GUIDELINES ON IMPLEMENTING A SECURE SOCKETS LAYER (SSL) VIRTUAL PRIVATE NETWORK (VPN)

By Sheila Frankel
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The protection of sensitive information that is transmitted across interconnected networks is critical to the overall security of an organization's information and information systems. The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued guidelines to assist organizations in strengthening their network security and in lessening the risks associated with the transmission of sensitive information across networks. NIST Special Publication (SP) 800-113, *Guide to SSL VPNs*, offers practical guidelines on implementing a Secure Sockets Layer (SSL) virtual private network (VPN).

SSL VPNs provide secure remote access to an organization's resources. A VPN is a virtual network, built on top of existing physical networks, which can provide a secure communications mechanism for data and other information transmitted between two endpoints. Because a VPN can be used over existing networks such as the Internet, it can facilitate the secure transfer of sensitive data across public networks. An SSL VPN consists of one or more VPN devices to which users connect using their Web browsers. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) protocol. This type of VPN may be referred to as either an SSL VPN or a TLS VPN. This guide uses the term SSL VPN.

SSL VPNs provide remote users with access to Web applications and client/server applications, and connectivity to internal networks. Despite the popularity of SSL VPNs, they are not intended to replace Internet Protocol Security (IPsec) VPNs. The two VPN technologies are complementary and address separate network architectures and business needs. SSL VPNs offer versatility and ease of use because they use the SSL protocol, which is included with all standard Web browsers, so the client usually does not require configuration by the user. SSL VPNs offer granular control for a range of users on a variety of computers, accessing resources from many locations. There are two primary types of SSL VPNs:

- **SSL Portal VPNs.** This type of SSL VPN allows a user to use a single standard SSL connection to a Web site to securely access multiple network services. The site accessed is typically called a portal because it is a single page that leads to many other resources. Remote users access the SSL VPN gateway using any modern Web browser, identify themselves to the gateway using an authentication method supported by the gateway, and are then presented with a Web page that acts as the portal to the other services. These other services might be links to other Web servers, shared file directories, Web-based email systems, applications that run on protected servers, and any other services that can be channeled through a Web page.

  SSL portal VPNs work with essentially any modern Web browser. Specifically, they work with browsers whether or not the browsers allow (or support) active content. Thus, SSL portal VPNs are accessible to more users than SSL tunnel VPNs.

- **SSL Tunnel VPNs.** This type of SSL VPN allows a user to use a typical Web browser to securely access multiple network services, including applications and protocols that are not Web-based, through a tunnel that is running under SSL. SSL tunnel VPNs require that the

Web browser be able to handle specific types of active content, which allows them to provide functionality that is not accessible to SSL portal VPNs, and that the user be able to run them. Examples of active content include Java, JavaScript, Active X, or Flash applications or plug-ins.

The tunneling in an SSL tunnel VPN allows a wide variety of protocols and applications to be run through it. For example, essentially any protocol that runs over Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) can be tunneled through such a gateway, making the remote user's experience of the protected network very similar to being directly on the network. To the user, an SSL tunnel VPN may appear quite different from a typical Web site because the tunneling plug-in or application needs to be loaded into the user's browser before the user can access the VPN. This might involve warning messages about the software being loaded, and it could also prevent users from entering the VPN if their Web browsers are instructed not to allow such programs to run. Because of the active content requirement, SSL tunnel VPNs may be accessible to fewer users than SSL portal VPNs.

NIST Special Publication 800-113, *Guide to SSL VPNs*

Written by Sheila Frankel of NIST, Paul Hoffman of the Virtual Private Network Consortium (VPNC), and Angela Orebaugh and Richard Park of Booz Allen Hamilton, this publication discusses the fundamental technologies and features of SSL VPNs. It describes SSL and how it fits within the context of layered network security. The guide presents a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments. It also compares the SSL VPN technology with IPsec VPNs and other VPN solutions. This information is particularly valuable for helping organizations to determine how best to deploy SSL VPNs within their specific network environments. The document is available at http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf.

NIST Recommendations for Implementing SSL VPNs

Implementing the following recommendations should assist in facilitating more efficient and effective SSL VPN use for federal departments and agencies.

Organizations planning SSL VPN deployments should identify and define requirements, and evaluate several products to determine their fit into the organization.

SSL VPN products vary in functionality, including protocol and application support. They also vary in breadth, depth, and completeness of features and security services. Some recommendations and considerations include the following:

- SSL VPN manageability features such as status reporting, logging, and auditing should provide adequate capabilities for the organization to effectively operate and manage the SSL VPN and to extract detailed usage information.
- The SSL VPN high availability and scalability features should support the organization's requirements for failover, load balancing, and throughput. State and information sharing is recommended to keep the failover process transparent to the user.
- SSL VPN portal customization should allow the organization to control the look and feel of the portal and to customize the portal to support various devices such as personal digital assistants (PDAs) and smart phones.

- SSL VPN authentication should provide the necessary support for the organization's current and future authentication methods and leverage existing authentication databases. SSL VPN authentication should also be tested to ensure interoperability with existing authentication methods.
- The strongest possible cryptographic algorithms and key lengths that are considered secure for current practice should be used for encryption and integrity protection unless they are incompatible with interoperability, performance, and export constraints. Federal agencies have more stringent requirements.
- SSL VPNs should be evaluated to ensure that they provide the level of granularity needed for access controls. Access controls should be capable of applying permissions to users, groups, and resources, as well as integrating with endpoint security controls.
- Implementation of endpoint security controls is often the most diverse service amongst SSL VPN products. Endpoint security should be evaluated to ensure that it provides the necessary host integrity checking and security protection mechanisms required for the organization.
- Not all SSL VPNs have integrated intrusion prevention capabilities. Those that do should be evaluated to ensure that they do not introduce an unacceptable amount of latency into the network traffic.

Federal agencies deploying SSL VPNs must configure them to only allow Federal Information Processing Standards (FIPS)-compliant cryptographic algorithms, cipher suites, and versions of SSL.

Some organizations, such as federal agencies, have strict requirements for encryption and integrity protection. SSL VPNs should support the required algorithms for symmetric encryption, key exchange, and hash functions. For government agencies, traffic that requires protection must employ FIPS-compliant cryptographic algorithms and modules. Many of the cryptographic algorithms used in some SSL cipher suites are not FIPS-approved, and therefore are not allowed for use in SSL VPNs that are to be used in applications that must conform to FIPS 140-2, *Security Requirements for Cryptographic Modules*. This means that to be run in FIPS-compliant mode, an SSL VPN gateway must only allow cipher suites that are allowed by FIPS 140-2.

Some of the cryptographic requirements, including allowable hash functions and certificate key lengths, will change at the end of 2010. Therefore, federal agencies who want to provide SSL VPN services after 2010 must ensure that their systems are upgradeable to the new FIPS-compliant cipher suites and key lengths before the end of 2010, and that their SSL VPN vendors guarantee that such upgrades will be available early enough for testing and deployment in the field.

Organizations should use a phased approach to SSL VPN planning and implementation.

A successful SSL VPN deployment can be achieved by following a clear, step-by-step planning and implementation process. The use of a phased approach can minimize unforeseen issues and identify potential pitfalls early in the process. The five phases of the recommended approach are:

1. **Identify Requirements.** Identify the requirements for remote access and determine how they can best be met.
2. **Design the Solution.** Make design decisions in five areas: access control, endpoint security, authentication methods, architecture, and cryptography policy.

3. **Implement and Test a Prototype.** Test a prototype of the designed solution in a laboratory, test, or production environment to identify any potential issues.

4. **Deploy the Solution.** Gradually deploy the SSL VPN solution throughout the enterprise, beginning with a pilot program.

5. **Manage the Solution.** Maintain the SSL VPN components and resolve operational issues. Repeat the planning and implementation process when significant changes need to be incorporated into the solution.

Organizations should be familiar with the limitations of SSL VPN technology.

SSL VPNs, although a maturing technology, continue to face several challenges. These include limitations on their ability to support a large number of applications and clients, the methods of implementing network extension and endpoint security, the ability to provide clientless access, the use of the SSL VPN from public locations, and product and technology education.

Organizations should implement other measures that support and complement SSL VPN implementations.

These measures help to ensure that the SSL VPN solution is implemented in an environment with the technical, management, and operational controls necessary to provide sufficient security for the SSL VPN implementation. Examples of supporting measures include:

- Establishing and maintaining control over all entry and exit points for the protected network, which helps to ensure its integrity;

- Incorporating SSL VPN considerations into organizational policies (e.g., identity management, remote access); and

- Ensuring that all SSL VPN endpoints are secured and maintained properly to reduce the risk of SSL VPN compromise or misuse.

Although SSL VPNs are flexible enough to meet many needs, there are certain cases when other types of VPNs may provide a better solution. Network layer VPN protocols, primarily IPsec; data link layer VPN protocols, such as Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Layer 2 Forwarding (L2F); and application layer security protocols, including OpenPGP and Secure Shell (SSH), are all effective alternatives to SSL VPNs for particular needs and environments.