Chapter 25

SECURING WEB COMMUNICATIONS WITH SSL VPNS

INTRODUCTION

Over the years the trend toward utilizing virtual private networks (VPNs) and the Internet for remote access connectivity has grown dramatically – and shows no sign of slowing down. At a time when most enterprises need to do more with less, today's enterprise users need every bit of productivity that technology can offer. Remote access to e-mail, applications, collaborative tools and information can extend the day when users are traveling or working from home after hours. The convenience and flexibility of anywhere, anytime access give users a needed productivity boost, as well as a sense of empowerment. Greater job satisfaction and higher morale result. Remote access also facilitates on-demand information and application sharing with business partners via extranets – a meaningful way to streamline operations and improve customer service [1].

The demand for flexible remote access is being met by the increasing deployment of secure sockets layer (SSL) VPNs, browser-based technology that supports access from laptops and desktops, home computers, Internet kiosks and personal digital assistants – anywhere an Internet connection exists. Compared with other solutions, SSL VPNs can deliver cost savings, simpler administration and easier connections with partners. Where traditional VPNs are not required, expect immediate value from investments in SSL VPNs in the form of easier deployment and support [1].

However, the very success of SSL VPN delivering flexible access from a diverse set of endpoints is also its weakness. Because SSL VPNs extend remote access to nearly any unmanaged endpoint, they can expose the enterprise to a variety of security threats. If not understood and managed properly, these threats could threaten the enterprise's performance and even its very existence. This chapter examines the security risks that arise from securing web communications with SSL VPNs and proposes strategies for remediation [1].

THE BUSINESS OF SECURE REMOTE ACCESS

As SSL VPNs provide connectivity to internal computing resources, common sense suggests that sensitive information and systems should be secured. But it goes beyond common sense. New U.S. regulations such as Gramm-Leach-Bliley and Sarbanes-Oxley mandate that customer data and other sensitive information must be secure, properly stored and easily retrievable – at the risk of severe fines and even criminal prosecution [1].

In healthcare, the Health Insurance Portability and Accountability Act (HIPAA) sets out security, privacy and access guidelines for patient medical records – a challenge for IT administrators when the remote computers of physicians are beyond their direct control. In commerce, security must extend to extranet communications among trading partners, where sensitive pricing and inventory information is constantly exchanged. Unauthorized access could put the enterprise at risk, yet manufacturers cannot control the remote computers of partners [1].

Security concerns extend beyond the confidentiality of information downloaded. Unmanaged SSL VPN endpoints expose the internal network to security risks from infiltrated systems. Since they exist outside the corporate perimeter and are dependent on the choices of individual users, remote endpoints form the weakest link in the security chain [1].

REMOTE ACCESS REQUIRES COMPREHENSIVE SECURITY

Day extenders accessing enterprise resources via SSL VPN connections pose higher security risks than employees working on site – especially if teleworkers provide their own, nonstandard equipment. Home-based users may share systems with other family members, making it impossible to enforce security policies or approved configurations. Internet connection sharing could allow unknown systems to access enterprise resources over SSL VPNs, and wireless home networks are notoriously insecure. To protect remote SSL systems, the users themselves must take on more of the security burden than their in-house counterparts. Yet such users tend to be the least technologically savvy and SSL VPN solutions must include some capability to check the security state of the endpoint [1].

The SSL VPN gateway poses another security concern. Although SSL encryption provides a level of data privacy and integrity, it does not confer access rights. SSL VPN solutions must allow administrators to limit access to those authorized and no one else. And just because users can establish SSL VPN tunnels does not mean they should have access to all resources. VPN users are considered *trusted* users, yet much damage, both unintentional and intentional, has been done by trusted users. Though SSL encryption does a good job of preventing others from reading private information, it provides no guarantee of information passing through the VPN [1].

SSL VPNs generally rely on the browser to access Web, fileshares or e-mail applications via their included Web portal. However, most SSL VPN solutions today offer the capability to provide full native network-level access. For access to clientserver applications, SSL VPNs employ Java browser plug-ins as agents. Because Java has been used as a vehicle for attack, such sessions could subject internal servers to attacks from compromised endpoints.