



ENTERPRISE & MOBILITY

Securing the Wireless Enterprise with Wireless Firewall

Traditional wired firewall and intrusion protection systems (IPS) do not provide adequate security for new wireless LAN threats- but wireless IPS solves this major challenge.

BROCADE

THE BUSINESS ISSUE

Businesses are expanding connectivity to the point of activity to save costs and achieve new levels of productivity. However, extending wireless connectivity to branch offices as well as outdoors leaves the enterprise vulnerable to new kinds of threats. Wireless vulnerabilities are increasingly being exploited by organized criminals seeking lucrative data such as customers' credit card numbers and personal information. Recent high profile data breaches have highlighted the need for wireless monitoring and intrusion prevention. The cost of a data breach from immediate fines and business disruption to long-term brand damage and legal liabilities is substantial.

Wired firewalls have matured through years of innovation and provide a comprehensive first line of defense for wired security. However, wired firewalls do not provide clean separation between wired and wireless traffic. Wired firewalls traditionally inspect only wired Internet traffic—corporate wireless traffic is not inspected. In addition, wired firewalls do not factor in attributes that are specific to wireless communications, such as encryption, authentication and location—limitations that leave the enterprise exposed to wireless-specific threats. Some wireless vendors are now offering firewall capabilities, but these first generation wireless firewalls lack many important functions, including Layer 2 stateful inspection of bridged traffic, leaving enterprises vulnerable to attacks such as ARP cache poisoning and DHCP spoofing. In addition, these devices often require significant redesign of the wired infrastructure—for example; the wireless switch/controller may need to be reconfigured as the default gateway—adding cost and complexity to wireless deployments.

THE BROCADE WIRELESS FIREWALL

Brocade's next generation Wireless Firewall provides clean separation between wireless and wired networks as well as within a wireless network—between sensitive corporate information and rest of the wireless traffic. Brocade® has designed a wireless firewall that takes into account wireless-specific attributes—including encryption, authentication and location—and every wireless packet is inspected before it enters the wired network.

In conjunction with Wireless Intrusion Protection System (IPS), Brocade's Wireless Firewall provides unparalleled traffic inspection at every network security layer, ensuring that sensitive corporate and customer information is safeguarded at all times. Brocade's wireless networking infrastructure is not only secure, it is easy to deploy and manage—especially crucial for enterprises with large distributed deployments and limited centralized networking IT staff.

WIRELESS FIREWALL FEATURES AND BENEFITS

Brocade's Wireless Firewall offers enterprises a reliable, secure, wireless network that not only protects the enterprise against threats, but also ensures compliance with regulatory and industry standards. Additional benefits include:

- **Protection against the greatest set of wireless threats:** Some Layer 2 attacks, such as DHCP spoofing or ARP cache poisoning, cannot be detected by current wireless LAN (WLAN) firewalls that operate at Layer 3. The Brocade Wireless Firewall can seamlessly detect and prevent such Layer 2 wireless threats.
- **Location-, user identity- and role-based policy enforcement:** Enterprises often need to implement access and security policies that take into account a user's identity, role and location. The Brocade Wireless Firewall integrates with leading enterprise authentication systems (including LDAP and Active Directory) and can leverage a built-in Real-Time Location Solution (RTLS) engine to enforce user identity-, role- and location-based security policies.

- **Ease of deployment:** The Brocade Wireless Firewall provides centralized policy configuration with distributed policy enforcement at the point of business activity. It does not require any redesign of existing network topology and offers complete protection by inspecting bridged and routed traffic.
- **Gap-free security:** The Brocade Wireless Firewall shares state with one or more switches within the enterprise, maintaining stateful firewall protection as users roam across the campus. At the same time, the firewall stops intruders right at the periphery of the network, acting as a barrier for malicious wireless threats. When combined with Brocade's AirDefense Wireless IPS and Spectrum Analyzer, the Wireless Firewall offers the most comprehensive wireless security in the market.

SUMMARY

Today's businesses are deploying wireless networks to better meet customer needs. The proliferation of these networks has led to a steady increase in security threats from organized criminals targeting lucrative data such as personal information, credit card numbers or vital company data. Businesses transmitting customer credit card and personal information can face steep fines per compromised record. Traditional wired security solutions, such as firewall and intrusion prevention systems (IPS) do not provide adequate protection against new types of wireless threats. Brocade's Wireless Firewall, in conjunction with Wireless IPS, solves this major challenge by creating a gap-free, secure wireless network that safeguards data against attacks at the point of business activity.

© 2011 Brocade Communications Systems, Inc. All Rights Reserved. 06/11 GA-TB-391-00

Brocade, the B-wing symbol, BigIron, DCFM, DCX, Fabric OS, FastIron, IronView, NetIron, SAN Health, ServerIron, Turbolron, and Wingspan are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, Extraordinary Networks, MyBrocade, VCS, and VDX are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.