Accelerated Software-Defined Security with Cisco Application Centric Infrastructure

Organizations are looking to deliver more agile private cloud infrastructure, from compute to storage to networking, to enable applications that can connect more easily and rapidly with end-users, customers, and partners. But networking and network security traditionally tied to rigid dedicated hardware increases OPEX costs and management complexity. Networking and Layer 4 through Layer 7 application services usually requires manual configuration and constant management updates to keep up with changes. In order to respond to agility requirements in the software-defined data center/private cloud paradigm shift, networking and application services also need to respond with automation based on predefined policies and on-demand orchestration.
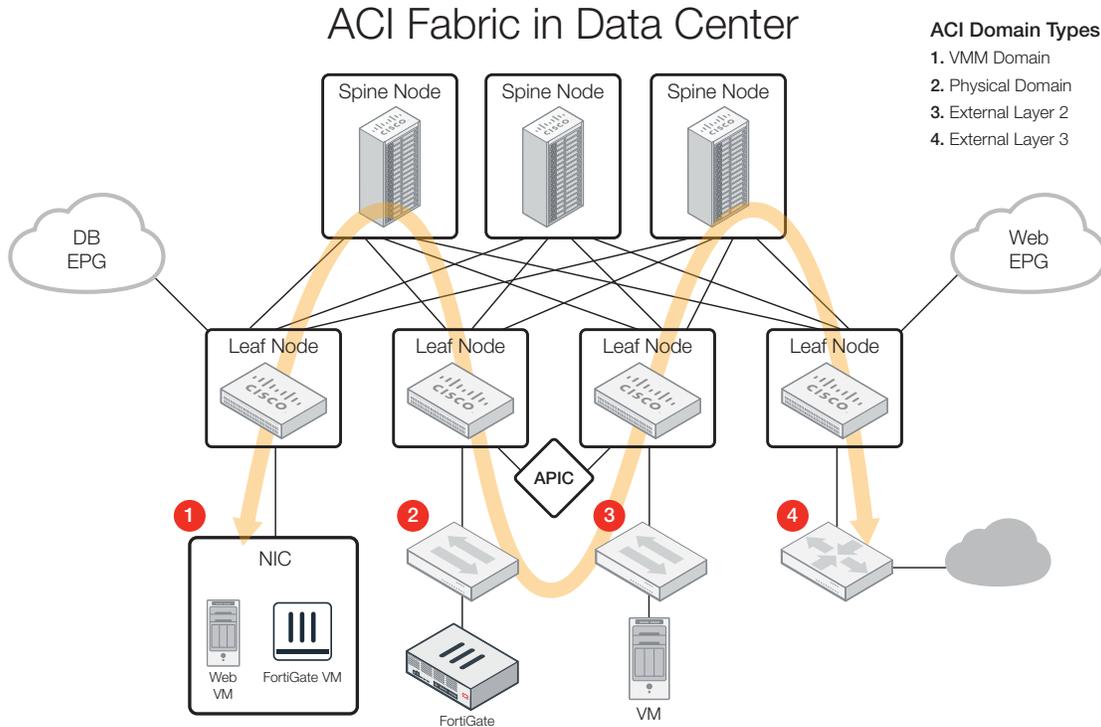
Cisco® Application Centric Infrastructure (ACI) integrates Fortinet FortiGate appliances for the private cloud to deliver application-centric security automation in modern data centers.

The integration of Cisco ACI architecture with the FortiGate solutions provides automated, predefined policy-based security provisioning and security policy updates for NGFW, UTM and VPN services. The solution enables transparent security services insertion anywhere in the network fabric through a single-pane-of-glass management.

Solution Highlights

- Better visibility and security correlated with overlay/underlay networks

- Lower TCO from reduced administrative OPEX Accelerated application and L4-L7 security deployment

- Increased efficiency in service provisioning and network security segmentation

F::RTINET®
Fabric-Ready

ACI Fabric in Data Center

ACI Domain Types
1. VMM Domain
2. Physical Domain
3. External Layer 2
4. External Layer 3

Figure 1: Cisco ACI and FortiGate Solution

Cisco ACI provides the improvements in terms of forwarding packets. The network's application-aware policy model is the foundation of security within Application Centric Infrastructure. It essentially "dictates what can talk to what on this network – it all gets enforced in appliances at the edge.

The integration of Cisco ACI and the Fortinet FortiGate solution comes with the following benefits:

- Consistency and transparency across physical and virtual application workloads

- Single-pane-of-glass management enablement from Cisco APIC with full visibility on security policy enforcement

- Predefined security policies are deployed rapidly through complete application deployment lifecycle

- Scale on-demand with automation

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
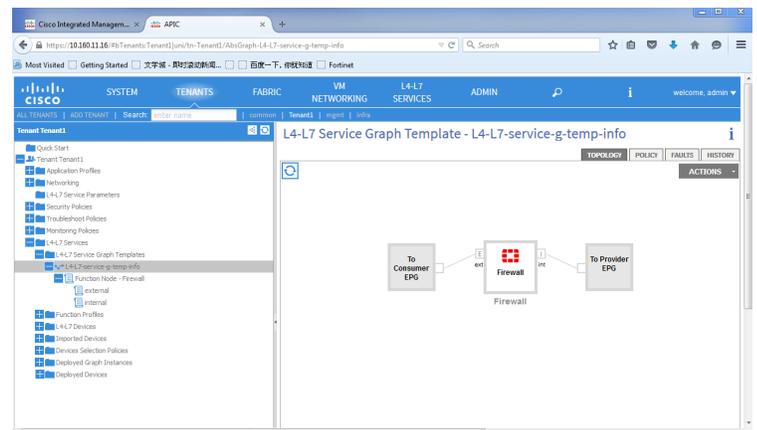

Figure 2: Service graph design in APIC controller simplifies logical application flow

Layer 4 and Layer 7 Service Insertion Flow

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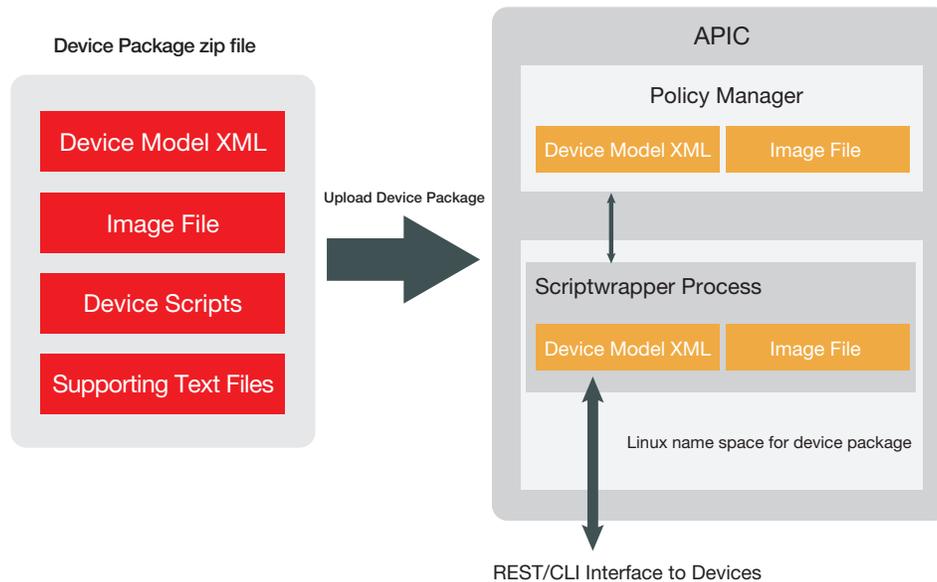

Figure 3: Device Package Architecture

The Cisco APIC integrates with Fortinet FortiGate appliances for the private cloud to simplify network security deployment. To connect the FortiGate appliance to the Cisco ACI fabric, the virtualization administrator simply needs to associate the predefined security policy with the virtual machine networks created by the Cisco APIC. Cisco ACI fabric is designed to provide overlay independence and can bridge frames to and from in the heterogeneous environments.

FORTINET.