

## USING IPSEC 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. Well-known security flaws in the current implementation of WEP (Wired Equivalent Privacy), such as the use of static keys, create a need for more robust security mechanisms. This technical note describes the use of IP Security (IPSec) in transport mode to provide end-to-end security for wireless LAN traffic in homogenous Windows 2000/XP networks.

The network architecture for this proposed wireless LAN implementation is shown below in Figure 1.

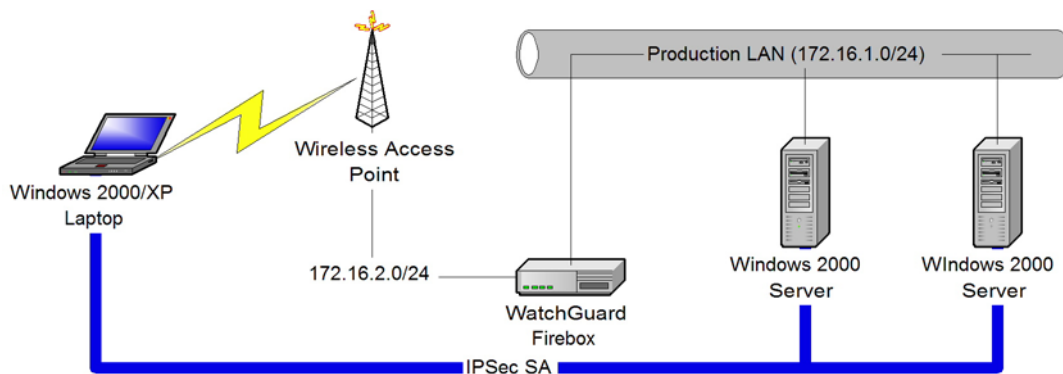


Figure 1. Using IPSec to secure end-to-end wireless LAN traffic

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

### 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, virtually any firewall product would work. The primary purpose of this device is to ensure that only authorized traffic is allowed to move from the wireless LAN onto the production (wired) LAN behind the firewall. The only requirement is that the firewall's NAT functionality can be disabled, as NAT breaks IPSec. For this reason,

Microsoft's Internet Security & Acceleration (ISA) Server 2000 could not be deployed in this scenario since NAT cannot be disabled on ISA. This document is written from the perspective of a network deploying a WatchGuard Firebox.

The second key component is IPSec itself. IPSec performs two key functions in this situation. First, it provides machine-level authentication through the use of X.509 certificates for Phase 1 authentication. This ensures that only authorized systems, with an appropriate and valid machine certificate, will be allowed to establish an IPSec security association (SA) with production LAN systems. Second, it provides stronger encryption through support for three-key Triple DES (3DES). This level of encryption is far stronger than even 128-bit WEP. Furthermore, while WEP performs encryption, it is widely recognized to have some security flaws (static keys) that can be reasonably easily exploited. IPSec is widely accepted not to suffer from such flaws.

Together, these two key components address the three primary security risks inherent in a wireless LAN deployment:

- **Unauthorized traffic from wireless LAN:** The firewall ensures that only authorized traffic (IPSec AH, IPSec ESP, IKE/ISAKMP, and ICMP) passes from the wireless LAN to the production LAN and vice versa.
- **Unauthorized use of bandwidth:** The firewall rules allow Internet access only from the production LAN, and not from the wireless LAN. Proxy servers can be used to allow wireless LAN systems to access the Internet if such is required.
- **Access to confidential information via wireless "sniffing":** IPSec's use of 3DES encryption ensures that wireless sniffers will not be able to gain access to any confidential information transmitted via the wireless LAN.

## More Information

Two basic steps are required to implement this security framework. First, the firewall must be configured correctly. Then, the appropriate IPSec policies must be created and installed on the systems involved.

## Configuring the Firewall

To configure the firewall, use the WatchGuard Control Center to modify the firewall's configuration as described in the following steps. Note that these steps are based on version 4.61 of the WatchGuard software; other versions may appear slightly different. Note also that the configuration for other types of firewalls may differ significantly.

1. Assign an IP address to the Optional interface. If the Firebox is currently running in routed mode, then assign the IP address directly to the interface itself. If the Firebox is currently running in drop-in mode, then assign the address as a related network on the Optional interface. In the diagram shown in Figure 1, the IP address that should be assigned to the Optional interface would be something like 172.16.2.1/24.
2. Enable service-based NAT. This allows for NAT to be disabled on the rule that allows IPSec traffic between the wireless LAN and the production LAN.
3. Add service definitions for IPSec. This includes IPSec ESP (IP protocol 50), IPSec AH (IP protocol 51), and IKE/ISAKMP (UDP port 500).

4. Add a service rule for IPSec, allowing traffic inbound from the Optional interface to the Trusted interface and outbound from the Trusted interface to the Optional interface. Be sure to disable NAT on the outbound connection; otherwise, the Firebox's NAT rules will kick in and IPSec will not function correctly. (The option to disable NAT won't appear unless you've enabled service-based NAT as indicated above.)
5. Add a service rule allowing Ping from the Optional interface to the Trusted interface and vice versa. Ping will be the traffic that is used to initiate the IPSec SA creation between systems on the wireless LAN and systems on the production LAN.

Optionally, some of the other service rules on the firewall can be configured to allow outbound traffic from "Trusted to Any" instead of the default "Any to Any." This prevents outbound traffic from the wireless LAN.

For more information on configuring the WatchGuard Firebox, refer to the following Technical Note:

- Service Definitions for a WatchGuard Firebox

## Creating the IPSec Policies

The IPSec policy is reasonably simple. It specifies that all IP traffic from the wireless LAN must be secured using IPSec. This involves the creation of one new filter list that includes the IP subnets of the wireless LAN and the production LAN. The default Require Security filter action can be used in this case. The security methods may need to be customized to provide maximum security (168-bit 3DES encryption and 160-bit SHA-1 hash).

For more information and more specific details on creating IPSec filter lists, filter actions, and IPSec policies, refer to the following Technical Note:

- Basics of IPSec Policies in Windows 2000

## Other Notes

This security architecture does not preclude the use of WEP and/or access lists based on MAC addresses. In addition, note that the technique 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 OS (Windows 2000/XP) is providing the enhanced encryption and authentication functionality through its native support of IPSec.

## 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.