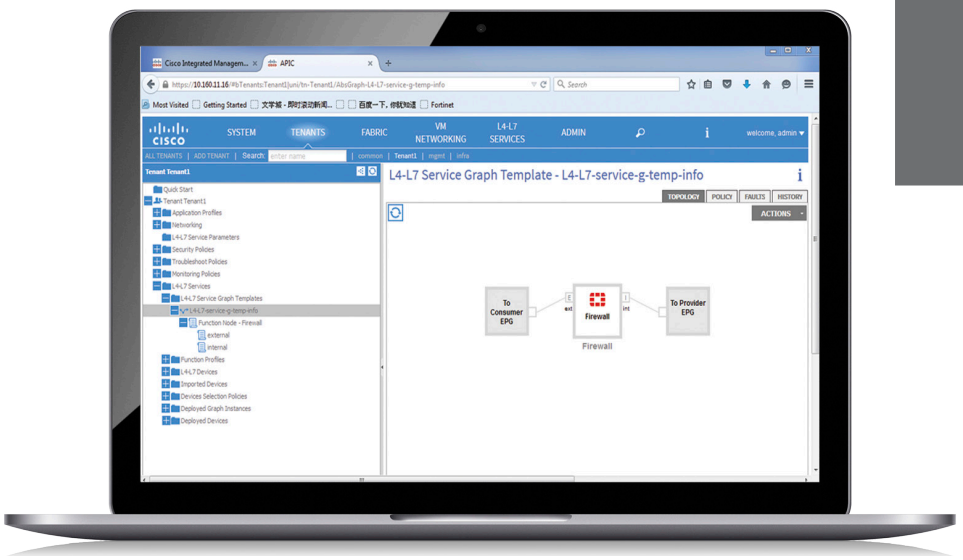
Fortinet Fabric Connectors for SDN and Cloud



Today's Challenges

Conventional network infrastructure lacks flexibility due to physical entities ranging from wires and 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.

Automated Object Synchronization in SDDC and Hybrid Cloud Environments

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, Azure, Oracle Cloud, and others.

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.

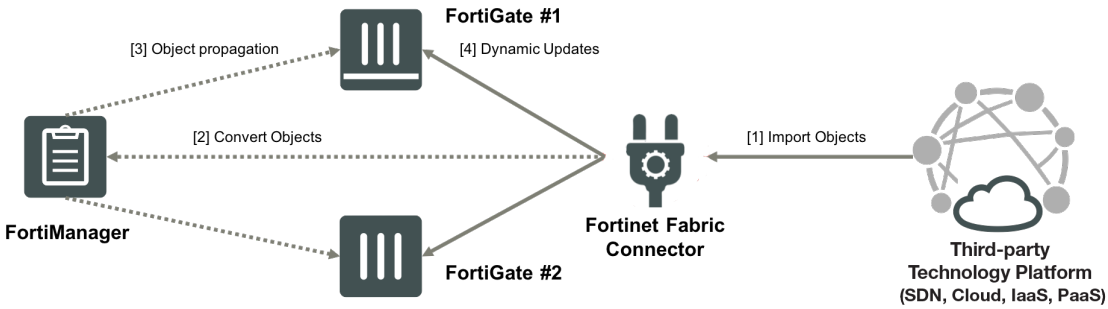
Low TCO

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 must be properly licensed according to each solution's licensing agreements for all components to function.

Feature Highlights

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 the FortiGate firewall policy protects. No matter how objects change their forms and locations in elastic and volatile fashions, FortiGate can identify them as Address objects, which 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.



[1] Security groups and/or relevant dynamic objects are imported to Fabric Connector objects.

[2] Objects are converted to the format that FortiManager uses (if FortiManager is not deployed, FortiGate will do the same).

[3] FortiManager propagates the definition of dynamic objects to all FortiGate instances under its management.

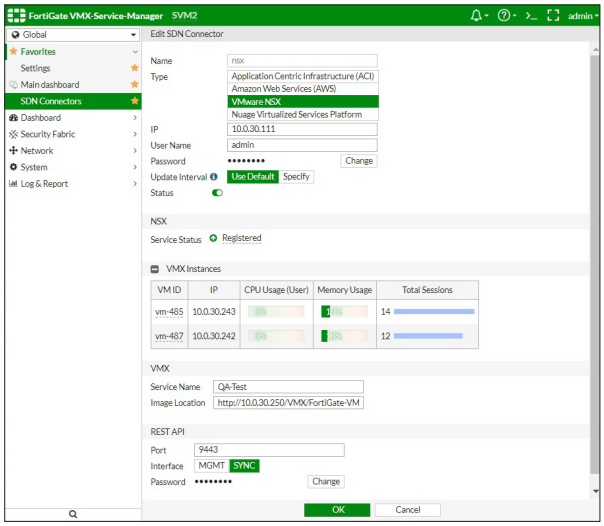
[4] FortiGate automatically updates Firewall Address objects containing IP addresses in order to identify them properly while maintaining connectivity.

Feature Highlights

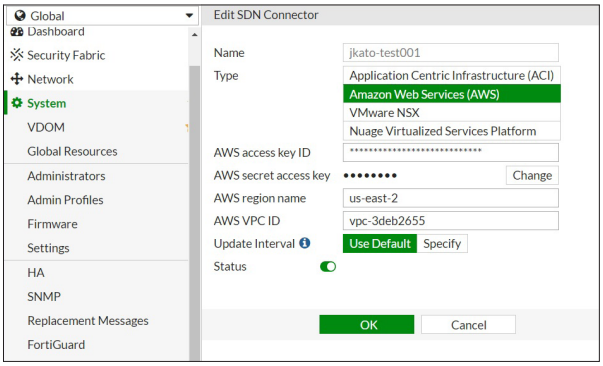
Initial Setup Summary

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

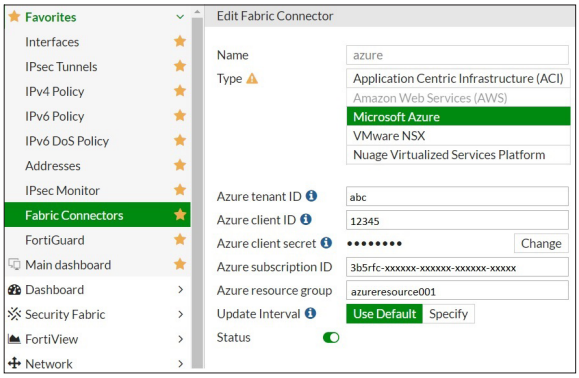
1. You have third-party SDN platforms or public cloud environments where virtual instances need to be protected by FortiGate.
2. Deploy FortiGate, or the combination of FortiGate and FortiManager, depending on the size of coverage in the network. If you have multiple sets of FortiGate, deploying FortiManager eases 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.



Connector configuration on FortiGate with VMware NSX



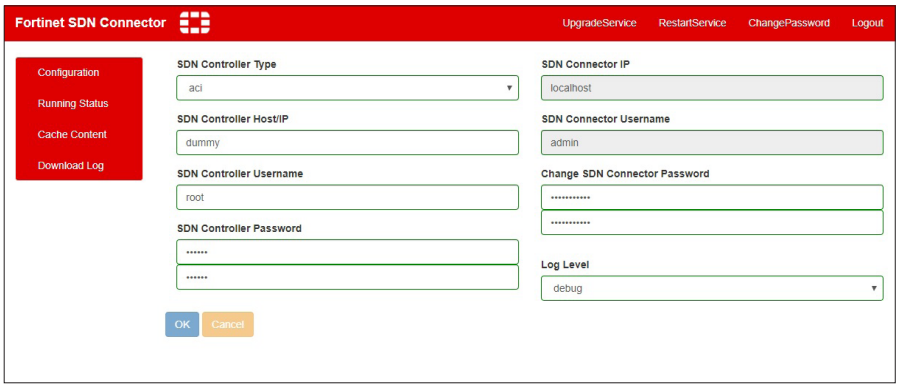
Connector configuration on FortiGate with AWS VPC



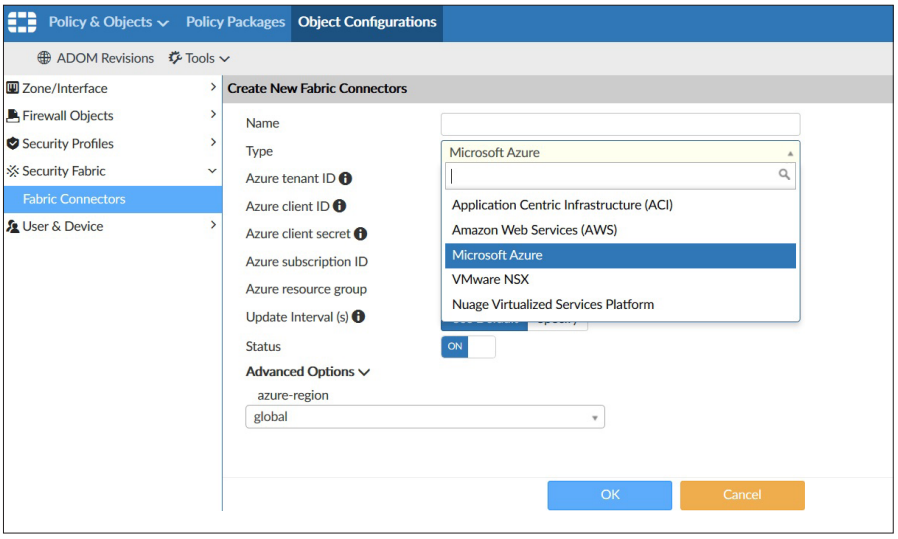
Connector configuration on FortiGate with Microsoft Azure

Feature Highlights

1. 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 must 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.
2. Create appropriate filter conditions to create specific groups of Address objects if required.
3. Once the Fabric Connector VM/FortiGate/FortiManager acquires connectivity to the SDN platform, it automatically imports 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.

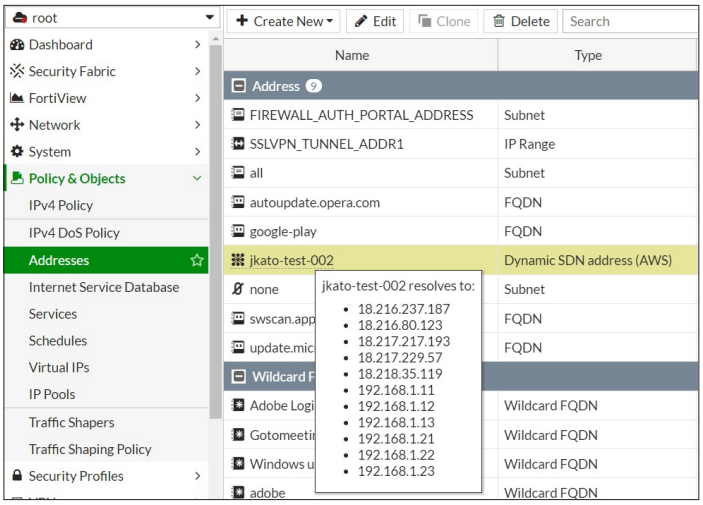


Off-the-box connector configuration on Fortinet Fabric Connector VM with Cisco ACI or Nuage Network VSP

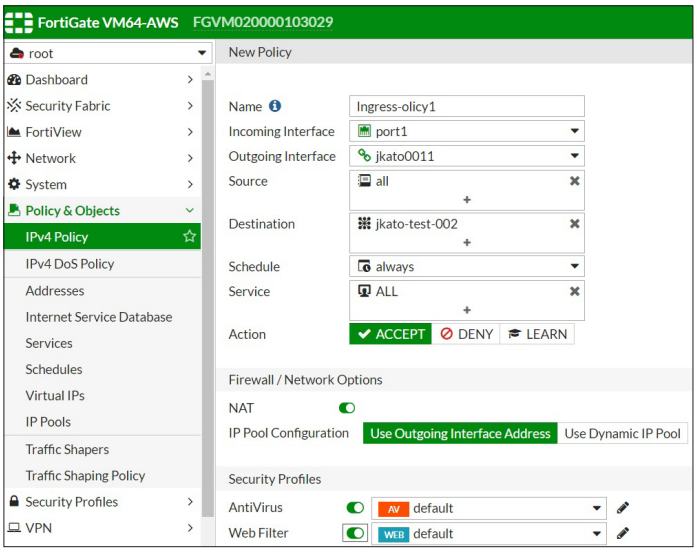


Connector configuration on FortiManager

Feature Highlights



Firewall Address objects are synchronized automatically



Create a Firewall Policy using the Address as a destination

Integration Matrix

				SUPPORTED VERSION OF	
THIRD-PARTY PRODUCT	VERSION	INTEGRATING CONNECTOR TYPE	DEPLOYMENT PREREQUISITES	FORTIGATE	FORTIMANAGER
CISCO ACI[4]	4.2 (3L, 4l)5	Out-of-the-box integration	A dedicated VM (VMware ESXi, KVM, and Hyper-V) to install Fortinet Fabric Connector v1.1.5 for Cisco ACI and Nuage Networks3	6.0.9+ / 6.2.4+ / 6.4.0+	6.2.5+ / 6.4.0+
		FortiGate or FortiManager built-in feature	Connectivity to Cisco ACI/APIC environment	6.4.1+	6.4.1+
VMWARE NSX-T	NSX-T 2.5.0+ / 3.0.0+ / 3.1.0+ (3.0/3.1 supports vSphere 7.0+)			6.4.3+ FortiGate-VM's certified versions with VMware NSX-T	6.4.4+
	NSX-T 3.1/3.2/4.0			7.0.6+	7.0.5+ / 7.2.1+
VMWARE ESXI AND VCENTER	VMware ESXi and vCenter vSphere 6.5+ / 6.7+ / 7.0+ or vCenter Server 6.5+ / 6.7+	FortiGate built-in feature	Connectivity to vSphere or vCenter environment	6.2.0+ / 6.4.0+	
	VMware ESXi 6.5+ / 6.7+ / 7.0+	FortiManager built-in feature	Connectivity to ESXi environment		6.2.0+ / 6.4.0+
	vCenter Server 6.5+ / 6.7+		Connectivity to vCenter environment		6.4.0+
AWS	N/A	FortiGate or FortiManager built-in feature	Connectivity to AWS VPC environment	6.0.0+ / 6.2.0+ / 6.4.0+	6.0.0+ / 6.2.0+ / 6.4.0+
MICROSOFT AZURE	N/A	FortiGate or FortiManager built-in feature	Connectivity to Azure VNet environment	6.0.0+ / 6.2.0+ / 6.4.0+	6.0.0+ / 6.2.0+ / 6.4.0+
ORACLE CLOUD INFRASTRUCTURE	N/A	FortiGate or FortiManager built-in feature	Connectivity to OCI VCN environment	6.0.1+ / 6.2.0+ / 6.4.0+	6.2.0+ / 6.4.0+
GOOGLE CLOUD	N/A	FortiGate or FortiManager built-in feature	Connectivity to GCP environment	6.0.2+ / 6.2.0+ / 6.4.0+	6.2.0+ / 6.4.0+
ALIBABA CLOUD	N/A	FortiGate or FortiManager built-in feature	Connectivity to AliCloud environment	6.2.0+ / 6.4.0+	6.2.0+ / 6.4.0+
LBM CLOUD VPC	N/A	FortiGate built-in feature	Connectivity to IBM Cloud Gen1 or Gen2	6.4.1+	
KUBERNETES	N/A	FortiGate or FortiManager built-in feature	Connectivity to a customer premise-located Kubernetes controller	6.2.0+ / 6.4.0+	6.2.0+ / 6.4.0+
			Connectivity to AWS EKS	6.2.0+ / 6.4.0+	6.2.0+ / 6.4.0+
			Connectivity to Azure AKS	6.2.0+ / 6.4.0+	6.2.0+ / 6.4.0+
			Connectivity to OCI OKE	6.2.0+ / 6.4.0+	6.2.0+ / 6.4.0+
			Connectivity to GCP GKE	6.2.0+ / 6.4.0+	6.2.0+ / 6.4.0+
OPENSTACK HORIZON	Rocky, Stein, Train, Ussuri, Victoria, Wallaby, and Xena	FortiGate or FortiManager built-in feature	Connectivity to OpenStack Horizon environment	6.0.3+ / 6.2.0+ / 6.4.0+ / 7.0.0+	6.2.0+ / 6.4.0+

1. FortiManager 6.0.5+ and 6.2.0+ add NSX-V 6.4.4 support.

2.FortiGate 6.2.1+ adds OpenStack Queens and Stein support.

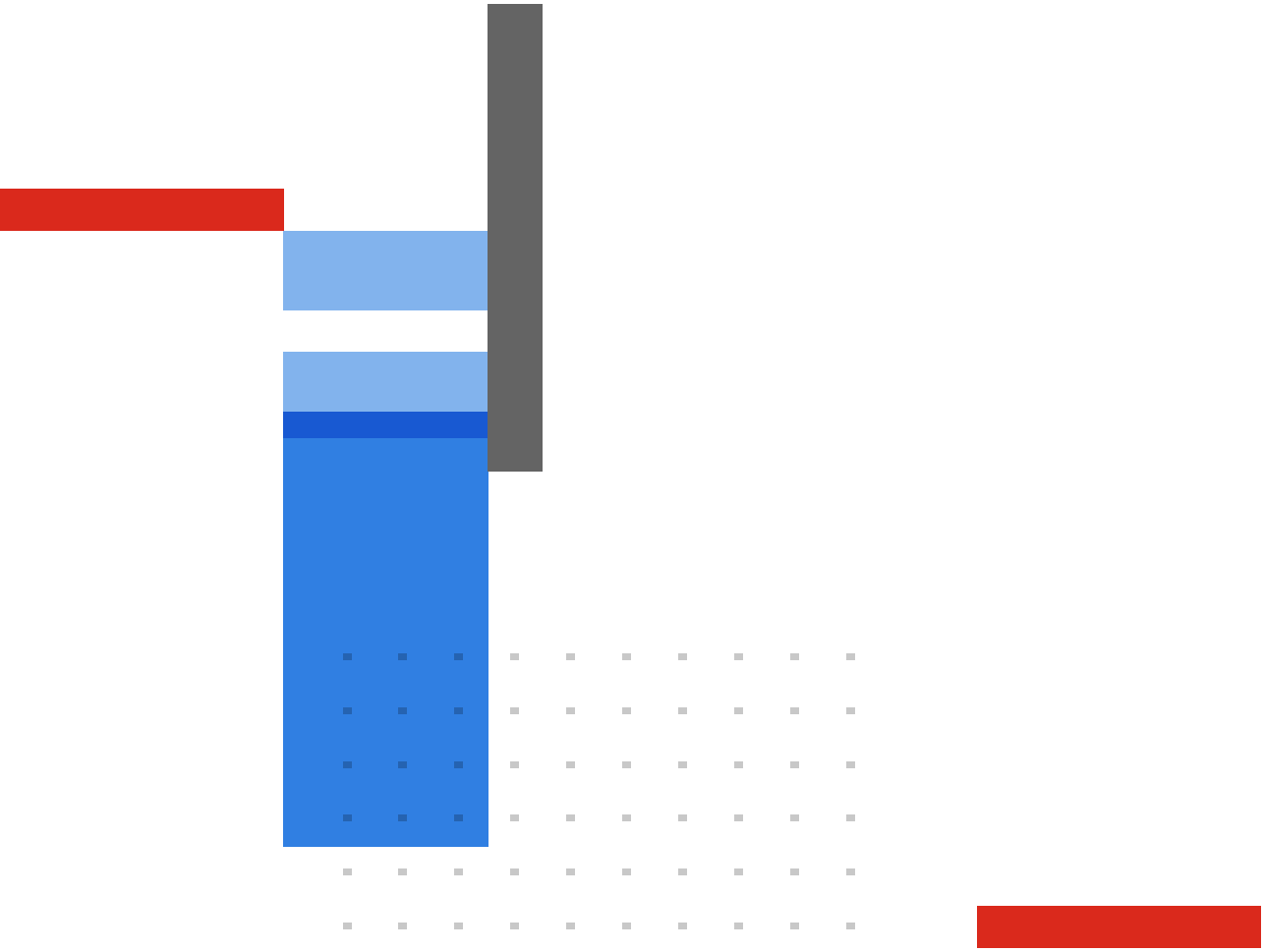
Ordering Information

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 and download the package or contact Fortinet technical support.

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



www.fortinet.com

January 10, 2023

FFC-DAT-R21-20230110