BACHELOR OF COMPUTER SCIENCE

Network Security

Virtual Private Networks

Kenneth Thilakarathna

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

Lesson Plan

- Requirement of remote access and private communication
- Private Communication (Virtual Private Network (VPN)) technologies and evolution
- VPN vs Secure VPN
- Details of a Secure VPN protocol - IPSec
- IPSec vs SSL-VPN
- Pros and Cons of Secure VPNs
- Summary of the lesson

Enterprise requirements for private communication

- **Remote access**
  Accessing organizations resources remotely and most of the time the access is ubiquitous.
- **Site-to-Site access**
  - **Intranet based**
    Connecting several branches of the same organization : E.g. Head office of a bank with its branches
  - **Extranet based**
    Connecting between two different organizations : E.g. Bank give access to the software development company

Private communication

Problem: Need to have a private communication link between two organizations or branches of the same organization.

Dedicated network link owned and maintained by you

- Not scalable
- Expensive investment
- Not flexible for remote connectivity only for short range site-to-site connectivity
- You are on your own (no maintenance or support otherwise)
- Upgrade cost would be very high

Leased Lines (dedicated communication link leased by you)

- Expensive still
- Not scalable beyond the service provider
- Not flexible for remote connectivity only for site-to-site connectivity
- Connecting two end points per leased line

What is a Virtual Private Network (VPN)?

Virtual Private Network can be described as a logical communication link that carries private traffic over public network.

In an VPN:

- Access to communication should only be for the defined users
- Communication should be private and not necessarily be encrypted: e.g. MPLS
- Communication should be abstracted from physical substrate (Virtual) i.e. does not change when physical layer technology changes.

Practical VPN applications

- Ubiquitous access to the cooperate resources : e.g. Working while traveling.
- Need of accessing private cooperate services from remote locations: e.g. Cooperate financial system
- Controlled/Private Access needed from many locations by different parties : e.g. software vendor accessing from their site
- Long distance where leased lines are not feasible : e.g. international employees / clients
- Infrastructure requirements such as extended LANs (PROD to DR) : e.g. Oracle DB deployments

VPN implementations

- MPLS - Multi-protocol Label Switching (no security)
- GRE Tunnels - Generic Routing Encapsulation (no security)
- PPTP - Point-to-Point Tunnelling Protocol (secure but considered vulnerable now)
  Use GRE for encapsulation
- L2TP - Layer 2 Tunnelling Protocol (no security)
  Use GRE for encapsulation and no security unless IPSec is incorporated
- IPSecurity (secure and de facto protocol for secure VPN implementations)
  We will be discussing in detail
- TLS (SSL VPN) - Transport Layer Security VPNs (secure)

What is a tunnel?

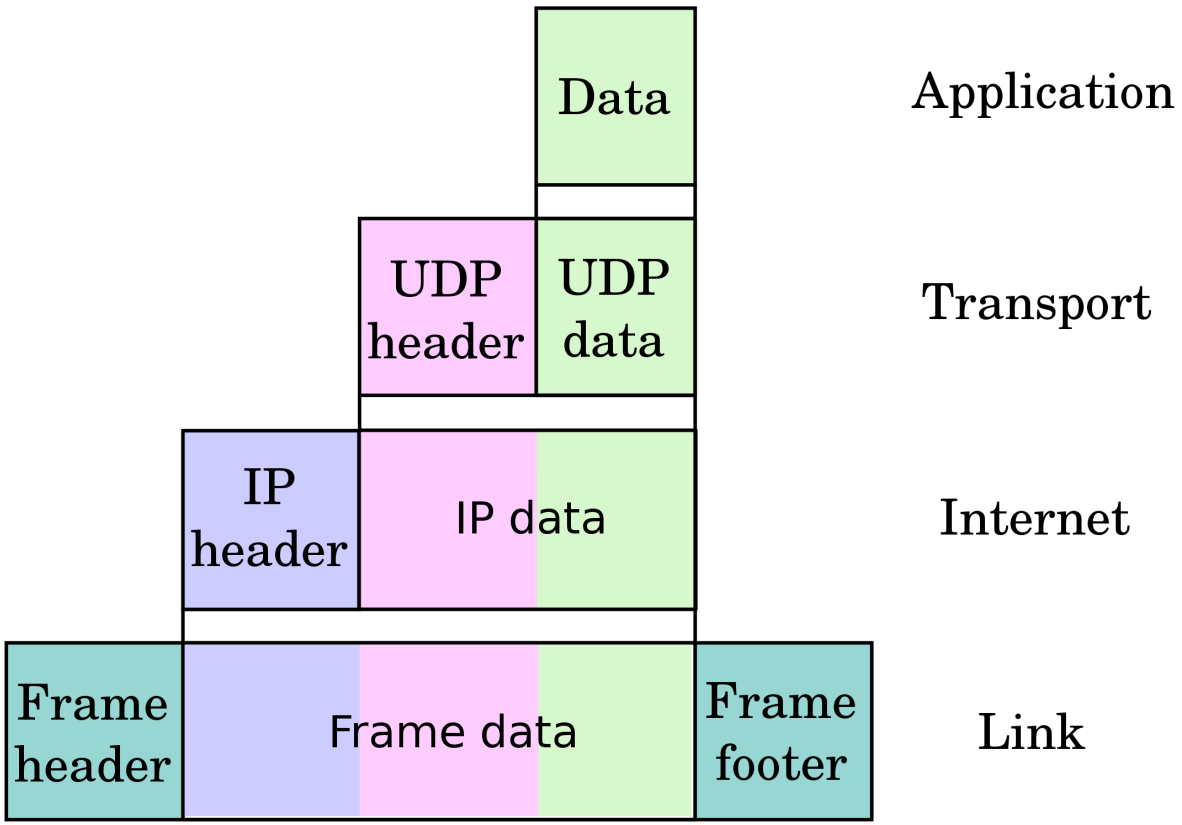
- A tunnel is a virtual path across a network that delivers packets.
- Tunnel can be created using encapsulation or encryption

Tunnelling through encapsulation

- A packet based on one protocol is wrapped, or encapsulated, in a second packet based on a different protocol (tunnelling protocol)

What is encapsulation?

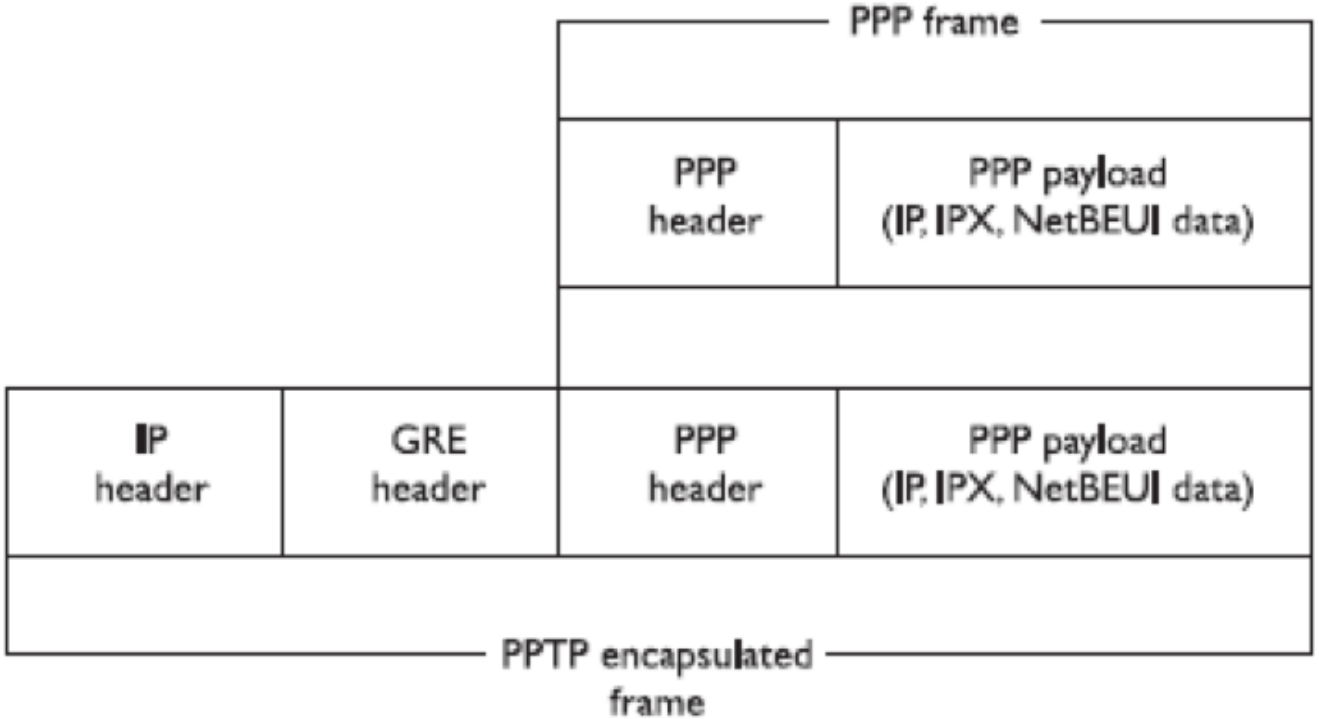
Encapsulation



src: *wikipedia.org*

PPTP use GRE Tunnelling

Example for tunnelling through encapsulation



Back to VPN implementations

Multi-protocol Label Switching - MPLS

- Not secure
- Use a labelling mechanism to isolate the network from other networks
- Can be implemented as a full mesh (not limited as leased lines)
- Within the service provider network and difficult to find service providers with global partnerships

VPN implementations

GRE Tunnels

- Not secure
- Use encapsulation to isolate the network from other networks
- Point-to-Point connectivity
- Cab be used to forward multicast traffic where other VPN protocols does not support

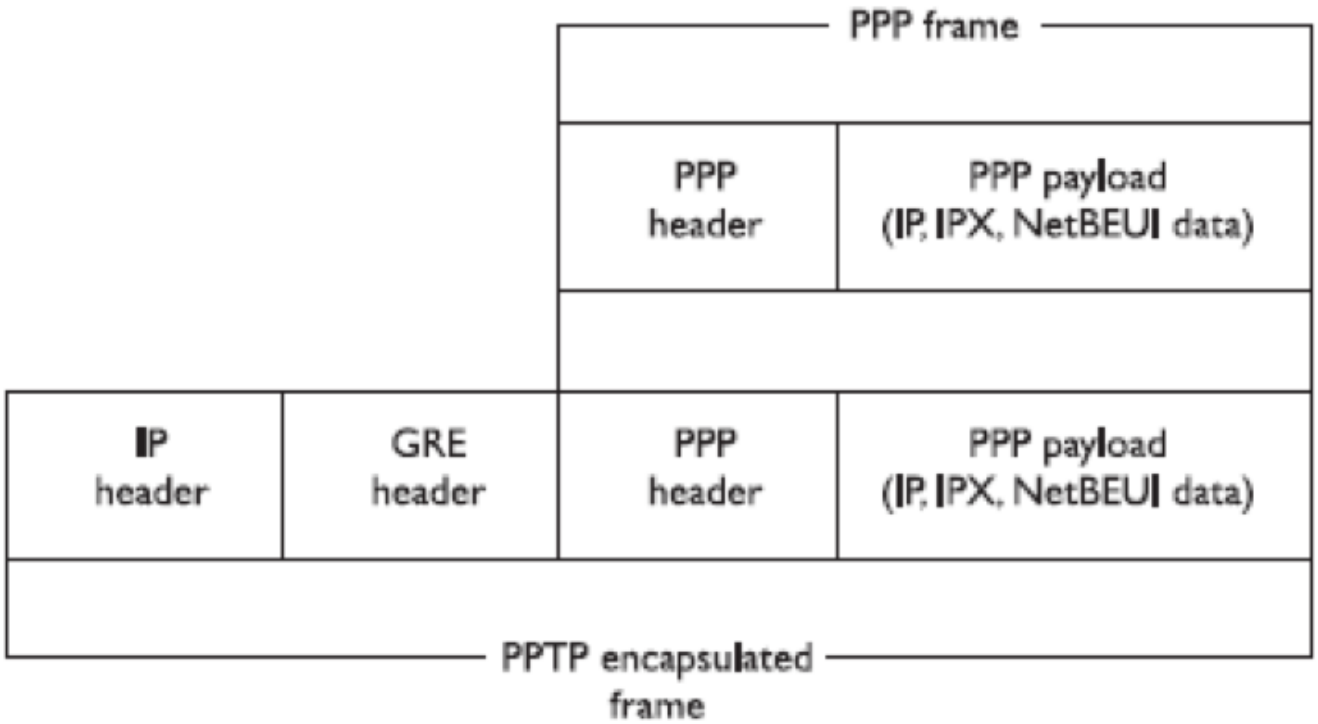
VPN implementations

Pont-to-Point Tunnelling Protocol

- Introduced by Microsoft way back and there were few versions
- Supported by many Operating Systems : Microsoft Windows, Mac OS, GNU/Linux
- Authentication is done using MS-CHAP
- Keys to encrypt payload is communicated during the authentication process
- Secure but considered vulnerable
- Use GRE for encapsulation and encryption vary by the implementation
- Point-to-Point connectivity
- Works only on IP networks
- A data link layer protocol

VPN implementations

Pont-to-Point Tunnelling Protocol



VPN implementations

Layer 2 Tunnelling Protocol

- L2TP provides the functionality of PPTP, but it can work over networks other than just IP
- L2TP does not provide any encryption or authentication services
- Need to combined with IPSec if encryption and authentication services are required
- The processes that L2TP uses for encapsulation are similar to those used by PPTP
- Point-to-Point connectivity
- A data link layer protocol

Secure VPN

Secure VPNs give you confidentiality, integrity and authentication for your communication.
Example protocols

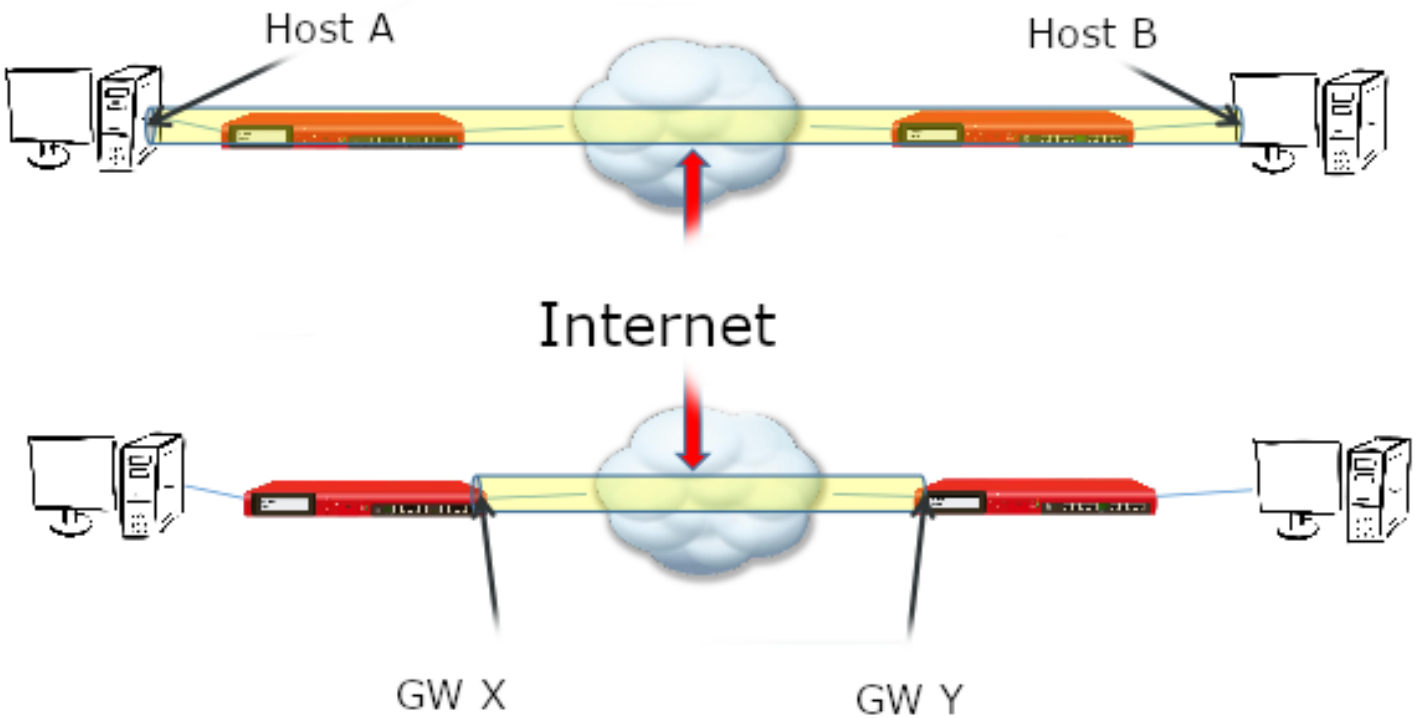
- PPTP
- IP Security
- SSL/TLS VPN
- SSH Tunnels

IPSec VPNs

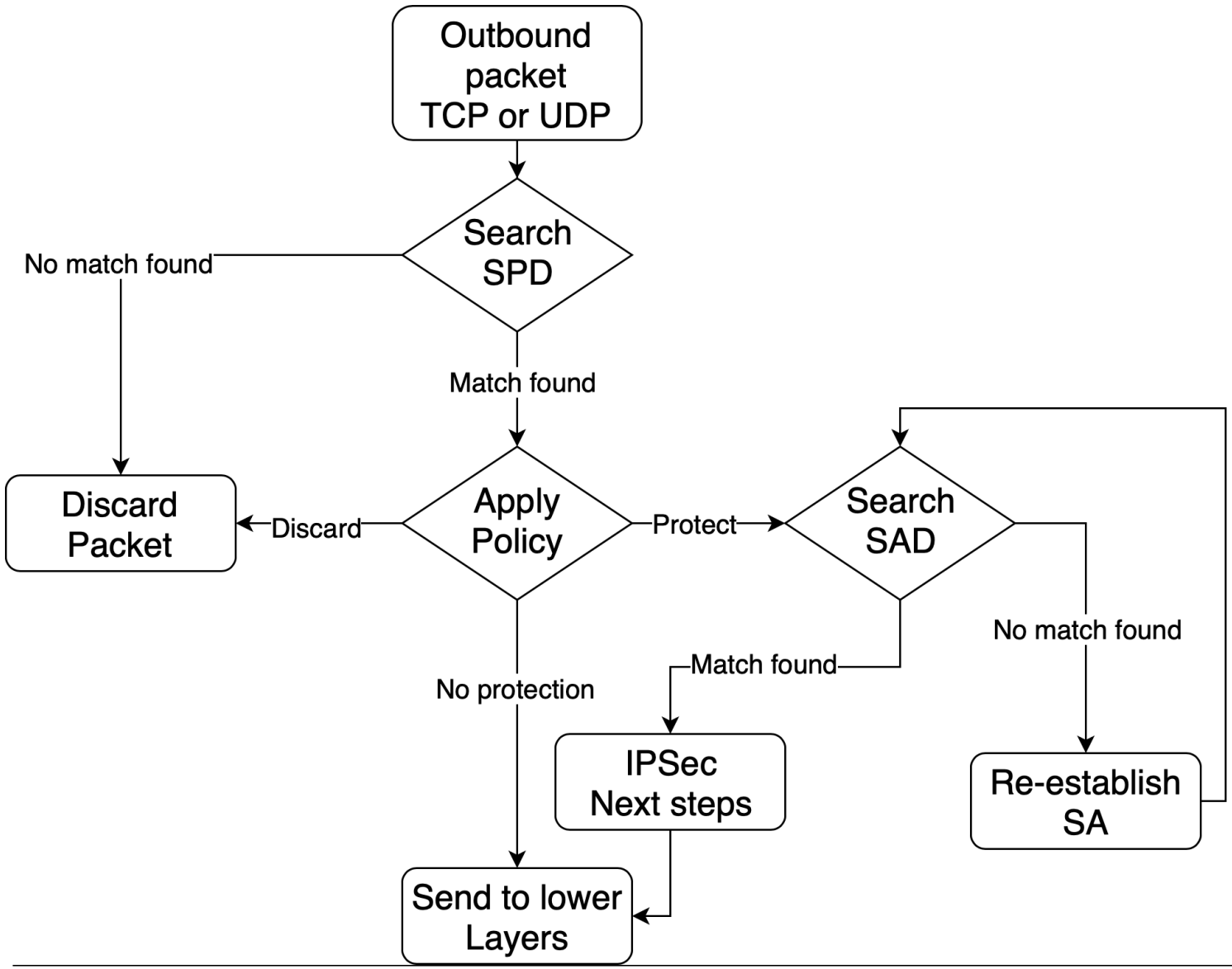
IP Security can be configured in multiple communication types.

- Host to Host
- Site to Site
- Host to Site

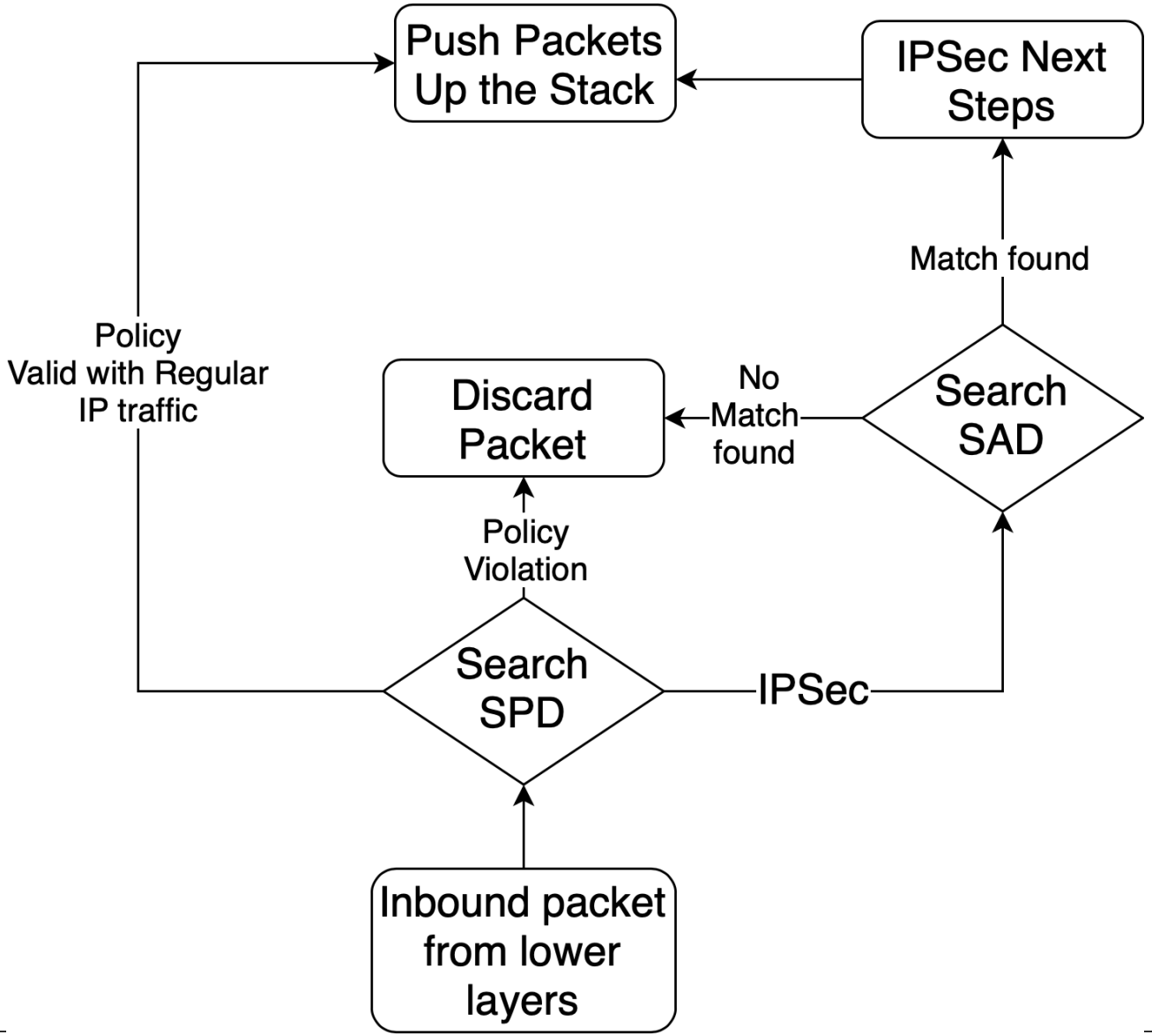
Host to Host vs Site to Site



IPSec - Flow of outbound packet



IPSec - Flow of inbound packet



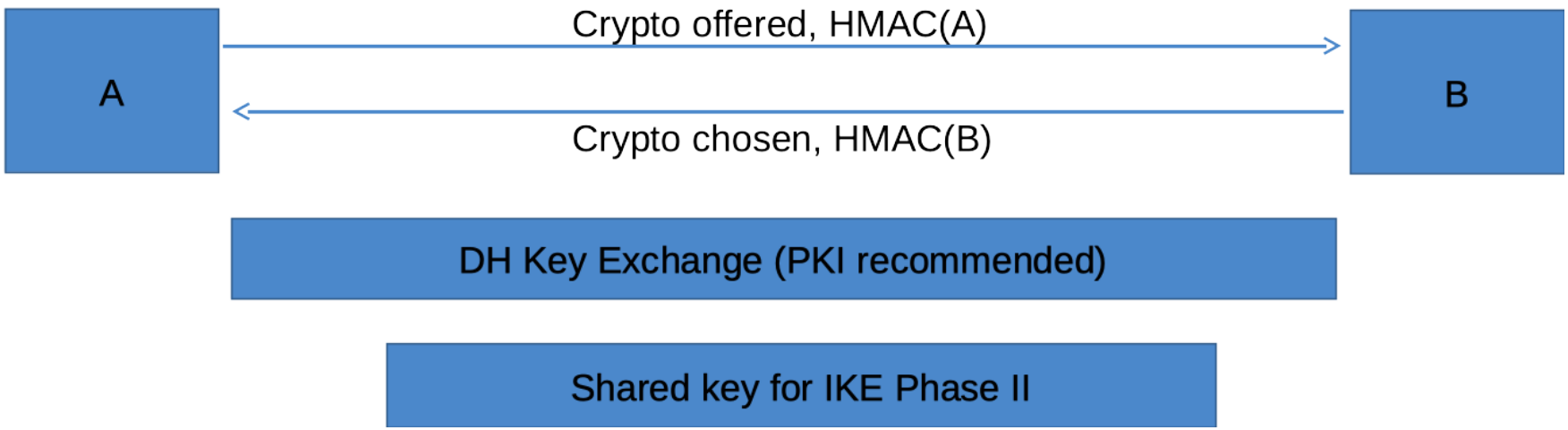
IPSec components

- IKE P I – ISAKMP SA - Bidirectional
- IKE P II - IPSec SA - Unidirectional

Internet Key Exchange - IKE Phase I

- Peers are authenticated either by a pre shared key or PKI certificates
- Diffie-Hellman protocol is used to create a common symmetric key which is known only to the peers
- ISAKMP SA (Internet Security Association Key Management), an agreement on keys, and algorithms for IKE phase II is the outcome of IKE phase I
- ISAKMP SA is valid for a certain period of time. On expiry, IKE phase I should be done again.
- IKE phase I is processor intensive than IKE phase II.

IKE Phase I - summary



Note that there are more technical stuff going which is not illustrated here.

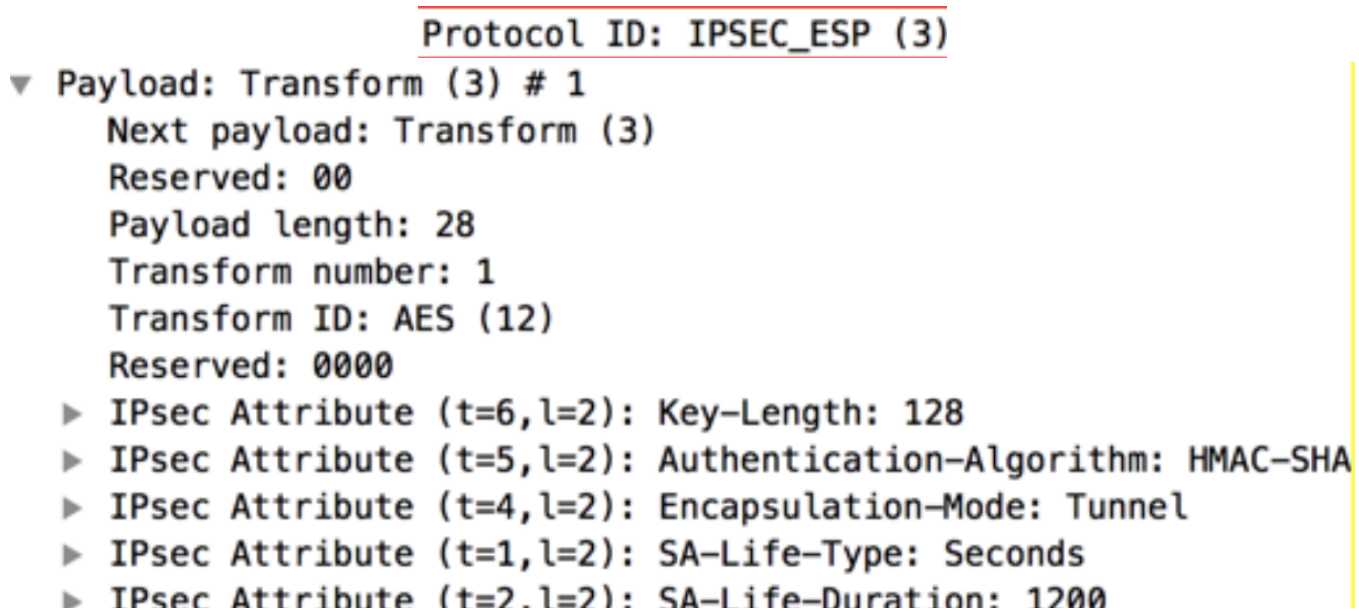
IKE Phase I - proposal

```
▶ IKE Attribute (t=1,l=2): Encryption-Algorithm: AES-CBC
▶ IKE Attribute (t=14,l=2): Key-Length: 128
▶ IKE Attribute (t=2,l=2): Hash-Algorithm: SHA
▶ IKE Attribute (t=4,l=2): Group-Description: 2048 bit MODP group
▶ IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key
▶ IKE Attribute (t=11,l=2): Life-Type: Seconds
▶ IKE Attribute (t=12,l=2): Life-Duration: 3600
```

IKE Phase II

- Use keys and algorithms agreed at IKE phase I
- Communicate information to generate Symmetrical IPSec keys through a secure channel using ISAKMP SA.
- IPSec Security Association is the outcome of IKE phase II.
- Decides which IPSec protocol to use - AH protocol or ESP protocol
- IPSec SA will expire in a shorter time than IKE SA.

IKE Phase II - association



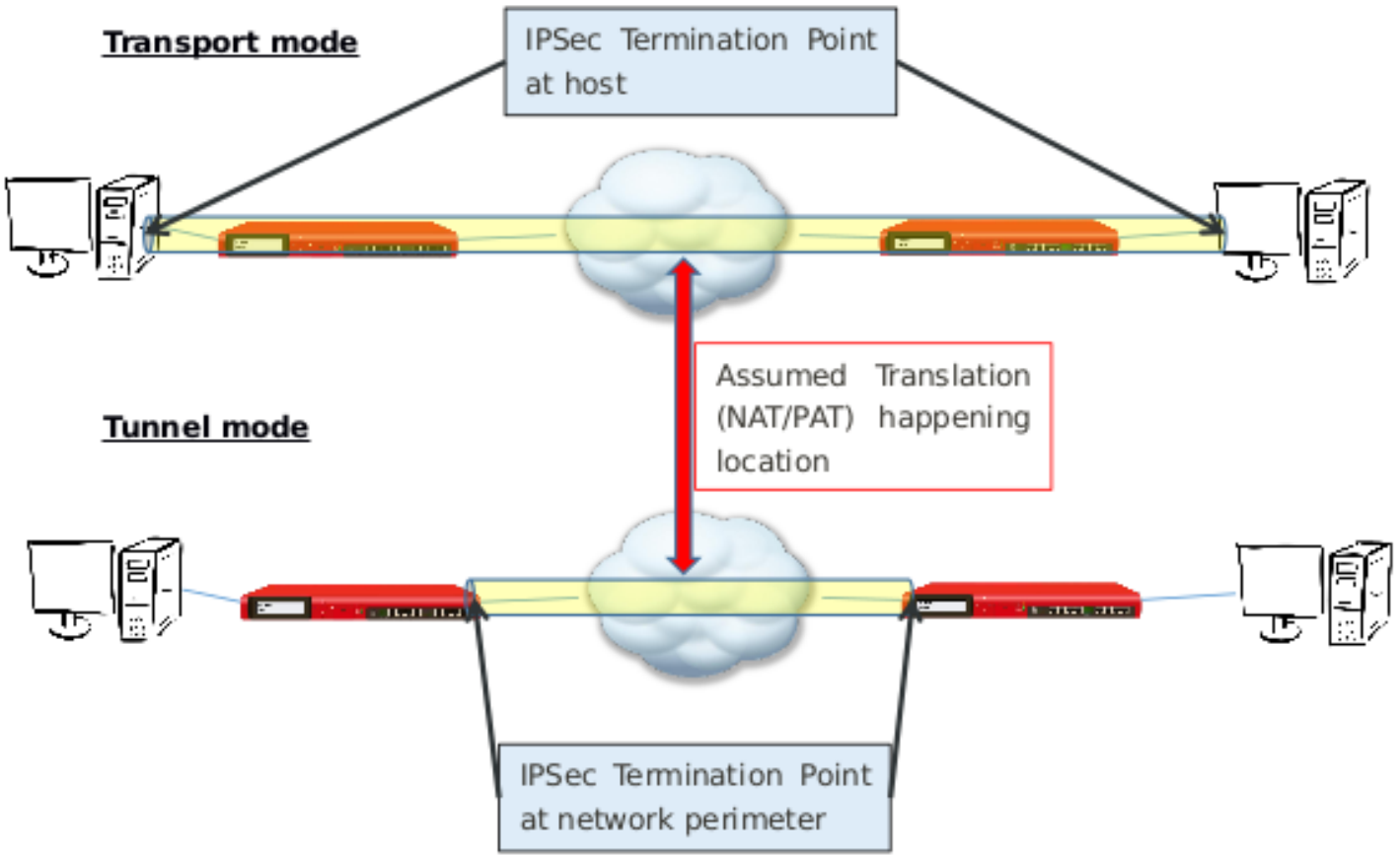
IPSec Security Associations (SA)

- One way cryptographically protected connection. i.e. for ESP it needs 2 SAs for sending and receiving.
- Defines how the relationship between sender and receiver
- SAs are stored in SAD (Security Association Database) where in SAD there is an entry for each SA:
  - Uniquely identified by three parameters:
    - Security Parameter Index (SPI)
    - Security Protocol Type (ESP , AH)
    - IP Destination/Source address

SAD, SPI and SPD

- SAD at sender holds following for receiver as an SA (dstip=Receiver)
  - Security Parameter Index
  - Keys
  - Algorithm
  - Sequence number
- SPI of a received packet from a sender will tell receiver where to look for above info required to process senders packet.
- SPD - Security Policy Database defines how traffic is treated (e.g. Authorisation for services) - i.e. which traffic to be protected.

Modes of IPSec communication

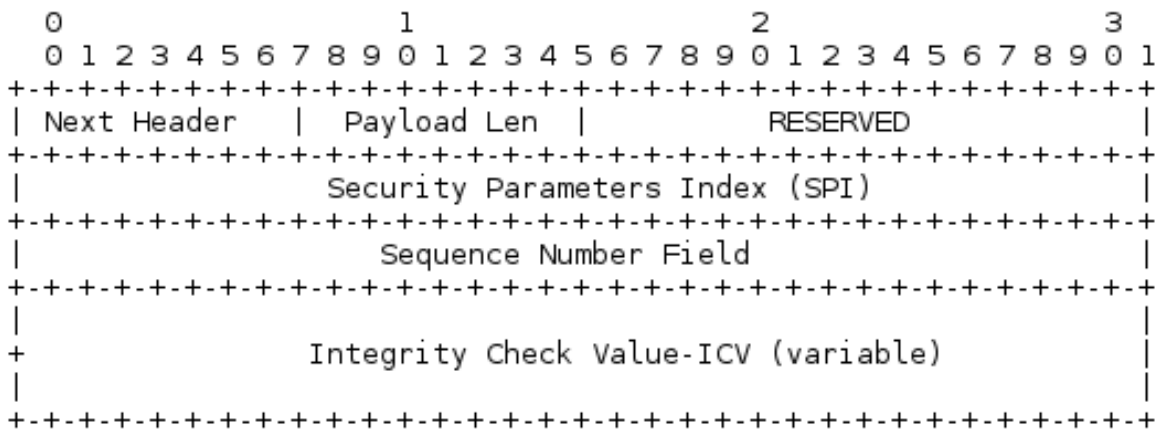


IPSec protocols

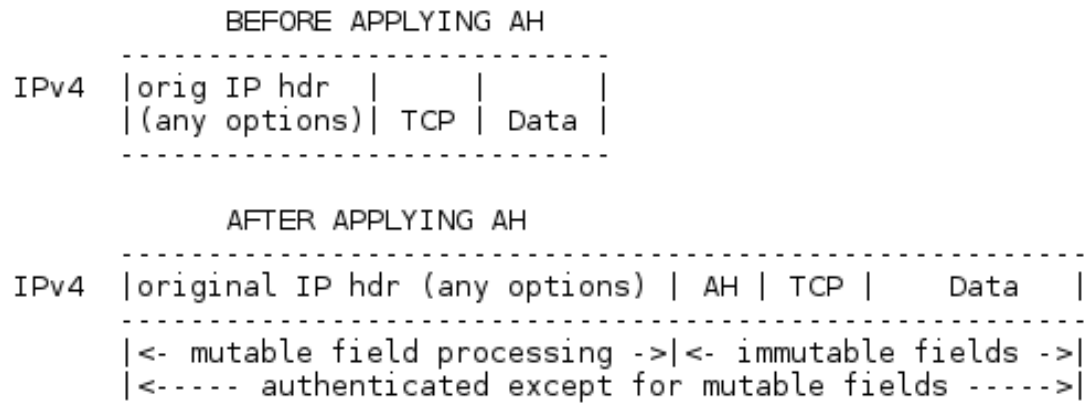
AH protocol - Authentication Header protocol is used when header level integrity should be maintained. However, no confidentiality is provided. This is not NAT friendly.

ESP protocol - Encapsulated Security Payload protocol protects mainly the payload and provides both confidentiality and integrity.

IPSec Architecture - Authentication Header



AH protocol with Transport mode



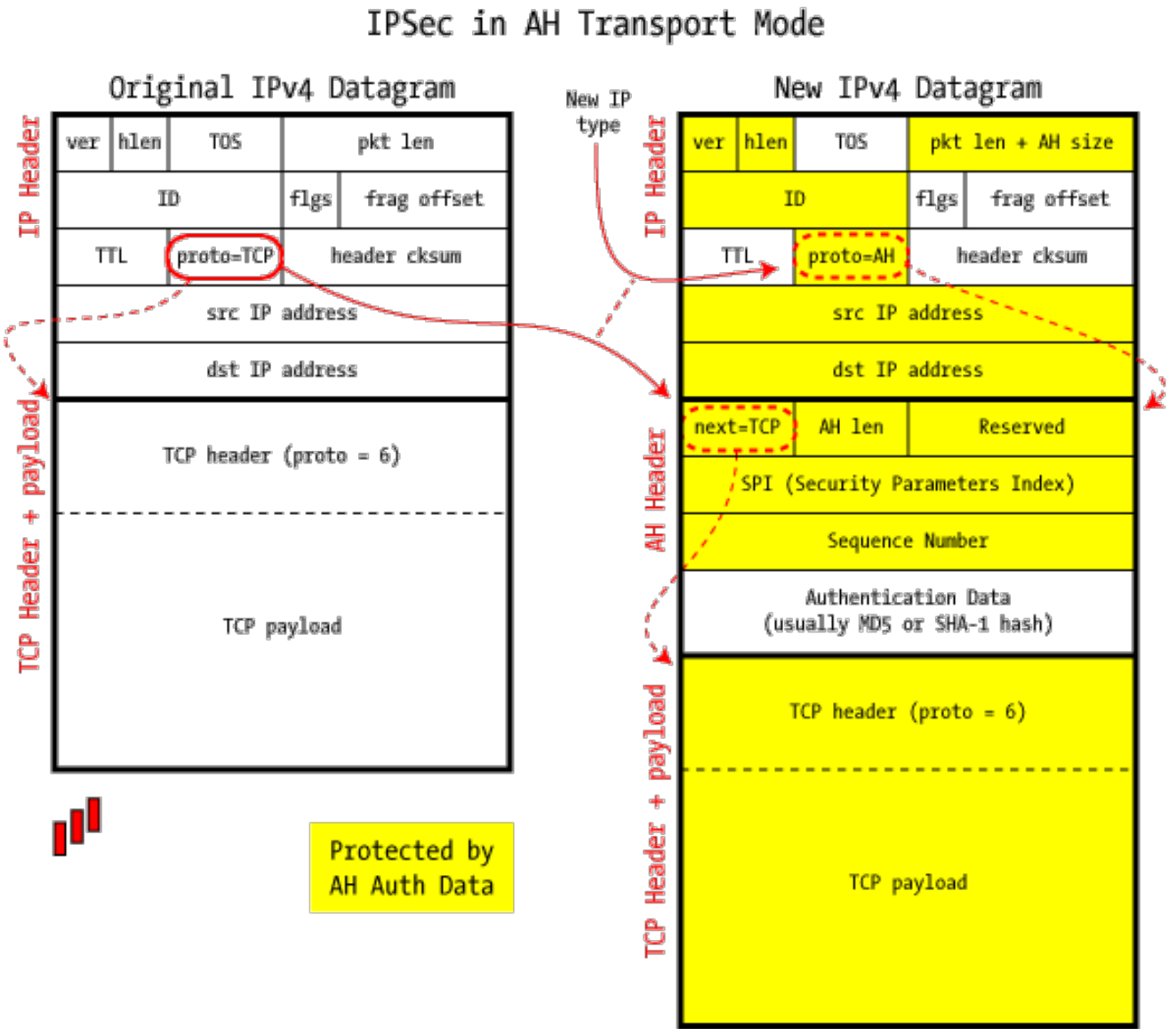
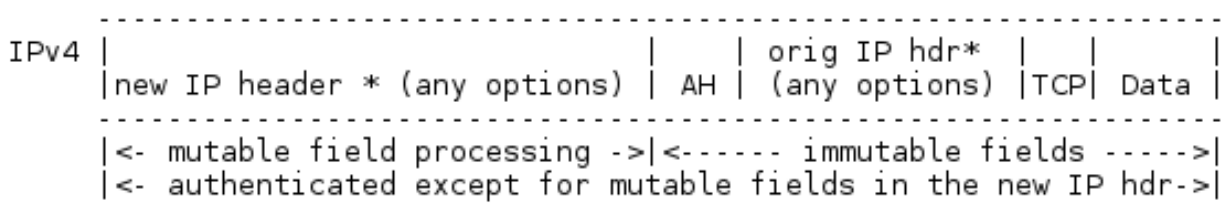


Figure: Ref: http://www.unixwiz.net/techtips/iguide-ipsec.html

AH protocol with Tunnel mode



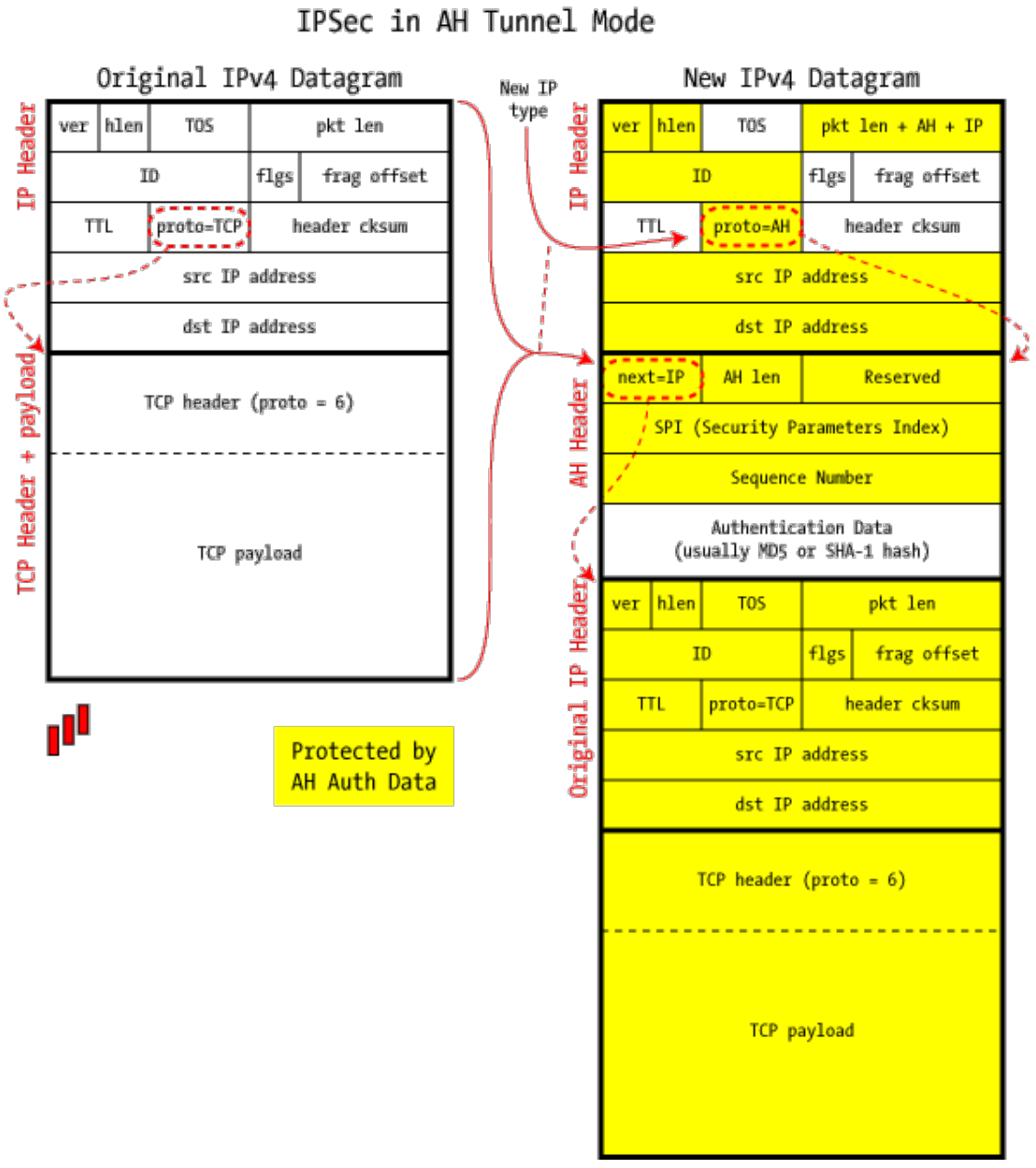
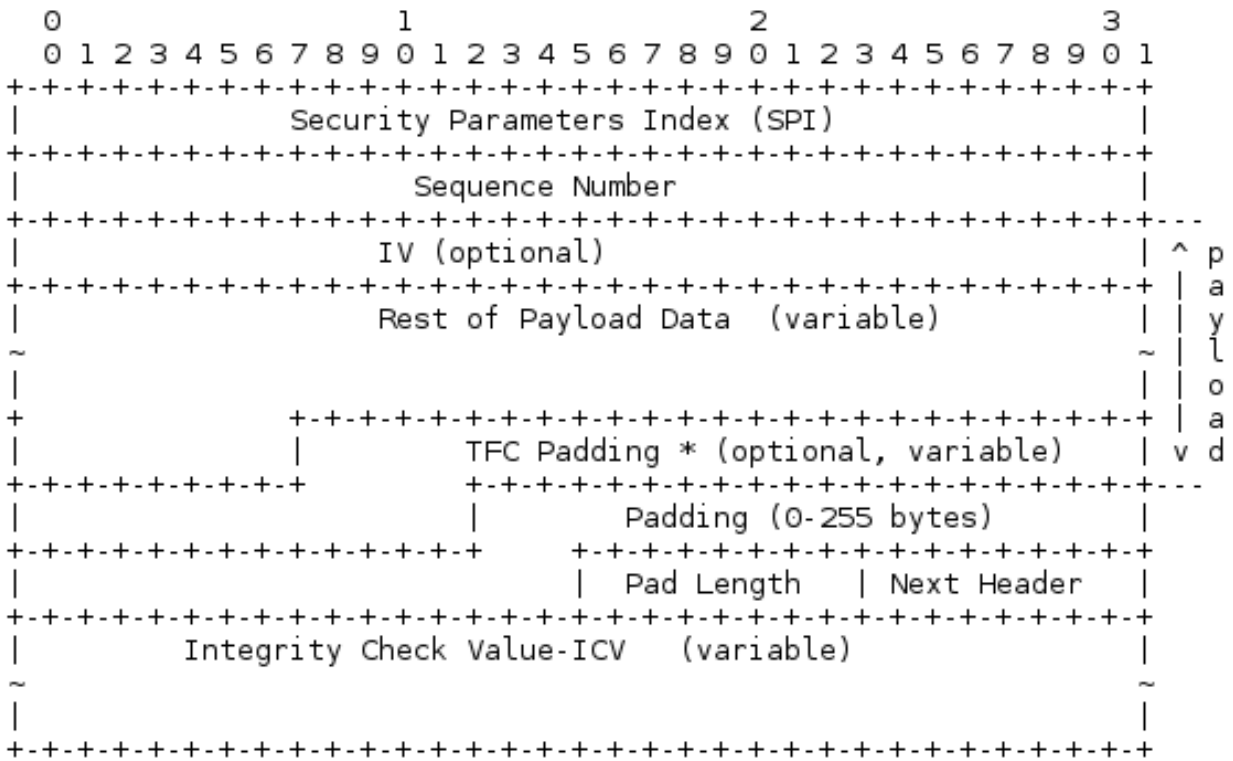
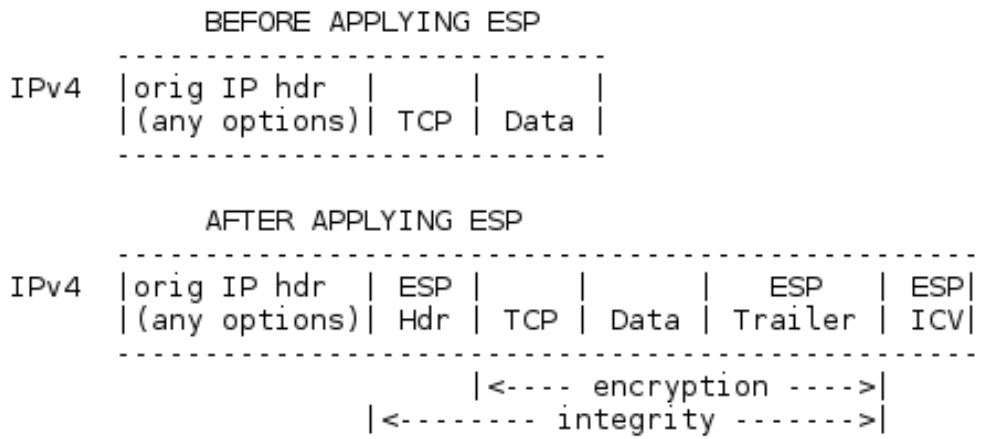


Figure: Ref: http://www.unixwiz.net/techtips/iguide-ipsec.html

Encapsulating Security Payload (ESP)



ESP protocol with Transport mode



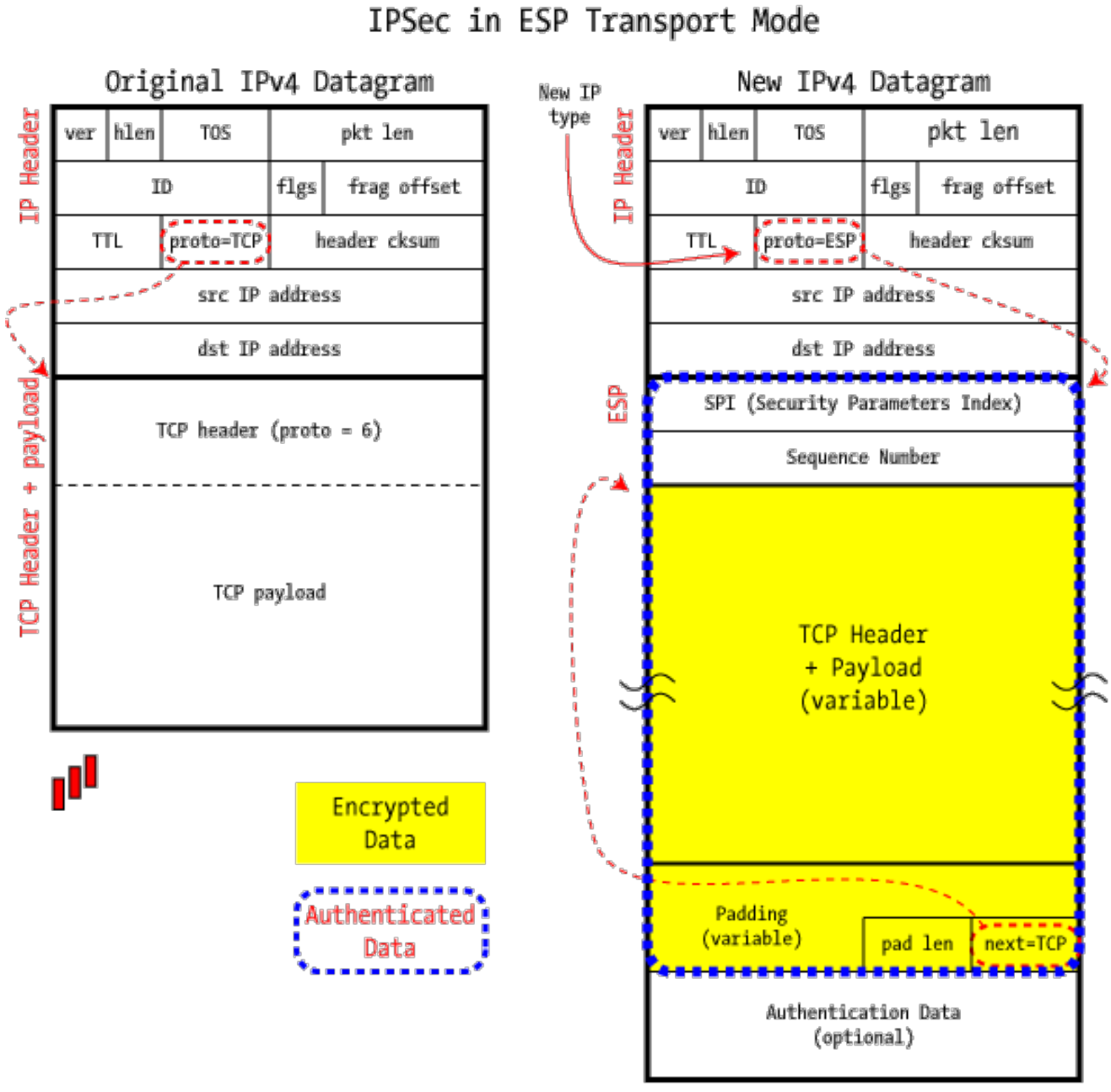
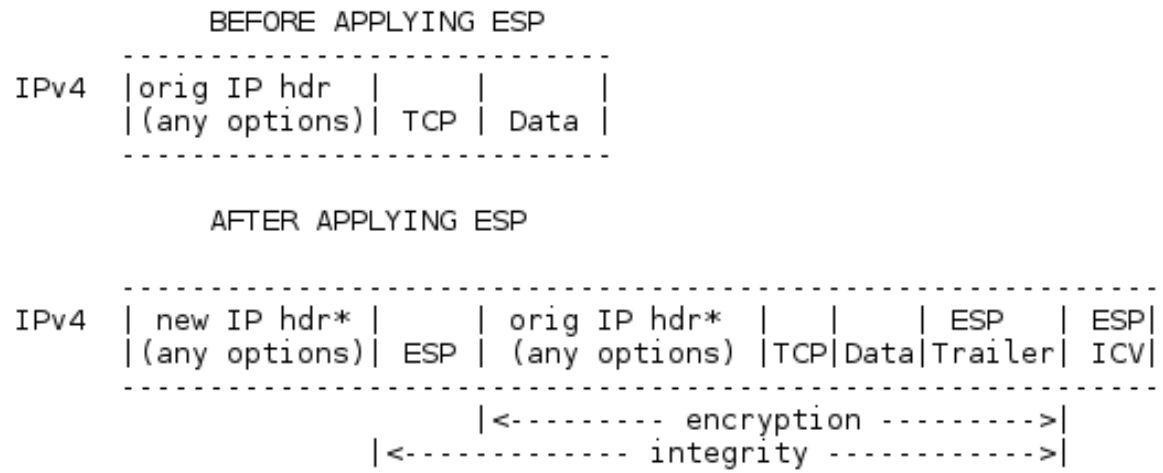


Figure: Ref: http://www.unixwiz.net/techtips/iguide-ipsec.html

ESP protocol with Tunnel mode



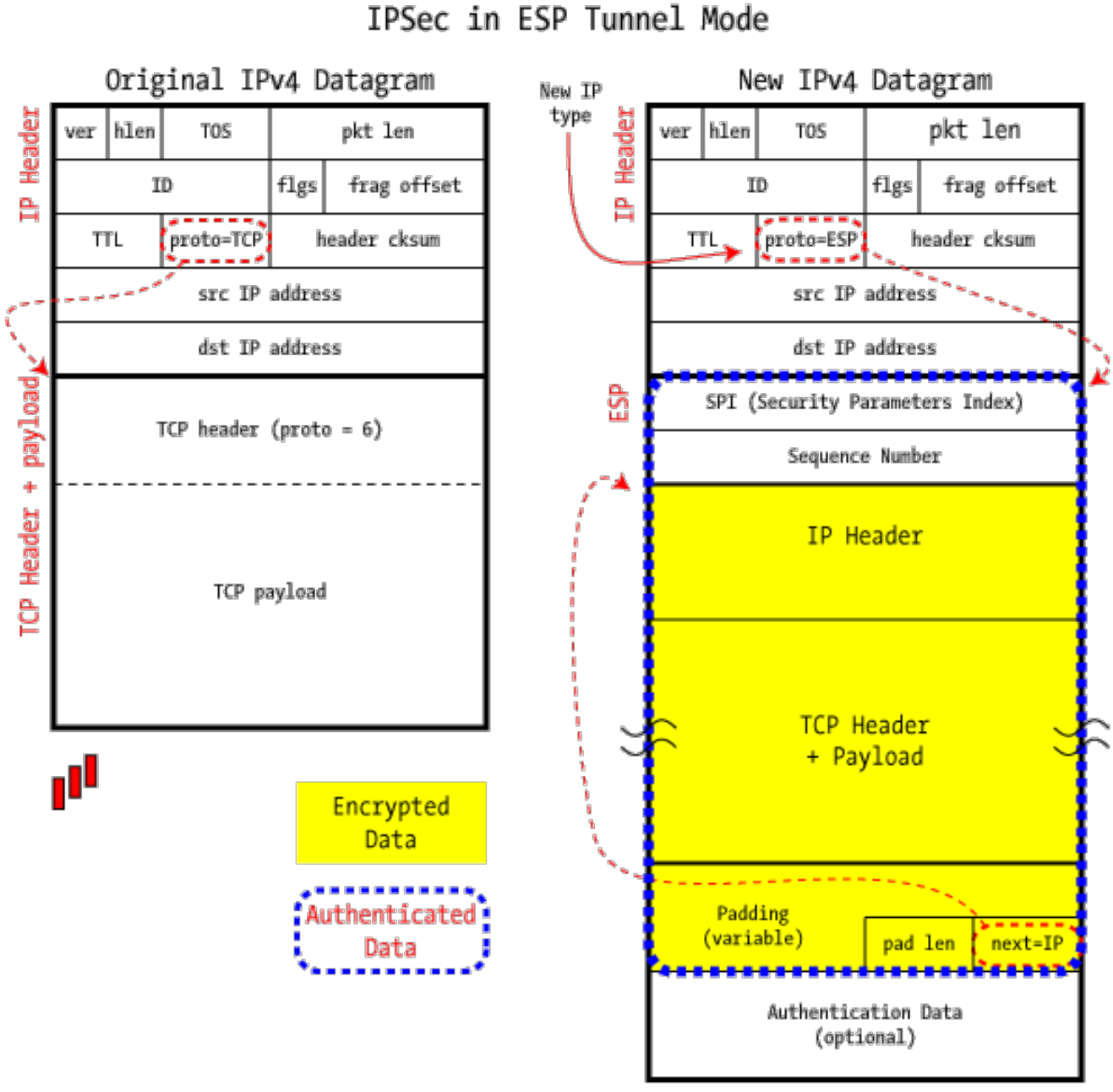


Figure: Ref: http://www.unixwiz.net/techtips/iguide-ipsec.html

ESP Tunnling mode vs Transport mode

- Both modes of ESP protocol support NAT.
- Tunnelling mode is used for site-to-site VPN whereas transport mode is used for host-to-host VPN.
- In tunnelling mode additional headers are added to the packet thus may limit the bandwidth slightly.
- Further reading: https://tools.ietf.org/html/rfc3715 for IPSec NAT compatibility requirements

Guidelines when using IPSec

- Always use AES (or 3DES)
- Use SHA-256 rather than SHA-160 or MD5
- Use Tunnel mode where possible as it is transparent to hosts' applications and scalable than transport mode
- Use AH and ESP together where you need more integrity as AH alone does not provide confidentiality. However, there are cases where you may need to implement AH only - e.g. some SOAP implementations
- Use Certificates for Key Exchange

IPSec VPN vs SSL VPN

- SSL VPN is more flexible than IP Sec VPN
  - Configuration is significantly easier
  - SSL/TLS VPN works on TCP 443 which most firewalls open by default as the same port is used to connect to HTTPS. However, IPSec VPN needs UDP 500 port opened.
- IPSec VPN is transparent to applications as it is implemented at Layer 3 (Network layer) whereas SSL VPN is implemented at application / transport layers.
- IPSec VPN can provide site to site VPN capability whereas SSL VPNs are not used for that purpose.
- SSL VPN is preferred for remote peer connectivity over IPSec VPNs due to flexibility of implementation and connectivity.

Benefits of using VPN over dedicated links or Leased lines

Not all VPNs provide all the benefits listed below

- Lower cost.
- Anywhere anytime access
- Privacy
- Confidentiality, Integrity, Authentication
- Access control

Disadvantages of using VPN over dedicated links or Leased lines

Not all VPNs have all disadvantages listed below

- Performance
- Different solutions from different vendors may not converge
- Security depends on how organization configures it
- Some VPNs are specific to certain connection types and protocols
- QoS is not well served in some VPNs
- Some VPNs does not support complex network setup (e.g. multiple NATs) or special network requirements such as multicasting
- Weakest link is its users

References

- https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13847.htm
- http://www.ciscopress.com/articles/article.asp?p=24833
- http://www.unixwiz.net/techtips/iguide-ipsec.html
- https://tools.ietf.org/html/rfc4301#page-7
- https://tools.ietf.org/html/rfc4306
- https://www.ietf.org/rfc/rfc4302.txt
- https://www.ietf.org/rfc/rfc4303.txt
- https://www.youtube.com/watch?v=TTIEHSeUeYI