A virtual private network (VPN) allows users to remotely access a private network and share data securely while using a public network (such as the Internet). VPNs are often described as exclusive tunnels that travel through the Internet; the key is that 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 public network. There are three main VPN technologies: trusted, secure, and hybrid.

Hybrid VPNs combine Multiprotocol Label Switching (MPLS) and Internet Protocol security (IPsec)-based VPNs that can run as part of a trusted VPN. Because Hybrid VPNs are still evolving, they are not part of this discussion. 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 VPN 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.

However, 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 viruses and spam attacks, snoopers, hackers, and corporate data thieves. It was at this point that Secure VPN developed into an important VPN technology.
Mobility

It’s unquestionable that the world has gone mobile. Recent statistics from the Pew Research Center (link here) show that the mobile device market continues to skyrocket! As of 2017, 77% of all Americans now own some type of smartphone (up from 35% in 2011).

Ownership of other devices also continues to grow. Approximately 80% of adults surveyed in the U.S. own desktop or laptop computers, about 50% own tablet computers, and approximately 20% use e-reader devices. According to StatCounter Global Stats (link here), as of October 2016, worldwide mobile and tablet Internet usage exceeds desktop usage for the first time.

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, snoopers who steal data are targeting smartphones and tablets.

There are multiple vendors with multiple OS systems, and thousands of apps that use the Internet to connect and share data. According to SimilarWeb’s State of Mobile Web report (link here), roughly 56% of consumer traffic leading to websites in the US is now from mobile devices. Additionally, the app industry is continuing to grow (app downloads have increased 15% in 2016), as is, time spent using the apps (total time spent in apps was up by over 150 billion hours totaling almost 900 billion hours in 2016) See link to TechCrunch.

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 be taken seriously and be made front-and-center. Secure VPN connections between these devices and their destination servers (physical and virtual) are more critical than ever.

Secure VPNs

Secure VPNs use special protocols 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 transmitted data, they could never decrypt any of it.

The entire process of tunneling includes the encapsulation, transmission, and de-encapsulation of data as shown in the illustration of the tunneling process in Figure 1.
A header is added to encapsulated data 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 de-encapsulated 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 (a local or restricted communications network) 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 by using sophisticated authorization measures and secret keys that are discussed in the rest of this Learn About.
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 logical path, so anyone that gains access to your data in the middle of its journey sees 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 content using their wireless 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.

- Allow roaming and remote clients to connect to LAN resources, and remote offices to connect to each other, in order 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 to only 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 commonly used Secure VPN protocols and their benefits.

IP Addresses
Unique decimal dot format addresses that devices use to identify and communicate with each other across a network.
Table 1  Secure VPN Protocols

<table>
<thead>
<tr>
<th>Secure VPN Protocol</th>
<th>Definition</th>
<th>Service Layer</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL/OpenVPN (Secure Sockets Layer)</td>
<td>Encrypts security information using public/private key technology (point-to-point topology), which requires a paired private key and authentication certificate (using a handshake method), before transmitting data across a network. Used extensively by online retailers and service providers.</td>
<td>Layer 3 (IPv4 and IPv6) Note: Although SSL is a Layer 7 protocol, it transports service at Layer 3.</td>
<td>Travels across Web proxies that provide the greatest connection potential for virtually any laptop or mobile device with an Internet connection. Implemented by tunnel endpoints. Offers full security including certificates, identity verification, and data encryption.</td>
</tr>
<tr>
<td>IPsec (Internet Protocol Security)</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 implemented in three parts: the authentication header (AH), the Encapsulating Security Payload (ESP), and the Internet Key Exchange (IKE). IPsec 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>Layer 3 (IPv4 and IPv6)</td>
<td>Provides robust functionality, offers security flexibility, 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>

MORE?  For an overview poster of all the various types of VPNs, see the last page of this Learn About, or download the PDF poster with this link - Day One Poster: What You Need to Know About VPNs.
Summary

Secure VPNs have enabled the tremendous growth of online banking, shopping, communication, and social media 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 be sure to use a Secure VPN no matter the mobile device you are using.

Further Reading

Juniper Networks provides high performance, scalable, and intelligent network security solutions for enterprises and service providers. New solutions are developing all the time.

- Juniper Networks Suite of Security Products and Solutions:

- Junos OS VPNs Configuration Guide:

- Juniper Networks TechWiki is a “tribal think-tank” for the J-Net community to share their solutions for using our products:
  http://forums.juniper.net/t5/TechWiki/ct-p/TechWiki
What You Need to Know About VPNs

<table>
<thead>
<tr>
<th>VPN Name</th>
<th>Service Layer</th>
<th>Topology</th>
<th>Security</th>
<th>Key Advantages</th>
<th>Key Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL/OpenVPN</td>
<td>Layer 3 (IPv4 or IPv6)</td>
<td>P2P</td>
<td>Implemented by tunnel endpoints.</td>
<td>Offers flexibility with security options.</td>
<td>Requires endpoint software or appliance. Tunnel is coupled to service, and difficult to scale.</td>
</tr>
<tr>
<td>Secure Sockets</td>
<td>Same as above</td>
<td>Same as above</td>
<td>SSL</td>
<td></td>
<td>Same as above. Additionally, does not connect across Web proxies, and needs GIE to support IP Multicast.</td>
</tr>
<tr>
<td>IPsec</td>
<td>Layer 3 (IPv4 or IPv6)</td>
<td>Same as above</td>
<td>IPsec AH (Authentication Header)</td>
<td>Offers flexibility with security options.</td>
<td>Provides no security and does not connect across Web proxies.</td>
</tr>
<tr>
<td>GRE/IP-in-IP</td>
<td>Layer 3 (IPv4 or IPv6)</td>
<td>Same as above</td>
<td>GRE. Note: GRE and IP-in-IP (IPRP) are similar. However, GRE is used more often because it allows encapsulation of any protocol on top of it.</td>
<td></td>
<td>Provides no security and does not connect across Web proxies.</td>
</tr>
<tr>
<td>MPLS/VPN</td>
<td>Layer 3 (IPv4 or IPv6), Junos OS</td>
<td>EVPN</td>
<td>MPLS. Provides a multipoint solution with more than two sites interconnected and MAC learning. Compared to MPLS/VPN, EVPL provides MAC learning at the control plane level. EVPL provides active-active redundancy, whereas MPLS/VPN only provides active-standby redundancy. All vendors agreed to use BGP signaling.</td>
<td></td>
<td>Provides no security and does not connect across Web proxies.</td>
</tr>
<tr>
<td>Multiprotocol Label Switching</td>
<td>Layer 2 (Ethernet, Frame Relay, ATM, PPP, or HDLC)</td>
<td>P2MP</td>
<td>MPLS tunnel signaling is performed on RSVP only.</td>
<td>Scaling issues because of the 1512 (tunnel) mapping, and it is P2MP.</td>
<td></td>
</tr>
<tr>
<td>VPLS VPLS (Virtual Private LAN Service)</td>
<td>Layer 2 (Ethernet only), Supports Ucast and Multicast 2 traffic, raw Ethernet frames, and VPLS-tagged frames.</td>
<td>MPLS can be P2MP or LDP.</td>
<td>Forwarding Plane: MPLS (P2M or P2F)</td>
<td>Depends on a Service Provider (or server of Service). This is not a self-provisioning solution. If geographically vast, then the MPLS VPLS needs a Service Provider with a huge presence, or an inter-AS solution.</td>
<td></td>
</tr>
<tr>
<td>VXLAN VXLAN (Virtual Extensible LAN)</td>
<td>Layer 2 (Ethernet), Supports Ucast and Multicast 2 traffic.</td>
<td>Transparent (to customer).</td>
<td>LDP.</td>
<td>Provides no security and does not connect across Web proxies.</td>
<td></td>
</tr>
<tr>
<td>EVVPN EVVPN (Ethernet VPN)</td>
<td>Same as above</td>
<td>Same as above</td>
<td>BUM traffic (broadcast, unknown unicast, multicast) is treated as Layer 2 Multicast.</td>
<td>No control plane (could use EVPH as the control plane for VXLAN).</td>
<td>Provides no security and does not connect across Web proxies.</td>
</tr>
</tbody>
</table>

Related Protocols/VPNs:
- SSL: TLS, HTTP
- IPsec: GRE, 10BaseT, PPP
- MPLS/VPN: BGP, IS-IS, IP, L2TP, MPLS (Pseudowire), VLL (Virtual-Linkless Ethernet)
- GRE/IP-in-IP: EVPN (Ethernet Virtual Private LAN Service), VLL (Virtual-Linkless Ethernet), EVPL (Ethernet Virtual Private Line), EVPH (Ethernet Virtual Private Hub), EVPLS (Ethernet Virtual Private Line Service)
- MPLS/VPN: E-LAN (E-Metro Ethernet), E-MPLS (E-Metro Virtual Ethernet), MPLS (Pseudowire), E-LAN (E-Metro Ethernet), E-MPLS (E-Metro Virtual Ethernet)

Legend:
- P2P = point-to-point
- P2MP = point-to-multipoint

Post concept:
Susan McCoy
Antonio García-Mingorri
http://www.juniper.net/junos/poster DAY ONE POSTER What You Need to Know About VPNs

© 2017 by Juniper Networks, Inc. All rights reserved. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.