

smt

Security Management Today



Morgan Rees

Secure IT

Last month, we explained why the need to provide a secure mechanism for access to the Internet is highly important. Having suggested that in-house managers must rethink their approach to IT security, here he evaluates client-side certificates and certificate revocation lists.

Borderless security takes shape

If used in conjunction with a proxy-based Web traffic manager, SSL (Secure Socket Layer) can be accelerated to provide lightning-fast access to Web applications. However, care must be taken such that the connection between the proxy and the Web application is either physically secure or uses SSL as well.

For the IT director or security manager deciding what secure Web traffic manager to pick, it's crucial to remember SSL on the inside support. SSL on the inside allows IT administrators to configure their proxies so that SSL connections between the proxy and the Web applications are encrypted as well.

"If used in conjunction with a proxy-based Web traffic manager, Secure Socket Layer can be accelerated to provide lightning-fast access to Web applications. However, care must always be taken such that the connection between the proxy and the chosen Web application is either physically secure or makes effective use of SSL as well"

If the Web application server is on a distant network, there are no issues with potential hackers sniffing the packets between the proxy and the server (particularly after so much effort has been expended in getting the traffic from the client to the proxy in a secure manner).

Client-side certificates
Other features to keep in mind when it comes to Internet security and secure access are client-side certificates and certificate

revocation lists. These features allow administrators to give electronic tokens to their users so that, without the token, the user cannot even arrive at a log-in prompt. Certificate revocation lists, meanwhile, allow administrators to revoke client-side certificates without having to take electronic tokens back.

Another important feature is SSL acceleration. Given the incredible amount of mathematics required to perform even simple cryptographic operations that are needed for the SSL protocol, it's important that hardware acceleration be available such that the proxy can focus on its primary task - that of secure Web traffic management.

Support for SSL is needed across all networks. While not all networks have to guarantee support for heavyweight security protocols, all networks must back up Web access. After all, without any form of Web access they're of limited (if any) use to anyone.

Therefore, using SSL in conjunction with HTTP makes sure that, wherever your system users are, they will be able to reach your Web applications.

▪ Morgan Rees is a vice-president of marketing