



Vault-Like Protection for 200 Financial Services Locations

A Case Study in Network Security

“The drag-and-drop VPN is an awesome thing. We tell the WatchGuard device to contact the home office, and ship it to the branch. Then we walk the people there through plugging in the cables. As soon as they plug it in, we see it from here. We do a drag-and-drop VPN, set the IPs, select our content-filtering rule from the drop-down menu, click ‘next’ about five times, click ‘finish’ and it’s done. Their Internet comes right up.” Corey Gary, Network Administrator, Southern Management

BACKGROUND

From its headquarters in Greenville, SC, Southern Management Corporation operates more than 200 financial services branches across six states. These locations provide tax services, offer personal loans, and accumulate a confidential cache of personal financial data that the company must protect. With a widespread territory to cover and a small IT staff, they needed a distributed security system that was tightly locked down and easy to administer. They found the perfect solution in WatchGuard®.

CHALLENGE

Each branch office has at least two computers, one configured for loans, another for tax work. On a daily basis, the data is transferred via a VPN tunnel to the corporate data center for storage, back-up, and auditing.

Corey Gary is the network administrator at Southern Management. When he arrived on the scene, he inherited a Symantec firewall and branch offices protected with basic SOHO-class routers. Reliability in the branches was sporadic. “The Internet was constantly dropping,” he recalls. “That’s 100% critical to the business.” Connection to the corporate data was lost, and loan processors in the branches could not pull credit reports or access other credit data.

So Gary began looking into a new firewall system. “I looked at Cisco and I looked at a bunch of other options - Sonicwall, Snapgear and others,” he says. “I had worked for an ISP and all I had ever used was Cisco, at least on the enterprise side of things. But we didn’t want to put a Cisco at each one of our branches, because we don’t have technical support there in case something goes down. It’s really hard to walk somebody through Cisco IOS if they don’t know anything about computers.”

WATCHGUARD® SOLUTION

The search for centralized security led to a series of referrals that in turn, led Gary to WatchGuard. He tested an evaluation unit and liked what he saw. He settled on WatchGuard Firebox® X Edge 10e-W’s for the branch offices and a Firebox X Peak™ 5500e for headquarters.

The first step was swapping out the old router. He recalls, “We put in the Peak box and ran it in parallel with our old router. Then my partner and I came in on a Saturday and Sunday and rolled out the whole deal, switching over 200 VPNs and all the policies, adding them into the Peak X5500e and getting the e-mail and everything working. It was very, very simple and easy to roll out considering the ‘damage’ we were doing.

“Luckily, two days later, the old router died on us. Literally, it completely died and shut down, and would not allow access to it. So we got the WatchGuard appliance just in the nick of time.”

BENEFITS

With the Peak unit in place, Gary began distributing all 200 Edge X10e-W’s to the field. Branch-by-branch, the dropped connections disappeared. And he began to discover the full ease-of-management of WatchGuard.

Drag-and-Drop VPNs, from South Carolina to Oklahoma

With the home office in Greenville and branches as far away as Texas and Oklahoma, travel for on-site installs would be prohibitively expensive. “We have nobody technical on site at any of the branches,” says Gary. “So the drag-and-drop VPN is an awesome thing. We tell the WatchGuard device to contact the home office, and ship it to the branch. Then we walk the people there through plugging in the cables.

“As soon as they plug it in, we see it from here. We do a drag-and-drop VPN, set the IPs, select our content-filtering rule from the drop-down menu, click next about five times, click finish and it’s done. Their Internet comes right up.”

And Gary says overall management is very simple. “We love the WatchGuard System Manager. I’ve been told that not every customer has been using it, and that most people just manually configure their

WatchGuard devices and let them sit. But for us, we absolutely have to have that central management piece. WatchGuard was the perfect solution for us.”

Financial Security – and Peace of Mind

Southern Management applies an extremely restrictive security policy: No inbound traffic from the Internet. Traffic is only allowed through the VPN. Web traffic goes through the main corporate connection and is subject to tight content filtering. And the wireless connections – used by visiting supervisors and directors who need to connect with headquarters – are subject to the same tight restrictions. WatchGuard’s heritage as a security device rather than a general-purpose router, with a highly secure configuration out of the box, made it ideal.

“Every time I put a WatchGuard appliance into a branch, I don't have to worry about it,” declares Gary. “We have financial information, including social security numbers. We lock our content filtering down to where people can't go to a bad web site and get a virus that's going to let somebody into their computers. We have five or ten sites that they can go to, and they're all credit related. Other than that, they can't go to Google, they can't go to MSN, Yahoo, anything.”

“WatchGuard has been awesome at locking that down. We created a rule in our WatchGuard System Manager to create a DNS proxy and state that any traffic coming over the VPN has to go through the proxy. We put in whatever sites we're going to allow, and deny everything else. That's it.”

So Intuitive, “It's Been Fun”

Gary and his team are nearing the end of the rollout and are just now thinking about getting training and certification on the WatchGuard devices. He admits, “I'll be honest with you, I've never read the manual. The sales engineer sent me an email once, with a small little piece on creating the VPN templates. In fact, I'm not sure I've ever seen the manual.

“The support has just been awesome. I get somebody who is pretty much dedicated to us whenever we need them. We appreciate all the help, and we've had some good times with it. It's been fun, actually.”

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has been building award-winning network security solutions that combine firewall, VPN and security services to protect networks and the businesses they power. These fully extensible threat management (XTM) solutions feature reliable, all-in-one security, scaled and priced to meet the unique security needs of small businesses to medium sized enterprises. Our products are backed by 7000 partners and 450 employees representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including healthcare, education, and retail. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and Firebox are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66611_072409