



“FirePass makes it a lot more manageable to customize or limit access for the 1,000 concurrent connections accessing the network at any given time.”

Camille Gardner
Information Security Analyst

Siemens Energy & Automation Deploys FirePass to Secure and Simplify Network Connections for End Users, IT Staff, Vendors, and Partners

Industry

Manufacturing and distribution, electrical engineering/automation products

Challenges:

- Provide secure, remote network access to employees, partners, and vendors
- Control and customize access for partners and vendors
- Troubleshoot and fix user access problems from any computer
- Adhere to strict data privacy laws

Solution

FirePass 4100 SSL VPN

Benefits

- Provided employees secure, reliable access to applications
- Delivered customized access control policies for partners and vendors
- Experienced fast company-wide adoption
- Reduced administrative duties and costs

Overview

In order to provide authorized, secure network access to a range of employees, business partners, customers, and vendors, Siemens Energy & Automation deployed F5 Networks' FirePass 4100 SSL VPN device. The FirePass device provides employees with remote, secured access—based on access policies—to the business applications they rely upon for day-to-day operations.

Authorization can be given to external partners with access permissions to specific applications on the network. Policy administration enables IT staff to securely administer the network and troubleshoot remote user access issues from any computer with Internet access.

The FirePass device replaced a previous VPN system, deemed by Siemens Energy & Automation to be lacking in security for confidential transactions. This was of particular concern to the parent company, Germany-based Siemens AG, as they needed to adhere to industry standards and European data privacy laws.

Challenge

As a global manufacturing company with a strong presence in the United States and Mexico, Siemens Energy & Automation needed a secure method for granting reliable and secure network access to roughly 8,000 authorized employees—from a plant manager in Latin America, to a customer-service rep in Atlanta, to a sales executive in an airport lounge. They also needed to provide a way for business partners and vendors to gain access to the applications they were authorized to use on the Siemens Energy & Automation network.

“We also needed flexibility to provide limited access for employees not using Siemens-owned laptops for [Microsoft] Outlook Web Access and other designated applications,” said Kathy Taylor, information security officer at Siemens Energy & Automation.

Siemens Energy & Automation employees might be accessing email via Outlook, running sales reports against a database, or transmitting confidential data about accounts. To conduct these tasks in a safe environment, the IT group sought an elegant solution that would secure information using two-factor authentication; that is, users could only access the network via.



use of a physical token plus a unique code known only to them.

Prior to the deployment of the F5 FirePass 4100 SSL VPN device, “we were using an application that was installed on the desktop, which required a user name and password to access the network,” said Camille Gardner, an information security analyst at Siemens Energy & Automation. “It fell short of providing a secure tunnel into the network, and there was minimal encryption.”

Accordingly, the FirePass device’s support for SSL encryption was a significant part of its appeal, Gardner said. Not only is SSL the commonly used encryption standard in information technology, but the parent company of Siemens Energy & Automation had specifically mandated encryption use, in part because Europe’s data privacy laws are more rigorous than those currently in place in the U.S.

Solution

In March 2005, Siemens Energy & Automation embarked upon a multi-phase rollout, including user training, distribution of users’ key fob tokens, and the gradual addition of users to the FirePass-controlled network.

In the two-factor authentication scheme, each user was given a key fob token (“something you have”) to use to access the network. Each user chose a unique Personal Identification Number (“something you know”) in order to complete the access. The token alone is useless should it be lost or stolen. “If I were to find one on the street, I would not be able to use it unless I knew the user’s network ID and token PIN,” Gardner said. “That’s the beauty of the two-factor approach.”

Gardner added: “We set up custom application tunnels to certain

products (for example, Outlook) that we use internally. In addition to enabling employees to use email and calendar features, FirePass serves a critical IT support role. IT staffers can set up remote terminal server sessions at any computer in order to troubleshoot problems on another computer elsewhere in the network.”

In addition to making it easier for IT to support users anywhere, the FirePass device enables users to securely access the network regardless of the computer they are using.

“You can create a secure link into an application that is specific to your company, like an intranet,” Gardner said. “We provide a link to that site and users authenticate with their two-factor authentication without having to be on their work computer.”

Once the IT team had put FirePass through its paces, Siemens Energy & Automation rolled out access to employees working onsite at the company’s headquarters to make any potential issues easy to address. The IT group also began a user education program to help users learn more about using the token and PIN. “We explained to our users what the difference was and helped them understand the advantages of logging into the network this way,” Gardner said.

The new system enabled increased functionality and a smooth transition for employees. “Typically, any business change is hard, and the old system had been in place for several years,” Gardner recalled. But after an initial increase of queries to the support desk, “the calls quickly died off,” Gardner said. “People realized it was to their advantage to access the network this way and it would provide more

security for them. And the solution also provides greater flexibility for our business. A telecommuter doesn’t need to incur the cost of a laptop, but can use a personally-owned home computer to access applications, file sharing, online training, and email. This has increased productivity and reduced costs for road warriors and non-road warriors alike.”

Next, Siemens Energy & Automation began permitting its business partners and vendors to access the network through FirePass. “One significant benefit has been that we can customize FirePass to provide limited customer, business partner, and vendor access to our network, using the same hardware,” Gardner said. “They can only view the applications they are authorized to view. We do not need dedicated resources to a separate environment for a business partner. FirePass makes it a lot more manageable to customize or limit access for external partners throughout the world.”

Finally, F5’s support team proved invaluable as Siemens Energy & Automation launched its FirePass deployment. “They were very helpful in troubleshooting and helping us learn FirePass. Along with an on-site F5 support engineer, we also took advantage of F5’s strong online support programs.”

About Siemens Energy & Automation

With more than 12,000 employees worldwide, 31 manufacturing and distribution facilities, 8 R&D facilities, and more than 100 area sales offices throughout the U.S., Siemens Energy & Automation Inc. is one of Siemens’ operating companies in the U.S. Headquartered in the Atlanta



suburb of Alpharetta, Ga., Siemens Energy & Automation manufactures and markets one of the world's broadest ranges of electrical and electronic products, systems, and services to industrial and construction market customers. Its technologies range from circuit protection and energy management systems to process control, industrial software, and totally integrated automation solutions. The company also has expertise in systems integration, technical services, and turnkey industrial systems. Visit their web site at

<http://automation.usa.siemens.com/index.html>.

About F5

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast, and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5's

extensible architecture intelligently integrates application optimization, protection for the application and the network, and delivers application reliability—all on one universal platform. More than 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to www.f5.com.

F5 Networks, Inc.
Corporate Headquarters
 401 Elliott Avenue West
 Seattle, WA 98119
 (206) 272-5555 Phone
 (888) 88BIGIP Toll-Free
 (206) 272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Asia-Pacific
 +65-6533-6103 Phone
 +65-6533-6103 Fax
info.asia@f5.com

F5 Networks, Ltd
Europe/Middle-East/Africa
 +44 (0)1932 582 000 Phone
 +44 (0)1932 582 001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.
 +81-3-5114-3200 Phone
 +81-3-5114-3201 Fax
info@f5networks.co.jp