in the VPC.

This interface will be associated with the protected interface (*in* interface) of the firewall.

Creating the private flexible network interface

In the COCKPIT 3DS OUTSCALE console, under the **Network/Security** menu:

1. Select **Flexible network interfaces**.
2. Click on **Create**.
3. Name the interface (e.g., *Documentation-Private-Interface*).
   You can add a **Description** (optional).
4. Select the private sub-network of your VPC (*Documentation-VPC-Private* in the example).
5. Enter an IP address for this private interface (e.g., *172.21.1.59*). This address must belong to the private sub-network selected in step 5.
6. Select the security group for traffic between protected hosts (*Documentation-Pass-All* in the example).
7. Click on **Create**.

Attaching this interface to the SNS EVA instance

In the list of interfaces:

1. Select the interface created earlier (*Documentation-Private-Interface* in the example)
2. Click on **Attach.**
3. Select the EVA instance (*Documentation-SNS-EVA* in the example).
4. For the device: select the value 1 (the external interface of the SNS firewall created by default with the instance that has 0 as its index).

Restarting the firewall

The SNS EVA firewall must be restarted to apply the new private interface:

1. In the **Compute** menu, click on **Instances**.
2. Select the instance to restart (*Documentation-SNS-EVA* in the example).
3. Click on **Restart**.
4. Confirm.

Disabling the Check Source and Destination option

To allow traffic to be routed transparently, i.e., the SNS firewall will filter it, this option must be disabled.

In the COCKPIT 3DS OUTSCALE console, under the **Compute** menu:

1. Select **Instances**.
2. Select your SNS EVA instance (*Documentation-SNS-EVA* in the example).
3. Click on the ··· menu in the upper right section of the instance configuration page.
4. Select **Attributes**.
5. Expand the **Check Source and Destination** field.
6. Click on the selector to show **False** as the value.
7. Confirm the configuration by clicking on **Close**.

Creating a new route table and a default route for the private network

The purpose of creating one is for protected hosts to take a default route to the private interface of the SNS firewall.

Creating the private route table

In the COCKPIT 3DS OUTSCALE console, under the **Network/Security** menu:

1. Select **Route tables**.
2. Click on **Create**.
3. Name your route table (e.g., *Documentation-Private-Route-Table*).
4. Select the associated VPC (*VPC Documentation* in the example).
5. Confirm by clicking on **Create**.

Creating the route in the private route table of the VPC

1. Select the private route table created earlier (*Documentation-Private-Route-Table* in the example).
   Details about the route table will appear in the lower section of the configuration window.
2. In the details of the route table, click on **Create Route**.
3. In the **Target** field, select the private interface of your SNS EVA instance (*Documentation-Private-Interface* in the example).
4. Click on **All IPs**.
   The value 0.0.0.0/0 will automatically be entered in the **Destination** field.
5. Confirm by clicking on **Create**.

Associating this route table with the private sub-network of the VPC

1. Select the private route table created earlier (*Documentation-Private-Route-Table* in the example).
2. Click on **Attach.**
3. Select the private subnetwork of the VPC (*Documentation-VPC-Private* in the example).
4. Click on **Attach** to confirm the configuration.
   The **Explicit associations** column reflects this new status (switched from 0 to 1).

Enabling the SNS EVA firewall

The default serial number of EVA firewalls is VMSNSX00Z0000A0.

When the firewall is enabled, the virtual firewall can be assigned a model, its permanent serial number, its license as well as the subscribed options.

Downloading the initialization kit

1. Log in to your private-access area on Mystormshield.
2. Go to **Products > Product management.**
3. Select the model and serial number of your firewall from the list of registered firewalls.
4. In the **Downloads** window, indicate the version of the activation kit that you wish to install.
5. Click on the **Download the activation kit** link.
6. Save this file on your workstation.

Changing the *admin* account password

1. Log in to the web administration interface of the firewall: https://firewall_public_ip_address/admin.
2. Enter the user name of the *admin* account and its password (instance ID).
3. Go to the **Configuration** tab in **System > Administrators > Admin account** tab.
4. Enter the **Old password** (instance ID).
5. Enter the new password in the **New password** and **Confirm password** fields.
6. Click on **Apply**, then on **Save** to confirm the changes.

Installing the initializing kit on the firewall

1. Go to the **Configuration** tab in **System > Maintenance > System update** tab.
2. Click on the selector to the right of the **Select the update** field and select the activation kit that was downloaded earlier (*.maj file).
3. Click on **Update firmware**.
   The firewall will restart during the installation of the initialization kit
   This operation may take several minutes.

Creating the web server instance

The purpose of creating one is to deploy a server instance (Linux/Ubuntu distribution used in this technical note) connected to the VPC, security group for traffic between protected hosts, private sub-network and SSH key created in the previous steps.

Creating the server instance

In the COCKPIT 3DS OUTSCALE console, under the **Compute** menu:

1. Select **Instances**.
2. Click on **Create,** then **Expert mode**.
3. Name the instance (e.g., *Documentation-Web-Server*) and click on **Next**.
4. Indicate the desired operating system type in the search field (Ubuntu in the example), then select the desired model.
5. Click on **Next**.
6. Select according to your requirements:
   - The **CPU Generation**,
   - The desired **Performance** level (3DS OUTSCALE parameter),
   - The number of **Cores**,
   - The amount of **Memory** (GB) allocated to the virtual machine.
7. Click on **Next**.
8. Select the **VPC** (*Documentation-VPC* in the example).
9. Select the private sub-network of the VPC (*Documentation-VPC-Private* in the example).
10. Enter the IP address of the server.
    This address (e.g., 172.21.1.60) must belong to the sub-network selected in step 9.
11. Select the geographic area in which this sub-network is available (*eu-west-2a* in the example).
12. Click on **Next**.
13. Select the security group for traffic between protected hosts (*Documentation-Pass-All* in the example).
14. Click on **Next**.
15. Select the SSH key (*Documentation-Keypair* in the example).
16. Click twice on **Next**.
    You will be shown a summary of the instance.
17. Confirm the creation of the instance by clicking on **Create**.

Configuring the SNS firewall

This section explains the most basic configuration required to protect the web server and allow it to be accessed through the SNS firewall.

Creating network objects relating to the web server

This section explains how to create network objects relating to the web server, which will be used in the firewall's configuration:

- A host object with the IP address of the web server instance,
- A port object, separate from the standard SSH object, to allow the SSH connection to the web server.

Connecting to the firewall

1. Log in to the web administration interface of the firewall: https://firewall_public_ip_address/admin.
2. Enter the user name of the *admin* account and its password.

Creating the host object for the web server

In the **Configuration** tab in **Objects** > **Network objects**::

1. Click on **Add**.
2. Select **Host** in the menu on the left.
3. Enter the **Object name** (e.g., *webserver*).
4. Enter the **IPv4 address** that you assigned to the server when the web server instance was created (172.21.1.60 in the example).
5. Click on **Create** to confirm the creation of the object.

Creating the port object for SSH redirection

In the **Configuration** tab in **Objects** > **Network objects**::

1. Click on **Add**.
2. Select **Port** in the menu on the left.
3. Enter the **Object name** (e.g., *SSH-Webserver*).
4. Enter the **Port** (2222 in the example).
5. Set TCP as the **Protocol.**
6. Click on **Create** to confirm the creation of the object.

Creating the filtering policy

Go to the **Configuration** tab in **Security policy** > **Filter - NAT**.

The active security policy, created automatically when the SNS instance is moved, appears: slot *(9) Outscale*. This policy contains a rule that allows SSH access to the firewall.

Adding the rule for HTTP access to the web server

1. Select the rule for SSH access to the firewall by clicking once.
2. Click on **New rule,** then **Single rule**.
   An inactive rule is added immediately after the rule selected in step 1.
3. Double-click on the new inactive rule.
   A window appears, allowing you to edit this rule.

General menu

Set the **Status** to *On*.

Action menu

1. Select the **General** tab.
2. Set the **Action** to *pass*.

Source menu

1. Select the **General** tab.
2. In the **Incoming interface** field, select the *out* interface.

Destination menu

1. Click on the **General** tab.
2. Click on **Add** in the **Destination hosts** field.
3. Type *firewall* to filter hosts, then select the *Firewall_out* object.
4. Select the **Advanced properties** tab.
5. In the **NAT on the destination** > **Destination** field, type *web* to filter hosts, then select the *webserver* object.

Port/Protocol menu

1. In the **Destination port** field, click on **Add**.
2. Type *http* to filter ports, then select the *http* object.
3. Confirm by clicking on **OK**.

Adding the rule for SSH access to the web server

1. Select the rule created earlier for HTTP access to the web server by clicking once.
2. Click on **New rule,** then **Single rule**.
   An inactive rule is added immediately after the rule selected in step 1.
3. Double-click on the new inactive rule.
   A window appears, allowing you to edit this rule.

General menu

Set the **Status** to *On*.

Action menu

1. Select the **General** tab.
2. Set the **Action** to *pass*.

Source menu

1. Select the **General** tab.
2. In the **Incoming interface** field, select the *out* interface.

Destination menu

1. Click on the **General** tab.
2. Click on **Add** in the **Destination hosts** field.
3. Type *firewall* to filter hosts, then select the *Firewall_out* object.
4. Select the **Advanced properties** tab.
5. In the **NAT on the destination** > **Destination** field, type *web* to filter hosts, then select the *webserver* object.

Port/Protocol menu

1. In the **Destination port** field, click on **Add**.
2. Type *ssh* to filter ports, then select the *SSH-Webserver* object.
3. In the Translated destination port field, select the *ssh* object.
4. Confirm by clicking on **OK**.

Adding the Internet access rule for protected hosts

1. Select the rule created earlier for SSH redirection to the web server by clicking once.
2. Click on **New rule,** then **Single rule**.
   An inactive rule is added immediately after the rule selected in step 1.
3. Double-click on the new inactive rule.
   A window appears, allowing you to edit this rule.

General menu

Set the **Status** to *On*.

Action menu

1. Select the **General** tab.
2. Set the **Action** to *pass*.

Source menu

1. Select the **General** tab.
2. In the **Incoming interface** field, select the *in* interface.

Destination menu

1. Click on the **General** tab.
2. Click on **Add** in the **Destination hosts** field.
3. Type *inter* to filter hosts, then select the *Internet* object.
4. Confirm by clicking on **OK**.

Adding rule separators (optional)

Rule separators can be added to the filter policy to make it easier to read.

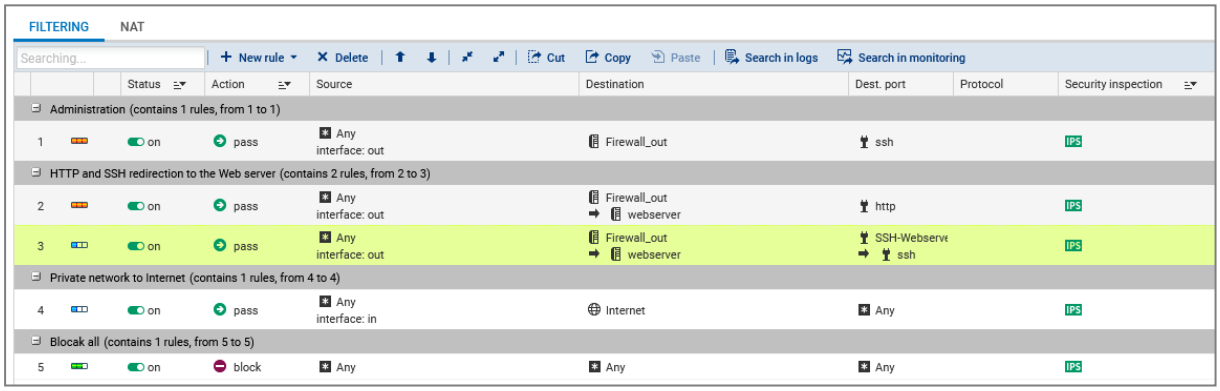
1. Select the rule before which you want to insert a separator by clicking once.
2. Click on **New rule**, then **Separator – rule grouping**.
   A rule separator is added immediately in front of the rule selected in step 1.
3. Double-click on the separator.
4. Enter text to describe each separator.

EXAMPLES

In the suggested configuration, four separators can be added. For example:

- Administration,
- HTTP and SSH redirection to the web server,
- Private network to the Internet,
- *Block all*.

The filter policy will then look like this:



Creating the NAT policy

A NAT rule is needed for connections from protected hosts to the Internet.

Creating the NAT rule

1. Go to the **Configuration** tab in **Security policy > Filter - NAT > NAT** tab.
2. Click on **New rule** then on **Single rule**.
   An inactive rule is added immediately after the rule selected in step 1.
3. Double-click on the new inactive rule.
   A window appears, allowing you to edit this rule.

General menu

Set the **Status** to *On*.

Original source menu

1. Select the **General** tab.
2. In the **Incoming interface** field, select the *in* interface.

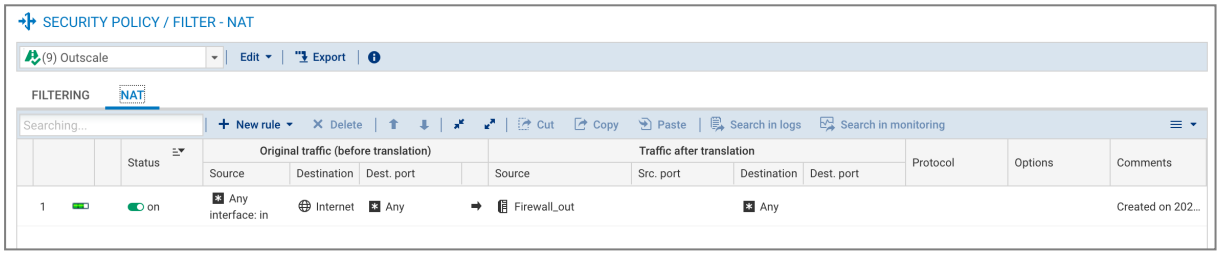
Original destination menu

1. Click on the **General** tab.
2. Click on **Add** in the **Destination hosts** field.
3. Type *inter* to filter hosts, then select the *Internet* object.

Translated source menu

1. Click on the **General** tab.
2. In the **Translated source host** field, type *firew* to filter hosts and select *Firewall_out*.
3. Confirm by clicking on **OK**.
4. Click on **Apply**, then on **Yes, activate the policy** to apply the changes.

The NAT policy will then look like this:



Installing the web server service

This section explains how to connect to the web server to install the Apache service on it.

The connection port used is the SSH redirection port (TCP port 2222 in the example) added to the security group for traffic from outside.

Connecting to the web server in SSH

1. Run a *Powershell* command window (Microsoft Windows workstations) or a *shell* window (Linux workstations).
2. Use the *cd* command to go to the folder containing the SSH key that was downloaded when it was created

EXAMPLE
`cd c:\Temp` (Microsoft Windows workstations)
`cd \home\documentation` (Linux workstations)

3. The preset user name to connect to the web server instance is *outscale*.
   Enter the command:

```
ssh -i file_name_SSH_key-p port_redirection_ssh outscale@public_ip_address
```

EXAMPLE
```
ssh -i Documentation-keypair.rsa -p 2222 outscale@1.2.3.4
```

You are now connected to the server.

Installing the Apache service on the web server (Linux/Ubuntu servers)

1. Type the command `sudo apt-get install apache2.`
2. Confirm the installation by typing *y*.
   The packets required for the Apache server to run are installed.

Testing access to the web server

On a client workstation:

1. Open a web browser.
2. Enter the URL `http://firewall_ip_address`.
   The welcome page of the web server should appear.

Further reading

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

documentation@stormshield.eu