Business Makes Access to Social Media Sites Safer

Customer Case Study

EXECUTIVE SUMMARY

Company: Swanson Health Products
Industry: Online Retailer
Headquarters: Fargo, North Dakota
Employees: ~630

Challenge

- Protect business and sensitive customer information from network security threats
- Help ensure security protections do not reduce productivity
- Simplify security management

Solution

- Deployed Cisco ASA 5585-X Adaptive Security Appliance with Next-Generation Firewall Services

Results

- Selectively gave employees access to different websites needed for jobs
- Improved compliance with Payment Card Industry (PCI) security standards
- Reduced help desk calls regarding website access by 50 percent

Swanson Health Products uses Next-Generation Firewall to control website access that employees need to do their jobs.

Challenge

Voted America's #1 Internet merchant in a 2013 survey[1], Swanson Health Products sells vitamins, supplements, and natural health products worldwide. To build loyalty, the company works hard to make sure that customers receive their products quickly. "To do that, we need to keep our website and internal network up and running," says Jason Kennedy, network systems administrator for Swanson.

One threat to availability is malware. Company computers became infected when Swanson employees clicked links to malicious websites in social networking sites or "phishing" emails. Another threat is Distributed Denial of Service (DDoS) attacks, which clog servers with meaningless traffic so that customers cannot get through.

At first, Swanson used two separate security solutions to protect the business. A Cisco® firewall blocked people outside the company from accessing the company's internal network. A third-party web-filtering solution kept employees from visiting social networking sites or personal webmail accounts.

But some employees need to visit these websites as part of their jobs. For example, a few dozen employees post product information on sites such as Twitter, Pinterest, Instagram, and Facebook. The company's marketing team tests out email campaigns by sending emails to their own webmail accounts.

"Our old web-filtering solution didn't let us block social sites for some employees and allow it for others," Kennedy says. "So the only way employees could visit Twitter or Facebook was by walking over to a conference room with guest Wi-Fi access. This wasn't a good use of their time."

Swanson decided to look for a more flexible yet secure way to control access to the web. One requirement was the ability to prevent employees who have access to payment card information from uploading or downloading files outside the company. This would help the company meet Payment Card Industry (PCI) security standards.

[1]ConsumerLab.com Vitamin and Supplement Users Survey: www.consumerlab.com/survey2013.

"With the Cisco Next-Generation Firewall, we can allow access to certain sites for some employees and block access for other users. Combining firewall and web filtering in one device simplifies management. And our networking team is already familiar with Cisco products, so we didn't need to spend time learning a new solution."

Jason Kennedy
Network Systems Administrator
Swanson Health Products

Solution

Now Swanson has granular control over who can visit which websites, and which website features they can use. The solution is a Cisco ASA 5585-X Adaptive Security Appliance with Next-Generation Firewall Services. It combines firewall, malware protection, and social media protection in one device. "With the Cisco Next-Generation Firewall, we can allow access to certain sites for some employees and block access for other users," says Kennedy. "Combining firewall and web filtering in one device simplifies management. And our networking team is already familiar with Cisco products, so we didn't need to spend time learning a new solution."

The network security team used a friendly interface to give employees the types of Internet access that they need to do their jobs. For example, employees who work on the company's Facebook page can now access the site, but they cannot use games or chat. Employees who work on email campaigns can visit their webmail accounts, but cannot upload or download files. Employees in the call center and other departments that work with payment card information also cannot email certain types of files.

Everyone can access the web, but Cisco Web Security Essentials (WSE) restricts access to sites with bad reputations, based on a reputation score that factors in country of origin, time in business, and dozens of other factors. The IT team decided to allow only a few employees to visit websites hosted in two countries with a high percentage of infected sites. "It's simple to create and modify access policies," Kennedy says.

Swanson also takes advantage of other Cisco security solutions to help keep the business up and running. Cisco Intrusion Prevention System (IPS) alerts the IT team to unusual activity on the network and can block these activities. And Cisco ACE Application Control Engine balances website traffic between multiple servers to help make sure that customers have a good experience even when traffic is highest.

"Not having to constantly walk back and forth to a guest Wi-Fi hotspot to visit social media websites gives employees more time to interact with customers."

Jason Kennedy
Network Systems Administrator
Swanson Health Products

Results

Balanced Security and Productivity

Now authorized Swanson employees can visit social media websites from their desks. They post about new products to stimulate sales, and respond to customer questions to improve satisfaction. "Not having to constantly walk back and forth to a guest Wi-Fi hotspot to visit social media websites gives employees more time to interact with customers," says Kennedy.

Flexible controls also helped solve a problem for the company's 150 contact center agents. When the company started issuing digital paychecks, employees had to access their personal email accounts to confirm their identity. But the company ordinarily blocks webmail access for all but a few employees. Enabling the 150 contact center agents to access webmail took just a few clicks.

Helped to Keep Business Up

The Next-Generation Firewall connects with Cisco Security Intelligence Operations (SIO) to shield Swanson's network from new "zero-day" malware and viruses. Dynamic updates from hundreds of thousands of sensors around the world are delivered to Swanson's device within a few minutes, often hours before other solutions. This capability helps to make sure that customers can place orders and employees can do their jobs. "We've had zero infections since 2009," Kennedy says. "The credit goes to our firewall policies and Cisco security solutions."

Complied with PCI Security Standards

The IT team set up the firewall to prevent employees in departments that work with payment card information from emailing attachments outside the company. This policy keeps credit card information safer. The solution also disables suspicious links in websites, which helps to protect Swanson from malware that sifts through email looking for sensitive information, or that logs keystrokes to steal passwords.

Saved Time for IT Team

Since Swanson implemented the Cisco Next-Generation Firewall, the number of help desk calls about Internet access has dropped by half. Employees who need website access have it. "Not having to deal with smaller IT issues like web access gives us more time to work on programs that improve the business and the customer experience," Kennedy says.

Easy-to-use management tools save more time. To configure and monitor the firewall, the IT team uses an intuitive dashboard called the Cisco Adaptive Security Device Manager (ADSM). When web access was slow one day, the dashboard showed that a terminal server was blocking web traffic. With this information, Kennedy was able to quickly fix the issue before it became a big problem. And using Cisco Prime Security Manager, the IT team just clicks to create website access policies that consider the application, micro-application (such as Facebook chat), user, group, and device.

Technical Implementation

The Cisco ASA 5585-X Adaptive Security Appliance filters content based on the identity of the employee who makes the request. Behind the scenes, Cisco Context Directory Agent connects with Microsoft Active Directory to make sure that the employee's login matches the device's IP address. "This way, we know that employees are who they say they are," Kennedy says.

Swanson started with one Cisco ASA 5585-X, deployed at the main office. Web traffic from the company's two distribution centers travels through the main office so that the firewall can allow or block the request. As web traffic increases, the company might install firewalls at the distribution centers, as well. Swanson might also replace its standalone Cisco IPS solution with a module in the firewall, simplifying management.

For More Information

To learn more about Cisco ASA 5585-X Next-Generation Firewall, visit: www.cisco.com/go/firewall.

PRODUCT LIST

Security

- Cisco ASA 5585-X Adaptive Security Appliance with Next-Generation Firewall Services
- Cisco Intrusion Prevention System (IPS) 4300 and 4200 Series
- Cisco Prime Security Manager

Data Center

- Cisco Nexus® 5548 Switches
- Cisco Nexus 1010 Virtual Services Appliance
- Cisco Catalyst 6504-E with Virtual Switching System
- Cisco ACE Application Control Engine

Wireless

- Cisco Aironet® Wireless Access Points 3602, 1200 Series, and 1100 Series
- Cisco Wireless Control System 5508 and 2504

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**.

EDCS-1348825 C36-731063-00 02/14