Virtual Private Network

A VPN is a service that offers secure, reliable connectivity over a shared, public network, infrastructure such as the Internet. It is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables the sending of data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.
To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public transit internetwork to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality.

The portion of the connection in which the private data is encapsulated is known as the tunnel. The portion of the connection in which the private data is encrypted is known as the virtual private network (VPN) connection.
Types of VPN

Remote Access Over the Internet
VPNs provide remote access to organization resources over the public Internet, while maintaining privacy of information. Using the connection to the local ISP, the VPN client creates a VPN connection between the remote access computer and the organization VPN server across the Internet.
Intranet VPN or Site to Site VPN. A private communication channel within an enterprise or organization that may or may not involve traffic traversing a WAN. 

Extranet VPN. A private communication channel between two or more separate entities that may involve data traversing the Internet or some other WAN.
Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network.

The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The logical path through which the encapsulated packets travel through the internetwork is called a **tunnel**. There are different protocols use in providing this tunnels and they include

- **Point-to-Point Tunneling Protocol (PPTP)**. PPTP allows multiprotocol traffic to be encrypted and then encapsulated in an IP header to be sent across an organization IP internetwork or a public IP internetwork such as the Internet.

- **Layer Two Tunneling Protocol (L2TP)**. L2TP allows multiprotocol traffic to be encrypted and then sent over any medium that supports point-to-point datagram delivery, such as IP, X.25, Frame Relay, or ATM.

- **IPSec tunnel mode**. IPSec tunnel mode allows IP packets to be encrypted and then encapsulated in an IP header to be sent across an organization IP internetwork or a public IP internetwork such as the Internet.
IPSec

IPSec is a set of security protocols and algorithms used to secure data at the network layer. It is the most commonly used protocol for tunneling. IPSec enables the following security appliance VPN features:

**Data confidentiality:** The IPSec sender can encrypt packets before transmitting them across a network.

**Data integrity:** The IPSec receiver can authenticate IPSec peers and packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

**Data origin authentication:** The IPSec receiver can authenticate the source of the IPSec packets that are sent. This service is dependent upon the data integrity service.

**Anti-replay:** The IPSec receiver can detect and reject replayed packets, helping to prevent spoofing and man-in-the-middle attacks.
IPSec consists of the following two main protocols:

- **Authentication Header (AH):** A security protocol that provides authentication and optional replay-detection services. AH acts as a “digital signature” to ensure that tampering has not occurred with the data in the IP packet. AH does not provide data encryption and decryption services. AH is not supported on your security appliance.

- **Encapsulating Security Payload (ESP):** A security protocol that provides data confidentiality and protection with optional authentication and replay-detection services. The security appliance uses ESP to encrypt the data payload of IP packets.

**Internet Key Exchange**
IKE is a hybrid protocol that provides utility services for IPSec: authentication of the IPSec peers, negotiation of IKE and IPSec security associations (SAs), and establishment of keys for encryption algorithms used by IPSec. IKE is synonymous with Internet Security Association and Key Management Protocol (ISAKMP) in security appliance configuration. It uses the following protocols and Algorithms
**Data Encryption Standard**
DES is used to encrypt and decrypt packet data. DES is used by both IPSec and IKE. DES uses a 56-bit key, ensuring high-performance encryption.

**Triple Data Encryption Standard**
3DES is a variant of DES that iterates three times with three separate keys, effectively doubling the strength of DES. 3DES is used by IPSec to encrypt and decrypt data traffic. 3DES uses a 168-bit key, ensuring strong encryption.

**Advanced Encryption Standard**
The National Institute of Standards and Technology (NIST) recently adopted the new AES to replace DES encryption in cryptographic devices. AES provides stronger security than DES and is computationally more efficient than 3DES. AES offers three different key strengths: 128-, 192-, and 256-bit keys.

**Diffie-Hellman**
DH is a public-key cryptography protocol. It enables two parties to establish a shared secret key over an insecure communications channel. DH is used within IKE to establish session keys.

**Message Digest 5**
MD5 is a hash algorithm used to authenticate packet data. The security appliance uses the MD5 Hash-based Message Authentication Code (HMAC) variant, which provides an additional level of hashing. A hash is a one-way encryption algorithm that takes an input message of arbitrary length and produces a fixed-length output message. IKE and ESP use MD5 for authentication.

**Secure Hash Algorithm-1**
SHA is a hash algorithm used to authenticate packet data. The security appliance uses the SHA-1 HMAC variant, which provides an additional level of hashing. IKE and ESP use SHA-1 for authentication.