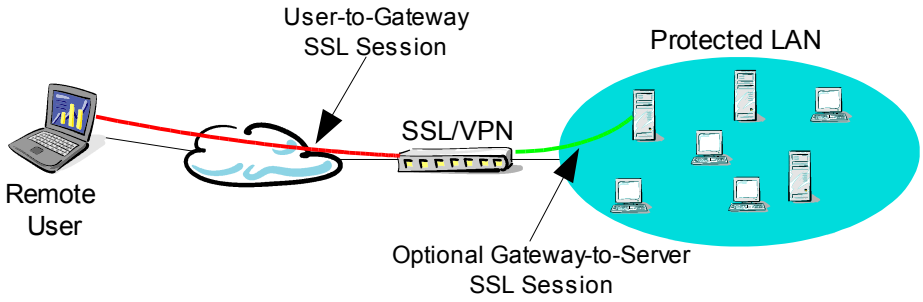
Unintended Consequences of SSL/VPNs

A Sevan White Paper

2003 was the year of the SSL/VPN. These products avoid many of the limitations of IPsec VPNs by using SSL as the security session. SSL/VPNs require no client software, are simpler to setup, and are compatible with NATs (Network Address Translation). As such SSL/VPNs unlock the promise of the internet for remote access. However, using an SSL/VPN will limit your ability to use SSL for application security. This Sevan white paper shows how SSL/VPNs prevent end-to-end certificate-based authentication of remote users.

SSL/VPN Background

A typical deployment of an SSL/VPNs is shown in the figure below. A remote user passes through the SSL/VPN gateway to gain access to the protected LAN. The SSL/VPN gateway builds an SSL connection to the remote user, authenticates the user, and allows authorized users into specified sections of the protected LAN. Some VPN/SSL gateways can also create an SSL session to a server within the protected LAN, so the connection between the remote user and the server can be protected with two SSL session: one between the user and the gateway and the other between the gateway and the server.



End-to-End Security

The SSL/VPN is ideal for protecting the information between the remote user and the gateway. There are instances where the information must be secured all the way to the server. For example,

- the application's access policy requires authentication of local as well as remote users, or
- the security policy demands encryption within the protected LAN.

As mentioned previously, most SSL/VPN gateways can build an SSL session with the server. Unfortunately the gateway-to-server SSL session might not be sufficient, since information from the remote user is decrypted in the SSL/VPN gateway and re-encrypted before being sent to the server. The information is in the clear in the gateway, which produces a vulnerability.

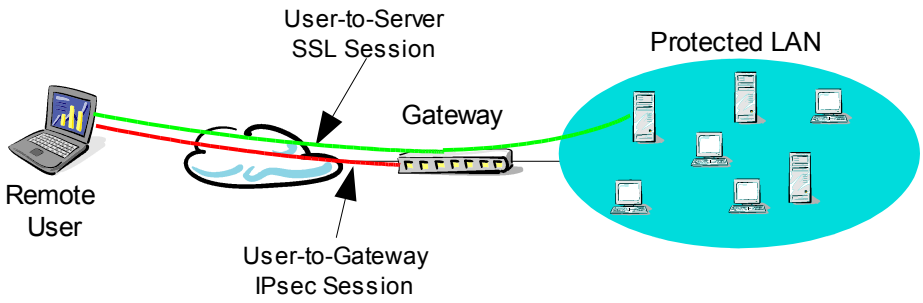
Even more disturbingly the gateway-to-server SSL session cannot support certificate-based user authentication. This is because the server's SSL session is terminated by the SSL/VPN gateway, not the user. As a consequence, remote users cannot be authenticated through SSL certificates. At this time, this is a modest limitation, since few organizations are using certificate-based authentication. However, as certificate-based authentication becomes more widely used, SSL/VPNs will become a major barrier.

Conclusions

SSL/VPNs prevent certificate-based authentication of remote users to applications. This means that applications can

use certificates for local users, but users on the go must resort to password authentication.

Fortunately there are strategies for providing remote access while enabling certificate-based authentication to the applications. The most promising is to use IPsec for remote access and SSL for application security. This arrangement is shown below: IPsec protects the connection to the network and SSL protects end-to-end. This more conventional use of networking technology supports user-to-application certificate-based authentication.



Sevan Networks, Inc
1310 Hollenbeck Ave, Ste F
Sunnyvale, CA 94087
Tel: 408.830.1000
Fax: 408.830.1001
www.sevannetworks.com