Learn About Secure VPNs, 2nd Edition

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.

Protocol
Rules determining the format and transmission of data between endpoints in a telecommunication connection.

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.

Service Provider
A company that provides access to the Internet and related services to individual customers and to other businesses. A few examples are AT&T, Verizon, Comcast, China Telecom, and Deutsche Telecom.

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.

For more see:
juniper.net/documentation

Susan McCoy is a Staff Engineer Technical Writer at Juniper Networks with over 20 years of experience writing and developing documentation for networking, telecommunications, manufacturing, and marketing.

Version History: Second Edition, April 2017 2 3 4 5 6 7 8 9

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

Tunneling
Allows the use of the Internet, a public network, to convey data on behalf of a private network. Also known as port forwarding.

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.

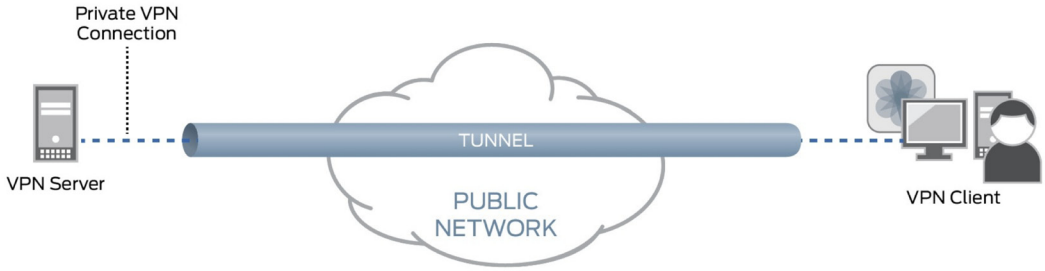

Figure 1 *Tunneling Overview*

Packet
Fundamental unit of information (message or fragment of a message) carried in a packet- switched network, for example, the Internet

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.

Client
A physical node, or software program, that requests services from a server.

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.

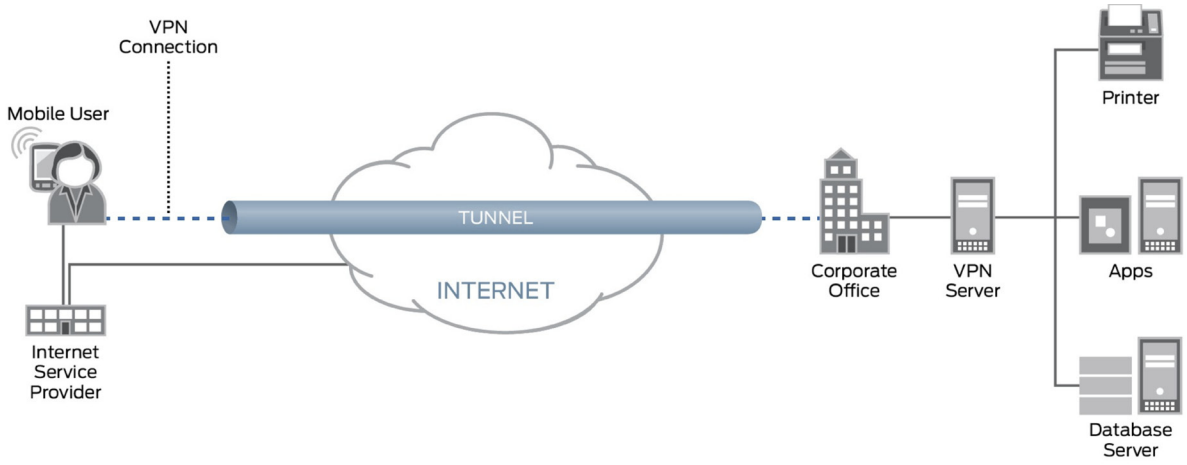

Figure 2 *Remote Access Over Internet*

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.

Internet Protocol (IP)
Provides the functions necessary to deliver blocks of data (datagrams) from a source to a destination over an interconnected system of networks, where sources and destinations are identified by fixed length addresses.

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

- 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.

Table 1 *Secure VPN Protocols*

Secure VPN Protocol	Definition	Service Layer	Benefits
SSL/OpenVPN (Secure Sockets Layer)	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.	Layer 3 (IPv4 and IPv6) Note: Although SSL is a Layer 7 protocol, it transports service at Layer 3.	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.
IPsec (Internet Protocol Security)	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.	Layer 3 (IPv4 and IPv6)	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.

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: http://www.juniper.net/us/en/products-services/security/
- Junos OS VPNs Configuration Guide: http://www.juniper.net/techpubs/en_US/junos12.3/information-products/pathway-pages/config-guide-vpns/index.html
- 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

JUNIPER NETWORKS

VPN Name	Service Layer	Topology	Security	Service Protocols	Tunnel/Transport Protocols	Key Advantages	Key Limitations
SSL/OpenVPN Secure Sockets Layer	Layer 3 (IPv4 or IPv6) Note: Although SSL is a Layer 7 protocol, it transports service at Layer 3.	P2P. The service is decoupled from the tunnels. The same tunnels can transport traffic from many different VXLANs.	Implemented by tunnel endpoints. Offers full security including certificates, identity verification, and data encryption.	RFC 2246 for SSL	SSL	Travels across Web proxies and provides greatest connection potential.	Requires endpoint software or appliance. Tunnel is coupled to service, and difficult to scale.
IPsec Internet Protocol Security	Layer 3 (IPv4 or IPv6).	Same as above.	Same as above.	RFCs: 4302, 4303, 5996, and 6071	IPsec AH (Authentication Header) IPsec ESP (Encapsulating Security Payload)	Offers flexibility with security options.	Same as above. Additionally, does not connect across Web proxies, and needs GRE to support IP Multicast.
GRE/IP-in-IP Generic Routing Encapsulation	Layer 3 (IPv4 or IPv6).	Same as above.	None! To implement security in tunnel, couple to IPsec using GRE over IPsec.	RFC 2890 for GRE RFC 1853 for IP-in-IP	GRE. Note: GRE and IP-in-IP (IP/IP) are similar. However, GRE is used more often because it allows encapsulation of any protocol on top of it.	Offers simplicity.	Provides no security and does not connect across Web proxies.
MPLS IP VPN Multiprotocol Label Switching	Layer 3 (IPv4 or IPv6). Junos OS enables the same VPN with IPv4/Unicast, IPv4 Multicast, IPv6 Unicast, and IPv6 Multicast services, together, or as a subset. In some products, Junos OS supports ISO VPNs, where the service protocol is ISO, not IP, so L3VPN applies but not MPLS IP VPN. ISO packets are transported, just like IP VPN packets.	Can be full mesh between PEs, partial mesh, or a hub-and-spoke topology. You can connect several VPNs in an extranet. Note: The Unicast service is decoupled from the tunnels. The same tunnels can transport traffic from many different VPNs of different types due to MPLS label stacking (one label for the service, one label for the transport).	Implemented by the Service Provider. Maintains separate per-VPN forwarding/routing instances, called VRFs (transparent to customer).	For Unicast IP Service: BGP only. For Multicast IP Service: BGP or PIM. (Juniper Networks, Nokia, and Huawei only support BGP for consistency with Unicast model.) RFCs: 4364, 4659, 6513, 6514, and 6826	Forwarding Plane: MPLS (P2P, or P2MP) or GRE (P2P, or P2MP). Transport tunnels for Unicast are P2P (PE-to-PE) and for Multicast are P2MP (one-PE-to-several-PEs). Multicast service may reuse the P2P tunnels for Unicast (with special configuration). Control Plane (tunnel signaling): If forwarding plane = MPLS, then LDP, RSVP, or L-BGP can perform tunnel signaling. You can use IGP with SPRING to establish MPLS forwarding path. If forwarding plane = GRE, then no tunnel signaling exists for Unicast services; and tunnel signaling is performed by PIM for Multicast services.	Scalability, flexibility, maturity, redundancy, and interoperability.	Depends on a Service Provider (or set of Service Providers). This is not a self-provisioning solution. If geographically vast, then the MPLS VPN needs a Service Provider with a huge presence, or an Inter-AS solution, or a combination of the MPLS VPN with an IP tunneling approach like IPsec.
CCC and TCC Circuit and Translational Cross-Connects	Layer 2: Ethernet, Frame Relay, ATM, PPP or HDLC.	P2P. The tunnel is coupled to service and each service, or cross-connect, has a different tunnel.	Implemented by the Service Provider. Maintains separate forwarding information for each cross-connect (transparent to customer).	RFC: In draft. Refer to 3985.	MPLS (P2P). Tunnel signaling is performed by RSVP only.	Service interfaces at each endpoint (PE1, PE2) for CCC must be the same type (for example, both Ethernet or both ATM). Service interfaces for TCC can be different types. Junos OS changes Layer 2 encapsulation without any Layer 3 routing (also known as L2.5 VPN).	Scaling issues because of the 1:1 (service:tunnel) mapping, and it is P2P.
Ethernet Pseudowires	Layer 2. Supports Unicast and Multicast Layer 2 traffic, raw Ethernet frames, and VLAN-tagged frames. Allows for VLAN tag manipulation at the endpoints (push, pop, and swap).	P2P. The service is decoupled from the tunnels. The same tunnels can transport traffic from many different VPNs.	Implemented by the Service Provider. Maintains separate forwarding information for each pseudowire (transparent to customer).	Protocols can be BGP or LDP. Junos OS interoperates between BGP and LDP signaled networks. RFC 6625 for BGP RFC 4447 for LDP	Forwarding Plane: MPLS (P2P) or GRE (P2P). Transport tunnels are P2P (PE-to-PE). Control Plane (tunnel signaling): If forwarding plane = MPLS tunnel signaling is either LDP, RSVP, or L-BGP. You can use IGP with SPRING to establish MPLS forwarding path. If forwarding plane = GRE, then there is no tunnel signaling.	Simplicity. You can internally connect pseudowires in a PE to another VPN. For example, you can stitch two pseudowires, or add the endpoint of a pseudowire to a VPLS/EVPN instance. When the service is signaled with LDP, advantage = wider interoperability; with BGP, advantage = better scalability and using BGP as MPLS service protocol.	Same as above. Pseudowires are P2P and do not implement MAC address learning. They emulate an extended wire, not a LAN.
VXLAN Virtual Extensible LAN	Layer 2. Supports Unicast and Multicast Layer 2 traffic.	P2P. The service is decoupled from the tunnels. The same tunnels can transport traffic from many different VXLANs.	Implemented by the Data Center/operator. Maintains separate forwarding information for each VXLAN (transparent to customer).	RFC 7348 Note: You can use EVPN as the control plane for VXLAN.	UDP Ethernet frames are encapsulated in UDP with an additional VXLAN header.	Extends the limitation of 4095 VLANs to 16 million VNI (VXLAN Network Identifiers) logical networks. Typically used in a Data Center environment.	No control plane (could use EVPN as control plane). Limited entropy for ECMP/Hashing (only source UDP port).
VPLS Virtual Private LAN Service	Layer 2 (Ethernet only). Supports Unicast and Multicast Layer 2 traffic. VPLS supports raw Ethernet frames, VLAN tagged frames. Allows for VLAN tag manipulation at the endpoints (push, pop, and swap).	VPLS can be a full-mesh between PEs, a partial-mesh, or a hub-and-spoke (tree) topology. Unicast service is decoupled from the tunnels. The same tunnels can transport traffic from many different VPNs.	Implemented by the Service Provider. Maintains separate per-VPLS forwarding instances (transparent to customer).	Protocols can be BGP or LDP. Junos OS interoperates BGP and LDP signaled networks. RFC 4761 for BGP RFC 4762 for LDP RFC 6074 for BGP and LDP	Forwarding Plane: MPLS (P2P or P2MP) or GRE (P2P). Transport tunnels for Layer 2: Unicast are P2P (PE-to-PE). Multicast are P2MP (one-PE-to-several-PEs). Control Plane (tunnel signaling): If forwarding plane = MPLS tunnel signaling is either LDP, RSVP, or L-BGP. You can use IGP with SPRING to establish MPLS forwarding path. If forwarding plane = GRE, then there is no tunnel signaling.	Compared to a pseudowire, VPLS provides a multipoint solution with more than two sites interconnected and MAC learning. Compared to EVPN, VPLS has less control plane signaling. When service is signaled with LDP, advantage = wider interoperability. With BGP, advantage = redundancy (active-backup), auto-discovery, and better scalability.	MAC learning is performed at the forwarding plane level. The entire VPLS traveling across the PEs functions as a single Ethernet switch.
EVPN Ethernet VPN	Same as above.	Same as above.	Implemented by the Service Provider. Maintains separate per-EVPN forwarding instances (transparent to customer).	RFC 7432 for BGP	Forwarding Plane: MPLS/MPLSoUDP/MPLSoGRE (P2P or P2MP), VXLAN, GRE (P2P). Transport tunnels for Layer 2: Unicast are P2P (PE-to-PE). Multicast are P2P, or P2MP (one-PE-to-several-PEs). Control Plane (tunnel signaling): If forwarding plane = MPLS tunnel signaling is either LDP, RSVP, or L-BGP. You can use IGP with SPRING extensions to establish MPLS forwarding path. If forwarding plane = GRE, then there is no tunnel signaling. BUM traffic (broadcast, unknown unicast, multicast) is treated as Layer 2 Multicast.	Compared to a pseudowire, EVPN provides a multipoint solution with more than two sites interconnected and MAC learning. Compared to VPLS, EVPN provides MAC learning at the control plane level. EVPN provides active-active redundancy, whereas VPLS only provides active-backup redundancy. All vendors agreed to use BGP signaling.	More signaling than VPLS due to the MAC address information exchanged through BGP.

Related Protocols/VPNs

SSL: TLS, HTTP

GRE/IP-in-IP: IP/GRE, IP/IP

MPLS IP VPN: BGP/MPLS VPN, L3VPN (for IPv4 Unicast), 6VPE (for IPv6 Unicast), MVPN (for IPv4/IPv6 Multicast)

CCC and TCC: PWE (Pseudowire Emulation) (refers to Layer 2 payloads at the endpoints), PWE3 (Pseudowire Emulation Edge-to-Edge), L2.5 VPNs often refer to TCC

Ethernet Pseudowires: PWE and PWE3. L2 Circuit, L2CKT, or L2VPN (for LDP-signaled service use L2 Circuit and L2CKT. For BGP-signaled service, use L2VPN.

E-Line: MEF (Metro Ethernet Forum), VPWS (Virtual Private Wire Service), VLL (Virtual Leased Line), EVPL (Ethernet Virtual Private Line), EVC (Ethernet Virtual Circuit).

VPLS: E-LAN: MEF (Metro Ethernet Forum), Multipoint-to-Multipoint EVC (Ethernet Virtual Circuit).

Legend

P2P = point-to-point
P2MP = point-to-multipoint

Poster concept

Susan McCoy
Krzysztof Szarkowicz
Antonio Sánchez-Monge

https://www.juniper.net/documentation/en_US/junos/topics/concept/vpn-security-overview.html

http://www.juniper.net/techpubs/en_US/learn-about/secure-vpns.pdf

DAY ONE POSTER

What You Need to Know About VPNs

Juniper Networks Information and Learning Experience (iLX)

www.juniper.net/posters