



PSS
Port Scanning Services Inc.

Network Security, IPSec and VPNs

PSS will provide a secure and reliable connection to its customers using what is known as a Virtual Private Network or VPN. The VPN software allows customers, clients and consultants a means to establish secure, end-to-end encrypted tunnels to corporate resources through the VPN Server/Firewall. VPN access policies and configurations can be downloaded from the central gateway and pushed to the client when a connection is established, allowing very secure connections. This thin-design, IP Security (IPsec) compliant implementation requires very little user intervention.

IPSec is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control used with VPNs. A VPN is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks. VPNs are used most often to protect communications carried over public networks such as the Internet. A VPN can provide several types of data protection, including confidentiality, integrity, data origin authentication, replay protection and access control.

VPNs create "virtual" point-to-point connections using a technique called tunneling. As the name suggests, tunneling acts like a "pipe" which penetrates through a network to connect two points. Normally activated by remote users, tunneling encrypts data into standard TCP/IP packets and encapsulates it for safe transmission across the Internet.

TCP/IP is widely used throughout the world to provide network communications. TCP/IP communications are composed of four layers that work together. When a user wants to transfer data across networks, the data is passed from the highest layer through intermediate layers to the lowest layer with each layer adding additional information. The lowest layer sends the accumulated data through the physical network; the data is then passed up through the layers to its destination. Essentially, the data produced by a layer is encapsulated in a larger container by the layer below it. The four TCP/IP layers, from highest to lowest, are shown below.

<p>Application Layer. This layer sends and receives data for particular applications, such as Domain Name System (DNS), HyperText Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).</p>
<p>Transport Layer. This layer provides connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally assure the reliability of communications. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are</p>
<p>Network Layer. This layer routes packets across networks. Internet Protocol (IP) is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).</p>
<p>Data Link Layer. This layer handles communications on the physical network components. The best-known data link layer protocol is Ethernet.</p>

Security controls exist for network communications at each layer of the TCP/IP model. As previously explained, data is passed from the highest to the lowest layer, with each layer adding more information. Because of this, a security control at a higher layer cannot provide full protection for lower layers, because the lower layers perform functions of which the higher layers are not aware. The following items discuss the security controls that are available at each layer:

- **Application Layer.** Separate controls must be established for each application. For example, if an application needs to protect sensitive data sent across networks, the application may need to be modified to provide this protection. While this provides a very high degree of control and flexibility over the application's security, it may require a large resource investment to add and configure controls properly for each application. Designing a cryptographically sound application protocol is very difficult, and implementing it properly is even more challenging, so creating new application layer security controls is likely to create vulnerabilities. Also, some applications, particularly off-the-shelf software, may not be capable of providing such protection. While application layer controls can protect application data, they cannot protect TCP/IP information such as IP addresses because this information exists at a lower layer. Whenever possible, application layer controls for protecting network communications should be standards-based solutions that have been in use for some time. One example is Pretty Good Privacy (PGP), which is commonly used to encrypt e-mail messages.
- **Transport Layer.** Controls at this layer can be used to protect the data in a single communication session between two hosts. Because IP information is added at the network layer, transport layer controls cannot protect it. The most common use for transport layer protocols is securing HTTP traffic; the Transport Layer Security (TLS) protocol is usually used for this. The use of TLS typically requires each application to support TLS; however, unlike application layer controls, which typically involve extensive customization of the application, transport layer controls such as TLS are much less intrusive because they simply protect network communications and do not need to understand the application's functions or characteristics. Although using TLS may require modifying some applications, TLS is a well-tested protocol that has several implementations that have been added to many applications, so it is a relatively low-risk option compared to adding protection at the application layer instead. One drawback of TLS is that it is only capable of protecting TCP-based communications, as opposed to UDP, because it assumes the network layer protocol is ensuring reliability.
- **Network Layer.** Controls at this layer apply to all applications and are not application-specific. For example, all network communications between two hosts or networks can be protected at this layer without modifying any applications on the clients or the servers. In many environments, network layer controls such as IPSec provide a much better solution than transport or application layer controls because of the difficulties in adding controls to individual applications. Network layer controls also provide a way for network administrators to enforce certain security policies. Another advantage of network layer controls is that since IP information (e.g., IP addresses) is added at this layer, the controls

can protect both the data within the packets and the IP information for each packet. However, network layer controls provide less control and flexibility for protecting specific applications than transport and application layer controls.

- **Data Link Layer.** Data link layer controls are applied to all communications on a specific physical link, such as a dedicated circuit between two buildings or a dial-up modem connection to an Internet Service Provider (ISP). Data link layer controls for dedicated circuits are most often provided by specialized hardware devices known as data link encryptors; data link layer controls for other types of connections, such as dial-up modem communications, are usually provided through software. Because the data link layer is below the network layer, controls at this layer can protect both data and IP information. Compared to controls at the other layers, data link layer controls are relatively simple, which makes them easier to implement; also, they support other network layer protocols besides IP. Because data link layer controls are specific to a particular physical link, they are poorly suited to protecting connections with multiple links, such as establishing a VPN over the Internet. An Internet-based connection is typically composed of several physical links chained together; protecting such a connection with data link layer controls would require deploying a separate control to each link, which is not feasible. Data link layer protocols have been used for many years primarily to provide additional protection for specific physical links that should not be trusted.

Because they can provide protection for many applications at once without modifying them, network layer security controls have been used frequently for securing communications, particularly over shared networks such as the Internet. Network layer security controls provide a single solution for protecting data from all applications, as well as protecting IP information.

Internet Protocol Security (IPSec) has emerged as the most commonly used network layer security control for protecting communications. IPSec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPSec is implemented and configured, it can provide any combination of the following types of protection:

- **Confidentiality.** IPSec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key—a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.
- **Integrity.** IPSec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.
- **Peer Authentication.** Each IPSec endpoint confirms the identity of the other IPSec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.

- **Replay Protection.** The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPSec does not ensure that data is delivered in the exact order in which it is sent.
- **Traffic Analysis Protection.** A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted.
- **Access Control.** IPSec endpoints can perform filtering to ensure that only authorized IPSec users can access particular network resources. IPSec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.

There are three primary components of the IPSec protocol, the Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) protocols.

ESP has two modes: transport and tunnel. In *tunnel mode*, ESP creates a new IP header for each packet. The new IP header lists the endpoints of the ESP tunnel (such as two IPSec gateways) as the source and destination of the packet. Tunnel mode can encrypt and/or protect the integrity of both the data and the original IP header for each packet. Encrypting the data protects it from being accessed or modified by unauthorized parties; encrypting the IP header conceals the nature of the communications, such as the actual source or destination of the packet. If authentication is being used for integrity protection, each packet will have an ESP Authentication section after the ESP trailer. ESP tunnel mode is used far more frequently than ESP transport mode. In *transport mode*, ESP uses the original IP header instead of creating a new one. AH, one of the IPSec security protocols provides integrity protection for packet headers and data, as well as user authentication. It can optionally provide replay protection and access protection. AH cannot encrypt any portion of packets. AH has two modes: transport and tunnel. In *tunnel mode*, AH creates a new IP header for each packet; in *transport mode*, AH does not create a new IP header. In IPSec architectures that use a gateway, the true source or destination IP address for packets must be altered to be the gateway's IP address. Because transport mode cannot alter the original IP header or create a new IP header, transport mode is generally used in host-to-host architectures. AH provides integrity protection for the entire packet, regardless of which mode is used.

The purpose of the Internet Key Exchange (IKE) protocol is to negotiate, create, and manage security associations. *Security association* (SA) is a generic term for a set of values that define the IPSec features and protections applied to a connection. SAs can also be manually created, using values agreed upon in advance by both parties, but these SAs cannot be updated; this method does not scale for real-life large-scale VPNs.

The most common use of IPSec implementations is providing VPN services. A *VPN* is a virtual network, built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks. 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. This is often less expensive than alternatives such as dedicated private

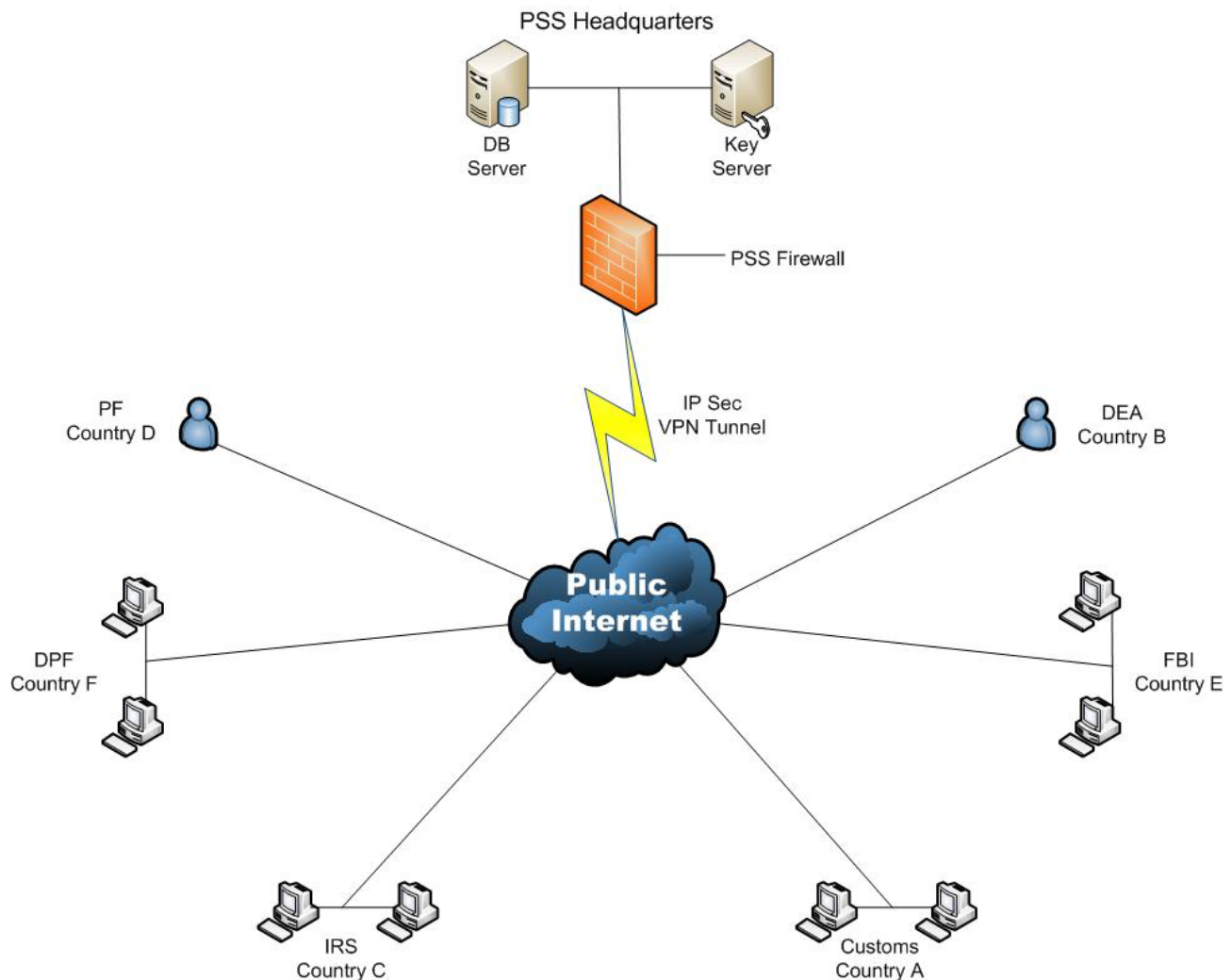
telecommunications lines between organizations or branch offices. VPNs can also provide flexible solutions, such as securing communications between remote telecommuters and the organization's servers, regardless of where the telecommuters are located. A VPN can even be established within a single network to protect particularly sensitive communications from other parties on the same network.

VPNs can use both symmetric and asymmetric forms of cryptography. *Symmetric cryptography* uses the same key for both encryption and decryption, while *asymmetric cryptography* uses separate keys for encryption and decryption, or to digitally sign and verify a signature. Symmetric cryptography is generally more efficient and requires less processing power than asymmetric cryptography, which is why it is typically used to encrypt the bulk of the data being sent over a VPN. One problem with symmetric cryptography is with the key exchange process; keys must be exchanged out-of-band to ensure confidentiality. Common algorithms that implement symmetric cryptography include Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), Blowfish, RC4, International Data Encryption Algorithm (IDEA), and the hash message authentication code (HMAC) versions of Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).

Asymmetric cryptography (also known as *public key cryptography*) uses two separate keys to exchange data. One key is used to encrypt or digitally sign the data, and the other key is used to decrypt the data or verify the digital signature. These keys are often referred to as public/private key combinations. If an individual's public key (which can be shared with others) is used to encrypt data, then only that same individual's private key (which is known only to the individual) can be used to decrypt the data. If an individual's private key is used to digitally sign data, then only that same individual's public key can be used to verify the digital signature. Common algorithms that implement asymmetric cryptography include RSA, Digital Signature Algorithm (DSA), and Elliptic Curve DSA (ECDSA).

Although there are numerous ways in which IPSec can be implemented, most implementations use both symmetric and asymmetric cryptography. Asymmetric cryptography is used to authenticate the identities of both parties, while symmetric encryption is used for protecting the actual data because of its relative efficiency.

An increasingly common VPN model is the host-to-gateway model, which is most often used to provide secure remote access. PSS deploys a VPN gateway onto their network; each remote access user then establishes a VPN connection between the local computer (host) and the VPN gateway. As with the gateway-to-gateway model, the VPN gateway may be a dedicated device or part of another network device.



In this model, IPSec connections are created as needed for each individual VPN user. Remote users' hosts have been configured to act as IPSec clients with PSS's IPSec gateway. When a remote user wishes to use computing resources through the VPN, the host initiates communications with the VPN gateway. The user is typically asked by the VPN gateway to authenticate before the connection can be established. The VPN gateway can perform the authentication itself or consult a dedicated authentication server. The client and gateway exchange information, and the IPSec connection is established. The user can now use the organization's computing resources, and the network traffic between the user's host and the VPN gateway will be protected by the IPSec connection. Traffic between the user and systems not controlled by the organization can also be routed through the VPN gateway; this allows IPSec protection to be applied to this traffic as well if desired.

VPNs ensure the confidentiality and integrity of information as it travels over the public internet because it requires:

1. Remote user identity authentication
2. Secure private transmission of data (no unauthorized listeners)
3. Verification of unadulterated data transmission

Some of the features and benefits of using this type of connection are;

- Support for x86 (32-bit) XP, Vista (including SP1 & SP2), and Windows 7; Linux (Intel); Solaris (UltraSparc 32 and 64-bit); and Mac OS X 10.4 & 10.5.
- VPN Virtual Interface Adapter present on Windows XP, Vista and Windows 7
- Application Programming Interface (API) allows you to control operation of the VPN client from another application
- System coexistence with Microsoft L2TP/IPsec client
- MSI (Windows Installer) package available for Windows
- Intelligent peer availability detection (DPD)
- Simple Certificate Enrollment Protocol (SCEP)
- Data compression (LZS)
- Command-line options for connecting, disconnecting, and connection status
- Configuration file with option locking
- Support for Microsoft network login (all platforms)
- Domain Name System (DNS) including DDNS/DHCP computer name population, Split DNS,
- Windows Internet Name Service (WINS), and IP address assignment
- Load balancing and backup server support
- Centrally controlled policies (including backup server list)
- Accounting information for tracking client use for security audits, billing or reporting purposes

This secure connection, along with other security methods, will allow geographically dispersed users access to only the database records they have been given access to. The database is accessible to all agencies via this secure encryption controlled access. These database records will include but not limited to;

1. Date/Time stamp of any video in which is available of container arriving at, during the scanning process or leaving the Scanning Operations Center
2. Date/Time stamp of any images in which is available of container arriving at, during the scanning process or leaving the Scanning Operations Center
3. Access to any video in which is available of container arriving at, during the scanning process or leaving the Scanning Operations Center
4. Access to any images in which is available of container arriving at, during the scanning process or leaving the Scanning Operations Center
5. Other documentation available which may be needed by searching our database by individual scanning equipment, port, region, country, exporter or importer and by container serial number.

The images are available from each scanning station live or by performing a search. Data can be kept from 24 hours up to 1 year. Each container will have a scanned copy of the import/export manifest, 3 sided X-Ray pictures, Radiation detection report, video evidence of the container going to the scanning process. Video is watermarked to resist tampering.

Dual work station for compliance officers located in PSS Headquarter.

