



## Improving the Business of Government With Secure Networks

*In order to achieve its goals, the information networks government uses to connect various constituencies must be secure from intrusion and disruption. This should not be an additional category of hardware, software and services. Rather, it should be an essential quality of the system components selected.*

### CONTENTS

Abstract	2
Government Information: To Protect And Serve	2
The Nature of Network Threats	3
Compliance and Good Sense	4
Secure Access, Transport and Storage	4
SonicWALL Solutions for Government	5
Summary	6

## Abstract:

*Federal, state and local government organizations are leveraging technology more than ever before to improve government services, making them more responsive, efficient, integrated, cost-effective and accessible. Because of this, they are like most businesses in the private sector. In order to achieve their goals, the information networks used to connect various constituencies must be secure from intrusion and disruption. This should not be an additional category of information hardware, software and services. Rather, it should be an essential quality of the system components selected.*

*The attacks of September 11, 2001 had a profound effect on the priorities of government IT provisioning. The e-Government initiatives that had set out to improve service levels through leveraged technology were now focused on public safety. As the attacks showed, all levels of government—Federal, state and local—need to be able to share information in real time. With secure networks in place, government agencies—especially first-responders—can execute their duties as quickly as possible with the best information available. This not only saves time, it can save lives.*

*Another realization that came out of the terrorist experience was that distributed or remote workers and workgroups could help assure continuity of government in the event of disaster, provided they are connected via secure networks.*

*In order to assure a minimum level of information security, government at various levels publishes standards and regulations regarding equipment and procedures. Because the Federal government has taken the lead on this and has the most resources and expertise, Federal guidelines have become the de facto standard for many state and local authorities as well. While this might sound like layers of red tape, these regulations and standards represent a collection of best practices. Information systems built on a secure foundation are practically assured of being in compliance with regulations regarding infrastructure.*

*The need for security can be addressed in three broad activities related to electronic information: transportation, access and storage. The infrastructure that enables this can therefore be divided into three general categories: Unified Threat Management, [Web and E-mail Security](#) and Continuous Data Protection.*

*By provisioning information systems with security as an integral consideration, government IT providers and managers can assure that every agency achieves its mission—protecting and serving the public—while satisfying all the pressures of tight budgets and complex regulations.*

## Government Information: To Protect and Serve

Large companies in the private sector are realizing cost-savings and improved customer service through the use of interconnected information systems. These same capabilities and benefits are also now being obtained by government agencies at all levels.

For example, the Texas Department of Protective and Regulatory Services has deployed mobile applications to more than 250 government inspectors who license and inspect over 23,000 childcare facilities. These applications enable inspectors to capture pertinent information and transmit inspection reports from the field, replacing the original manual, paper-based system.

An example at the Federal level comes from the National Oceanic and Atmospheric Administration (NOAA). They have networked secure national weather satellite station communications to warn the United States about dangerous weather and its location.

With real-time visibility into crucial information, agencies can speed decision-making and improve the quality of information that guides those decisions. Just as in the private sector, this lowers costs while improving services. Of course, the crucial difference with government services is that lives may be at stake. So information integrity and timeliness are essential.

The Parsippany, New Jersey, Police Department has deployed a wireless Computer Aided Dispatch System and Records Management System over a virtual private network (VPN) to provide police officers with remote access to critical real-time data. The ability to transmit data quickly and reliably to the police officer responding to a call is critical. "Our officers can complete an entire [records] search in just four seconds, a dramatic improvement over our previous average of eight minutes," says the terminal agency coordinator officer at the Parsippany PD.

And, in the same way that private enterprise is turning to telecommuters to cut costs, government agencies can employ part-time and remote resources for all kinds of administrative and facilities savings. The non-profit Telework Consortium notes that using distributed, remote resources is an ideal way to assure continuity of government in the event of a natural disaster or terrorist attack.

The technology certainly exists to securely connect dispersed resources, assure timely and complete access to vital information and to speed its delivery. But one of the chief barriers to adoption of the technology has been the perceived vulnerability of such remote access networks.

## The Nature of Network Threats

In May, 2005, the United States Government Accounting Office (GAO) issued its assessment of emerging cybersecurity threats facing U.S. Federal government systems. Highest among these were spyware, spam and phishing. Of course, these threats are not unique to the Federal government.

- Spyware is a hybrid of viruses and hacking. In effect, it automates hacking—gaining surreptitious access to a computer to steal or corrupt information. According to the National Cyber Security Alliance and America Online, 89% of users found to have spyware on their systems were unaware that it was there. IDC notes that spyware is the 4th greatest threat to network security, and is a serious threat to that security. It accounts for up to 30% of all help desk calls today.
- Spam represents two kinds of threats to information systems. The sheer volume of nuisance communications can be a drain on resources. Estimates are that spam makes up over 67% of all e-mail. And it can carry malicious code, viruses and fraudulent solicitations.
- Phishing e-mails— fraudulently appearing to come from and link to a trusted source like a government agency—trick people into divulging passwords, personally identifiable or financially valuable information. IBM said that there were more than 35 million phishing attacks launched to steal critical data and personal information for financial gain in the first half of 2005. "Spear phishing" — highly targeted and coordinated attacks at a specific organization or individual designed to extract critical data — increased more than tenfold in that time.

All these menaces have now come together in what is called blended threats. These are attacks using spam e-mail to deliver automated threats—viruses, spyware, bots (that secretly take control of infected machines), and more—under cleverly constructed false pretenses. According to the GAO Report, blended threats are especially damaging to government agencies for several reasons:

- Security breaches can be critical to national security – there is concern about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering and acts of war.
- As greater amounts of money are transferred electronically, sensitive economic and commercial information exchanged and the defense and intelligence communities rely on commercially available information technology, the risk of attack that threatens national interests increases.
- Identity theft undermines the public's trust in e-government, putting the confidentiality, integrity and availability of agency systems at serious risk.

Given the considerable number of network threats and their ever-changing nature, regulations have emerged to help guide the architecting and provisioning of government information systems.

## Compliance and Good Sense

At first look, the number and detail of government regulations related to securing information systems might seem overwhelming. And it's true that Federal Chief Information Systems Officers are spending 23% more time on Federal Information Security Management Act (FISMA) compliance reporting activities—an average of 49 minutes per day, up from 40 minutes in 2004.

But these regulations are, in fact, on a par with the private sector. And just like their private counterparts, the regulations actually represent a set of best practices. This means that information systems and managers do not need to become legal scholars before they can do their job. They just need good information and good judgment.

The general categories of compliance include:

- Build and maintain a secure network, which requires the creation of firewalls
- Protect sensitive data, including data segmentation to ensure that secure, encrypted data is only accessible to authorized, authenticated users
- Maintain a vulnerability management program to protect data from the growth of network worms, viruses and malicious code
- Maintain strong access control measures that restrict access both technically and by policy enforcement
- Regularly monitor and test networks, including recording information for compliance reports and audits
- Maintain an information security policy that directs all constituencies as to their responsibilities

Not only are the categories of concern relatively straightforward, the approach to specifying the enabling technology can be too. By specifying hardware, software and services that have been developed with security as an integral consideration, you can address a number of the compliance considerations with no extra effort or expense.

## Secure From the Edge to the Core

Given the wide range of users who need to use government information, network security must account for users and connections of all kinds. The systems must be able to securely protect, transport and backup two categories of information: shared information like public records, and protected information like personal health records.

Network protection can be conceived as three essential categories of systems:

### **Perimeter**

This is the most common conception of network security—a wall around the network resources to protect them from outside threats. In practice, a distributed network may connect multiple locations so that the perimeter is actually a bright line between “trusted/approved” versus “unknown.”

In this construct, it is necessary to inspect all traffic for any of the myriad of threats that can come from the outside. The most common tool for this is a firewall or security appliance. In their most advanced form, such hardware devices become platforms for executing a complete analysis of the traffic to identify “unknown” elements, analyze them, and either approve or deny their transmission.

The most common applications for traffic analysis include: Anti-Virus, Anti-Spyware and Intrusion Prevention. The applications that perform the analysis/approval/denial can either be implemented as modules or as a collective, cohesive whole. The advantages of the collective approach include:

- Traffic analysis can be performed just once to minimize any network latency

- Analytical applications are likelier to interoperate, avoiding potential conflicts
- Collective updates can be performed to simplify maintenance
- Policy can be implemented more quickly and cost-effectively at a single point of control

SonicWALL, a world leader in network security, IDC has dubbed this collective approach Unified Threat Management (UTM). The SonicWALL complete UTM solution provides intelligent, real-time network protection against sophisticated application-layer and content-based attacks. Comprising Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention, UTM is delivered as a subscription service on a PRO or TZ Series network security appliance to further simplify maintenance and administration for network managers. The UTM solution flushes out both internal and external threats by addressing multiple threat access points and thoroughly scanning all network layers using a technology called Deep Packet Inspection.

SonicWALL Email Security leverages a global end-to-end attack monitoring network to deliver the highest level of protection from all inbound threats including spam, phishing attacks and viruses.

#### **Internal User Level**

The GAO report cited earlier noted that 54% of the agencies surveyed had identified spyware in their users' systems which had adversely affected productivity and network performance. Since spyware almost always requires user installation (albeit, inadvertent), the spyware example points up a larger issue: users—or, more specifically, user behavior—constitute a threat of their own. In addition to being duped into launching viruses or installing spyware, users can engage in high-risk activities that open vulnerabilities of all kinds. Such activities include file-sharing, streaming recreational media files or instant messaging with someone outside the enterprise.

SonicWALL addresses these threats with Web and e-mail security. These controls can prevent users from accessing unacceptable Web sites and downloading files that contain infected or malicious code. They can also prevent the negative impact such activities have on staff productivity, network bandwidth or exposing your agency to legal liabilities related to copyrighted material and material that is unacceptable in the workplace. SonicWALL Email Security also stops the outbound threat of noncompliant e-mail traffic.

#### **Core Assets**

Threats of network disruption or data corruption in transit are the most obvious security concerns. But every security standard—including FISMA, HIPAA and others—include guidelines regarding protection of stored information. Not only is such information frequently a target of attacks, but it can be a secondary victim of system failures during an attack that impacts network operations.

To assure preservation and restoration of such information, SonicWALL offers Continuous Data Protection (CDP). CDP is a dedicated data backup and recovery appliance that provides end-to-end data protection for the small and medium-sized organizations, including individual locations. The disk-based solution includes user-level instant data recovery with the touch of a button. Managers do not have to wait for an IT expert to come reload the information that was lost. They can do it themselves, instantly, so there's no down time or loss of productivity. Central administration and SonicWALL's hands-free local and offsite data protection technology also eliminates the need for data to be manually transported to multiple locations which means less administrative hassle.

## **SonicWALL Solutions for Government**

As a market leader in network security solutions, SonicWALL is dedicated to serving the security needs of federal, state and local government organizations. Offering both appliance-based products and value-added security subscriptions, SonicWALL can deliver the kind of protection needed to counter multiple security threats. SonicWALL solutions include network security with deep packet inspection when enable with Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Web and e-mail security, secure remote access, backup and recovery and an award winning management and reporting application.

## **FIPS Compliant**

SonicWALL, understanding the importance of compliancy issues for federal government organizations, works closely with the U.S. National Institute of Standards and Technologies (NIST). A number of our firewall/VPN appliances, including the TZ 170 and PRO 3060, have received Federal Information Processing Standard (FIPS) 140-2 Level 2 certification. FIPS 140-2 is required for cryptography related products in use by Federal government agencies.

## **Affordable Solutions**

A heightened sense of security coupled with serious budgetary constraints is leading many government organizations to seek comprehensive multifunction security solutions that are both affordable and easy to implement. SonicWALL offers fully integrated and competitively priced bundles designed especially to meet the needs of government customers—SonicWALL Government Editions.

## **Deep Packet Inspection**

All SonicWALL network security appliances can employ a unique technology called deep packet inspection. This technology goes beyond Stateful Packet Inspection which simply scans packet headers. Deep packet inspection actually examines the content of the packet to find viruses, worms, Trojans, spyware, and other concealed threats in e-mails, Web sites and downloads. SonicWALL deep packet inspection operates in real-time to assure optimum network performance and cannot be overwhelmed by fast data rates or large files sizes.

## **SonicWALL Government Edition Appliances**

### ■ **SonicWALL TZ 170 Government Edition**

A powerful but complete firewall/VPN solution for smaller networks, serving as a platform for other advanced SonicWALL security capabilities.

### ■ **SonicWALL PRO 3060 Government Edition**

A total security platform for complex networks, providing enterprise-class firewall throughput and VPN concentration for a cost-effective price-point.

### ■ **SonicWALL PRO 5060c Government Edition**

A high-performance, multi-service security gateway for large networks.

### ■ **SonicWALL Secure Wireless Solution**

A total security solution that integrates universal 802.11a/b/g wireless with an enterprise-class firewall/VPN gateway.

## **SonicWALL Threat Protection Services**

### ■ **Complete Anti-Virus**

Developed in partnership with McAfee®, SonicWALL Complete Anti-Virus provides organizations with a highly automated and enforced solution, eliminating machine-by-machine anti-virus and anti-spyware deployment.

### ■ **Gateway Anti-Virus, Anti-Spyware and Intrusion Protection Services**

This unique solution features a high-performance deep packet inspection engine that delivers threat protection directly on the security gateway by matching downloaded, e-mailed and compressed files against an extensive signature database.

## ■ **Content Filtering Service (CFS)**

CFS Standard and Premium Editions feature a powerful rating and caching architecture that leverages a database of millions of continuously updated Web sites to eliminate non-productive or even potentially harmful use of the Internet.

## **Email Security**

SonicWALL Email Security provides the highest level of protection from both inbound and outbound e-mail threats by leveraging a unique end-to-end e-mail attack monitoring system. It provides effortless control with simple configuration, easy customization and automated maintenance, all through an easy-to-use, Web-based administrative interface.

## **Secure Remote Access (SRA)**

The SonicWALL SSL-VPN Series, featuring the SSL-VPN 200 and SSL-VPN 2000, provides organizations of all sizes with an affordable, simple and secure clientless remote network and application access solution that requires no pre-installed client software.

## **SonicWALL Continuous Data Protection (CDP)**

CDP provides enterprise-class features such as continuous data protection. Users can restore seemingly lost data with the touch of a button, without IT intervention, without enterprise-class cost.

## **SonicWALL Policy and Management**

Global Management System (GMS) provides flexible, powerful and intuitive tools to manage a few up to thousands of remote SonicWALL Internet security appliances, all from a central location.

## Summary

Private industry has achieved considerable improvements in productivity, cost savings and customer service by leveraging securely networked information systems. These same improvements are available to government agencies at the Federal, state and local level. With complete records instantly available, personnel can be enabled to make better decisions faster, thereby reducing the time spent processing work.

Networks can be provisioned using conventional equipment. And that same equipment can provide all the necessary security features, provided it has been designed as a secure device. What's more, a network built on a secure foundation goes a long way towards satisfying the various relevant regulations. A well-provisioned network even provides the management systems necessary for satisfying the audit requirements that are a part of that compliance.

By seeing to the three elements of information security—the perimeter, the users, and the data—you will have the foundation of a much more productive, efficient and successful organization.

©2006 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice. WP\_Government\_US\_0206.