Accelerated Security Automation with Cisco Application Centric Infrastructure and Fortinet Solution Overview

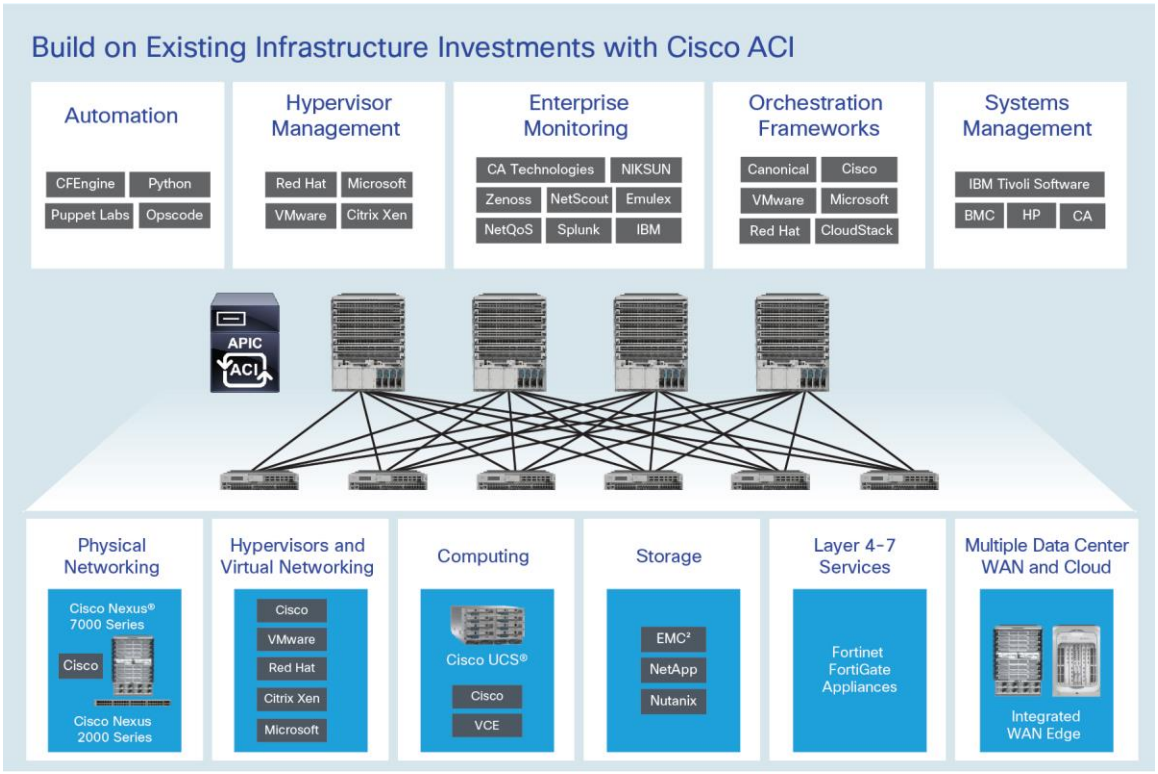
BENEFIT SUMMARY

- Better visibility and security correlated with overlay and underlay networks
- Lower total cost of ownership (TCO) from reduced administrative operating expenses (OpEx)
- Accelerated application and Layer 4 through 7 network security deployment

Organizations are seeking to deliver agile data center infrastructure, including computing, network, and storage resources, to enable applications to be delivered easily and efficiently to end users, customers, and partners. But networking and network security traditionally has been tied to rigid dedicated hardware, an approach that increases data center operating expenses (OpEx) and management complexity. Networking and Layer 4 through 7 application services usually require manual configuration and constant management updates to keep up with data center changes. To meet today's agility requirements, networking and application services need to respond quickly through automation, with predefined policies and on-demand orchestration.

The Fortinet FortiGate firewall solution integrated into the Cisco® Application Policy Infrastructure Controller (APIC) delivers application-centric security automation in modern data centers. The solution provides automated and predefined policy-based security provisioning for next-generation firewall services. It enables transparent security service insertion anywhere in the network fabric through single-pane management. Figure 1 provides an overview of the solution.

Figure 1. FortiGate Integration with Cisco ACI



Cisco Application Centric Infrastructure (Cisco ACI™) enhances packet forwarding with application-workload awareness. The integration of Cisco ACI and the FortiGate solution offers the following benefits:

- Consistent and transparent deployment of workload security across physical and virtual application environments
- Single-pane management through the APIC with full visibility into security policy enforcement
- Predefined security policies deployed on command and automated through the complete application deployment lifecycle

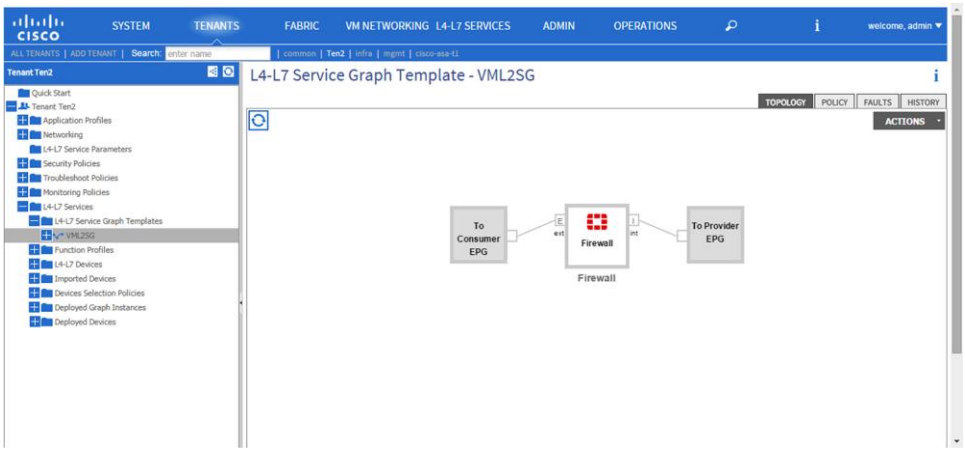
How Does the Joint Solution Work?

Cisco and Fortinet jointly introduced a unified solution that provides rapid security provisioning through the high-performance Cisco ACI fabric. The Fortinet Software-Defined Network (SDN) Security (SDNS) framework provides the visionary path for security integration in SDN and network function virtualization (NFV) deployments. The framework enables service policy automation through representational state transfer (REST) APIs, JavaScript Object Notation (JSON) scripts, and XML data formats to provide a transparent and easy-to-use experience using Cisco's Layer 2 through 3 network fabric.

The joint Fortinet FortiGate Connector for Cisco APIC solution requires two major components from Fortinet:

- FortiGate device package for the APIC
- FortiGate physical or virtual appliances

Figure 2. L4-L7 Service Insertion in Cisco APIC



IT administrators can easily define the application security rules for different workloads in the APIC and configure the policies within the FortiGate appliances. When a security policy is triggered during the application deployment lifecycle, the Cisco controller redirects the application traffic through the FortiGate appliances for advanced firewall inspection - including IP reputation, web filtering, antivirus, Domain Name System (DNS) filtering, Secure Shell (SSH) inspection, intrusion prevention system (IPS), and distributed denial-of-service (DDoS) attack monitoring services - without manual intervention.

Conclusion

Security concerns remain the biggest obstacle for cloud deployment. Application workloads are constantly modified, added, changed, and deleted through error-prone manual security provisioning. The integration between FortiGate and Cisco ACI helps eliminate cumbersome processes and automates security policies, enabling central orchestration with better traffic visibility and scalability based on application workloads.

For Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

More Information

http://www.cisco.com/go/aci

http://www.fortinet.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-735898-01 08/16