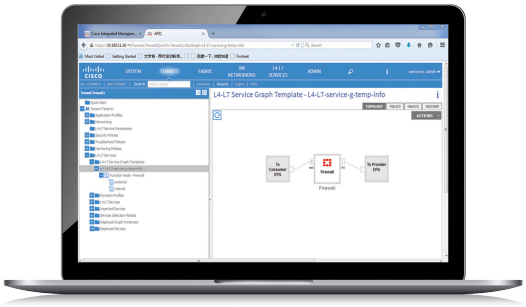
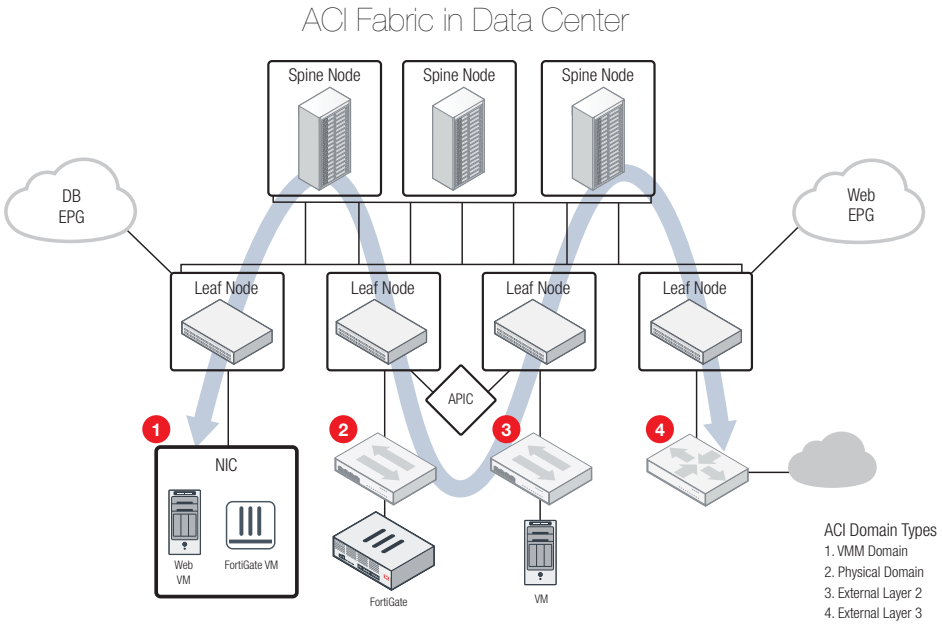
DATA SHEET

FortiGate® Connector

For Cisco ACI Device Package



Fortinet's FortiGate next generation data center firewall solution integrates with Cisco Application Policy Infrastructure Controller (APIC) to offer complete automation of Layer 4 through 7 security policies and supports a defense-in-depth strategy while enabling deep visibility, automated policy compliance, and accelerated threat detection and mitigation. The integration of FortiGate (both virtual and physical appliance) with Cisco APIC is the best approach that focuses on the application by delivering segmentation that is dynamic and application-centered.



FortiGate L4–L7 Security Services integration with Cisco ACI

Key Features

- Automated security policies
- Deep defense strategy
- Clear visibility
- Policy compliance
- Accelerated threat detection and mitigation

FEATURES

The FortiGate Connector for Cisco ACI Device Package is an add-on, system-based approach to address security needs for next generation data centers and clouds. It is unlike the software-only network overlay approach based on host virtualization, which offers limited visibility, performance, and scale and requires separate management of underlay and overlay network devices and security policies. Instead, the FortiGate Connector for Cisco ACI Device Package integration approach addresses the security needs of the next generation data center by using an application-centric, unified, and automated approach to security policies in the data center and cloud infrastructure that is decoupled from the underlying network topology, supports application mobility, offers real-time compliance lifecycle management, and reduces the risk of security breaches.

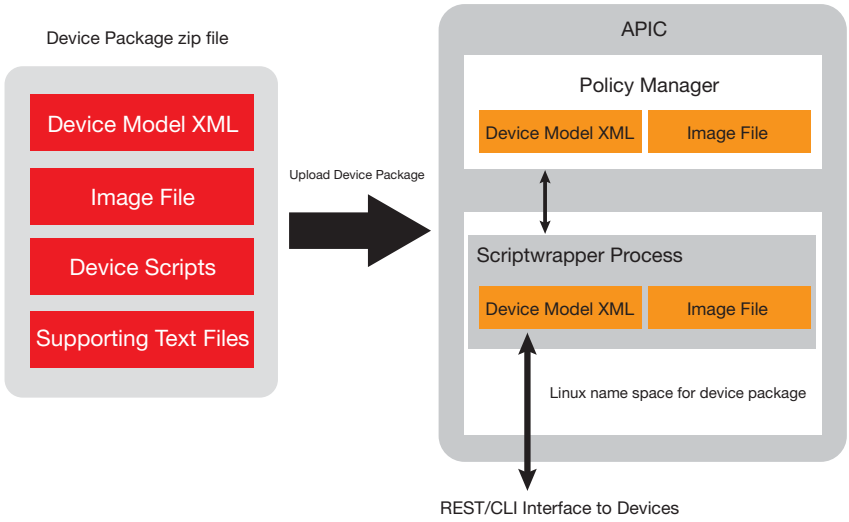
How does it work together?

Fortinet Software-Defined Security (SDS) framework provides the visionary integration path for software-defined networking (SDN), network function virtualization (NFV), and programmable switches platforms and enables service policy automation through RESTful APIs, scripting with JSON and XML data format.

The integration requires two components:

- Fortinet FortiGate device packages to be uploaded to APIC
- Cisco ACI-certified FortiGate appliances both physical and virtual

Device Package Architecture



Centralized Policy Lifecycle Management and Layer 4 through 7 Service Automation

FortiGate Connector for Cisco ACI Device Package automates and centrally manages Layer 4 through 7 security policies in the context of an application using a unified application-centric policy model that works across physical and virtual boundaries as well as FortiGate devices. This approach reduces operational complexity and increases IT agility without compromising security.

FortiGate Connector for Cisco ACI Device Package automates and centrally manages security policies in the context of an application using a unified and innovative security policy abstraction model that works across physical and virtual boundaries. The central definition of these security policies through the Cisco ACI group-policy model is performed at the Cisco Application Policy Infrastructure Controller (APIC), either directly through the GUI or through JavaScript Object Notation (JSON) or XML through the open northbound Representational State Transfer (REST) API.

Layer 4 to Layer 7 Service Insertion

Cisco ACI Device Package also supports Fortinet L4-7 security service insertion and policy automation for critical security services such as NGFW, UTM, and VPN in the application flow associated with one (or more) ANPs, regardless of the location of these Fortinet security services in the data center. This feature allows the security administrator to keep, integrate, or extend previously defined security policies by using these Fortinet security services and devices when connecting them to the Cisco ACI fabric.

Security administrators define service policies like High Availability, virtual IP, port-forward and so on for different applications in APIC and create service graphs to identify the set of network or service functions that are needed by the applications. When a security policy is triggered during the application deployment lifecycle, Cisco APIC will force the package to route through the FortiGate for advanced firewall inspection without manual configuration.

FEATURES

How does FortiGate Connector for Cisco ACI Device Package Address Key Challenges?

CHALLENGE	SOLUTION
Security concerns are the biggest obstacle for 'cloud readiness'	FortiGate Connector for Cisco ACI Device Package security solution integration provides automated security provisioning and a full range of security protections and threat-prevention capabilities in a highly dynamic and agile data center. FortiGate Security Firewalls can be deployed as physical or virtual solutions and address today's ever-changing threat landscape with a modular and dynamic security architecture.
Manual security provisioning is error-prone	FortiGate Connector for Cisco ACI Device Package security solution provides centralized and automated lifecycle management of Layer 4 through 7 network security policies across the entire data center network.
Application workloads are being modified, added, changed, and deleted (MACD) in agile data center environment	FortiGate Connector for Cisco ACI Device Package security solution automates service modifies, adds, changes, deletes and eliminates the challenge of managing the complex techniques of traditional service configuration, therefore reduces operating costs.
Compliance with industry regulations like PCI and HIPPA	Cisco ACI helps ensure that the configuration in the fabric always matches the security policy. Cisco APIs can be used to pull the policy and audit logs from the Cisco Application Policy Infrastructure Controller (APIC) and create compliance reports (for example, a PCI compliance report). This feature enables real-time IT risk assessment and reduces the risk of noncompliance for organizations.
Limited visibility into the traffic	FortiGate Connector for Cisco ACI Device Package security solution provides deep visibility and accelerated threat response based on real-time network intelligence.

ORDER INFORMATION

All FortiGate customers can use this device package. This feature is available for download free of charge. The latest connector package can be downloaded from support.fortinet.com. Go to Download > Firmware Images > Select FortiGateConnector in Product, click Download tab, choose CiscoACI > v2.00 > 2.6.

FortiGate Connector for Cisco ACI supports the following predefined models:

	SUPPORTED VERSIONS				
FortiGate Connector for Cisco ACI versions	**v2.2**	**v2.3***	**v2.4***	**v2.5***	**v2.6***
Supported Cisco APIC versions	**3.2 (1m), 3.1 (2o)**	**3.2 (1m), 4.0 (2c), 4.0 (1h)**	**4.1 (2g), 4.2 (1j)**	**4.2 (1j), 4.2 (3l)**	**4.2 (6h)**
FG-300D	✓	✓	✓	✓	✓
FG-300E	✗	✗	✓	✓	✓
FG-301E	✗	✗	✓	✓	✓
FG-600D	✓	✓	✓	✓	✓
FG-800D	✓	✓	✓	✓	✓
FG-900D	✓	✓	✓	✓	✓
FG-1000C	✓	✓	✓	✓	✓
FG-1000D	✓	✓	✓	✓	✓
FG-1200D	✓	✓	✓	✓	✓
FG-1500D	✓	✓	✓	✓	✓
FG-1800F / 1801F	✗	✗	✗	✗	✓
FG-2200E / 2201E	✗	✗	✗	✓	✓
FG-2600F / 2601F	✗	✗	✗	✗	✓
FG-3000D	✓	✓	✓	✓	✓
FG-3100D	✓	✓	✓	✓	✓
FG-3200D	✓	✓	✓	✓	✓
FG-3300E / 3301E	✗	✗	✗	✓	✓
FG-3400E / 3401E	✗	✗	✗	✓	✓
FG-3600E	✗	✗	✓	✓	✓
FG-3700D	✓	✓	✓	✓	✓
FG-3980E	✓	✓	✓	✓	✓
FG-4200F / 4201F	✗	✗	✗	✗	✓
FG-4400F / 4401F	✗	✗	✗	✗	✓
FG-6300	✓	✗	✗	✓	✓
FG-6500	✓	✗	✗	✓	✓
FG-VM	✓	✓	✓	✓	✓

* v2.3 and later supports Service Manager mode. For more details, refer to the deployment guide.
Note: Please attempt to use Fortinet Device Package for Cisco ACI with any FortiGate model with caution. Only those listed above have been confirmed for support. While using an unknown FortiGate model, manually configure and ensure that the port names match the actual FortiGate model. For more information, please contact the support team.

FGC-DAT-R15-20220517