



## Oil and Gas Business Solutions Company Has a Direct Pipeline to their Customers

A Case Study in Network Security

*“Over the past year with the WatchGuard appliance, it’s basically been ‘set and forget’. I check once in awhile and make an exception in WebBlocker and that’s it. I don’t even have to think about it any more. I just make sure that the policies are correct.”* **Nicholas Connor, Manager, Information Technology, WellPoint Systems, Inc.**

### BACKGROUND

WellPoint Systems is a leading supplier of business information solutions to mid-tier oil and gas companies. Their BOLO product line provides US Upstream Oil & Gas companies with innovative financial management software solutions tailored to the specific requirements of the industry. They offer a fully integrated suite of land, production and accounting, combining powerful data processing with robust reporting functionality – helping companies run their businesses better. BOLO by WellPoint products meet the changing needs and complexity of oil and gas accounting, land, and production departments.

In their search for a solution to their network needs, WellPoint worked closely with Saje Professional Services. Saje, a WatchGuard Partner, provided assistance in planning, design, implementation, and support of the BOLO network.

### CHALLENGE

BOLO’s customers exchange sensitive and important financial data, relying on dependable and secure connections to BOLO Customer Support and the WellPoint network from their offices. There is no

room for dropped connections or extensive down-time when dealing with highly critical business processes and business data. Nicholas Connor, Information Technology Manager at WellPoint Systems, Inc., explains the situation, “We need reliable VPN connectivity back to the BOLO server so that our consultants and customer care groups can support a customer’s in-house servers or our ASP environment.” With over 120 VPNs to manage and secure, both internal and customer-facing, Connor faced problems maintaining solid connections, “We encountered a lot of glitches when using customer or third-party hardware to set up VPN tunnels. Configuring against these other devices was a VPN nightmare. Connections were dropped causing a lot of time to be spent on support calls.”

WellPoint also faced the challenge of keeping their numerous international and domestic offices connected. With offices in Canada, South Africa, Tunisia and Denmark, as well as several in the United States, keeping secure connections alive was a high priority for WellPoint.

## **WATCHGUARD® SOLUTION**

With proven results from configuring VPN tunnels from WatchGuard device to WatchGuard device, WellPoint made the decision to include a WatchGuard Firebox X Edge 10e appliance as part of their BOLO connectivity solution. Connor explains, “We buy the X10e for the customer and bundle it as part of the sale, we then put the firewall in a DMZ or assign it a public IP address, configure it as a VPN endpoint, plug it into the second network interface on the BOLO server and it provides a direct connection between us and our customers.”

Setting up secure VPN tunnels with customers wasn’t a problem for Connor. “We have a myriad of connectivity methods back to customers but the most secure and easiest for us to set up is a hardware based VPN using WatchGuard equipment... specifically an IPSec tunnel with AES as it offers the best encryption. All of our boxes need a high level of security and encryption for a connection back to the WellPoint network and that’s why we use WatchGuard,” says Connor.

## **BENEFITS**

### **Time Savings Translate to Cost Savings**

With third-party connection problems plaguing WellPoint, Connor was spending unnecessary time trouble-shooting bad VPN connections. Connor laments, “Before we deployed the WatchGuard devices, I was probably on the phone 4-6 hours a week trouble-shooting VPN connectivity back to customers. This was very frustrating for us, as well as for our customers. The connectivity solution saved a great deal of time and increased customer satisfaction. We just don’t have those issues anymore... it’s just gone away.”

When BOLO was acquired by WellPoint the decision was made to switch to WatchGuard. BOLO had a history of success with WatchGuard appliances and the ISA servers that were in use presented their share of problems “The ISA servers presented huge challenges when configuring VPN tunnels, it was painful at best, they dropped a lot, logging was terrible. It took 15 to 20 minutes to process a change and see if the change made was the one you wanted. With WatchGuard our tunnels are incredibly stable,” explains Connor. That stability is of utmost importance in conducting business for WellPoint. Says Connor, “Branch offices rely on Denver for Exchange and SharePoint among other applications. We need the connection to be stable for employees to do their work. With Firewall® the IPSec VPN and MultiWAN support is outstanding.” With downtime a thing of the past, employees remain productive at all times.

### **Management Made Easy**

In order to maintain the 120 plus VPN tunnels internally and externally, Connor needed a security solution that delivered easy-to-use and intuitive management. With the implementation of WatchGuard devices

across the board, Connor got what he needed. "I've seen the other products - Cisco, Sonicwall, Checkpoint - and the WatchGuard interface is a lot cleaner and easier to manage than the other devices," he says.

### **What's good for the Customer...**

WellPoint not only provides their customers with the robust protection of WatchGuard appliances, but also relies on these appliances to provide secure connectivity and unified threat management (UTM) within the organization. "We use Firebox X Core 550e and 1250e and Firebox X Edge 10e and 20e appliances in our offices," (in Canada, Tunisia, Denmark, South Africa, and the United States) Connor reports. He's noticed increased performance at all locations, "We brought Calgary up first in February of 2008. Prior to that our VPN would bounce two or three times an hour, throughput was terrible. VPN throughput was doubled with WatchGuard. We brought up the other offices in June and July and saw significant improvements all around, especially in South Africa where latency is always an issue."

### **Cost Savings and Peace of Mind**

Spare time to review and approve quotes for security subscription renewals is not a luxury that most IT Managers have. With that in mind, Saje Professional Services suggested that Connor implement the UTM Suite with a common expiration date for all services provided. Cindy Cary of Saje Professional Services explains, "Since Bolo utilizes more than one of WatchGuard's security services on their corporate firewalls, it made sense to offer them the UTM Suite. For convenience, we suggested that Nicholas select a date to have all of his corporate firewall security subscriptions renew." By implementing the bundle, Connor and WellPoint were able to recognize significant cost savings and avoid the headache of multiple renewals. Cary continues, "WellPoint was able to save 42% by going with the UTM Suite, Nicholas doesn't have to worry about subscription renewals for well over a year, and there was still money left in the budget for HA, providing peace of mind for a busy IT department facing a myriad of daily challenges."

### **Set and Forget**

For Connor, the daily support calls are a thing of the past. With WatchGuard devices in place he is able to focus on other important aspects of his job. "Over the past year, with the WatchGuard appliance, it's basically been set and forget," he explains. "I go in once in awhile and make an exception in WebBlocker and that's it. I don't even have to think about it any more. I just make sure that the policies are correct."

WatchGuard products have made life easier for Connor and the WellPoint organization and improved their level of service to their customers. "We've solved each and every one of the huge pain points by dropping in a WatchGuard box. That said, we've had a number of customers who have bought WatchGuard devices to use as their primary firewall after their experience with us."

---

**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 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. WGCE66643\_072709