TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

VMWARE NSX: SNS FIREWALL AS AN EDGE ROUTER

Product concerned: SNS 1 and higher versions

Date: February 6, 2019

Reference: sns-en_VMWare-NSX-SNS-Edge-Router_technical-note

Table of contents

Getting started

VMware NSX Data Center is a network virtualization platform for Software-Defined Data Centers (SDDCs), which provides all network and security features in the form of a program, and is isolated from the physical underlying infrastructure.

NSX Data Center therefore allows a virtual cloud network to be set up by guaranteeing end-to-end connectivity with applications and data, no matter where they are located.

Integrating an SNS firewall into an NSX architecture can therefore provide advanced filtering and security features to protect such data and applications.

The various components of a vSphere environment are as follows:

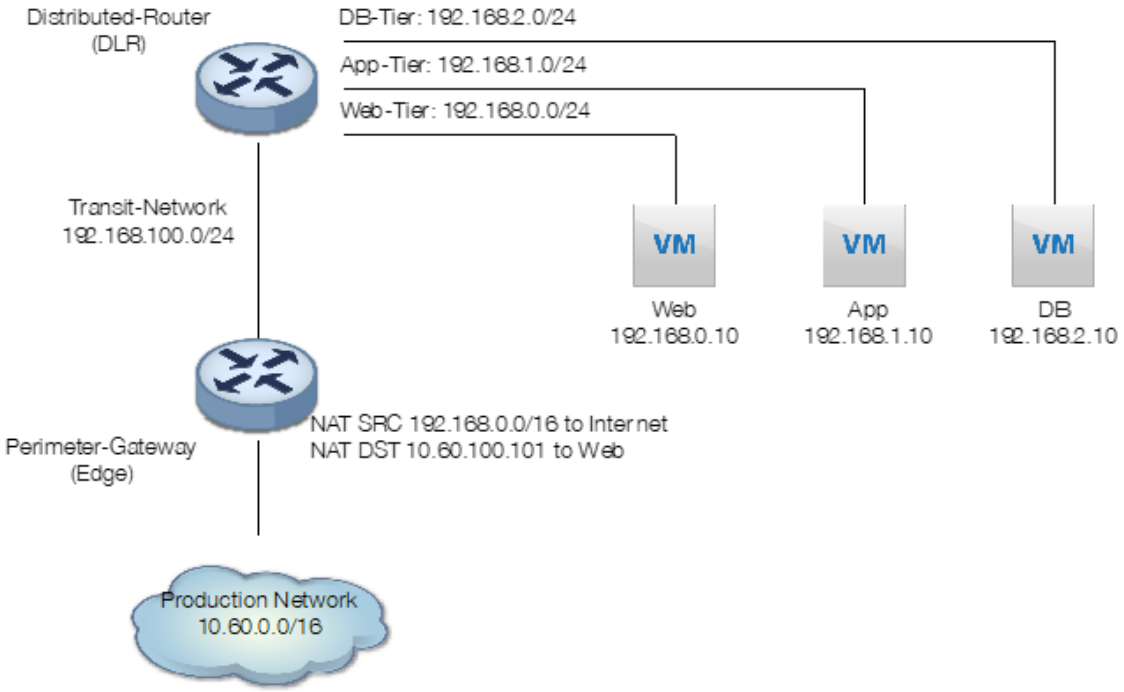
- ESXi: hypervisor on a hardware platform (bare metal),
- vCenter: centralized virtual machine manager,
- vSphere: vCenter - ESXi hypervisor connection,
- vSphere Enterprise: version of vSphere that includes Distributed Virtual Switches (DVS) and the Distributed Resource Scheduler (DRS).

Do note that this document does not cover the installation of a firewall from an OVA file that can be obtained from your client area. The installation procedure is available in the document *Stormshield Network Virtual Firewalls - Installation guide*.

Topology

The web application in this example relies on three virtual servers:

- A web server,
- An application server, and
- A database server.



Each server is connected to its own virtual network.

The Distributed Logical Router (Distributed-Router) interconnects these three virtual networks, while the perimeter router (Perimeter-Gateway) connects the physical network to these three virtual networks through a virtual transit network (Transit-Network).

The perimeter router also performs address translation:

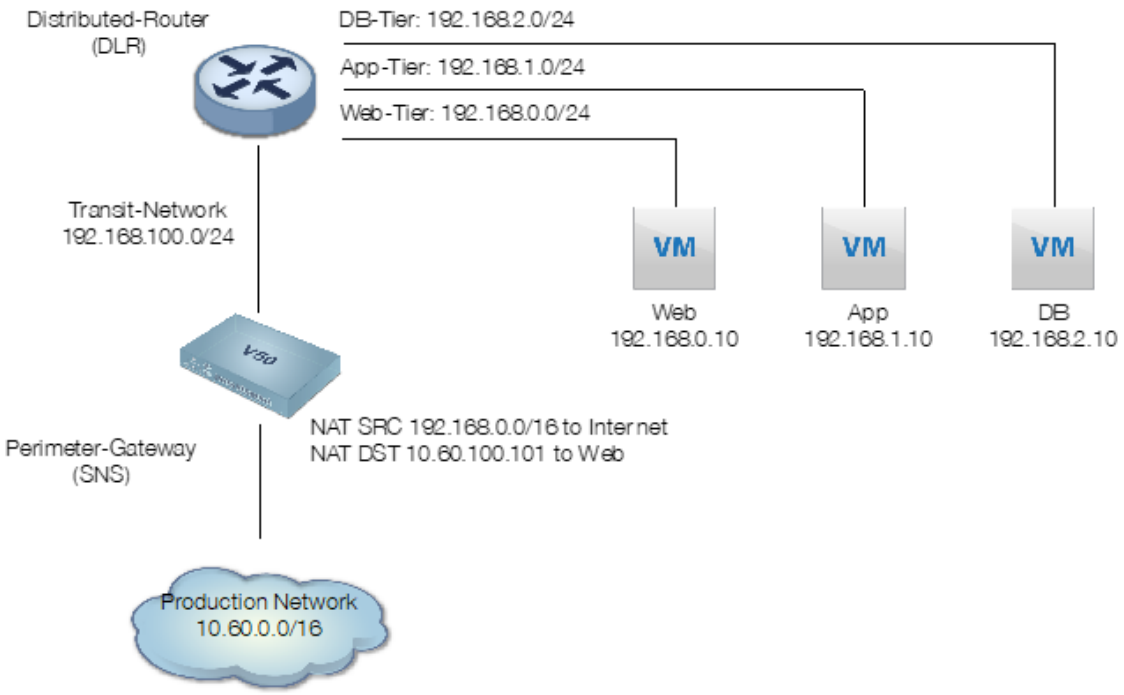
- Source NAT to allow servers to communicate with the Internet,
- Destination NAT to redirect requests from a public address to the web server.

In this architecture, the rules of the distributed firewall integrated into NSX (perimeter router) resemble the following:

No.	Name	Rule ID	Source	Destination	Service	Action	Applied To
	Web Application (Rule 1 - 2)						
1	web src NAT ip	1006	any	Web NAT	HTTP HTTPS	Allow	Distributed Firewall
2	Web Tier to App & DB Tier	1005	Web-Tier	App-Tier DB-Tier	any	Allow	Distributed Firewall

Integrating an SNS firewall as a peripheral router

The SNS firewall can be used to an advantage as a peripheral router offering advanced filtering features:



Setting up this architecture requires a virtual SNS firewall deployed on the platform with two interfaces taken out of the bridge created by default:

- A protected interface with an address in the **Transit-Network** network (*in* interface renamed **transit** and bearing the address 192.168.100.1 in this document),
- An unprotected interface with an address in the network named **Production Network** (*out* interface bearing the address 10.60.100.100 in this document),

The following firewall configuration operations will be explained in this technical note:

- Creating the network objects needed on the firewall,
- Defining static routes on the firewall,
- Configuring filter rules on the firewall,
- Configuring NAT rules on the firewall,

Creating network objects

You need to create the following objects:

Object name	IPv4 address in this example	Role
Transit-Router	192.168.100.2	Distributed router (DLR)
Web-NAT	10.60.100.101	IP address of the web server as seen from external networks
Web-Srv	192.168.0.10	Real IP address of the web server
Web-Tier	192.168.0.0/24	Network dedicated to web servers

Object name	IPv4 address in this example	Role
App-Tier	192.168.1.0/24	Network dedicated to application servers
DB-Tier	192.168.2.0/24	Network dedicated to database servers

Transit-Router, Web-NAT and **Web-Srv** objects

1. Log on to the firewall's web administration interface as an administrator.
2. In the **Objects** > **Network objects** menu, click on **Add**.
3. In the column on the left, select **Host** and fill in the mandatory fields for the **Transit-Router** object by following the example in the table above:
   - **Object name**,
   - **IPv4 address**.
4. Click on **Create and duplicate**.
5. Repeat steps 3 and 4 for the **Web-NAT** object.
6. Repeat step 3 for the **Web-Srv** object.
7. Click on **Create**.

Objects **Web-Tier**, **App-Tier** and **DB-Tier**

1. In the **Objects** > **Network objects** menu, click on **Add**.
2. In the column on the left, select **Network** and fill in the mandatory fields for the **Web-Tier** object by following the example in the table above:
   - **Object name**,
   - **IPv4 address**.
3. Click on **Create and duplicate**.
4. Repeat steps 3 and 4 for the **App-Tier** object.
5. Repeat step 3 for the **DB-Tier** object.
6. Click on **Create**.

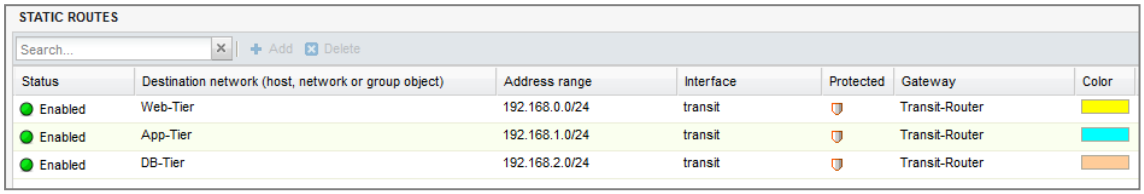
Defining static routes on the firewall

In the **Network** > **Routing** menu > **Static routes** tab:

1. Click **Add**.
2. In the **Destination network (host network or group object, network or group object)** column in the new line.
3. Select the **Web-Tier** object.
4. Click in the **Interface** column.
5. Select the **transit** interface.
6. Click in the **Gateway** column.
7. Select the **Transit-Router** object.
8. Double-click on the **Status** column to enable the route.
9. Repeat steps 1 to 8 to create the route to the **App-Tier** network.

10. Repeat steps 1 to 8 to create the route to the **DB-Tier** network.
11. Click on **Apply** to validate the configuration.

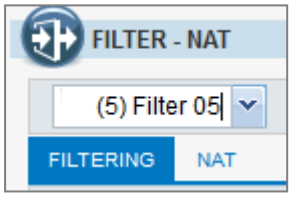
The firewall's static routes will then resemble the following:



Configuring filter rules on the firewall

To define the various filter rules needed:

1. Go to the menu **Security policy** > **Filter - NAT** > **Filtering** tab.
2. Select the desired security policy using the drop-down list:



Allowing virtual networks to access the Internet

1. Click on **New rule**.
2. Select **Single rule**.
3. Double-click on the newly added rule.
4. In the **General** menu, set the **Status** to *On*.
5. In the **Action** menu > **General** tab, set the **Action** to *pass*.
   You can also select the value *Log (filter log)* for the **Log level** field.
6. In the **Source** menu > **General** tab, click on **Add** and select the network object *App-Tier*.
7. Repeat the operation to add the objects **Web-Tier** and **DB-Tier**.
8. For the **Incoming interface** field, select the transit interface.
9. In the **Destination** menu > **Advanced properties** tab, select the *out* interface as the **Outgoing interface**.
10. Validate the rule by clicking on **OK**.

Allowing external networks to access the web server

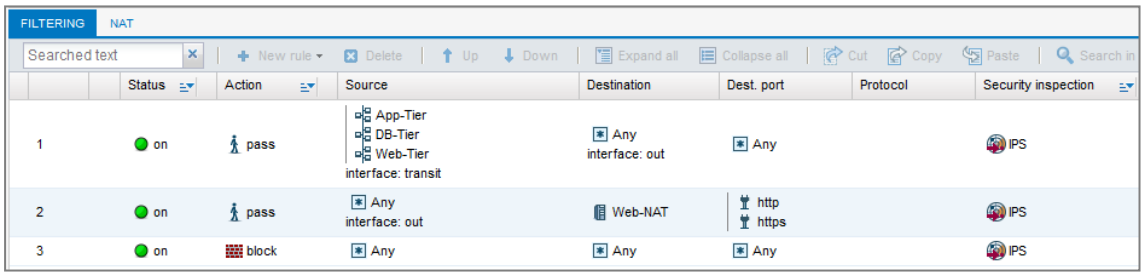
1. Click on **New rule**.
2. Select **Single rule**.
3. Double-click on the newly added rule.
4. In the **General** menu, set the **Status** to *On*.
5. In the **Action** menu > **General** tab, set the **Action** to *pass*.
   You can also select the value *Log (filter log)* for the **Log level** field.

6. In the **Source** menu > **General** tab, select the *out* interface as the **Incoming interface**.
7. In the **Destination** menu > **General** tab, click on **Add** and select the network object *Web-NAT*.
8. In the **Port / Protocol** menu > under **Port**, click on **Add** and select the *http* object.
9. Repeat the operation to add the *https* object.
10. Validate the rule by clicking on **OK**.

Prohibiting all other traffic

1. Click on **New rule**.
2. Select **Single rule**.
3. Double-click on the newly added rule.
4. In the **General** menu, set the **Status** to *On*.
5. Validate the rule by clicking on **OK**.
   The newly added rule will therefore block all other traffic.
   Ensure that this rule is the last in your filter policy (where necessary, you can select it and move it using the **Up** and **Down** buttons.

The filter policy on the peripheral firewall will then look like this:



Configuring NAT rules on the firewall

To define the various NAT rules:

1. Go to the menu **Security policy** > **Filter - NAT**.
2. Select the security policy that contains the filter rules added earlier.
3. Click on the **NAT** tab.

Hiding virtual networks when they access the Internet

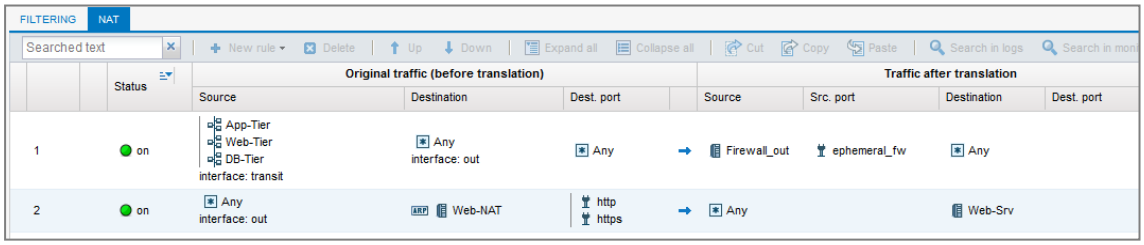
1. Click on **New rule**.
2. Select **Source address sharing rule (masquerading)**.
3. Double-click on the newly added rule.
4. In the **General** menu, set the **Status** to *On*.
5. In the **Original source** menu > **General** tab, click on **Add** and select the network object **App-Tier**.
6. Repeat the operation to add the objects **Web-Tier** and **DB-Tier**.
7. For the **Incoming interface** field, select the **transit** interface.

8. In the **Original destination** menu > **Advanced properties** tab, select the **out** interface as the **Outgoing interface**.
9. In the **Translated source** menu > **General** tab, select the **Firewall_out** network object for the **Translated source host** field.
10. Validate the rule by clicking on **OK**.

Redirecting external HTTP/HTTPS requests to the web server

1. Click on **New rule**.
2. Select **Single rule**.
3. Double-click on the newly added rule.
4. In the **General** menu, set the **Status** to *On*.
5. In the **Original source** menu > **General** tab > **Incoming interface** field, select the **out** interface.
6. In the **Original destination** menu > **General** tab > under **Destination hosts**, click on **Add** and select the network object **Web-NAT**.
7. In the **Destination port** section, click on **Add** and select the **http** object.
8. Repeat the operation to add the **https** object.
9. In the **Advanced properties** tab, select the **ARP publication** checkbox.
10. In the **Translated destination** menu > **General** tab > **Translated destination host** field, click on **Add** and select the object **Web-Srv**.
11. Validate the rule by clicking on **OK**.

The NAT policy on the peripheral firewall will then look like this:



Enable the filter and NAT policy by clicking on **Save and enable**.

Testing the configuration

Using a host located on the production network, set up a web connection to the application's homepage.

Once the connection has been established, the corresponding logs and NAT operations can be seen in the firewall's web administration interface (**Logs - Audit logs** > **Views** > **Network traffic** module and **Logs - Audit logs** > **Logs - Logs** > **Network connections** module).

STORMSHIELD

documentation@stormshield.eu