Security Filtering—Access Control Lists and VPN

by Sophia

WHAT'S COVERED

In this lesson, you will learn about security filtering and how to use access control lists and VPNs.

Specifically, this lesson will cover the following:

BEFORE YOU START

It is important to control who or what can access a network by identifying the specific computers and individuals who have the right to gain access to it and its resources. But how do we do this? There are some basic ways to safely allow selected computers to have access to your network. There are also ways to keep those that are unwanted, out.

1. Access Control Lists

The first line of defense is something called security filtering, which broadly refers to ways to let people securely access your resources. This process is twofold and includes ensuring that only authorized computers get to enter your network and making sure that the data you are sending back and forth between networks are secured so they cannot be intercepted and translated by malicious attackers.

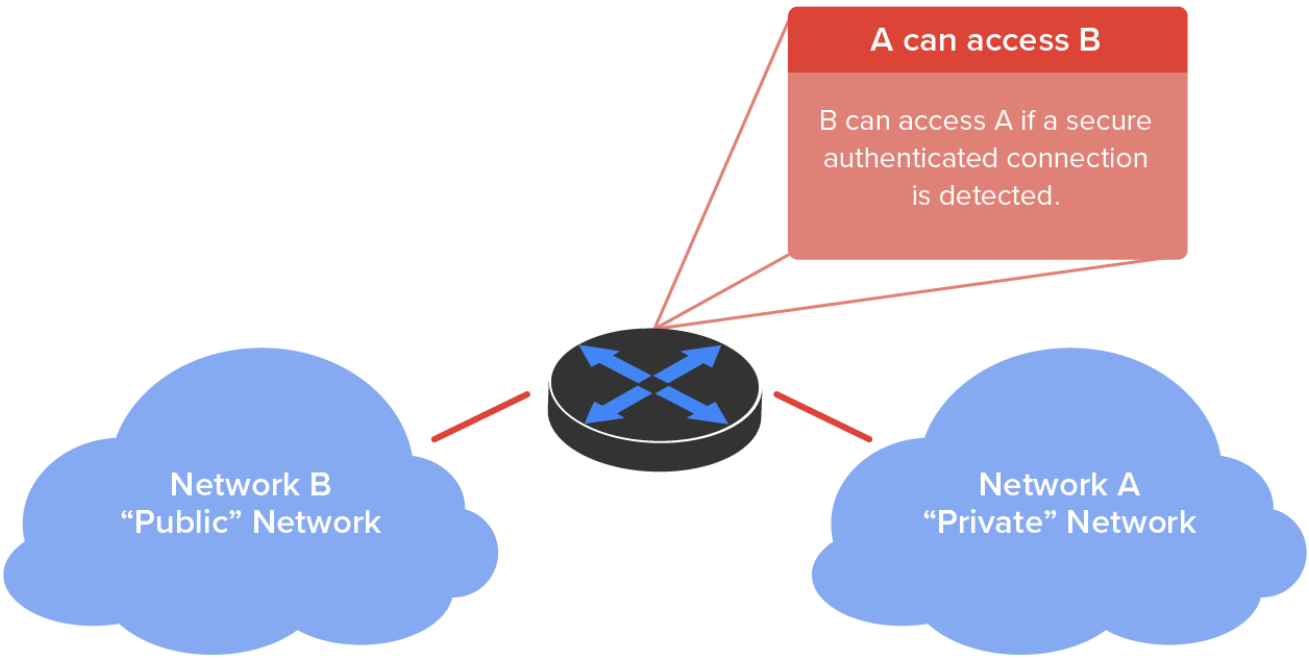
It is rare to find a network around these days that is not connected to the internet. The internet is clearly a public internetwork that anyone can connect to, but your personal network and that of your company are private ones. Every time you connect to the internet from a private network, you may be vulnerable to security break-ins. This

is where a **firewall** comes into play. Firewalls are basically tools that you can implement to prevent any unauthorized users roaming around on public networks from gaining access to your private network.

BIG IDEA

One method to control access to your network is the use of **access control lists (ACLs)**. ACLs typically reside on routers to determine which packets are allowed to route through them based on the requesting device's source or destination IP address.

EXAMPLE The illustration below demonstrates how ACLs prevent unauthorized users on Network B from accessing Network A.



What we see above is that users in Network A can pass through the router into Network B. This means that an IP **spoofing** attack, where someone pretends to have a network address inside a firewall to gain network access, can still happen if a user in Network B pretends to be located in Network A.

You can create a wide array of ACLs, from the very simple to the highly complex, depending on exactly what you want to have them do for you. One example of the use of an ACL places separate inbound and outbound ACLs on a router. This ACL ensures that the data that are leaving your network come from a different source than the data that are coming into it.

KEY CONCEPT

When configuring ACLs between the internet and your private network to mitigate security problems, it is a good idea to include the following four conditions to prevent any unwanted outside access to your network:

- Deny any addresses from your internal networks

- Deny any local host addresses (127.0.0.0/8)
- Deny any reserved private addresses
- Deny any addresses in the IP multicast address range (224.0.0.0/4)

None of these addresses should ever be allowed to enter your private network. Let's look at a variety of methods for controlling access.

TERMS TO KNOW

Firewall

The software that monitors traffic in and out of a private network or a personal computer and allows or blocks such traffic depending on its perceived threat.

Access Control Lists (ACLs)

Lists that typically reside on routers to determine which packets are allowed to route through them based on the requesting device's source or destination IP address or MAC address.

Spoofing

A method of attacking a computer program in which the program is modified so as to appear to be working normally when, in reality, it has been modified with the purpose of circumventing security mechanisms.

1a. MAC Filtering

Most of the time, it is wise to configure ACLs so that they will allow or deny access based on the IP address of the source or destination device. If your network is running a protocol other than Transmission Control Protocol/Internet Protocol (TCP/IP), you can filter traffic based on a medium access control (MAC), or hardware, address instead of an IP address. You can still use an ACL based on a MAC address if you are running TCP/IP, but keep in mind that it is a lot easier to deal with IP addresses than MAC addresses.

HINT

Even though most firewalls and routers will allow you to create both IP-based and MAC-based ACLs, doing so can create a complex situation where access is denied when it really should not be.

1b. Port Filtering

ACLs can also be used to filter based on port numbers as well as IP addresses. In fact, most firewalls default to allowing only the open ports that you specify. When managing a firewall, it is important to know the port numbers of all traffic that needs to be allowed through it. This means that for some of your applications, you will need to read and learn the port numbers being used. It is important to know the port numbers of security protocols like SSL (TCP port 443) and IPSec (UDP port 500).

HINT

Successful firewall management involves being aware of and allowing only the ports to keep authorized services running.

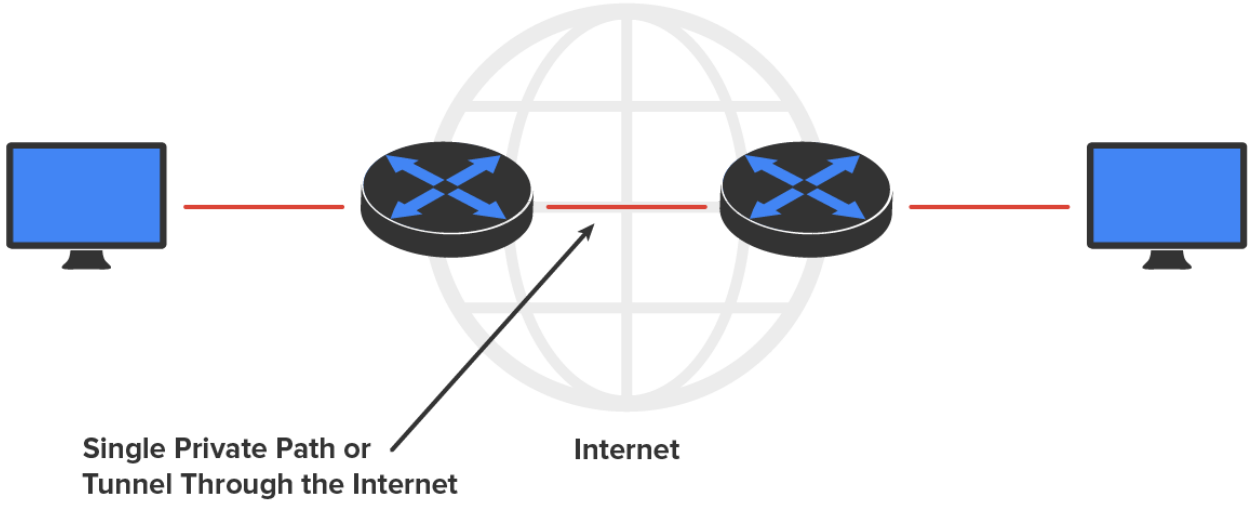
1c. Tunneling

A huge amount of sensitive data is sent out over the internet without any encryption or security. Security protocols are sets of conditions or rules that define how a secure connection is maintained when we send sensitive data through an unsecured medium like the internet or a wireless connection. Before talking about security protocols, let's define a few terms.

The first is a concept called **tunneling**, which basically means encapsulating one protocol within another to ensure that a transmission is secure.

> EXAMPLE We typically use IP known as a **payload protocol** that can be encapsulated within a **delivery protocol** like Internet Protocol Security (IPSec). If you took a look at these packets individually, you would see that they are encrypted. If you look at the process as a whole, it appears that a point-to-point tunnel is created on the internet.

The diagram below illustrates this:

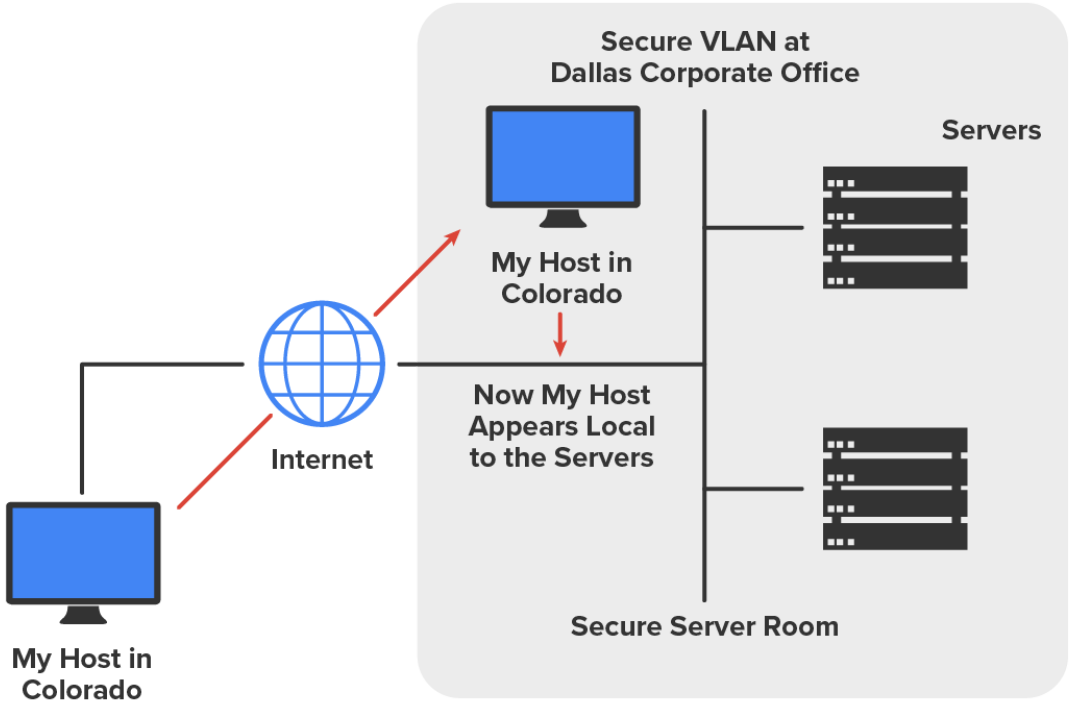


Let's move on to discuss various tunneling protocols.

A **virtual private network (VPN)** fits somewhere between a LAN and WAN and many times may seem just like a WAN link because your computer, on one LAN, connects to a different, remote LAN and uses its resources remotely. The key difference with VPNs is security. A typical WAN connects two or more remote LANs together using someone else's network—for example, your telecommunications provider. Your local host and router see these networks as remote networks and not as local networks or local resources. This would be a WAN in its most general definition. A VPN actually makes your local host part of the remote network by using the WAN link that connects you to the remote LAN. The VPN will make your host appear on the network as though it's actually local on the remote network. This means that we now have secure access to the remote LAN's resources.

> EXAMPLE The diagram below shows this example of a host using a VPN connection from Boulder to Dallas, which allows access to remote network services and servers as if the host were right there on the

same VLAN as the servers.



A VPN allows you to connect to resources by locally attaching to the VLAN through a VPN across the WAN. The different types of VPNs are named based on the kind of role they play in a real-world business situation. There are three different categories of VPNs:

Remote-access VPNs allow remote users like telecommuters to securely access the corporate network wherever and whenever they need to.

A **host-to-host VPN** is somewhat like a site-to-site VPN in concept, except that the endpoints of the tunnel are two individual hosts. In this case, all traffic is protected from the time it leaves the NIC of one host till it reaches the NIC of the other host.

Site-to-site VPNs, or intranet VPNs, allow a company to connect its remote sites to the corporate backbone securely over a public medium like the internet instead of requiring more expensive WAN connections like MPLS. This is probably the best solution for connecting a remote office to the main company office.

Extranet VPNs allow an organization's suppliers, partners, and customers to be connected to the corporate network in a limited way for business-to-business (B2B) communications.

TERMS TO KNOW

Tunneling

A means of encapsulating one protocol within another to ensure that a transmission is secure.

Payload Protocol

A protocol that carries the part of the transmitted data that is the actual intended message.

Delivery Protocol

A protocol that encapsulates a payload protocol.

Virtual Private Network (VPN)

A public network connection that emulates a private network connection by using encryption to keep information secure.

Remote-Access VPN

Allows remote users like telecommuters to securely access the corporate network wherever and whenever they need to.

Host-to-Host VPN

Supports tunneling between two individual hosts.

Site-to-Site VPN

Enables an organization to connect its remote sites to the enterprise's backbone securely over a public medium like the internet instead of requiring more expensive wide area network connections like MPLS.

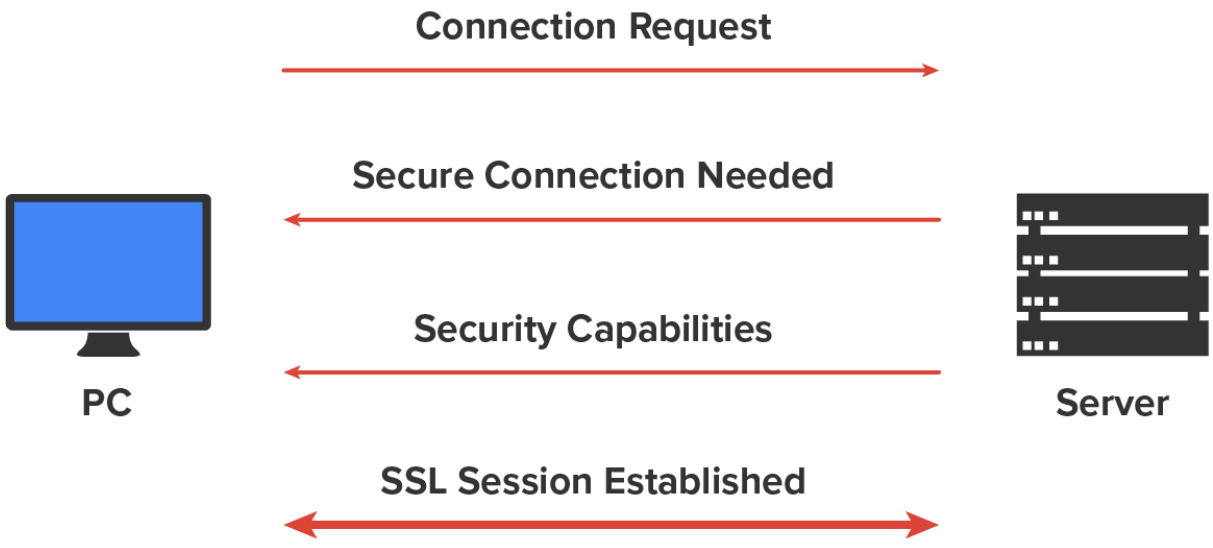
Extranet VPN

Allows an organization's suppliers, partners, and customers to be connected to the corporate network in a limited way for business-to-business (B2B) communications.

1d. SSL and SSL VPN

Secure Sockets Layer (SSL) is a security protocol based on the RSA public-key encryption that is used to enable secure connections over the internet between a web browser and a web server. SSL is service independent, meaning a lot of different network applications can be secured with it. SSL was merged with other security protocols to form a new protocol called Transport Layer Security (TLS). The latest version of TLS (TLS 1.3) provides a number of enhancements over earlier versions.

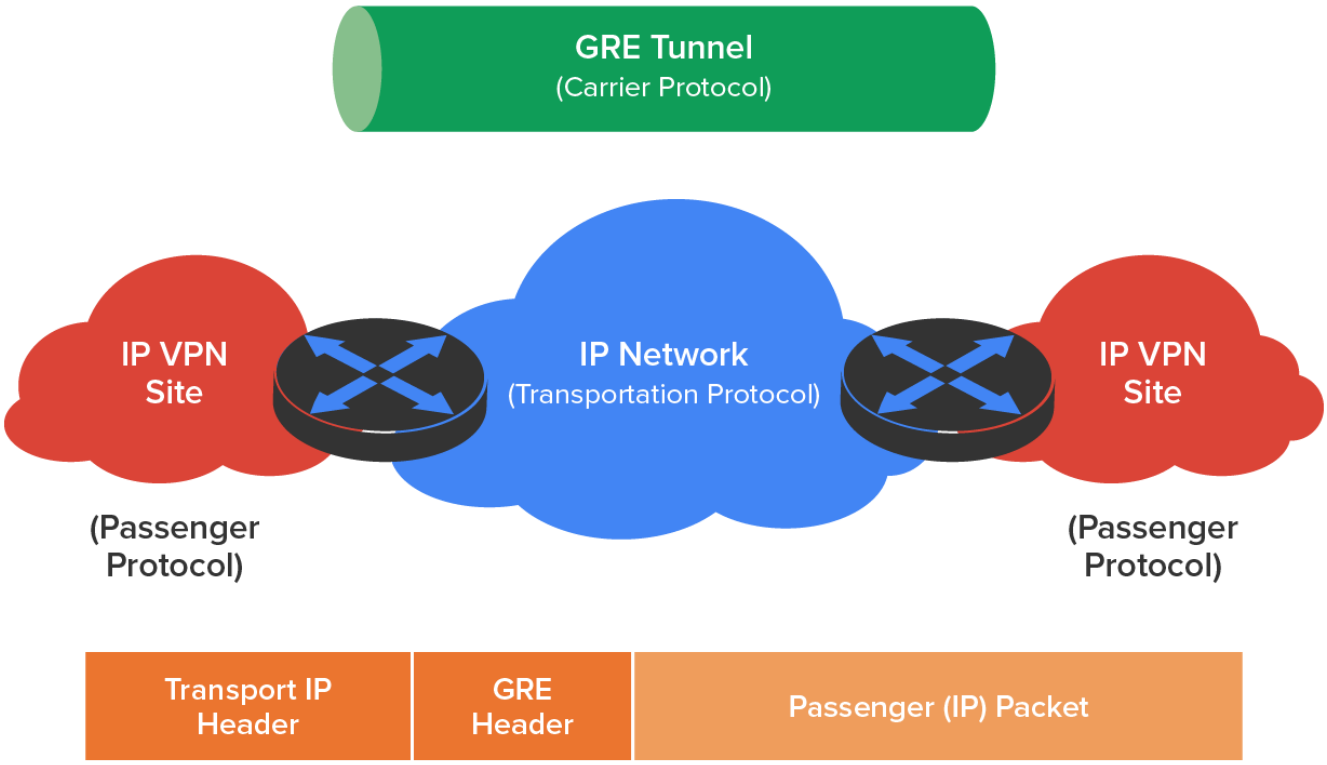
EXAMPLE The diagram below shows the SSL connection process.



Layer 2 Tunneling Protocol (L2TP) was created by the Internet Engineering Task Force (IETF). It comes in handy for supporting non-TCP/IP protocols in VPNs over the internet. L2TP is actually a combination of Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technologies.

Point-to-Point Tunneling Protocol (PPTP) acts by combining an unsecured Point-to-Point Protocol (PPP) session with a secured session using the Generic Routing Encapsulation (GRE) protocol.

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate many protocols inside IP tunnels. Some examples would be routing protocols such as EIGRP and OSPF and the routed protocol IPv6. The diagram below shows GRE.



IP Security (IPSec) was designed by the IETF for providing authentication and encryption over the internet. It works at Layer 3 (network) of the OSI model and secures all applications that operate in the layers above it. Because it is sanctioned by the IETF and designed to work with IPv4 and IPv6, it is the standard for VPNs on the internet today.

The two major protocols you will find working in IPSec are **Authentication Header (AH)** and **Encapsulating Security Payload (ESP)**. AH provides authentication services, but ESP provides both authentication and encryption abilities. Both of these protocols can be used with either mode discussed in the following paragraph.

The **Internet Security Association and Key Management Protocol (ISAKMP)** defines procedures and packet formats to establish, negotiate, modify, and delete security associations (SAs). SAs contain the information required to execute security services, such as header authentication and payload encapsulation. ISAKMP's real value is its ability to provide a framework for safely transferring key and authentication data independent of the key generation technique, encryption algorithm, and authentication mechanism. ISAKMP is integrated into IPSec.

TERMS TO KNOW

Secure Sockets Layer (SSL)

A security protocol based on the RSA public-key encryption that is used to enable secure connections over the internet between a web browser and a web server.

Layer 2 Tunneling Protocol (L2TP)

A tunneling protocol used to support virtual private networks (VPNs)

Point-to-Point Tunneling Protocol (PPTP)

A legacy method for implementing virtual private networks.

Generic Routing Encapsulation (GRE)

A tunneling protocol that can encapsulate many protocols inside IP tunnels.

IP Security (IPSec)

A secure network protocol suite that authenticates and encrypts packets of data to provide secure encrypted communication between two computers over an IP network.

Authentication Header (AH)

A protocol that ensures connectionless integrity by using a hash function and a secret shared key.

Encapsulating Security Payload (ESP)

A protocol that provides origin authenticity through source authentication, data integrity through hash functions, and confidentiality through encryption protection for IP packets.

Internet Security Association and Key Management Protocol (ISAKMP)

A protocol that defines procedures and packet formats to establish, negotiate, modify, and delete security associations.

SUMMARY

In this lesson, you learned about security filtering using **access control lists** and VPNs. We discussed **MAC filtering**, **port filtering**, and **tunneling**. You also learned about various tunneling protocols, including **SSL**, L2TP, PPTP, GRE, IPSec, and ISAKMP.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Access Control Lists (ACLs)

Lists that typically reside on routers to determine which packets are allowed to route through them based on the requesting device's source or destination IP address or MAC address.

Authentication Header (AH)

A protocol that ensures connectionless integrity by using a hash function and a secret shared key.

Delivery Protocol

A protocol that encapsulates a payload protocol.

Encapsulating Security Payload (ESP)

A protocol that provides origin authenticity through source authentication, data integrity through hash functions and confidentiality through encryption protection for IP packets.

Extranet VPN

Allows an organization's suppliers, partners, and customers to be connected to the corporate network in a limited way for business-to-business (B2B) communications.

Firewall

The software that monitors traffic in and out of a private network or a personal computer and allows or blocks such traffic depending on its perceived threat.

Generic Routing Encapsulation (GRE)

A tunneling protocol that can encapsulate many protocols inside IP tunnels.

Host-to-Host VPN

Supports tunneling between two individual hosts.

IP Security (IPSec)

A secure network protocol suite that authenticates and encrypts packets of data to provide secure encrypted communication between two computers over an IP network.

Internet Security Association and Key Management Protocol (ISAKMP)

A protocol that defines procedures and packet formats to establish, negotiate, modify, and delete security associations.

Layer 2 Tunneling Protocol (L2TP)

A tunneling protocol used to support virtual private networks (VPNs)

Payload Protocol

A protocol that carries the part of the transmitted data that is the actual intended message.

Point-to-Point Tunneling Protocol (PPTP)

A legacy method for implementing virtual private networks.

Remote-Access VPN

Allows remote users like telecommuters to securely access the corporate network wherever and whenever they need to.

Secure Sockets Layer (SSL)

A security protocol based on the RSA public-key encryption that is used to enable secure connections over the internet between a web browser and a web server.

Site-to-Site VPN

Enables an organization to connect its remote sites to the enterprise's backbone securely over a public medium like the internet instead of requiring more expensive wide area network connections like MPLS.

Spoofing

A method of attacking a computer program in which the program is modified so as to appear to be working normally when, in reality, it has been modified with the purpose of circumventing security mechanisms.

Tunneling

A means of encapsulating one protocol within another to ensure that a transmission is secure.

Virtual Private Network (VPN)

A public network connection that emulates a private network connection by using encryption to keep information secure.