Wireless VPN

White Paper

SkyFidelity, Inc.

http://www.skyfidelityinc.com

Abstract

Wireless VPN advances the 802.11 standard to next level, making the technology a viable solution for a secure corporate world. SkyFidelity Industries is the first to integrate a Wireless Access Point with a VPN server in order to provide a turnkey solution that minimizes the impact on current network infrastructure. Each SkyFidelity unit creates a private wireless sub network for all wireless users. Based on security settings the unit will allow anonymous users to establish links and receive a non-routable IP. This link is used to request the VPN tunnel into the corporate network giving the authenticated user access to the needed resources.

The architecture scales gracefully horizontally: a SkyFidelity based backbone in a corporate environment can handle from one to thousands of users by simply adding more SkyFidelity units1. Each SkyFidelity unit enhances performance by managing the encrypted VPN tunnels locally, thus distributing the load among all the installed units.

SkyFidelity user management can be performed locally on each unit or centralized by the use of a RADIUS server. The RADIUS server can leverage current windows user name and passwords making the integration between wireless and wired networks seamless.

This white paper describes: key features of the Wireless VPN; the core technologies used in SkyFidelity's architecture; and deployment strategies for a corporate environment.

07/16

---

1 Available bandwidth is necessary by the wired networks in order to access resources.

Introduction

Wireless VPN

As corporate America searches for ways of increasing productivity and lowering costs, wireless technologies is playing a key role. Over the last couple of years the wireless technology has stabilized and it's been widely accepted. Wireless systems help to remove the overhead of running wires to every cubicle or room. Expanding access to new areas of a company can be performed at the time of need by employing wireless technologies, reducing the investment and associated costs when moving into new offices.

As with any new technology, weaknesses are exposed in its infancy. With wireless in particular the biggest flaw is Wired Equivalent Privacy (WEP), which attempts to secure the data that is being transmitted. SkyFidelity Industries has identified and provided a solution to this and other problems by providing the first integrated Wireless Access Point and a VPN server, which seamlessly integrates with Windows® or Mac VPN clients.

The high power units provide excellent indoor coverage for areas as large as 10,000 sq/feet per unit2.

Wireless VPN units have a simple web interface that only allow secure configuration of the units through SSL. Using these proven standards we ensure that no vital information will be gatherer when a user attempts to configure the units through the wireless interface. The web interface provides status information as well as configuration screens in order to setup the unit to work with the environment of deployment.

On the Ethernet interface the unit can act as a DHCP client in order to configure Domain, Gateway, DNS, and IP. This is the preferred method if users don't have to access the unit from the LAN side or if the DHCP server is leasing static IP addresses.

On the Wireless interface the unit can act as DHCP server leasing IP address to all the clients that establish a connection. Although a client is able to establish a link, all client requests will terminate at the base unit. This makes our unit a firewall within the corporate LAN; ensuring only authenticated users have access. The Wireless interface supports the hiding of Network Name or ESSID. This prevents occasional users from connecting to the wireless network with an ESSID of ANY. The Wireless interface also supports blocking clients by MAC address. This prevents unauthorized users to establish links with any SkyFidelity units making the wireless network a very secure environment.

Once a user has established a link to a unit they will have to be authenticated by the VPN server on the unit. The VPN server can be configured for local or remote user authentication. Local user authentication is kept in secure file systems which uses AES

---

2 This number can vary depending on the material used inside a building to separate offices and objects that might block the signal.

128 bit encryption. Even if someone tampers with the unit and tries a memory dump, they will not be able to retrieve usernames and passwords. Remote user authentication can point to any RADIUS server and use it to validate users against the domains user names and passwords or to a user database. By using this type of authentication the administrator's policies are inherited by the SkyFidelity based wireless network. This provides seamless integration between the wired and wireless networks for administrators and users.

Architecture

Connectivity

The SkyFidelity unit uses two powerful 300 to 600 mw radios that provides signal strength four times stronger that some of the existing wireless units, out in the market. In the event that the signal is being block or the distance is too great, wireless repeaters can be added to increase the reach. As the user travels from base to repeaters the established connection will continue to function. This makes the roaming from base to repeater seamless.

Security

Security is a big concern when ever you have data that's being transmitted and it can be captured by anyone that's listening. Wireless technology uses Wired Equivalent Privacy (WEP) as an out of the box solution to keep wireless network safe and reduce the administrative effort. WEP uses a shared key encryption, in theory those users who have the key will be the only ones able to decrypt the information being received. Unfortunately someone listening to a stream of about five minutes in length can identify the key that's being used to encrypt the data, rendering the solution useless.

SkyFidelity wireless VPN solves the issue of unauthorized users capturing corporate information that may be transmitted via the airwaves. Using MPPE 128 bit stateless encryption, we ensure that the key that's used to encrypt the data changes with every packet.

MPPE stands for Microsoft Point-To-Point Encryption Protocol. As the name implies, MPPE is an end-to-end encryption scheme representing Point to Point Protocol (PPP) packets in an encrypted form. The functioning is as follows: a client negotiates PPP with the ultimate tunnel terminator to initiate an encrypted session.

PPP packets are then encrypted using the MPPE protocol prior to injection into the PPTP tunnel. Because the encrypted tunnel is end-to-end, interim tunnel switches do not have the ability to decrypt the packets. MPPE supports the standard PPTP included in Microsoft Networking with integrated encryption. A 40-bit of MPPE is included with Windows® 95 through Windows® 7. A 128-bit version is also available as part as normal browser upgrades (constringent on export restrictions). Our system supports both 40 and 128 bit.

User Authentication

The authentication of users is done with the MS CHAP v2 standard, which works the following way:

1. The unit sends a challenge to the remote client, which contains a session identifier and a random challenge string.
2. The remote client responds with the following:
    a. The user name
    b. A random peer challenge string
    c. One way encryption of the received challenge string
    d. The session identifier

The unit or radius server checks the response from the client and responds with the following:

    e. A success or failure
    f. An authenticated response based on the sent challenge string
    g. The peer challenge string
    h. The encrypted response of the client

3. The remote client verifies the authentication response is valid and uses the connection. If the authentication response is not correct, the remote access client terminates the connection.

This method of authentication is used by Windows® servers, in order to provide seamless integration the SkyFidelity provides the same type of authentication.

Client Support

Client support is very important in order to provide a solution that will be widely accepted by all your users. The SkyFidelity unit uses the Point to Point Tunneling Protocol, in order to establish VPN sessions from wireless clients. The PPTP protocol is supported from Windows® 95 to Windows® 7, ensuring that most of the corporate users will be able to access the wireless network.

Deployment

Existing Infrastructure

Common corporate infrastructure is guarded by a firewall opening certain protocols and ports for access. The firewall provides protection from outside users and only users that are physically in the location have access to corporate resources.

Wireless VPN Integration

When a wireless access point is introduced into the network, there's a potential created for users outside the corporate network to gain access. The SkyFidelity unit provides the security of a mini firewall protecting the LAN from unauthenticated users. Once the user established a tunnel they will have access to the corporate resources. By using this technique the deployment of a wireless VPN is very simply. Each unit will dynamically assign non-routable IP address. When the user is authenticated a tunnel is created

and an internal IP address is assign from a previously configured pool. With minimal configuration and equipment the users will be able to go from wired to wireless network connectivity.

Summary

The SkyFidelity unit provides a secure and simple way for corporate users to have access to network resources. By using a similar architecture to that of a corporate firewall, the unit is able to use proven technology to keep the LAN secure. By using standards such as PPTP and MS CHAP v2 the unit ensures a seamless integration with Windows client and servers. This transparency of technology will make the deployment of a wireless solution a lot smoother.