Securing Event Network Operations with the Cisco Adaptive Security Virtual Appliance

Cisco IT Insights

Protecting Network Operations at Cisco's Largest Event

The Cisco Live!™ U.S. conference is Cisco's largest annual event. To provide network connectivity for the 27,000 people who attended the 2014 conference in San Francisco, Cisco IT built a wired and wireless event network that was a full production deployment. To manage that network, Cisco IT also built an on-site network operations center (NOC).

Per Hagen, the Technical Marketing Engineer for Adaptive Security Appliances (ASA) at Cisco, was tasked with ensuring the security of the NOC systems and applications while allowing access by authorized users. The event's NOC team needed both wireless and VPN access to NOC resources from the event's venue at the Moscone Center, their rooms at adjacent hotels, and the Cisco campus located 40 miles to the south.

The challenge for wireless connectivity was to keep the NOC constantly accessible to authorized users while blocking connections from anyone who might want to show off his or her hacking skills at a high-profile event. Another challenge was positioning secure VPN access in a physical form factor given the restraints of space, power, and cooling in the event environment.

To address these challenges, Cisco IT used the FlexPod, an integrated computing, networking, and storage solution developed by Cisco and NetApp. FlexPod components include Cisco® Unified Computing System (Cisco UCS®) servers, Cisco Nexus® switches, and NetApp unified storage systems.

For optimum performance and security of VPN access, Hagen and his team wanted to put a security appliance in a particular part of the FlexPod where everything was already virtualized and a physical firewall wasn't feasible.

PRODUCT LIST

Network Management

- FlexPod Datacenter with:
  - 2 Cisco UCS 5108 Blade Servers
  - 2 Cisco UCS 6248UP Fabric Interconnects
  - 2 Cisco Nexus 7004 Switches
  - 2 NetApp FAS8040 Storage Systems
  - VMware vSphere Server Virtualization Platform

Security

- In the FlexPod:
  - Cisco ASAv30 Virtual Security Appliance
  - Cisco AnyConnect® SSL VPN

Security in a Virtual Appliance

For NOC security at Cisco Live 2014 in San Francisco, Hagen chose the Cisco Adaptive Security Virtual Appliance (Cisco ASAv). Implemented in the FlexPod, the Cisco ASAv software was installed in a VMware environment running on Cisco UCS B-Series Blade Servers, with connection to the event network over multiple 10-GB links. (Figure 1)

Using a Cisco ASAv instead of a physical ASA meant the security team could put the firewall exactly where they needed it in the FlexPod to protect the NOC systems and applications. The team defined networks inside the FlexPod to support the remote access VPN for the NOC, then connected those networks to the full event network via the Cisco ASAv.

The virtual Cisco ASAv worked in parallel with the multiple Cisco ASA 5585-X hardware appliances deployed to secure connectivity in the event network, as shown in Figure 2.

Hagen notes, "The Cisco ASAv has all the capabilities of a regular ASA, and you can deploy it in all the same places and in some additional ones. From a management point of view, there is no difference. Using the virtualized form factor made it very easy for us to deploy this solution compared to a physical appliance for the on-site NOC. We didn't have to think about physical wiring. We just gave it access to the correct VLANs."

Figure 1. Cisco ASAv Implementation on Cisco UCS Servers in the FlexPod System for Cisco Live

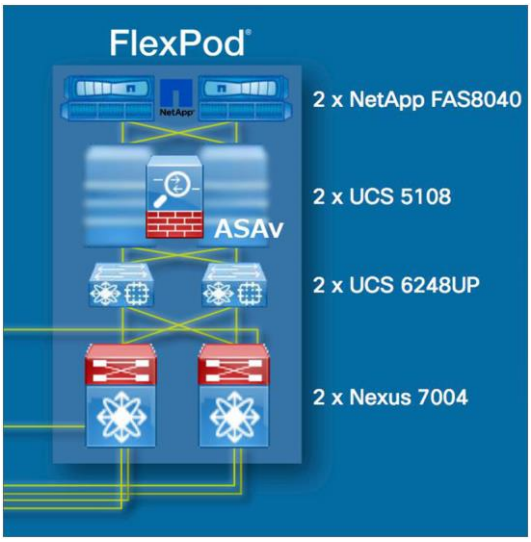
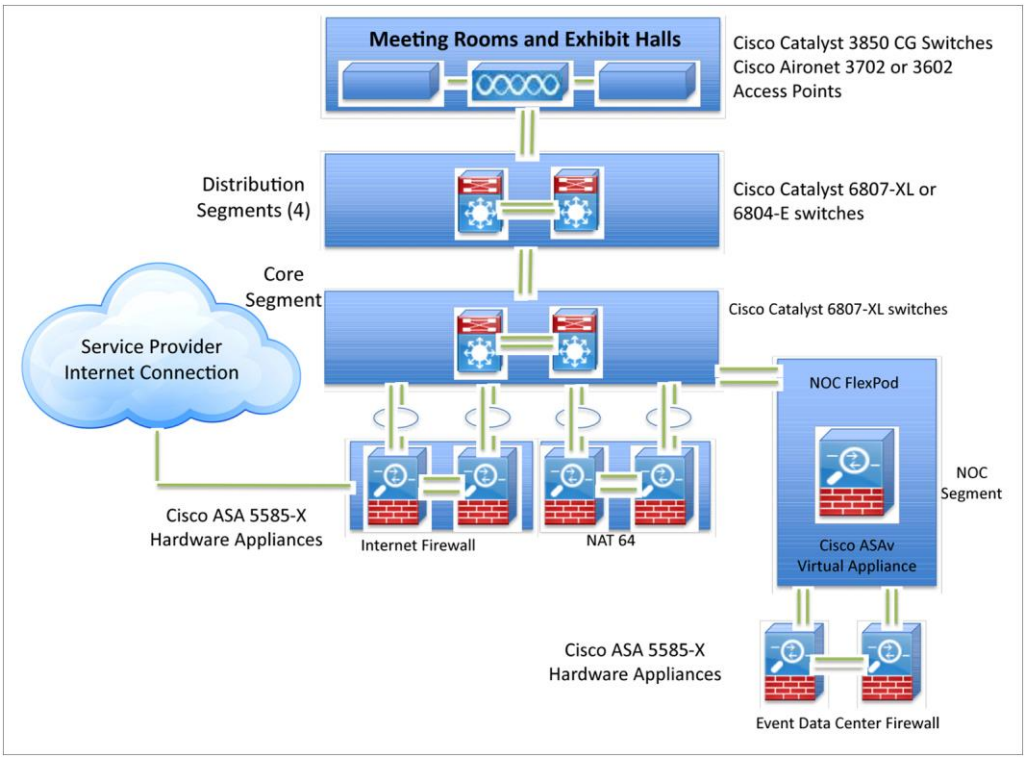


Figure 2. Cisco Live 2014 San Francisco Event Network Topology



The Cisco ASAv also controlled access to NOC resources for wireless users. All event administrative staff had Active Directory accounts and was authenticated against an Active Directory instance in the event NOC. This authentication design made it easy to add new access capabilities for new users or to remove access when someone no longer needed a certain service. After authorized users logged in to the secure NOC environment, they had access to all management functions for running the event network and recording conference presentations.

Although the Cisco ASAv supports stateful redundancy, that capability wasn't needed for the Cisco Live U.S. conference. Instead, Hagen and his team deployed a single instance of Cisco ASAv and relied on the redundant design of other FlexPod components. For example, if a problem developed with the underlying server, Cisco ASAv could have been activated on the other server within minutes. Additional FlexPod built-in redundancy included two Cisco Nexus 7000 Series Switches configured with Cisco Virtual Port Channels (vPC) technology connected to dual NetApp Fibre Channel Fabric-Attached Storage (FAS) servers. Those storage servers were running VMware VMotion, so if the primary server failed, the other would have taken over immediately.

Fast Deployment, Solid Performance

Hagen and his team were extremely pleased with this high-profile deployment of the Cisco ASAv in a large, production network. "The appliance was rock solid. It had 100 percent uptime, and there were no performance issues, even though we encountered some denial-of-service and other attacks," he says. "Nobody even knew that we were running a virtual ASA instead of a physical ASA."

The flexibility of a virtual ASA meant the team could deploy a firewall in 15 to 20 minutes, from the time required to download the software to when the Cisco ASAv was up and running. Then it took only a short time to configure the remote access VPN. "That's way faster than you could do it with a physical ASA, because there's no mounting and no physical wires," says Hagen. "It also meant that I could deploy the Cisco ASAv remotely instead of going to the Moscone Center to 'rack and stack' a physical appliance."

Hagen is already thinking about how he can make greater use of Cisco ASAv virtual appliances at next year's Cisco Live U.S. conference. For example, virtual ASA appliances could be used in parts of the network outside the NOC where a physical ASA would not be possible or easy to deploy. Additionally, the Cisco ASAv can be deployed on existing servers to avoid the extra costs of powering a physical security appliance. Says Hagen, "The Cisco ASAv is a versatile product, and I'm looking forward to seeing what else we can do with it."

For More Information

To learn more about the Cisco Adaptive Security Virtual Appliance, visit http://www.cisco.com/go/asav

To learn more about FlexPod, visit http://www.cisco.com/go/flexpod

To read Cisco IT case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT http://www.cisco.com/go/ciscoit

To view Cisco IT webinars and events about related topics, visit Cisco on Cisco Webinars & Events

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

Printed in USA XXX-XXXXXX-XX 12/14

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

XXX-XXXXXX-XX 12/14