Insurance Company Deploys In-depth Network Defense

EXECUTIVE SUMMARY

CIGNA Corporation

- Philadelphia, Pennsylvania, United States
- 28,000 employees worldwide

Business Challenge

- Strengthen security while simultaneously enabling access for customers and partners to just the information they require. Protecting EPHI data during network transmission and strengthening network security controls are primary objectives.
- Phase out obsolete technology, improve operational efficiencies and increase availability.
- Enable future business application and network services to be delivered over the network, such as voice and video

Network Solution

- Implemented Routed Access architecture to support network segmentation
- Updated network foundation to support new services

Business Results

- Deliver significant competitive advantage with in-depth security defense
- Enable IT to isolate network threats before they enter the core network
- Support separation of applications, data, and users

CIGNA Corporation uses a Cisco Routed Access solution for enabling innovative security controls and improving manageability.

BUSINESS CHALLENGE

CIGNA Corporation provides employee benefits plans for organizations and offers health care, and disability and life insurance coverage products and services in 30 countries. The company relies heavily on its network to provide access to information for members, members' employees, care providers, and business partners. With the high volume of privileged information that it maintains, CIGNA must comply with Health Insurance Portability and Accountability Act regulations that govern information privacy, as well as with Sarbanes-Oxley requirements. And like many large organizations, CIGNA faces an ongoing barrage of viruses, worms, and other threats to its network and information assets.

"We wanted to deploy in-depth security defenses, but our legacy network infrastructure made it extremely difficult to deploy and manage the security measures that we wanted while allowing us to easily add new business and network services in the future," says Michael McKenna, Director of Information Protection for CIGNA.

After performing an extensive network assessment, CIGNA developed a list of requirements for its new infrastructure. It had to be able to provide secure guest access privileges for consultants and vendors, as well as secure zones and remediation LANs to minimize the impact of viruses and other threats. The network had to be hardened to add a network layer of security control, support logging and auditing capabilities for meeting compliance requirements. Future plans called for delivering voice and video over the network and adopting Multiprotocol Label Switching. Based on these requirements, CIGNA developed a new network architecture and identified specific solutions that would meet the company's current and projected needs.

"We have been a Cisco customer for many years and decided to evolve our network to meet our new requirements," says Craig Shumard, chief security officer for CIGNA. "Interoperability and manageability were important, especially with the security strategy that we planned to adopt. We chose Cisco solutions again."

NETWORK SOLUTION

The new network architecture was designed to support CIGNA's innovative security approach. CIGNA identified multiple levels of risk associated with various applications, data sources, and user groups and then segmented access to these resources based on the associated risk profile. Appropriate security controls are then added to specific applications, data, and users.

Data is further classified into categories, each with a unique risk profile. Highly sensitive data includes financial-reporting or business-planning information. Restricted data includes member data. Proprietary data contains internal documents, and public data is everything that can be posted on the company's public Website. Within each category, additional controls are implemented.

Each application may require data from multiple sources with differing risk levels, so existing applications are being converted to Service Oriented Architecture (SOA). Using a SOA application approach will enable CIGNA to deploy fine-grained security controls to its infrastructure, applications, data, and users and extend these controls across the entire enterprise.

To support this segmented approach, CIGNA chose to implement a Cisco® Routed Access solution using the Open Shortest Path First (OSPF) routing protocol in its wiring closets. Routed Access distributes network intelligence to the network edge, allowing CIGNA to extend multiple security layers and defenses to the point where users first enter the network.

"It made more sense to immediately authenticate the user certificate at the edge switch prior to even enabling the port, rather than waiting until a potential threat hits the core network," says John Balzano, senior director of Infrastructure Delivery Services for CIGNA. "For example, if a user has a virus on his or her PC and plugs into our network, it can be caught at the network edge, denied access to production network and isolated to a security zone for remediation before affecting core business processes."

CIGNA will use Cisco Catalyst® 3750 Series Switches in closets and branch offices to implement its Routed Access solution. In these locations, the solution can also be used to route traffic between multiple separate Virtual LANs (VLANs). For example, guest visitors can be authenticated and placed on a VLAN separate from CIGNA employee users. With routing capabilities at the closet, CIGNA can provide guest users with filtered Internet access for retrieving email from their home networks and limited network services while never gaining visibility or access to CIGNA applications. Internal users can be segmented on separate VLANs, yet still take advantage of collaborative applications through the Routed Access solution. Because the network employs Routed Access in the closets, traffic is load balanced across the network more effectively, which contributes to increased network resiliency.

"The functionality of our Cisco products allows us to implement a segmented network and application architecture efficiently," says McKenna. "The infrastructure will be all new and sized appropriately, so it will deliver the high availability, scalability, and management capabilities that are integral to our design."

Today CIGNA locations are connected through a Frame Relay service and point-to-point connections. Depending on each branch office's size and function, it will receive a Cisco Catalyst 6500 Series or 3750 Series Switch, Cisco Integrated Services Router with a security pack, and a variety of servers. VPNs are used to provide access for doctors, care providers, member employers, and hospitals through externally facing portals.

> **"The new network enables us to minimize the number of steps that any user can take into the network to get what they absolutely need. The fewer the steps, the less risk to the network and to the company. At the same time, we gain high manageability and the ability to deploy future functionality."**
> **—Craig Shumard, Chief Security Officer for CIGNA**

BUSINESS RESULTS

The new network will give CIGNA the ability to quickly isolate viruses and threats—even down to a specific building or floor—and prevent them from affecting other parts of the network or locations. With Routed Access deployed at the network edge, CIGNA can provide guests with convenient access while eliminating the need to install external broadband connections—which represent risky "back doors" to the network.

By using a common protocol like OSPF, the Routed Access solution also simplifies network management and troubleshooting, because fewer tools are required and the network is less complex. As CIGNA adds new services, such as voice and video, the Routed Access solution will allow them to easily scale enterprisewide.

"Much of what we are doing today is enabling new technology," says Shumard. "With the new network, we can deploy appropriate controls, based on risk, and build a whole security framework around that. Highly sensitive data cost more to protect, so with the ability to put the right security around the right data, ultimately, we will improve control and reduce its cost."

The new architecture also makes it easier for CIGNA to prove that the company meets the appropriate regulatory requirements and demonstrate to customers that their information is safe. CIGNA customers actually audit CIGNA's network, so the ability to prove compliance, document security, and demonstrate high availability is a significant competitive advantage for the company. With the segmented network approach and risk-based security controls in place, CIGNA expects to significantly enhance its information offerings to members, allowing them to ultimately gain more control over their healthcare.

NEXT STEPS

CIGNA expects the new infrastructure to be completed by the end of 2007. As vital core infrastructure is deployed, branch offices will be upgraded as well—approximately 28 locations are expected to be upgraded by the end of 2006, with the remaining 117 completed in 2007.

"The new network enables us to minimize the number of steps that users can take into the network to get what they absolutely need," says Shumard. "The fewer the steps, the less risk to the network and to the company. At the same time, we gain high manageability and the ability to deploy future functionality. With those three pieces, it really made sense to do it the right way."

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 6500 Series Switches
- Cisco Catalyst 3750 Series Switches
- Cisco 3800 Series Integrated Services Routers HSEC Bundle

Security and VPN

- Cisco IDS Services Module for Cisco Catalyst 6500
- Cisco PIX® Security Appliances

FOR MORE INFORMATION

To find out more about Cisco Solutions and Services, visit: http://www.cisco.com

To learn more about Cisco Security and VPN Solutions, visit: http://www.cisco.com/go/security

To learn more about CIGNA HealthCare, visit: http://www.cigna.com

This customer story is based on information provided by CIGNA HealthCare, and describes how that particular organization benefits from the deployment of Cisco 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.

Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA CXX-XXXXXX-XX 10/06