FortiGate-VM - VMware-NSX Security Fabric integration

Version 6.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 20, 2018
FortiGate-VM 6.0 VMware-NSX Security Fabric integration
01-601-000000-20180820

TABLE OF CONTENTS

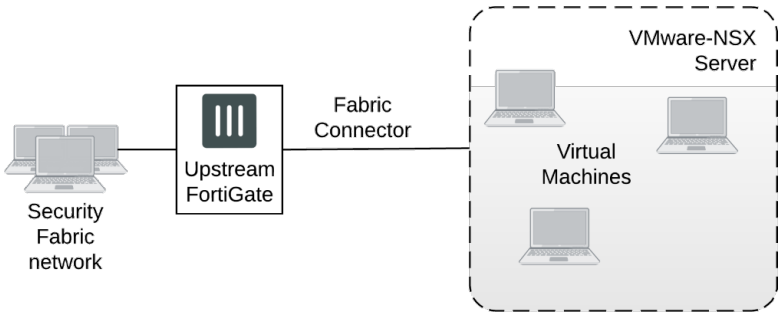
Change Log

Date	Change Description
2018-08-20	Initial release.

VMware-NSX Security Fabric integration

This example configuration describes setting up secure dynamic communication between the upstream FortiGate in a Security Fabric-protected network and virtual machines on a VMware-NSX server. This fabric connector configuration allows traffic between virtual machines on the VMware-NSX server and the Security Fabric even if network addressing dynamically changes on the VMware-NSX server. The process requires four configuration steps:

1. On your VMware-NSX server, create a security group to contain the addresses of virtual machines on the NSX server to be accessed from the Security Fabric.
2. On the upstream FortiGate, create a VMware-NSX fabric connector that supports dynamic communication with the VMware-NSX server. You can only create one VMware-NSX fabric connector.
3. On the upstream FortiGate, create a dynamic firewall address and import addresses from the VMware-NSX security group into it using the `execute nsx group import root <security-group-name>` command. After the initial import, the fabric connector keeps the dynamic firewall address in sync with the security group.
4. On the upstream FortiGate, create a firewall policy that allows traffic between the upstream FortiGate and the VMware-NSX server. In this example, the firewall policy allows Security Fabric users to connect to virtual machines on the VMware-NSX server.



Creating a VMware-NSX security group

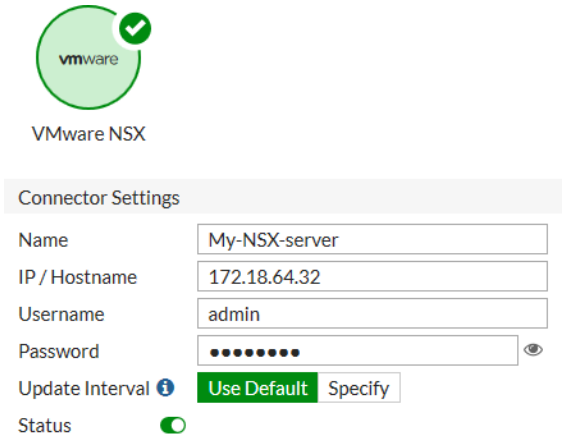
A security group is a collection of assets or objects from your vSphere inventory. For VMware-NSX security fabric integration, you can create a security group containing addresses of virtual machines in the VMware-NSX server that you want Security Fabric users to have access to.

You create a security group at the NSX manager level using the vSphere web client. See VMware-NSX Create a Security Group for the complete procedure. Make sure to record the name of the security group, as you will need it to set up the dynamic firewall address later in this procedure.

Creating the VMware-NSX fabric connector

Use the following steps to create a VMware-NSX connector that allows dynamic communication between the VMware-NSX server and your Security Fabric.

1. Go to *Security Fabric* > *Fabric Connectors* and select *Create New*.
2. Under *SDN*, select *VMware NSX*.
3. Set a *Name* for the Fabric Connector.
4. Set *IP/Hostname*, *Username*, and *Password* to the settings for your VMware-NSX server.
   IP/Hostname is the IP address or host name used to connect to the VMware-NSX server, and *Username* and *Password* are the username and password of an account that has administrative access to the VMware-NSX server. The username and password should also have access to the security group that you have added to the VMware-NSX server.



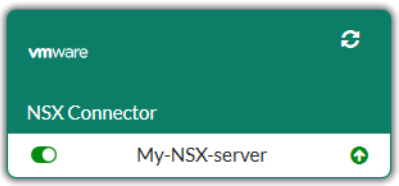
5. Select *OK*.

You can also add the connector from the CLI:

```
config system sdn-connector
   edit My-NSX
      set type nsx
      set server 172.18.64.32
      set username admin
      set password <password>
   next
end
```

Viewing the VMware-NSX connector status

Go to *Security Fabric* > *Fabric Connectors* to view the status of the VMware-NSX connector (whether its enabled or disabled and whether it is connected to the VMware-NSX server). You can also refresh the status and enable or disable the connector.



Importing addresses from the VMware-NSX security group

Log in to the upstream FortiGate CLI, and enter the following command to create a dynamic firewall address and import addresses from the VMware-NSX security group into it:

```
execute nsx group import root <security-group-name>
```

The command creates a dynamic firewall address with the same name as the VMware-NSX security group and imports the addresses from the security group into the firewall address. After you complete this step, the VMware-NSX fabric connector keeps the dynamic firewall address up to date when the security group changes on the VMware-NSX server.

Viewing the status of the dynamic firewall address

On the upstream FortiGate, to view the status of the dynamic firewall address, including the IP addresses that have been added to the address from the VMware-NSX security group, go to *Policy & Objects* > *Addresses* and hover over the firewall address to see its status information, including the IP addresses that it resolves.

You can also use the following command:

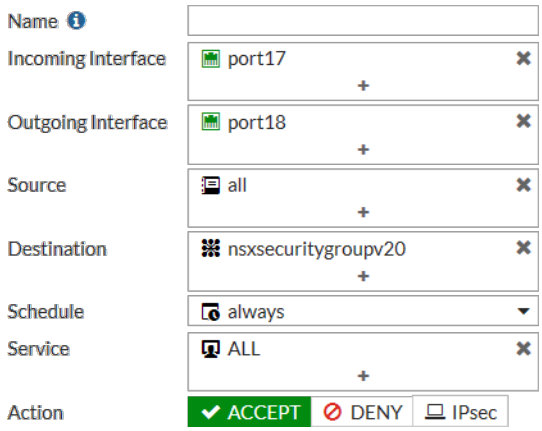
```
show firewall address "<security-group-name>"
    config firewall address
        edit "&lt;security-group-name&gt;"
            set uuid c5fea93c-764a-51e8-3e58-734564e8bc26
            set type dynamic
            set obj-id "15"
            config list
                edit "10.1.100.136"
                next
                edit "10.1.100.15"
                next
                edit "10.1.100.16"
                next
                edit "10.1.100.200"
                next
            end
            set sdn nsx
        next
    end
```

Crate a firewall policy to allow access to the VMware-NSX server

On the upstream FortiGate, use the following steps to add a firewall policy that allows users on the Security Fabric to access virtual machines on the VMware-NSX server.

1. Go to *Policy & Objects* > *IPv4 Policy* and select *Create New*.
2. Set a *Name* for the policy.
3. Set the appropriate *Incoming Interface* and *Outgoing Interface*.

4. Set the *Source* address to *all* and the *Destination* address to <security-group-name>. (In the example below, the security group name is nsxsecuritygroup20.)
5. Set other policy settings, as required.



6. Select *OK*.

You can also add the firewall address from the CLI:

```
config firewall policy
   edit 0
      set name <name>
         set srcintf port17
      set dstintf port18
      set srcaddr all
      set dstaddr nsxsecuritygroupv20
      set action accept
      set schedule
      set service
   next
end
```

Testing the configuration

With this configuration in place, users on the network connected to the port17 interface of the upstream FortiGate should be able to connect to virtual machines on the VMware-NSX server. You can verify this by attempting to ping any of the addresses dynamically added to the firewall address from a PC on the protected network.