

Airport Seals off Sensitive Information to Protect Passengers

Cleveland Hopkins International relies on security solutions to defend against internal and external threats and help ensure flight safety.

EXECUTIVE SUMMARY

Cleveland Airport System

- Industry: Transportation
- Location: Cleveland, Ohio, United States
- Number of Employees: 350

Challenge:

- Strengthen protection against internal and external threats
- Reduce IT administrative requirements
- Streamline regulatory compliance efforts

SOLUTION

- Overhauled network defenses with security, remote connectivity, and network monitoring solutions

Results:

- Achieved stronger defenses and more rapid incident response
- Reduced administrative and compliance burden
- Saved thousands of dollars annually

Challenge

Cleveland Hopkins International Airport (CLE) is one of the busiest airports in the United States, serving more than 11.4 million passengers in 2007. With the IP infrastructure supporting airport-wide voice and business applications, emergency communications systems, airspace tracking systems, and applications that report on runway ice and snow conditions, passenger safety often directly depends on maintaining a stable and available network.

“All of these applications are mission-critical for us, even basic Internet connectivity,” says Mark Hogan, chief information officer of Cleveland Airport System, the department of the City of Cleveland that operates CLE and a second smaller airport in the region. “Almost all of the weather information that

we get is Internet-based. If our connectivity were to go down during a snow event, it would be paralyzing.”

As with any airport, CLE could also pose an attractive target for terrorists or criminals, so the airport’s physical security network requires the strongest defenses as well.

“The access control systems, the system handling the airfield gates, the systems that make security badges; all of those could be very useful to someone intending to do harm,” says Hogan. “Even on our administrative network, we keep extremely sensitive information regarding our facilities, so we can’t take chances with network security.”

The IT team had successfully protected the airport for many years, but by 2008, the time had come for a security upgrade. Hogan wanted to add new firewall and intrusion prevention capabilities, reduce administrative requirements (particularly for supporting remote users), and implement more comprehensive network security monitoring.

“We had some network monitoring, but it was not an automated or systematic solution,” he says. “If I wanted to know if something had been blocked, I had to scour through device logs.”

The team also wanted to simplify regulatory compliance and reporting processes. With emergency rescue operations onsite, the airport must meet Health Insurance Portability and Accountability Act (HIPAA) security guidelines, and Hogan anticipates other regulatory demands in the future. Cleveland Airport System was also beginning to offer fee-based network and IP phone services to airport tenants, which would pose even greater security challenges.

“Over the next year and a half, I anticipate adding as many as 60 different outside parties to our network infrastructure,” says Hogan. “We’re very concerned about unauthorized access from an internal resource, and we can no longer assume that everyone on the network is one of our employees.”

“There is no doubt in my mind that we have a greatly enhanced security posture as a result of our Cisco products.”

--Mark Hogan, Chief Information Officer, Cleveland Airport System

Solution

CLE had relied on Cisco® routing, switching, Unified Communications, and security solutions for many years. After considering several options, the organization’s leaders chose Cisco once again to support the airport’s mission-critical security and high-availability requirements.

“I have the highest confidence in the reliability of Cisco devices,” says Hogan. “We have a Cisco Catalyst® core switch that we just upgraded that ran for nine years without a single incident. Across the board, that’s been my experience with Cisco.”

The Cleveland Airport System team began with the network perimeter and the points where the administrative and physical security networks overlapped, replacing the existing Cisco PIX® firewalls with Cisco ASA 5500 Series Adaptive Security Appliances. “The Cisco ASA 5500 Series provide a lot more flexibility to lock down those connections, and the new user interface is very easy to manage” says Hogan.

In a complex environment like CLE, the ability to visually see how access control rules are operating makes it much easier for Hogan’s team to safeguard sensitive resources.

“I can’t overemphasize the ease-of-use factor in our decision to go with the Cisco ASA 5500 Series,” says Hogan. “It’s nice to be a certified network engineer and know when you’re looking at command line code that it does what you think it does. But when you can actually watch a packet move through a diagram and visually see where it’s stopped or let through, it gives you an immediate sense of security.”

The Cisco ASA 5500 Series’ built-in support for secure virtual private network (VPN) connectivity was also compelling. The ASA supports both the traditional IP Security (IPsec) connections that the airport had used in the past, as well as more flexible Secure Sockets Layer (SSL) tunnels.

To lock down access among internal users, the IT team segments the network into dozens of virtual LANs (VLANs), making it nearly impossible for users to reach any area of the network for which they are not authorized. The organization uses Cisco Catalyst 6500 Series Firewall Services Modules (FWSMs) in the core network switches to control and protect all of those VLANs.

The Cleveland Airport System team also deployed a Cisco IPS 4200 Series Intrusion Prevention System (IPS) appliance to provide an additional layer of protection against malicious threats. To serve as the intelligent core for all of these new security capabilities, the team implemented the Cisco Security Monitoring, Analysis, and Response System (MARS). Continuously gathering data from all Cisco solutions in the network, the Cisco Security MARS provides real-time visibility into the environment.

"The Cisco IPS solution, with its constant attack signature updates, gives us an automated response to any kind of internal or external threat," says Hogan. "In conjunction with the Cisco Security MARS, we gain the ability to quickly identify and respond to any suspicious activity."

"At Cleveland Airport System's two major satellite locations (the smaller Cleveland Burke Lakefront Airport and a data center in City Hall), security is just as critical as security at Cleveland International. The IT team relies on Cisco IOS® Software security features in Cisco Integrated Services routers. The integrated defense capabilities provide strong firewall and intrusion prevention services to protect voice and data services at these locations, allowing them to take full advantage of their existing network infrastructure without deploying additional hardware.

Results

Today, the Cleveland Airport System IT team is more confident than ever before that passengers and sensitive resources are well protected from internal and external threats. The new intrusion prevention and monitoring capabilities in particular have made a huge difference.

"In the past, we were relying on network administrators to check traffic stats and utilization graphs across the network to detect problems," says Hogan. "That requires a significant manual effort, but it also means that identifying potential problems is somewhat subjective. Now, our Cisco IPS solution literally goes through every single packet in the network and alerts us to any issues. That real-time monitoring and alerting capability is far more extensive than what we had previously."

When a problem is discovered, the Cisco Security MARS solution helps the IT team diagnose and resolve the issue much more quickly.

"We can not only see that a potential problem has popped up, we can easily trace it through the topology of the network and identify the source," says Hogan. "Just being able to see that visually saves a considerable amount of time in determining whether something is a real problem or a false positive. The Cisco Security MARS also has a wide array of pre-built reports that help us rapidly assess incidents without having to pore through lines and lines of log files."

The new Cisco security solutions are also allowing the IT team to operate more efficiently. For example, thanks to the streamlined administration of the Cisco ASA 5500 Series, when the administrator responsible for managing perimeter security devices changed jobs, no replacement was needed. Instead, an existing employee took on those responsibilities, eliminating the need to hire a new full-time engineer at a cost of approximately US\$100,000 annually.

The new SSL VPN capabilities have also provided a huge cost savings simply by eliminating the need to manually install and configure VPN clients on each remote user's machine.

"Before, we were looking at two to three hours of travel and installation time for each VPN client," says Hogan. "Now, we can just connect users remotely through our web portal. That saves us several hours for every user and hundreds of thousands of dollars over the life of the product."

The ability to view and manage the entire infrastructure with Cisco Security MARS is also streamlining regulatory compliance and reporting—both for current needs and for expected future requirements.

“If there were a security incident, the Department of Homeland Security would expect us to be able to demonstrate that a breach had not occurred in our environment. Cisco Security MARS would be hugely beneficial in doing that because of the ease with which we can document how traffic has moved through our network.”

Ultimately, the Cisco security solutions are helping the IT team fulfill its most important requirement: protecting the thousands of passengers who fly in and out of Cleveland Hopkins International Airport every day.

“There is no doubt in my mind that we have a greatly enhanced security posture as a result of our Cisco products,” says Hogan.

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 6500 Series Switch
- Cisco 2600 and 2800 Series Integrated Services Router

Security and VPN

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco IPS 4200 Series Sensor
- Cisco Catalyst 6500 Series Firewall Services Module
- Cisco Security Monitoring, Analysis & Response System

Unified Communications

- Cisco Unified Communications Manager
- Cisco Unity®
- Cisco Unified IP Phones 7900 Series

Next Steps

In the coming months, the Cleveland Airport System IT team is planning to better integrate its Cisco management products and increase automation of security monitoring and alerting. The team may also investigate converting to Cisco Network Admission Control (NAC). This additional layer of protection will further safeguard airport resources by helping ensure that all devices accessing the network are in compliance with organizational security policies (such as having up-to-date antivirus and operating system software) before gaining access.

For More Information

To find out more about Cisco security solutions, visit <http://www.cisco.com/go/security>.



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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)