How Cisco IT Uses Extranets to Connect Global Partners to Cisco

Cost-effective menu of link architectures provides secure, reliable connections for Cisco partners.

Cisco IT Case Study / Routing and Switching / Partner Extranet: This case study describes the Cisco Internet Services Group's managed extranet service, which Cisco IT provides for Cisco internal clients that need extranet connectivity for their partners. The Cisco global network is a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

> With access to Cisco network resources and processes, a partner in Scotland or Malaysia can manufacture products with the same quality that Cisco does in San Jose, without any incremental setup time. The extranet has made a difference in Cisco's ability to manufacture high-quality products at low costs.

CHALLENGE

A guiding strategy for Cisco Systems® is to focus on the core business and outsource context activities to partners. For example, Cisco manufactures in-house for new product introductions only—to work out the details—and then engages a manufacturing partner for ongoing work. "Partners provide world-leading expertise and economies of scale that keep our costs low and margins higher," says Henry White, senior manager of IT infrastructure.

To outsource ongoing functions such as manufacturing, engineering, finance, technical support, and advanced network services, Cisco needs secure, affordable connectivity between its own network and partner sites. Before shipping a product, for example, a manufacturing partner would need to access the Cisco Enterprise Resource Planning system to validate the unit configuration and test status and another Cisco system to print shipping labels.

The Cisco IT Internet Services Group (ISG) began developing an extranet strategy in 1998. "Our mission is to provide secure extranet access to internal Cisco resources," says Julie Nordquist, IT project manager for the ISG. Some companies address this challenge by duplicating all the resources that partners need and placing them in a secure network connected to the Internet behind a firewall in what's called a "demilitarized zone," or DMZ. "Given our extensive resource base, creating a special DMZ was not an option because of the cost and complexity," she says. Instead, Cisco IT chose to build a separate and secure managed network access for each partner to the needed corporate resources, protected by Access Control Lists (ACLs).

The extranet strategy is needed to address three types of connectivity requirements. One is partner access to the Cisco network. Another is Cisco access to these customer Extranet networks, for remote troubleshooting and support. A third is reciprocal network access between Cisco and its partners.

Security and affordability ranked high as design goals. Cisco needs to protect its resources from security threats such as intruders and viruses. The affordability of the extranet connection directly affects margins and is an especially big issue outside the continental United States, where leased lines (usually frame relay links) can be prohibitively expensive.

SOLUTION

In 1999, Cisco deployed its first extranet connections in the United States, for manufacturing partners and for remote support and troubleshooting of customer networks. The next year, Cisco added extranet connections for other types of outsourced partner activities, including engineering development. Also in 2000, Cisco completed the distributed extranet backbone architecture in all theaters (Asia and the Pacific; the Americas; and Europe, the Middle East, and Africa) with strategically located points of presence (POPs) in Australia, India, China, Japan, Netherlands, and the United Kingdom. During the economic slowdown of 2001, Cisco gained efficiencies by out-tasking more context activities, which created the need for more extranet connections. And in 2002, Cisco dramatically cut the costs of extranet connectivity by introducing secure VPN connectivity as an alternative to leased-line deployments.

Today, the Cisco extranet network provides a secure, highly available connection to the Cisco intranet for companies that supply Cisco with manufacturing, software development, and call center functions, as well as financial, legal, fulfillment, marketing, and publications services. About 30 percent of the company's extranet partners provide manufacturing services and are fully integrated into Cisco supply chain applications and processes.

ISG's clients are internal Cisco organizations that request extranet access to connect their partners and customers to the Cisco network. ISG provides extranet connectivity as a managed service, supplying and managing Cisco equipment for the partner site. ISG bills the internal client organization for one-time hardware costs, recurring dedicated circuit costs for leased-line connectivity, and monthly support.

Connectivity

Depending on each partner's requirements for reliability, bandwidth, support, and cost, Cisco ISG deploys one of three types of extranet connections: leased line, site-to-site VPN, or user-based VPN.

Leased Line

For leased-line connectivity, ISG offers either dual frame relay leased lines with load balancing, or one leased line as the primary link and Basic Rate ISDN as the backup depending on performance, reliability and cost requirements. Cisco ISG manages this service, and provides three different service levels for each Extranet link: Platinum, Gold, and Silver. The Platinum service level typically is provided for partners that need around-the-clock service or provide critical or real-time functions, such as direct fulfillment or outsourced "priority one" (P1) technical support. The Gold service level usually is provided for partners that need critical support during business hours only, and Silver is for partners needing noncritical (best-effort) support during business hours only. ISG bills its Cisco internal clients for support costs according to the service level.

Cisco manages leased-line extranet connections end-to-end including the equipment at the partner site, providing a Cisco 7606 VXR router at the Cisco POP, and Cisco 3745 multiservice access routers and Cisco 3550 switches at the partner site.

Site-to-Site VPN

In 2002 Cisco IT began providing VPN connectivity over the internet as an alternative to leased line Extranet access. This VPN technology significantly reduces the costs of extranet connectivity because it eliminates monthly circuit costs. Since VPN has been offered as an alternative Extranet option, the ratio of requests for VPN connectivity compared to leased line has risen to 5-to-1. Chief benefits of VPN extranet connectivity are:

- Eliminating the cost for WAN circuits used for "traditional" extranet connectivity.
- Eliminating hardware costs for internal clients and reducing inventory management for the ISG
- Accelerating implementation
- Facilitating short-term extranet connectivity
- Supporting partner telecommuters with user-based VPNs who previously had no Extranet connectivity options (see next section)

To set up a site-to-site VPN, Cisco ISG deploys a Cisco 7606 VXR router at the Cisco POP. At the partner site, the tunnel terminates at a VPN device that the Cisco ISG manages or a Cisco VPN router that the partner manages.

User-Based VPN

Before Cisco IT provided VPN Extranet options for partners, mobile partners had no real options for connecting to Cisco intranet resources. Now, when mobile individuals need secure access to the Cisco intranet, Cisco ISG sets up a user-based VPN. Extranet access is therefore tied to the individual instead of a particular site. The sponsoring client works with the partner to sign a network connection agreement, and, in addition, the individual user signs a nondisclosure agreement. After the administrative details have been completed, the extranet team provides the partner user with authentication software to connect to a VPN concentrator dedicated for extranet use. The user-based VPN is a popular approach to disaster contingency. For example, if the ordinary extranet connection becomes unavailable to a partner providing technical support, the user-based VPN provides an alternative way to access the network from either an active Internet connection or a completely different location. Currently, user-based VPNs are available in the United States and the Asia Pacific region.

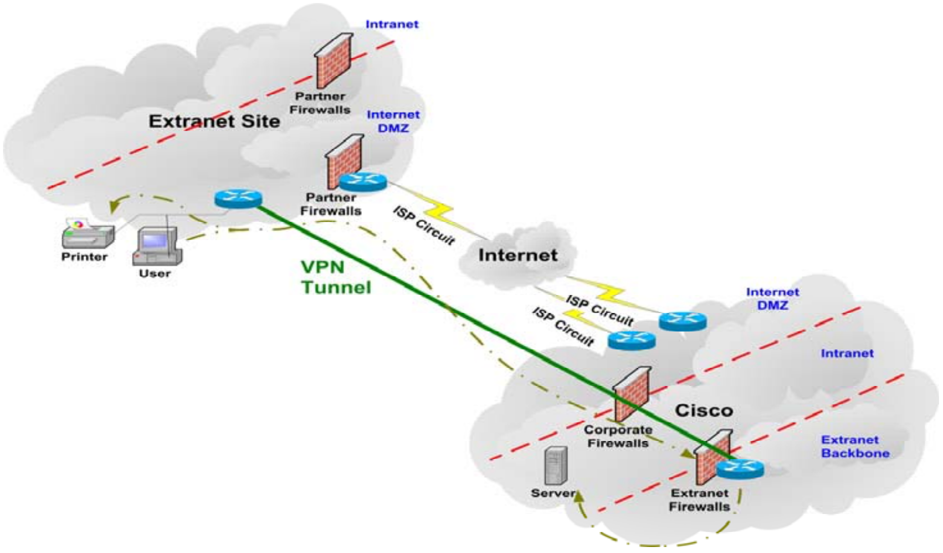
Extranet Topologies

For both leased-line and site-based VPN connectivity, ISG can support either a remote-LAN or interconnect network topology. Which is better depends on the partner's business needs.

Remote LAN Model

A remote LAN is an extension of the Cisco network at the partner site. A managed Cisco router at the partner side terminates the transport connectivity from Cisco and connects to one or more managed switches at the partner location (Figure 1). The Cisco internal client typically provides the PCs and printers connected to the remote LAN. This extranet solution is most common for manufacturing, Global Positioning System (GPS), and Auto-Test partners. "Manufacturing partners generally need to print files from servers at the Cisco site, which they couldn't do if the printers were on their own network, as opposed to the Cisco network," says Nordquist. Similarly, GPS and Auto-Test partners need to set up their own routers on the Cisco remote network in order to test. The remote LAN topology isolates the Cisco internal client's subnetwork so that it cannot inadvertently send test data over the production network.

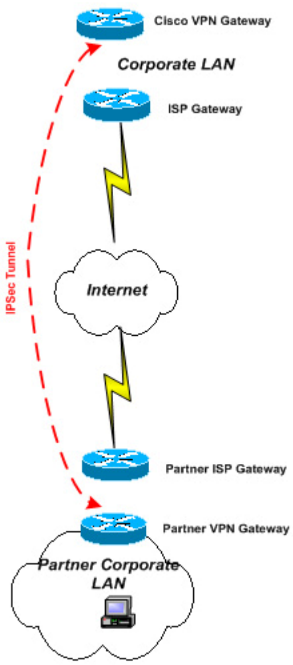
Figure 1. Remote Model for Site-Based VPN Extranets



Interconnect Model

With the interconnect model, a partner connects through its own corporate LAN, which interconnects with the Cisco LAN (Figure 2). Firewalls at each side protect each company's respective resources. Partners can connect from any desktop on their LANs. By contrast, with the remote LAN model, they are limited to desktops that are physically connected to the remote LAN. Some sites incorporate both topologies. This flexibility is helpful, for example, if a manufacturing partner's buyer wants to access buying information from her own desk instead of walking to the product manufacturing area in the warehouse.

Figure 2. interconnect Model for Site-Based VPN Extranets



Security

ISG works closely with the Cisco Information Security group to ensure the security of extranet connections. "A chief challenge is that we can't control our partners' perimeter security," says Michelle Koblas, manager of Corporate Information Security. "If we open our network to partners that don't have adequate security, we have opened a back door into our environment." Potential risks that the groups work together to mitigate include denial-of-service (DoS) attacks, spreading of viruses, hop-off threats, and the possibility that Cisco might not be informed when partner employees are terminated, for example.

The Cisco Information Security group takes a three-pronged approach to these challenges: legal measures, access restrictions, and enforcement. The legal tactic is to require extranet partners to sign two agreements. One is a non-disclosure agreement that each individual must complete. The other is a company-wide network connection agreement that stipulates expected user behavior and security policies that the partner organizations are expected to enforce.

Access restrictions include the following:

- **Firewall permissions—**Cisco firewalls between the partner and Cisco limit machine-to-machine access at the protocol level. Use of access control lists (ACLs) in routers enables Cisco to establish network-to-network connectivity, both per-host and per-service. Currently, partners enforce their own restrictions on incoming traffic to their networks.

- **Web proxy—**Firewalls restrict traffic by host or by port: A partner that has access to a particular host can generally take advantage of any service on that host, including Web, FTP, or Telnet. The Cisco Information Security group is investigating the use of Web proxy features of the Cisco CSS 11500 Series Content Services Switch to filter access on a per-URL basis.
- **Sandbox infrastructures—**To protect against partners "hopping off" a host they are authorized to access to one they are not, Cisco has implemented what is called a sandbox infrastructure. That is, partners can work on the host for which they are authorized, but that host is restricted from initiating traffic to other hosts or networks.
- **Authentication and authorization—**Cisco provides authentication and authorization at the host and application layers. The Cisco Information Security group is investigating ways to regularly validate authorized employees with partners so that employees who have left the project, for example, no longer have access.

Finally, Cisco enforces extranet security with a combination of intrusion detection systems, occasional physical audits of partner environments, and periodic ACL reviews to ensure that partners still need access to the same hosts and services. "We follow what we call a 'defense in-depth' model," says Koblas. "That is, we implement as much security as possible—not just at the network level but also the host and application levels."

RESULTS

Currently, ISG supports about 200 extranet connections globally, about half of those in the United States and about a third of them used for manufacturing. "In 1999, approximately 40 percent of Cisco product was manufactured at extranet sites," says White. "Since 2000, the proportion has risen to 75 percent."

Cisco has experienced measurable business benefits from its extranet. "The extranet has changed the way we do business by providing our partners with access to real-time data," says Nordquist. "Our partners' ability to access purchase orders in real-time, for example, accelerates product introduction." In fact, ISG recently received recognition from the Cisco Finance group for its contribution to a record-setting Days Sales Outstanding (DSO), a measure of how quickly a company collects receivables. "Our extranet was instrumental in allowing Cisco to hit 32 DSO, an unprecedented accomplishment," says White. "Our ability to achieve this metric of financial health is directly attributable to using world-leading finance partners, and the extranet is the linchpin of those partnerships."

The Cisco extranet also frees in-house Technical Assistance Center (TAC) employees to apply their expertise to more challenging cases while passing along routine cases to partners. "Some 80 percent of TAC cases are Web-generated," says White. "The extranet gives us the flexibility to assign them to the best partner for that particular challenge."

Among the greatest beneficiaries of the extranet is the Cisco manufacturing organization. "Before taking on a task, the Cisco manufacturing organization considers whether a partner can do it more efficiently, at less cost, or with higher quality," says White. "If so, we give them an extranet connection to the internal resources they need."

NEXT STEPS

ISG anticipates that an ever-larger portion of extranet connections will be VPN-based. To further extend cost savings to more critical partner activities, such as an outsourced TAC, Cisco is looking at ways to provide Platinum-level service using VPN technologies. Low-cost VPN connectivity with high priority support will render a partner's location irrelevant. "With access to Cisco network resources and processes, a partner in Scotland or Malaysia can manufacture products with the same quality we do here, without any incremental setup time," says White. "The extranet truly has made a difference in our ability to manufacture high-quality products at low cost."

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.**