Cisco IT Insights

Network Security at the 2016 Rio Olympic Games

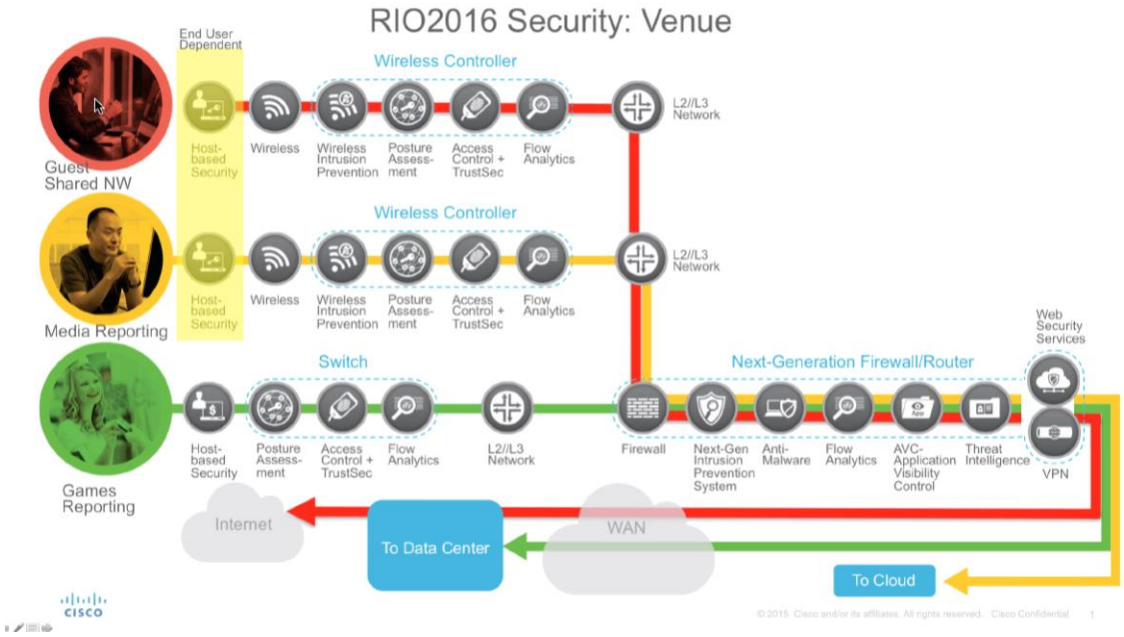
What: Secure Network for Record-Setting Media Event

Cisco built the network for the 2016 Rio Olympic Games. It was a monumental undertaking. Athletes and fans counted on reliable, immediate results from events in 37 competition venues. More than 25,000 reporters from 200 news agencies depended on the network to transmit stories to their own clouds. For NBC alone, network outages from malware or cyberattacks could affect 27.5 million TV viewers watching 6755 hours of programmed viewing—and decimate advertising revenue.

With stakes like these, the 2016 Rio Olympics organizers needed the most advanced network security. They hired us to design and build a network using the same security solutions we use in our own enterprise network. “We didn’t build a network and then add on security,” says Doug Dexter, senior security advisor with the Cisco Security Trust Organization. “We designed security into the network from the beginning. Identification and authentication are as essential as connectivity.”

The network we designed had three separate subnets: guest, media reporting, and timing and scoring (Figure 1). When any device attempted to connect, the network asked, “Who are you?” If the network didn’t recognize the device—a guest’s smartphone or tablet, for instance—the device connected over the guest network to the public Internet. Reporters’ devices connected to the media-reporting network. Devices authorized to transmit timing and scoring results connected to the timing and scoring subnet—the only subnet connected to the Olympics data center. The news that Usain Bolt ran the 100M final in 9.81 seconds and that Simone Biles scored 15.966 in floor exercise came across the timing and scoring subnet.

Figure 1. The Rio Olympics Network Automatically Connected Devices to Media Reporting, Timing and Scoring, or Guest Subnet



Security Solutions

We built the network backbone using Cisco ASR 9000 Aggregation Services Routers. We protected it by using multiple Cisco security solutions to:

- Identify devices and connect them to the right subnet. Reporters and Olympics officials installed the Cisco AnyConnect Secure Mobility Client on their laptops and mobile devices. Cisco Identity Services Engine (ISE) recognized the user and device, and then connected the device to the media reporting or games reporting VPN. ISE connected unrecognized devices to the Internet.
- Block unauthorized access. Cisco Adaptive Security Appliances (ASAs) provided firewall services at each data center and event venue. We deployed 148 ASAs.
- Monitor network activity to detect threats that made it past defenses. Cisco Sourcefire FIREsight and Lancope Stealthwatch provided intrusion detection.
- Detect malware. Cisco Advanced Malware Protection (AMP) continuously analyzed file activity across the Olympics network. Security administrators used the information to quickly detect, contain, and remove advanced malware.
- Block illegitimate websites. Olympics guests used search engines to look up lodging, buy tickets, background on athletes and events. Illegitimate websites like “10DollarOlympicstickets” often carry malware. We blocked access to these sites by using the OpenDNS cloud service. OpenDNS constantly learns about fake websites because it sees two percent of the world’s Internet traffic. Every day, OpenDNS filtered an average of 22 million DNS lookups from Olympic networks and denied access to an average of 22,000 malicious networks. “These lookups are especially concerning because they originate from within the network,” Dexter says. “Denying guest devices access to malware sites is critical to maintaining a clean, safe network operating environment.”

We recommended third-party solutions for network auditing, DDoS mitigation, phishing, and more.

Why: Keep Network Working Before, During, and After Attacks

Major events attract cybercriminals eager to defraud guests, extort organizers, or just grab attention. Advanced security enables people and things to access the systems they need to do their jobs. It also protects the network from infections and outages that could affect guests, athletes, TV viewers, and revenues.

We followed two main design principles. First, we used the same Cisco technologies we use in our own network to protect the network before, during, and after attacks. Second, we designed the network so that devices couldn’t get to one subnet from another subnet. “An IP phone on the media reporting network couldn’t attack a phone on the scoring or reporting networks, for instance,” Dexter says. “The only way a device could connect to a subnet was to go through all of its security layers, starting with Cisco ISE.”

Despite many threats, the 2016 Rio Olympics network never went down. Hundreds of millions of people around the world enjoyed watching the world’s best athletes, without interruption. Behind the scenes, the Cisco network worked constantly to:

- Stop 5 million unauthorized access attempts, 21 of them serious. Gold medal to Cisco Adaptive Security Appliances (ASAs).
- Block an average of 23,000 attempted connections to malware-infected websites every day. Gold medal to the OpenDNS cloud service.
- Detect and block an average of 141,000 intrusion attempts every day. Gold medal to Cisco FirePOWER Appliances.

For More Information

Cisco IT Case Study: How Cisco IT Implemented OpenDNS.

To read additional Cisco IT case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

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.

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.**