TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

DEPLOY SNS FOR CLOUD (2 NETWORK INTERFACES) ON MICROSOFT AZURE

Product concerned: SNS 1 and higher versions

Date: August 2018

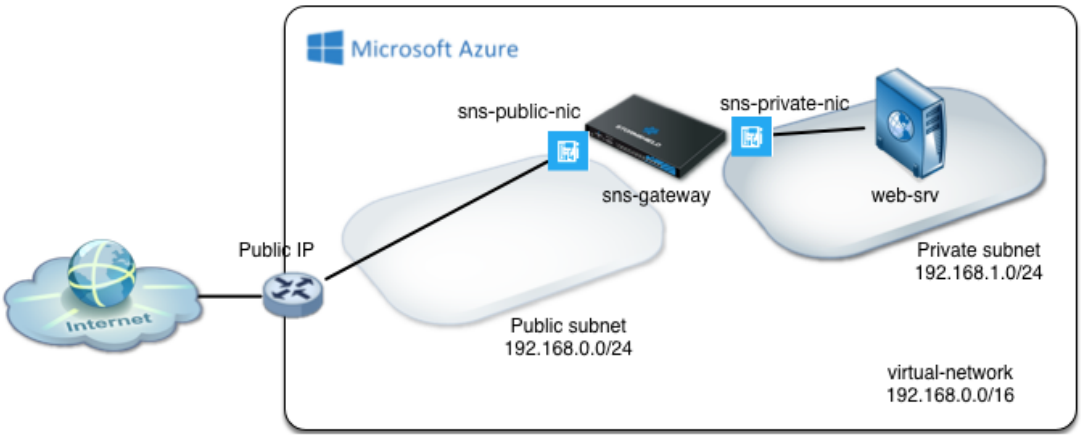
Reference: sns-en-sns_for_cloud_microsoft_azure_technical_note

Table of contents

Getting started

This technical note explains how to deploy a Standard_D2s_v3 Stormshield Network Security for Cloud firewall equipped with two network interfaces — a public (unprotected) interface and a private (protected) interface — on a Microsoft Azure hosting platform.

You will also find examples of filter and NAT rules to protect web servers hosted on the firewall's private network.



Obtaining the firewall license

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

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

Deploying the virtual firewall

Stormshield's Microsoft Azure Marketplace page does not allow step-by-step deployments of SNS firewalls that have more than one network interface.
The method presented is therefore based on the use of a customized template which you can find in Stormshield's *Github* area.

1. Go to Stormshield's Github page by clicking on the following link: https://github.com/stormshield/azure-templates/tree/master/sns/sns-2-nics,
2. Click on **Deploy to Azure**,
3. Log on using your Azure or Microsoft account.
   The pre-entered deployment form will then appear.
4. All the values suggested in this template's fields can be customized.

Basic information

- **Subscription**: select an Azure subscription associated with your account.
- Select or create a resource group (*SNS-Documentation* in the example).
- Select the geographic location in which your firewall is hosted.

Settings

- **SNS Admin password**: type the password assigned to the firewall's *admin* account.
- **Vnet Name**: enter the name of the virtual network that groups the firewall's public and private networks (*virtual-network* in the template).
- **Vnet Prefix**: indicate the network and network mask of this virtual network (*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**: enter the name of the sub-network in which the firewall's public interface is located (*Public* in the template).
- **Public Subnet Prefix**: indicate the network and network mask of this public sub-network (*192.168.0.0/24* in the template). This must be a sub-network of **Vnet Prefix**.
- **Private Subnet Name**: enter the name of the sub-network in which the firewall's private interface is located (*Private* in the template).
- **Private Subnet Prefix**: indicate the network and network mask of this private sub-network (*192.168.1.0/24* in the template). This must be a sub-network of **Vnet Prefix**.
- **SNS Name**: specify the name assigned to your virtual firewall (*sns-gateway* in the template).
- **SNS If Public Name**: indicate the name assigned to the firewall's public interface (*sns-gateway-public-nic* in the template).
- **SNS If Public IP**: indicate the IP address allocated to the firewall's public interface (*192.168.0.100* in the template). This address must belong to the network defined in the **Public Subnet Prefix** field.
- **SNS If Private Name**: indicate the name assigned to the firewall's private interface (*sns-gateway-private-nic* in the template).
- **SNS If Private IP**: indicate the IP address allocated to the firewall's private interface (*192.168.1.100* in the template). This address must belong to the network defined in the **Private Subnet Prefix** field.

- **VM Size**: select a virtual machine model that supports several network interfaces (*Standard_D2s_v3* in the template). Find out more about the characteristics of various virtual machine models on this page.
- **Public IP Name**: Enter a name that describes the public IP address that Microsoft Azure has allocated to the firewall (*sns-gateway-public-ip* in the template).
- **Route Table Name**: give a name to the firewall's private routing table (*route-table-private* in the template).

When all mandatory fields have been entered, read the Microsoft Azure Marketplace conditions carefully, select the "I agree to the terms and conditions stated above" checkbox and click on **Purchase**.

The deployment of the firewall will begin. A "Deployment successful" notification will appear when the firewall is created on the hosting platform.

Deploying a virtual web server

Deploying the server in a resource group

This chapter briefly describes the steps that would enable the deployment of a web server (based on a Linux Ubuntu Server distribution) on the network protected by the virtual firewall (*Private* in the example):

1. In the Microsoft Azure Marketplace, search for "Ubuntu Server *XX.XX* LTS" and select the desired distribution,
2. Select a deployment template and click on **Create**,
3. Assign a name to this machine (*Web-Documentation-Server* for example),
4. Create a user (*azureuser* for example) and his password,
5. Select the geographical location for hosting,
6. Select the resource group created during the deployment of the firewall (*SNS-Documentation* in the example),
7. In the options, select the virtual network associated with the resource group, then the private sub-network created earlier (*Private* in the example).
8. Confirm.

Configuring the firewall to allow traffic to and from the server

Retrieving the public IP address of the virtual firewall

On the portal's homepage:

1. Click on **Resource group**.
2. Select the virtual firewall's resource group (*SNS-Documentation* in the example).
3. Click on the **public IP address** entry (*sns-gateway-public-ip* in the example),

4. Take note of the public IP address that has been assigned.
5. Likewise, take note of the private IP address assigned to the *Web-Documentation-Server* server (192.168.1.4 in the example).

Configuring the firewall to allow traffic between the Internet and the web server

1. In a web browser, log on to the firewall's administration interface at https://*firewall_public_ip_address*/admin.
2. Authenticate with the *admin* account and password defined during the creation of the virtual firewall.
3. Remember to install your license as soon as possible in order to benefit from all the features you have subscribed with your Stormshield distributor.

Creating the necessary network objects

In the **Objects** > **Network objects** module, create:

- Two network objects. In the example: **Private_Net** (192.168.1.0/24) and **Public_Net** (192.168.0.0/24).
- A host object corresponding to the web server (in the example: **Web_Documentation_Server** - 192.168.1.4).
- A port object for the customized SSH port (in the example: **sshwebsrv** - 222/TCP).

Creating filter rules and updating the security policy

1. In the *Filtering* tab of the **Security policy** > **Filter - NAT** module, select the the filter policy created by default ((9) Azure default).
2. Create a rule that allows hosts hosted on the private network to access all hosts using the following values:

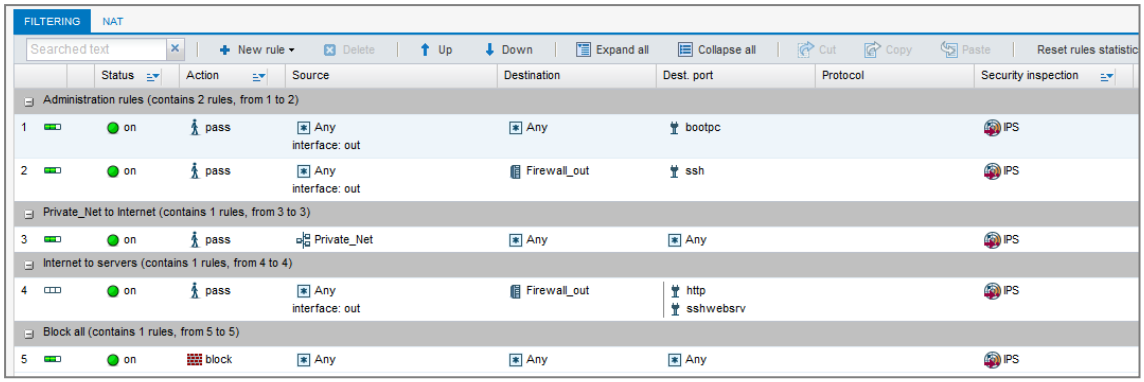
- **Action**: pass,
- **Source**: the **Private_Net** object,
- **Destination**: the **Any** object,
- **Destination port**: the **Any** object,
- **Security inspection**: IPS.

3. Create a rule that allows all machines to log on to your web server in HTTP and SSH:

- **Action**: pass,
- **Source**: the **Any** object via the **out** incoming interface,
- **Destination**: the **Firewall_out** object,
- **Destination port**: the **http** and **sshwebsrv** objects,
- **Security inspection**: IPS.

4. Using the **Up** and **Down** buttons, place these two rules above the block rule. You may also add rule separators to organize your filter policy.

The filter policy will then look like this:



Creating address translation (NAT) rules

1. In the NAT tab, create a rule that redirects SSH traffic meant for the firewall's public interface to the web server:

Original traffic (before translation)

- **Source**: the **Any** object via the **out** incoming interface,
- **Destination**: the **Firewall_out** object.
- **Destination port**: the **sshwebsrv** object,

Traffic after translation

- **Source**: the **Any** object,
- **Destination**: the **Web-Documentation-Server** object.
- **Destination port**: the **ssh** object,

2. Create a rule that redirects HTTP traffic meant for the firewall's public interface to the web server:

Original traffic (before translation)

- **Source**: the **Any** object via the out interface,
- **Destination**: the **Firewall_out** object.
- **Destination port**: the **http** object.

Traffic after translation

- **Source**: the **Any** object,
- **Destination**: the **Web-Documentation-Server** object.
- **Destination port**: the **http** object.

3. Cthe rule that redirects traffic from hosts in the DMZ to hosts located beyond the firewall:

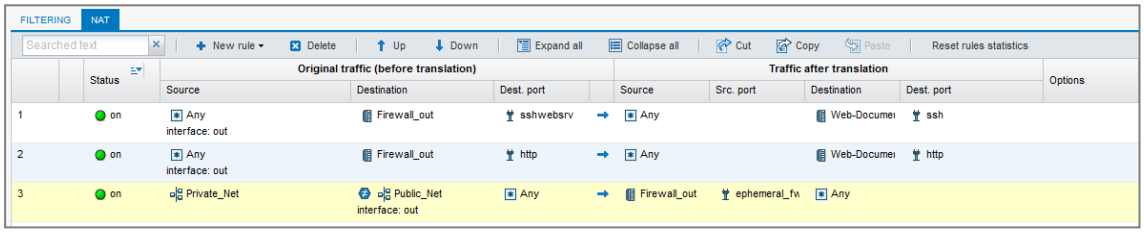
Original traffic (before translation):

- **Source**: the **Private_Net** object,
- **Destination**: anything that is not the ( ) **Public_Net** object and which leaves by the **out** interface,
- **Destination port**: the **Any** object.

Traffic after translation:

- **Source**: the **Firewall_out** object.
- **Source port**: the **ephemeral_fw** object.
- **Destination**: the **Any** object.

The address translation policy will then look like this:



4. Enable the modified security policy by clicking on **Save and enable**.

Installing the web service on the server

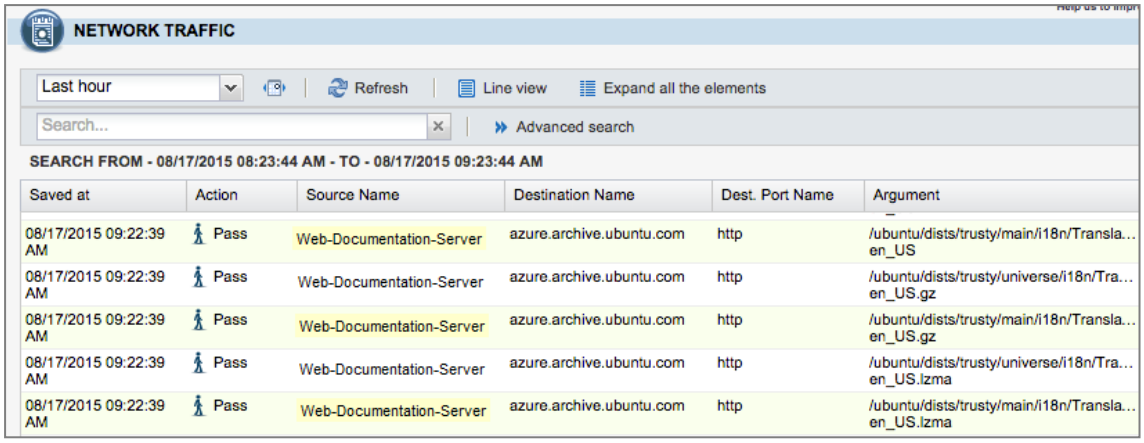
1. Log on to your server in SSH.
2. Install the Apache service and its dependencies.

Testing the configuration

Testing outgoing traffic (from the DMZ to the Internet)

From the web server (*Web_Documentation-Server* host in the example), establish an HTTP connection to an external web server.

As the firewall analyzes connections, logs corresponding to such connections may be looked up in the **Logs and activity reports** application (**Logs > Views > Network traffic** module):



Testing incoming traffic (from the Internet to the DMZ)

From a machine located outside the Microsoft Azure infrastructure, set up a web connection to the *index.htm* page of the virtual web server.

When the connection has been set up, matching logs as well as NAT operations may be looked up in the **Logs and activity reports** application (**Logs > Views > Network traffic** module).

STORMSHIELD

documentation@stormshield.eu