TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY
ELASTIC VIRTUAL APPLIANCE

DEPLOYING AN SNS EVA VIRTUAL FIREWALL IN MICROSOFT AZURE

Product concerned: SNS 4.x

Document last updated: September 9, 2022

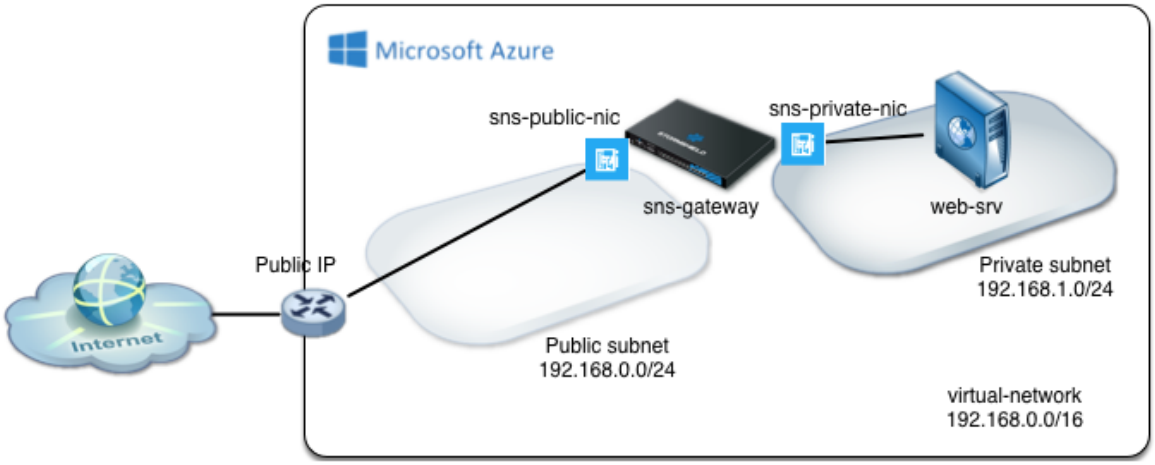
Reference: sns-en-eva_on_microsoft_azure_technical_note

Table of contents

Getting started

This technical note explains how to deploy an SNS EVA virtual firewall equipped with two network interfaces - a public (unprotected) interface and a private (protected) interface - in Microsoft Azure.

You can perform the operations explained in this document when you deploy an SNS EVA virtual firewall. Some of them work in all situations while others work in an architecture that serves as an example. Since there are many possible configurations, adapt these examples to your own requirements.



"Stormshield Network Security Elastic Virtual Appliance" is referred to as "SNS EVA" in the rest of this document.

Requirements and technical characteristics

Requirements

- **An Azure or Microsoft account.**
  To create an account, go to the Stormshield Elastic Virtual Appliance page on Microsoft Azure Marketplace and click on **Get it now**.
- **An active Azure subscription.**
  To check or manage your subscriptions, log in to the Microsoft Azure portal and click on **Subscriptions**.
- **An SNS EVA product license.**
  If you do not already have a license, get in touch with your Stormshield distributor to order one. Use our search engine to locate a distributor close to you.

Technical characteristics of Microsoft Azure instances

Azure instance	vCPU	RAM	Network interfaces	Bandwidth (Mb/s)	EVA model
F1	1	2	2	Moderate: 750	EVA1
F2	2	4	2	High: 1500	EVA2 or EVA3
F4	4	8	4	High: 3000	EVA4
F8	8	16	8	High: 6000	EVAU
F16	16	32	8	Very high: 12000	EVAU

Technical characteristics of SNS EVA firewalls

Model	RAM	HDD	vCPU
EVA1	max = 2 GB	10 GB (2 GB for swap)	max = 1
EVA2	max = 3 GB	10 GB (2 GB for swap)	max = 2
EVA3	max = 6 GB	10 GB (2 GB for swap)	max = 4
EVA4	max = 8 GB	10 GB (2 GB for swap)	max = 4
EVAU	max = 64 GB	10 GB (4 GB of swap)	max = 16

Registering your SNS EVA product

To register your SNS EVA product, you will need its serial number and registration password. You can find them in the e-mail you received after your order was placed.

Once you have gathered all this information, you can register your firewall in the MyStormshield personal area, where you can link your product to your MyStormshield account. The registration process varies depending on whether you already have an account.

You already have a MyStormshield account

1. Log in to your MyStormshield personal area.
2. Go to **Products > Product management**.
3. Click on **Register an SNS appliance**.
4. If the conditions of use and user license appear, read them before accepting them.
5. Fill in the required information until your product is registered.

For further information, refer to the guide on Registering products.

You do not have a MyStormshield account

Your product will be registered when your account is created.

To do so, refer to the guide on Creating an account and registering a product.

Deploying the SNS EVA virtual firewall

There are two ways in which the SNS EVA virtual firewall can be deployed in Microsoft Azure:

- From the Microsoft Azure portal: this method makes it possible to deploy a firewall with a single interface. An additional operation will be required after deployment to add more interfaces.
- From the Stormshield *azure-templates* area on GitHub: with this method, you can deploy a firewall with two pre-configured interfaces by using a custom template.

Deploy your SNS EVA virtual firewall according to the method of your choice. Remember, you need an active Azure subscription (see Requirements).

Deploying the firewall from the Microsoft Azure portal

Deploying the firewall

1. Sign in to the Microsoft Azure portal.
2. Click on **Create a resource**.
3. Search for the resource **Stormshield Elastic Virtual Appliance** and go to its page.
4. Click on **Create**.
5. In **Project details**:
   - **Subscription** field: select an Azure subscription linked to your account,
   - **Resource group** field: select or create a resource group (*SNS-Documentation* in the example).
6. Fill in the form with information about your deployment.
7. Click on **Review + Create**.

Adding a new interface to the firewall

1. In the Microsoft Azure portal once again, click on **Create a resource**.
2. Search for the resource **Network interface** and go to its page.
3. Click on **Create**.
4. In **Project details**:
   - **Subscription** field: select an Azure subscription linked to your account,
   - **Resource group** field: select the firewall's resource group.
5. Fill in the form and click on **Review + Create**.
6. Search for the firewall's virtual machine and click on its name.
7. Click on **Stop** and confirm. Wait for the status of the virtual machine to turn to **Stopped**.
8. In **Settings > Networking**, click on **Attach network interface**.
9. Select the network interface to attach and confirm.
10. Search for the new network interface and select it to show information about it.
11. In **Settings > IP configurations**, enable **IP forwarding**. This setting allows the firewall to redirect traffic from protected virtual machines.
12. Restart the firewall's virtual machine.

Once this is done, continue to the chapter Activating the SNS EVA virtual firewall.

Deploying the firewall from the Stormshield *azure-templates* area on GitHub

1. Go to the Stormshield *azure-templates* area on GitHub.
2. Click on **Deploy to Azure**.
3. Sign in to the Microsoft Azure portal. The customized deployment form will then appear. All of the values can be customized according to your requirements.
4. In **Project details**:
   - **Subscription** field: select an Azure subscription linked to your account,
   - **Resource group** field: select or create a resource group (*SNS-Documentation* in the example),
5. In **Instance details**, review and enter the information in the following fields:

Field	Description
Region	Geographical location in which the firewall is hosted.
SNS Admin password	Firewall's *admin* account password.
Vnet Name	Name of the virtual network that groups the firewall's public and private networks (*virtual-network* in the template).
Vnet Prefix	Virtual network and its mask (*192.168.0.0/16* in the template). This network needs to be chosen from the IP address ranges that are not routed over the Internet.
Public Subnet Name	Name of the subnet in which the firewall's public interface is located (*Public* in the template).
Public Subnet Prefix	Public subnet and its mask (*192.168.0.0/24* in the template). This prefix must be a subnet of **Vnet Prefix**.
Private Subnet Name	Name of the subnet in which the firewall's private interface is located (*Private* in the template).
Private Subnet Prefix	Private subnet and its mask (*192.168.1.0/24* in the template). This prefix must be a subnet of **Vnet Prefix**.
SNS Name	Name of the firewall (*sns-gateway* in the template).
SNS If Public Name	Name of the firewall's public interface (*sns-gateway-public-nic* in the template).
SNS If Public IP	IP address of the firewall's public interface (*192.168.0.100* in the template). This address must belong to the subnet **Public Subnet Prefix**.
SNS If Private Name	Name of the firewall's private interface (*sns-gateway-private-nic* in the template).
SNS If Private IP	IP address of the firewall's private interface (*192.168.1.100* in the template). This address must belong to the subnet **Private Subnet Prefix**.
VM Size	The Azure instance with technical properties that match the SNS EVA virtual firewall model that you need (see technical characteristics).
Public IP Name	Name of the public IP address that Microsoft Azure has assigned to the firewall (*sns-gateway-public-ip* in the template).
Route Table Name	Name of the firewall's private routing table (*route-table-private* in the template).

6. When all this information has been entered, click on **Review + Create**.

As soon as the deployment is complete, continue to the chapter Activating the SNS EVA virtual firewall.

Activating the SNS EVA virtual firewall

Your firewall must be activated so that you can assign an EVA model, permanent serial number, license and subscribed options to it.

Retrieving the firewall's public IP address

1. Sign in to the Microsoft Azure portal.
2. Click on **Resource group**.
3. Select the firewall's resource group (*SNS-Documentation* in the example).
4. Click on the **public IP address** entry (*sns-gateway-public-ip* in the example),
5. Take note of the public IP address.

Downloading the activation kit

1. Log in to your MyStormshield personal area.
2. Browse the list of products until you identify the relevant product. Click on it.
3. On the right side of the **Downloads** section, select the **4.x** version branch.
4. Click on the **Download the activation kit** link, then accept the download.

Importing the activation kit

1. Log in to the firewall's administration interface: https://*firewall_public_IP_address*/admin.
2. Authenticate by using the *admin* account and the associated password.
3. In **Configuration > System > Maintenance**, **System update** tab, **Select the update** field: select the activation kit downloaded earlier.
4. Click on **Update firmware**. The firewall will automatically restart.

Checking whether the firewall must be updated

1. In the firewall administration interface, look in the upper banner for the SNS version currently installed.
2. In the MyStormshield, personal area, identify the most recent version in **Downloads > Downloads > Stormshield Network Security > Firmware > 4.X**.
3. If the most recent version is already installed on your firewall, continue to Deploying a virtual server. Otherwise, refer to the version release notes to find out what the latest available version contains.
4. Click on the link corresponding to the EVA firewall model to download the version.
5. In the firewall administration interface, go to **Configuration > System > Maintenance**, **System update** tab.
6. In the **Select the update** field, select the update file.
7. Click on **Update firmware**. The firewall will automatically restart.

Deploying a virtual server

You can deploy a virtual server on which services of your choice can be hosted. This server will be deployed in the network that the SNS EVA virtual firewall protects.

This chapter briefly explains the steps involved in deploying the virtual server. In this example, we will install Ubuntu Server to set up a custom backup server. Since there are many possibilities, adapt these examples to your own requirements.

Deploying the server in a resource group

1. Sign in to the Microsoft Azure portal.
2. Search for the resource that you want to install and go to its page.
3. Click on **Create**.
4. Assign a name to this machine (*Web-Documentation-Server* in the example).
5. Create a user and password.
6. Select the geographical location in which the server is hosted.
7. Select the firewall's resource group (*SNS-Documentation* in the example).
8. In the options, select the virtual network associated with the resource group as well as the private sub-network.
9. Confirm.

Retrieving the public IP address of the virtual server

1. In the Microsoft Azure portal once again, click on **Resource group**.
2. Select the resource group in question (*SNS-Documentation* in the example).
3. Click on the **Public IP address** entry (*Web-Documentation-Server* in the example).
4. Take note of the public IP address.

Installing the desired service on the server

1. Log in to your server.
2. Install the desired service and its dependencies. In the example, we installed Apache.

Allowing traffic to and from the virtual server on the SNS EVA virtual firewall

Now that the firewall and virtual server have been deployed, you must configure the firewall's filter policy to allow traffic to and from the virtual server.

The operations explained in this chapter must be performed when the user is logged in to the firewall's administration interface at: https://*firewall_public_IP_address/*admin.

Creating required network objects

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. Select the desired object type on the left.
4. Give the object a name.
5. Fill in the relevant information according to the required configuration.
6. Click on **Create**.

In the example, we added the following objects:

Object type	Object name	Information about the object
Network	Private_Net	IPv4 address: 192.168.1.0/24
Network	Public_Net	IPv4 address: 192.168.0.0/24
Host	Web_Documentation_Server	IPv4 address: 192.168.1.4
Port	sshwebsrv	Port/Protocol: 222/TCP

Configuring the filter and NAT policy

The filter and NAT policy contains a set of filter rules and NAT rules. The firewall uses the **(9) Azure Default** policy by default, in which administrators of the firewall can access the administration interface and block all other connections.

When you configure your firewall's filter and NAT policy:

- Always save changes in progress by clicking on **Apply**,
- Be careful not to enable incomplete or incorrect filter and NAT policies that may prevent your firewall's administration interface from being reached,
- Remember that the firewall blocks traffic: any traffic that is not explicitly described in the policy will be rejected without being logged, even when this rule does not appear.

Configuring the filter policy

The filter policy can be configured in **Configuration > Security Policy > Filter - NAT, Filtering** tab. We added three rules to meet the following requirements:

1. Allow the hosts that are hosted on the private network to access all hosts.
2. Allow all hosts to connect to the virtual server in HTTP.
3. Allow all hosts to connect to the virtual server in SSH.

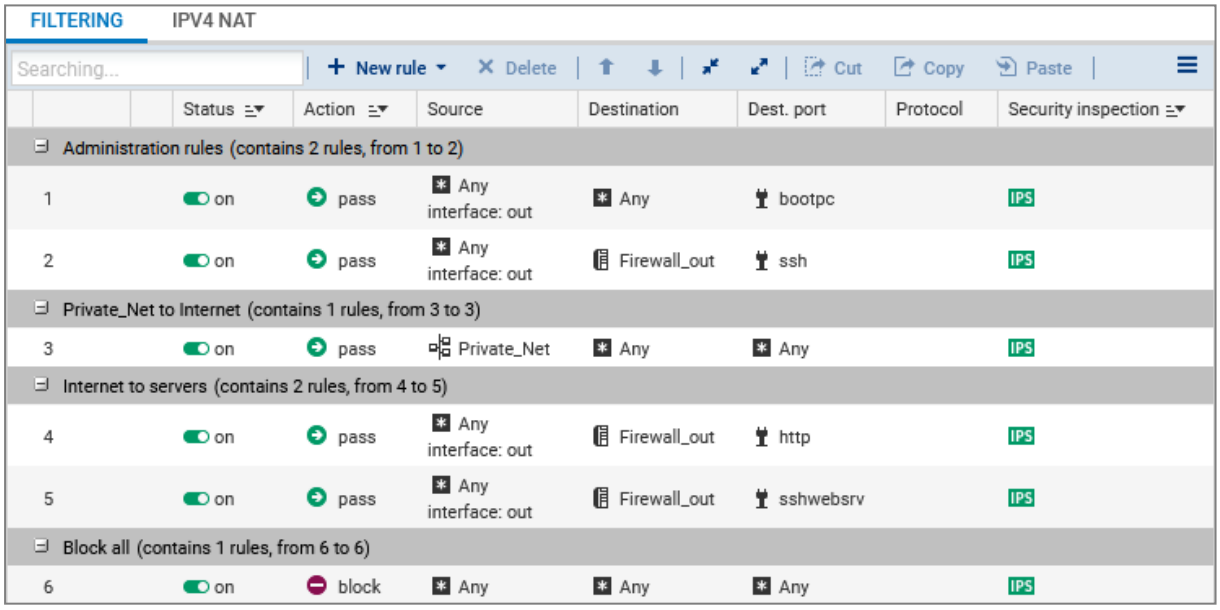
> **TIP**
> Add separators to your filter policy for better organization.

To add rules:

1. Click on **New rule** > **Single rule**.
2. Double-click on the number of the rule to edit it; a new window will open.
3. In the **General** tab, **Status** field, select **On**.
4. Configure the rule according to your requirements by browsing through the tabs on the left.
5. Click on **OK**.
   Position these rules above the block rule with the help of the **Up** and **Down** buttons.

In our example, we added the following rules:

Action	Source	Destination	Dest. port	Security inspection
pass	Private_Net	Any	Any	IPS
pass	Any, via the out interface	Firewall_out	http	IPS
pass	Any, via the out interface	Firewall_out	sshwebsrv	IPS



Configuring the NAT policy

The NAT policy can be configured in **Configuration** > **Security Policy** > **Filter - NAT, NAT** tab. We added three rules to meet the following requirements:

1. Redirect SSH traffic meant for the firewall's public interface to the web server.
2. Redirect HTTP traffic meant for the firewall's public interface to the web server.
3. Redirect traffic from hosts in the DMZ to hosts located beyond the firewall.

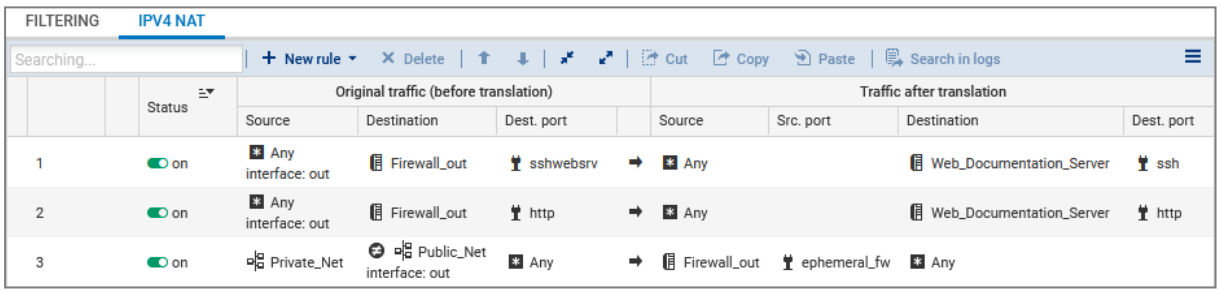
To add rules:

1. Click on **New rule** > **Single rule**.
2. Double-click on the number of the rule to edit it; a new window will open.
3. In the **General** tab, **Status** field, select **On**.

4. Configure the rule according to your requirements by browsing through the tabs on the left.
5. Click on **OK**.

In our example, we added the following rules:

Original traffic (before translation)			Traffic after translation			
Source	**Destination**	**Dest. port**	**Source**	**Src. port**	**Destination**	**Dest. port**
Any, via the out interface	Firewall_out	sshwebsrv	Any		Web_Documentation_Server	ssh
Any, via the out interface	Firewall_out	http	Any		Web_Documentation_Server	http
Private_Net	Different from Public_Net, via the out interface	Any	Firewall_out	ephemeral_fw	Any	



Testing the configuration and backing it up

Now that your firewall is configured, ensure that everything is running correctly. If so, we recommend backing up the configuration of your firewall so that you can restore it whenever necessary.

Testing the configuration

If certain components are inaccessible when the configuration is finalized, check whether the malfunction relates to the configuration of your firewall. To do so:

- Check the rules in your filter and NAT policy to identify errors, if any,
- You can position a *pass all* rule at the beginning of a filter policy to test whether a rule in particular is too restrictive. Be cautious, however, as this may compromise the security of your environment while you perform your tests.

In our example, we will conduct the following tests:

1. **Tests on outgoing traffic (from the DMZ to the Internet)**
   - Establish an HTTP connection from the web server (*Web_Documentation-Server* in the example) to an external web server,
   - Look up the logs for these connections in the firewall's administration interface in **Monitoring > Logs - Audit logs > Network traffic.**
2. **Tests on incoming traffic (from the Internet to the DMZ)**
   - Establish a web connection from a host located outside the Microsoft Azure infrastructure to the *index.htm* page of the virtual web server,
   - Look up the logs for established connections as well as NAT operations in the firewall's administration interface in **Monitoring > Logs - Audit logs > Network traffic.**

Backing up the configuration

Back up the firewall's configuration manually in **Configuration > System > Maintenance**, **Backup** tab. Enable automatic backups of its configuration in this module.

For more information, refer to the chapter on **Maintenance** in the SNS user manual.

Further reading

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

- Technical documentation on VPN topologies.
- SNS technical documentation website (version release notes, user guides, technical notes, etc.).
- Partner locator tool if you need assistance on more complex configurations.
- Stormshield knowledge base (authentication required).
- MyStormshield Online help.

STORMSHIELD

documentation@stormshield.eu