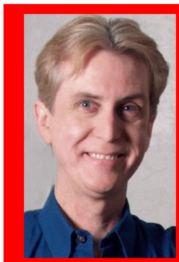
£6.00 www.smtdirect.co.uk

smt

Security Management Today



Morgan Rees

Secure IT

With applications moving to the World Wide Web at breakneck speed, the need for providing a secure mechanism for access is becoming increasingly important. However, the problems of providing secure access are changing. In the first of a two-part article, we suggest that a complete re-evaluation of how Internet security can work for the enterprise is long overdue.

A word to the Web wise...

There's a global trend towards users who don't want to be chained to their desks or IT departments, but who need to access corporate applications wherever they may be working. The populist solution is one that involves taking advantage of the fact that the applications use the ubiquitous HTTP protocol. Alas, this method isn't always reliable, particularly when you consider the difference between corporate networks and the Internet.

Corporate networks tend to separate the world into two parts: the inside (corporate) and the outside (Internet) that are kept apart by firewalls. Generally, corporations don't reveal all of their internal servers to the outside world for security reasons. This is different to the Internet... when a Web-based application interacts with a user, it then sends a number of embedded URLs for navigation purposes.

Having been developed under the assumption that the application will always work inside the protection of the corporate network, many such applications embed URLs that would never work on the Internet. Therein lies the problem (ie Web applications need to be corrected in order to function effectively on the Internet and corporate networks alike). URLs: inside out and outside in Web Resource Mapping can be used to unify the URLs generated by Web applications, making access far more secure for remote workers. When carried out securely through a Web traffic manager, the conversion will happen transparently and doesn't need any intervention by administrators of the Web-based application. Web 'proxies' can also help with the problem of remote working, presenting as they do a single point of entry to all Web applications. A key issue to bear in mind with such a proxy is that it must be able to address the issues of authentication, authorisation and accounting for each Web request that it processes.

Individual Web applications tend to design their own authentication, authorisation and accounting (AAA) systems for the purpose of tracking and managing users. While this may be necessary, it does present a problem to both users and administrators. Since each application presents its own view of user management, users must learn the nuances of each system and, in turn, administrators have to learn how to configure the authorisation policies of each Web application. This can become tedious and error prone for all parties.

Security without borders

By using a secure Web traffic manager, it's possible to centralise AAA into one place with one system. Web applications can benefit from these authentication systems by using a security token that's passed with every request from the proxy to the application. By using the token, Web applications don't need to authenticate again. SSL also provides an end-to-end solution, enabling 'borderless' security through an encryption mechanism. SSL keeps traffic encrypted all the way to the application, and not just to the edge of the corporate network. Indeed, SSL support is ubiquitous across all operating systems and Web browsers, making the IT security manager's life much easier.

■ **Morgan Rees is a vice-president of marketing**