

“The ultimate goal was to reach zero security events – and FirePass is helping us reach that goal.”

Bob Grafals
Director of Solutions Development

Georgia Technology Authority Standardizes on F5's FirePass SSL VPN to Enable Secure Remote Access for State Agencies



Industry:

Government

Challenges:

- Remote access using both managed and unmanaged client devices
- Scalability for a growing number of users
- Security requirements, including HIPAA

Solution:

FirePass SSL VPN

Benefits:

- Easy to install, manage and administer
- Highly secure access meets state and federal mandates
- Easy to use

Overview

The Georgia Technology Authority's (GTA) goal is to deliver secure, reliable technology services and solutions, and provide guidance and oversight that lead to sound decisions for Georgia government. GTA is the provider of IT and networking services to a majority of state departments and agencies.

GTA implemented a secure remote access capability for one of its customers, the Georgia Bureau of Investigation (GBI), who was under a federal mandate to provide secure access to sensitive criminal records data.

GTA, through the help of system integrator LCM Security, eventually chose two FirePass 4150 SSL VPN products, a secure remote access solution from F5 that provides secure access to corporate applications and data using a standard web browser. FirePass helps increase the productivity of those working from home or on the road while keeping data secure, and can offer remote access services to some 8,000-10,000 users at the GBI alone. GTA is currently rolling out FirePass access to other state agencies for their secure remote access needs.

In addition, GTA is also using F5's BIG-IP LTM to efficiently manage

application traffic, and F5's WANJet products to accelerate applications including file transfer, e-mail, and client-server applications on the wide area network.

Challenge

Initially, GTA proposed an IPSec-based remote access solution for the GBI. After 6 months of testing, though, GTA determined that the IPSec solution would be inadequate for their needs. Several discussions later, the IPSec vendor agreed to replace the solution with an SSL VPN-based solution. After several more months of testing, however, this particular vendor's next solution was still unable to meet the requirements set forth by GTA.

Some of these requirements included the ability to remotely access email, web portals, network file services, and other key enterprise applications, from both managed and un-managed client devices. Also, due to the sensitive nature of the accessible data, GTA required strong endpoint security that would prevent infected PCs, hosts, or users from connecting to the network. This included automatic detection and re-routing for infected PCs so that users would always have the most up-to-date virus protection when accessing data, along with automatic protection from infected file uploads or email attachments.





Additionally, GTA needed a remote access solution that could easily scale to an increasing number of users, and to the various types of access devices (laptops, PDAs, home office computers) that were in use. Finally, due to limited resources, the solution needed to be easy to install, configure and administer.

LCM Security, a leading international provider of advanced Internetwork security solutions, won a competitive bid to research and identify a new SSL VPN secure remote access solution that would meet GTA's and GBI's requirements. After a careful review, LCM Security contacted F5 Networks and introduced them to GTA.

Solution

F5 provided evaluation equipment and after a three month evaluation GTA purchased their first set of FirePass 4150s. They have since purchased a subsequent set and plan to increase the cluster as demand continues to increase. Today, GBI users regularly access data and applications remotely through FirePass. In addition, several other departments and state agencies besides the GBI have requested they be added to the FirePass system.

According to Bob Grafals, Director of Solutions Development for GTA, FirePass SSL VPN has been one of the most well received products by their customers in several years,

not in least due to the product's strong security posture.

"One of our initial mandates for GBI was to provide connectivity to remote law enforcement officers, and to secure those connections to the criminal justice center databases. The ultimate goal was to reach zero security events – and FirePass is helping us reach that goal," said Grafals.

Maintaining secure data is indeed a key issue – especially for GBI.

"Being a state agency, we deal with very sensitive data," said Grafals. "There are multiple laws and requirements – from HIPAA to IRS compliancy -- that require different levels of data encryption for different types of agencies and users. It all has to be secure – and FirePass is exceeding those requirements."

Of course, security is nothing without control. With so many different devices being used by so many different types of users at various agencies spread across the state, the ability to control who has access to what, and when, was also an important consideration.

"With FirePass, we will eventually have the ability to clean the caches or ensure that a person's anti-virus protection is enabled," Grafals said. "If they don't have that protection, FirePass sends them to a site for automatic updates."

The reduction or elimination of unnecessary administrative chores was a big attraction to the FirePass product, according to Grafals.

"The state is no different than many other businesses – too much to do, and not enough people to do it," he said. "We needed something that could easily scale for our various types of uses, but that was also very easy to install, configure and administer."

In terms of ease of use and performance for customers, FirePass continues to gain new fans throughout Georgia's myriad state agencies – something not lost on Grafals.

"With FirePass, we can work just as effectively at home as in the office," he said. "I can't tell any difference when I'm accessing email and file shares from either location. It works incredibly well.

Finally, the company support behind FirePass has gone beyond expectations.

"The support we've received directly from F5 as well as LCM Security has been outstanding," he said. "They've been with us every step of the way – from implementation to helping us with our architecture up front. Overall I've been extremely pleased with the whole process."

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

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

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

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