

BLACK & DECKER BRINGS INTERNATIONAL LOCATIONS UNDER A CENTRALIZED NETWORK USING VPN

ABSTRACT

The Black & Decker Corporation, a global manufacturer of power tools and accessories, hardware and home improvement products, and technology-based fastening systems, implemented a virtual private network (VPN) architecture from Cisco Systems® to support its international business operations. This customer success story describes how the company:

- Extended its global network and enterprise applications to underserved sites in Europe, South America, Asia, and elsewhere
- Deployed a Cisco® VPN over the public Internet without sacrificing service levels
- Increased network performance and brought new sites online while reducing network costs

“Between last year and this year, we’ve reduced the network budget for our European business by ten percent. But at the same time, we’ve quadrupled our network capacity and we’ve increased our service levels.”

—William Thompson, Director of Network Services, The Black & Decker Corporation

BACKGROUND

The Black & Decker Corporation is a global manufacturer and marketer of power tools and accessories, hardware and home improvement products, and technology-based fastening systems. Headquartered in Towson, Maryland, the company operates manufacturing facilities in 10 countries and sells its products in more than 100. In 2003, the company’s businesses generated sales of more than US\$4.5 billion.

CHALLENGE

As one of the world’s leading power tool and security hardware manufacturers, Black & Decker operates sales, marketing, manufacturing, and customer service operations around the globe. Supporting a dispersed, diverse workforce requires a technology infrastructure that encompasses more than 160 sites in more than 40 countries, as well as more than 1500 “remote workers.”

Over the years, Black & Decker has deployed a wide range of enterprise applications, including Service Advertising Protocol (SAP), QAD, and Manugistics, to enhance the productivity of its worldwide workforce and support its global manufacturing and sales. However, as these solutions proved more and more valuable at some core Black & Decker sites, the company realized that many remote operations, particularly outside the United States, were not fully benefiting from them. At these sites, Frame Relay or dial-up network connections were just too slow and too costly to viably support the emerging solutions.

“We had very low-speed, high-cost circuits serving our locations in South America, Asia, and elsewhere,” says William Thompson, Director of Network Services for Black & Decker. “These sites had connection speeds of 64 or 32 kbps that could not handle our growing traffic demands.”

As a result, many locations outside the United States were either running their own sales and manufacturing systems (making it impossible to centrally process real-time global data), or were running no enterprise applications at all. Black & Decker wanted to bring these international sites online and into a single, global architecture. But providing certain international sites with the necessary bandwidth to support the required applications could carry a substantial cost. In some countries, the cost to upgrade to high-speed Frame Relay links could be as much as 10 times the cost of the same circuit in the United States. And under Black & Decker’s distributed operational model, each remote site had to budget for and fund its own network services.

“It was really a dilemma for our smaller locations,” says Thompson. “Some of our international marketing sites sell two or three million [US] dollars a year in product. They can’t absorb a hundred thousand dollars per year in network costs. It comes right out of their bottom line.”

Black & Decker’s networking services team needed to find a way to “connect” the company’s critical enterprise applications to more international sites at a cost that even smaller operations could afford. And, since the “extended” systems would be useless if parts of the network went down, the team also needed to build the new architecture with maximum redundancy—assuring high availability.

SOLUTION

Black & Decker’s network services team decided that migrating its international Frame Relay sites to a virtual private network (VPN) could provide an ideal solution for reducing network costs, increasing bandwidth, and bringing new sites online. But to keep costs as low as possible, the team opted to provision the VPN over the public Internet, rather than contracting with a network service provider.

“As a manufacturing company producing a high quality product at a competitive price, we’re looking to lower costs wherever we can,” says Thompson. “When you look at networking costs overall, the transport costs represent the largest share, in our case more than fifty percent. That’s the area we had to target.”

Deploying and managing a global VPN-enabled WAN is a large enough task in and of itself. Black & Decker’s networking team didn’t want to worry about networking equipment going down. They needed a dependable, highly manageable VPN solution. The company had used a wide range of Cisco solutions for several years to support its worldwide network, including Cisco Catalyst® 6500, 3500, and 2950 series switches, 7500 and 1600 series routers, 3600 and 2600 series multiservice platforms, and Cisco PIX® 500 Series security appliances. Recognizing the superior reliability and performance of the Cisco solutions, as well as the management benefits offered by a single vendor environment, the team chose Cisco VPN 3000 Series Concentrator appliances to support the global VPN.

Black & Decker began with a controlled implementation at sites in Australia and New Zealand. Options for these locations using a traditional Frame Relay connection would be at a cost of US\$75,000 per year. The networking team found that the Cisco VPN solution could support these sites at a fraction of that cost while delivering more bandwidth and better application performance. The pilot deployment was so successful that the solution was rapidly expanded to other Black & Decker sites around the globe.

Initially, the networking team planned to phase in VPN at its larger sites as a backup to the existing Frame Relay network. But the VPN solution was so effective that it quickly supplanted the network it was intended to back-up. VPN became the primary network, with Frame Relay providing the backup network service.

Today, the company uses the Cisco VPN solution to support its Power Tools and Accessories business units in Europe, South America, and Asia, as well as manufacturing sites in the Czech Republic and elsewhere. Sites are outfitted with Cisco VPN 3005, 3015, or 3030 concentrators, depending on the size of the operation. At larger sites, the VPN concentrators work in tandem with a Cisco 2600 Series Multiservice Platform.

Each remote site connects back to one of Black & Decker’s primary data centers in the United States, England, or Hong Kong. The sites are configured with multiple routes to a primary data center, so if one path goes down, the network automatically fails over to a secondary path. And because the entire system runs over the Internet, if any parts of the redundancy systems fail, Black & Decker’s networking team can create a new VPN tunnel to another data center in minutes.

According to Thompson, “The way we’ve architected this solution, if anything fails, we still have more redundancy than we’ve ever had before.”

RESULTS

The Internet-enabled Cisco VPN architecture has delivered significant cost savings and network performance enhancements at Black & Decker’s international locations. In the company’s 40-site Power Tools Europe network alone, the solution has cut network connection costs by 10 percent annually. And, more importantly, VPN has made it possible for Black & Decker to fully deploy its manufacturing, sales, and enterprise resource planning applications globally.

“Between last year and this year, we’ve reduced the network budget for our European business unit by ten percent,” says Thompson. “But at the same time, we’ve quadrupled our network capacity, and we’ve increased our service levels. Our business is driven by product cost and maintaining margins, so we have to come up with solutions that help take costs out of the business. With this technology, we’ve been able to do that.”

By using the Internet and managing the Cisco VPN solution internally, Black & Decker has also been able to achieve its goals at a fraction of the cost of deploying a comparable Frame Relay network or using a service provider’s private VPN backbone.

“I can buy an E-1 Internet connection for far less than equal capacity in a managed Frame Relay or Multiprotocol Label Switching [MPLS] network,” says Thompson. “We could expect to pay a service provider between thirty and fifty thousand [US] dollars per month more for MPLS service to get close to what we’re running today on our VPN.”

Bringing New Sites Online

The Cisco VPN solution has provided Black & Decker with the greatest benefits at its smaller sites in South America and Asia—sites that previously relied on low-speed dial-up connections or were not networked at all. For example, two years ago the company was not running its Manugistics application for demand and supply planning in Asia, because the network bandwidth was not adequate. Today, Black & Decker has standardized that and other enterprise applications for its entire Asia market, running from a single data center in Hong Kong.

“We’ve lowered the ‘hurdle’ for bringing a site on network,” says Thompson. “In Asia and South America, there were several locations we wanted to bring into the network, but we couldn’t justify the cost when we looked at the annual sales these businesses generated. Now, we can put those sites on the network for less than one thousand [US] dollars per month.”

Deploying and Managing the Solution

Using a single vendor to support the new VPN solution and its entire worldwide network architecture, Black & Decker enjoys better network performance, easier management, and lower total cost of ownership. All network routers and switches use Cisco IOS® Software and a common, Web-based graphical user interface, enabling streamlined IT management and reduced training costs.

The Cisco VPN solution also provides tremendous flexibility. Black & Decker had previously deployed Cisco VPN 3000 series concentrators at some sites to provide remote connectivity, and securely extend network services to individual employees working outside the office. At these sites, the company was able to use the same appliance to support the site-to-site WAN connection. And, now that the Cisco VPN solution is deployed throughout the world, Black & Decker can expand its remote connectivity or VPN capabilities as its needs require.

“Today, we have Cisco VPN appliances around the world in fifty to sixty locations, and we can turn up services at any location as we need to,” says Thompson.

NEXT STEPS

Over the next several years, Black & Decker plans to continue expanding its global VPN architecture and exploring new technologies such as class of service and converged voice and data. By using versatile Cisco solutions to support its global network, the organization knows its network investment will be protected and its operations can continue generating attractive returns.

“Cisco is continually adding features and functions to its products through Cisco IOS,” says Thompson. “The ability to upgrade a product in software and get more functionality out of it is very important to us. We believe that our installed base of Cisco equipment will support new functionality as our needs evolve over time.”

This customer story is based on information provided by Black & Decker 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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, Cisco IOS, and PIX are registered trademarks or 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.
(0402R) EC/LW6064 04/04