CASE STUDY

A Municipal Utility Agency Lights the Way toward Efficient and Effective OT Network Security with Fortinet

One municipal utility agency serves approximately 100,000 electric and 58,000 water customers around Michigan. "We are a midsize provider of bulk electricity generation and distribution for the Michigan area. And in addition to power and water, for some larger corporate and state buildings downtown, we also provide steam for heating and chilled water for cooling," says the agency's network architect for OT. "Our mission is to offer a safe, reliable, and affordable utility experience through public ownership, climate consciousness, and innovative strategies."

That innovative spirit became apparent when the agency redesigned its OT network several years ago. The agency keeps its mission-critical OT network completely separate from its business and IT systems. "If there were a security breach or successful attack on our OT network, the light switches wouldn't work throughout the city," says the agency's spokesperson. "Keeping the OT network functioning is my top priority."

The agency's legacy OT network was challenging to manage. "Rather than being built all at once with security in mind, it was more of a flat network that had been added onto over the years, with solutions from an assortment of vendors," he reports. Even the eight firewalls guarding the perimeter of the agency's two data centers came from multiple providers. This made management of the networking and security environment challenging.

"Some security products are very difficult to manage, and our legacy firewalls were two of the worst, in my opinion," he says. And because they were difficult in different ways, having both in place made management even more complicated. As the agency planned implementation of a new energy management system, the team of three began designing a new OT network that would be more secure and would fully comply with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cybersecurity standards.

Construction of a Fortinet-Centric Infrastructure

The team had worked with Fortinet solutions previously and saw the Fortinet Security Fabric as a good option for simplifying the agency's architecture. "Our 'before' network had a complex design and required somebody with intense skills," he explains. "My philosophy with this redesign was to build the network so that I, personally, would not have to be there so that other team members could also do the work."

"In the final meeting, the NERC CIP auditors commented that our network was designed the way they like to see networks designed and that the products we had in place made their job a lot easier. They also said that, from a security point of view, we are ahead of the curve."

Network Architect for OT

Details

Industry: Power and Utilities

Location: Michigan

Business Impact

- Better visibility into security issues facilitates much faster threat response
- Improved security: Tight access controls and network segmentation limit traffic to necessary paths
- Automated updates keep FortiGuard security services up-to-date with no staff effort

"Finding people with networking and security skills is very difficult right now," he continues. "I wanted to bring in products that would be easy to train people on, where someone could start as an administrator and get exposed to the firewalls—learning about creating policies or doing log searches, for example—without getting overwhelmed. Fortinet was the right path for that. It is very easy to take non-networking people and give them the tools they need to work on the network."

The team redesigned the agency's OT network based on the enhanced Purdue model for industrial control system security. "That enabled us to provide maximum firewall protection to the different parts of the OT network," he says. "Within our data centers, our critical control systems sit in Level 2 and are protected by firewalls in both Level 3 [operation and control] and Level 3.5 [the DMZ, or demilitarized zone]." And unlike the legacy environment, the new OT network design includes a single connection in the DMZ with very limited access to IT computers.

The spokesperson and his colleagues decided to roll out FortiGate Next-Generation Firewalls (NGFWs) in each data center, with FortiSwitch secure Ethernet switches for internal connectivity. They also selected FortiClient to provide VPN connectivity, FortiAuthenticator and FortiToken to secure network access with multi-factor authentication, and FortiManager and FortiAnalyzer to unify the network operations and security operations center management through a true single pane of glass. The team worked with Fortinet partner Trace3 to implement the new network and security infrastructure.

"We built our OT network so that it was completely separate from either the agency's IT network or our existing OT network at the time," he says. "We tapped into Fortinet support and Trace3 for help setting it up. Once it went live, we shut off our old OT network, and they assisted us with management."

An OT Network That Is "Ahead of the Curve"

The NGFWs segment the OT network, and through tight integration with FortiClient and FortiAuthenticator, they ensure that individual users can reach only the resources they need. "No one can get into our OT network without being on the VPN," he says. "And once traffic is in, it has to follow a predetermined path. We do not allow users to just go anywhere they want. Some of our vendors need access to their equipment for maintenance or monitoring purposes. We enable them to log in and do what they need to do, but their VPN connections feed into jump hosts, so they never get true access to our OT network."

The spokesperson points out that the agency's practice of intentionally using different products to protect its OT and IT environments is a best practice. "That ensures if the IT side has a zero-day problem, it will not affect us," he says. "Because our product set is different, an attacker that is successful on the IT side will not be able to use the same tools to break into our OT network. The reverse is true, as well. If we experience a zero-day attack on our Fortinet environment, our IT network will remain protected."

Business Impact (contin.)

- Successful NERC CIP compliance audit, with auditors praising network security design
- Security infrastructure requires less difficult-to-find, specialized skills to manage
- Accelerated staff training, with team members able to easily fill in for one another
- Entire new network costs about the same amount as annual support contract for eight legacy firewalls

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiClient
- FortiAuthenticator
- FortiToken
- FortiManager
- FortiAnalyzer

Services

- FortiGuard AI-Powered Enterprise Protection Bundle
- OT Security Service

The new network has improved security in other ways, as well. The agency's FortiGate NGFWs have the FortiGuard AI-Powered Enterprise Protection Bundle and OT Security Service. "I like that the services are tuned for OT," he says. "It is also very nice that the FortiGuard updates are automated. We set up the firewalls and let them go; they handle the updates themselves."

FortiManager provides single-pane-of-glass visibility across all the agency's NGFWs and switches, and FortiAnalyzer generates reports in which "security issues within the traffic stick out like sore thumbs," he says. "We can look at them and say, 'Why is someone on the other side of the world trying to log in?' The Fortinet solutions have greatly increased our ability to access that kind of information, so we can respond more quickly if there is an incident. Plus, the network segmentation means even a successful attack could not spread."

In addition to security, the Fortinet solutions have improved the agency's ability to meet compliance requirements. Whereas the agency's legacy environment made NERC CIP compliance challenging, the Fortinet Security Fabric streamlines compliance activities.

"A good example is the fact that NERC CIP requires two-factor authentication, along with reporting on who has access to the OT network," he says. "The combination of FortiAuthenticator and FortiToken enables us to require two-factor authentication, and FortiAuthenticator can easily produce the required report. We just put that spreadsheet in our evidence folder, and we are done." That is a capability his team did not have previously: "In our legacy environment, none of that was being reported."

In fact, the security improvements introduced with the Fortinet Security Fabric rollout enabled the agency to pass its NERC CIP audit a few years ago. "The last audit we had was right after we had cut over," he says. "In the final meeting, the NERC CIP auditors commented that our network was designed the way they like to see networks designed and that the products we had in place made their job a lot easier. They also said that, from a security point of view, we are ahead of the curve."

"Because security data is consolidated and the Fortinet solutions have a similar interface, management of our networking and security environment takes us a lot less time now. We log in, and everything we need is right there."

Network Architect for OT

"Because security data is consolidated and the Fortinet solutions have a similar interface, management of our networking and security environment takes us a lot less time now. We log in, and everything we need is right there."

Network Architect for OT

Security Solutions That Are Reliable, Trustworthy, and Easy to Use

In addition to improving security, the new architecture greatly simplifies management of the agency's OT network. "Putting in the FortiManager single pane of glass makes life a lot easier," he says. "FortiManager can manage FortiGates and FortiSwitches together and provide security insights through integration with FortiAnalyzer, all from the same FortiManager console."

"And because the Fortinet solutions are intuitive to use," he adds, "they do not require years of specialized expertise to operate. The FortiOS-based management interface takes away a lot of the nervousness and anxiety from people who have not used Fortinet solutions before. They can figure it out pretty easily, and then going from a FortiGate to a FortiSwitch—the look and feel carry through. In the past, we had to hire specialists because if we did not apply firmware properly, for example, we would destroy the firewall and have to recover it. Now, we have enterprise security in place, but we can hire junior staff and train them on how to use the Fortinet tools."

Perhaps equally important, networking and security engineers do not have to specialize in one or two tools. Everyone can use all the Fortinet solutions, which means team members can fill in for one another when someone needs time off. On a team of three, this is a crucial benefit, the spokesperson says.

The stability of the network is another key benefit. "Since rolling out the Fortinet infrastructure a few years ago, we have not had a single network outage or security event," he says. "Other than one firewall that we needed to replace because of a power surge, the FortiGates have been rock-solid. In fact, our entire Fortinet infrastructure is very reliable. The hardware is stable and well-made. I trust it."

Next up on the agency's radar is the deployment of the FortiClient EMS endpoint management server, which will streamline management of FortiClient and VPN access to the OT network. And the team is currently in the middle of a proof of concept on the FortiNDR network detection and response solution, which is expected to support new NERC CIP requirements that are on the horizon.

Significant Cost Savings and Happy Network Engineers

Despite improving security, compliance, reliability, and ease of management compared with the legacy environment, the agency's new infrastructure is also less expensive. "The Fortinet solutions cost us considerably less," he says. "We were able to build the entire network for about the same cost as just the annual support contract for our legacy firewalls."

Beyond the direct hardware and support costs, the agency would have had to hire an additional staff member or two, the spokesperson adds, to comply with all NERC CIP requirements if it had not transitioned away from its former infrastructure.

When the agency first transitioned to Fortinet, the spokesperson said, "Our other two network engineers were not as sold on Fortinet as I was. We were just talking about this the other day: They have since become believers."

"The Fortinet solutions are intuitive to use, [so] they do not require years of specialized expertise to operate. People who have not used Fortinet solutions before can figure it out pretty easily. We have enterprise security in place, but we can hire junior staff and train them on how to use the Fortinet tools."

Network Architect for OT

"Since rolling out the Fortinet infrastructure a few years ago, we have not had a single network outage or security event. The FortiGates have been rock-solid; in fact, our entire Fortinet infrastructure is very reliable. The hardware is stable and well-made. I trust it."

Network Architect for OT

March 5, 2025 10:58 AM / CS-49-0-0-EN