CASE STUDY

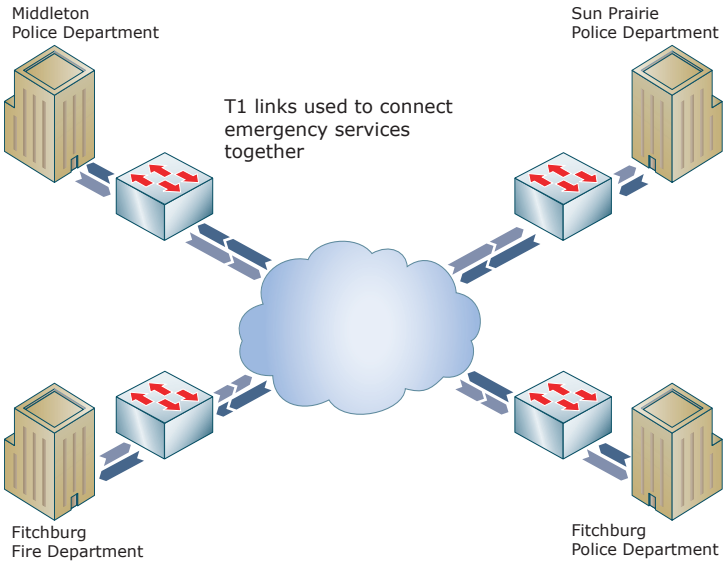
Municipal Security

The 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. The MPSIS team designed much needed upgrades to their shared network infrastructure to facilitate their objectives.

The records management is the biggest part of the network. 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.



The Requirements

The RFP issued by MPSIS required that 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 must have uninterrupted access to data and the dispatchers must maintain location awareness of the squad cars in the field.

With all three police departments requiring access to 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.

The Bidding Process

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

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

MPSIS contacted CipherOptics directly, who proposed CipherEngine and ESG100 Ethernet Security Gateways as a solution that would meet each of the requirements for native Layer 2 security, availability, performance and cost. After an evaluation of the proposed solution, the bid was awarded to CipherOptics and the wireless vendor who recommended them.

The Installation

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

However, upon receiving the CipherEngine 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 CipherEngine 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 to CipherOptics 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."

"The simplicity of policy and key management with CipherEngine has enabled us to protect our sensitive data in a way that was never possible"

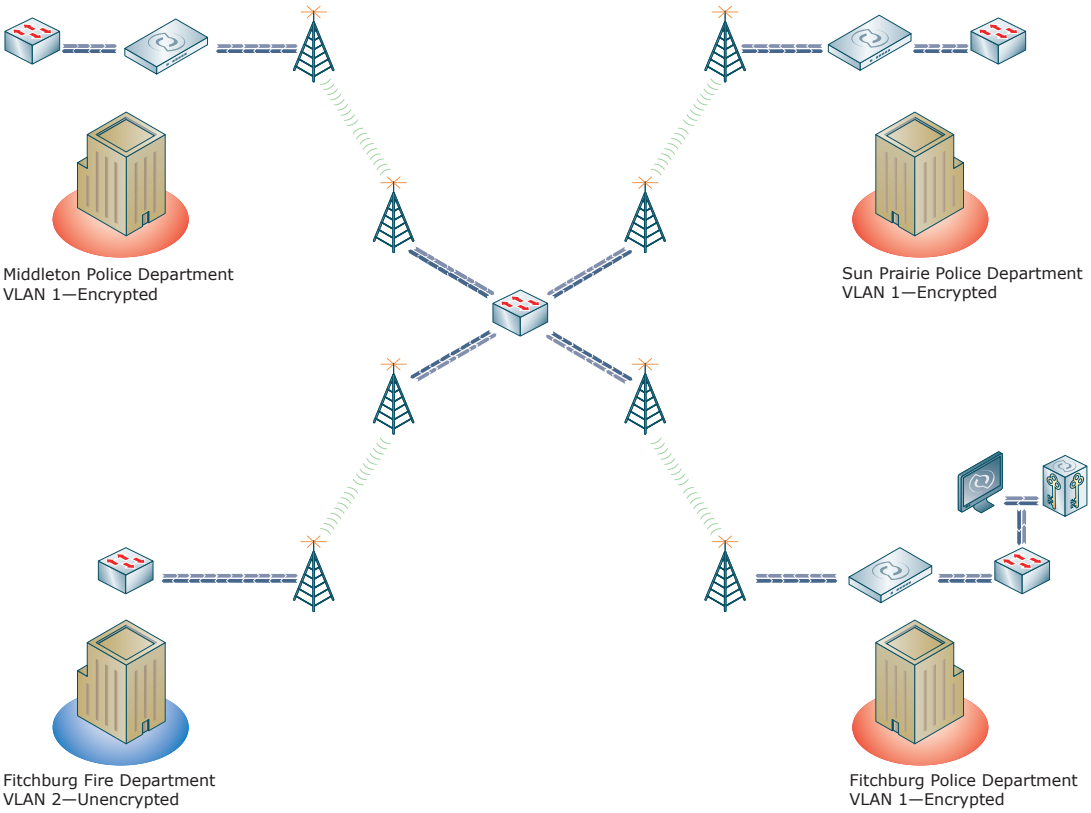
Matt Prough
Network Administrator
MPSIS

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

The 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 with CipherEngine 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. CipherEngine has given us the flexibility to protect our data network-wide without having to change the way we use our network."



Because of the positive experience and proven performance of the CipherEngine solution, MPSIS is confident in expanding their encryption solution architecture with CipherEngine 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.

CIPHER OPTICS
www.CipherOptics.com