

## USING A VPN TO SECURE WIRELESS LAN TRAFFIC

*Products: 802.11b; Windows 2000 Professional, Server, or Advanced Server; WatchGuard Firebox; Windows XP Professional*

### Overview

Wireless LAN (WLAN) technologies such as 802.11b provide end-users and IT professionals alike a tremendous amount of flexibility. However, for the IT professional, security is a paramount concern. WEP (Wired Equivalent Privacy) and MAC-level access lists are a good start, but they do not address the entire picture. This technical note describes a framework for securing WLAN traffic using a network-layer virtual private network (VPN).

The network architecture for a VPN-secured WLAN implementation is shown below in Figure 1.

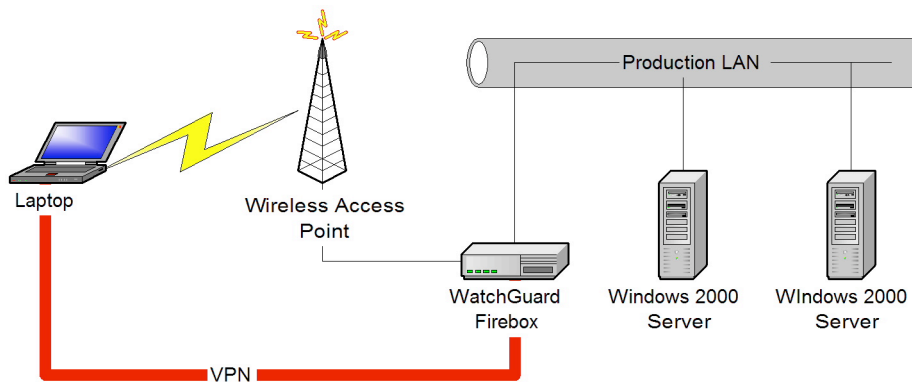


Figure 1. A framework for a secure WLAN installation

This security architecture is described in greater detail in the following section.

### More Information

#### Key Components

The primary component in this wireless LAN security architecture is the firewall that screens WLAN traffic before it enters the production LAN. Although Figure 1 displays a WatchGuard Firebox performing this function, just about any firewall product with built-in VPN functionality would work. This includes a Cisco PIX with an IPSec license (preferably a 3DES IPSec license for 168-bit encryption) or Microsoft's Internet Security & Acceleration (ISA)

Server 2000, which employs L2TP over IPSec (again, preferably with 3DES support enabled to provide 168-bit encryption). This document is written from the perspective of a network deploying a WatchGuard Firebox.

The second key component is the VPN itself. While WEP performs encryption, it is widely recognized to have some security flaws (static keys) that can be reasonably easily exploited. The use of VPN technologies such as PPTP, pure IPSec, or L2TP over IPSec provide better encryption levels and dynamic key exchanges that mitigate the weaknesses of WEP. In addition, the authentication required by the VPN adds another layer of control over access to the production LAN by wireless clients. Depending upon the firewall used, the VPN authentication can be integrated into services available on the production LAN. For example, with ISA Server 2000 deployed between the wireless LAN and the production LAN and providing VPN functionality, authentication on the VPN can be integrated with Active Directory and Active Directory's remote access policies. These remote access policies could be used to control WLAN access based on day of the week, time of day, or any number of other criteria. Alternately, a device offering RADIUS functionality could be integrated into Active Directory via Windows 2000's Internet Authentication Service (IAS), again offering the ability to control WLAN access through remote access policies. (The use of IAS as a RADIUS server for 802.1x authentication of wireless clients is also a possibility.) Of course, the most secure form of authentication would involve two-factor authentication and one-time passwords, such as that employed by RSA Security's ACE/Server line of products. Again, this document is written from the perspective of using a WatchGuard Firebox with built-in PPTP support and internal authentication.

## WLAN Security Risks

There are two potential security risks inherent in a WLAN deployment. The first is uncontrolled and unauthorized access to internal (private) resources. In this scenario, that security risk is addressed through the use of the DMZ port on the firewall. Unless traffic is specifically defined as allowed from the DMZ interface to the internal (or trusted) interface, then the traffic is denied. This ensures that only authorized traffic from the WLAN is allowed to enter the corporate network. (In addition, in this scenario, the only authorized traffic is VPN traffic from authenticated users.)

The second potential security risk is the unauthorized use of bandwidth. Instead of using the WLAN to access private resources, unauthorized users may just "ride" the Internet connection, denying access to that bandwidth for legitimate users and processes. This issue must be addressed in the configuration of the Firebox (a typical configuration would not address this problem).

To fix this problem, the security rules for the Firebox must be modified so that outgoing traffic is only allowed from the trusted interface. By default, most services installed in a typical Firebox configuration specify outgoing rules of "Any to Any"; this default configuration would allow outbound access from the DMZ (or optional) interface to the Internet. By replacing "Any to Any" with "Trusted to Any," the restriction is immediately enforced that only traffic originating on the trusted interface is allowed to the Internet. Of course, this then precludes access to the Internet from the WLAN.

To implement this secure WLAN framework, two basic steps are required:

- Configure the Firebox for PPTP-based VPNs.
- Configure the Firebox to allow only VPN traffic from the optional (DMZ) interface, and to allow outbound Internet access only from the trusted (internal) interface.

Additional details on how to configure a WatchGuard Firebox for PPTP-based VPNs is found in the technical note titled, "Configuring PPTP-Based VPNs on a WatchGuard Firebox, Version 4.61." The information in that technical note is based strictly on version 4.61 of the WatchGuard Firebox System software; other versions may vary slightly.

## **Other Notes**

This security architecture does not preclude the use of WEP and/or access lists based on MAC addresses. Also note that the VPN and firewall functionality could conceivably be split onto separate devices, such as dedicated firewall and dedicated VPN concentrator. Third, the framework described in this technical note is platform-agnostic from the respect that it will work with any vendor's wireless access points and wireless NICs (the functionality resides in the firewall itself, which must be VPN enabled, and in the Windows operating system). Finally, alternate methods of adding security to wireless LANs also exist, such as the use of IPSec in transport mode in homogenous Windows 2000/XP networks. These methods may be described in future technical notes.

## **Related Articles/Resources**

None

## **Legal Information**

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.