

## Common Network Terminology

### **Authentication Header (AH)**

Provides connectionless integrity and data origin authentication for IP data-grams and protection against replays.

### **Bandwidth**

The width of a band of electromagnetic frequencies. It is used to mean (1) how fast data flows on a given transmission path, and (2), the width of the range of frequencies that an electronic signal occupies on a given transmission medium.

### **Border Gateway Protocol (BGP)**

A robust and scalable path vector protocol that is used to span autonomous systems on the Internet. BGP-4 supports the CIDR (Classless Inter-Domain Routing) addressing scheme, which has increased the number of available IP addresses on the Internet.

### **Broadband**

High-speed Internet transmission using cable modems, DSL, or satellite.

### **Channel Service Unit (CSU)**

A device used to terminate a dedicated circuit at a company site.

### **Dedicated**

Permanent connection between machines over a special line provided by the local telephone company (such as T1).

### **Demilitarized Zone (DMZ)**

A computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

### **Dial-up**

Temporary connection between machines over a standard telephone line.

### **Digital Service Unit (DSU)**

Data side of a CSU/DSU.

### **Digital Subscriber Line (DSL)**

Technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. A DSL line can carry both data and voice signals, and the data part of the line is continuously connected.

### **Domain Name Server (DNS)**

A distributed name and address mechanism used on the Internet to map an IP address to a host name, and vice versa.

### **Dynamic Host Configuration Protocol (DHCP)**

Allows TCP/IP connected devices to automatically obtain the IP address assignment and network configuration parameters they require to participate in LAN and WAN communications.

### **Dynamic Packet Filtering**

Adapts to traffic by learning which ports are needed for a session, and closes all others. When a legitimate session is initiated, the firewall monitors the requests to open ports between the terminating points and opens only those. When the session ends, the firewall immediately closes the ports. No security holes are left on the firewall for hackers to enter. It performs highly sophisticated filtering algorithms and detects even the most obscure methods of unauthorized entry.

### **Encapsulated Security Payload (ESP)**

Provides confidentiality (encryption), data origin authentication, connectionless integrity, an anti-replay service, and limited traffic flow confidentiality. ESP provides both encryption and/or authentication.

### **Encryption Algorithm**

A mathematical formula for data encryption. It uses a block cipher with a 128-bit key, and is generally considered to be very secure.

### **Ethernet**

Local Area Network standard technology used to transmit information between computers.

### **Extranet**

An extranet is a private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.

### **File Sharing**

Shared folder can be used to save and access files and other data to the WolfPac platform from computers connected to your protected LAN. File sharing allows a number of people to use the same file by some combination of being able to read or view it, write to or modify it, copy it, or print it. Typically, a file sharing system has one or more administrators. Users may all have the same or may have different levels of access privilege.

### **File Transfer Protocol (FTP)**

A TCP/IP protocol that allows a user on one system to transfer files or access information on another system over a network.

### **Firewall**

Network security system that prevents unauthorized users from accessing information on the protected LAN.

# Glossary



## Common Network Terminology

### Frame Relay

Fast type of packet switching network that uses smaller packet sizes and less error checking for WAN connections.

### Gateway

A device such as a server or router that connects two or more networks together. For example, a protected LAN to the Internet.

### Generic Routing Encapsulation (GRE)

A method for encapsulating and routing a payload packet. The resulting GRE packet can then be encapsulated in some other delivery protocol and then forwarded to its destination.

### Hypertext Transfer Protocol (HTTP)

Application-level protocol for distributed, collaborative, hypermedia information systems. It is the protocol of the World Wide Web (www).

### Integrated Services Digital Network (ISDN)

A type of digital transmission over standard telephone lines.

### Internet Control Message Protocol (ICMP)

A protocol that manages control and error messages at the IP layer.

### Internet Key Exchange (IKE)

A method for establishing a security association (SA) that authenticates users, negotiates the encryption method, and exchanges the secret key. IKE is used in the IPsec protocol.

### Internet Message Access Protocol (IMAP)

Allows a client e-mail program to access both new and opened/saved messages as if they were local.

### IP Address

Internet Protocol Address. Network layer for TCP/IP. IP addresses are 32 bits long, and consist of two parts: a network portion and a host portion. The host portion is further divided into a subnet and host address. Subnets are used for routing within an organization.

### IPsec(urity)

Designed to provide high quality security for IPv4, the current version of IP (Internet Protocol). The set of security services offered includes access control, connectionless integrity, data origin authentication, encryption, protection against replays, and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

### Local Area Network (LAN)

Local Area Network. Group of interconnected machines (PC's or workstations) that share a common server.

### Media Access Control (MAC) Address

A unique hexadecimal address assigned to every Ethernet card.

### Netmask

A string of 0's and 1's that mask or screen out the network part of an Internet Protocol (Internet Protocol) IP address so that only the host computer part of the address remains.

### Network Address Translation (NAT)

Technology used to make a network invisible to outside Internet users by hiding the protected LAN's IP addresses.

### Network Basic Input/Output System (NetBios)

A program that allows applications on different computers to communicate within a local area network.

### Open Shortest Path First (OSPF)

A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.

### Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

### Packet Filters

Verify that all incoming data packets coming from the Internet have been requested by an authorized user on a protected LAN.

### Ping

Packet Internet Gopher. A utility used to determine whether a specific IP address is accessible.

### Plain Old Telephone Service (POTS)

Standard telephone system.

### Point-to-Point Protocol (PPP)

Type of network configuration that connects only two terminals.

### Point-to-Point Tunneling Protocol (PPTP)

A set of communication rules that allows companies to extend their own corporate network through private "tunnels" over the public Internet.

# Glossary



## Common Network Terminology

### Post Office Protocol (POP)

Allows user authentication and mailbox manipulation, with a password transmitted as clear text serving as the method of authentication.

### Proxy

Process in which one system answers protocol requests on behalf of another system.

### Proxy Applications

Provide a service by issuing commands on behalf of clients on the protected LAN to the Internet.

### Proxy Server

Prevents unauthorized Internet access to the protected LAN.

### Router

Device that connects a network (or networks) together. A router's purpose is to determine which packets of data go to what machines.

### Routing Information Protocol (RIP)

A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers and is known for wasting bandwidth. It also has a limit of 15 hops.

### Secure Socket Layer (SSL)

SSL is widely used to securely send credit card and other sensitive data to a vendor's web site. When an SSL session is initiated, the web server sends a digital certificate to the browser for authenticating the web site. The browser maintains an inventory of the certificates of public certificate authorities (CA) and contacts the CA to see if the certificate has been revoked.

### Server Message Block (SMB)

A protocol that provides a method for client applications in a computer to read and write to files on and to request services from server programs in a computer.

### Simple Mail Transfer Protocol (SMTP)

Standard host-to-host mail transport protocol on the Internet.

### Stateful Packet Filters

Verify that all incoming data packets coming from the Internet have been requested by an authorized user on the protected LAN.

### T1

Digital carrier facility used for transmitting a stream of DS1 data over standard telephone wires at 1.544 Mb/sec. Telco Abbreviation for the local telephone company.

### Telnet

Provides terminal access to a machine utilizing a user command and an underlying TCP/IP protocol for access.

### Transmission Control Protocol over Internet Protocol (TCP/IP)

Suite of protocols (transport or application) protocols that run over IP.

### User Datagram Protocol (UDP)

Standard transport protocol that does not ensure delivery or acknowledgment of delivery.

### Voice over IP

The two-way transmission of voice over a packet-switched TCP/IP network.

### Virtual Private Networking (VPN)

VPN allows a company to securely send data from a computer at one office to another computer at a different office, using the Internet.

### Virtual Router Redundancy (VRRP)

Designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first hop router by end-hosts.

### Web Access Control

Allows the administrator to specify which users on a protected LAN can access the web.

### Web Caching

All web pages visited by a user are stored and are available locally the next time they are requested reducing the amount of bandwidth used across the Internet.

### Wide Area Network (WAN)

Wide Area NetWork. Type of network that encompasses a large geographical area.