

VPN Overview

Secured remote access to corporate resources through the use of a **Virtual Private Network (VPN)** has become an essential requirement in today's enterprise as businesses extend network access to home workers, road warriors and business partners across the globe. One of the most efficient and cost-effective methods for fulfilling remote access requirements at many organizations is a Secure VPN, which to ensure security sends encrypted traffic over a public network such as the Internet. The two dominant types of Secure VPN technology are **IPsec** and **SSL**.

IPsec VPNs

IPsec, short for Internet Protocol Security, can run in either *transport* or *tunnel* mode, each having significantly different implications particularly with regard to security – tunnel mode will encrypt both the header information as well as the data transmitted, whereas transport mode will encrypt only the data. Keys must be shared by both the sender and recipient in order to correctly decrypt the transmission.

IPsec works at Layer 3, or the Network Layer of the OSI Model, which enables it to operate independently of any application. An IPsec VPN creates a tunnel between two endpoints through which any number of connections and protocol types (Web, email, file transfer, VoIP) can travel. The original IP data packet is re-encapsulated so that all application protocol information is hidden during the actual transmission of the data.

A typical deployment will consist of one or more VPN gateways to the secured networks. Special VPN client software must be installed on each remote access user's computer, and each VPN client must be configured to define which packets should be encrypted and which gateway is to be used for the VPN tunnel. Once connected, the client becomes a full member of the secured network, able to see and access everything just as if that system was actually physically connected to the network.

SSL VPNs

SSL (Secure Socket Layer) VPNs are often referred to as transparent, or clientless, due to the lack of any additional client-side VPN software that must be explicitly installed. The SSL components required to create a secure channel from the remote system are a part of all major Web browsers, at least one of which is always already available on virtually every modern computer. The only new item that is necessary is a designated SSL VPN server, to act as the gateway between the secured network and all remote systems.

The SSL protocol operates in Layer 7, the Application Layer, allowing it to act as a proxy for the secured resources. Authentication of both the client and the server is achieved during the initial handshake routine where both parties identify themselves via digital certificates. The handshake process also generates session keys which are used to encrypt all traffic sent and received during a remote access session.

An SSL VPN can maintain and enforce finer-grained access control policies, to individual internal resources as well as by individual users, by intercepting all traffic between the authenticated remote system and the requested resource inside the secured network. This introduces greater flexibility since now virtually any computer with an Internet connection can be used for secure remote access – home computers, computers on customers' premises, and even Internet cafés!

IPsec vs SSL VPNs

IPsec and SSL each have their own advantages, so what is “better” may often come down to what is most suited for your network, but many organizations are increasingly turning to SSL VPNs for the additional benefits available.

Reliance on Network Membership

Because an IPsec VPN connects on a network level, the remote computer is assigned an internal IP address upon connection and becomes a part of your intranet. For some remote users, however, the IP address space used by the IPsec VPN and/or the DNS servers for the secured network may conflict with the existing IP address space and DNS servers already in use at the remote location, or the special ports required for VPN access may be blocked. Special NAT rules may be needed to ensure that remote sites are able to access certain internal-only systems, or special provisions made so that the internal DNS servers are accessible to the remote site without limiting existing access. When these types of issues arise, a non-trivial effort on the parts of both the remote user and the I.T. department may be required to resolve these issues.

No network addressing conflicts exist when an SSL VPN is used because the remote system need not maintain an address on the internal network, so no additional customizations either remotely or locally would be required.

Limiting Range of Access

Once connected via an IPsec VPN, everything that the authenticating user has access to when on-site will also be available with remote access. Any and all types of transmissions between the authenticated remote computer and the secured network are allowed through unfiltered, providing the remote computer with access to everything in the network with no extra permission settings required, and allowing it to be seen and accessed in return.

This does mean, however, that there is no easy way to *prevent* access by an offsite user to resources that should only be available to those who are physically on the premises, such as systems containing confidential data or even the printer in the CEO's office. It also introduces a possibly unsecured entry point into your network, since an infected remote computer can be the source of unanticipated infiltration such as by a virus or other malware. As a result, most organizations prefer to limit the use of IPsec remote access whenever possible, and to only a relatively small portion of their user base.

In contrast to the wide-open access provided by an IPsec VPN, an SSL VPN operates as a proxy so that only authorized traffic destined for approved resources are allowed through, cutting off any chances of accidental infection spreading to other internal resources on the network. Authorization can be given not just for the remote system to access the secured

network, but also for only designated users to access a particular internal resource. This prevents the need to have the same access permissions forced upon all remote users, since the system administrator can now easily adjust access to specific internal resources on a user-by-user basis without performing any additional configuration changes on the networked resource.

Support and Maintenance

When using an SSL VPN, the lack of specialized VPN software clients for the end-user means that there is one less application that your I.T. department will have to support and maintain. SSL components are updated as part of browser maintenance, with any additional modules that may be required being dynamically downloaded during an encrypted session.

The Barracuda SSL VPN

The Barracuda SSL VPN is an integrated hardware and software solution that provides the advantages of both IPsec and SSL, enabling secure, clientless remote access to internal network resources from any Web browser.

Taking only minutes to install, the Barracuda SSL VPN is extremely fast and easy to deploy to all or just some of your user base, no matter what the size of your organization. Integration with popular authentication protocols such as LDAP allows you to import user information directly from your user database or LDAP server, or you can create local accounts if you so desire. And with no client to distribute and no additional network configurations required, all you need to do now is to configure your access policies and you're ready to go.

The Barracuda SSL VPN can also provide full network connectivity using the Barracuda Network Connector, so that specific authorized users can be provided wide-open access to the entire network in a manner similar to what is provided by IPsec.

To set more secure access rules, the easy-to-use administrator interface allows you to instantly identify categories of resources such as "Web Forwards" or "Applications", and view and set policies by an individual resource (internal Web applications or network shares, telnet or SSH-based access, or even remote desktop access such as by RDP or VNC). Policies can also be viewed and modified for individual users (locally created or imported from LDAP) or by groups, so that when remote users log in, they will be able to tell at a glance from their own personalized home page on the Barracuda SSL VPN exactly which internal resources are available for that session.

Organizations must balance their growing remote access needs against their available IT resources, and a remote access solution must be easy to set up and maintain while having minimal impact on the IT helpdesk. By incorporating the Barracuda SSL VPN into your remote access strategy, you gain the benefits of secure remote access without the cost and complexities of an IPsec solution.