Virtual Private Networks

Applied Cryptography

Virtual Private Network

- Provides a method of extending access to one or more internal hosts or networks, using a public network
- Enables the use of fire-walled internal services (e.g. DNS, web, file sharing, authentication) without having to configure the firewall to provide access to each service
- Enables the use of LAN protocols securely with remote clients using encryption to prevent eavesdropping and detect tampering
- Can be used by bad actors to exfiltrate data and bypass firewall restrictions

VPN Implementations

- Various protocols for VPNs have been defined
- IPsec IETF RFC 6434, designed for and with IPv6 but works with IPv4 with some problems, provides security at the transport level, requires routable IPs
- SSL/TLS VPNs (e.g. OpenVPN, SoftEther VPN), simplified universal offshoot of IPSEC that uses TLS
- DTLS (e.g. Cisco AnyConnect VPN, OpenConnect VPN), similar to TLS but run over UDP and designed for streaming
- MPPE/PPTP (e.g. Windows feature), Microsoft product, old, vulnerable, replaced by L2TP
- SSH (e.g. OpenSSH tunnels), alternative to OpenVPN/OpenConnect VPN that doesn't require root but is worse than other solutions in every other way
- Wireguard, proposed replacement for all other VPNs, it's great, it's amazing, it's fairly new, it ignores all the hard stuff so you have to solve those things outside of wireguard

IPSec Overview

https://en.wikipedia.org/wiki/Wolpertinger

- IPSec evolved in the 1990s as one result of several competing research efforts by multiple US government agencies as well as private companies
- IPSec was developed alongside IPv6, which it is intended to secure although it also works with IPv4, mostly
- Trusted Information Systems (TIS) produced the first commercial IPSec VPN product around 1994 (the Gauntlet Firewall)
- IPSec is connectionless and operates at layer 3 of TCP/IP, the transport layer
- IPSec can be used to encrypt some or all of the traffic between two co-operating devices
- IPSec can be used in a transport mode or in a tunnel mode transported using ordinary UDP packets on port 500 or 4500 to solve NAT traversal problems
- IPSec can use AH and ESP protocols to protect packet contents

IPSEC

- IP Security Architecture

ESP

- Encapsulation Security Payload

AH

- Authentication Header

NAT

- Network Address Translation

IPSec Connection Management

- ISAKMP protocol provides a framework for establishing security associations between endpoints
- It is key exchange protocol independent, so multiple key exchange protocols may be used within the ISAKMP framework
- IKE, IKEv2 and KINK are key exchange protocols that are used within ISAKMP to exchange security information when establishing connections, such as identity exchange, algorithm selection, key generation and exchange, and selection of security options for connections
- Completed connections result in the creation of security associations, or SAs which are stored in a database at each end of the connection called the SADB, and only an index (the SPI) into the database is transmitted with each packet once the session is established
- AH and ESP protocols are used to carry the application communications once SAs are in place - in AH and ESP protocols, authentication means unaltered packet content

ISAKMP

- Internet Security Association and Key Management Protocol

SA

- Security Association
- A simplex logical communications path

IKE,IKEv2

- Internet Key Exchange

KINK

- Kerberized Internet Negotiation of Keys

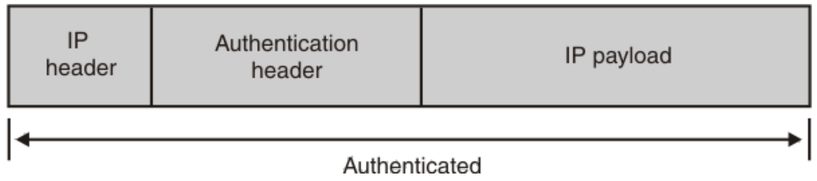
SPI

- Security Parameter Index

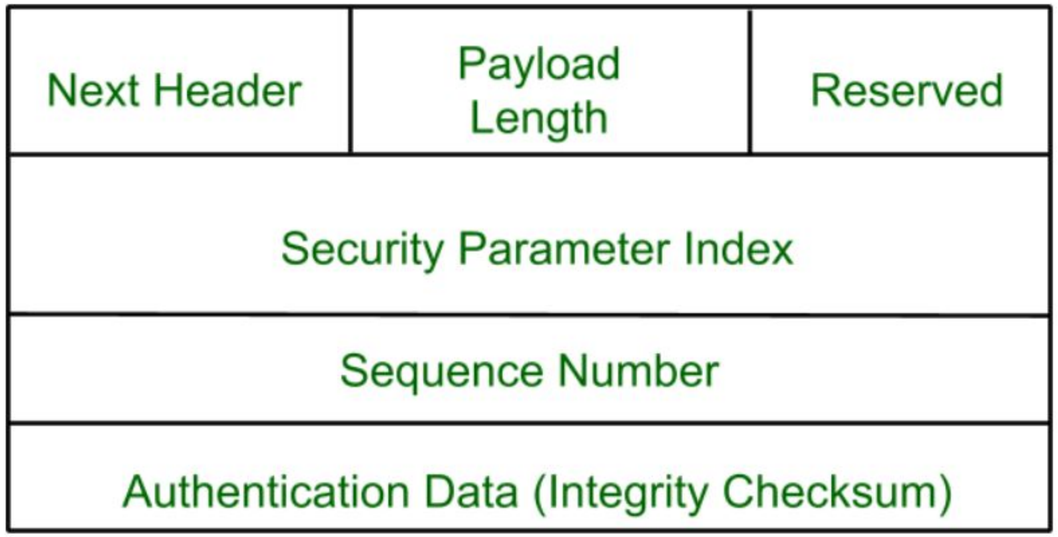
SADB

- Security Association Database

IPSec
Authentication Header



https://www.ibm.com/docs/en/zos/2.2.0?topic=encapsulation-transport-mode-tunnel-mode

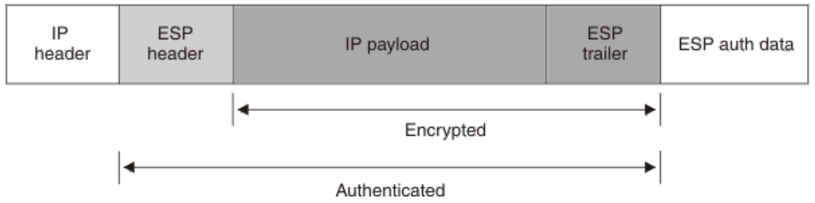


https://www.geeksforgeeks.org/ipsec-architecture/?ref=rp

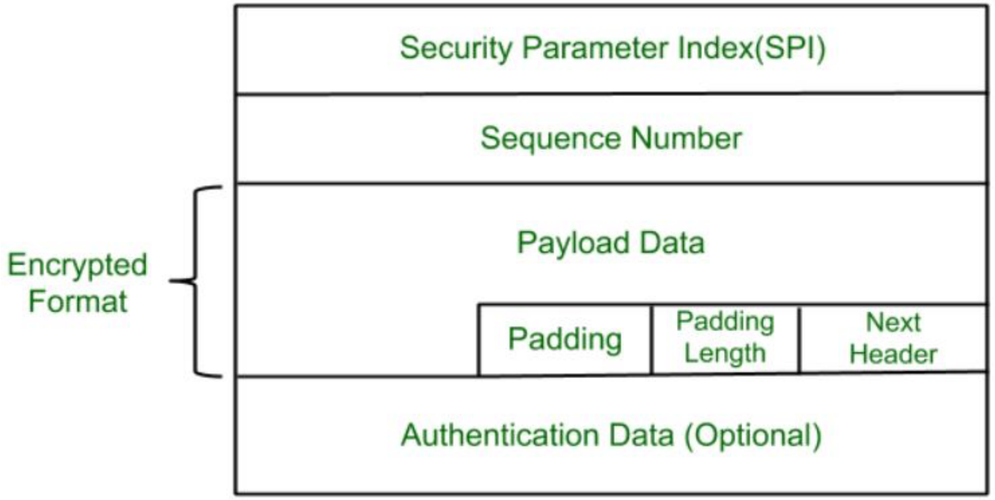
- AH packets provide protection (a keyed hash) for IP packets when IPSec is used in transport mode
- AH use is negotiated as part of ISAKMP
- AH does not protect parts of the IP header which may be reasonably expected to change, such as the TTL
- AH cannot be used if NAT is involved, because the hash-protected packet content includes the IP address information

IPSec

Encapsulation Security Payload



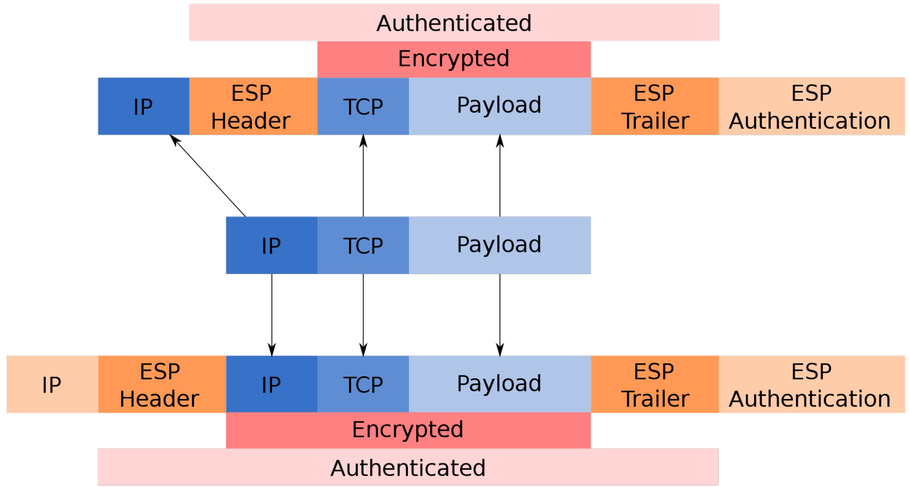
https://www.ibm.com/docs/en/zos/2.2.0?topic=encapsulation-transport-mode-tunnel-mode



https://www.geeksforgeeks.org/ipsec-architecture/?ref=rp

- ESP protocol packets provide optional authentication (via HMAC), data integrity, confidentiality for the original packet
- ESP supports authentication-only and encryption-only but encryption without authentication is strongly discouraged
- ESP does not protect the transport IP header in tunnel mode

IPSec
Transport vs. Tunnel Mode



ESP Transport Mode

ESP Tunnel Mode

https://en.wikipedia.org/wiki/IPsec

- When IPSec is used between hosts, the Encapsulated Security Payload (ESP) protocol encapsulates the application data and transport header and both parties must be able to directly connect to each other without NAT or any other kind of proxying between the hosts
- When IPSec is used between a gateway and either a host or another gateway, the ESP packet also encapsulates the original application IP control info and places the entire packet inside a UDP packet for transport allowing IPSec to be carried across NAT
- Tunnel mode is the one we usually mean when we discuss IPSec VPNs

IPSec Issues

- Comparatively complex system
- Closed source commercial applications are prevalent
- Many of the features of IPSec are optional, and leaks are possible in a session if not configured properly (when it doesn't break things to configure them poorly, they just leak)
- Questions about NSA interference and concerted efforts to quietly break IPSec
- Corruption due to fragmentation which leads to interesting problems during IKE
- Most of IPSec's issues are ameliorated by using tunnel mode or are expected to go away like magic when IPv6 is the only kind of addressing used

TLS/SSL VPNs

- Similar to the tunnel mode of IPSec, TLS VPNs create a virtual network connection by proxying network traffic on and off of an application layer tunnel
- There are different kinds and implementations of TLS tunnel based VPNs
- PKI is commonly used for authentication with a pre-shared key usually added to increase security of the connection establishment
- Since the tunnels are built at the application layer, the applications providing the connections and proxying can implement security mechanisms as appropriate including MFA

VPN Certificate Authorities

- Certificates are commonly used to authenticate TLS-based VPN servers and clients to each other using 2-way TLS authentication
- Internet PKI certificates and a real CA can be used as long as the client and server both use the same CA, but additional authentication factors (e.g. tls-auth, login/password) should be used
- A private CA can be generated and used by the server to sign certificates, servers and clients signed by that CA can trust each other, this is the preferred method
- The CA does not have to be installed on the same machine that provides VPN service, but the CA's certificate must be present on the VPN server

OpenVPN

- OpenVPN is an example of a TLS-based VPN solution
- Commercial and community versions are available and the community version is under GPL
- Certificate and key based, can also use a pre-shared private key for connection establishment and/or login/password MFA trivially
- Client software available for all popular platforms
- Server version available for many platforms, also available as a commercial VM VHD and in commercial cloud-aware configurations from openvpn.net
- Server and client do not have to be using the same operating system

DTLS

- DTLS is basically TLS using UDP instead of TCP
- Responsibility for packet reordering and loss is in the application instead of the network stack
- Higher transmission speeds and loss tolerance are its main goals
- Primarily used for secure streaming service (e.g. in conjunction with RTP to create SRTP)
- Vulnerable when used with CBC encryption modes, they are not to be used with DTLS

PPTP

- An insecure and obsolete VPN technology from 1999 commonly deployed on Windows
- Uses non-standard GRE packet formats to create a tunnel to encapsulate PPP
- PPTP provides no significant authentication or encryption
- PPTP expects the encapsulated protocol to protect itself
- PPP can do PAP, CHAP, MS-CHAP v1/v2 for client authentication and is what is usually run through the GRE tunnel
- PPTP connections are initiated on TCP port 1723 which is used to set up and manage the GRE tunnel
- Just Don't Do It

L2TP

- L2TP is a tunnelling protocol that operates virtually at layer 2 of the TCP/IP stack, the IP layer
- L2TP is carried inside UDP packets, with the server end known as the LNS (L2TP Network Server) and the client end known as the LAC (L2TP Access Concentrator)
- Like PPTP, L2TP provides no significant authentication or encryption features
- Like PPTP, PPP is most commonly used over L2TP
- IPSec can also be used with L2TP, known as running L2TP/IPSec (interestingly, L2TP gets run over IPSec)
- Multiple virtual networks can be carried over a single L2TP tunnel

SSH

- OpenSSH has built-in VPN tunnelling support, not to be confused with channels for application proxying
- It requires openSSH at both ends of the connection
- It is not enabled by default and is straightforward but not trivial to set up
- PPP can be run over an SSH channel
  - Set up an SSH proxy forwarder
  - Run pppd on the server end
  - Connect with a PPP client over the forwarder

Wireguard

- Wireguard is a fairly new UDP-based protocol and application for VPNs
- It was created to be easier to set up and maintain than either IPSec or OpenVPN
- It is multi-platform and free open source software
- 1/100th of the code that is found in IPSec, and does not carry around a metric ton of legacy capabilities (e.g. only supports Curve25519 key exchange and ChaCha20 encryption)
- Wireguard has similar connection establishment protections to OpenVPN
- It is still very new in the crypto world, and is trying very hard to steal OpenVPN's lunch