

Secure WLAN Best Practices and Topology

Michael J. Martin

Wireless LANs have become an unsafe, insecure and untrustworthy networking technology. That is a pretty bold statement, but I will clarify in a few moments. WLAN connectivity is not going away. Users love it, and its public accessibility is only growing. If a user can have wireless access in their home, at McDonald's, or even on an airplane, you can be sure that if you do not provide a secure solution in the office, your users will provide an insecure one. With this in mind, we will adopt the view that "if you're going to have to live with the devil, you need to protect your soul." As a network administrator, you will need to deal with wireless networking requirements for your enterprise. The question you need to ask yourself is, "Do I want to spend my time hunting down wireless, or supporting it?"

If you take a class or read an article on wireless security, you will more than likely be exposed to a list of WLAN "dos and don'ts." The list tells you how and why wireless networking is so insecure. Fundamentally, when you compare wired Ethernet to wireless Ethernet, you find that they are both insecure. Yet, an overwhelming majority of the world's network implementations are based on Ethernet. For it is not the transmission technology's security that matters as much as how that technology is implemented.

Rogue wireless access points (APs) are the most common wireless security issue we deal with. They are dangerous because they provide open access to the network that you (the network administrator) don't know anything about. In addition to the blindness factor, in almost all cases when rogue APs are discovered, they have been configured using the "out of the box" settings. They do not use WEP, have generic SSID, and are directly connected to the LAN, providing access to anyone.

The second most common wireless security problem is poorly conceived wireless network implementations. What actually makes these worse, for a networking pro, is that they are deliberately implemented and yet they are insecure. Other security threats include war driving, wireless mooching, WEP key cracking, etc. All of these are largely made possible by the first two problems I explained.

Following is the requisite list of wireless security "dos and don'ts" according to yours truly and presented with the hope that you will take them to heart and go forth and implement a secure wireless network.

Provide only specific services, i.e., HTTP, HTTPS, SMTP, etc. No matter how secure you think your WLAN is, you should always consider it insecure. You would not let LAN users have unrestricted access to the Internet, would you? The same rules apply to the WLAN. Users should have access to specific services; this makes monitoring and security a whole lot easier.

Control access between the WLAN and LAN with a firewall. The WLAN should be self-contained; think of it as an another DMZ network. Control data flow using a stateful inspection or, even better, a proxy firewall. That will enable you to implement the "do" above.

Use the AP for access only. Today, APs come with DHCP servers, firewalls, and all sorts of added functions. Disable them. While it may seem more complicated, it is far better to use solutions you are already familiar with to secure your WLAN. If you use a Microsoft DHCP server, deploy another one for the WLAN. Use PIX Firewalls, add an additional DMZ interface, or deploy a separate one between the WLAN and LAN.

Secure WLAN Best Practices and Topology

Michael J. Martin

Configure the AP properly. Change the AP's default SSID, define RF channels, and assign management IP addresses that are not routable from the WLAN. If your AP cannot support multiple networks, set the AP's IP address to an IP other than that used on the WLAN. If you need to connect to the AP to make a change or update code, join the SSID with a workstation configured with an IP in the same range as the AP's management address. Connect, change or upgrade the AP, then change your IP address to the proper subnet.

Implement Wired Equivalency Protocol (WEP) using a 40/64-bit key (good), or, if available, a 104/128-bit key (better). I know WEP has a reputation for being insecure, because there are tools such as Aircrack, Aircrack-ng, WepLab, and dwepcrack around. But let's put this into perspective. First, WEP was not designed to be a super-powerful security solution. It was designed to provide "data obscurity" equivalent to that provided by wired Ethernet, which is a shared medium broadcast technology saddled with its own security limitations. If you are connected to the wire, you can see the data transmitted by other hosts. Ethernet switching increased the security of wired Ethernet by limiting transmission visibility to only the hosts connected to the switch port. That reduced wired Ethernet's security exposure, but did not eliminate it.

With wireless Ethernet, anyone can see the RF signal. WEP provides limited encryption capabilities designed to make it harder to break into the network, not eliminate the possibility. The biggest problem with wireless Ethernet in most cases is that WEP is not even enabled, leaving the network completely exposed. WEP may not be perfect, but it's better than no security measures. If implemented, WEP will obscure the data transmitted by the users connected to the WLAN from each other.

Breaking into WEP also involves cracking the key. The original WEP cracking tool, Aircrack, worked by collecting 5 to 10 million packets then looking for weak initial vectors (IVs) to crack the key. To thwart this attack, wireless card manufacturers adopted improved algorithms. That did not eliminate the problem, but increased the number of packets required to crack the key, requiring the attacker to dedicate more time. The newer tools like Aircrack-ng and WepLab use the KoreK statistical cryptanalysis attack code, which depend on collecting a number of unique IVs instead of weak ones. That reduces the number of packets to 200,000 to 500,000.

However, the biggest problem with WEP is the key. Most WEP implementations use weak keys that can be cracked using simple brute-force dictionary attacks. The reason for weak keys is simple -- it's easier to remember the key "wireless" than, say, "00aFba1c2e." Using a strong WEP key increases the amount of time it takes to crack the key, thereby increasing the exposure time of the attacker. If someone wants to get into your wireless network, they probably will, but if someone is just looking for free access they will move on and find an "open" AP.

Use a VPN to secure communication between WLAN and LAN resources. Implementing a VPN to access the LAN removes the need for WEP to some degree and provides data security for all of your applications, at least to the point where the VPN terminates onto the LAN. The downside to VPNs is the need for clients and user accounts. A good compromise is to use WEP to secure access to the WLAN and protect access to certain services (such as Internet HTTP/HTTPS) and use VPN to provide additional access to applications that need greater security (like access to the LAN).

Secure WLAN Best Practices and Topology

Michael J. Martin

Implement Media Access Control (MAC) address filtering. Control access to the WLAN resources by implementing MAC filters on the AP or the LAN switch port to which the AP is connected. As with VPNs, there is additional administrative overhead with this approach because the MAC address of each wireless adapter needs to be added to the filter before network access is possible. This can be reduced somewhat by having the DHCP server and AP share the same LAN switch port and then implementing the MAC filter on the switch. The DHCP server's lease binding database can be used to learn the MAC address of new wireless stations. It does not eliminate the administrative overhead, but at least the user doesn't have to figure out what her MAC address is.

If possible, use a HTTP/SHTTP proxy to access the Internet. This is a good idea for providing any Internet access, not just for the WLAN. Proxy servers provide performance improvements and enforce protocol access policies. P2P, IM, and a variety of other applications "tunnel" their network connections over TCP port 80 and 443 to work around stateful firewalls, which simply track connection states and packet structure. A number of firewall vendors are now offering deep packet inspection. This verifies that the data being sent over a specific port is using the protocol assigned to the service port. If it is not, the packet is dropped. A proxy server achieves the same result; only protocols specific to the proxy can be handled. If the data request does not conform to the proxy's protocol, the packet is dropped. And, you can get a 30% performance improvement to boot.

Now that the obligatory "dos and don'ts" are out of the way, let's discuss implementing a secure WLAN solution that implements the "dos" we just outlined. Not all solutions are applicable to all environments. Designing any network requires a balance of a number of factors: cost, performance, usability and security. Wireless network implementations provide an interesting challenge to network administrators in these areas for a number of reasons.

Cost: This is always a factor with any network implementation, but wireless networks are not primary path infrastructure. Your network backbone is not dependent on your wireless network; wireless is a convenience network. So you want to keep the cost in check. APs have come down in price a great deal in the last few years. A basic AP will cost around \$75.00, and beyond that price you are paying for features like enhanced security methods, adjustable RF power, multiple SSID and 802.1q/p support.

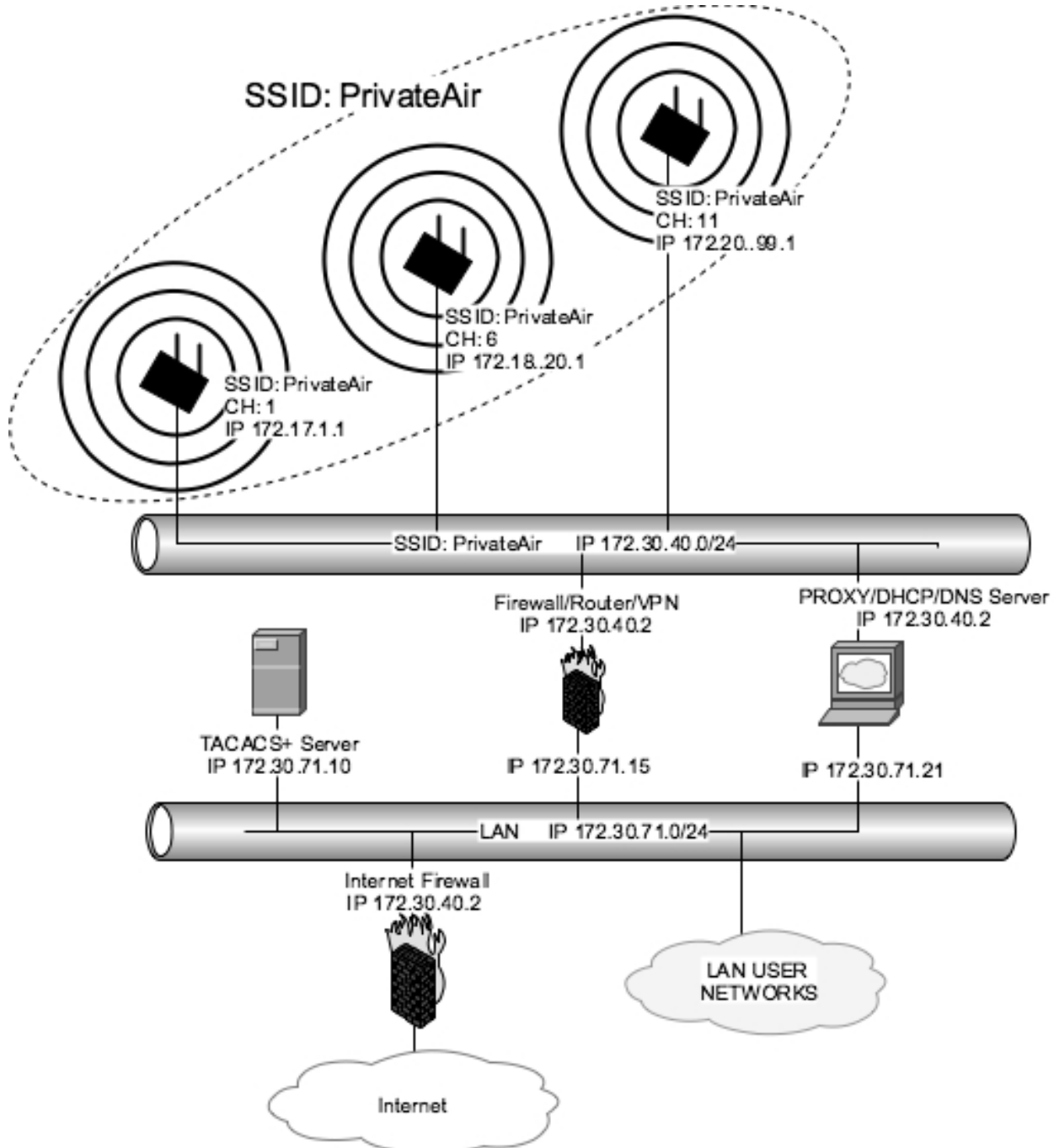
Performance: 802.11b is acceptable for checking e-mail and basic Web access, but 802.11a or 802.11g are needed if any degree of network performance is required. A nice compromise is to deploy a combination of 802.11g and 802.11a. Use 802.11g for guest access and 802.11a for LAN access. This allows you to widely deploy a closed wireless environment, provide performance and isolate guest and LAN user traffic.

Usability and security: In the case of wireless, these two factors go hand in hand. If the network requires too much access control, the users will either not use it (and deploy rogue APs) or drive the network support team crazy with security access requests. Network administrators need to have a good understanding of their user population's ability and tolerance. The best way to gain this perspective is to run some user impact forums. Review possible security solutions with the user community, get feedback, and take it into account. Even if you have a management mandate, implementing wireless requires user buy-in, otherwise you will be AP hunting.

Secure WLAN Best Practices and Topology

Michael J. Martin

To ensure broad appeal, our example will utilize generic 802.11g APs that can support WEP, hard RF channel settings and, if possible, adjustable RF power. A Cisco 17XX or 26XX IOS router can provide firewall, DHCP, VPN and auth-proxy support. A standard Linux workstation/server can provide HTTP/HTTPS proxy, DNS and DHCP support. A closed 802.11g network segment can support up to three APs connected to a common Layer 2 Ethernet segment or VLAN along with the router and Linux server. Here is a WLAN example illustration:



Secure WLAN Best Practices and Topology

Michael J. Martin

The WLAN and LAN are segmented using the firewall/router and the proxy/DNS/DHCP server. Along with the hardware and topology, the WLAN solution will incorporate the following concepts:

- The WLAN should be deployed using a discrete closed network topology utilizing discrete hardware and interconnection paths apart from the LAN. Access to all but basic network access services is provided by gateways.
- The basic network access services for the WLAN are limited only to DHCP and DNS, as both are required for network access. Special use HTTP servers will also need to be deployed to support proxy configuration. Access to the WLAN can be regulated using non-broadcast SSIDs and/or WEP authentication. DHCP leases can be provided openly or to only "known hosts" using MAC addresses as host identifiers.
- The WLAN will support two levels of network access. One for LAN or "known" users and another for "guest" network access.
- Guest-level network services are limited to DNS and HTTP and HTTPS via proxy. Users connect to the proxy either manually or using auto proxy discovery. HTTP and HTTPS connections are intercepted by the router (using IOS auth-proxy) and responded to with an informational page on configuration.
- Authenticated "known user"-level network access to the LAN can be providing using IOS auth-proxy authentication or Cisco VPN client or both. Known users are also provided unauthenticated or authenticated HTTP and HTTPS access via proxy.

With the solution and topology defined, we're ready to move on to the implementation, which can be broken into two components: the Linux proxy server and the IOS firewall/VPN configuration. The next article in this series will deal with the configuration of the Linux proxy server. Then will conclude the series with the IOS firewall/client VPN support.