How Cisco IT Controls Building Security over the Enterprise WAN

Centrally managed IP-based building security system saves costs and improves safety and responsiveness.

Cisco IT Case Study / Security and VPN / Enterprise Network Building Security: This case study describes how and why Cisco Systems transitioned from standalone access control systems to an IP networked system to help secure its business facilities. Cisco's global security network is a leading-edge enterprise environment and one of the largest and most complex in the world. Cisco customers can draw on our real-world experience in this area to help support similar enterprise needs.

"Cisco safety and security operations personnel monitor and provide response to alarm events at all facilities worldwide. By standardizing on one global access-control and intrusion detection system and by networking these systems, we've been able to centrally manage access and alarm monitoring for more than 46,000 employees and contractors, in 271 sites, and more than 50 countries globally."

– Bill Jacobs, corporate Security, Technology & Systems manager

BACKGROUND

Enterprise Access Control

At Cisco Systems®, the corporate Security, Technology & Systems (STS) team manages physical security for more than 271 Cisco® facilities in 50 countries worldwide. Their job is to make sure that only people authorized to have access to these Cisco facilities gain entry, and to detect and respond to all unauthorized entries. Securely and cost-effectively controlling this access across the global enterprise is one of the primary challenges for the Cisco.

Based on the size and risk level of a facility, Cisco deploys security technologies such as intrusion detection and physical electronic security-access-control systems, including closed-circuit TV (CCTV), for surveillance. These technologies include:

- Lock and key systems for doors, offices, desks, and cabinets
- Badge readers in front of doors or labs or locked storage rooms, and sometimes even elevators
- Video cameras at front of entry and perimeter exit doors, elevators, and other strategic locations
- Door-latch sensors and controls, motion detectors, glass-break detectors, and other sensors (including fire and smoke detectors)

Together, these technologies help Cisco provide intrusion detection and physical access control. The information they gather is transmitted to centralized security operations centers, where it is reviewed and responded to by the STS department.

History of Physical-Security Issues in Cisco

Several years ago, Cisco began addressing how to resolve the following physical-security-management problems:

- Providing one access card for all needs (building entry, lab entry) that is unique to each user, and still administer general access to a global user population of more than 46,000 badged employees and contractors

- Managing a physical-security-system program in 50 countries worldwide, with limited resources
- Managing global integration and service and support issues for all these disparate systems

In 1997 traditional models of security management were in place. “There were no network-based access control systems then,” says Bill Jacobs, Corporate Security, Technology & Systems manager. “Access control was a standalone function at every single facility. Each site was likely to have its own security system, and we sometimes had different systems at different sites.” This approach had several disadvantages. For example, employees traveling to different sites experienced difficulty because their badge (which they used to gain entry into their regular work facility) wouldn’t work at other sites until it was manually programmed into the local badge authorization database. Also, for Cisco to remotely monitor the electronic sensors used at other sites, the STS team had to lease individual (and expensive) phone or leased lines to carry the signal back to the main security operations center.

Lack of connectivity also limited video surveillance cameras to recording information for later examination, rather than alerting Cisco during a security breach. Surveillance cameras sent their signals into banks of videotape recorders; tapes were kept for 30 days then reused. Because security systems were isolated from one another, a dedicated site administration manager was required at each facility (although not always on a full-time basis).

At that time, security systems were deployed with minimal or no managerial oversight and, with the exception of two main U.S. campuses, remote monitoring capabilities were nonexistent. Badge-reader access systems were installed to secure facilities and to serve as a convenience feature for employees. After a system was installed, facility administrators were required to administer disparate system databases (usually on a PC with special software managing the access-control systems at that site) with no corporate consistency. Maintaining all these technical systems and databases required a variety of skills, most of which were outside the expertise of security personnel. Security staff was also burdened with managing service- and system-integration support.

Employees in the Cisco STS department conducted a study to determine which physical-site-security solution would best fit Cisco corporate growth, management, and logistical needs. They needed a system to provide on-demand, real-time information from any alarm system at any location worldwide. They also needed skilled equipment-maintenance people at every location to support the system, and skilled database systems administrators (DBAs) to support database systems. This would allow the STS staff to focus on maintaining a safe and secure environment, protecting Cisco employees and physical assets.

CHALLENGE

The Cisco STS department faced the following challenges:

Defining and developing a corporate physical-security philosophy. After meeting with executive staff members, a philosophy was defined, which included a primary goal of providing 24-hour access to all Cisco employees. This enabled mobility and higher levels of employee productivity, making it easier for employees to work any time of the day or night while still maintaining physical security. Contractors, vendors, and other temporary workers were restricted depending on location or time of day.

Defining and developing a corporate physical-security design standard. This standard was to be developed based on the corporate culture and, as always, a balance between culture, practical security applications, and costs. “The Cisco culture is based on an environment of trust,” says Jacobs. “We expect that our employees will be responsible for Cisco assets, and take the right steps to make sure that facility security is enforced. It is a culture of trust and employee empowerment, and we had to make sure that our security standard took that culture into account. At the same time, we had to make sure that this didn’t impair our ability to maintain a secure work environment, and our ability to keep costs, and losses, to a minimum.”

The agreed-upon security standard was implemented globally and communicated through the facilities organization to the general contractors and integrators. Details rarely varied, but the three individual regions (Americas International; Europe, Middle East, and Africa [EMEA]; and Asia Pacific and Japan) had influence in the change-

management process.

Cisco was pioneering the vision of enterprises using the power of IP networks to provide a standard set of services to everyone in the company independent of location. Cisco STS wanted to develop an enterprisewide security system with centralized management, whereby data distribution and reconciliation would take place in regional security servers.

The plan was to use the corporate IP WAN to reduce networking costs, and to minimally impact the rest of the corporate traffic. Although a worthy goal, it was a new industry concept that had not been developed as of late 1997. “You could go out and buy an access control system for any facility around the globe,” says Jacobs. “But each system had its own separate database that had to be managed separately. We wanted to be able to query each system from a central site, and manage them all from a single point of control to reduce our management overhead. We wanted to get out of the business of managing 150 separate controllers; we wanted to manage everything from one site, with one group of people. We ended up with three systems in three global theaters, which we can manage from a single PC anywhere on the network.”

Building a global systems-integration support model. This was the most challenging issue and remains the most difficult to manage today, because numerous complex systems in various locations worldwide must be supported. The technology is new and somewhat complex, and there are few companies that have the global presence and technical skill needed to support and maintain the equipment. Cisco STS worked with global systems integrators to implement a global support model, and found single strategic integrators in each region to manage the solution. Cisco STS also used the current staff of Cisco IT database administrators to monitor and maintain the centralized database servers after they were consolidated into central Cisco data centers.

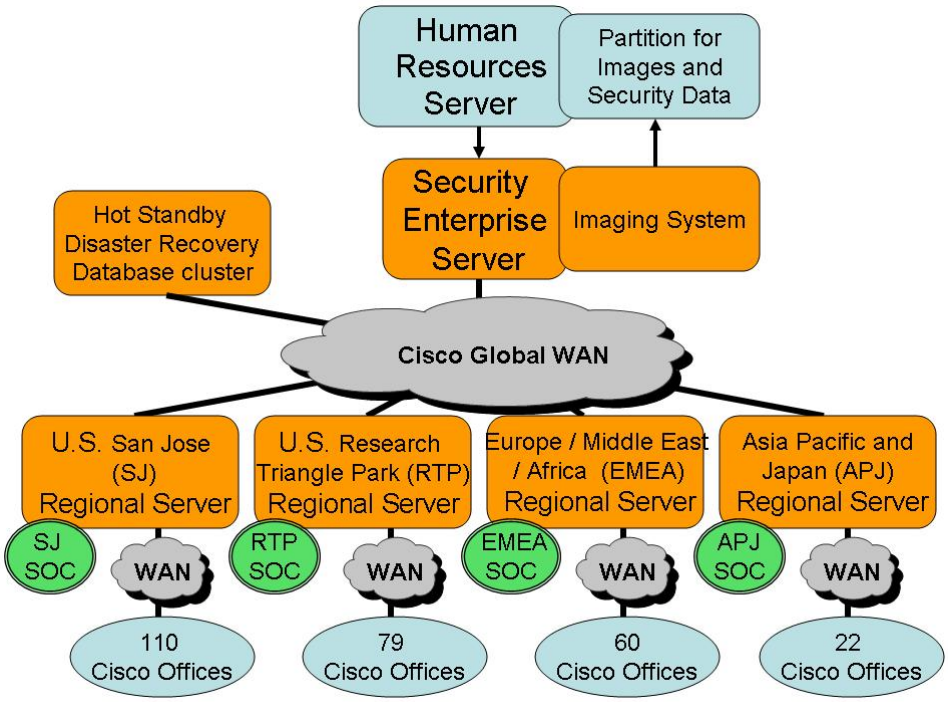
SOLUTION

Centralized Server Architecture and WAN

Cisco STS developed a centralized server architecture based on a single set of equipment standards, supported by regional security servers worldwide. These centralized servers were located in data centers that Cisco IT supports and connected to the Cisco human resources servers. Using the existing Cisco IP WAN, the centralized servers are linked to each other and to each access control system at each of the almost 300 Cisco sites worldwide. Cisco IT required that the servers meet server and OS standards, which initially created extra work for the STS team. The advantage to IT is that it is easier to manage a limited set of standard servers. The advantage to the security and safety department is that it is no longer responsible for managing and maintaining its servers and software patches and updates. The department can now concentrate on its primary security issues.

Cisco also standardized the access-control and alarm systems at every site, and supports them with a single set of software tools. These standard systems are maintained by a global software and services vendor that provides technology compatible with the current security database system, and installs and supports the systems globally at a competitive price. Together, Cisco STS and the vendor developed the first true enterprise system solution. Figure 1 shows the architecture of this security system.

Figure 1. Present Day Cisco Enterprise Security System

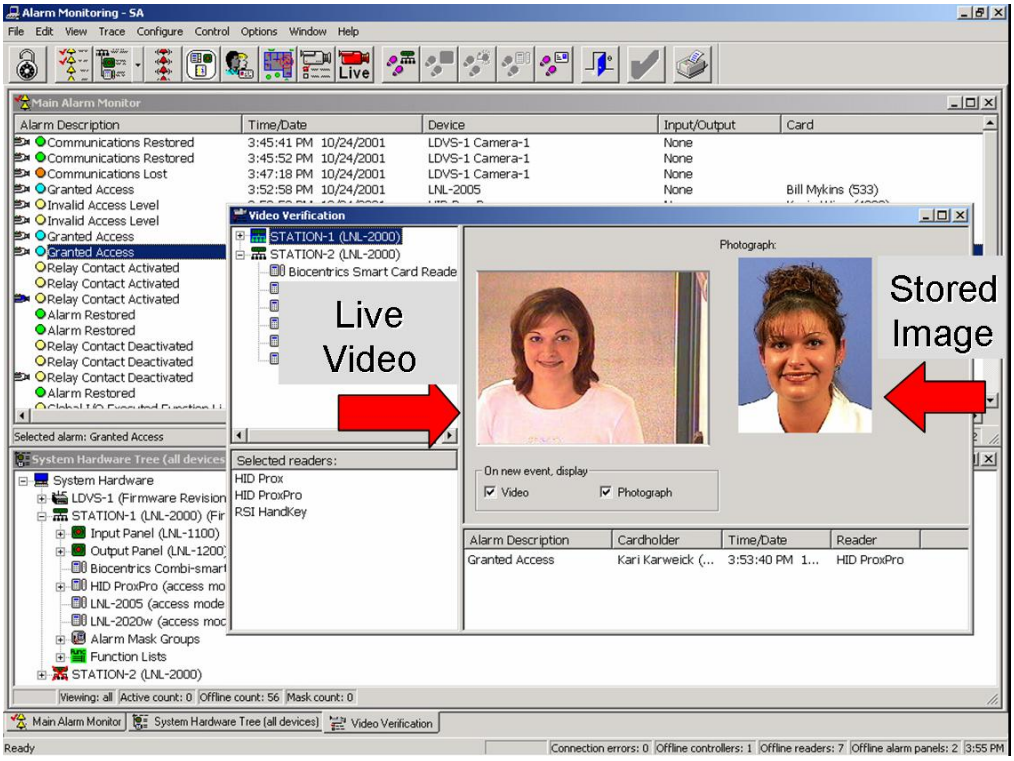


Database administration occurs at region-centric administration points and data records are reconciled and updated between all the servers on a preset schedule.

Cisco has a database of all its employee records that is updated when an employee joins or leaves Cisco. After a background check, new employees are added to the database, and go to the local Cisco security office to obtain a badge with their picture on it. Badges are unique to each employee, and can be used only at Cisco locations. Not only is the employee's picture on the badge, but the embedded badge number is used to identify the employee every time the badge is used to open a door. The picture is copied from the regional security server to the global enterprise system, and also copied to the employee directory where it is available to all employees.

Access to company resources is determined by an employee profile, which is assigned automatically based on the person's employee status and geography and then customized according to individual job needs. Some engineers, for example, need access to special labs, whereas IT personnel need access to wiring closets. Because everyone has access to the employee database, building staff can compare the picture in the database with the employee in front of them if the employee has a lost or misplaced badge and needs building access. And because security personnel have access to this database and to IP video streams, they can view a video stream and compare a person on camera to the pictures of people who are authorized to be at that location (Figure 2).

Figure 2. Comparing Employee Picture to a Video Camera Output



This global enterprise system replicates all employee data to each of the regional servers, making each employee's badge a "global" badge. Any employee can go to a Cisco building anywhere in the world to work, without badge updates. This convenience saves time and makes Cisco a more comfortable environment for traveling global employees.

Security Operations Centers

Security operations centers are the focal points for alarm management and response programs (Figure 3). All incident or event information is sent automatically from each office to the regional server and from there to the central server. All fire alarms, glass-break alarms, door-opening alerts, in all about 60 to 80 monitor points per Cisco building, are sent to the regional and global Security Operations Center (SOC). The SOC security personnel can log on to the closed-circuit video camera near an area in question and determine whether they should call the local private security patrol or the local police to manage an incident. Many alarms are "false alarms," for example, a secure door being held open by an employee, the wind, or a faulty door latch. Because the SOC can view each event in real time using CCTV cameras over the corporate IP network, the number of false alarms that Cisco and the local police have had to respond to has significantly reduced. This benefit, coupled with the professionalism and skill of the SOC personnel, has helped to maintain credibility and good relationships with local police departments worldwide.

Figure 3. Present-Day Security Operations Center

The SOC also acts as a central emergency call center for Cisco employees. All emergency calls are routed to the nearest SOC personnel, who know where the call is coming from and are trained to respond immediately in an emergency. They alert the appropriate local emergency-response team and direct these teams to the emergency.

Outsourcing Systems Integration

Centralizing systems installation and support functions, just as centralizing database structure, saves the Cisco STS team money and time.

The enterprise access-control systems are composed of numerous physical and software components. The Cisco team needs to maintain more than 6600 proximity badge readers at building and lab entrances and special secure room entrances (Figure 4). More than 2600 closed-circuit cameras in building and parking lot locations stream video to networked video recorders or across the WAN. Thousands of access-controlled doors signal when they are opened or closed; thousands of smoke and fire alarms, glass-breakage alarms, motion detectors, etc. all need to be maintained, and installed in new offices. These access-control systems all connect into more than 500 building alarm access panels. Doors and cameras, in particular, need occasional maintenance.

Figure 4. Proximity Badge Reader

Finding a single systems integrator was critical to reducing the costs associated with managing complex multiple business relationships and contracts and working procedures. Having a single point of contact also allows Cisco to manage a single security standard.

The security group wanted a single global systems integrator to centrally manage and maintain all its access-control systems but could not find one. Instead, Cisco developed two separate support models. In the United States, Cisco employs one nationwide systems integrator. In the Asia-Pacific and EMEA regions, it employs another integrator. This allows managerial efficiencies in the form of single points of contact for each major integration component: program management, project management, and service coordination.

In the United States a single integrator supports regional offices throughout the country. Local offices of the systems integrator's parent company perform installations and service. In EMEA a different integration model was developed due to the lack of pan-European systems integrators at the time. In this model, Cisco works with a security systems integrator in Australia. In that region this systems integrator worked with Cisco to understand its standards and requirements, and it became the single point of contact in that part of the world. The systems integrator subcontracted work to best-in-class systems companies in specific geographic regions. This worked so well for Cisco that it encouraged that company to follow the same model in EMEA, which it did. The company located and worked with excellent local systems providers (LSPs) in the United Kingdom, France, Belgium, Netherlands, and Germany, and developed ways to make sure that Cisco security quality specifications were met in the same way in all regions throughout Europe. The primary systems integration company became the single point of contact as in the U.S. model for program management, project management, and service coordination. What differed was the requirement for them to collaborate with LSPs. Here the management company qualified LSPs, whose expertise was based within their country of origin. Problems such as language barriers, local code issues, and billing in local currency were eliminated. The systems integration company also built a contingency plan for Cisco. Should the management company change, after the model was built and tested, the LSPs could perform independently.

What made this centralization of access-control systems management successful was the ability to document requirements and procedures in detail, and the integrator's ability to locate and work with best-in-class LSPs to meet Cisco standards.

RESULTS

From 1997 to 2004, Cisco has tripled in size, growing from 10,700 to more than 35,000 employees, and more than doubled the number of locations. In that time the STS team has remained about the same size mostly because of the efficiencies gained from automating many of its access-control systems, centralizing its management, and

outsourcing the maintenance of these systems to trusted partners. The primary access-control system is globally managed by an in-house staff of four. This efficiency has also produced a highly reliable service model. The access-control servers have an uptime average of 99.97 percent. And the STS team has been able to use the capabilities of the corporate IP WAN to centralize its management of access-control systems, and to see and control all its global systems from a single location.

This integrated system allows the STS team to immediately add or remove people from its database, or update their permissions, and have that information spread to all its locations around the world in a matter of minutes. This global model allows employees to travel and work at any location without needing to get checked in at each site first.

Using the corporate WAN for low-bandwidth alarm information saves Cisco the cost of separate dial-up or data lines; and the WAN is sufficiently large to carry the necessary IP video information whenever the SOC personnel need to see what is happening at any local site, without requiring separate data lines for video. Migrating to network-based digital video also eliminated the need to visit each building to replace and store tapes, and gives the SOC live, real-time information about local events and alarms.

Outsourcing maintenance of Cisco security servers to IT keeps the servers well managed and up-to-date. It eliminates concern about servers being compromised by viruses or outages. And outsourcing the maintenance of local systems at more than 300 locations worldwide allows Cisco to keep its security staff small, and still maintain high security standards, even in locations where operations are difficult.

Because these high standards and clear processes create a strong sense of professionalism, and because its IP video camera system allows the security team to double-check alarm conditions at remote sites, the security team has established good and trusted working relationships with private security and police groups at regional sites. This is extremely valuable to Cisco in effectively protecting its employees and business assets at every Cisco location.

“The goal of a security program in any corporation is to protect employees and assets,” says Jacobs. “Back in 1997 there was no such thing as an enterprise access-control system. If we had wanted to provide a similar level of access-control security today, without our enterprise access-control system, to all of our more than 300 locations, it would cost us several million dollars more than we spend today for security. We would need to put a security officer in each lobby, with a video-monitoring terminal to view the cameras, and a PC to access the alarm systems. This officer would also probably be the event responder—dealing with open doors, alarms, and so on. In the evening the officers would all go home, after turning on the remote alarm system. Alarms would now be received over phone lines to a security service that would send out private patrols or call police in just the way our SOC does today. We would need to have a database administrator at many sites doing part-time work to manage our employee records.”

“We’ve saved Cisco millions of dollars by eliminating the 300 security officers, and by monitoring everything worldwide using three people working from each region’s centralized SOC. Our employee records database is now just one of several databases being managed in a standardized server cluster in Cisco IT’s data center. By centralizing, automating, and using the IP network, we have consolidated several hundred jobs into just a few, and provided very high-quality security and safety services for Cisco.”

NEXT STEPS

The STS department is monitoring the evolution of IP-based security applications. Its vision is to develop IP card readers and IP door-control modules that are appliances connected to the local IP network. Traditional access-control panels may be replaced with software controls, which will help reduce costs and improve reliability.

The STS department is also exploring the possibility of linking local police departments to its closed-circuit video systems over the Internet, to allow them to view each site before they send officers into an unknown situation. This capability also will benefit other security-monitoring groups, allowing them to reduce the number of false alarms.

Wireless technology will play a role in all solutions in the future. Cisco is currently running a pilot program where a patrol vehicle is equipped with a wireless tablet PC running its security management and video applications. Alarm events and video are transmitted securely using IP Security (IPSec) over 802.11g “hotspots” at all Cisco locations. Mobile security patrols will become mobile command centers, accessing all alarm information and able to access video camera streams as needed.

As more applications become known, smartcard technology is being considered. Smartcards can store more information than badges about each employee. “This could allow us to use biometrics readers, keeping individuals’ biometric information on their card instead of in our databases,” says Deon Chatterton, STS . program manager. “Smartcards could also contain information about medical needs, or could be used as Cisco credit cards in our employee cafeterias.”

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

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.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**