City of West Haven, Conn.

Citywide Unified Threat Management Deployment

Case Study

Situation

West Haven, Connecticut is part of the 3rd U.S. Congressional district and is proud to be Connecticut's youngest city having been established in 1715. Contributing to the growing trend in e-government, West Haven proudly deploys technological solutions to increase citizenry communications, internal data management and public safety.

The City of West Haven realized the serious risks of inbound Internet attacks against the municipal network and the need to create an active yet flexible security policy. Additionally, the municipality sought to protect city end users from accidentally going on malicious Websites (e.g. spyware, gray-ware, key-loggers, porn etc). After initial discussions and site surveys with the City of West Haven's Information Technology team, it was determined that a solution was needed to meet the following objectives: 1) provide highly intelligent and secure network Web filtering, active intrusion protection and antivirus scanning throughout the municipality's facilities 2) provide flexible and scalable virtual private networking capabilities on a standard platform with low administrative overhead and reduced total cost of ownership and 3) allow for secure remote access for various aspects of municipal workforce (e.g. inspectors, administration, etc.).

Solution

Working closely with The Business Network Group, a network integration solution company offering sales, service, support, consulting and installation for local and wide area network technologies, the City selected Fortinet to provide a unified threat management solution throughout its enterprise network. The City implemented the Fortinet unified threat management platform by deploying security appliances at sites including: the police station data center, fire stations at six locations, the senior center, public works facility, City Hall data center and building inspectors laptops.

Emergency Services

As part of an Emergency Services network build out, a joint task force was created by the city's IT Manager, Alan Olenick, Assistant Chief Scott Schwartz of the West Haven Fire Department, Chief Ronald Quagliani of the West Haven Police Department, as well as Sergeant Joseph Wynosky and Detective Joseph Vecellio of the Police Department's Information Technology Team (DOIT). Together with The Business Network Group, the team focused on improving network communications and security, while ensuring a manageable yet scalable solution for future growth.

The team has implemented site-to-site virtual private networks (VPNs) using a FortiGate™-60B appliance from all six firehouses to the West Haven Police department's Data Center which houses the E911 Public Safety Answering Point. These secure channels provide a cost effective solution for the purpose of computer aided dispatch (CAD) and subsequent mandatory state and federal fire reporting requirements.

Prior to the Fortinet VPN deployment, firefighters had to look through a book of local addresses and figure out where to go. By the time they got the directions, they were either already at the location or too much time had been wasted. Now, when an emergency is reported, firefighters can easily VPN into the Police department's network and get directions as well as a picture of the building –all before they leave the fire station.

Municipal Sites

Additional deployments of the Fortinet security appliances were also installed at the city's data center and two remote sites including the senior center and public works facility. Again, VPN deployments via the FortiGate-200A appliance provide a cost effective solution to traditional T-1 transport circuits. Furthermore, this deployment provides the city's IT manager standardization of appliance and security configurations for Web content filtering and antivirus protection.

A Fortinet FortiGate-60 appliance is located at the senior center to help protect the computer lab which provides the seniors high speed access the Internet. Previously having limited firewall protection, the FortiGate appliance is being used for antivirus and intrusion protection as well as Web content filtering.

An additional FortiGate-60 has also been deployed at the public works building. Similar to the senior center deployment, the public works building previously had limited firewall protection. The FortiGate appliance is enabling municipal end users secure VPN access to City Hall network resources such as email, shared network drives and a municipal enterprise resource system.

FortiClient™ is also installed in the laptops of the building inspectors for VPN connectivity to City Hall so that they can access building permit information, email and other job related applications. The deployment allows for ubiquitous access for building inspectors to spend more time at construction sites while giving them access to documents located at their offices. Prior to the deployment, the inspectors would have to go to their office, get the data they needed and then go back to the construction site. Too much time was wasted driving back and forth from the office to sites.

A FortiAnalyzer™-100A appliance is located at the City Hall data center to analyze all data traversing the network at City Hall, the senior center, public works building and for the laptops of the building inspectors. A FortiAnalyzer-100B is located at West Haven Police Department to analyze all data traversing the network at the police and fire stations.

Deployment:
FortiGate-300A
FortiGate-200A
FortiGate-60B
FortiGate-60
FortiClient
FortiAnalyzer-100

Industry:
Government

"I don't generally like to put all my eggs in one basket because of a possible single point of failure, but with Fortinet's multi-threat approach to network security I am completely sold on unified threat management. Since deploying all the Fortinet appliances, they have all worked like a charm," said Alan Olenick, manager of information technology at the City of West Haven, Conn.

Success

Since the deployment of the Fortinet unified threat management solution, a city-wide security policy has been implemented using the Fortinet security appliances. Specifically, detailed "protection profiles" have been created for each municipal location, including the emergency service points of presence. Hence, this policy seeks to protect municipal data assets and information from various intrusion attacks, virus, and malicious Web content. The FortiGate systems immediately met the City's needs by providing multiple functions of network security at each of the six deployments without impacting network throughput.

Fortinet's unified threat management solutions made it easy for the City to build out its network security infrastructure. Being able to consolidate multiple security functionalities into a single appliance became a very important benefit since the City has a limited IT staff. With Fortinet's multi-threat approach to network security, if the City decides to add a security function to any of its deployments, it's a simple task rather than having to purchase new appliances for added features.

In addition to being able to consolidate appliances, having one vendor for all network security functionalities allows the City to reduce IT spending.

Another added benefit of the Fortinet deployment is that employees are more efficient. Building inspectors can now spend more time on-site rather than having to drive back and forth between City Hall and building sites. With the increase in productivity by being able to VPN into City Hall, the municipality realizes various cost savings through lower cost of ownership and static staffing levels. Additionally, benefits extend into the city's public safety. For example, the fire departments will now have a platform to launch computer aided dispatch and the potential of viewing critical information on industrial buildings through the building departments servers.

Finally, being able to report on network usage is another added benefit of Fortinet's solutions. FortiAnalzyer is allowing the small IT staff to easily manage the amount of traffic traversing the distributed networks and to report on network usage.

"What started out as just a senior center deployment quickly evolved into a citywide deployment of Fortinet products. We are very happy with the protection that the Fortinet appliances are offering us as well as the ability to consolidate multiple security functionalities," concluded Olenick.

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in seven programs by ICSA Labs: (Firewall, Antivirus, IPSec, SSL, Network IPS, Anti-Spyware, and Anti-Spam). Fortinet is privately held and based in Sunnyvale, California.

CAS177-0208