VPN Access for mobile users: IPSec or SSL?

Mike Cochrane
mike@resnet.net.nz

October 2004

Abstract

Virtual Private Network (VPN) Access for mobile users presents a very different set of challenges to those of a traditional Site-to-site VPN. This paper provides an overview of two distinct VPN solutions, contrasting their features and ultimately looks at the question; Which VPN solution suits mobile users?

Introduction

Virtual Private Networks (VPNs) provide remote users and sites with access to resources on corporate networks. Traditionally VPN access was been restricted to branch offices and other fixed sites.

VPNs bridge the gap, between the corporate head office and remote branch offices, using public networks such as the Internet. Through the use of encryption and authentication protocols, data is transferred between sites in a way that guarantees both the confidentiality and integrity of the data.

Increasing numbers of mobile users, needing access to corporate networks, is changing the requirements for VPNs. The remote site is no longer fixed in location, nor is it always owned by the corporate. Remote sites are now as varied as the users that use them, from cyber cafés and airport kiosks, to laptops connected to

WiFi hotspots, to corporate parters. Traditional VPN solutions are not always the most appropriate solution or even an option for mobile users.

Until recently, Internet Protocol Security (IPSec) Virtual Private Networks have been the only option to connect sites via public networks[AVE04]. As the number of users requiring remote access increases, the suitability of IPSec VPNs has decreased. SSL VPNs have been created to fulfil the new requirements of mobile users. SSL VPNs are based on the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol, a protocol that has been used for a number of years to secure websites.

IPSec VPNs

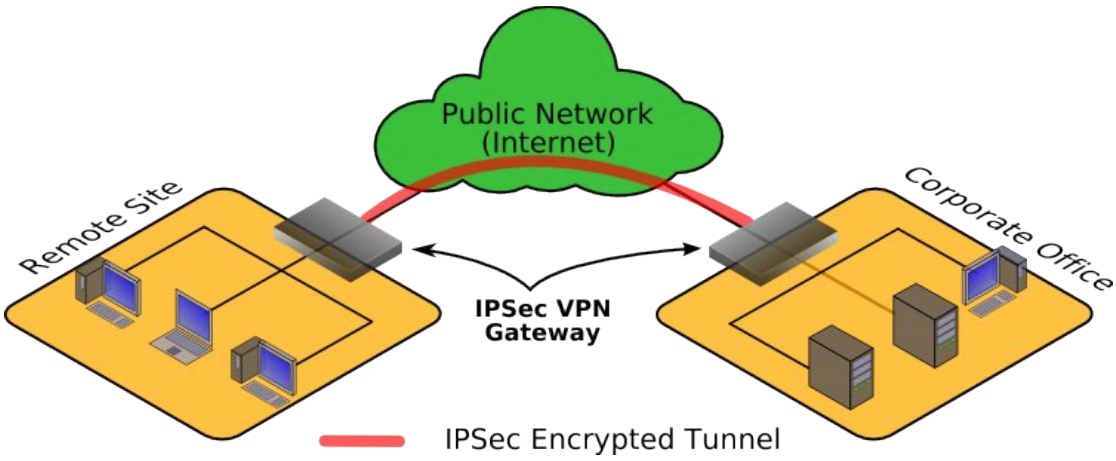
History

Internet Protocol Security (IPSec) is included as part of the the Internet Protocol version 6 (IPv6) created by the Internet Engineering Task Force (IETF).[BMY02] IPv6 is expected to be the replacement to the current version, IPv4.

Usage

IPSec VPNs has been implemented on many different platforms, including Windows, Linux, and also on network equipment from infrastructure vendors such

Figure 2. A typical IPSec VPN. Remote users connected in an edge-to-edge model. All data is encrypted from the edge of the corporate network to the edge of the remote site network.

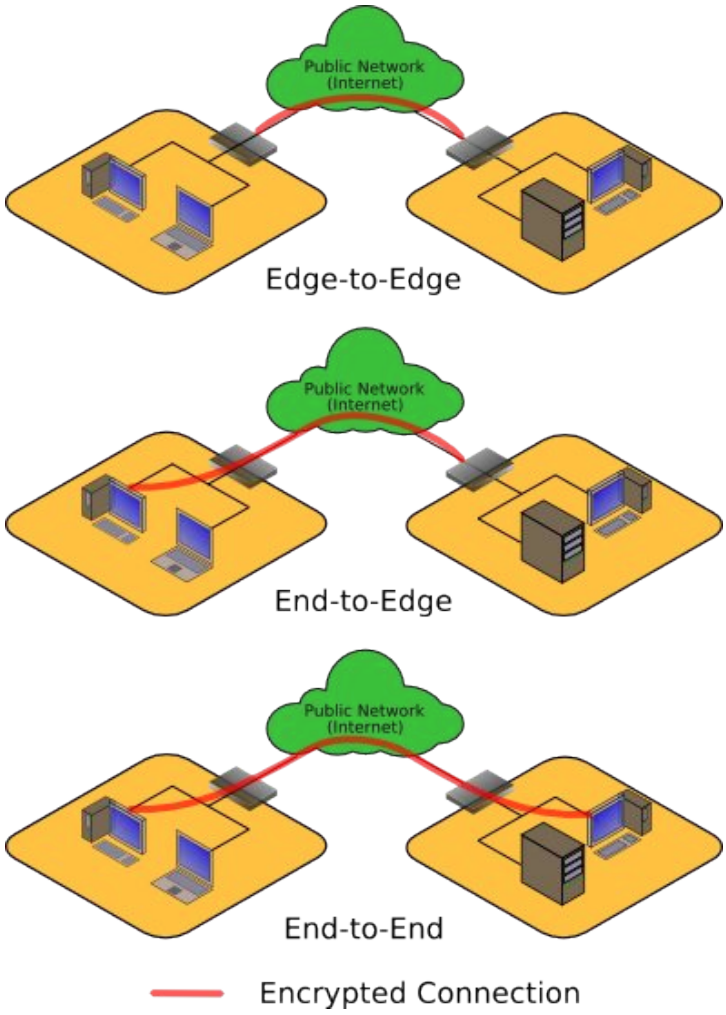


as Cisco and Nortel.[AVE04] Site-to-site VPNs have been the main use of IPSec VPNs, typically connecting a branch office to a corporate centre via the Internet or a Metropolitan Area Network (MAN). A router or VPN gateway is normally installed on the edge of the two networks and a VPN connection established between the two gateways. This is also know as a site-to-site network, or an edge-to-edge connection.

Features

IPSec is not itself a protocol, but a framework that covers a number of different protocols and functions. IPSec has two modes, transport and tunnel. [BMY02] Tunnel mode creates a "tunnel" through the Internet and transports data using this tunnel. This tunnel provides data integrity, origin authentication, and encryption to all the data flowing through it. Tunnel mode is used to connect a host to a VPN gateway to give it access to an entire network. After a tunnel is established, the hosts at the remote site can act as if it is connected directly to the remote site, this is know as an edge-to-edge VPN (see Figure 2). Transport mode can only be used between two hosts, and provides a similar set of features as a tunnel.[RFC 2401]

Figure 2. Secure Connection scenarios. Three different scenarios where secure connections are used. Edge-to-Edge between networks. End-to-edge between a single host and a network. End-to-end between two individual hosts.



IPSec has a number of extensions, including one for data compressions (IPComp), and Anti-replay services. [RFC

2401] There are a minimum set of features that must be implemented to a ensure computability, most suppliers have added a number of the optional features to provide additional security.

IPSec VPNs can also be used in an end-to-edge situation, where an individual client connects directly to a VPN gateway. The mobile client requires IPSec client software to be installed and correctly configured to access the resources of the remote network or the use of a separate VPN gateway to handle the connection.

IPSec provides a transport of all data regardless of protocol (e.g. TCP, UDP, ICMP) between the two ends of the connection. This allows almost any IP based application to work seamlessly on the remote client.

IPSec VPN Security

To consider the security of IPSec for mobile users, only the tunnel mode is being considered. IPSec provides security for all data while it is in transit between the two sites. It also provides a level of security against traffic flow analysis by combining all the data flows into a single flow, through the tunnel.

The minimum level of encryption required for IPSec is DES-CBC encryption, this is known to have weaknesses. [RFC1829][HAE97] Using IPSec with the minimum level of encryption is not advisable. When using IPSec systems from different manufactures it is important to check they have implemented a common, strong, encryption method so the minimum level is never used and confidentiality can be assured.

IPSec VPNs give full view of the network they are connected to, giving access to possibly multiple servers and other hosts on this network. While this may be desirable, the security of all these systems must be carefully audited and

maintained. The access controls all these systems may need to be updates every time a VPN users is added or removed, adding considerable administrative overhead.

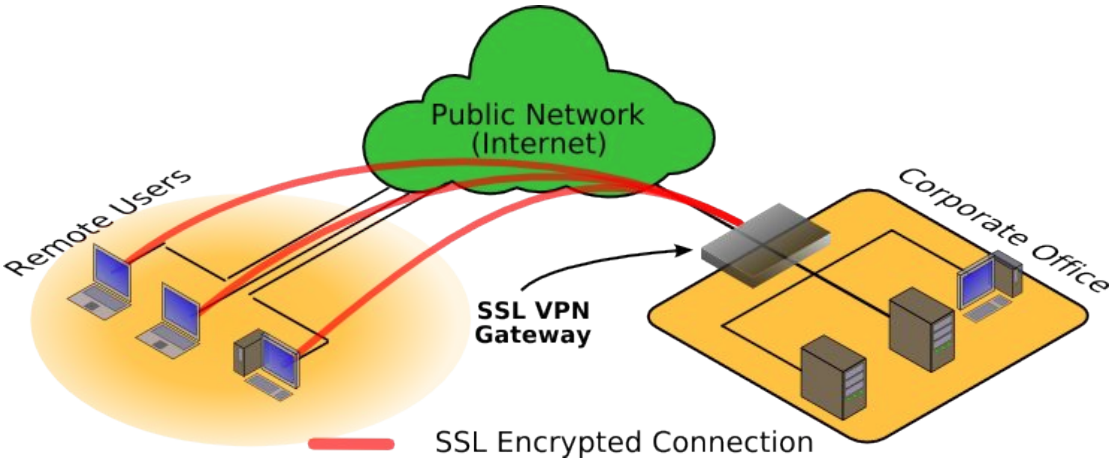
Mobile users are often working on laptops or other computers that are not controlled by the corporations. These computers may have worms of virus on them, there is potential for the worm to infect other computers on the network via the VPN connection. Further the use of packet sniffers to identify infected systems is not usable as all the packets are being encrypted and are unidentifiable without decryption.

SSL VPNs

History

Virtual Private Networks based on the Secure Socket Layer/ Transport Layer Security(SSL/TLS) protocol are referred to as SSL VPNs. The SSL protocol was originally developed by Netscape Communications in 1994 and approved by the IETF as a standard in 1999 under the more general title, Transport Layer Security [BMY02][RFC 2246]. SSL was created to secure connections between users and web sites. It has since been used to secure other protocols, such as mail protocols (IMAP, SMTP).

Figure 3. A typical SSL VPN. Remote users connected in an end-to-edge model. All data is encrypted from the edge of the corporate network to the end user.



Usage

SSL can be implemented in two way at the corporate office end. The first way is through using SSL enabled applications, common examples are secure web servers (HTTPS) and mail servers.

The second is to add a SSL VPN gateway to the network. This gateway receives the connection from the remote user, then transforms it into a request that is appropriate to the local network and make the request on behalf of the remote user. [HAR03] This solution is by far the most flexible method, giving access to applications and resources that were not originally designed to be accessed over an SSL connection using Reverse-Proxy technology. The VPN gateway provides a central point where all access rights are specified and maintained.

The client side of SSL VPNs is typically a standard web browser. All the major web browsers (Internet Explorer, Mozilla etc.) have SSL support built in. Installation of additional client software is not normally required. A number of other common user applications have built SSL support such as email clients (neg Outlook) and address books (via LDAP).

Features

SSL provides encryption and data integrity at the application level. SSL VPNs require applications that are aware of SSL.

The SSL protocol allows for varying strengths of encryption. The SSL specification defines over 20 ciphers. This gives SSL a range of encryption options that vary in strength and computationally complexity. Allowing for a lower processor load cipher to be used on lower power portable computers such as PDAs and laptop computers.

SSL has a number of extensions, including data compression, using the same method as IPSec's IPComp extension.

SSL VPN Security

In considering the security of a SSL VPN, only an installation using a SLL VPN Gateway will be considered. This gives the most complete set of features and is similar to an IPSec VPN using a tunnel, as previous looked at.

The security of SSL depends partially on the cipher being used, SSL has the same minimum encryption as IPSec, which has known weaknesses. Fortunately SSL is a very mature protocol and almost all implementations include a number of the strong encryption ciphers.[MAY03]

Typically all SSL VPN connections to the gateway are done via port 443, this port is almost always accessible from any corporate network as it is used for accessing secure websites. No additional outgoing ports need to be opened on the firewall. This avoids any potential drop is security to connect to the VPN gateway.[ARA03]

The SSL protocol authenticates the server it is connecting to, in an SSL VPN situation it verifies the identity of the SSL VPN Gateway, remote users can be assured they are actually connecting to the gateway and that their connection has not been redirected to a malicious gateway. The protocol also provides for client authentication, so the remote user can also be authenticated at the time of connection.

Traffic flow analysis is a possibility in an SSL VPN. The pattern of traffic could be used to guess at the type of data being transferred, while this is posses no risk to the confidentiality of the data being transferred, in some situations it may not be desirable.

SSL provides end-to-edge and end-to-end options. SSL VPN traffic is encrypted as

soon as it leaves the remote computer. There are no parts where data is transferred in clear text, as with an IPSec VPNs.

What mobile users want

Mobile users have a specific set of requirements. These are often different from the requirements of users who work from home, or other remote users such as corporate partners. The requirements of mobile users also varies between organisations and industries. Some requirements to consider and how IPSec or SSL VPNs may fulfil these:

Easy to use

Mobile users don't want to be dealing with difficult to use systems before getting access to what they want. SSL VPNs are as easy as accessing any other secure website, for most users this is a very easy to use solution. IPSec VPNs typically require a connection process before the data is available, a number of software vendors are releasing products that automatically complete this process.

Seamless Roaming

Seamless roaming, the ability to move between sites and connections without losing access. Complicated procedures to re-establish a connection after moving between wireless hot spots, or from a wired network to a wireless network, are undesirable and prone to user errors. IPSec tunnels need to be reconnected if the network address of the mobile user changes. Some VPN software will automate this, but not all software running over IPSec connections will continue running when the tunnel is disconnect and reconnected. SSL VPNs only establish a secure connection for the few moments when data is being transferred, permanent connections are not created. Roaming will only affect a SSL VPN if the transition happens during a transfer of information, in most cases a simple re-request of the information is all this is needed. SSL VPN applications are designed to support

connections being created only when needed, roaming is unlikely to cause any issues.

Access from Anywhere

Restrictions on where and how mobile users can get access, impacts productivity and freedom to have a truly mobile workforce. IPSec VPNs require client software to be installed and configured before connecting, for mobile users who always use the same computer (e.g. a laptop or PDA) to connect this is not a problem. For users who need access from any Internet connected computer an SSL VPN is likely to be the simplest option. Any computer with a web browser will allow the user to access the site. Many firewalls in hotels and wireless hot spots restrict what protocols can be used, SSL VPNs use a widely used protocol and almost all firewalls, even heavily restricted ones, will allow access to a SSL VPN. IPSec VPN connections require access to ports that are specific to IPSec VPNs and are potentially not accessible.

Which VPN solution suits my mobile users?

The most important thing to consider in selecting a VPN solution for mobile users is to look at what the users need access to.

For mobile users needing access to a wide range of resources from a small number of locations, an IPSec solution may prove to be the most appropriate. A wider range of software will be accessible over an IPSec VPN with little, or no, modification or reconfiguration.

For users needing access from anything that can connect to the Internet (airport kiosks, cyber-cafés, hotels, tablet PCs, PDAs, mobile phones etc.) SSL VPN solutions are probably going to be the simplest solution allowing consistent access of a large range of clients. [ARR02]

Where the mobile users are very dynamic, with many short term users, or user access requirements change frequently, SSL VPN solutions are likely to require the lease amount of time to manage. Adding new users needs to be done only on the gateway, individual servers do not require knowledge of individual users. Clients only need to be given a user name and password to authenticate, and get the access they need, immediately. No software needs to be distributed, installed and set-up.

It is clear that both IPSec and SSL VPNs have a place in mobile solutions, and which is right for your particular user base is dependent on the specific requirements of those users. Many large organisation may find a combination of both IPSec and SSL VPN solutions both appropriate and necessary to support the needs of a varied business world.

References

[ARA03] Ken Araujo, "SSL VPN Gateways: A new approach to secure remote access", October 2003, *Continuity Central*, http://www.continuitycentral.com/feature038.htm

[ARR02] ArrayNetworks, "SSL VPN vs. IPSec VPN", July 2002, *ZDNet*, http://itpapers.zdnet.com/abstract.aspx?docid=38804

[AVE04] Aventail Corporation, "Comparing Secure Remote Access Options: IPSec VPNs vs. SSL VPNs", August 2004, *ZDNet*, http://itpapers.zdnet.com/abstract.aspx?&docid=45944

[BMY02] Christian Blaafjell, Mei-Pin Lan, John O'Dwyer, Hong Jieh Daniel Yang, "A Comparative Analysis of IPSec and SSL", 2002

[HAE97] Haeni, Reto H., "IPV6 vs. SSL - Comparing Apples with Oranges", January 1997, The George Washington University, Archived: http://www.cu.ipv6tf.org/seguridad.htm

[HAR03] Andrew Harding, "SSL Virtual Private Networks", July 2003, *Computers & Security*, Volume 22, Issue 5, Pages 416-420

[MAY03] Susan May, "SSL or IPSec? Or both?", October 2003,

Communications News,
http://www.comnews.com/stories/articles/c1003ssl.htm

[RFC 1829] Karn, Metzger & Simpson, "The ESP DES-CBC Transform", August 1995, *IETF Internet Working Group*, http://www.ietf.org/rfc/rfc1829.txt

[RFC 2246] Dierks & Allen, "The TLS Protocol Version 1.0", January 1999, *IETF Internet Working Group*, http://www.ietf.org/rfc/rfc2246.txt

[RFC 2401] Kent & Atkinson, "Security Architecture for IP", November 1998, *IETF Internet Working Group*, http://www.ietf.org/rfc/rfc2401.txt