

Software Services Company Locks Down Small Office Network

Scotweb uses Cisco IOS Security services embedded in an office router to protect critical business services.

EXECUTIVE SUMMARY
Customer Name: Scotweb Solutions Limited <ul style="list-style-type: none"> Technology Services Edinburgh, Scotland
CHALLENGE <ul style="list-style-type: none"> Protect small office network against Internet threats Reduce time and effort required to manage network security Reduce disruptions to customer-facing services
SOLUTION <ul style="list-style-type: none"> Replaced standalone security solutions with Cisco IOS Security services integrated into a small office router
BUSINESS RESULTS <ul style="list-style-type: none"> Strengthened network defenses Reduced security management from hours per month to minutes Improved service uptime and availability

Challenge

Scotweb Solutions Limited is a small web design and application service provider located in Edinburgh, Scotland. Scotweb's core business is a web-based scheduling application called MedicalRota.com that lets physicians and nurses view and update shift schedules online, request time off, and even receive text message alerts when schedules change. Since hospital schedules are constantly in flux, the solution offers a huge improvement over the way hospitals typically handle this process—relying on hand-written charts that are constantly out of date.

Scotweb's MedicalRota service is now used heavily by a local hospital, and the company is working to expand the application throughout Scotland. To make this vision a reality, however, Scotweb must provide a secure, highly available service. As a small business, this is no small task. Scotweb's application servers are hosted at a remote data center, but the company maintains several important network services out of a home office, which must be protected at all times.

"We replicate our databases between the data center and our office, and handle development and beta testing here, as well as our DNS [Domain Name Service] servers," says Michael Simpson, Scotweb's chief technology officer. "We like the control that we can maintain by hosting these services ourselves, but that also means we're open to Internet attacks."

These threats were becoming even more significant as Scotweb upgraded its network from IP version 4 to IP version 6. The upgrade provided the company with critical new control capabilities, but it also unleashed a new level of Internet threats. "The degree of probes and scans that we started receiving took a huge jump upwards, as much as 10 or 20 times what we were seeing before," says Simpson.

Because Scotweb hosts patient information, its servers need to be protected at all times. But even more important is preserving the availability of the application itself, because lives may literally depend on it. For example, the MedicalRota system's auto alert feature sends text messages out to clinicians. In the event of a major medical emergency, the hospital would rely on that system to alert nurses and physicians that they were needed.

"If an attack were to reach the DNS servers and bring down the service, it could be disastrous," says Simpson. "It would compromise important hospital functions and damage our reputation enormously."

To protect the small office network, Scotweb used a standalone firewall and an intrusion detection system (IDS) application running on a separate server. Simply maintaining the separate routing, IDS, and firewall solutions required many hours per month—a significant burden for such a small staff. Software updates were also problematic. If a critical security patch were released for the firewall, for example, it had to be installed immediately, even if that meant taking down the network temporarily and cutting off user sessions in progress.

Solution

As part of Scotweb's migration to IPv6, Simpson upgraded the Cisco IOS® Software in the company's Cisco® 877 Integrated Services Router to support advanced IP services. He quickly realized that he could now manage many security functions using the Cisco IOS security services embedded within the router itself and substantially simplify the network security management burden.

To protect critical servers against Internet threats, Scotweb implemented Cisco IOS Intrusion Prevention System (IPS). Designed to provide strong threat defense for small businesses and branch offices, the solution provides inline deep-packet inspection features that mitigate a broad range of network attacks.

Scotweb also deployed Cisco IOS Firewall. This solution provides stateful packet inspection to block unwanted traffic while maintaining the integrity of legitimate business traffic. It also includes advanced application inspection features that control unauthorized application use and protect against software vulnerabilities.

"I used to configure firewall and access control features manually, but I find the Cisco IOS Firewall to be significantly easier to use," says Simpson. "It allows me to help ensure that services that need to access the Internet for any reason are able to do so without opening holes in my environment that would leave me vulnerable to attack."

Despite placing a larger security burden on the Cisco router, Scotweb has not experienced any decline in the performance of the network or the applications it supports. "We've seen no performance hit whatsoever," says Simpson. "In fact, by moving everything to a single host, we've actually sped things up."

To keep the Scotweb network protected at all times, the company makes sure that the Cisco IOS IPS is always updated with the latest attack signatures. Despite the fact that maintaining signature updates can be challenging for some small businesses, Simpson has found the process for the Cisco IOS IPS to be invariably quick and easy.

"Attacks are always evolving, so you need to be sure that you're using the most current signatures available," says Simpson. "I load and install new signatures for every service we're running as soon as they come out. It's not difficult in the slightest. You just download the signature package from Cisco, copy it to the router, and you're done."

In general, Simpson has found the Cisco IOS Security services to be very easy to manage, even for a very small IT department.

"With the browser-based tools that Cisco provides, management and configuration are simple," he says. "You don't need to know command line interface, the Cisco Security Device Manager interface handles everything for you out of the box. Basically, anyone can set it up easily."

"Using Cisco IOS Security Services embedded in the Cisco router has significantly reduced the time that I have to devote to security tasks and the effort required to keep us secure."

—Michael Simpson, Chief Technology Officer, Scotweb Solutions Limited

Results

Today, Scotweb and the clinicians relying on its web-based service are more secure than ever before. Despite potentially opening the company up to new attacks with the adoption of IPv6, the company has had no security issues since the migration. In fact, within two months of implementing the Cisco IOS Security services, Simpson realized that the standalone firewall had become unnecessary, so he decommissioned it. He maintained the standalone IDS solution, but found that he was no longer receiving alerts—the Cisco IOS IPS solution was handling everything.

“The Cisco IOS Software has effectively taken over those security services completely,” says Simpson. “It’s hugely beneficial. I can now access all of the security information for the network right from the Cisco router and very quickly get a handle on exactly what is going on in our environment.”

The strong network defense capabilities are vital for Scotweb and its customers. But for Simpson, the most noticeable advantage of the Cisco IOS Security services is the ease and efficiency with which he can now manage and monitor network security.

“It’s nice to have all of these security services controlled from one central place, and be able to configure everything from one interface rather than having to configure and maintain three separate devices,” says Simpson. “It means that instead of spending a substantial amount of time each day probing all of the different systems, I can now just perform a cursory inspection. Using Cisco IOS Security Services embedded in the Cisco router has significantly reduced the time that I have to devote to security tasks and the effort required to keep us secure.”

Being able to support services that previously required three separate devices with a single solution also represents a cost savings. In fact, the Cisco 877 Router actually costs less than what Scotweb had paid for the standalone firewall and the server running the IDS. As Scotweb continues to grow, the ability to manage those services with a single device will allow the company to invest its resources in other business priorities.

The most important benefit of the Cisco IOS Security services, however, is that Scotweb can now deliver higher availability and a higher level of service to the company’s demanding healthcare customers. For example, when a software update is released to correct a vulnerability, the Cisco IOS IPS provides such tight control of network traffic that Simpson doesn’t have to rush to implement the patch, and doesn’t have to disrupt service.

“In the past, if a vulnerability came out, I had to react immediately,” says Simpson. “Regardless of what a server might be doing, it needed to be patched and rebooted then and there. With the Cisco IOS Security services, I can wait until the middle of the night, when users won’t be affected. It gives me the extra leeway and flexibility that I need to help ensure minimal downtime for my users who are depending on this system.”

PRODUCT LIST

Routing and Switching

- Cisco 877 Router

Security and VPN

- Cisco IOS IPS
- Cisco IOS Firewall

For More Information

To find out more about Cisco IOS Security solutions, visit

<http://www.cisco.com/go/iossecurity>.



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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered 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. (0903R)