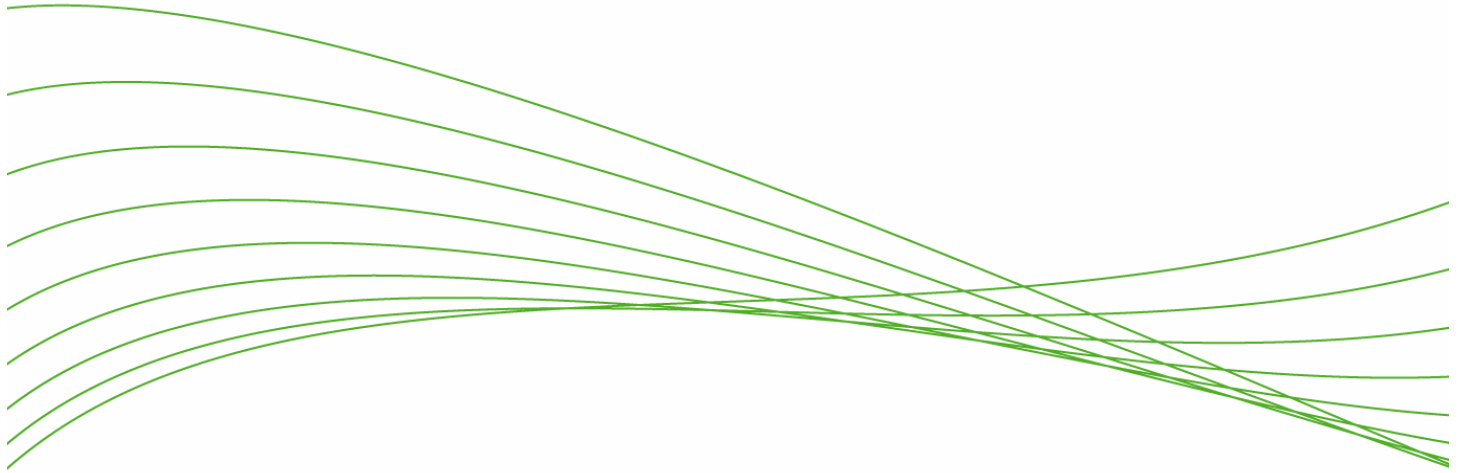


ProCurve Secure Access 700wl Series Wireless Data Privacy Technical Brief



Introduction	2
The Data Security Problem in the Wireless World	2
ProCurve 700wl Series Wireless Data Security	3
Distributed VPN Termination Service	4
Industry-Standard Security Protocols	5
Flexible Policy-based Security Requirements	5
Summary	6
For more information	7

Introduction

Security in a wireless network really addresses two separate, albeit related and complementary issues: protecting the network and its resources from unauthorized access; and protecting data as it travels over the air between the user and the network. The two ProCurve Secure Access 700wl series Technical Briefs, “Identity-Based Access Control” and “User Authentication and Authorization” discuss how the ProCurve 700wl series handles the network security problem. This Technical Brief addresses the issue of protecting data as it travels over the air between the user and the network.

The Data Security Problem in the Wireless World

Data security is an issue when traffic must travel over uncontrolled, potentially hostile paths to reach a particular network resource. Whether this is over the Internet or over the airwaves, traffic may be vulnerable to data theft or to being intercepted and changed, as well as posing a risk to the network itself from unauthorized users. Therefore, traffic must be protected to ensure data privacy and to prevent hackers from using these connections to launch attacks on the network. In the wireless world, where network traffic travels through the air on RF signals, traffic integrity is even more of a concern due to the ease of intercepting the traffic stream.

To address the problem of wireless data security, the 802.11 standard includes Wired Equivalent Privacy (WEP) – a method for providing encryption and authentication between wireless clients and Access Points (AP). However, WEP has proved to be weak and relatively easily broken, leaving data and the network vulnerable. The newer Wi-Fi Protected Access (WPA/WPA 2) delivers robust security with strong encryption but implementation requires an upgrade to the wireless infrastructure and WPA/WPA2 support on the wireless client. Therefore, alternate methods of ensuring data security are needed.

In the wired network world, Virtual Private Networks (VPNs) were developed to address the problem of data security for remote users that had to travel over insecure paths such as phone lines and the Internet. VPNs transmit data through encrypted tunnels that provide point-to-point security from the user to the VPN termination point within the network. This same technology can be adapted to wireless networks by encrypting and tunneling wireless traffic using the same VPN protocols such as Point-to-Point Tunneling Protocol (PPTP), or Layer 2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPsec) using strong encryption such as 3DES or AES.

VPNs, as designed for remote users connecting over relatively slow-speed dial-up connections, are usually implemented using centralized VPN termination, which provides a single VPN termination point within the network. However, wireless LAN users are likely to place a much greater strain on VPN termination services than do dial-up users, due to higher bandwidth connections as well as the potentially larger numbers of users entering the network through multiple connection points. Existing VPN services are not likely to be adequate. The need is for a distributed implementation (multiple VPN termination points) that can support the throughput and number of users that growing wireless use will require. Given that VPN services will need to be upgraded in any case, it makes sense to implement a distributed model for VPN termination that will allow for the flexibility and expansion that will be required over time.

Further, a design using a centralized VPN termination point means that the wireless network must be flat – i.e. all wireless access points must reside in the same broadcast domain, along with the VPN termination service – since a single VPN termination point would not support L3 roaming across subnets. This means that the organization must implement an overlay network, and cannot choose to integrate the wireless network into the wired network. By adopting a centralized VPN termination approach, a wireless network cannot take advantage of all the features of the wired infrastructure (i.e. redundant paths, reliability and so on).

Another disadvantage of a centralized VPN termination design for a wireless network is the relative inefficiency of the path packets must take from client to their eventual destination. In a centralized design, packets must travel through the network to the VPN termination point before they can be decrypted and then sent to their destination (see Figure 1).

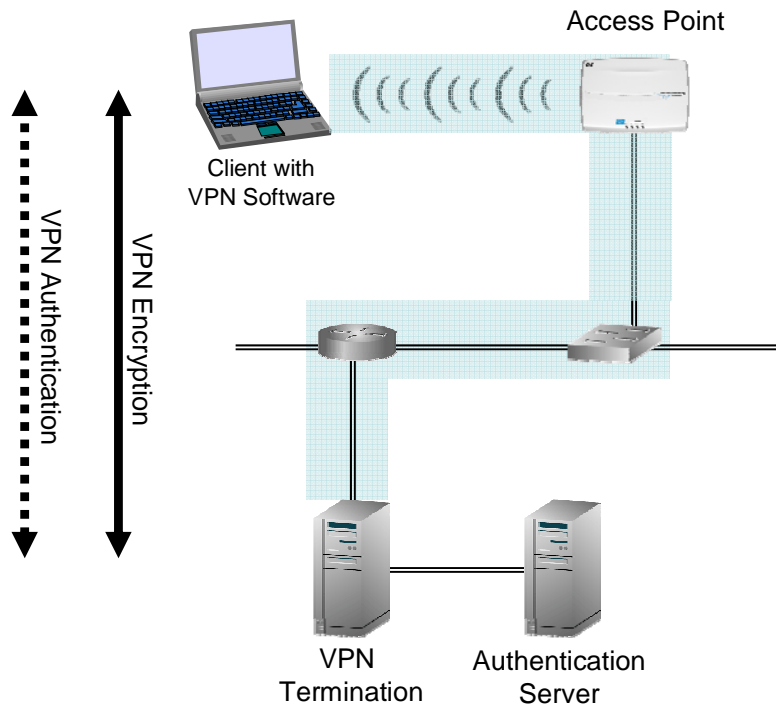


Figure 1: Data path for packets when VPN termination service is centralized

The goal of VPN termination in a wireless implementation is to provide secure termination for traffic traveling over the airwaves. Once that traffic reaches the network, it is not necessary to maintain the secure tunnel any further. Providing VPN termination services as close to the network entry point as possible minimizes network overhead and provides a more efficient path for packets from wireless clients – a packet will not need to traverse the network to a central VPN termination site, but rather can take a more direct route to its true destination.

ProCurve 700wl Series Wireless Data Security

The ProCurve Secure Access 700wl series adopts the same VPN technology used for remote clients in wired networks to protect traffic between wireless clients and the network, but implements it in a distributed service that provides the flexibility and scalability needed in a wireless environment.

Using VPN technology, the ProCurve 700wl series provides a point-to-point encrypted tunnel between the wireless client and ProCurve Switch xl Access Controller Module – a termination point within the network (see Figure 2). The client traffic is tunneled through the access point to the ProCurve series 5300xl switch with xl Access Controller Module, and does not depend on a centralized VPN termination service.

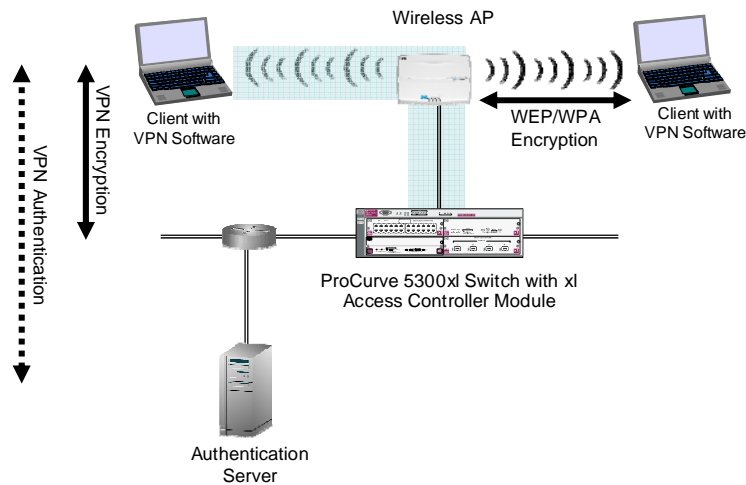


Figure 2: Distributed implementation with ProCurve Switch xl Access Controller Module as VPN termination service

The ProCurve 700wl series provides the flexibility and scalability needed for the growing demands of a wireless network – as requirements increase, the addition of ProCurve series 5300xl switch with xl Access Controller module automatically adds VPN termination services. Because these services are distributed at the points where wireless traffic enters the network, the issue of packet path inefficiency can be avoided. Also, this design means that the wireless network can be integrated into the wired network to take advantage of the network infrastructure, without sacrificing L3 client roaming.

Distributed VPN Termination Service

With the ProCurve Secure Access 700wl series, VPN termination services are enabled and configured centrally (through the ProCurve Access Control Server 745wl) but are actually implemented within each Switch xl Access Controller Module. This enables VPN termination at the point where wireless clients enter the network.

Having the termination point at the edge of the network, close to the client, is much more efficient for packet processing – packets do not need to travel to a centralized termination server before their end destination is known. But this method still terminates the traffic far enough from the client – i.e. within the network itself – to ensure robust protection for traffic over the airwaves.

Further, the ProCurve 700wl series implementation of VPN tunneling allows clients to roam while maintaining their secure tunnel – even when they roam between different subnets (L3 boundaries). The ProCurve Switch xl Access Controller Module can securely tunnel traffic between different Access Controllers without requiring the user to re-authenticate or lose session connectivity. This means that the wireless network does not need to be flat – it is not necessary to implement an overlay network structure to enable wireless client roaming. The wireless network can be integrated into the wired network, if desired, to take advantage of the wired network infrastructure features for reliability, redundancy and the like, without sacrificing the ability for wireless clients to roam.

Finally, by distributing VPN termination services, the ProCurve 700wl series can easily scale to support growing numbers of wireless users. As the number of users wanting network access grows, VPN termination needs grow also. In a centralized VPN server model, scalability may be limited by bandwidth and a single server as a bottleneck. With ProCurve 700wl series solution, adding additional Access Controller Modules not only provides more connection points for clients, but automatically expands the VPN termination capability to support those additional clients.

Industry-Standard Security Protocols

The ProCurve 700wl series supports industry-standard encryption protocols including Internet Protocol Security (IPsec), Layer 2 Tunneling Protocol (L2TP) over IPsec, and Point-to-Point Tunneling Protocol (PPTP). It also supports connection using SSH with port forwarding. Any or all of these protocols can be enabled and simultaneously used in the ProCurve 700wl series.

If IPsec is enabled, it can be configured to use either a Public Key Certificate or a shared secret, and to use any of a number of methods for IKE and ESP encryption, including DES, 3DES, AES, Blowfish or CAST for encryption, and MD5 or SHA-1 for integrity, as well as Diffie-Hellman Groups 1, 2 or 5.

The benefit of using standard VPN protocols, in addition to the high level of data security that they provide, is that many of them are supported by standard client software provided as part of operating systems such as Windows 2000, Windows XP, or Mac OS-X. No proprietary client software is required – the user simply needs to configure the appropriate network connection using the built-in capabilities on his client system.

Flexible Policy-based Security Requirements

An important benefit of the 700wl series security implementation is that encryption requirements can be enforced on a per-user basis. This allows you to distinguish the needs of various types of users – requiring strong encryption for users with access to sensitive data, while allowing other users – guests, for example – to connect without using any end-to-end encryption.

The 700wl series can be configured to use any or all of the standard security protocols. However, once the basic security configuration is in place, (with the selected protocols enabled) the actual enforcement of security requirements is done on a case-by-case basis through the Rights Manager Access Policy of the ProCurve Access Control Server 745wl.

One of the functions of an Access Policy is to define the encryption methods that should be allowed or required for users affected by that Access Policy. An Access Policy can be configured to *allow* selected encryption methods – meaning that both clients that use a selected encryption protocol as well as clients that do not use encryption may be granted access to network resources per the Access Policy. If an Access Policy is set to *require* an encryption protocol, then only clients using the required protocol will be granted access.

For example, you may want wireless users connecting to sensitive corporate resources to use encrypted connections, but you may not want to require encryption for visitors if you only provide them with Internet access, as they may not normally use encryption. To accomplish this, you can create Access Policies that require different levels of encryption. This is needed because it is entirely possible for the different types of users, Employees vs. Guests, for example, to come into the network through the same Access Point. Therefore, the wireless deployment needs to recognize different types of users and enforce the appropriate encryption policies for each type.

For example, you could create an Access Policy for finance personnel that requires L2TP over IPsec. Then only finance users connected using L2TP/IPsec will be granted access. A finance user not using encryption will not be granted access even though he or she would otherwise be authorized to access those resources.

Having this type of control is extremely helpful in that when a policy is configured to require encryption, no packets will be accepted from that client outside of the encrypted tunnel. This means that an unauthorized user cannot try to “piggy back” on an existing session since they cannot get into the encrypted tunnel.

For visitors, you could leave the Guest Access Policy set with encryption disabled. Thus, visitors would be able to directly log in as a guest without needing to set up an encrypted client connection.

See the “ProCurve Secure Access 700wl Series: User Authentication and Authorization Technical Brief” for more information about the other aspects of access control in the ProCurve Secure Access 700wl series.

Summary

The ProCurve Secure Access 700wl Series provides a very powerful solution for enabling wireless access to an organization's network while at the same time providing a high level of security for client traffic as it travels the airwaves to reach the network. The ProCurve 700wl series provides termination services for a number of standard secure protocols (PPTP, L2TP, IPsec, and SSH) that can be used to ensure data privacy without requiring proprietary software on the client. Because the ProCurve 700wl's VPN termination services are distributed, the system can provide this high level of data security while at the same time providing full L3 client roaming, along with the scalability and flexibility required for a wireless network implementation.

For more information

For more information about ProCurve Networking products and solutions, visit www.procurve.com.

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com



© 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

5982-8265EN, Revision 1, 6/2006