Federal Government solution brief

Federal government information security: a strategic convergence

As one of the earliest and foremost pure-play information security companies, Dell™ SonicWALL™ has always been guided by two principles:

- The best implementation of proven technologies and techniques
- Defining and executing to a roadmap of technology and threat environment evolution

The products of these principles have consistently yielded future-proof best-in-class solutions that are a source of calm and comfort to the business information technology professionals who are our customers.

With the installation of Vivek Kundra as the first federal CIO, the federal government is now undertaking to bring a cohesive vision and strategy to its use and provisioning of technology. Even if the scope is large, the mission is focused. Kundra "reject[s] the view that the public sector has to lag behind the private sector."

This brings the Federal Government into perfect alignment with Dell SonicWALL's consistent direction. And, in turn, the Dell SonicWALL solutions portfolio pairs up extremely well with the federal government's security agenda.

Cybersecurity: On the right side of history

No segment of the FCIO's portfolio is more critical than cybersecurity. The American homeland depends on its information infrastructure. For this reason, that infrastructure has become a hidden theater of electronic skirmishes between the US and hostile regimes as well as independent actors.

As these threats have intensified, they have also become more sophisticated. Increasingly, private individual systems are being secretly hijacked to serve as foils for these schemes. This is the cyber equivalent of urban warfare: Hostile forces hiding amongst civilians and disguising the origins of attacks. In a networked environment, the parallel continues. There is the likelihood of "collateral damage" if blunt instruments are used to counter these threats.

Instead, information security must be smarter and faster than ever before. This includes:

- The ability to scan network traffic in real time
- The capacity to handle unlimited quantities of information
- The capability to scan at the application layer
- The ability to share real-time intelligence at every crucial point of the network—from the endpoint, to the access point, right up to the entrance to the datacenter.

Dell SonicWALL solutions offer competitive or industry-leading capabilities in each of these categories.

One other capability is worth noting: the ability of security devices to share information regarding intrusion attempts and the discovery of malware and other dangerous file types. The current government-wide program to have all security systems share such information has been dubbed Einstein 2, with an Einstein 3 initiative in the works. The information can then be added to signature databases, analyzed for patterns, and studied for further strategy development. This concept is familiar to Dell SonicWALL. Dell SonicWALL's Global Response Intelligent Defense (GRID) Network has been conducting this kind of collaboration for years. The inherent awareness and intelligence capabilities that serve the GRID Network are perfectly suited for use in the Einstein initiatives.

Teleworking: Making threats more remote

As last winter's blizzard-related shutdown of the Federal Government offices highlighted, telecommuting offers a wide range of benefits for continuity of operations. This is in addition to lowered facilities costs, the "green" benefits of reduced automotive commute traffic, and the ability to more easily and precisely match human resources to project needs. The GSA has targeted having 50% of eligible government employees conducting telework by this year (2010)1. This runs directly into the most serious threat to networked information systems: improperly secured end-points.

To address this, the National Institute of Standards and Technology (NIST) advises "all the components of telework and remote access solutions, including client devices, remote access servers, and internal resources accessed through remote access, should be secured against expected threats…."[2] NIST recommends use of secure VPN appliances for enabling telework. And Special Publication 800-46 identifies two key considerations in the selection of such appliances: Device Performance and Traffic Examination as relates to speed of throughput and the comprehensiveness of examination.

Dell SonicWALL SSL VPN solutions address each of these issues with best-in-class technical specifications. They also offer the advantage of centralized management capabilities, which is a core principle of all NIST security guidance.

Virtualization: Dealing with the hard realities

Virtualization is increasingly being embraced as a way to reduce the equipment and maintenance costs for client systems by hosting the applications and data in data centers.

But, according to analysts at Gartner, 60% of virtual servers are less secure than the physical servers they have replaced. They further report that this is only likely to improve to 30% by 2015[3]. The core problem is the traffic between virtual machines on the same physical server. Because this traffic breaks from the traditional "outside-in" network model, it can go uninspected. This, in turn, can enable threats to propagate, undetected, across multiple physical drives.

Dell SonicWALL network security appliances can be configured to process intra-VM traffic just like ordinary traffic. Because of their multi-core processing power, no latency is introduced into the operations. What's more, the application intelligence and control embedded in Dell SonicWALL systems is not dependent on network-centric details such as IP address, directional orientation, and other characteristics of the physical or logical environment. The Dell SonicWALL Application Intelligence and Control Service is equally capable of enforcing policies and inspecting communications traffic for threats based on higher-layer attributes, such as the specific applications and services being used, who is using them, and when they are used. This gives E-Class NSA appliances an unmatched level of granularity and resilience in terms of being able to account for and fully protect dynamically shifting workloads.

Cloud computing: Securing thin air

Cloud computing is the natural adjunct to virtualization. Once the processes are abstracted from the client machine, it is an easy conceptual step to distributing those processes and the underlying data across physically dispersed IT resources.

Perhaps nowhere is the move by the Federal Government to emulate private enterprise IT practices more apparent than in its foray into "cloud" computing and storage. This is a bold initiative for myriad departments, agencies and commissions that have been traditionally siloed. Cloud operations can yield huge cost efficiencies in both equipment and facilities. It also offers benefits in continuity of operations and scalability. Interestingly enough, cloud operations both enhance as well as exacerbate the security concerns.

Because cloud operations can transcend traditional purviews, the security issues are being examined at the highest levels, including the National Security Council. A report for that body prepared by Crucial Point LLC[4] noted that because data is distributed across multiple locations and never any one place, it is more secure.

On the other hand, cloud operations are entirely network-dependant. That raises the stakes for keeping networks up and clean, and keeping traffic moving. The demands for security appliances that can operate at line speed will continue to grow. These appliances will have to be more adept at discerning intrusions amidst a sea of distributed session activity. And they must recognize malware in increasingly fragmented packets. All of this points towards faster, smarter security systems and services.

Dell SonicWALL Next-Generation appliances are the perfect match for this need. Their multi-core architecture yields best-in-class throughput—performing Reassembly-Free Deep-Packet® application-layer scans at line speed—thereby enabling them to handle files of virtually unlimited size, including streamed video and audio.

Continuity of operations: Infrastructure for the inevitable

Assuring the continuity of federal operations has been the focus of planning since the advent of the nuclear era. But the reliance on information systems for every aspect of government operations has increased the likelihood that such plans will have to be acted on. So the Federal Emergency Management Agency requires that all federal departments and agencies prepare and regularly update a Continuity of Operations (COOP) Multi-Year Strategy and Program Management Plan. COOP is used by all federal government organizations to help restore operational (IT) support for personnel, partners and constituents in the event of an emergency that causes a loss of facilities or information assets.

Agencies must also ensure electronic records are backed up and mirrored at a second location. Most federal agencies are constantly looking for ways to cost effectively speed recovery, enhance network security, and provide offsite recovery locations. COOP and telework have become linked as a way for federal workers to access files when they cannot get to their offices. This is also some of the impetus behind the cloud and virtualization initiatives.

Compliance: Surpassing expectations

Mandates and legislation such as the Homeland Security Act of 2002, National Strategy to Secure Cyberspace, Common Criteria Evaluation Assurance Level (EAL) and the Federal Information Processing Standard (FIPS) help safeguard public information by setting out guidelines and recommendations for a secure government infrastructure.

Dell SonicWALL firewalls are certified for FIPS 140-2 and EAL4+. In fact, many Dell SonicWALL NSA and E-Class NSA firewalls have achieved FIPS 140-2 Level 2 certification, including the Dell SonicWALL NSA 3500, NSA 4500, NSA 5000 and the entire E-Class NSA Series. The foundation of Dell SonicWALL firewalls is our SonicOS firmware, a purpose-built hardened platform that stands alongside alternatives from the other leading network appliance providers. In addition to FIPS 140-2 certification, SonicOS is Common Criteria certified on all fifth-generation Dell SonicWALL firewalls in certain implementations.

Dell SonicWALL firewalls are not the only Dell SonicWALL products to achieve FIPS 140-2 certification. Dell SonicWALL Aventail™ Secure Remote Access (SRA) solutions including the E-Class SRA EX6000 and E-Class SRA EX7000 have achieved FIPS 140-2 Level 2 certification. All of the Dell SonicWALL products mentioned are on the GSA schedule and available today.

Open government and privacy: Peace of mind for the people

Since the Paperwork Reduction Act of 1995, the federal government has been consistently progressing towards conducting its business with citizens and vendors via electronic channels. From the very start, security has been a huge consideration, including satisfying all the relevant portions of the E-Government Act and the Privacy Act. As a result, the mandated annual report by the Office of Management and Budget at the end of FY 2008 showed the percentage of systems with:

- Certification and Accreditation – 96%
- Tested Contingency Plan – 92%
- Tested Security Controls – 93%

However, with the move to consolidation of information assets and the virtualization of applications, the old security architecture will be undergoing continuous re-evaluation for some time to come.

Summary

In March of 2009, David Powner, the Director for Information Technology Management Issues, testified that "our nation is under cyber attack, and the present strategy and its implementation have not been fully effective in mitigating the threat." With the government inexorably moving towards even greater reliance on electronic information systems to cut costs and improve citizen services, the need for better information security continues to grow.

Among the dimensions for improvement of the federal government information security are:

- Depth of threat analysis—the ability to identify threats at the application layer
- Better throughput, affecting both speed of analysis and file size capacity
- Network awareness and intelligence
- Flexible, dynamic network topologies that securely accommodate fixed resources, mobile and remote users, and emerging endpoint devices like phones and netbooks
- Secure preservation of data and the capacity for quick restoration of systems in the event of disruptionWith the installation of the first federal CIO, the drive for more electronic infrastructure can be expected to accelerate. This means more need for security solutions.

Dell SonicWALL is ideally positioned to address current and emerging needs. Dell SonicWALL's roadmap for technology and services development has foreseen the requirements now being promoted throughout the federal government. So, in a sense, Dell SonicWALL solutions were designed to work for the Federal Government.

[1] Gautham Nagesh, Continuity of Operations, http://www.govexec.com/basics/coop.htm

[2] NIST Special Publication 800-46 Revision 1, "Guide to Enterprise Telework and Remote Access Security" June, 2009

[3] Matthew Broersma, ZDNet UK, March 15, 2010

[4] Bob Gourley, Crucial Point LLC, "Cloud Computing and Cyber Defense," March 21, 2009

Software