



ACS Aviation uses WatchGuard to make its global connections from Melbourne to Dublin.

As the global economy continues to unify, the global demand for flights rose 7.5 percent in August compared to last year.

As more travelers take to the air, the need for the airlines to be aligned on compliance issues and international standards continues to be in high demand. This is why ACS Aviation Solutions has experienced tremendous growth. Along with that growth has come tremendous demand on its network that supports a global, remote staff of 70 field workers, analysts and consultants. ACS runs an enterprise-grade IT infrastructure and needed bulletproof security, powerful centralized management, and fail-over capability for always-on high performance. Photo Courtesy of Wikipedia: http://upload.wikimedia.org/wikipedia/commons/d/dc/Boeing_B-17G.png It found that solution with WatchGuard's XTM unified threat management (UTM) platform. ACS deployed XTM appliances across its global offices to support its staff. ACS needed a solution that was secure for employees, but also provided access to its customers to highly sensitive documents and reports. Given the nature of ACS' work, all data is highly confidential and security is paramount as it routinely communicates with global regulatory bodies. Additionally, it needed to have the failover that large enterprises expect from a unified threat management system. In fact, the WatchGuard system was quickly put to the test after being implemented. The domain controller in ACS' Dublin office went down due to a hardware interruption. Because the server was not available, Dublin traffic was rerouted through Melbourne, enabling all staff to log on and operate as normal with no experienced downtime. ACS plans to begin using WatchGuard's UTM platform to manage VPN connections for remote users, ensuring validation of connections occurs at the firewall, rather than in the server. This is like a doorman who asks visitors to wait outside while he checks their credentials, rather than first inviting the stranger in. The upshot is that traffic is validated between the firewall and the server, rather than between the server and the user. It's an important distinction as it provides yet another layer of protection for the network.

Since implementing WatchGuard's UTM platform, ACS has been able to experience the benefit of a secure network that hosts the company intranet, supports collaboration due to ease of document sharing, and provides reliable, robust disaster recovery capability. WatchGuard XTM is a great fit for any business and our extensive lineup of appliances means that there is one that fits your needs. If you're ready to learn how WatchGuard can fit into your business, learn more about WatchGuard now.

You can also read the full details of the case study below. Background ACS Aviation Solutions is a leading global professional services organisation that specialises in compliance, safety, and operational excellence in the aviation industry. It is one of only eight companies worldwide – and the only organisation in the southern hemisphere – authorised by the International Air Transport Association (IATA) to conduct safety audits on airlines. Other services include operational reviews, specialist aviation training, recruitment, finance and leasing. For more than a decade, the company, which maintains offices in Melbourne, Dublin and Tokyo, has successfully completed hundreds of projects around the world, working with large international carriers and small local charter operations.

Challenge: Protecting the Network from Intruders Jorge Silveira, IT Manager of ACS Aviation Solutions, describes the organisation as a small business with a considerably large network management requirement. "We run an enterprise-grade infrastructure with virtual machines, thin clients, physical computers, high availability servers, Windows services, backups and more," Silveira explains. From an IT perspective, ACS has approximately 20 power users working across the three offices, plus another 50 auditors and field workers who require remote access. Given the nature of ACS' work, all data is highly confidential and security is paramount.

Deploying Cutting-Edge Security from WatchGuard To protect the network, Silveira deployed a WatchGuard XTM 330 unified threat management (UTM) appliance in the Melbourne office. The XTM 330 is designed for small enterprises that require the next-generation of network security. It combines firewall functionality and a suite of security options with fast throughput and advanced networking features, including state-of-the-art management and reporting tools. "I was looking to increase security and had worked with WatchGuard products before," says Silveira. I like the fact they [WatchGuard appliances] are easy to use, have an excellent user interface, and they offer enterprise-grade features at low cost. In terms of traffic monitoring, I can log into the system and monitor what comes in and out of the network. I can see what traffic has been blocked and can determine whether it should be allowed or not."

Shortly after deploying the XTM appliance, ACS upgraded its internet to fibre. "With that [fibre], we got a range of IP addresses and WatchGuard has been able to handle all those addresses correctly, exactly the way I want them handled within the network," explains Silveira. "For example, one address is used for remote users, another is for Internet traffic, another is for telephony traffic, and so on."

A Melbourne to Dublin Connection When ACS relocated its Dublin office, Silveira used the opportunity to deploy a second WatchGuard XTM 330, which he then connected to the XTM in Melbourne, creating a secure site-to-site connection and a highly reliable virtual private network (VPN) tunnel. Next, using the tunnel and Windows 2012 Server replication capabilities, Silveira set the system up so that all activity on the Dublin server would be replicated in Melbourne in real time, and so that all Melbourne activity would be replicated in Dublin. The result– a secure network that hosts the

company intranet, supports collaboration due to ease of document sharing, and provides reliable, robust disaster recovery capability. "It allows people to view our infrastructure as one single network," notes Silveira. "If anything happens to users in one site, they can still securely access their files from the other."

WatchGuard Keeps Data (Securely) Flowing The infrastructure was tested earlier this year when the domain controller in Dublin went down due to a hardware interruption. Because the server was not available, Dublin traffic was rerouted through Melbourne, enabling all staff to log on and operate as normal. "The WatchGuard XTM 330 is not just a firewall. Yes, we use the firewall component, but we also use the gateway to create a branch-to-branch VPN tunnel," Silveira adds.

Moving Forward with WatchGuard In the next few months, Silveira plans to begin using the XTM appliance to manage VPN connections for remote users. This will ensure validation of connections occurs at the firewall, rather than in the server. Silveira likens the approach to a doorman who asks visitors to wait outside while he checks their credentials, rather than first inviting the stranger in. The upshot is that traffic is validated between the firewall and the server, rather than between the server and the user. It's an important distinction as it provides yet another layer of protection for the network.

Silveira admits that there's a great deal of functionality on the XTM 330 that he has yet to tap. He hopes to use the devices to establish a fully redundant internet connection for both the Melbourne and Dublin sites before the end of the year, and is interested in pursuing Application Control further down the line. "WatchGuard products are very attractive for the price they charge and their support is among the best I've ever had. The company's response times are unbelievable. WatchGuard has definitely enabled ACS to take the next step in expanding the business internationally by providing office-to-office communication and a pretty bulletproof disaster recovery system," Silveira assesses.

LogicalTech is one of the leading Professional Partner with WatchGuard Technologies in Australia. Find out more by contacting an authorized WatchGuard reseller, LogicalTech today. This partner product release is submitted by Cassidy Poon, National Marketing Manager for LogicalTech Group and Cassidy Poon is one of Australia's leading technology media publicist for B2B Enterprise Technology.

Contacts

Cassidy Poon
0386436448
mailto: cassidyp@logicaltech.com.au