



# Countywide Government Network Stays Secure with WatchGuard Solution

## A Case Study in Network Security

### **BACKGROUND**

The Goshen County government operates one of the most advanced networks in the state of Wyoming. The county hosts its own Internet server, has its own WAN and a private/public co-op using a VPN to link data and services to the state government and other law enforcement networks. The county also operates a 180-extension VoIP phone system with remote locations over a LAN, as well as WAN and VPN connections. Additionally, the county offers free Wi-Fi service with both a public and a private network.

"We support all government entities in the county," explains Matt Rolf, IT Director for Goshen County. "Every firehouse and police station in the county is on the network. Some of the small town governments in Goshen County use our network as well. We supply them with software, desktops, tech support, email, web hosting, and in some cases Internet access. This is cost-effective for small towns that might have only two employees working in the town hall, who can't afford tech support or their own IT system. Working off our network saves them money and costs us practically nothing. And it makes things productive for all citizens of the county."

### **CHALLENGE**

As the Goshen County government network has grown, so has the need for enhanced security to protect mission-critical services and government information. As a government agency, they are responsible for protecting confidential data according to government compliance standards, including Criminal Justice Information System (CJIS) security policies set forth by the FBI.

Goshen County faced a number of challenges in finding an effective security solution for its network. First, the solution had to be robust and scalable enough to handle the ever-increasing number of VPN connections and Internet-based applications on the network.

In addition, the security solution needed to be cost effective. Goshen County's entire annual budget is \$6.2 million. Its annual IT budget is \$120,000, including salaries. With the high cost of commercial bandwidth, the county cannot afford leased lines and uses residential services for its network.

The low quality of Goshen County's residential-grade Internet providers posed another challenge. Goshen County uses cable, DSL, and wireless providers, and one of these will typically go down every day. The county cannot afford a connection with guaranteed uptime, so the security solution needed to provide redundancy, as well as failover that would not be noticeable to the end user.

A special concern was the county's ability to offer free Wi-Fi services to the general public in its government buildings, while still protecting the county's private network from potential outside attacks from wireless-capable devices.

## **WATCHGUARD® SOLUTION**

After consulting with WatchGuard® Technologies about Goshen County's security needs, Rolf selected and installed a WatchGuard Firebox® X Core™ 750e appliance with a Fireware® Pro advanced appliance software enhancement. The X750e appliance allowed Goshen County to unite its multi-site network environment under a single unified threat management (UTM) solution, in compliance with CJIS regulations.

During the initial consultation, WatchGuard referred Rolf to CDW-G, the division of Computer Discount Warehouse that sells IT products and services for government clients. Rolf purchased the WatchGuard products he needed from CDW-G and did the installation himself. "WatchGuard offered the only security solution that could affordably handle more than two ISPs. CISCO wanted \$25,000 for a similar solution. I also looked at Juniper and SonicWall, but they could not provide the solution we needed." said Rolf. "And it was a relatively painless installation."

"WatchGuard was the only company that had enough confidence in their technology to offer us a free one-month trial," Rolf commented. "They gave us time to test the product and see if it was what we really wanted."

## **BENEFITS**

### **Reliable, Secure Connections for Multi-Site Networking**

The X750e with Fireware Pro can handle up to four ISPs, provides multi-WAN load balancing, and delivers application layer security and remote location encryption for multiple VPN tunnels.

WatchGuard Firebox allows the secure exchange of government information over Goshen County's network, while providing proactive, multiple-layered inspection of network traffic to block cyber attacks. All network traffic on Goshen County's LAN is locked into the internal firewall known as the "Trusted Interface Zone," which allows no traffic except what is specifically designated by Goshen County's security policies. All inbound and outbound traffic on Goshen County's LAN passes through the Firebox's various proxy policies where it is scanned for viruses, spyware, and other malware, and logged.

"A few months ago, we had a Distributed Denial-Of-Service attack," said Rolf. "The attacker sent us a deluge of malformed packets designed to block up the traffic on our network. Receiving 10,000 packets per second overwhelmed our network. The WatchGuard Firebox firewall blocked the attacks, but we still had to process traffic on the network. We used the Firebox System Manager to monitor network traffic to see what was hitting in the interfaces. Using this information, we were able to coordinate with our ISP providers to stop the attack."

### **Effective Security for Public/Private Wi-Fi Access**

The Firebox X includes security options that allow Goshen County to provide regulated Internet access to certain users through the county network, while still protecting confidential government information. For example, Goshen County has free public Wi-Fi access for wireless-capable devices in government buildings. The government also has agreements with organizations and programs that are considered "non-trusted entities" who are not official government agencies but occupy office space in the Goshen County government buildings.

On the Goshen County network, all outbound Internet traffic from public wireless users and non-trusted entities is routed through a special security interface on the WatchGuard firewall known as the "DMZ." With the DMZ option, public Wi-Fi users and non-trusted entities have access to the Internet through Goshen County's ISPs, but are isolated from accessing the county's government network. The DMZ interface includes security options set up by Goshen County to regulate Internet access by these users. For example, all Internet traffic from public Wi-Fi users through the DMZ is limited to an access speed of 256k.

### **Redundancy**

The X750e provides redundancy to Goshen County's DSL, cable, and wireless ISPs using a "round-robin" checking system. The firewall moves traffic between all three ISPs to share bandwidth, and periodically pings each ISP to make sure it is still working. If the pinged ISP returns three failure responses, the firewall determines that the ISP has gone down, and directs traffic to the other two ISPs. When the ISP is restored, the firewall pings it again, and must receive three positive responses before it allows traffic to be routed onto the ISP once more.

By upgrading to Fireware Pro advanced appliance software, which enables policy-based routing, Goshen County can direct traffic to a designated provider based on the traffic's source, destination or protocol. For example, Fireware Pro uses policy-based routing derived from protocol to route all outbound email traffic from Goshen County's network over a specific ISP. If this ISP fails, the Fireware Pro software has a specific failover order that automatically re-routes all outbound email traffic over another ISP. The same principle applies to web-browsing traffic and outbound VoIP on Goshen County's network.

### **Real-Time Bandwidth Utilization Monitoring**

Goshen County came to rely on the Firebox's real-time bandwidth utilization monitoring feature, which allows the county to monitor the use of its networks. "With real-time bandwidth utilization monitoring, we can monitor our ISPs," said Rolf. "If we are not getting as much access as we should, we can contact the provider about it. It makes me feel better to know what's going on in the network."

### **Dependable Products, Exceptional Support**

Rolf has also been impressed with the reliability of the appliances and software from WatchGuard. "We've never had to replace WatchGuard's technology, and it has never failed. We feel comfortable with the WatchGuard support agreement behind it. The WatchGuard LiveSecurity® plan is designed specifically for IT professionals like me. It gives me peace of mind to know that WatchGuard is there to help when I need them."

For more information about WatchGuard security solutions, visit us at [www.watchguard.com](http://www.watchguard.com), or contact your reseller.

---

#### **ADDRESS:**

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

#### **WEB:**

[www.watchguard.com](http://www.watchguard.com)

#### **U.S. SALES:**

1.800.734.9905

#### **INTERNATIONAL SALES:**

+1.206.613.0895

#### **ABOUT WATCHGUARD**

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest products – the WatchGuard SSL 500 and SSL 1000 – make secure remote access easy and affordable, regardless of the size of your network. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit [www.watchguard.com](http://www.watchguard.com).

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. ©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Firebox, Fireware, Core, and LiveSecurity 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. WGCE66518\_072409