Mitigating Security Breaches with Firewalls and Intrusion Prevention

Barnhart Crane & Rigging leverages ASA 5500-X with IPS in active-standby deployment.

EXECUTIVE SUMMARY

BARNHART CRANE & RIGGING

- Heavy equipment lifting and transportation
- Memphis, Tennessee, USA
- 600 employees

BUSINESS CHALLENGE

- Prevent hacker intrusions into network
- Get improved visibility into firewall to find potential vulnerabilities
- Segment traffic for greater security and administrative efficiency
- Deploy network security system that can be modified during business hours without loss of protection

NETWORK SOLUTION

- Cisco ASA 5500-X Series Next-Generation Firewalls with Intrusion Prevention System (IPS) modules
- Firewall and intrusion prevention in one device
- Active-standby configuration

BUSINESS RESULTS

- Provides robust intrusion prevention
- Simplifies administration for better visibility, improved security
- Allows most maintenance to be performed without firewall outages or IT overtime

Business Challenge

Based in Memphis, TN, and with 28 sites across the United States, Barnhart Crane & Rigging serves demanding customers in construction and other time-sensitive industries and knows that it cannot afford disruptions to its computer network. So when hackers took advantage of a hole in the company's non-Cisco firewall to hijack its Internet bandwidth, systems engineer Gene Shinall and his colleagues knew it was time to address the larger issue of protecting its data and digital assets.

"They got around our firewall, hacked into a Windows box, and used the Windows machine to get into another server," Shinall says. "Then they used our bandwidth to attack other systems outside our network."

The result: Barnhart's Internet connection was virtually unusable by its own employees. The firewall itself was part of the problem.

As Shinall says, "In the old firewall system, it was very hard to view the NAT translations and the firewall rules that were set up. So it was difficult to see that we even had a hole in our firewall."

Barnhart's IT staff realized that they needed a more effective and a more easily manageable intrusion prevention solution. They also wanted a solution that could segment traffic coming from or going to the Internet, Barnhart's network edge, and employee VPN connections. Finally, they wanted a resilient security solution that offered an active-standby capability, so that they could carry out maintenance on their security infrastructure during normal business hours without leaving their network vulnerable.

Network Solution

Barnhart chose Cisco® ASA 5500-X Series devices with Intrusion Prevention System (IPS) modules. Specifically, the company placed two 5525-X devices at its Memphis headquarters and another at its disaster-recovery site near Knoxville, TN.

The two units in Memphis give Barnhart full active-standby capability, helping ensure that the company's network had firewall and intrusion prevention protection even if one of the devices needed to be serviced. The active-standby configuration also allows the IT staff to perform routine maintenance, and even handle most unforeseen events, without working overtime.

The Cisco ASA 5525-X bolsters the efficiency and security of Barnhart's network by permitting it to be easily segmented. Shinall has configured the units with segments for the Internet, Barnhart's DMZ, and employee VPN connections. This segmentation enables the IT group to set different access policies for different devices and services on the network.

A network service provider manages a Multiprotocol Label Switching (MPLS) network that connects 14 of Barnhart's sites; that service provider also manages the Internet firewalls at its supported branches. The remaining sites are managed by Barnhart's own IT staff and are connected to the main office via VPN tunnels. For greater efficiency, all the branches split traffic, so that Internet traffic goes directly to the requested website, while company traffic uses the appropriate internal network.

Barnhart's staff credits Cisco customer support as one of the deciding factors in expanding their network infrastructure with a Cisco security solution. "Every time I've called, it's been outstanding customer service," says Shinall.

Business Results

The Cisco ASA 5525-X with IPS is helping Barnhart's IT staff block attacks and segment the network, providing both better security and easier administration. It also enables employees to securely access Barnhart resources from any of the company's own remote sites, client sites, or wherever else they may be. With a Cisco solution in place, Shinall says, "I feel very secure behind our ASA 5525-X active-standby pair."

The security solution at Barnhart's headquarters integrates with branch equipment, some of which is managed by Barnhart's IT group and some by a network service provider. The switch to a Cisco firewall/IPS device has resulted in a number of administrative benefits to Barnhart's IT staff. Because the intrusion prevention system is integrated into the firewall, they only have one device to manage, and the two functions are designed to work smoothly with one another.

Also, Barnhart's network infrastructure equipment already consisted mainly of Cisco products, including Cisco switches and routers at the main office and the branch sites. As a result, IT personnel were able to come up to speed quickly on the new device. The ASA 5525-X gives Barnhart's IT staff better visibility into their security configuration, so that they can spot potential problems faster and more easily.

PRODUCT LIST

Network Management

- Cisco Adaptive Security Device Manager (ASDM)
- Cisco IPS Device Manager (IDM)
- Cisco Identity Services Engine Command Line Interface (CLI)

Security

- Cisco ASA 5525-X with IPS

For More Information

To learn more about Cisco ASA 5500-X Series Next-Generation Firewalls with IPS, please go to: cisco.com/go/ips.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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 C36-728974-00 07/13