



Securing the All-Wireless Enterprise with Motorola's Wireless Firewall

EXECUTIVE 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 \$200-\$300 USD 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. Motorola'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.

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 and home offices as well as outdoors leaves the enterprise vulnerable to new kinds of threats. Wireless vulnerabilities in verticals such as retail, hospitality and financial services are increasingly 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 is substantial — from immediate fines and business disruption to long-term brand damage and legal liabilities — often averaging as much as \$200-\$300 USD per record.

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 on wireless switches and controllers. These first generation wireless firewalls lack many important functionalities, 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 Motorola Wireless Firewall

Motorola's next generation Wireless Firewall provides clean separation between wireless and wired networks as well as within a wireless network — between sensitive customer credit card information and rest of the wireless traffic — ensuring compliance with the latest Payment Card Industry (PCI) Data Security Standards. By leveraging our vast knowledge as an industry leader in the development and deployment of wireless solutions, Motorola has designed a wireless firewall that offers the highest level of wireless security available. Wireless-specific attributes are taken into account — 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),

Motorola's Wireless Firewall provides unparalleled traffic inspection at every network security layer, ensuring that sensitive personal information and credit card data is safeguarded at all times.

Motorola'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. With Motorola's One Point Wireless Suite — which includes a comprehensive suite of integrated tools such as LANPlanner, RF Management System and Spectrum Analyzer — IT departments can quickly plan, deploy, manage and secure large distributed wireless network infrastructures.

The Motorola Wireless Firewall features and benefits

Motorola'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 Motorola 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 Motorola 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 Motorola 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 Motorola 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 Motorola's AirDefense Wireless IPS and Spectrum Analyzer, the Wireless Firewall offers the most comprehensive wireless security in the market.



MOTOROLA

motorola.com