In increasingly dynamic network environments, security solutions must be ever more tightly coordinated with networking and other IT infrastructure to provide agility in the face of fast-paced and rapidly changing operations. Fortinet Fabric Connectors feature APIs and other interfaces to make them highly extensible platforms. They provide out-of-the-box or built-in integration mechanisms and orchestration of FortiGate or FortiManager with key SDN and public cloud solutions — including with leading vendors such as Cisco, VMware, Nuage Networks, AWS, and Azure.

**Ease of Deployment**

Depending on the vendor platform, Fortinet Fabric Connectors can often be installed and configured within a matter of minutes to provide turnkey connectivity between FortiGate security and existing vendor infrastructure.

**Low TCO**

Fortinet Fabric Connectors are free of charge and supported by both physical and virtual form factors of FortiGate and FortiManager. FortiGate, FortiManager, and the third-party SDN and cloud platform have to be properly licensed according to licensing agreements of each solution in order for all components to function.

**Today’s Challenges**

- Conventional network infrastructure lacks flexibility due to physical entities ranging from wires, servers, to rack spaces. This type of network cannot easily respond to evolving security threats.
- Multi-clouds are still co-existent isolated sets of private clouds, public clouds, and physical entities requiring different security management methodologies which have become burdens to administrators.
- Dramatically increasing number of instantiated entities with elastic workloads raises risks of unattended vulnerabilities.
- Inconsistent security management with assortment of security solutions at different sites and tenants.
Features

How do they work?
Fortinet Fabric Connectors for SDN (private clouds) and Cloud (public clouds), formerly known as Fortinet SDN Connector, enable either FortiGate as a standalone system, or FortiManager, which manages multiple FortiGates, to integrate with the third-party SDN or cloud platforms to synchronize dynamic address group objects that are protected by FortiGate firewall policy. No matter how objects change their forms and locations in elastic and volatile fashions, FortiGate will be able to identify them as Address objects (can be used as sources and destinations) and apply appropriate firewall policies automatically without administrator's manual intervention. Fortinet Fabric Connector is deployed to integrate between FortiGate or FortiManager and third-party technology solutions. FortiManager is optional.

Summary of Initial Setup
Although there are slight differences in how you make an initial setup depending on platforms you use, the following are the general steps:

1. You have third-party SDN platforms or public cloud environments where virtual instances need to be protected by FortiGate.
2. Deploy FortiGate, or the combination of FortiGate and FortiManager, depending on the size of coverage in the network. If you have multiple sets of FortiGate, deploying FortiManager will ease management.
3. Ensure that any preliminary configuration required on the third-party SDN/cloud platform side is configured properly.
4. For out-of-the-box integration (such as with Cisco ACI and Nuage VSP), deploy a dedicated Fortinet Fabric Connector VM instance. For other integrations, there is no need to have one because Fabric Connector service runs within FortiGate/FortiManager as a built-in feature.

1. Security Groups and/or relevant dynamic objects will be imported to Fabric Connector objects.
2. Objects will be converted to the format that FortiManager uses (if FortiManager is not deployed, FortiGate will do the same).
3. FortiManager will propagate the definition of dynamic objects to all FortiGate instances under its management.
4. FortiGate will automatically update Firewall Address objects containing IP addresses in order to identify them properly while maintaining connectivity.
Features

5. Log in to the Fabric Connector VM and FortiGate/FortiManager, open the GUI console, and configure Fabric Connector to import dynamic address group objects from the SDN (or third-party) platform. Make sure that Fortinet components can properly access the SDN platform. You will need to check the following:
   a) Where authentication is required, make sure you have allowed Fortinet components to pass it.
   b) Where network access is required, make sure you have opened relevant ports between the SDN platform and Fortinet components.

6. Create appropriate filter conditions to create specific groups of Address objects if required.

7. Once the Fabric Connector VM/FortiGate/FortiManager acquires connectivity to the SDN platform, it will automatically import dynamic address group objects based on matching filters and then store them as Firewall Address objects. If the content of the dynamic objects changes, it is automatically updated through the Fabric Connector. No manual action is required.

Connector configuration on Fortinet Fabric Connector VM with Cisco ACI or Nuage Network VSP

Connector configuration on FortiManager

Firewall Address objects are synchronized automatically

Create a Firewall Policy using the Address as a destination
## Integration Matrix

<table>
<thead>
<tr>
<th>THIRD-PARTY PRODUCT</th>
<th>VERSION</th>
<th>INTEGRATING CONNECTOR TYPE</th>
<th>DEPLOYMENT PREREQUISITES</th>
<th>SUPPORTED VERSION OF FORTIGATE®</th>
<th>SUPPORTED VERSION OF FORTIMANAGER®</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nuage Networks VSP</td>
<td>4.0.8</td>
<td>Out-of-the-box integration</td>
<td>A dedicated VM (VMware ESXi, KVM, and Hyper-V) to install Fortinet Fabric Connector v1.1.1 for Cisco ACI and Nuage Networks&lt;sup&gt;33&lt;/sup&gt;</td>
<td>5.6.3+ / 6.0.0+ / 6.2.0+</td>
<td>5.6.3+ / 6.0.0+ / 6.2.0+</td>
</tr>
<tr>
<td>Cisco ACI&lt;sup&gt;33&lt;/sup&gt;</td>
<td>2.3 (11)</td>
<td>Out-of-the-box integration</td>
<td>FortiGate or FortiManager built-in feature</td>
<td>5.6.2+ / 6.0.0+ / 6.2.0+</td>
<td>5.6.2+ / 6.0.0+ / 6.2.0+</td>
</tr>
<tr>
<td>VMware NSX-V&lt;sup&gt;34, 35&lt;/sup&gt;</td>
<td>NSX-V 6.2.4+ / 6.3.0+ / 6.4.0+&lt;sup&gt;4&lt;/sup&gt;</td>
<td>FortiGate or FortiManager built-in feature</td>
<td>Use case 1: FortiGate VMX Service Manager&lt;sup&gt;2&lt;/sup&gt; and VMX security node instances Use case 2: FortiGate-VMX or FortiManager, and connectivity to VMware NSX Manager</td>
<td>FortiGate-VMX built-in feature and connectivity to VMware NSX Manager</td>
<td>6.2.1 special build</td>
</tr>
<tr>
<td>VMware NSX-1&lt;sup&gt;34&lt;/sup&gt;</td>
<td>NSX-1 2.4.1+ / 2.5.0+</td>
<td>FortiManager built-in feature</td>
<td>Connectivity to VMware NSX Manager</td>
<td>6.2.0+</td>
<td>Future support</td>
</tr>
<tr>
<td>VMware ESK and vCenter</td>
<td>VMware ESK and vCenter vSphere 6.5+ or vCenter 6.7+</td>
<td>FortiGate built-in feature</td>
<td>Connectivity to vSphere or vCenter environment</td>
<td>6.2.0+</td>
<td>Future support</td>
</tr>
<tr>
<td>AWS&lt;sup&gt;37&lt;/sup&gt;</td>
<td>N/A</td>
<td>FortiGate or FortiManager built-in feature</td>
<td>Connectivity to AWS IPC environment</td>
<td>5.6.3+ / 6.0.0+ / 6.2.0+</td>
<td>5.6.3+ / 6.0.0+ / 6.2.0+</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>N/A</td>
<td>FortiGate built-in feature</td>
<td>Connectivity to Azure IaaS environment</td>
<td>5.6.4+ / 6.0.0+ / 6.2.0+</td>
<td>5.6.4+ / 6.0.0+ / 6.2.0+</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>N/A</td>
<td>FortiGate built-in feature</td>
<td>Connectivity to GCP environment</td>
<td>6.0.1+ / 6.2.0+</td>
<td>6.2.0+</td>
</tr>
<tr>
<td>Alibaba Cloud</td>
<td>N/A</td>
<td>FortiGate built-in feature</td>
<td>Connectivity to USC GKE</td>
<td>6.2.0+</td>
<td>Future support</td>
</tr>
<tr>
<td>Kubernetes</td>
<td>N/A</td>
<td>FortiGate built-in feature</td>
<td>Connectivity to a customer premise-located Kubernetes controller</td>
<td>6.2.0+</td>
<td>Future support</td>
</tr>
<tr>
<td>OpenStack Horizon</td>
<td>N/A</td>
<td>FortiGate built-in feature</td>
<td>Connectivity to OpenStack Horizon environment</td>
<td>6.2.0+</td>
<td>Future support</td>
</tr>
<tr>
<td>Fortinet Connectors</td>
<td>N/A</td>
<td>FortiGate built-in feature</td>
<td>Connectivity to FortiGate-VMX Service Manager&lt;sup&gt;2&lt;/sup&gt; and VMX security node instances</td>
<td>6.2.0+</td>
<td>Future support</td>
</tr>
<tr>
<td>Fortinet Connectors</td>
<td>N/A</td>
<td>FortiGate built-in feature</td>
<td>Connectivity to FortiGate-VMX Service Manager&lt;sup&gt;2&lt;/sup&gt; and VMX security node instances</td>
<td>6.2.0+</td>
<td>Future support</td>
</tr>
</tbody>
</table>

<sup>1</sup> For Cisco ACI Device Package, there is another solution called "FortiGate Connector for Cisco ACI Device Package" available for the download. For more details refer to the download.

<sup>2</sup> FortiGate-VMX is the component of FortiGate VMX, which specifically supports VMware NSX. Service Manager communicates with NSX Manager (and FortiManager if it co-exists) by integrating all managed FortiGate VMX nodes.

<sup>3</sup> Service Manager is the component of FortiGate VMX, which specifically supports VMware NSX. Service Manager communicates with NSX Manager (and FortiManager if it co-exists) by integrating all managed FortiGate VMX nodes.

<sup>4</sup> There is a compatibility between FortiGate and FortiManager versions. Ensure to use compatible versions for both products. https://docs.fortinet.com/d/fortimanager-compatibility

<sup>5</sup> Supported minor versions of NSX V.1.1+ depend on a VMware's carrying-forward policy for version compatibility. It may not mean all subsequent versions.

<sup>6</sup> There is a compatibility between FortiGate and FortiManager versions. Ensure to use compatible versions for both products. https://docs.fortinet.com/d/fortimanager-compatibility

<sup>7</sup> FortiGate-VMX's certified versions with VMware NSX supports NSX-V 6.3.3 and above<sup>4</sup>.

<sup>8</sup> FortiGate built-in feature Connectivity to VMware NSX Manager supported by FortiManager.

<sup>9</sup> FortiGate built-in feature Connectivity to VMware NSX Manager supported by FortiManager.

<sup>10</sup> FortiGate built-in feature Connectivity to VMware NSX Manager supported by FortiManager.

<sup>11</sup> FortiGate built-in feature Connectivity to VMware NSX Manager supported by FortiManager.

<sup>12</sup> FortiGate built-in feature Connectivity to VMware NSX Manager supported by FortiManager.

<sup>13</sup> FortiGate built-in feature Connectivity to VMware NSX Manager supported by FortiManager.

<sup>14</sup> For Cisco ACI Device Package, there is another solution called "FortiGate Connector for Cisco ACI Device Package" available for the download. For more details refer to the download.

<sup>15</sup> Service Manager is the component of FortiGate VMX, which specifically supports VMware NSX. Service Manager communicates with NSX Manager (and FortiManager if it co-exists) by integrating all managed FortiGate VMX nodes.

<sup>16</sup> FortiGate-VMX is not a certified product with VMware NSX (NetX integration). However, since FortiOS is used in common, the same NSX versions are supported on the connector feature.

<sup>17</sup> There is a compatibility between FortiGate and FortiManager versions. Ensure to use compatible versions for both products. https://docs.fortinet.com/d/fortimanager-compatibility

<sup>18</sup> Supported minor versions of NSX V.1.1+ depend on a VMware's carrying-forward policy for version compatibility. It may not mean all subsequent versions.

<sup>19</sup> FortiGate 6.2.0+ supports multiple Fabric connector configurations for the same type.

<sup>20</sup> FortiManager supports a single Fabric connector configuration for the same type.

<sup>21</sup> FortiManager 6.0.5+ and 6.2.0+ adds support of NSX-V 6.4.4.

<sup>22</sup> The connector package is downloadable from here. Go to Use case 1: Select FortiSDNConnector in Product, click Download lab, choose v1.0+ or v1.1+. Obtain the appropriate file depending on your hypervisor platform: .vhd: Microsoft Hyper-V / zip (OVF): VMware ESXi / img: KVM

<sup>23</sup> OpenStack Horizon 5.6.2+ / 6.0.0+ / 6.2.0+ supports NSX-V 6.3.3 and above<sup>4</sup>.

<sup>24</sup> Use case 2: FortiManage-VMX or FortiManager, and connectivity to VMware NSX Manager

<sup>25</sup> FortiGate 6.2.1+ adds support of OpenStack Queens and Stein.

## Order Information

How to obtain Fortinet Fabric Connectors package:

Fortinet Connectors are free of charge. For out-of-the-box integrations, log in to [https://support.fortinet.com](https://support.fortinet.com) and download the package or contact Fortinet technical support.