SSL VPN for Secure Wireless LAN Access

Overview

Have you been tasked with deploying a wireless LAN (WLAN) infrastructure at your company? Are employees and co-workers clamoring for wireless access but unable to get manager approval "because it is not secure and our data is too valuable?" You've probably done some research and might be looking at products from WLAN vendors such as Cisco® Systems, Aruba Networks®, Trapeze Networks™, Symbol Technologies, or others. While these WLAN vendors offer valuable products, you might not need their solution if you already have an SSL VPN device or appliance in place, or are planning to implement one (perhaps to replace your IPSec VPN).

Challenge

For most deployment scenarios, an SSL VPN appliance can provide many of the features and benefits of a special purpose WLAN controller for wireless access, but at a much lower cost and with greater flexibility. The basic premise is very simple: treat your wireless LAN (for example, 802.11g) users the same as you would treat a remote user accessing your network from home or a coffee shop. In other words, from an implementation and policy perspective, treat remote users and corporate wireless users exactly the same. This is also helpful for the end user because their user experience will be exactly the same whether they are accessing the network from home or over the corporate wireless network. They will not have to launch a separate client for wireless access or go to a different URL or portal.

Solution

So how does an SSL VPN solution for WLAN access compare to what a WLAN vendor might offer? Below are the key selling points for WLAN solutions and an explanation of how SSL VPN can offer similar, complementary, or greater functionality.

1. **Centralized security and management**

   An SSL VPN is a centralized point for security and management. The appliance is the single point of contact for all remote access traffic and, therefore, it is where traffic is terminated and unencrypted. Because all traffic comes through the appliance, it is the perfect place to define user policies and collect statistics such as who accessed what, and when.

   In fact, if an enterprise deploys both an SSL VPN and a WLAN controller, in some sense they are taking away one of the main advantages of centralized management: a single or centralized place to define access policies. Clearly one way to prevent this is to deploy SSL VPN for both remote and wireless access needs.

2. **Strong and scalable data encryption for maximum security**

   Data encryption is a strong point of SSL and is used to secure the most sensitive transactions (for example, online banking) on the Internet. To address scalability, many SSL VPN device vendors provide hardware-based SSL acceleration. The encryption and overall data security provided by SSL VPN devices is as good or better than that provided by any WLAN vendor.

3. **Scalability**

   Scalability is typically measured in terms of number of concurrent users on a given appliance (for example, 2,000) and throughput (Mbps or Gbps). On this measurement, WLAN appliances and enterprise-grade SSL VPN appliances are in the same range.

4. **Endpoint security**

   Many SSL VPNs offer endpoint security that is superior to what is offered on most WLAN appliances. For example, some SSL VPNs offer a wide array of endpoint checks such as the presence of a specific antivirus (for example, Symantec) or personal firewall software.

5. **Roaming or mobility**

   Some WLAN controllers have features that enable a user to “seamlessly” roam across access points (for example, a user can walk from one building to another without losing access). Roaming support is not common with SSL VPNs but at least one vendor offers a feature called “auto reconnect.” This feature will automatically reestablish a connection if it is temporarily interrupted when moving from one access point to another or when there is a glitch in the Wi-Fi signal, for instance. With auto reconnect enabled, most applications will not time out and will continue as before once the lower layer connection is reestablished.

6. **RF monitoring and planning**

   This mainly revolves around tools to help efficiently position wireless access points (APs) to avoid dead spots (holes in Wi-Fi coverage), detect sources of RF interference, or identify faulty access points. These tools don’t have anything to do with securing your applications or data and are therefore complementary to an SSL VPN solution. In other words, you can install SSL VPN to secure wireless access and also choose to use these tools if you feel the need for better RF monitoring and planning.

   While these tools may be helpful for large (for example, hundreds of APs) deployments, they may not be needed for the vast majority of medium size enterprise installations. One thing to keep in mind is that these tools will only work with a particular WLAN vendor’s APs; therefore, you have very little flexibility. With an SSL VPN approach you can use any AP on the market and, in many cases, you can overcome deployment problems by simply installing low cost APs.

7. **Rogue access point detection**

   A rogue AP is one that the company does not authorize for operation. For example, an employee might plug an AP in to an open data port and suddenly anyone with Wi-Fi capabilities can use that access point. Rogue AP detection is a part of what some WLAN vendors refer to as “securing (or locking) the air.”

   Rogue AP detection and other methods used to prevent unwanted users from jumping onto an access point are complementary to SSL VPNs. These methods provide a first-level of defense against someone exploiting an access point, but even if they do exploit it, the SSL VPN is in place to make sure that the critical applications and data are protected. Because of the defense offered by the SSL VPN, many enterprises are OK with just deploying WEP or WPA encryption on the access point, despite the widely publicized shortcomings of these security measures. The thinking behind this is that if bad guys might break down the first door, you have an even stronger one behind it.

   In summary, if you are currently using an SSL VPN for remote access, you already have a robust wireless access solution in place and may not even realize it. There is no reason to treat your corporate wireless LAN access any differently than you do for remote (for example, home) access. From an IT management and end user perspective, these two access scenarios are nearly identical—so why not treat them the same?

About F5

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5's extensible architecture intelligently integrates application optimization, protects the application and the network, and delivers application reliability—all on one universal platform. Over 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to www.f5.com.