Cisco Public.

VIRTUAL PRIVATE NETWORKS (VPN)

Cisco on Cisco E-Learning Series - Executive Track

TRANSCRIPT

INTRODUCTION

Helping employees work productively anytime, anywhere is a necessity in many organizations. Offering secure remote access to corporate intranets is an important solution for meeting this objective.

Cisco's global VPN serves more than 11,000 concurrent users. With remote access to corporate data, applications, and voice services, Cisco employees can work with greater convenience and efficiency, anytime, anywhere.

Welcome to the VPN Executive Module part of the Cisco on Cisco Learning Zone E-Learning Series initiative. The Learning Zone is a complete program of training from Cisco IT, aiming to empower employees, at a number of proficiency levels, to be well versed in Cisco on Cisco.

My name is Sanjay Pol, VP of advanced security services, and I'll be talking with you for the next few minutes about the role of VPNs within Cisco Systems today. This module aims to outline an executive overview of the deployment, the benefits, where we are today, and what the future holds.

The program intends to help build sales lead generation, offer customers best practices they can implement in their own network, and build confidence in Cisco solutions—and the company—as the leading expert.

LEARNING OBJECTIVES

By watching this program, you will:

- Learn about Cisco's worldwide VPN deployment and its benefits to employees and the company.
- See how VPN access is delivered and secured in an employee's home.
- Understand how remote network access and VPNs have evolved at Cisco.

AGENDA

Here's our agenda for this program:

- We'll begin by describing how Cisco implements VPN access.
- Next, we'll look at the concept of the networked home for employees.
- We'll discuss the importance of security in a VPN.
- Then, we'll review the past and future of VPN capabilities implemented by Cisco.
- And, we'll conclude with a brief look at the benefits Cisco obtains from its VPN.

VPN ACCESS AT CISCO

We'll begin by describing how Cisco has implemented its virtual private network.

One goal of Cisco IT is to support secure and reliable network access for Cisco employees wherever they are located: in the office, on the Cisco campus, at home, or when traveling. Wired and wireless connectivity are critical to this access. But also important is a secure virtual private network or VPN. With a VPN, an employee can remotely access Cisco's internal network over a secure Internet connection. Cisco VPN clients are installed on employee laptop computers. Every laptop is a portable office, with a VPN client, wireless connection software, Cisco IP Communicator software for phone calls, a Web browser, and access to Cisco's voice, voicemail, and data applications. Wherever an employee can connect the laptop computer to the Internet, they can communicate and work productively.

Cisco employees are encouraged to find the best possible Internet access for their homes, whether cable, DSL, ISDN, or another method. Within a reasonable price limit, employees are allowed to charge back this expense to Cisco. This encourages telecommuters and after-hours work by employees at home.

Cisco uses its own products to deploy a secure, scalable, and global VPN. A core product is the Cisco VPN 3000 Series Concentrator, which is deployed in 13 locations around the world. Today, these concentrators support 11,000 concurrent VPN connections that are made by employees and selected suppliers and partners.

EXECUTIVE SUMMARY

VPN access is made through both software and hardware clients.

Cisco employees use the VPN software client to access the Cisco intranet securely over any Internet connection. Because this client works in both Windows and Linux environments, it also gives certain partners secure, yet controlled access to certain Cisco business applications. By using the VPN, Cisco can connect new partners much more quickly and at a lower cost than leasing a Frame Relay or TDM link.

Cisco IT also supports the Cisco 831 router as the standard hardware VPN client. Deployed primarily in employee homes, the VPN router supports Dynamic Multipoint VPN and security features such as the Cisco IOS Software firewall, an intrusion detection system, and network admission control. The router is ordered and shipped to the employee, who then connects it to the Internet and authenticates the connection to the Cisco network. The router's configuration is then pushed over a VPN tunnel, which makes it simple for employees to install the router and eliminates any IT configuration or setup. From a central location, Cisco IT can monitor, manage, and automatically push image updates to each of these remote routers.

VPN ACCESS POINTS

This map shows Cisco's VPN access and concentration points around the world.

Before 2000, Cisco IT installed VPN concentrators only at Internet gateways located at our major data centers in San Jose, Research Triangle Park, Amsterdam, and Sydney. As more users needed remote access to the company intranet, Cisco IT added VPN concentrators at locations near large groups of engineers and salespeople. These locations included Boxborough, Massachusetts and Richardson, Texas as well as Tel Aviv, Tokyo, Bangalore, Singapore, and Hong Kong. Today, VPN concentrators are also deployed in Milan and Johannesburg.

Security at these gateway sites is critical. To protect the internal network we use Cisco PIX Security appliances and Cisco Firewall Services Modules, as well as several other layers of security.

NETWORKED HOME

Let's take a look at the products and strategies that Cisco uses to give employees remote VPN access in their homes.

Enterprise Class Telecommuter or ECT is a VPN solution based on Cisco IOS Software. It serves full-time teleworkers, employees who extend the workday at home, and for branch networking. The ECT solution connects PCs and Cisco IP phones into a home network that can be used as a secure extension of the employee's office.

Dynamic Multipoint VPN provides an efficient way to manage the secure Internet tunnels that are created by VPN users. Traditional remote access solutions require users to set up tunnels from their location to a central hub concentrator, then communicate to each other through this hub. With Dynamic Multipoint VPN, users locate each other through the hub, then establish secure encrypted tunnels directly through the Internet, bypassing the hub site. This method is a far more scalable way of building secure connections over the public Internet than traditional spoke-and-hub connections.

The Cisco router at each employee's home supports Cisco IOS firewall features and Network Based Application Recognition or NBAR, which allows Cisco IT to track application usage and flow. Network Admission Control features check the PCs to ensure they meet Cisco's latest protection standards before they are allowed to connect. The router also supports quality of service or QoS to improve voice quality on the Cisco IP phones, even when calls are carried across the Internet.

SECURING HOME ACCESS

Security is critically important in a VPN.

Cisco IT uses several strategies to ensure security for VPN access from an employee's home.

The Cisco router utilizes a standard configuration that is periodically updated from the Cisco IT central management system. A browser-based menu guides the employee through the steps for installing the router, without any oversight from Cisco IT. Installing Cisco IP phones at home offices is also "zero-touch" because it does not require any router configuration to add the new phone.

Another important strategy is employee education about security risks and practices. Employees can violate company security rules, and good sense, by actions such as connecting an unsecured wireless access point to the ECT router or allowing family members to use Cisco PCs. Education on security policies and the reasons behind them, as well as enforcement of these policies, helps employees understand their role in securing the Cisco network.

EVOLUTION OF THE CISCO VPN

Let's look at how remote network access is evolving at Cisco.

In 2001 we had a mix of modem dial-up at 56 K, ISDN at 128 K, and some users in a few U.S. areas who were using a managed DSL service. Dial-up charges in the U.S. were inexpensive, but they were very high in Europe and Asia where employees had to make international long-distance

calls to access the regional hubs.

IT management costs were also high for remote access. We needed several IT engineers to maintain the modem pools and to work with the DSL provider in supporting Cisco employees with setup and performance issues.

Because of slow performance, employees were using dial-up only to check e-mail. We found that when employees had high-speed access, they stayed connected for about 2 hours more per day. Much of that time was spent productively because the employees could use corporate applications. Also, employees with high-speed access were much happier with their online experience and felt better able to do their jobs.

Today we have migrated all Cisco employees to the VPN as their primary remote access method. Employees select the best Internet provider in their area for home service. And with wireless Internet access available in so many places, employees can work at customer sites, hotels, and coffee shops. VPN access has reduced the remote access cost per employee by over 100 percent, while vastly improving the performance of the intranet connection.

With the Cisco VPN, employees and key suppliers connect to Cisco via the Internet from around the world, around the clock. The VPN is secure and scalable, which means it can easily accommodate new employees, partners, and services as the company grows.

Employees find that working remotely can be as productive as working from the office. The Cisco 800 Series router in employee homes provides the critical security features for VPN access. The router can also support new communication capabilities such as Cisco IP phones and wireless home LANs that separate family and employee traffic.

Cisco employees are using hand-held PDA devices more often, and Cisco IT is creating methods to give them simple and secure VPN access. Cisco IT is also deploying rich media applications, both in corporate office and home settings, to enhance information access and collaboration for remote employees.

VPN SNAPSHOT

Here are a few key points to remember about Cisco's VPN deployment.

Cisco's goal is to give secure, reliable intranet access to employees whether they are in the office, at home, or traveling. To achieve this goal, Cisco supports a virtual private network as an extension of our secure internal network. Once connected through a secure VPN tunnel to the Cisco intranet, employees can access the same voice, video, and data services they use in their offices. Secure remote access is a strong enabler of employee productivity and global collaboration.

Remote access functionality has been provisioned through a worldwide deployment of VPN Concentrators at 13 locations. These concentrators are capable of supporting thousands of employees via software or hardware VPN clients. At any given time, we have over 11,000 concurrent VPN connections.

Today, Cisco's VPN delivers the benefits of low telecom per-minute and IT costs while connecting 11,000 global employees and key suppliers connect to Cisco via the Internet 24 hours a day. By using the VPN, Cisco employees maintain productivity close to in-office levels when working outside of the office. For the future, Cisco IT is working towards implementing worldwide access to rich-media information.

OUTRO

If you're viewing this program via the Internet, you'll have access to a number of resources including: subtitles, a glossary of terms and links to further information.

TAKING THE TEST FOR THIS MODULE

Thank you for watching the Virtual Private Networks Executive Module.

To accompany this module, there is a short test that will allow you to demonstrate your understanding of the topics we have covered. Successfully passing this test will allow you to be acknowledged as being familiar with the Cisco on Cisco Virtual Private Networks solution at an Executive level.

If you have completed all modules in the Security Specialist Path, and this is your final module, you will be eligible to become a Cisco on Cisco Executive Security Specialist.

If you have completed all modules in the Executive Learning Track, and this is your final module, you will be eligible to become a full Cisco on Cisco Executive Expert.

For more information on further training opportunities, please see the Cisco on Cisco Website.

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.**

Printed in USA C78-331727-01 10/06

