Building Secure Wireless Local Area Networks

A White Paper By
Colubris Networks Inc.

Author: Pierre Trudeau (President)

COLUBRIS.COM

Introduction

Ubiquitous network access without wires. This is the powerful drawing card for the deployment of wireless networking technology. But, for many, this powerful advantage is seen as double-edged providing increased flexibility and ease-of-use on one side, tempered by heightened security risks on the other.

Essentially, the inability to physically secure a wireless network is considered to be its Achilles heel. But this conclusion is flawed since it places the burden for security at the physical layer instead of at the network layer where it makes much more sense. To dispel the wireless security myth, this white paper explains how to protect your data with a secure wireless implementation.

Understanding wireless security challenges

In addition to the great benefits wireless networks provide, enterprises that deploy this technology must understand and deal with the security issues related to radio transmission. Radio waves cannot be controlled and travel freely through most physical barriers, easily spreading confidential data beyond the walls of an office or home. With the transmission power of today s devices, ranges of 300 feet or more are common. If not handled properly, this potentially creates a major security hole in a network.

However, this lack of security is not just limited to wireless technologies. Data transmission technologies that rely on cables are not any more secure. They only happen to be easier to protect with physical barriers. Should the physical barriers be broken, then the actual security of the network can easily be compromised. For example, Ethernet LANs or dial-up Internet connections are both vulnerable to simple cable tapping.

Since wireless technology has no inherent physical protection, it forces us to take a more critical look at current network security practices and acknowledge their weaknesses. Once this is done, we can create solutions using existing proven technology.

Finding a solution

The fact is that today, most local area networks function without data security at the physical or logical link layers, as do the majority of dial-up and broadband Internet connections. They are generally only protected from intruders through some form of user authentication or Internet firewall. When data security is required, it is usually implemented at layer 3 or above. For example, transactions on the Web are secured with HTTPS (SSL). Remote access to corporate networks is secured with virtual private networking (VPN).

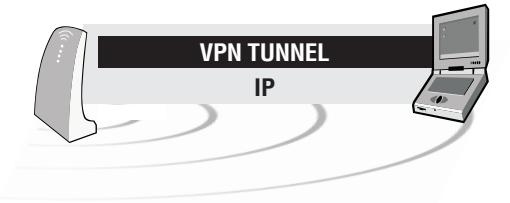
One of the main reasons for this, is that implementing security at the physical layer is not always practical because a logical connection between two devices may be carried across more than one physical link. Providing end-to-end security between the two endpoints of a connection is more desirable because it functions independently of the underlying data transport. This type of security is best implemented at layer 3, the IP layer, since an IP datagram is the smallest addressable unit of data that is carried on an IP network.

If we view wireless technology in this context, the approach shifts from trying to encrypt the radio transmissions (as is done by most wireless access points using Wired Equivalent Protection or WEP), to creating secure end-to-end connections between stations. Currently, the most flexible method for doing this is to use an access point that integrates virtual private networking (VPN).

The VPN solution

VPN technology provides the means to securely transmit data between two network devices over an unsecure data transport medium. It is commonly used to link remote computers or networks to a corporate server via the Internet. However, it is also the ideal solution for protecting data on a wireless network.

VPN works by creating a *tunnel*, on top on a protocol such as IP. Traffic inside the tunnel is encrypted, and totally isolated.



VPN technology can be used to create a secure tunnel over an unsecure protocol like IP.

VPN technology provides three levels of security: user authentication, encryption, and data authentication.

- Authentication ensures that only authorized users (over a specific device) are able to connect, send, and receive data over the wireless network.
- Encryption offers additional protection as it ensures that even if transmissions are intercepted, they cannot be decoded without significant time and effort.
- Data authentication ensures the integrity of data on the wireless network, guaranteeing that all traffic is from authenticated devices only.

By implementing VPN technology, wireless networks become more secure than their unprotected wired counterparts, and can be used to solve even the most mission critical networking challenges without security concerns.

Implementing VPN security

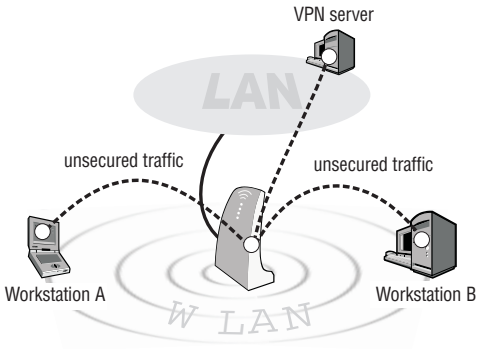
Applying VPN technology to secure a wireless network requires a different approach than when it is used on wired networks. This is due to two factors:

- The inherent repeater function of wireless access points automatically forwards traffic between wireless LAN stations that communicate together and that appear on the same wireless network.
- The range of wireless network will likely extend beyond the physical boundaries of an office or home, giving outsiders the means to compromise the network.

The ease with which wireless networking solutions can be deployed and their scalability, makes them ideal solutions for many different environments. As a result, implementation of VPN security will vary based on the needs of each type of environment.

Enterprise

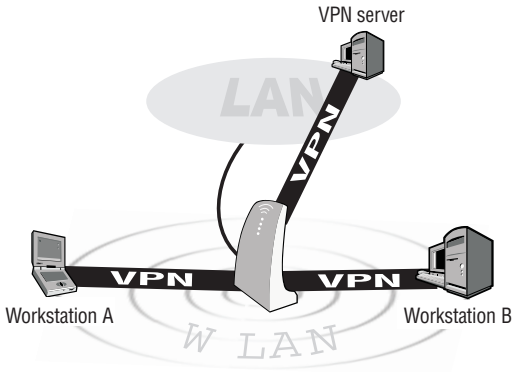
In business environments, total security of the wireless network is crucial. This can be impossible to achieve with wireless solutions that rely exclusively on an external server for all VPN functionality. A security hole is created because access must be granted to the wireless network to enable computer users to reach the VPN server and login. Traffic flow on the wireless network cannot be completely secured.



Wireless access point with an external VPN server.

To make effective use of VPN technology, the access point must have its own VPN server, or at the very least, be VPN-aware. A VPN-aware access point only accepts and forwards VPN traffic to an

external VPN server, discarding all other traffic. Both implementations provide complete security for the network, as the access point will not allow wireless traffic *outside* of a VPN unless that traffic is to establish a VPN.

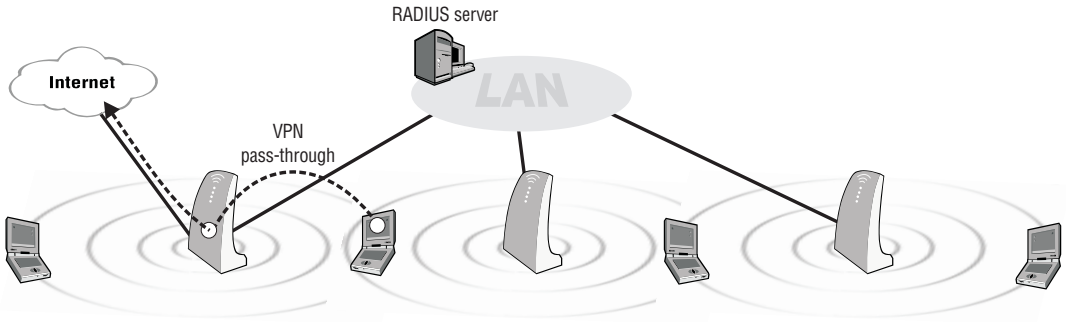


Wireless access point with integrated VPN server.

Public access

In public access applications (airports, hotels, convention centers), the wireless service does not need to provide more security than what is offered by traditional dial-up services. This means that secure authentication for accounting purposes (usually via a centralized RADIUS server) achieved over an upstream VPN connection needs to be complemented by a wireless service that provides the ability to transparently support user-provided security on-demand (typically a VPN connection to the corporate VPN server).

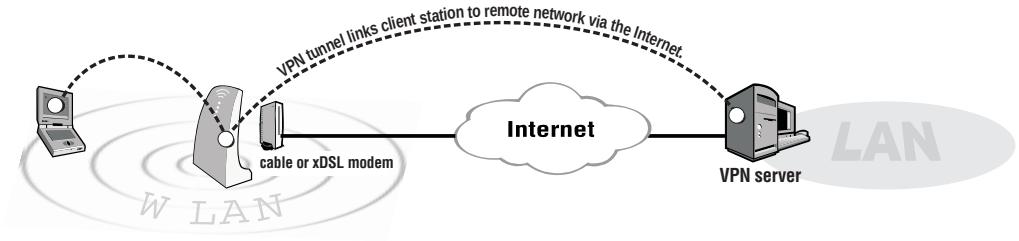
To protect individual stations from one another requires that the repeater function must be disabled.



Multiple access points covering a large public area.

Home/SOHO

Home/SOHO users may only need *moderate* protection for local traffic on the wireless network. This can usually be satisfied by implementing WEP encryption. However, for communication with a remote corporate network, it is important that the access point supports VPN security in pass-through mode or by embedding a VPN client that can be shared between some of the devices connected to the wireless LAN.



Access point with VPN pass-through.

Note: This method does not address security concerns regarding data exchanged between client devices attached to the same wireless LAN.

Enhancing wireless security

The benefits of VPN technology can be enhanced by combining it with other security features. For example:

- *Token-based authentication:* Once a network is secured with VPN, user authentication can be strengthened. Additional verification of user identity can be implemented through hardware-based password generation (Entrust, RSA/SecurID, VASCO, etc.).
- *VPN profiles:* RADIUS or LDAP services can be used to manage individual user profiles. White/black lists can be created to control access to specific network resources or subnets.

Conclusion

The issue is not *are wireless networks less secure?* but rather *what are the best methods to secure a wireless network ?* Adopting the use of Virtual Private Networking leads to the application of a sound strategy based on strong user authentication and encryption achieved at the network (IP) layer without limiting the benefits of wireless LANs.