VPN

What is a Virtual Private Network?

Commonly known as a VPN and defined differently by different entities, it is a group of two or more computer systems, typically connected to a private network (a network built and maintained by an organization solely for its own use) with limited public-network access, that communicates "securely" over a public network, such as the Internet. VPNs may exist between an individual machine and a private network (client-to-server) or a remote LAN and a private network (server-to-server).

What are the trends driving VPNs?

A convergence of business, social, and technology trends are driving the dispersion of today's enterprise into a distributed workplace:

- Rapid proliferation of powerful, affordable PCs and other small office technologies.
- Emergence of the Internet as the global data communications network for linking geographically dispersed locations.
- Demand by employees for flexible work arrangements in response to growing commute times and family needs.
- Drive for improved productivity and reduced costs by companies.
- Need for recruiting and retaining talent located outside the confines of the local geographical area.
- Explosive availability of affordable, broadband Internet connections (DSL, cable and wireless).

What are the advantages of using VPNs?

- Cost Savings – By leveraging third party networks, with VPN, organizations no longer have to use expensive leased or frame relay lines and are able to connect remote users to their corporate networks via a local Internet service provider (ISP) instead of via expensive 800-number or long distance calls to resource-consuming modem banks
- Security – VPNs provide the highest level of security using advanced encryption and authentication protocols that protect data from unauthorized access.
- Scalability – VPNs allow corporations to utilize remote access infrastructure within ISPs. Therefore, corporations are able to add a virtually unlimited amount of capacity without adding significant infrastructure.
- Compatibility with Broadband Technology – VPNs allow mobile workers, telecommuters and day extenders to take advantage of high-speed, broadband connectivity, such as DSL and Cable, when gaining access to their corporate networks, providing workers significant flexibility and efficiency.

NETGEAR's VPN Firewall Routers and Client Software

VPN Firewall Routers

NETGEAR's ProSafe VPN Firewall router products ensure maximum privacy and security with the high-level encryption your business demands. We offer a choice of standards-based wired and wireless VPN/Firewall routers, equipped with 2 to 100 VPN tunnel support capability, as well as all-in-one devices composed of an access point, router, and print server. Our products are easy to configure and provide reliable, secure Internet connectivity. Standard features include Stateful Packet Inspection (SPI), AES and 3DES Encryption, Denial of Service (DoS) protection, Network Address Translation (NAT), and DHCP, plus support for VPN tunnels for extra secure Internet connectivity.

Combined with NETGEAR's ProSafe VPN client software, NETGEAR Firewall routers deliver a total solution for secure data transmission. NETGEAR's security products are VPNC tested and certified in order to ensure interoperability with many other popular security products.

VPN Firewall Routers enable your office LAN (Local Area Network) to securely communicate with other networks that are geographically distant from each other and the Internet via an ISDN or broadband connection (using modems). Virtual Private Network (VPN) VPN functionality enables secure connectivity between remote locations and telecommuters by encrypting traffic over the Internet. Interoperability is an important feature in a VPN environment. All NETGEAR products are VPNC-certified for Basic Interoperability and many are ICSA firewall-certified.

Wired or Wireless VPN Firewall Routers

NETGEAR offers a choice of wired and wireless VPN firewall routers to connect to an Ethernet cabled network or a wireless network. If your office network is a combination of Ethernet and wireless networking, choose a wireless VPN firewall router as this type of device contains an antenna for wireless communication and switch ports for Ethernet connectivity.

VPN Firewall Routers Perform Three Main Services:

Protected Internet Access Using a Firewall

The VPN Firewall Router is the security-conscious device that sits between your network and the outside world. The Firewall is a set of security protocols that protect your business network that prevents Internet users from wandering into your LAN and ‘hacking’ your network and systems. The Firewall within the VPN Firewall Router is the first line of defense for any network that is connected to the Internet. You should never connect a business network to the Internet without configuring the Firewall features within a router.

Business-class firewall protection includes Denial of Service (DoS) to prevent intruders or hackers continually trying to damage your network, Stateful Packet Inspection (SPI) to look at the contents of data packets entering the network to prevent viruses and content filtering to filter out unwanted information. The VPN Firewall Router will also provide real-time alerts and tracking of unwanted network activity.

Some organizations certify firewalls to the most recent profiles—ICSA is a widely accepted certification organization that verifies both protection against common attack profiles as well as optimized settings for firewalls. Many NETGEAR firewalls have attained ICSA certification.

Secure Corporate Communications using a VPN (Virtual Private Network)

Many businesses operate across multiple locations, either remote branches or home offices. Each remote location requires access to the corporate network and its resources, typically held at the Head Office. Virtual Private Networks (VPNs) enable businesses to use a public network, such as the Internet, as a secure link between defined locations. VPN Firewall Routers enable organizations to create Virtual Private Networks between the head office and remote locations and/or users.

VPN Firewall Routers

A VPN Firewall Router and associated remote located software will enable an organization needs to establish a Virtual Private Network. VPNs may exist between an individual computer (remote home worker) and the corporate LAN, or between two LANs, i.e. a head office and a branch office. VPNs include encryption, strong authentication of remote users or offices and mechanisms for hiding or masking information about the structure and design of the organizations' network from potential hacker attacks.

To illustrate, it would be equivalent to two people speaking in an unknown language in a public place that only they know how to speak. There are plenty of people that can hear you speaking (hackers), but they do not know what you are saying. Similarly, VPNs provide the unknown "language" that is decipherable between two parties, but no one else knows what is being said.

VPNs are traditionally used for:

- Intranets: Intranets connect an organization's locations. These locations range from the headquarters office, to branch offices, to a remote employee's home.
- Remote Access: Remote access enables telecommuters and mobile workers to access e-mail and business applications. A dial-up connection to an organization's modem pool is one method of access for remote workers, but is expensive because the organization must pay the associated long distance telephone and service costs. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communication link to the organization. VPN client software is available to provide end-to-end security. NETGEAR ProSafe VPN Client software enables remote connectivity for Microsoft Windows-based PCs and laptops.
- Extranets: Extranets are secure connections between two or more organizations. Common uses for extranets include supply-chain management, development partnerships, and subscription services. These undertakings can be difficult using legacy network technologies due to connection costs, time delays, and access availability. IPSec-based VPNs are ideal for extranet connections. IPSec-capable devices can be quickly and inexpensively installed on existing Internet connections.

Business-class Firewall Protection

Stateful Packet Inspection (SPI)
Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection "states." Using stateful packet inspection, an incoming packet is intercepted at the network layer, and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections.

All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through, or will be rejected.

For example:

- When the router with SPI notices pings over a certain time from the same address, the packets are dropped.
- SPI allows a router to know if the packet source address is inside a LAN. If an attack is launched from the WAN using an internal address, SPI routers compare packets to previous packets, and drop those violating the rules. A non-SPI router would slow overall traffic, as it would be unable to tell where to respond.

With SPI, the router looks at individual packets for patterns similar to known hacker techniques, such as Denial of Service (DoS) attacks, Ping of Death, SYN Flood, LAND Attack, and IP Spoofing. For example, Ping of Death attacks are avoided by dropping packets larger than the allowed IP size.

Network Address Translation (NAT)
NAT allows several networked computers to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). Only the single IP assigned to the router is visible from the Internet.

This has two benefits. First, all systems on a LAN can share a single (static or dynamic) IP address to access the Internet. And second, the network addresses of all systems on the LAN are hidden outside the LAN. Hiding the network addresses of systems in this way helps strengthen overall security.

Content Filtering and URL Blocking
Content filtering prevents objectionable content from reaching designated computers. The firewall controls access to Internet content by screening for keywords within Web addresses and blocking access to those sites. The firewall can be configured to log and report attempts to access objectionable Internet sites. Filtering can be set for particular times of day and days of the week. For example, you might not want sports Web sites accessed during business hours or school days.

Virtual Private Network (VPN) Client Software

Software can help businesses grow their network. For example, easy-to-use VPN client software can safely extend the LAN to telecommuters and mobile workforce. And. as more users are added, your business will need a more insight into your infrastructure to control and optimize network operation.

With VPN client software, telecommuters and mobile workers establish a private connection to their LAN over the Internet, using security technology conforming to the IPSec standard. IPSec secures and protects all communication and sensitive information available on corporate headquarter servers.

VPNs establish a secure, end-to-end IPSec session between a computer and a VPN gateway, typically located at the main office. The VPN client software on the PC or laptop authenticates the user on the network and protects the user's data from attack or eavesdropping. VPNs include encryption, strong authentication of remote users or hosts, and mechanisms for hiding or masking information about the private network topology from potential attackers on the public network.

Every company has a unique security configuration, and may use different encryption standards, authentication requirements, access controls, and so on. This may vary by employee—for example, the time of day someone may log on, or whether they need to use a smart card to authenticate as part of the logon process. The IPSec standard creates a rigorous framework for safe network computing, but VPN client software makes it easy to set up and configure a secure, remote session.

This includes:

- Key management: Facilitates online or manual enrollment, with either PKI or IKE. Some companies set up a private Certificate Authority (CA), while others may want to use trusted third-party CA's.
- Data encryption: IPSec supports AES, DES, and 3DES, which provide different levels of encryption. Note that more encryption is considered safer, but requires more CPU power to use.
- Security policy: Who can connect and what they can connect to are all determined by a company's security policy. VPN client software should enable the system administrator to enforce a company's security policy for remote connections.
- Logging: Keeping track of all remote connections is always a good idea. For example, if the same user is logged on at the same time from two different locations, perhaps the user has loaned out log-in information.

Quality VPN client software helps users with more than security. For example, NAT traversal enables small network users to work from home, where they may have a NAT gateway router. Reliability can be improved with redundant gateway and keep-alive capabilities. Designed to work with Virtual Private Network Consortium (VPNC) compliant devices such as routers, NETGEAR's standards-based ProSafe VPN client software makes it easy to safely connect to your company's network assets, works with all major operating systems, and supports Netgear ProSafe VPN Firewall and other IPSec-compliant VPN devices.