

Clean Wireless

Adding security, performance, manageability and value to wireless deployments

SONICWALL[®]

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Table of Contents

What's Holding Up Wireless?	1
Wireless Security	2
Wireless Performance	3
Wireless Manageability	4
Wireless Value	5
SonicWALL Clean Wireless	6
Conclusions	7

What's Holding Up Wireless?

Wireless Local Area Networks (WLANs) offer the flexibility of working from more locations, boosting productivity for employees, on-site partners, contractors, and guests. At retail and professional settings, such as cafés or clinic waiting rooms, WLANs enhance customers' experience and satisfaction, increasing sales and loyalty. WLANs can also offset costs of deploying a wired infrastructure.



WLANs offer many benefits,

but have been burdened with many concerns.

Businesses want wireless now. So what's holding it up? The delay relates to ongoing IT concerns over:

- Wireless Security
- Wireless Performance
- Wireless Manageability
- Wireless Value

Wireless Security



Well-publicized stories about past WEP vulnerabilities, “war driving” (roaming hackers searching for vulnerable WiFi wireless networks) and other wireless network infiltration techniques have raised awareness of the need for a tighter wireless security solution.

Security for wireless networks has to be at least on par with wired networks running deep packet inspection.

- To be as secure as wired networks, WLANs also need other security features, such as:
- Deep packet inspection (DPI) to scrub traffic using an array of intrusion prevention, anti-virus and anti-spyware technology
 - Wireless intrusion detection and prevention (WIDS/WIPS) to block rogue access and denial-of-service (DoS) attacks
 - Application-level security to control unauthorized application usage and prevent leaks of confidential information
 - Access control features to condition access based upon presence and status of endpoint security software and settings

Wireless Performance

Wireless performance levels must now be capable of supporting latency-sensitive applications like Voice over IP (VoIP) to guarantee adequate quality of service (QoS) levels. While 802.11n deployments can deliver up to 600 Mbps throughput, they can also receive performance hits when mixed into an existing 802.11 a/b/g environment.



Increasing wireless services to more users and applications may decrease network performance.



A flexible approach can help avoid a performance tradeoff. For example, where possible, IT might take steps to:

- Restrict access to just 802.11n clients
- Guarantee a minimum amount of bandwidth to each wireless client in order to prevent disproportionate bandwidth consumption by a single user
- Use dual-band/dual-radio access points to confine 802.11n clients to the 5 GHz band, leaving the 2.4 GHz band for use by 802.11 b/g endpoints
- Establish controls over wireless bandwidth utilization by user, time, date and type of application being used
- Deploy dual-radio functionality to have one radio channel perform compliance testing while the other radio continues to support users

Wireless Manageability

As more wireless services are added, deployment, configuration and ongoing management becomes increasingly complex. This is especially true for solutions with a wider range of features and functionality.

*Ideally, a solution should **simplify not only the deployment, but ongoing management as well.***



Centralized management is just a starting point. Other management capabilities should include:

- Robust monitoring and reporting to support troubleshooting, policy control and configuration
- Power over Ethernet (PoE) to ease deployment of access points
- Auto-discovery and auto-provisioning of new access points using centrally defined and maintained configurations
- Automated distribution of firmware and time-sensitive patch updates

Wireless Value

Complexity adds cost. In order to establish comprehensive wireless solutions, IT has often supplemented existing WPA2 or WIDS/WIPS by adding separate firewall, VPN, intrusion prevention services (IPS), Next-Generation Firewall or multi-function Unified Threat Management appliance behind the Wireless Access Switch/Controller (WAC). However, this incurs the added costs of multiple appliances.

*Next-generation solutions can offer
lower Total Cost of Ownership (TCO)
by combining WAC and DPI on a single device.*



Combined WAC/DPI appliances should be purpose-built and optimized to offer the full functionality and performance of standalone components. Additional cost-reducing capabilities should include:

- A unified policy model to enable creation of policy and object definition through a single centralized management interface
- PoE Injector to eliminate or minimize costs of extending electrical infrastructure
- Backward compatibility for earlier generations of wireless clients to ensure maximum utilization rates without having to refresh client systems

SonicWALL Clean Wireless™

SonicWALL® Clean Wireless™ unites high-speed secure wireless with high-performance Reassembly-Free Deep Packet Inspection™ technology through the deployment of SuperMassive E10000, SonicWALL E-Class NSA (Network Security Appliance), NSA or TZ Series firewalls in conjunction with SonicWALL SonicPoint Series (SonicPoint-Ni, SonicPoint-Ne and SonicPoint-N Dual-Radio) access points.



SonicWALL Clean Wireless adds
security, performance, manageability and value.



SonicWALL Clean Wireless delivers the innovative dual protection that you need and that can:

- 1** Encrypt and protect wireless traffic on the high speed 802.11n wireless networks
- 2** Clean the traffic and protect the wireless network using high-speed SonicWALL Reassembly-Free Deep Packet Inspection to deliver comprehensive protection from viruses, spyware and other attacks, while also delivering application control

The dual protection of the SonicWALL Clean Wireless solution secures the wireless network by encrypting wireless traffic and decontaminating it from network threats while also protecting the network from wireless intrusion attacks. The SonicWALL Clean Wireless solution goes beyond mere secure wireless solutions by making wireless networks as secure as wired networks using deep packet inspection, delivering organizations of all sizes greater security, value, performance, and ease of management.

Conclusions



Wireless LAN deployment benefits for retail, manufacturing, healthcare and other enterprise organizations have been overshadowed by IT concerns over security, performance, manageability and value.

Businesses no longer have to settle for one-dimensional wireless security that only relies on encryption.

SonicWALL Clean Wireless brings wireless network security to the level of wired networks that run deep packet inspection, thus providing both the high-speed secure wireless connectivity together with high performance deep packet inspection protection in order to deliver:

- Tighter wireless security
 - Higher wireless performance
 - Easier wireless management
 - Greater wireless value
- 

How Can I Learn More?

- Download the Whitepaper “AimPoint Group: Secure Wireless Made Easy – Selecting a Next-Generation Solution for Pervasive WLAN Implementations”
- Opt-in to receive SonicWALL Newsletters

For feedback on this eBook or other SonicWALL eBooks or whitepapers, please send an e-mail to feedback@sonicwall.com.

Forward to a Friend

About SonicWALL

Guided by its vision of Dynamic Security for the Global Network, SonicWALL develops advanced intelligent network security and data protection solutions that adapt as organizations evolve and as threats evolve.

SonicWALL's line-up of dynamic security solutions



NETWORK
SECURITY



SECURE
REMOTE ACCESS



WEB AND E-MAIL
SECURITY



BACKUP
AND RECOVERY



POLICY AND
MANAGEMENT

SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124

T +1 408.745.9600 F +1 408.745.9300

www.sonicwall.com