

Customer Situation

The Wisconsin cities of Fitchburg, Middleton, and Sun Prairie made a strategic decision to collaborate on a joint effort to provide common records management, dispatch, and locationing services for and between their individual municipal police and fire departments. A joint task force with members of each of these cities was formed and named the Multi-Jurisdictional Public Safety Information System (MPSIS) team.

Within the network, the records management has the most information, however, the dispatch systems, locationing services and database access are critical components of the network, requiring connections between the three cities to remain available at all times. Fitchburg serves as the centralized network hub, the area data center and the location of the network administrator.

The network had been in place for a number of years using relatively slow T1 links to connect Middleton and Sun Prairie police departments to the Fitchburg network hub. MPSIS recently approved a project to upgrade these network connections to high-speed wireless.

CASE STUDY

Municipal Wireless

Shared wireless network encrypted without changes to infrastructure



Solution Requirements

The RFP issued by MPSIS for the network upgrade required the connections to Middleton and Sun Prairie operate over native Layer 2 links to preserve the existing IP network addressing scheme, maintain the performance of high availability applications running on the network, and to avoid disruptive architecture changes to the network infrastructure. MPSIS had already determined that in the event of a server outage, failover to a back up server would take several minutes in a routed network, as opposed to seconds in a switched network. This gap in availability could present a public safety issue and was not acceptable. All three police departments require uninterrupted access to data and the dispatchers must maintain location awareness of the squad cars in the field.

With all three police departments accessing both state and federal databases, the upgrade needed to comply with the Criminal Justice Information Services (CJIS) security requirements. As part of that compliance, the existing traffic from the network hub to the Fitchburg Fire Department would have to remain in clear text and separate from the Police Departments traffic. This requirement for data segmentation was a particular concern for MPSIS as the inability to preserve this existing link would increase the overall cost of the project.

Building Process

MPSIS released the RFP and received five bids. Two of the bids proposed wireless radios with built-in encryption. The three remaining bids proposed wireless network connections, but did not address the CJIS security requirements.

After weighing the alternatives it was decided to go with a wireless network solution due to concerns regarding the overall cost, bulkiness and slow performance of the radio solutions. A wireless network solution, however, did not address securing the information over this connection. MPSIS determined encrypting data on the wireless network was the most efficient and effective method of securing the wireless connections between the towns and complying with CJIS security requirements. Accordingly, the remaining vendors were told that a third party solution for the wireless encryption had to be found prior to awarding the bid. One of the wireless equipment vendors recommended that MPSIS look at the Certes Networks solution.

MPSIS looked at the policy and key management solution and the low-latency encryption appliances as an option that would meet each of the requirements for native Layer 2 security, availability, performance and cost. After a brief evaluation, the bid was awarded and the wireless vendor who recommended the Certes Networks encryption solution.

Deployment

After the contract was awarded, MPSIS planned a simultaneous installation, but it became clear that the delivery of the wireless network would take longer than the encryption solution. They decided to take delivery of the encryption equipment and wait until the wireless vendor was ready. As part of the standard purchase agreement, installation support was offered once the customer was ready to roll out the solution.

Upon receiving the encryption solution, Matt Prough, the network administrator for MPSIS, read through the installation guide and had this to say:

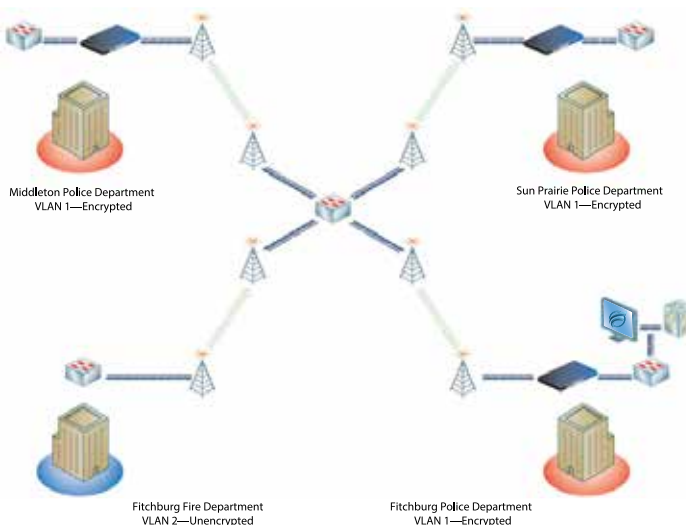
“I was impressed with the simplicity of the design and the straightforward installation documentation I received, so I decided to pre-stage the solution on my own. Setting up the encryption for the network hub and all three cities only took me a couple of hours and required just a brief phone call for assistance in setting up specific policies in order to preserve and cryptographically segment the police VLANs with encryption, while maintaining the flow of unencrypted traffic to the fire department.”

Once the wireless solution was installed, it was a simple matter of deploying the solution on the new network. Again, the network administrator did this without the need for onsite or phone support.

Results

Since the installation, the high-speed encrypted network has been running without interruption or performance issues and has met all of the requirements for security, performance and cost.

“The simplicity of policy and key management has enabled us to protect our sensitive data in a way that was never possible before” said Prough. “It is a simple solution to an otherwise complex problem. We deployed the entire solution in a matter of hours and found it to be simple to use and transparent to our network and our applications. Certes Networks has given us the flexibility to protect our data network-wide without having to change the way we use our network.”



Adding the Certes Networks encryption solution to this network protects the data between the Police Department sites, while all other traffic remains in the clear.

Because of the positive experience and proven performance of the encryption solution, MPSIS is confident in expanding their encryption solution architecture as new and ever-increasing encryption and regulatory compliance requirements present themselves. MPSIS knows that they have a scalable, robust security solution that will simply overlay onto their network without impacting their network design or operation.

About Certes Networks

Certes Networks protects data in motion. The company’s award-winning CryptoFlow® Solutions safeguard data traffic in physical, virtual and Cloud environments, enabling secure connectivity over any infrastructure without compromising network device or application performance. Companies around the world rely on network encryption products from Certes Networks to protect data, accelerate application deployment, simplify network projects, reduce compliance costs, and improve the return on investment in IT infrastructure.

For more information visit CertesNetworks.com



Contact Certes Networks
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108
Tel: 1 (888) 833-1142
Fax: 1 (412) 262-2574
CertesNetworks.com

North America Sales
sales@certesnetworks.com

Government Sales
sales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
sales@certesnetworks.com

Europe, Middle East
and Africa Sales
emea@certesnetworks.com