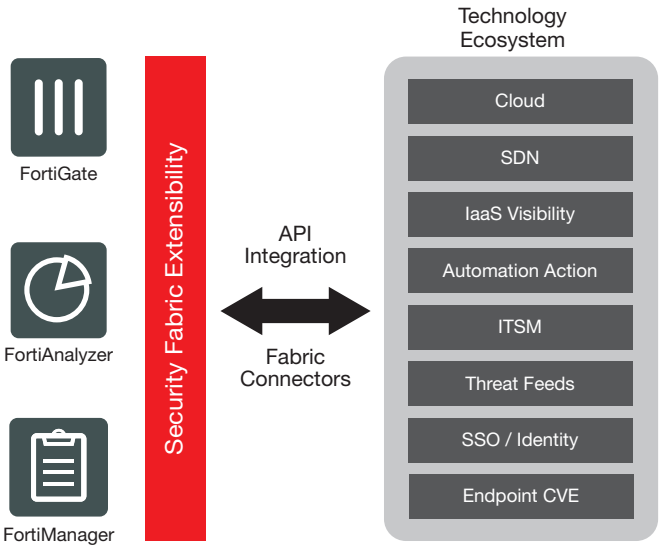
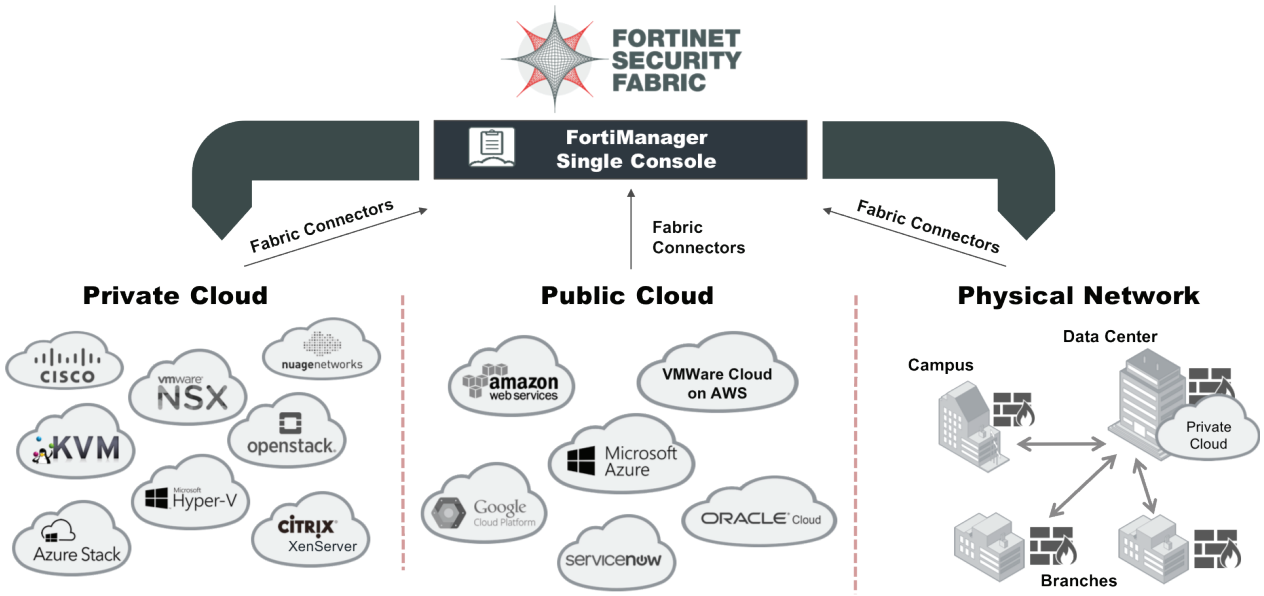
Introducing Fortinet Fabric Connectors

Open, One-click Integration

Fabric Connectors deliver turnkey, open integration with many different types of partner technologies in a multi-vendor ecosystem, promote security policy consistency through automation, reduce management burden, and support DevOps processes.



Fortinet Fabric Connectors break down the siloes in customer ecosystems that inhibit security visibility and management between and across multiple vendors' products, applications and data. By delivering open API-based integration of FortiGate or FortiManager with customer's existing vendor IT infrastructure, Fabric Connectors synchronize security with dynamic operational changes, automate security tasks, support DevOps processes and time to market, while ensuring coverage of the entire attack surface from IoT to the cloud.



Overview

Fortinet has built an immense ecosystem of industry leading Partners that are integrated into the Security Fabric through APIs and a variety of scripts using DevOps tools.

Now with Fabric Connector technology, Fortinet has developed an even deeper integration using partner API or specific code to provide security automation with simplified, consistent management and DevOps support in a dynamic, multi-vendor environment. Built by Fortinet, Fabric Connectors deliver a comprehensive, open approach to security that provides protection across the customer's entire operational ecosystem.

Customers benefit in several ways:

- simplified management and reduced latency by eliminating time consuming manual processes for security tasks
- improved security by closing security and compliance gaps that can be introduced when technology platforms don't talk to each other
- significant cost savings from more efficient resource utilization
- single security console

Customer Challenges and Solution

Enterprise applications and data today reside everywhere: on-premises, private, public and hybrid cloud. The growing adoption of cloud, shortage of resources and the lack of automation has increased the complexity of managing disparate, multi-vendor ecosystems while networks become more dynamic and the attack surface continues to expand. The lack of security integration with operational processes has slowed DevOps and impacted rapid application delivery.

Fortinet Fabric Connectors solve the pressing problem of ensuring that security keeps up with the rapid pace of operational changes in increasingly complex technology ecosystems with mostly manual processes. Fabric Connectors automate security synchronization with operational changes, reduce security gaps, and promote consistent management and security across hybrid environments. Fabric Connectors provide open API integration and orchestration of FortiGate or FortiManager with multiple SDN, cloud and partner technology solutions — including with leading vendors such as AWS, Azure, Cisco, Google, Nuage Networks, Oracle, ServiceNow, and VMware. Fabric Connectors are easily deployed without requiring hardware or software modifications to the third party technology platform.

Several different Connector types are available that extend security automation and ease the management burden in multi-vendor environments.

Fabric Connectors

FABRIC CONNECTOR TYPE	DESCRIPTION	AVAILABLE CONNECTORS WITH FORTIOS 6.0
Dynamic Policy Cloud	Integration with multi-cloud platforms (PaaS, IaaS) for dynamic policy objects	AWS, Microsoft Azure, Oracle Cloud, Google Cloud Platform*
Dynamic Policy SDN	Integration with SDN platforms (private, public) for dynamic policy objects	Cisco ACI, Nuage Networks, VMware NSX, Horizon OpenStack
IaaS Visibility	Fabric visibility into cloud infrastructure service resources	Future
Automation Action	Integration of Fabric Automation rules to automatically trigger actions based on events	AWS Lambda, FortiClient EMS Quarantine
ITSM/Incident Response	Integration with IT service management and incident response workflows	ServiceNow, Webhook
Threat Feeds	Integration to obtain external sources of threat feeds and automate security remediation for workloads	AWS GuardDuty
SSO/Identity	Integration with existing directory & identity servers to centrally manage user information and automatically apply security protection profiles assigned to each user	Microsoft Active Directory, Radius
Endpoint CVE	Integration to invoke auto quarantine of compromised endpoints when IOC is suspected	FortiClient EMS

Cisco ACI Connector

The Fabric Connector for Cisco ACI seamlessly integrates the L4-L7 network and security service insertion for both physical and virtual FortiGate appliances. Available as a downloadable device package imported into Cisco APIC and integrated into FortiOS 6.0 for enhanced functionality, the ACI Connector ensures that SDN workloads receive best-in-class security service insertion consistently throughout the network with dynamic policy automation.

Nuage Networks VSP Connector

The Fabric Connector delivers full integration of FortiManager with the Virtualized Services Controllers (VSC) to automate dynamic policy changes in the software defined data center. The integrated solution maximizes protection while utilizing the dynamic and reactive adaptability of the Nuage Networks VSP to deliver exceptional service velocity for multi-tenant and other virtualized data center applications.

VMware NSX Connector

The Fabric Connector for VMware NSX enables enhanced visibility, micro-segmentation and L4 – L7 security for east-west virtual traffic. The integration provides automated FortiGate VM deployment and management orchestration in the NSX environment, with the additional benefits of enhanced multi-tenancy and advanced security services. Dynamic objects (NSX tags or security group objects) are automatically imported by the Connector, resulting in dynamic policy updates in FortiGate without the need to understand complex management processes.

Horizon OpenStack Connector

The Fabric Connector for Horizon OpenStack enables a FortiGate physical or virtual appliance to operate as a security node in the OpenStack environment, and deliver the best of both worlds in advanced security and network performance. Available as a built-in capability in FortiGate, the Fabric Connector automatically populates and updates changes to OpenStack dynamic objects in FortiGate, ensuring firewall policies are updated based on any changes to instances, without needing manual intervention. Security is automatically synchronized by the Connector, in a single seamless package with OpenStack orchestration, management and traffic routing.

Public Cloud Connectors for AWS, Microsoft Azure, Oracle Cloud

Fabric Connectors for Cloud feature built-in integration to multi-cloud technology partners including AWS, Microsoft Azure, Google Cloud Platform*, and Oracle. Available as built-in integration, Fabric Connectors for the Cloud are easily deployed in a matter of minutes, and are used to retrieve dynamic object information from the multi-cloud technology platform and update firewall policies in FortiGate. FortiManager may optionally be used to orchestrate the dynamic object changes.

* Available in future FortiOS release

AWS GuardDuty Connector (IOC + Block)

The Fabric Connector for AWS GuardDuty automates security remediation for enterprise workloads running on Amazon Web Services. This integration accelerates time-to-protection for threats detected by the AWS service and automates the creation of network firewall rules in FortiGate to mitigate those threats, rather than relying on manual incident response and human intervention.

AWS Lambda Connector

The AWS Lambda Connector enables you to automate actions using AWS Lambda code in your environment. Depending on the events or incidents that occur, the Connector will initiate FortiOS to trigger automated actions by running the code.

ServiceNow Connector

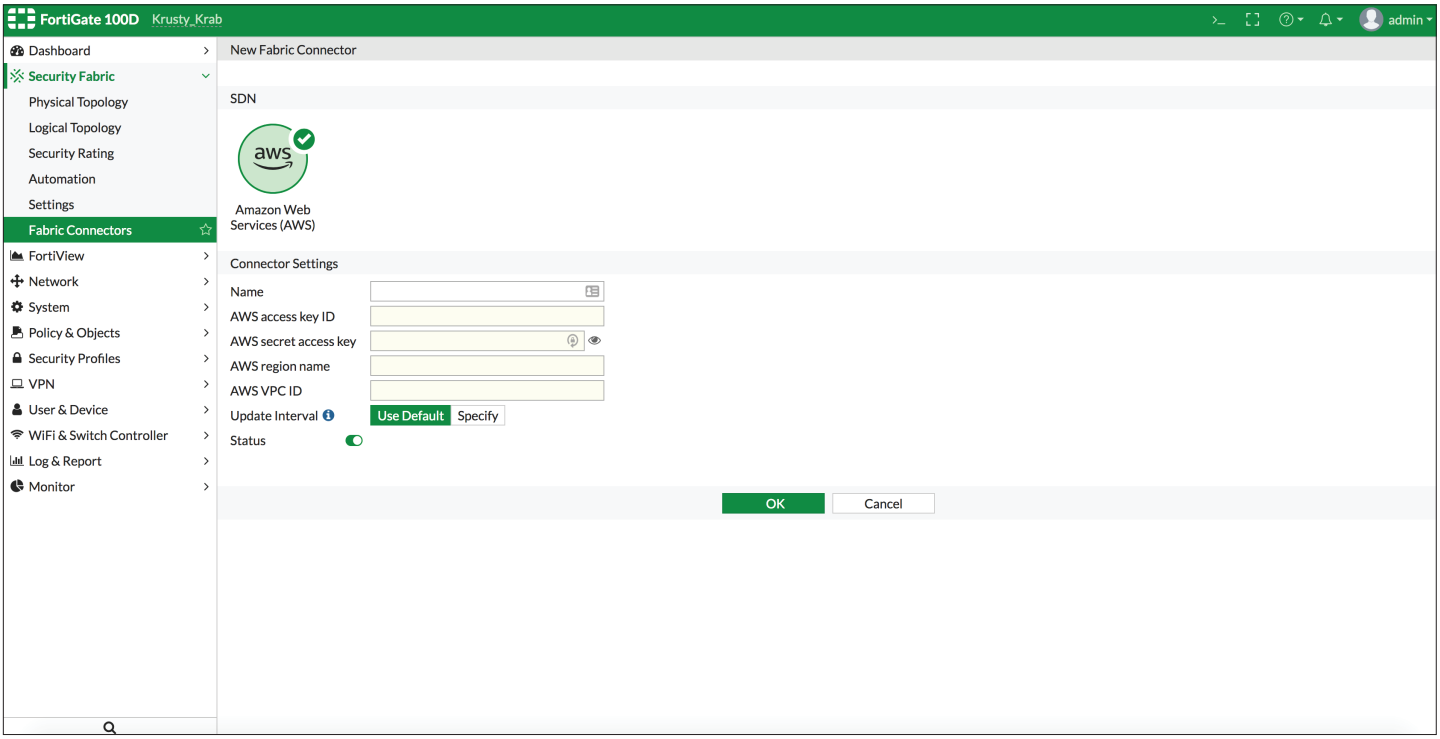
The Fabric Connector for ServiceNow security operations & ITSM (IT Service Management & Incident Response) platform automates changes to security policy and configurations when work order tickets are created and deployed. For example, any policy or configuration changes resulting from dynamic ticketing and workflow updates will automatically trigger firewall policy updates to the FortiGate virtual firewall (via FortiManager) without requiring manual synchronization. This ensures security is synchronized at all times without needing security staff intervention.

FortiClient EMS Quarantine Connector

The Fabric Connector integrates FortiGate with FortiClient EMS for endpoints connecting to FortiGate, to automate quarantine of compromised hosts. When an IOC (indicator of compromise) is suspected, FortiGate initiates an auto quarantine by EMS of the compromised endpoint, eliminating the need for manual configuration. The quarantined endpoints are visible in Fabric topology views for analysis and remediation actions.

SSO (Single Sign On)/Identity Connectors

The Fortinet Single Sign On (FSSO) agent enables FortiGate appliances to authenticate network users for security policy or VPN access without asking them again for their username and password. By using the SSO/Identity Fabric Connector, organizations can leverage their existing directory and identity servers to centrally manage user information and at the same time automatically apply the security protection profiles assigned to each user.



Fabric Connectors are easy to deploy, with one-click activation

GLOBAL HEADQUARTERS
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard
#12-01 Suntec Tower Three
Singapore 038988
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

FST-PROD-PB-FFC

FFC-PB-R2-201810