ISAS Report

Remote Access for VPNs

Presenter: Aureo P. Castro

Good Evening. I will be presenting the results of my research on the topic: Remote Access for Virtual Private Networks. I will first discuss the features of the two basic types of VPNs based on the encrypting technology used. Then, I will show typical architectural models of the two basic types and then give examples of clients used in accessing the VPN services or applications.

IPSEC VPN

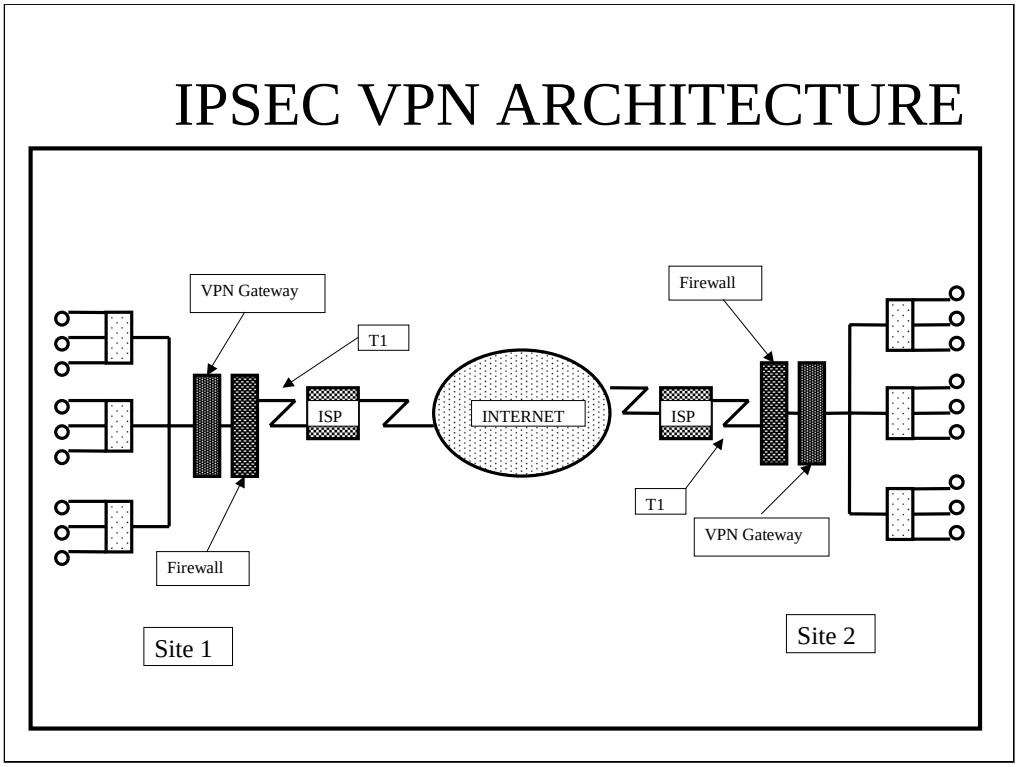
- Uses IPSEC protocol to provide secure end-to-end connections
- All IP types and services supported
- Connectivity adversely affected by firewalls, NAT and proxy devices
- Requires client installation and configuration
- Same technology used for both site-to-site and remote access
- Fail-over without dropping session is available
- Client can be more securely configured

The IPSEC type of VPN uses the IPSEC set of protocols to provide for a secure end-to-end connectivity among the company's LAN sites. This type of VPN is a complete solution that may be used either to connect two sites and at the same time to provide remote access for the company's road warriors. In addition, it provides for a wide range of IP services typically found inside of a LAN environment. It is a more stable and robust solution as it provides for a fail-over feature without dropping on-going sessions. However, remote access is implemented using a custom designed client which needs to be installed and configured for employees who need to perform remote access connections. Lastly, the IPSEC type of VPN suffers from connection issues raised by the presence of firewalls, NAT and proxy servers.

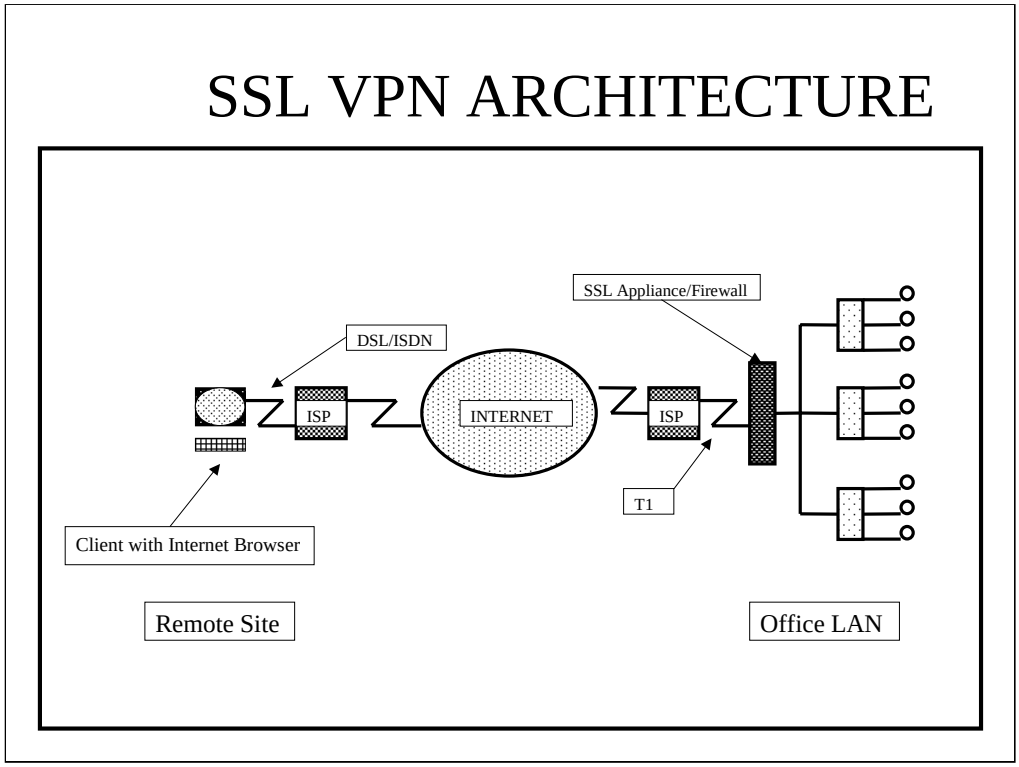
SSL VPN

- Uses SSL to provide secure connection between client and SSL appliance or software
- Supports only TCP services, HTTP and POP3/IMAP/SMTP over SSL
- Operates transparently across NAT and proxy devices
- HTTPS client bundled with all leading operating systems
- Only used for client-to-client and client-to-site access
- No known vendor implements fail-over while maintaining sessions
- No control on the security of the client system

SSL VPNs use the SSL protocol to provide for a secure connection between a client and an SSL appliance or software. It supports only a limited range of IP services such as TCP, HTTP and POP3/IMAP/STMP. Its application is rather limited for client-to-client and client-to-site access. It doesn't provide for any fail-over in case of dropped sessions. In addition, this type of VPN does not provide for any security control on client systems. However, it does not require any client application because the Internet browser is used to make the secure connection with the application server. In addition, it does not have any known issues with regard to firewalls, NAT and proxy devices.



Here is an IPSEC architectural model which is used typically to securely connect two LAN sites. In this model, a VPN gateway is installed on each site. The encryption is typically carried out between the two VPN gateways. The secured packets use the ISP's point of presence to enable the packets to be transported safely through the insecure Internet cloud. A typical T1 connection with the ISP provides for a high speed movement of packets from one site to another.



The IPSEC architectural model is more commonly used for remote access by users using any device from any point where there is Internet connection as long as the client has a browser that can support the HTTPS protocol. An SSL appliance or software with firewall features is installed between the customer and the ISP which are typically connected using a high speed line. At the other end, the remote user connects to the ISP's point of presence using either a DSL or an ISDN line.

VPN CLIENTS

- IPSEC VPN Clients
  - AT&T Global Network Client
  - CISCO VPN Clinet
  - VeriSign GUI Client
- SSL VPN Clients
  - Internet Explorer
  - Netscape Communicator
  - Mozilla
  - Opera

To enable remote access, the IPSEC VPN requires a custom designed client application which should be installed and configured on all client systems that need to perform remote access connections. Examples of this client system include the AT&T Global Network Client, the CISCO VPN Client and the VeriSign GUI Client. The SSL VPN does not require any client application and instead use any SSL enabled Internet browser provided for in most currently available operating systems. Examples include the Internet Explorer, Netscape Communicator, Mozilla and the Opera Internet browser.

End of Presentation

Thank you very much!

In conclusion, we may observe that the kind of remote access model that needs to be used depend entirely on what type of VPN is implemented. Large companies that need to connect dispersed LANs will typically use the IPSEC model and will therefore enable remote access using a custom designed client application. Small companies that need only provide remote access for a selected applications may do well on implementing an SSL based solution that will only need an SSL capable Internet browser to connect to the office LAN using am SSL appliance or software with embedded firewall capabilities.

This is the end of my presentation and thank you very much for your attention.