

White paper

Why Your Firewall, VPN, and IEEE 802.11i Aren't Enough to Protect Your Network

Overview

Like any network technology, wireless local area networks (WLANs) need to be protected from security threats. Though recent developments in IEEE standards have been designed to help ensure privacy for authenticated WLAN users, WLAN clients and enterprise infrastructure can still be vulnerable to a variety of threats that are unique to WLANs. Mischievous hackers may try to attack the network, or a negligent employee may create a security breach that leaves the corporate WLAN or a client device vulnerable to attack. These threats cannot be mitigated by traditional firewall technologies and virtual private networks (VPNs), nor eliminated through encryption and authentication mechanisms used in conventional enterprise network security systems. With a comprehensive approach to WLAN security, an intrusion detection and prevention system (IDS/IPS) for WLANs adds to IEEE standards-based technology and wired network security mechanisms. An IDS/IPS specifically designed for WLANs addresses the risks associated with this networking technology.

A new class of security threats to enterprise networks

The prevailing model of enterprise network security is rooted in the axiom that being “*physically inside is safe and outside is unsafe.*” Connecting to a network point within the enterprise is generally considered safe and is subject to weaker security controls. On the other hand, tight security controls are enforced at the network traffic entry and exit points using firewalls and VPNs.

A WLAN breaks the barrier provided by the building perimeter as the physical security envelope for a wired network because invisible radio signals used by the WLAN cannot be confined within the physical perimeter of a building, and usually cut through walls and windows. This creates a backdoor for unauthorized devices to connect to the enterprise network. Some specific security threats from WLANs are described below.

Contents at a glance

Overview	1
A new class of security threats to enterprise networks	1
Protecting enterprise networks from WLAN threats	3
About HP ProCurve Mobility	4



Rogue APs: WLAN Access Points (APs) are inexpensive, easy to install, and small enough to be carried by a person. Unauthorized WLAN APs can be connected to an enterprise network unwittingly or with malicious intent—without the knowledge of IT—by simply carrying the device inside the enterprise and connecting it to an Ethernet port on the network.

Since rogue APs are typically deployed by employees looking for quick wireless access, they are usually installed without any WLAN security controls (such as Access Control Lists, Wired Equivalent Protocol, 802.1X, 802.11 i, etc.). These can be connected to virtually any Ethernet port on the network, bypassing existing WLAN security control points such as the HP ProCurve* Intelligent Mobility System (IMS) and firewalls. The radio coverage of rogue APs cannot be confined within the building perimeter of the enterprise, meaning that unauthorized users can connect to the enterprise network through these rogue APs using their radio spillage. The invisibility of wireless medium makes this kind of access difficult to prevent.

Soft APs: With client cards and embedded WLAN radios in PDAs and laptops, a threat called “soft AP” is on the rise. A soft AP functions as an AP under software control and can be launched inadvertently or through a virus program, allowing unauthorized users to connect to the enterprise network through soft APs using radio spillage.

MAC spoofing: APs in a WLAN transmit beacons (or probe responses) to advertise their presence in the air. The beacons of an AP contain information about its MAC address, which is its identity, and SSID, which is the identity of the network it supports. Wireless clients listen to beacons from different APs in the vicinity. Clients typically connect to an AP that advertises the desired SSID and transmits a strong beacon signal. A number of WLAN AP models available in the market allow their MAC addresses and SSIDs to be user defined. APs as well as many software tools enable setting of MAC addresses and SSIDs of AP devices to virtually any user-defined values.

In MAC spoofing, the attacker programs the AP to advertise exactly the same identity information as that of the victim AP. A MAC spoofing AP can also launch disruptive attacks such as packet dropping and packet corruption and modification. A MAC Spoofing AP can even connect to the wired enterprise network as a rogue AP and evade detection by conventional site survey tools. In addition, a MAC spoofing AP can lure authorized wireless clients in the enterprise WLAN into establishing a connection and providing confidential information.

Honeypot APs: Wireless networks can coexist in the same space, enabling users to connect to any available network, whether one’s own network or another network in the vicinity with overlapping radio coverage. This access to co-existing WLANs can be exploited by intruders who set up an unauthorized wireless network by powering on an AP in the vicinity (e.g. street or parking lot) of the enterprise wireless network. These APs, called “Honeypot” APs or “Evil Twins,” entice authorized enterprise clients into connecting to them by transmitting a stronger beacon signal and MAC spoofing. An authorized user unwittingly connecting to a Honeypot AP creates security vulnerability by inadvertently providing sensitive information such as its identity. Authorized wireless clients in the enterprise WLAN can also accidentally connect to non-malicious neighboring APs called “client mis-associations,” creating security vulnerability as the wireless clients may inadvertently provide confidential information to such APs.

Denial of service: WLANs are being increasingly entrusted with carrying mission-critical applications such as database access, VoIP, e-mail, and Internet access. These applications can be disrupted by a denial of service (DoS) attack, causing network downtime, user frustration, and loss of productivity.

Because 802.11 WLAN transmissions are a shared medium, they are easily susceptible to DoS attacks. Additionally, “soft spots” in the 802.11 MAC protocol can easily be exploited to launch DoS attacks. DoS attacks such as authentication, association, de-authentication or disassociation floods, NAV attacks, CTS floods, and EAP and EAPOL message floods are easy to launch and can bring down the entire enterprise WLAN.

* The products referred to in this publication were developed and sold by Colubris Networks Inc, which was acquired by HP ProCurve in 2008. References to HP ProCurve herein refer only to Colubris Networks Inc., or those products acquired from Colubris Networks and not the HP ProCurve product line generally.

Ad hoc networks: The 802.11 WLAN standard has provisions for establishing peer-to-peer wireless connections between wireless clients, which can then form an ad hoc network among themselves. However, the ad hoc networks can create security vulnerability. For example, an intruder on the street can form a peer-to-peer ad hoc wireless connection with an authorized laptop in the enterprise premises and can then launch security attacks on the laptop using this wireless connection. For example, if the laptop has a setting to share certain resources (files, directories, etc.) with other authorized laptops in the enterprise, the intruder can get access to these resources.

The seriousness of threats to enterprise network security from rogue APs, mis-configured APs, soft APs, and ad hoc networks should not be underestimated. Unauthorized devices connecting to the enterprise network through such APs can engage in data theft, data rerouting, data corruption, impersonation, denial of service, virus injection, and other types of attacks. This vulnerability exists in organizations that have official WLAN deployments as well as those which have banned wireless usage.

Protecting enterprise networks from WLAN threats

The emergence of WLANs has created a new breed of security threats to enterprise networks, which cannot be mitigated by traditional firewall technologies and VPNs. The firewall blocks unauthorized wired traffic from reaching the internal trusted enterprise network, while a VPN protects enterprise data from traveling beyond the boundaries of the enterprise network into the public Internet. However, these technologies as well as the encryption and authentication mechanisms such as WEP, WPA2, 802.1X, and 802.11i cannot plug the security holes created by rogue APs and soft APs. Conventional enterprise network security systems are not designed to detect and prevent threats from MAC spoofing, honeypots, DoS, and ad hoc wireless networks.

Included in HP ProCurve WLAN solutions is security technology that alleviates threats from WLANs through:

- Monitoring wireless activity inside and out of the enterprise
- Classifying WLAN transmissions into harmful and harmless
- Preventing transmissions that pose a security threat to the enterprise network
- Locating participating devices for physical remediation

Security technology is comprised of wireless sensors for wireless monitoring, which are placed spatially to cover the enterprise premises in order to keep a constant vigil on the “enterprise air” and create a radio frequency (RF) shield to reduce the risk of security threats.

The five key features of the Wi-Fi firewall are planning, detecting, classifying, protecting, and locating. These are described below.

1. Planning WLAN RF coverage: The spatial layout in the enterprise and materials (walls, columns, windows, furniture, etc.) interact with the radio coverage of the sensor, creating confusion about where to place APs. A systematic, scientific, and scalable RF planning process is therefore required for determining the right placement of access points and wireless sensors. This process must account for the spatial layout of the premises and indoor RF signal propagation characteristics in order to ensure that there are no holes in the security coverage.

2. Detecting WLAN Transmissions: Security technology needs to scan all of the radio channels in the 2.4 GHz (b, b/g) and 5 GHz (a) band and capture any wireless activity detected on these channels using spatially distributed sensors. The information collected by different sensors then needs to be appropriately analyzed, aggregated, and correlated.

3. Classifying WLAN transmissions: With increasing penetration of WLANs, there is a need to accurately and automatically sort harmful activity from harmless activity in the shared wireless medium. For example, in organizations with no official WLAN deployment, wireless activity detected in the air is either due to a rogue AP or is emanating from an external (neighbor’s) WLAN. In organizations using an HP ProCurve IMS WLAN infrastructure, the security differentiates between authorized, rogue, and external wireless activities. From a security standpoint, this type of classification minimizes false alarms and volumes of irrelevant alerts, both of which make the security system unusable.

4. Protecting against intrusion: The security technology must automatically and instantaneously block harmful wireless activity detected by its wireless sensors. For example, the technology must block any client from connecting to a rogue AP or a MAC spoofing AP, prohibiting formation of ad hoc networks, and mitigation of DoS attacks. Further, it must block harmful wireless activity until physical remediation has taken place. Prevention of harmful WLAN transmissions must be carried out without disturbing legitimate WLAN activities and without risk of bringing down the entire wireless network. The prevention must be able to minimize false alarms and block all unauthorized activities.

5. Locating WLAN devices: Physical remediation—i.e., disconnecting and powering off the WLAN device(s) taking part in harmful activity—requires knowledge of the physical location of these devices. The security technology must provide the location coordinates of the device inside and around the perimeter of the enterprise premises. There should be no need for specialized client-side software or hardware.

About HP ProCurve Mobility

HP ProCurve provides an optimized WLAN switch, the HP ProCurve Intelligent Mobility System (IMS)*. IMS couples distributed intelligence with centralized WLAN management to optimize performance, mobility, scalability, and investment protection. HP ProCurve products have been honored with an array of awards, including *Red Herring's* Top 100, the *Fierce Wireless* "Fierce 15," and *Network World's* "World Class" Award.

* The products referred to in this publication were developed and sold by Colubris Networks Inc, which was acquired by HP ProCurve in 2008. References to HP ProCurve herein refer only to Colubris Networks Inc., or those products acquired from Colubris Networks and not the HP ProCurve product line generally.

For more information

To learn more about HP ProCurve Networking, please visit ProCurve.com

© Copyright 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA2-3197ENW, November 2008