A virtual private network (VPN) allows users to securely access a private network and share data remotely while using the public network, aka the Internet, for the transmission of that data back and forth. VPNs are often likened to exclusive tunnels that travel through the Internet; the key is no one can peer into your tunnel and no one else can use it. VPNs are private networks but they’re virtual, like your wi-fi network at home, created by networking protocols to appear and act like a private network. There are three main VPN technologies: trusted, secure, and hybrid.

Hybrid VPNs are Secure VPNs that can be run as part of a trusted VPN. Because Hybrid VPNs are a new VPN technology that is still evolving and being standardized, it is not part of this discussion at this time. This Learn About will introduce you to Secure VPNs.

In the early days of the Internet, trusted VPNs were the first VPNs to be deployed, and they typically operated between service providers and large companies. Service providers leased one or more circuits to their corporate customers, creating a trusted private network where each leased circuit functioned as a single wire in a network controlled by specific customers who could operate these leased circuits just as they would use physical cables in their local network. Service providers assured companies that no one else would use the same circuits, so companies trusted those service providers to maintain the reliability and security of those circuits.

But once companies started employing the Internet as their standard corporate communications medium, security and cost became critical company factors. Leasing dedicated lines from service providers for branch office communications was very expensive, and companies quickly realized that trusted VPNs did not provide credible security after all. As a result, their data was extremely vulnerable to virus and spam attackers, snoopers, hackers, and corporate data thieves. At this point Secure VPN developed into an important VPN technology.

### Mobility

The world has unquestionably gone mobile. Recent statistics from Gartner (link here) show that the mobile device market continues to skyrocket! In 2012, 821 million smartphones and tablets were purchased globally. That number is expected to exceed 1.82 billion by the end of 2013.

In 2013, Pew Research (link here) stated that half of all U.S. adults have smartphones, and approximately one-third of all U. S. adults own some type of tablet device.
Also, according to Gartner, mobile phones will overtake PCs as the most common Web access device worldwide by the end of 2013. However, unlike laptops and workstations, new mobile devices tend not to be conceived of, designed for, or built with security in mind. As a result, phones and tablets are being targeted by snoopers who steal data.

There are multiple vendors with multiple OS systems, and thousands of apps that use the Internet to connect and share data. According to Forbes, global mobile traffic now represents roughly 13% of all Internet traffic. Portio Research forecasts that 82 billion apps will be downloaded worldwide in 2013, and by 2017, there will be more than 200 billion downloads per year.

All of these statistics strongly indicate that with so much data and information (financial, personal, corporate, and government) being shared over so many diverse network connections, security must now be taken seriously and be made front-and-center. Secure VPN connections between these devices and their destination servers are more critical than ever.

Secure VPNs

Secure VPNs use special protocols (sets of communication rules) to encrypt and decrypt data as it is sent over the Internet from the originating computer, or network, to the receiving computer or network. This method of transferring data traffic through a logical path is called tunneling. Tunneling creates a temporary direct session that enables companies and individuals to secure sensitive data when connecting to remote data centers. All data sent using a Secure VPN is encrypted to such a degree that even if a hacker or snooper managed to obtain a copy of the data or siphon off some of the transmitted data, they could never decrypt any of the data.

The entire process of tunneling includes the encapsulation, transmission, and decapsulation of data in the illustration of the tunneling process shown in Figure 1.

Data is encapsulated with a header that provides routing information allowing it to traverse the public network to reach its endpoint. The tunnel (logical path) contains private data that has been encapsulated, and the VPN contains private data that has been encrypted. The encapsulated data (or packets) are encrypted for confidentiality so if any packets are intercepted on the public network, they are indecipherable without encryption keys. Once the encapsulated frames have been transmitted over the public network, the frames are decapsulated and sent to their final destination.
In addition to protecting data, Secure VPN enables mobile employees to connect to their respective VPN servers by using VPN client software installed on their laptop or mobile device that uses the Internet to complete the connection. Mobile employees can access printers, file servers, shared applications, and tools just as if they were physically present at the office. Figure 2 shows an overview of a mobile user connecting to an Intranet via remote access over the public Internet.

To use Secure VPN, the mobile user runs client software on a laptop or mobile device, connecting through the Internet. The client program then shares a secure certificate containing shared secrets with the VPN server using public/private keys to create an encryption key. After the client connects to the VPN server and the user is authorized, all traffic traveling along the established channel is wrapped with an encrypted package that hides its contents from view.

It’s important to note that all mechanisms for establishing and maintaining Secure VPN connections are contained at the destination network. This prohibits attempts to access the company’s network from unauthorized VPN database users, using sophisticated authorization measures and secret keys that are discussed in the rest of this Learn About.

![Figure 2 Remote Access Over Internet](image)

**Problems Addressed by Using Secure VPNs**

Secure VPNs are used to effectively solve these commonly experienced situations:

- **Security** – When connecting to the Internet from a hotel, airport, or coffee shop, most Web browsing can be intercepted by other users on the same wireless network, or by someone with access to any public network between the hotel router and the final Web address to which you are connecting. By using a Secure VPN, all traffic is encrypted and passes through a tunnel, so anyone that gains access to your data in the middle of its journey sees only only garbled characters.

- **Access to Local or Corporate Networks** – Mobile users can use a Secure VPN to access file systems, shared printers, and shared applications on local (and private) networks.

- **Port Blocking** – Port blocking is used to protect sensitive services by blocking ports that can be used to attack the network – and some wireless hotspots and hotels may employ port blocking to prevent users from sending out **SPAM** using their wireless networks.

**SPAM**
The term **SPAM** is not a networking or computer acronym but refers to the lunchmeat brand, and originally to a specific Monty Python sketch, according to Wikipedia.
hotspot IP address. To send email using your own email account and software, use a Secure VPN to connect – it functions just as if you were sitting onsite within your destination network.

**Secure VPN Requirements**

An effective remote Secure VPN networking solution should:

- Provide easy yet controlled access to information and resources.
- Support common protocols used in the public network, such as IP and IPX/SPX.
- Allow roaming and remote clients to connect to LAN resources, and remote offices to connect to each other, to share resources and information.
- Ensure data privacy (particularly for client and VPN addresses) and integrity to sensitive information as it travels across the Internet, or across the destination Intranet.
- Restrict access to the Secure VPN only to those VPN clients it can identify, and provide audit and accounting logs for tracking.
- Encrypt and authenticate all traffic. Data must be rendered unreadable to unauthorized users.
- Generate fresh encryption keys at will for both the client and VPN server.
- Prevent anyone from outside of the VPN to change the security properties (for example, weakening the encryption) of the VPN, and the administrators of the two endpoints of the tunnel must agree to the security properties of the tunnel.

**NOTE**

The most important requirement for a Secure VPN is that the VPN administrator must be able to determine what data will and will not be contained within the VPN.

**Prevention vs. After the Fact**

From software to services, the security solutions provided by Juniper Networks stop threats before they can do harm. Company networks are accessed by a wide variety of employee, customer, and guest-owned tablets, smartphones, and laptops. That means it’s not always possible to control which devices connect, what’s on them, or how secure they are, yet it’s still necessary to provide consistent, secure, and seamless connectivity.

Additional preventative security measures can be implemented at the client level. One of the easiest ways for a hacker to break the security of a VPN is by stealing or possessing the actual tablet, smartphone, or laptop that is used to dial in for a VPN connection. Unfortunately, a stolen device will most likely have the user’s ID, secret key, and VPN client software all stored on the device. If so, then the thief has everything he or she needs to access a network, steal personal data, and cause undo havoc to daily life in minutes.

An important rule of thumb is to never save the password to the VPN tunnel on the mobile device. All users utilizing BYOD (Bring Your Own Devices) to establish VPN connections with a network should be taught preventative security maintenance, including updated anti-virus software that is installed and running each time they access their devices, personal firewall software set ups, and enabled BIOS passwords.
Commonly Used Secure VPN Protocols

Secure VPN uses special protocols to encrypt and decrypt the transmitted data, and for a tunnel to be established, both the tunnel client and tunnel server must use the same tunneling protocol. Table 1 lists some of the more commonly used Secure VPN protocols and their benefits.

<table>
<thead>
<tr>
<th>Secure VPN Protocol</th>
<th>Definition</th>
<th>OSI Reference Model Layer</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Socket Layer (SSL)/Transport Layer Security (TLS)</td>
<td>Encrypts security information using public/private key technology, which requires a paired private key and authentication certificate (using a handshake method), before transmitting data across a network. SSL/TLS VPNs are often referred to as transparent or clientless because no additional client-side VPN software must be explicitly installed. These protocols are used extensively in the security of online retailers and service providers.</td>
<td>SSL and TLS operate at Layer 7 (Application Layer) and act as a proxy for secured resources.</td>
<td>Maintains and enforces finer-grained access control policies by intercepting all traffic between the authenticated remote system and the requested resource inside the secured network. Provides greater flexibility since virtually any laptop or mobile device with an Internet connection can be used for secure remote access. IT departments have fewer applications to support and maintain.</td>
</tr>
<tr>
<td>Internet Protocol Security (IPsec)</td>
<td>Provides security to Internet Protocol (IP) flows through the use of authentication and encryption: Authentication verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization with whom they believe they are communicating. Encryption makes data confidential by making it unreadable to everyone except the sender and intended recipient. IPsec security is usually implemented in three parts: the authentication header (AH), the Encapsulating Security Payload (ESP), and the Internet Key Exchange (IKE). IPsec is often used to secure Internet connections and can operate in two different modes: tunnel mode (encrypts both header and transmitted data) or transport mode (encrypts only the data packet message itself.</td>
<td>IPsec operates at Layer 3 (Network Layer). It functions independently of any application so IPsec essentially has no impact on the higher network layers.</td>
<td>Provides robust functionality and protects any application traffic across an IP network. Optimized for remote access and distinguishes itself through universal application, simple operation, high performance, transparency, and safety. Indifferent as to whether application traffic is being transported using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) protocols.</td>
</tr>
</tbody>
</table>

Table 1: Secure VPN Protocols
Table 1 Secure VPN Protocols continued

<table>
<thead>
<tr>
<th>Secure VPN Protocol</th>
<th>Definition</th>
<th>OSI Reference Model Layer</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Point-to-Point Tunneling Protocol (PPTP)</strong></td>
<td>PPTP is a proposed standard sponsored by Microsoft and other companies. PPTP provides user-friendly management and control of connections. It divides all the information to be transmitted into two types of messages: control messages and data messages. PPTP [which is an extension of the Internet’s Point-to-Point Protocol (PPP)] allows IP or Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) traffic to be encrypted and encapsulated in an IP packet header that is sent across your company’s Intranet or the Internet. Similar to L2TP, it does not do encryption. PPTP generates the tunnel and encapsulates the data packet, and a secondary protocol, such as Generic Routing Encapsulation (GRE) or Transmission Control Protocol (TCP) encrypts the data. PPTP operates at Layer 2 (Data Link Layer) and establishes a direct connection between two networking nodes.</td>
<td></td>
<td>Widely available and easy to set up. It requires very little bandwidth to operate, so more users can take advantage of a connection without slowing down transmission. Supports a variety of different security measures such as authentication, encryption, and packet filtering. For smaller companies, PPTP is more affordable because it doesn’t require special hardware or software, and usually comes free with most operating systems.</td>
</tr>
<tr>
<td><strong>Layer 2 Tunneling Protocol (L2TP)</strong></td>
<td>L2TP is a combination of PPTP and Layer 2 Forwarding (L2F) technology and a proposed standard offered by Cisco Systems. L2TP uses a User Datagram Protocol (UDP) port for communication. Because it does not provide any security for data such as encryption and confidentiality, an encryption protocol such as IPsec is often used with L2TP (often referred to as L2TP/IPsec). L2TP generates the tunnel, whereas IPsec handles the encryption, channel security, and data integrity checks. L2TP encapsulates PPP frames (data in variable-size units) to be encrypted and sent over any medium that supports point-to-point datagram (basic transfer unit) delivery, such as IP, Frame Relay, or Asynchronous Transfer Mode (ATM) networks. L2TP operates at Layer 2 (Data Link Layer) and is a session layered protocol. L2TP is known as Virtual Dialup Protocol because of its service of the Point-to-Point Protocol (PPP) extension over Internet.</td>
<td></td>
<td>Provides (with IPsec) cost-effective and significant deployment for client-server remote access Secure VPNs. Scalable, fast, and flexible, and provides efficient connectivity for critical applications. Provides the best authorization policy for users with VPN authentication.</td>
</tr>
<tr>
<td>Secure VPN Protocol</td>
<td>Definition</td>
<td>OSI Reference Model Layer</td>
<td>Benefits</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Multi-protocol Label Switching (MPLS) IP</td>
<td>MPLS is a standards-based technology used to speed up the delivery of network packets over multiple protocols. MPLS IP is a VPN that is built on top of an MPLS network, usually from a service provider, to deliver connectivity between enterprise office locations. It provides secure, private, any-to-any service over a dedicated MPLS network while leveraging the scalability of a global infrastructure.</td>
<td>MPLS operates at a hybrid Layer 3 (Network Layer) and Layer 2 (Data Link Layer), a type of “Layer 2.5” protocol. For both IPv4 and IPv6, both unicast and multicast are fully supported in Junos.</td>
<td>Provides scalability, flexibility, maturity, redundancy, and interoperability. It is THE VPN solution. Improves application performance by prioritizing network traffic and allocating bandwidth according to usage and service requirements. Delivers mission-critical and cloud applications, such as VoIP and video, with increased reliability and security.</td>
</tr>
<tr>
<td>Virtual Private LAN Service (VPLS)</td>
<td>Ethernet-based multipoint-to-multipoint Layer 2 VPN service used for interconnecting multiple Ethernet LANs across an MPLS backbone. VPLS is protocol independent and easily supports IP, IPX, and other legacy protocols.</td>
<td>VPLS operates at Layer 2 (Data Link Layer) and is for Ethernet only. It supports both unicast and multicast Layer 2 traffic.</td>
<td>Allows security-conscious businesses to maintain control over routing and does not share Layer 3 routing tables with the service provider. Transports both IP and non-IP traffic over the same network privately and reliably. Ability to easily create a full mesh network where each node captures, disseminates, and relays data for itself and other nodes. Achieves the highest levels of network performance, cost-efficiency, and scalability with competitive SLAs/Class of Service (CoS) options.</td>
</tr>
<tr>
<td>Pseudowire (also known as L2VPN and L2 Circuit)</td>
<td>Emulates a bi-directional point-to-point connection (“extended wire”) over a packet-switching network. Provides flexibility to transmit any type of traffic, such as Ethernet frames, ATM cells, Frame Relay, time-division multiplexing circuits, etc. Pseudowires decouple services (protocols and applications) from the underlying facilities transmitting them, which can be used to build converged networks. L2VPNs are constructed using pseudowires between Provider Edge (PE) routers and are most often used to provide Ethernet services such as Carrier Ethernet.</td>
<td>Pseudowire operates at Layer 2 (Data Link Layer) Pseudowire enables an operator to transport legacy services, including Layer 2 services, over a Layer 3 network.</td>
<td>Ability to transport legacy services (which are already generating revenues and with which customers are already familiar) yet enables companies to leverage the high speed and wide connectivity of their new and scalable IP/MPLS networks, thereby lowering the cost of legacy services and extending them into new markets. Widely used in mobile backhaul, multiple pseudowires enable 2G and 3G traffic to be transmitted across a single network. Ability to statically or dynamically manage changes in the traffic mix and support fine-grained QoS. Provides fast failover from a primary to a backup uplink, and resiliency in the case of uplink or network failure.</td>
</tr>
</tbody>
</table>
Juniper Networks Implementation of Secure VPNs

Juniper Networks provides comprehensive security solutions (which include hardware devices and software/mobility applications) from the data center all the way to end users’ devices, including endpoint security checks, ensuring that access is only granted to healthy devices. New solutions are appearing all the time. Please check www.juniper.net/security for current additions to Juniper’s suite of security solutions.

NOTE
The Junos Pulse product line is now owned and supported by Pulse Secure, LLC. Juniper will continue selling and supporting Pulse through the remainder of 2014. For more information on ongoing development and support of Pulse technology products, please reference: www.pulsesecure.net.

Summary

Secure VPNs have enabled the tremendous growth of online banking, shopping, and communication by providing speed, convenience, and security to millions of transactions transmitted daily. Secure VPNs have also enabled today’s modern business trends of increased telecommuting and global support operations where geographically diverse workers have the ability to connect to central resources and communicate with each other. You can be remote and have secure communications – just always use a Secure VPN no matter the mobile device you are using.

Further Reading

VPN Overview and Common Configuration:

Juniper Networks SRX Series Services Gateways product page:

The Juniper-sponsored J-Net Communities forum is dedicated to sharing information, best practices, and questions about Juniper products, technologies, and solutions. Register to participate at this free forum.
http://forums.juniper.net/t5/SSL-VPN/bd-p/SSL_VPN

“The Virtual Private Network Consortium, better known as VPNC, is the international trade association for manufacturers in the VPN market Founded in 1999, some of the primary purposes of the VPNC are to increase interoperability between members to help them better serve their potential customers, and serve as the forum for the VPN manufacturers throughout the world.” – VPNC
http://www.vpnc.org
Learn About Secure VPNs
by Susan McCoy

A Virtual Private Network (VPN) is a technology you may recognize by name without understanding what it does or how it works. Chances are, much of the time you spend on the Internet is probably spent using a Secure VPN – when you’re mobile and pinging the office, at home telecommuting, or using the cloud to connect to a data center. Learn about Secure VPNs and what Juniper Networks is doing to improve them by making them ever-more reliable, and of course, more secure.