CUSTOMER SUCCESS STORY

XB NETWORKS SECURES ITS CUSTOMERS' NETWORKS AND ITS MARKET ADVANTAGE WITH CISCO SECURITY SOLUTIONS

EXECUTIVE SUMMARY

CUSTOMER NAME

XB Networks

INDUSTRY

Managed Security Service Provider

BUSINESS CHALLENGE

- Needed robust firewall solution for a managed security services offering to customers
- Required manageability
- Needed to build a foundation for delivering additional services as customers need

NETWORK SOLUTION

- Cisco Systems routing and switching solutions
- Cisco IOS Software Firewall, configured to satisfy ICSA Labs Firewall certification criteria, with the Cisco IOS Firewall Feature Set, which integrates stateful packet filtering; application-based filtering; dynamic per-user authentication and authorization; defense against network attacks; and real-time alerts.
- Cisco Router and Security Device Manager (SDM) bundles for devices running Cisco IOS Firewall

BUSINESS VALUE

- Enables rapid, easy deployment of enterprise-quality managed network security services to customers
- Improves manageability, enabling XB Networks to proactively report to customers on benefits of the security service
- Helps secure full range of Cisco CPE routers deployed at customers' locations

BUSINESS CHALLENGE

As technology evolves, so does the role of service providers. XB Networks of The Netherlands began as an Internet service provider (ISP) and has expanded its mission to provide a comprehensive range of managed services, in addition to Internet access services. In response to increasing customer demand for solutions that integrate security into their networks, today the company provides managed network security solutions for small and medium-sized businesses in The Netherlands—in addition to its managed service portfolio of broadband access, hosting, and IP virtual private networks (VPNs) solutions.

Often, service providers that specialize in security offer high-end solutions that are designed—and priced—for large enterprise customers. Smaller companies had to either create and maintain their own network security solutions or purchase services from a local reseller with no way of knowing exactly how their networks were being secured. XB Networks sought a firewall solution that would complement its current managed services portfolio and bring affordable, reliable large-enterprise-quality managed security capabilities to its small and medium-sized business customers. The solution also had to be easy to deploy and manage.

The company has four criteria for any new service it offers. The service must be complete; it should be both scalable and flexible; and it must be easy to manage to that XB Networks can assure optimized levels of service and reliability for its customers. After considering another vendor's firewall solution, XB Networks chose the Cisco IOS® Firewall with Cisco Router and Security Device Manager (SDM) 2.0 from Cisco Systems®.

NETWORK SOLUTION

To provide its customers with the managed services and communication links they require, XB Networks uses a variety of Cisco routers at customers' premises. Every connection XB Networks sells is equipped with a Cisco router. The Cisco network security solution enables the company to combine many new security features, including an intrusion prevention system, into one piece of equipment, making deployment and management more efficient.

"We chose the Cisco solution because it presented us with a complete package," explained Erik van Laar, managing director of XB Networks. "The Cisco IOS Firewall runs on our Cisco customer premises equipment, which provide enterprise-class connectivity for delivering services to our customers' sites. So it was easy to deploy firewall services on the customers' existing equipment. And because our staff is already familiar with Cisco networking, we did not need to spend much time in additional training and management. The solution fits in with our existing environment."

The XB Networks core network is based on Cisco 12000 Series routers, which scale from 2.5 Gbps/slot to 40 Gbps/slot and enable carrier-class IP/Multiprotocol-Label-Switching (IP/MPLS) core and edge networks. One-gigabit fiber links connect the Cisco 12000 Series routers to Cisco 7200 Series routers, which are among the industry's most widely deployed universal services router for enterprise edge applications. The Cisco 7200 Series routers distribute traffic via Gigabit Ethernet or 155-Mbps links (STM-1) to customer locations, where a range of Cisco access routers are deployed. Depending on the customer's needs, access routing platforms can include Cisco 800, Cisco 1700, Cisco 2600 and Cisco 3700 series routers.

For customers that subscribe to the XB Networks' managed security offering, Cisco Router and Security Device Manager (SDM) 2.0 and Cisco IOS Firewall run on the CPE edge routers. Cisco IOS Software integrates state-of-the-art firewall functionality and intrusion prevention for network perimeters. It provides powerful security features such as stateful, application-based filtering; dynamic per-user authentication and authorization; defense against network attacks; Java blocking; and real-time alerts. It not only enables a single point of protection at the perimeter of a network, but Cisco IOS Firewall also makes security policy enforcement an inherent component of the network itself.

"We have always used the normal access control list feature in Cisco IOS Software, but now we can take advantage of the Cisco Advanced Feature Set," says Marcel Knol, Technical Director of XB Networks. "By combining Stateful packet filtering with Cisco Network Admission Control (NAC) policies and other features, we are equipped to protect against both internal and external threats."

Context-based Access Control (CBAC) in Cisco IOS Firewall is an advanced traffic filtering technology that intelligently filters transmission control protocol (TCP) and user datagram protocol (UDP) packets to determine whether they contain malicious viruses or worms. CBAC can be configured to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network to be protected. Without CBAC, traffic filtering is limited to access list implementations that examine packets at the network layer or at the transport layer. CBAC examines not only these but also the application-layer protocol information to learn about the state of a TCP or UDP session. Another feature, the Per-User firewall, allows service providers to offer a managed firewall solution via download of firewall, access control lists (ACLs), and other settings on a per-user basis, using a profile in the Authentication, Authorization, and Accounting (AAA) server.

Running in conjunction with the Cisco SDM 2.0 and Cisco IOS Firewall is the Cisco Intrusion Prevention System (IPS). Cisco IPS scans for certain traffic patterns and packets that could indicate malicious activity and defends against viruses, worms, and other security threats by integrating security measures throughout the network. Traffic is scanned and compared to a "fingerprint database," which is maintained by Cisco, and offending activity is blocked at the network edge. The solution defends communication networks from viruses, worms, and other security threats by integrating security measures throughout the network. Network-wide security integration provides a comprehensive defense without inhibiting the access of legitimate users and, as a result, preserves the rich productivity advantages of IP-based communications.

"The support from Cisco enables us to ensure that the threat database is maintained at all times," van Laar explains. "As a managed security service provider, we want to team with the best in the industry to protect our customers, and the Cisco solution is a key part of our total managed security service package."

"We have options to bring video, voice, and data onto a single platform and deliver security solutions that compete successfully with the costly offerings of larger, specialized service providers. The Cisco security solutions enable us to prove to the market that customers can rely on us."

—Erik van Laar, Managing Director, XB Networks

BUSINESS VALUE

The new network security solution enables XB Networks to offer its customers an enterprise-class security solution as a cost-effective service. More than just a simple means of inspecting packet headers, the Cisco routers with Cisco IOS Firewall can inspect complete data packets themselves in order to determine if they contain malicious viruses or worms.

"Another significant benefit has been the solution's manageability," says van Laar. "The Cisco solution allows us to deliver excellent managed services to the customer while making it simple for us to manage. We already have Cisco knowledge and training. Adding the Cisco IOS Firewall was a reasonably easy step and eliminated the need for us to invest in complete re-training for our staff."

Today, XB Networks can use the combination of Cisco products to demonstrate their added value—mitigating a wide range of risks that otherwise could have had significant consequences to the customer's business. In addition, van Laar's team can now proactively deliver customer data that is automatically generated by the Cisco solution. For example, a staff member can review the system error cards and report to a customer that their CPE routers were updated 32 times the previous month to prevent virus attacks.

Besides protecting the perimeter of the network from external threats, firewalls can also prevent users from accessing a particular subnet, workgroup, or local area network (LAN) within a corporate network. XB Networks provides managed security to the large Dutch insurance company CZ, which must interconnect with many different partner networks to exchange healthcare information. Secure VPN services are provided to Kroymans, a large luxury car dealership, which must communicate with Jaguar, Cadillac, Saab, Ferrari, Aston Martin, and other manufacturers and dealer partners. XB Networks has also secured many local municipal offices in the Netherlands, where Cisco 2600 Series routers with Ethernet and digital subscriber line (DSL) interfaces running Cisco IOS Firewall keep traffic secure and subnets separate.

"The Cisco solution gives us a distinct competitive advantage," van Laar says. "When implemented with the Cisco IPS, even the most advanced security service providers cannot compare with our offering because they cannot replicate the tremendous information-collection resources behind the Cisco IPS database or maintain vigilance 24 hours a day."

NEXT STEPS

The Cisco routing and switching platforms, enhanced by Cisco advanced security technologies gives XB Networks the ability to easily integrate its network security solution with its management tools and daily business processes.

"I think that's the greatest advantage for us," says van Laar. "We have options to bring video, voice, and data onto a single platform and deliver security solutions that are as secure as the big companies' offerings. The Cisco solutions enable us to prove to the market that we are the company that customers can rely on."

FOR MORE INFORMATION

To find out more about Cisco routing solutions, go to: http://www.cisco.com/go/routing.

To find out more about Cisco switching solutions, go to: http://www.cisco.com/go/switching.

To find out more about Cisco security solutions, go to: http://www.cisco.com/go/security.

To find out more about Cisco managed services solutions, go to:

http://www.cisco.com/go/managedservices

http://www.cisco.com/en/US/netsol/ns465/networking_solutions_program_category_home.html

To find out more about XB Networks, go to: http://www.xbn.nl/

This customer story is based on information provided by XB Networks 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 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

DR/LW7552 12/04

Printed in the USA