IDC Government Insights

V E N D O R S P O T L I G H T

The Need for Federal Agency Improvement of Information Access Security with FIPS-Certified Solutions

November 2011

Adapted from *Managing the Merger: Physical and IT Security* by Shawn P. McCarthy, IDC #lcUS22224410

Sponsored by F5

Network security incidents within the U.S. federal government have increased 650% over the past five years, according to a 2011 report from the Government Accountability Office (GAO-12-137). This explosive growth in security incidents endangers the implied confidentiality and integrity of sensitive government information and also indicates that agencies have not fully implemented all necessary elements to support a robust information security program. Now, at a time when many agencies are moving toward cloud-based solutions for many of their IT needs, they are obliged to rethink their approach to system access control. This Vendor Spotlight discusses the need for government facilities to control who has access to their systems and information and what technologies are available for that control — especially when multiple IT services and remotely hosted applications are being made available to a wide range of government knowledge workers. The paper also looks at the role of F5 and its Federal Information Processing Standards (FIPS)–certified solutions in this important sector.

Work Is Needed on Security and Access Control

Administrators of government networks already are faced with an array of solutions for controlling system access for more people and more IT services. Meanwhile, an ever-growing, dispersed, and increasingly mobile workforce demands the opening of government networks to allow remote access for a wider range of devices.

This trend is putting ongoing pressure on government agencies to improve their compliance with specific regulations, including the 2002 Federal Information Security Management Act (FISMA) and the National Strategy to Secure Cyberspace (2003). Multiple other bills have been introduced that may compel additional security requirements for agencies. Some examples are the proposed Data Accountability and Trust Act (DATA) of 2011 (H.R. 1841) and the proposed SAFE Data Act (H.R. 2577).

Making the matter even more complex, the White House issued an executive order in October to outline needed "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." Basically, the order directs certain structural reforms to ensure accurate sharing and safeguarding of classified information on computer networks that shall also "be consistent with appropriate protections for privacy and civil liberties." The order clearly states that federal agencies bear the primary responsibility for meeting the twin goals.

Clearly, the rise in government security breaches mentioned earlier, coupled with the corresponding rise in proposed regulatory compliance rules, places new security pressures on government IT managers and bureau supervisors. This includes an urgent need for positive identification of those seeking access. In fact, the new security executive order recommends that agencies form steering committees to research and make decisions on how this issue will be addressed on an enterprise level. In an increasingly open

world, passwords are proving again and again to be the weakest link. The following trends are also playing pivotal roles in the security environment of government networks:

- Anywhere/anytime access to both enterprise IT systems and personal data is becoming the norm, not the exception. End users on government networks expect this level of access, and IT administrators are under pressure to provide it without compromising security.
- Plugging multiple cloud computing solutions and outsourced services into government networks places new pressure on systems administrators and network managers to support strong user authentication mechanisms.
- How can you "trust" the endpoint? Identity and access management (IAM) provides the who, what, where, when, and how of user/system activity within an organization. The technology can be used to grant access based on role, location, and privilege, or even time of day. The ability to grant appropriate access at the point of entry with the appropriate levels of security — e.g., Secure Sockets Layer (SSL), single sign-on (SSO) authentication, fraud detection, quarantine, virtual private networks (VPNs) — is invaluable to organizations. A multipronged approach is needed to ensure trusted endpoint configurations.

More Effective Use of Secure Single Sign-On

As incidents of ID fraud, theft, and compromise continue to occur, customers and legislators continue to demand tighter controls. This is resulting in ever-increasing compliance and audit requirements across both industry and government worldwide. This in turn creates demand for more robust security and increased protection of online personal information and digital identities. The move to cloud adoption to achieve IT economies of scale will underscore the need for identity and access management (IAM) technology and identity-driven trust frameworks. SSO is a keystone for these implementations.

As organizations move to public, private, and hybrid clouds, IDC believes demand for Web SSO (WSSO)/federated SSO (FSSO) will increase as well. This technology enables the extension of the enterprise-defined identity to cloud resources and applications (the enterprise being the identity provider here). Secure single sign-on provides many benefits, including better end-user experience and streamlined user access. Perhaps more importantly, SSO helps organizations satisfy compliance control requirements to ensure that access to cloud resources is governed by the enterprise and meets all policy and control objectives.

The security executive order cited earlier also requires agencies to review both internal and external threats to information systems. Accurate and reliable authentication systems are a key way to address this challenge.

Traditional approaches to authentication served government offices well for many years. But the effectiveness of these solutions is diminishing. Some agencies are replacing their legacy authorization systems. For example, this year, NASA began its transition from multiple local RSA SecurID servers to a centralized RSA SecurID server with mandated Two-Factor Token Infrastructure (TFTI), which will support SecurID authentication throughout the agency. Many agencies also have role-based access control systems that offer adequate controls but that may not easily expand to encompass multiple systems.

Another issue to consider is the strict attention that must be applied to role definition and role design. Business or division/department chiefs must be rigorous in defining separation of duties (SoDs). Centralizing the rules/roles process is key to success because it also feeds into the appropriate levels of privileged identity management, fine-grained entitlements, levels of authentication, etc., in an increasingly open computing world.

As these changes unfold, the increasing demands of a highly mobile workforce are further complicating and taxing existing technologies. This may serve as a catalyst for agencies to make

important choices about their access control systems. With many vendors serving this space, it can be difficult for government IT system managers to know whom to trust and whether that trust can be extended to new systems.

In December 2010, President Obama signed into law the Telework Enhancement Act of 2010. The goal of this act is to improve mobile systems access for all workers. One requirement of the act is that agencies must work with the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST) to "ensure the adequacy of information and security protections for information and information systems used while teleworking." A key issue is whether the multiple devices in use all meet compliance and privacy regulations set by FISMA and other government edicts.

More than ever, it is clear that highly trusted enterprisewide access control systems are needed to help federal agencies meet the needs of their end users and to comply with multiple federal requirements.

Security Complications Come with the Cloud

As these changes have unfolded, OMB also issued a "cloud first" policy approximately 10 months ago. This policy essentially means that agencies that need new IT solutions should avoid building their own systems whenever possible and instead look to see if they can procure the solutions via a cloud service provider.

This also means that access control to increasingly sprawling government systems can be a complicated issue. If security isn't easy to use, end users tend to avoid using it or look for ways to work around it. Passwords alone can be notoriously weak, and many end users don't want to carry extra tokens or cards if they can avoid it. Building the authentication into the system itself (as much as possible) is an ideal solution.

Single sign-on solutions can help. In such cases, end users need to log in to their network only once. The access control system handles their right of entry and admission to other systems. This greatly streamlines the end-user experience and also eliminates multiple management challenges, such as maintaining separate system access control points, and it reduces the help desk workload when people forget passwords or experience access control difficulties.

Today, across the government, there are multiple types of SSO solutions, which basically enforce password policies and eliminate the need for employees to remember multiple passwords. The following basic list provides details on how the solutions differ:

- Traditional enterprise SSO is concerned mainly with employee to host access within organizational boundaries. ESSO enables users to log in to internal applications, databases, and other corporate systems with just one identity. Host SSO solutions enforce password policies and eliminate the need for employees to remember multiple passwords.
- Web SSO allows for SSO between Web domains. WSSO and FSSO provide the ability to share a user's log-in and authentication data across different Web sites and applications, both internal and external to the organization, using secure, standards-based protocols. The user is able to sign on to multiple Web sites regardless of the provider or identity domain, and organizations are able to separate employees from external parties to better meet compliance regulations.
- Federated SSO has historically been plagued by both complexity and a proliferation of standards. For most large-scale enterprises today, Security Assertion Markup Language (SAML) has emerged as the federated standard of choice. Many of these organizations are now looking at cloud or managed service providers to handle the task of providing federated infrastructure as outsourcing emerges as a more cost-effective path for many government agencies.

One key for properly managing an SSO solution is access policy management (APM). Proper and accurate creation and assignment of policies is critical, and the ability to manage them in a business workflow is essential. The ability to accurately deploy an APM strategy essentially marries the end user, technology, and business processes themselves to provide a secure method of resource allocation and process execution within a single workflow. It is basically the "who had access to what when" workflow, which increasingly needs to be reviewed by both IT and line-of-business managers. Solutions such as APM are also important to attestation and access certification, which in turn helps greatly in meeting compliance regulations.

The need for endpoint inspection also is important for access control systems. This can be achieved via detection, protection, rerouting, and quarantine. Can end users access all, some, or none of an organization's enterprise resources? In essence, this means that the access control processes are being continually monitored to proactively ensure that only the right people or entities are being granted admission to the site.

The Unique Needs of Government Systems

Because of the mission-critical nature of government information systems, there is a strong need for network standards and implementations that include not only LTE security standards but also network monitoring, incident management, end-user device protection, and, especially, access policy management. Systems capable of monitoring and confirming individual personal identity credentials and allowing access to multiple systems based on those credentials are one of the most important solutions sought by government IT managers at this time.

It's worth noting that virtual desktop solutions (including thin-client and hybrid solutions) could act as an additional catalyst for the growth of SSO solutions. When using a virtual desktop, all applications load from other systems. It's not uncommon for end users to access databases from one server, applications from another, storage from another, and so on. Enabling functionality to support single sign-on could help support a streamlined user experience. Participants have access to all business applications, without worrying where on the cloud those applications reside.

Applications running across networks encounter a wide range of performance, security, and availability challenges. These problems cost organizations an enormous amount in lost productivity, missed opportunities, and damage to reputation.

Considering F5

F5 is a company dedicated to aligning an organization's business strategy needs with its enterprise IT infrastructure. It develops products that offer strategic points of control throughout the enterprise IT infrastructure, with an eye toward scalability and the ability to realign as business demands change.

F5's BIG-IP product family is an integrated set of application delivery services. At its heart, BIG-IP is a Linux-based network appliance that runs on F5's Traffic Management Operating System (TMOS). In turn, this can run one or more product modules to help set business policies and adjust network conditions and rules and organization business policies. Supported solutions include load balancing, SSL offload, Web acceleration, application security, and access control.

As stated earlier in this paper, access control is a major security focus for today's government agencies. F5 offers an Access Policy Manager module for its BIG-IP platform. Positioned between the applications and the users, BIG-IP Access Policy Manager creates a strategic control point in the network. One goal of this solution is to consolidate remote access, LAN access, and wireless connections within a single management interface while providing policy-based, context-aware access. This approach addresses the multiple access control and security issues we've outlined here. For example, government networks need to comply with FIPS for multiple types of connections. F5 offers FIPS-Certified SSL Accelerator to

provide enhanced and highly secure connections for Web services and applications. This is very important for tapping into multiple IT services across multiple networks.

In this realm, the solution offers *multifaceted authentication*, which goes beyond the traditional definitions of authentication to include additional context points such as location, time of day, connected platforms, and other configurable conditions. This F5 solution also supports endpoint inspection, using a combination of automatic detection, protection, rerouting, and quarantine to establish appropriate levels of trust so that an organization can determine whether a user can access all, some, or none of its infrastructure resources. It also helps establish SSL virtual private networks and SSO access control systems.

FIPS Compliance

F5 has taken the approach of bundling and abstracting many critical security access technologies into a FIPS-certified endpoint offering that can be configured easily to meet a client's specific needs. The F5 offering can be tailored to meet expanding (or decreasing) requirements as IT operations change in response to business (government) demands.

Through FIPS, federal agencies and departments can validate whether an information technology solution they want to use is certified to meet specific standards. FIPS 140-2 is a specific computer security standard used to accredit cryptographic modules. The standard covers both hardware and software components. F5's FIPS models are fully FIPS 140-2 Level 2 compliant with the added benefit of the tamperproof security features (key destruction) that come with the Level 3 certification of the FIPS card.

Level 2 and 3 features include the following:

- FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication and for physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module and its other interfaces.

F5 also can help with LDAP solutions. The Lightweight Directory Access Protocol is a widely used authentication protocol within government networks. F5 provides solutions for creating a high-availability LDAP authentication configuration, specifically through the BIG-IP LDAP monitor.

F5 is a proven, government-tested security solution that combines several different aspects of both traditional and emerging areas of security (the aforementioned multifaceted authentication). IDC has long advocated that a secure platform for IT involves the layering of several strong security products, and the ability to offer these from a single vendor should make deployment easier for IT customers. Complexity is often necessary for a secure environment, but in this case, the vendor has managed to hide much of this from the customer to achieve a more easily adoptable solution. The ability to support LDAP will also be increasingly important as government agencies need to interact with outside entities on a more frequent basis to obtain necessary data and information.

F5 already has a substantial government presence. For example, F5 provided key components, including BIG-IP and associated modules, for the network associated with the Emerging Technologies Laboratory built by Northrop Grumman (for the Army Knowledge Online/Defense Knowledge Online system). Fifteen U.S. Executive Branch departments rely on F5 solutions, as do many defense and civilian agencies and government contractors. The company also has worked with multiple state and international governments, including the Georgia Technology Authority and the Australian Education Department. F5's customer base also extends to the commercial sector as well, encompassing enterprises, service and cloud providers, and leading online companies worldwide.

Challenges

F5 faces challenges in the government market, however. Responsibilities for security and privacy increase as the number of access points increases, and within a widely distributed cloud environment, these represent continually moving identity and security issues.

Companies and organizations must ensure endpoint access security regardless of device type or location, and the ability to monitor and record user actions once users have been granted access is important as well. In addition to the IAM technologies outlined previously, software that provides data loss prevention (DLP) and security information and event management (SIEM) is essential as part of the overall solution to achieve a strong governance, risk, and compliance (GRC) platform within a computing community.

F5 will need to partner, if necessary, to provide a holistic security profile and must be willing to educate customers, if need be, about the multidimensional approach required to secure endpoints, multiple devices, and ever-changing roles to meet the challenges of a continually changing end-user population.

Conclusion

Clearly, government IT systems are entering a new phase of development where security improvements are a top consideration. The evolving authentication needs of government's new service-oriented architecture and cloud services mean that single sign-on authentication services will be in high demand.

Government agencies should carefully research these solutions — and be prepared to select the ones that best meet their needs — with an eye toward FIPS compliance. To the extent that F5 can successfully address the challenges described in this paper, the company has an opportunity to be on the short list for agencies looking to improve their authentication security and access control.
