



Gavel-to-Gavel Protection for a High-Profile Event

A Case Study in Network Security

“There were going to be people smarter than us, seeing a WatchGuard device and trying to get around it. I gave all the configs to everybody at WatchGuard and had them try to hack it. Then after we ran everything through WatchGuard engineering, they turned the configs over to a third-party hack team that they use. They couldn’t break it, either.” Eric Frydenlund, Senior Engineer, CIT

BACKGROUND

The eyes of the world were on St. Paul, Minnesota – host city to the 2008 Republican National Convention. Approximately 45,000 delegates and alternates, party dignitaries, volunteers, guests and members of the media were poised to converge on the city. Teams of organized protesters were waiting as well, bent on grabbing a piece of the limelight. Meanwhile, black hats around the world were preparing to penetrate the city’s infrastructure and impact the public safety response.

The police department was ready, thanks to longtime relationships with WatchGuard Technologies and also with CIT, a technology solutions firm serving the cities of Minneapolis and St. Paul. Both companies played instrumental roles – from the earliest planning to the final gavel.

CHALLENGE

Two years of planning in conjunction with federal authorities made it clear what the city was up against. “We had a lot of contact back and forth with the FBI, Homeland Security and other intelligence agencies,” recalls Karen Edmond, Information Systems Consultant for the St. Paul Police Department. “They gave us information and intelligence about the kinds of activities we could expect, and who would be making them – attempts to disrupt our communications or police operations.

“Also, there were the sensitive documents of the convention to protect,” she says, “the schedules of individuals and information and timelines around convention events. Those secrets could be in emails or in documents that came through secured channels. They might be sitting on a drive on the network, a PC or a notebook. We needed to protect all that information.”

WATCHGUARD® SOLUTION

To prepare for the event, CIT upgraded the department’s security with a pair of Firebox® X Peak™ 5500e units, configured for high availability with active/passive failover. These protected the main police operations including the computer-assisted dispatch system, internal information systems, 300 desktops at headquarters, and wireless connections to 700 laptops in the patrol cars. They also secured the connections to the state of Minnesota and federal information systems.

More than 100 closed-circuit TV cameras deployed at various sites around the city were a special concern. Connected locally through unsecured fiber and wireless links, they were an especially tempting intrusion target and a potential entry to the police network. So a third X5500e unit was dedicated to firewalling between the camera network and police network. WatchGuard also provided a fourth X5500e unit on loan at no charge. It was on standby at police headquarters if needed during the convention.

BENEFITS

The WatchGuard appliances handled an extraordinary amount of traffic during the convention. There were many newsworthy incidents, but no security incidents. That was a testament not just to the devices, but extraordinary measures taken by WatchGuard and CIT to harden the security configuration.

Intrusion Prevention Taken to the Ultimate

CIT and WatchGuard pulled out all the stops to prepare for a dynamic situation. Eric Frydenlund, Senior Engineer with CIT, recalls, “I attended the WatchGuard partner conference and met with literally everyone at WatchGuard, notifying everybody that this event was coming up. I said, „We need more support than you’ve ever given out. We are going to have to respond at warp speed, and we won’t have time to analyze logs. I can’t tell you what’s going to be coming. But we have to be able to respond.””

Frydenlund devised a configuration and called on all of the support services of WatchGuard to verify it. As he explains, “There were going to be people smarter than us, seeing a WatchGuard device and trying to get around it. I gave all the configs to everybody at WatchGuard and had them try to hack it. Then after we ran everything through WatchGuard engineering, they turned the configs over to a third-party hack team that they use. They couldn’t break it, either.”

Nothing was left to chance, as Edmond recounts. “The city of Saint Paul also contracted with a third party, because they wanted an objective look at the system. During the pen test, I opened some of the ports for them. In the first 16 hours, they were not able to penetrate. Then, I wanted to know if the WatchGuard devices really worked, so I closed the ports without telling them. Once I closed the firewall to them, they didn’t get anything. The contractor said, „You gave us the wrong IP.””

Billions of Packets Passed, Millions Blocked Daily

Throughout the convention, the WatchGuard units did everything that was expected of them – and beyond. Edmond gained an idea of the magnitude on the first day of the convention, when after a reset she happened to glance at the traffic counters. “I usually just glance at that stuff,” she recalls, “but in this case I was paying attention, and noticed we were getting billions of hits.”

On day three of the convention the police-department firewall logged six billion packets and the closed-circuit camera firewall processed almost two billion. Then, says Edmond, “On the fourth day there was a huge event, where they had blockaded all these people on a bridge over the freeway. A ton of people were all trying to view the camera system.” The traffic on the CCTV firewall more than doubled to almost four billion. The ability to withstand such a barrage, according to Edmond, “speaks to the quality of the product.”

During the convention, the WatchGuard appliances denied approximately twenty million packets per day. Investigating the source IPs identified a large number coming from one foreign country in particular, and from militia groups based in the U.S. that are well known to law enforcement and the security community.

‘We Could Not Allow for a Failure’

The stakes were incredibly high for everyone involved. Declares Frydenlund of CIT, “St. Paul had never seen anything like this before. It’s not often that you have a global event with viewership on 28 network channels, morning to night. If it went off transparently without a hitch, everybody would be happy. If it didn’t, people would say that the city of St. Paul and everyone involved had failed. We could not allow for a failure.

“We had the loaners, we worked directly with the WatchGuard VP of Support to secure a lot of support avenues, and we set up special support lines with cell numbers. They were all on standby just in case something happened. The planning paid off. We didn’t have to use any of them.”

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 has been building award-winning unified threat management (UTM) network security solutions that combine firewall, VPN and security services to protect networks and the businesses they power. We recently launched the next generation: extensible threat management (XTM) solutions featuring reliable, all-in-one security, scaled and priced to meet the unique security needs of every enterprise. Our products are backed by 15000 partners representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including retail, education, and healthcare. WatchGuard is 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. WGCE66654_092409