

SonicWALL Shovel Ready Network Security Solutions

GOVERNMENT

Easy and flexible security solutions to enable shovel ready projects

Overview

The U.S. Government stimulus package is anticipated to provide an estimated \$85 billion commitment to infrastructure over two years, including \$30 billion on highways and bridges, \$12 billion on transit, and \$5 billion on aviation and rail projects. The majority of these funds will be applied to "shovel ready" state improvement projects that have cleared regulatory and planning processes and are simply awaiting fund allocation to begin. Companies such as contractors, engineering firms and suppliers that are prepared to quickly ramp-up to meet the requirements of these shovel ready projects will be best positioned to take advantage of these stimulus package revenues.

Types of Projects

Each state decides what projects to place on their submission list, in expectation that some of the projects will be funded. All stimulus funding must be obligated by September 2010, with at least 50% of the funds being obligated within 120 days of the project being funded. States have taken different strategies to maximize their share of the stimulus funds. Some states have submitted lists that contain mostly road maintenance and bridge repair projects. These types of projects require little if any environmental review, are easy to get started and can quickly create jobs in economically hard-hit communities. With funding for these types of projects in hand, states could invest their own funds in larger, longer term projects that are not ready to start.

Other states have chosen to submit high-impact projects such as updating or creating a shipping facility or upgrading mass transit systems. These projects are typically near completion in their environmental impact reviews and could be started in the next few months. These types of projects could easily last for years and have the ability to generate long term jobs. The downside is that such projects are less likely to be funded as the intent of the stimulus funds program is to create jobs now. Still, some of these larger projects will be funded as they are beneficial to the community over the long term.

The Shovel Ready Challenge

A company will face many challenges as projects are funded by the stimulus program. Companies that slimmed down over the past year or two will need to hire more staff, and many new companies will be formed. In either case, infrastructure to support this new staff will need to be purchased and deployed. In addition, the transitional nature of construction projects often means that they may have little or no broadband cabling, or even telephone or power line drops directly to the site. Yet connectivity, whether to the headquarters, suppliers, inspections or vendors, will be required from day one. The challenge will be to rapidly establish a functional and secure network for core business applications and communications, anywhere and on short notice.

Another challenge will be the heightened interest in stimulus projects in general. While strict reporting requirements could be expected, there could also be local and national media attention especially if there are project delays or cost overruns. As such, reporting and compliance requirements for stimulus projects may be just as important as the actual work being accomplished.

The SonicWALL® Shovel Ready Network Security Solution

The SonicWALL Shovel Ready solution leverages easily-deployed, automatically updating and centrally-managed security technology to quickly deliver mobile, distributed and remote access networking to shovel-ready improvement sites. Integrated support for 3G wireless, 802.11 a/b/g/n wireless and SSL VPN provide protection against today's complex threats while providing the deployment flexibility and ease of set-up and operation demanded by shovel ready projects. By quickly ramping up secure on-site operational networks, SonicWALL Shovel Ready Network Security solutions help businesses quickly and successfully tackle stimulus funded projects.



Deployment Scenarios

While each stimulus project will present its own unique set of challenges, below are two common deployment scenarios which demonstrate the power, security and flexibility of SonicWALL Shovel Ready solutions.

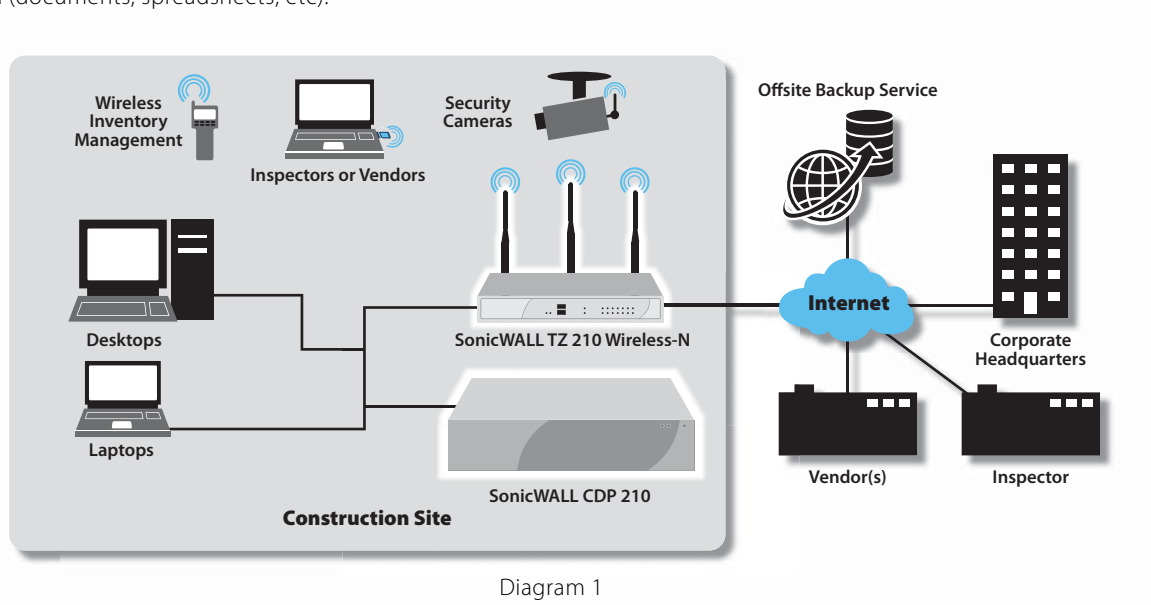
Shovel Ready Scenario 1: Construction Site Field Office

Site Layout and Requirements

- No on-site phone lines or network connectivity
- Electricity is provided by generator
- Must support office staff in field office and provide the following services:
 - Secure wireless Internet access for staff laptops, inspectors and vendors
 - Collection and transfer of office data back to headquarters (HQ)
 - Support for wireless inventory management equipment
 - Support for video cameras used to monitor equipment yard and storage

SonicWALL Solution

SonicWALL provides two critical components to the solution (Diagram 1). The TZ 210 firewall enables Internet connectivity, network security, wireless connectivity, and secure remote access, while the Continuous Data Protection (CDP) system automatically stores locally generated data (documents, spreadsheets, etc).



SonicWALL TZ 210 Wireless-N network security appliance delivers:

- Unified Threat Management services
- 3G wireless connectivity to HQ (primary or failover)
- 120V/12V field power options
- Two 1 Gb and five Fast Ethernet ports
- Site-to-site VPN tunnels and Global VPN clients
- SSL VPN client support
- 802.11 a/b/g/n wireless support with multiple wireless zones and guest services for inspectors and suppliers
- VoIP support for phone and video transmission

SonicWALL CDP 210 delivers:

- Automatic multi-version backup of field site servers, desktops, laptops
- Site-to-site backup to secondary CDP at HQ or Offsite Data Backup Service

Shovel Ready Scenario 2: Field Warehouse with Office

Site Layout and Requirements

- Phone and electric limited to office portion of warehouse
- Must support office staff and provide the following services:
 - Secure wireless internet access for staff desktops and laptops, inspectors and vendors
 - Collect office data and store both locally and off-site
 - Support for wireless inventory management equipment
 - Support for video cameras used to monitor warehouse and loading dock

SonicWALL Solution

SonicWALL provides critical components to the solution (Diagram 2). The NSA 240 firewall enables Internet connectivity and network security. SonicPoint-N access points provide wireless connectivity, the SonicWALL SSL VPN 200 provides secure remote access, and the SonicWALL Continuous Data Protection (CDP) 5040 automatically stores locally generated data, and backs this data up automatically to an off-site facility.

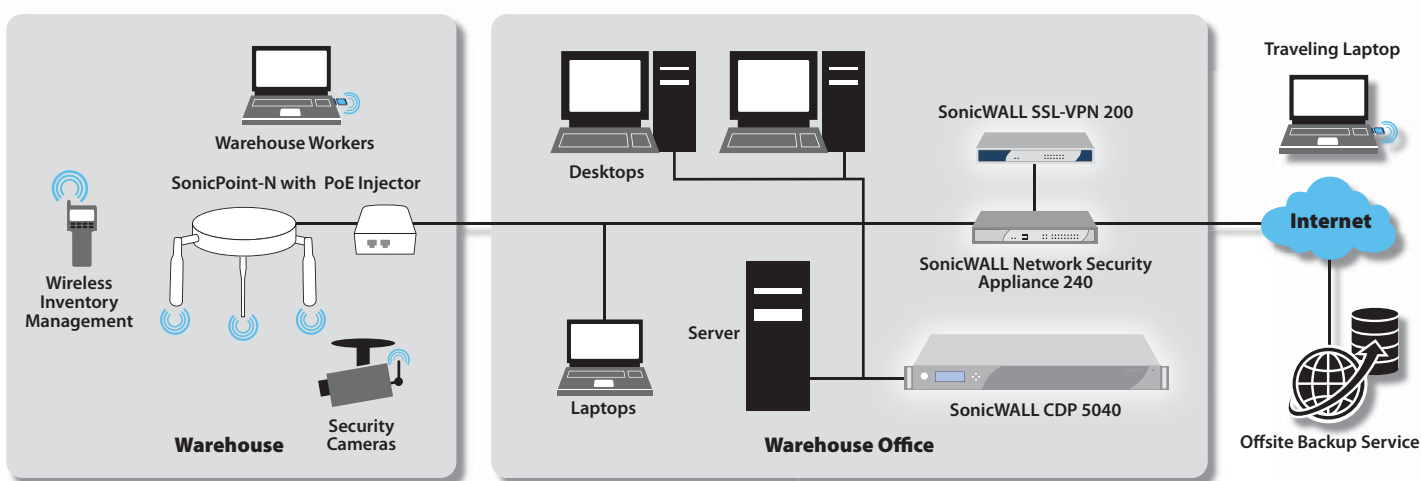


Diagram 2

SonicWALL Solution: NSA 240, SSL VPN 200, CDP 5040, SonicPoint-N and PoE Injector

- SonicWALL NSA 240 delivers:
 - High performance 110 Mbps Unified Threat Management and 3 GbE ports
 - Clean Wireless management of both wired and wireless networks
 - Site-to-site VPN tunnels and Global VPN and SSL VPN clients
 - Application Firewall
- SonicWALL SSL VPN 200 delivers:
 - NetExtender for PC, Mac and Linux devices
 - Web-based remote access
 - Virtual Assist remote technical support
- SonicWALL CDP 5040 delivers:
 - Automatic multi-version backup of field site servers, desktops, laptops
 - CDP Site-to-Site Backup to secondary CDP at headquarters or Offsite Data Backup Service
- SonicWALL SonicPoint-N and PoE Injector delivers:
 - High-performance 802.11n and 802.11a/b/g wireless management
 - Power directly from Ethernet and Gigabit Ethernet (GbE) cabling for easy deployment where electrical power is not readily accessible

The Benefits of SonicWALL

The SonicWALL Shovel Ready Network Security solutions scale to meet the most demanding project requirements by flexibly incorporating elements of SonicWALL Network Security (TZ, NSA and E-Class NSA), Secure Remote Access (SSL VPN and Aventail E-Class SRA), Continuous Data Protection (CDP) and Global Management System (GMS) solutions. Features and benefits include:

1. **Rapid ramp-up** is facilitated by a host of auto-configuring and dynamically updating security features, field-deployable firewall appliances, clientless VPNs, and flexible local, site-to-site and offsite backup.
2. **Unified Threat Management (UTM)** services deliver superior and complete threat protection.
3. **Clean VPN** permits off-site workers access the network as easily and securely as if they were in the main office.
4. **Clean Wireless** uses auto-detecting, auto-configuring SonicPoints to create instant Wireless Local Area Networks (WLANs) and secure Guest Services.
5. Advanced policies and protection with **Application Firewall** services provide bandwidth management services, IPS list blocking, content analysis and more.
6. **3G wireless support** delivers primary access or secondary automatic failover.
7. **VoIP readiness** is provided by ultra-high performance throughput that won't inhibit latency-sensitive phone or security video feeds.
8. **Industry leading throughput performance** maximizes bandwidth while providing unparalleled security and peace-of-mind.

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

