VoIP and VPNs

Why?

VPNs are a popular way to provide controlled access to enterprise network resources though the Internet, using existing connections or low-cost alternatives to leased lines. The remote site is connected to corporate resources using protocols that offer authentication, authorization, an accounting of user access. VPNs encrypt data as it traverses the public network, providing confidentiality. The cost of VPN access is typically drastically less than using point-to-point communication links, and makes the extension of the corporate VoIP infrastructure feasible from a security standpoint as well. Surprisingly, another benefit of using VPN technology for VoIP can be to improve the quality of the call! An excellent study of VoIP and SSL VPNs by Joel Snyder for Network World has shown that the use of an SSL VPN connection can retain the order and regularity of the data streams over the chaotic public network better than best-effort UDP delivery, actually resulting in better call quality.

Once the corporate network is extended beyond the enterprise security perimeter, the carefully designed secure corporate infrastructure is exposed to remote networks and the impact of the public networks in between. The task of maintaining the secure VoIP infrastructure becomes much more complicated with the addition of components which are not under direct control of the enterprise.

VPNs

There are two basic types of VPN connections: remote access and site-to-site. Remote-access connections usually provide an ad hoc “tunnel” between a host and a service or a network. An example of this might be a VPN connection from a notebook PC (using a software client) to an enterprise network (VPN endpoint or gateway) for the purpose of retrieving e-mail from an internal server. Site-to-site VPNs usually provide an encrypted connection from one private network, such as an enterprise network, to another private network, such as a branch office. Site-to-site VPNs are implemented between two VPN gateways, which might be dedicated devices or services provided by other network elements such as routers or firewalls. A site-to-site connection might be used to share unique resources, such as a database server.

The two most commonly deployed VPN technologies are IPSec and SSL VPNs. IPSec was the first widely used VPN, because it is standards-based and compliant vendors could interoperate. IPSec supports both remote-access and site-to-site connections, which makes it useful for many applications. Branch offices can be connected using site-to-site connections, using a variety of edge network devices. Mobile users can securely connect to their corporate LAN from home, a hotel, a hotspot, or the airport. However, remote access connections with IPSec have a few constraints. First, the remote host must have IPSec client software. This software was first introduced at a time when small form factor devices could not support the necessary computing power to perform the necessary encryption/decryption, so client software wasn’t available for every system. Another issue was the inability to pass IPSec data through some networks, typically dialup or hospitality networks. Some providers would forward only a short list of protocols (POP, HTTP, HTTPS); proxy others (SMTP, DNS), and block the rest. Dialup providers needed additional infrastructure to move from supporting mostly connections that lasted maybe an hour to connections that were up all day long for teleworkers, so VPN connections through these services were often discouraged. Inventive network administrators began to reconfigure their VPN gateways and mobile clients to use the HTTP port (80) in order to work around this problem, promoting the bastardization of port 80 and raising significant security issues. That’s not a perfect solution, since today’s intrusion detection/prevention systems (IDS/IPS) can recognize non-HTTP traffic running on the HTTP port, but for the most part it worked. Even so, the ability to use IPSec on almost any random machine in the enterprise just wasn’t there.

SSL VPNs support remote access connections, often requiring only an SSL-enabled browser (i.e., virtually all Web browsers). This addressed several concerns, starting with the platform ubiquity that extends to Internet access kiosks to PDAs and Web-enabled phones. Products can leverage existing SSL support in a product and provide new functionality. As a protocol, SSL is well-established over port 443 (HTTPS), one of the ports that the network user community has demanded of access providers. HTTPS is unlikely to be blocked even on heavily filtered networks. SSL VPNs can use SSL over port 443. This causes the VPN SSL stream to appear as HTTPS traffic, so IDS/IPS devices can inspect the protocol itself without special

considerations.

For applications that require more support than a Web interface, most SSL VPN endpoints can provide an enhanced connection through the browser using Java or ActiveX. These dynamically loaded modules can actually modify the IP stack of the host to provide transparent access to the remote network for non-browser applications, such as VoIP. Once the VPN connection is terminated, the system resources used should be released, and there should be no lasting impact to the host system. It's a very lightweight way to provide a network tunnel.

A third type of SSL VPN connection still uses SSL to communicate, but requires a standalone client program. This method of connection can provide enhancements such as on-demand transparent connections to the corporate network. This is desirable for the very mobile user who wishes to use VoIP from the road and might benefit from custom features of the client.

VoIP and VPNs

VoIP traffic has different characteristics than typical data traffic. Packet reordering, delay, jitter, and retransmissions can seriously degrade the audio quality of a VoIP call or even lead to dropped calls. Since IPSec and VoIP both use datagrams (UDP), it seems logical that VoIP over IPSec would not be at risk of packet reordering.

SSL VPN connections, on the other hand, are initiated with TCP, so it seems intuitive that the call quality could be substantially worse due to retransmissions. Additionally, delayed TCP acknowledgments on networks using Nagle's algorithm can cause upwards of 500 milliseconds of delay. Interestingly, the Network World SSL VPN tests show that TCP connections can actually improve voice quality.

Summary

VPN technology can provide an effective way to secure VoIP over remote access methods without breaking the bank. IPSec and VPN solutions are both viable transport mediums for VoIP. IPSec VPN traffic delivery will typically be more deterministic but has heavier client requirements, and may have trouble traversing some networks. SSL VPNs may provide a better VoIP experience, and may be easier to use on some networks than IPSec VPNs, but keep in mind that this will be highly dependent on your environment.

References

- "VPN"– http://en.wikipedia.org/wiki/VPN
- "Test shows VoIP call quality can improve with SSL VPN links" by Joel Snyder, Network World, 02/20/06 – http://www.networkworld.com/reviews/2006/022006-ssl-voip-test.html
- "Nagle's Algorithm" – http://en.wikipedia.org/wiki/Nagle%27s_Algorithm