Cisco Internetworking Bootcamp

An Introduction To VPNs

Agenda

- What is a VPN
- Different kinds of VPN tunnels
  - PPTP
  - L2TP
  - L2TP over IPSEC
  - IPSEC over GRE
- IPSEC Protocol Suite

What is VPN ?

- **A Virtual Private Network Carries Private Traffic Over a Public Network**

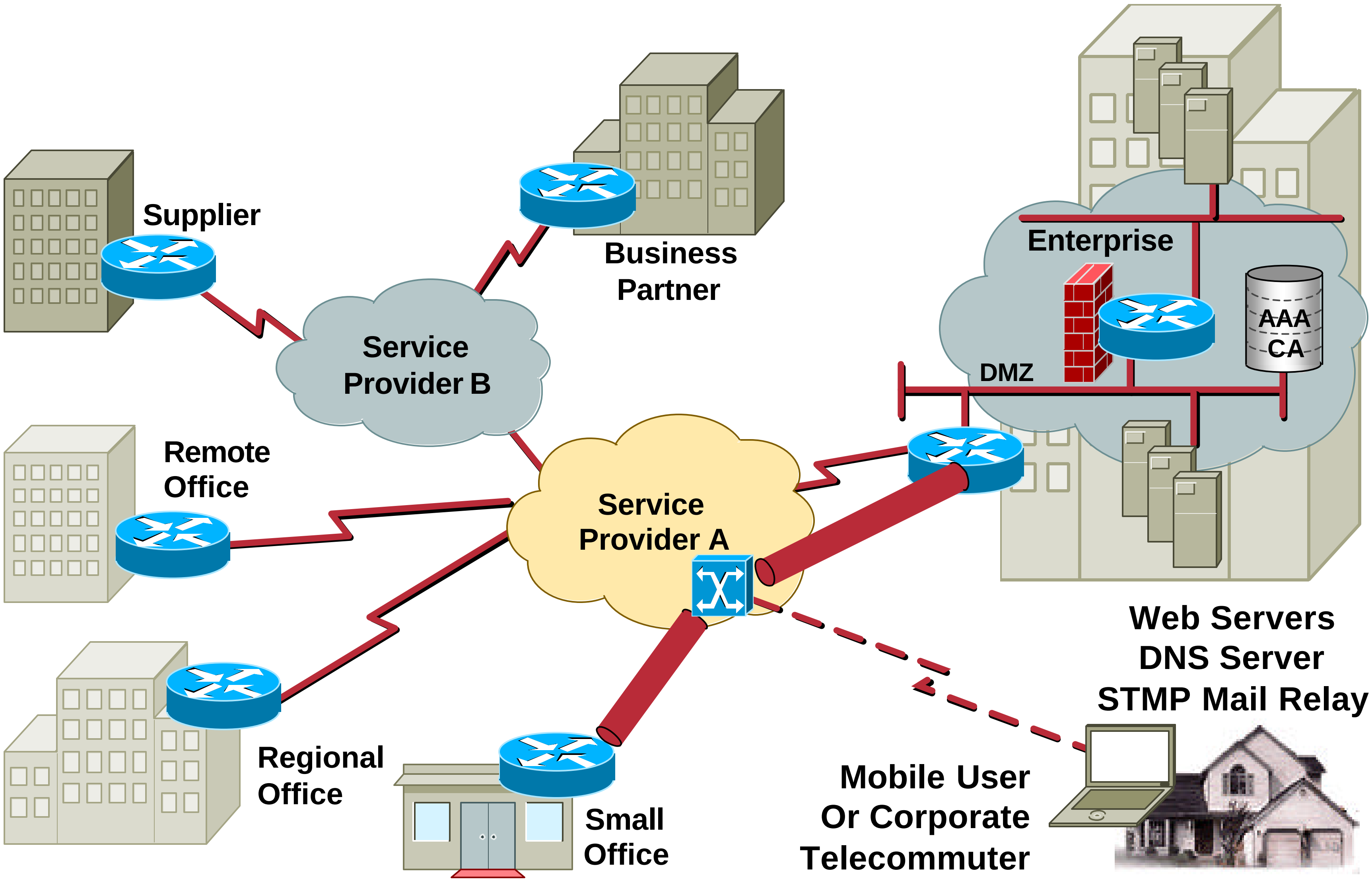
Secure VPN Services

- Confidentiality
- Authentication
- Integrity
- Nonrepudiation
- Access Control

VPN Technologies

- Non-Cryptographic Approaches
  - GRE Tunneling
  - MPLS VPN
- Cryptographic Approaches
  - PPTP (MPPE)
  - L2F / L2TP (Protected by IPSEC)
  - GRE (Protected by IPSEC)
  - IPSEC

VPN Scenarios



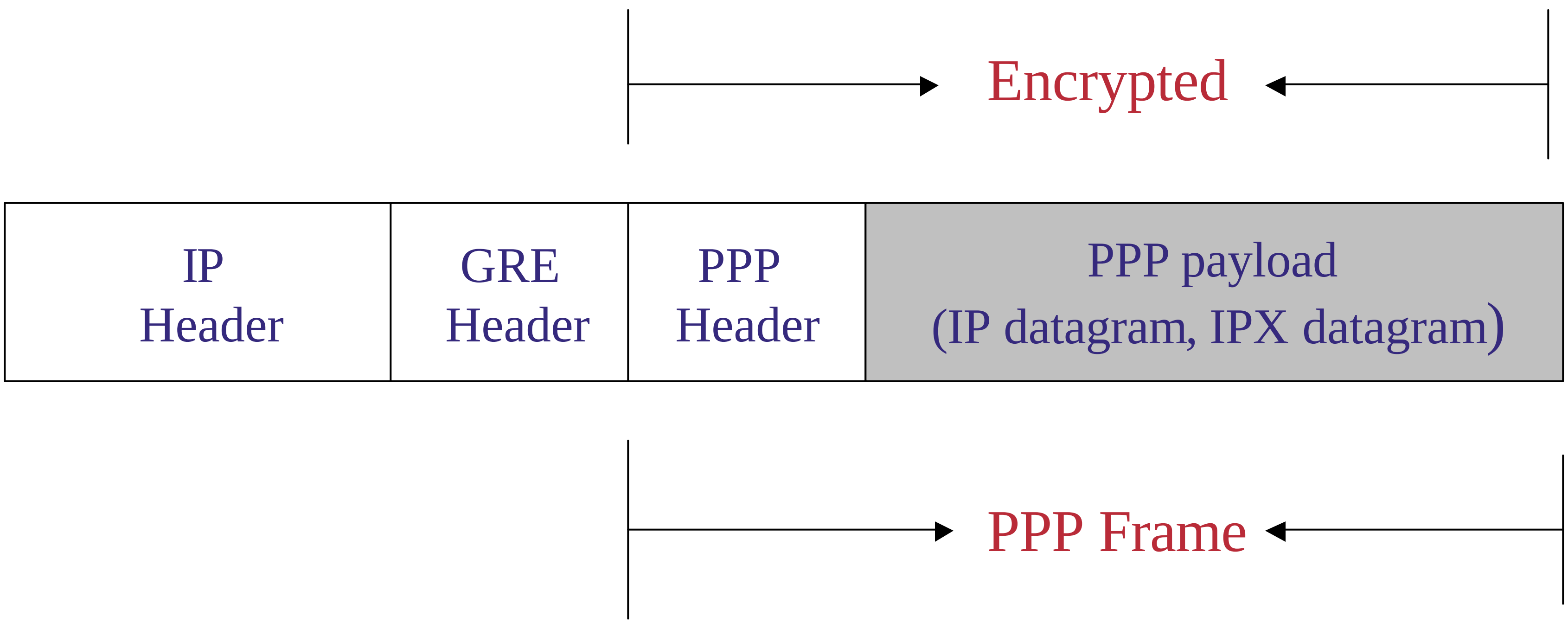
Point To Point Tunneling Protocol(PPTP)

Cisco.com

- Encapsulates PPP Frames in IP datagrams to transmit over an IP internetwork.
- Used for remote access
- Ports used are TCP 1723 and GRE (IP Protocol type 47)
- Documented in RFC 2637

Point To Point Tunneling Protocol(PPTP)

PPTP packet diagram



Layer 2 Tunneling Protocol(L2TP)

- Combination of PPTP and Layer 2 forwarding (L2F)
- Encapsulates PPP frames to be sent over IP,frame relay ,ATM and X.25 networks.
- Used for remote access
- Uses UDP port 1701
- Documented in RFC 2661

Layer 2 Tunneling Protocol(L2TP)

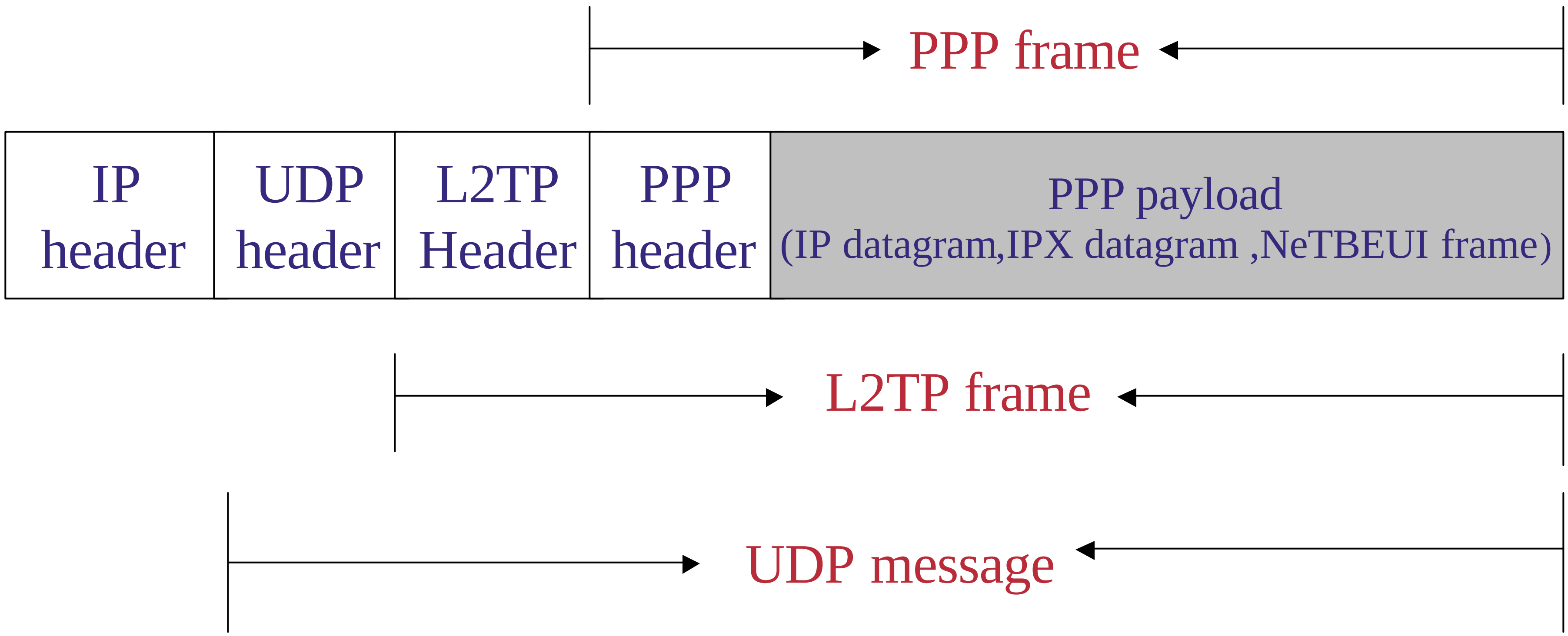


Figure : L2TP packet diagram

L2TP over IPSEC

- L2TP does not provide any data encryption.
- In order to provide encryption services
WIN2000 uses IPSEC encapsulation
Security payload (ESP) to encrypt the
L2TP packet

L2TP over IPSEC

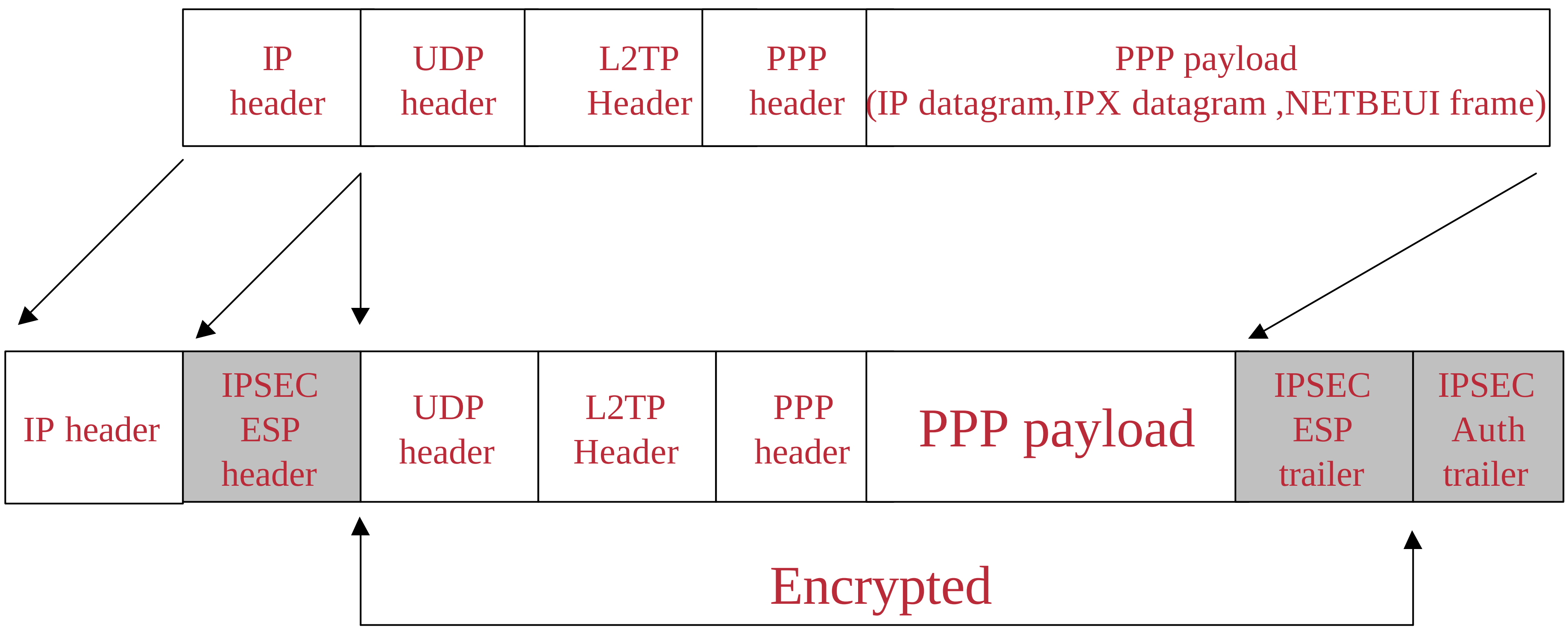


Figure : L2TP over IPSEC packet

IPSEC over GRE

- **GRE does not provide any authentication, confidentiality or data integrity.**
- **In order to provide the above mentioned services , the original GRE packet is encrypted using IPSEC**

IPSEC over GRE

Original IP datagram

IP header	IP payload

GRE encapsulation

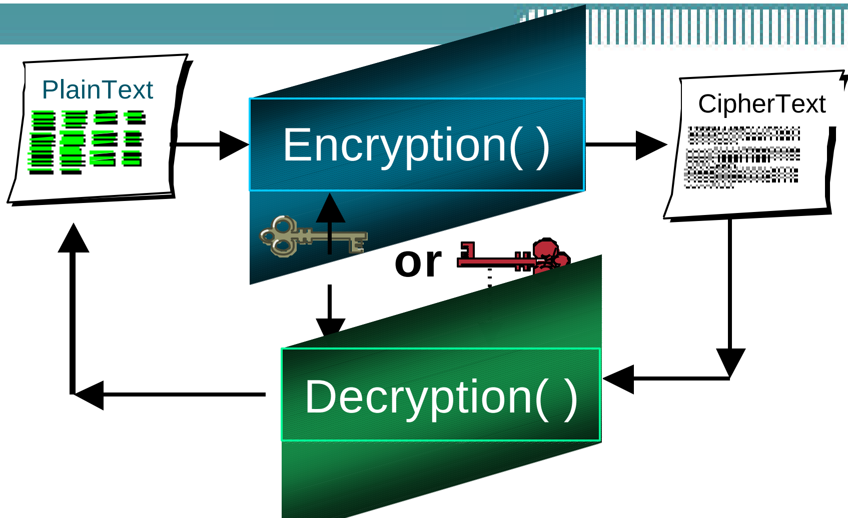
GRE header	Original IP header	IP payload

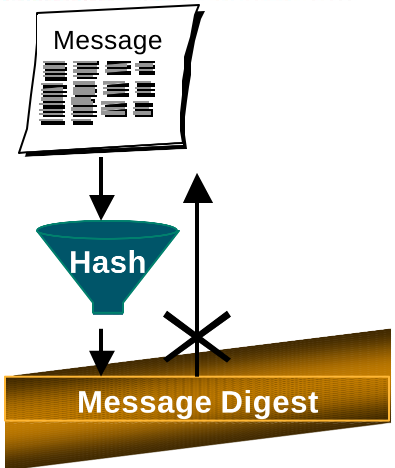
IPSEC used to encrypt GRE packet

New IP Header	ESP header	GRE header	Original IP header	IP payload	ESP trailer

Encryption vs. Hash

Cisco.com

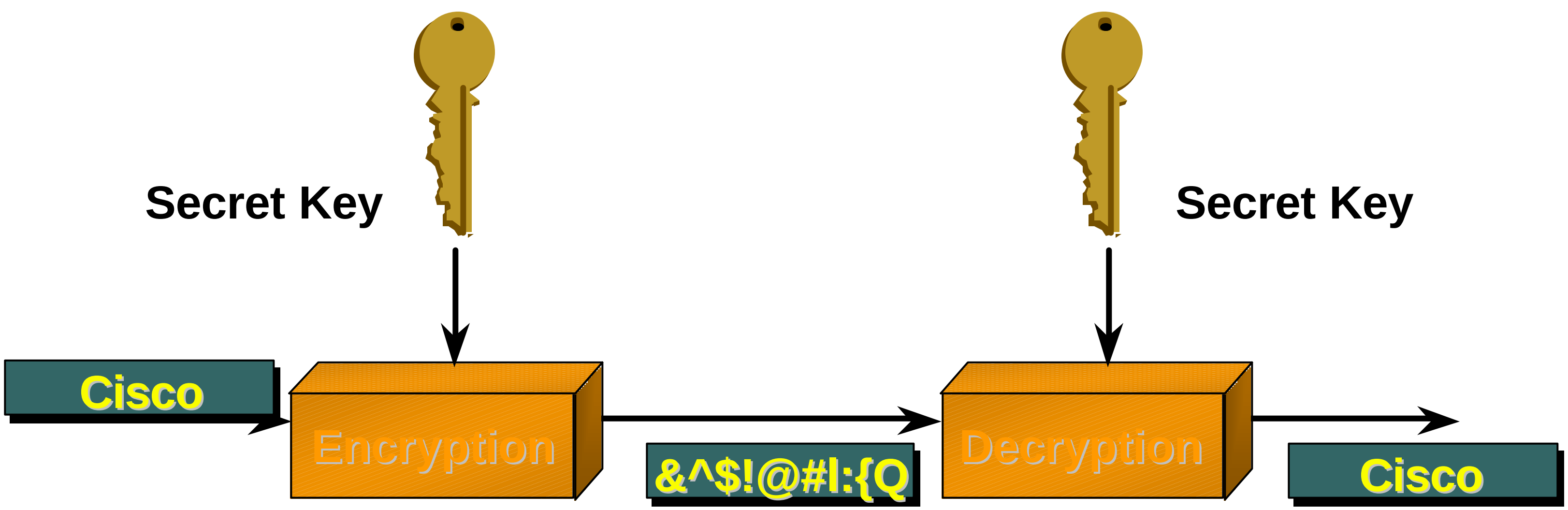




- Encryption transforms data into unrecognizable characters.
- Encrypted data can be decrypted by using the correct keys.
- Encryption keeps communications Private.
- Encryption and decryption can use same or different keys.
- Achieved by various algorithms, e.g. DES, CAST.

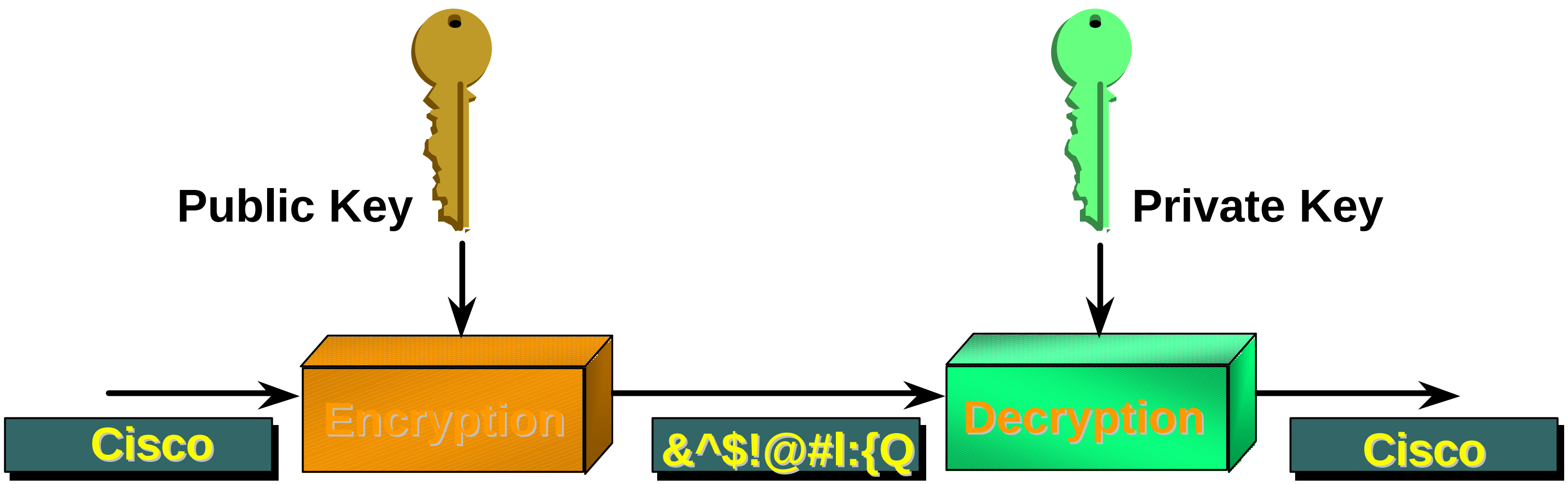
- Hash transforms message into fixed-size string (“message digest”).
- Hashed data can NOT be converted back to original form.
- Used for message integrity check and digital certificate.
- Message digest can be viewed as “digital fingerprint”.
- Eg: SHA , MD5

Symmetric Encryption



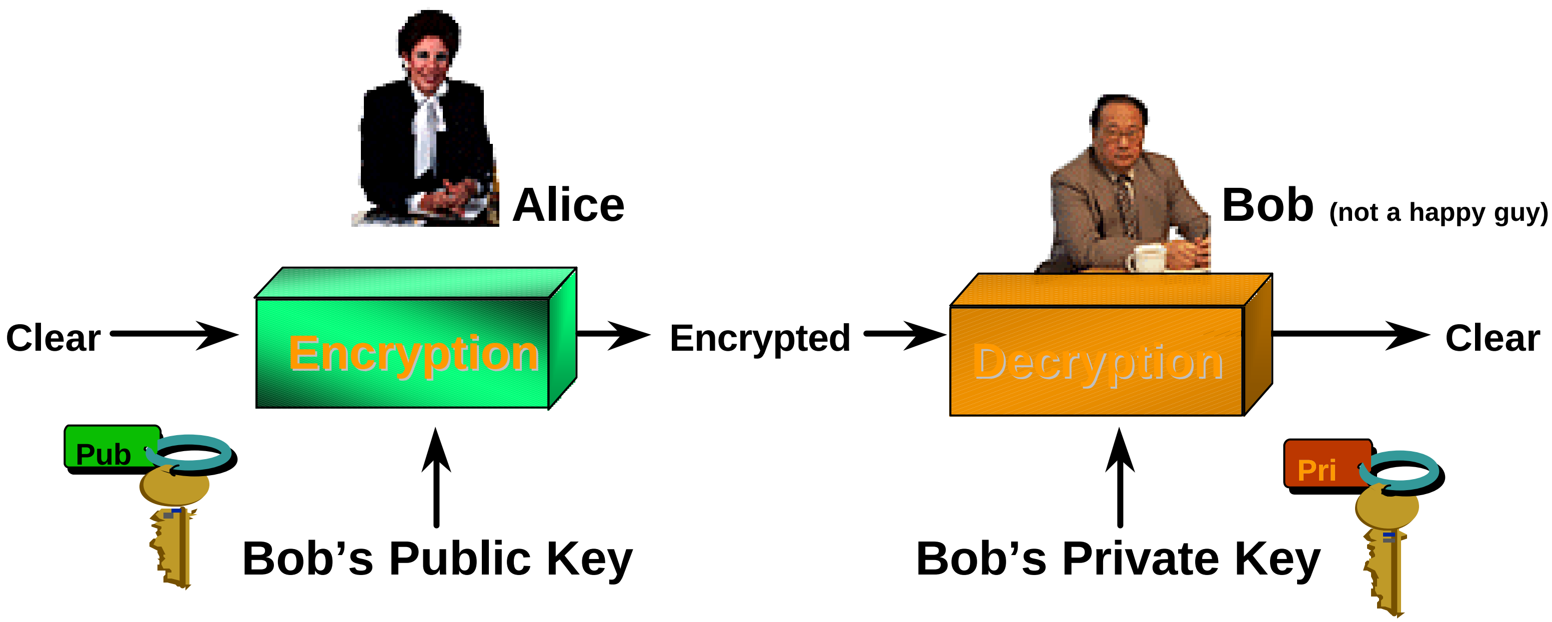
- Encryption and decryption use same mathematical function
- Encryption and decryption use same key
- Example: Data Encryption Standard (DES, 3DES)

Asymmetric Encryption



- Encryptor and decryptor use different keys
- Example: public key algorithms
  (RSA and DSS)

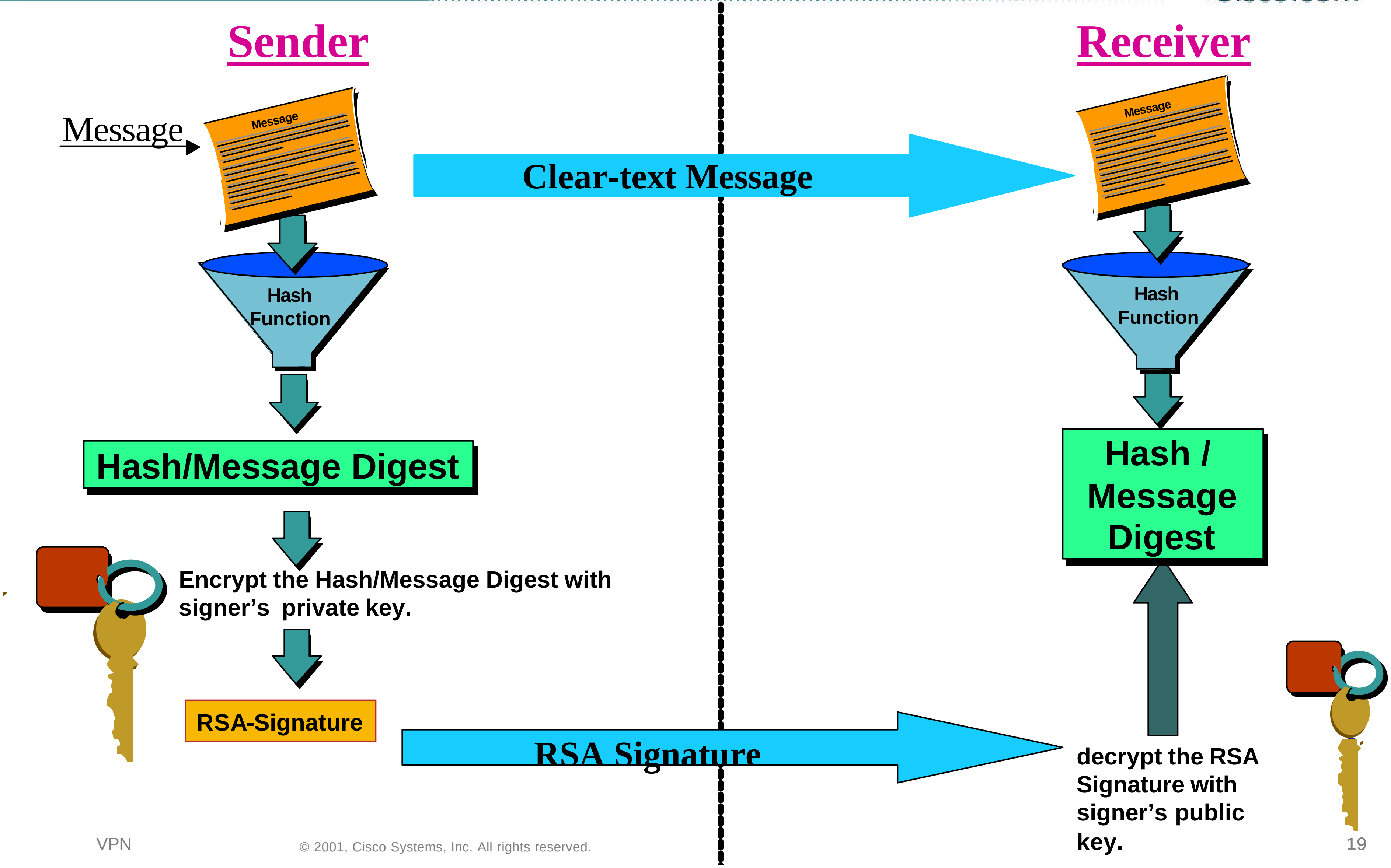
Data Confidentiality



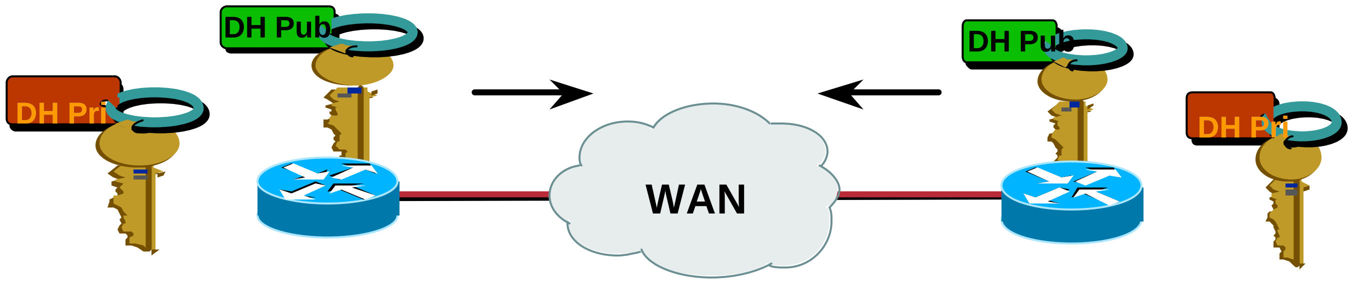
- Alice gets Bob's public key
- Alice encrypts message with Bob's public key
- Bob decrypts using his private key

Verifying the digital signature

Cisco.com



Deriving Secret Keys Using Public Key Technology (Diffie-Hellman)



- **Each device has two keys:**
  1. **A private key, generated by each device, which is kept secret and never shared**
  2. **A public key, calculated from the private key by each device, which is non-secret**

IPSec Protocol Overview

Cisco.com

- IPSEC Definition and Services
- IPSEC Modes
- AH and ESP
- IPSEC Security Association
- IKE
- ISAKMP
- Case study

What is IPSEC

- IPSEC stands for IP Security

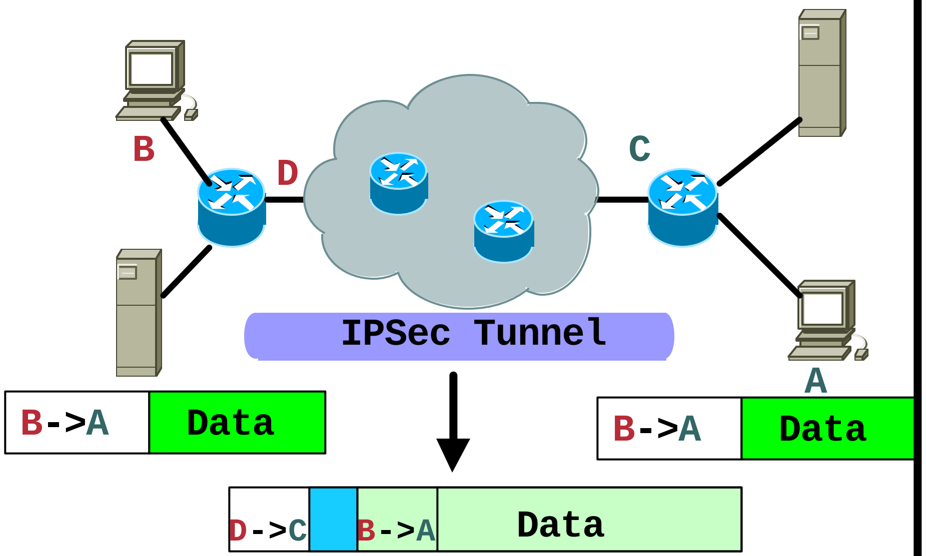
"A security protocol in the network layer will be developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality" (IETF)

What IPSEC Offers

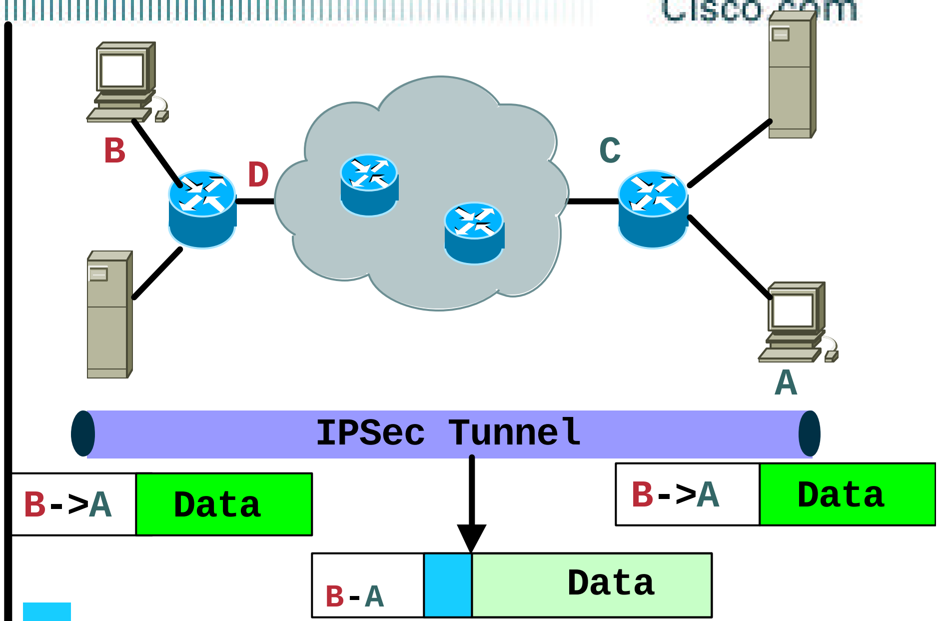
IPSEC is a combination of three primary protocols (ESP, AH and IKE) (protocol 50, protocol 51, UDP/500)

- **Authentication: Authentication Header (AH) and Encapsulating Security Payload (ESP)**
- **Integrity: Encapsulating Security Payload (ESP)**
- **Confidentiality: Encapsulating Security Payload (ESP)**
- **Replay Detection**
- **Access control and Traffic flow confidentiality**

IPSEC Modes



IPSec header



IPSec header

Tunnel Mode

- Encrypt IP traffic flowing ***through*** IPSec peers
- Original IP header is encrypted
- Traffic flow confidentiality

Transport Mode

- Encrypt IP traffic between IPSec peers
- Less overhead
- Some portion of original IP packet is visible

Authentication Header (AH)

- Data Integrity – data has not been modified during transmission.
- Origin authentication– data is indeed coming from IPSec peer.

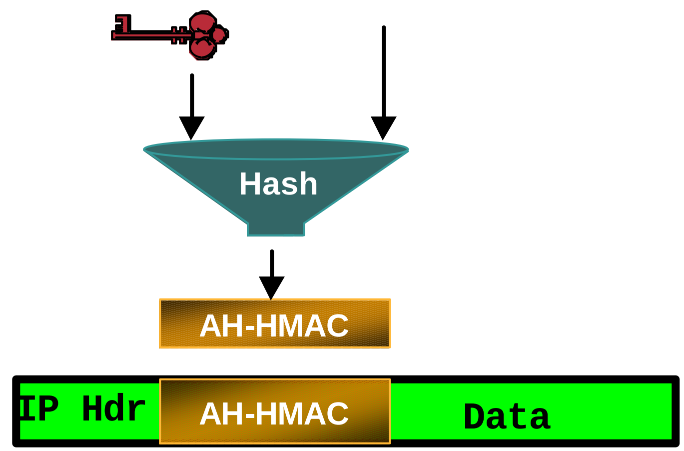
HMAC-MD5-96
HMAC-SHA-1-96

- Anti-replay detection

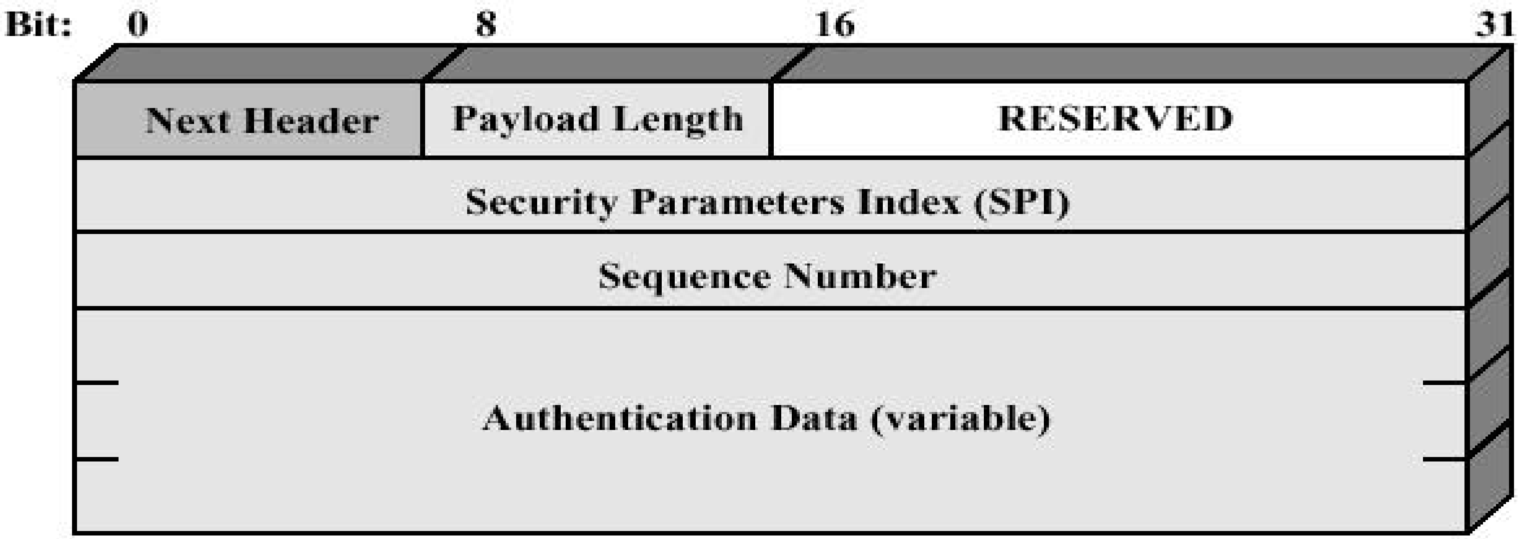
Sequence no.
& Sliding window

- Data in cleartext – NO confidentiality.
- Use IP protocol 51
- Defined in RFC 2402
- Can be used in Tunnel or Transport Modes

Most part
Of IP header
+ data



Authentication Header



Transport Mode

Original IP Header	TCP	Data

Original IP Header	AH	TCP	Data

← Authenticated except mutable field →

Tunnel Mode

Original IP Header	TCP	Data

New IP Header	AH	Original IP Header	TCP	Data

← Authenticated except mutable field in new ip header →

Encapsulating Security Payload (ESP)

- Data confidentiality

  DES-CBC
  3DES

- Data integrity (does not cover ip header)
- Data origin authentication

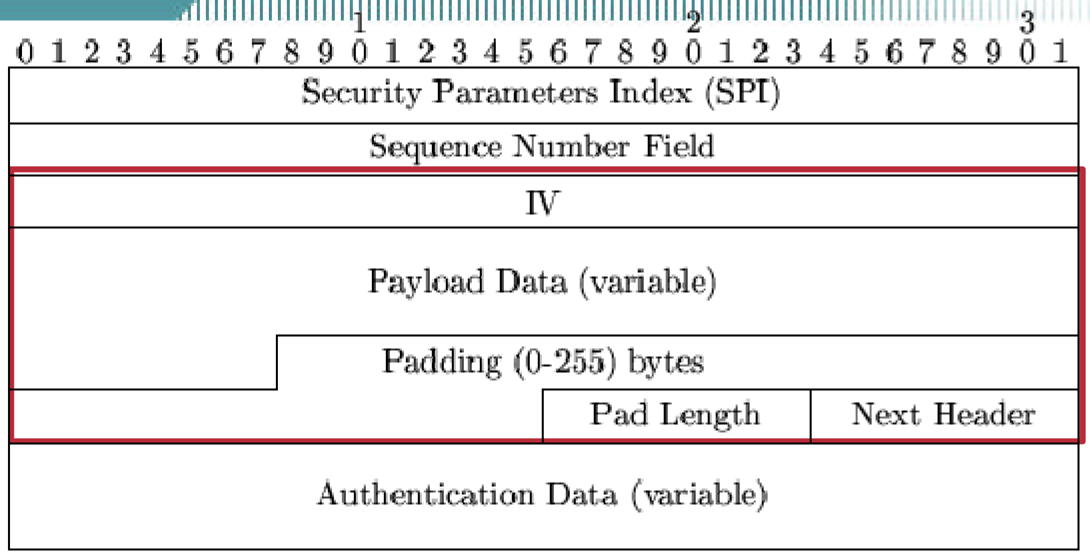
  HMAC-MD5-96
  HMAC-SHA-1-96

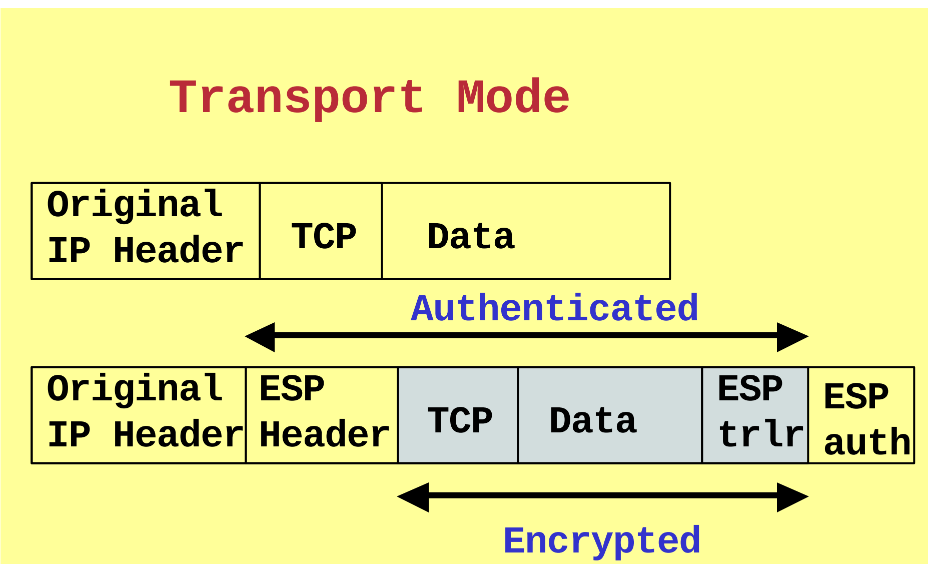
- Anti-replay detection

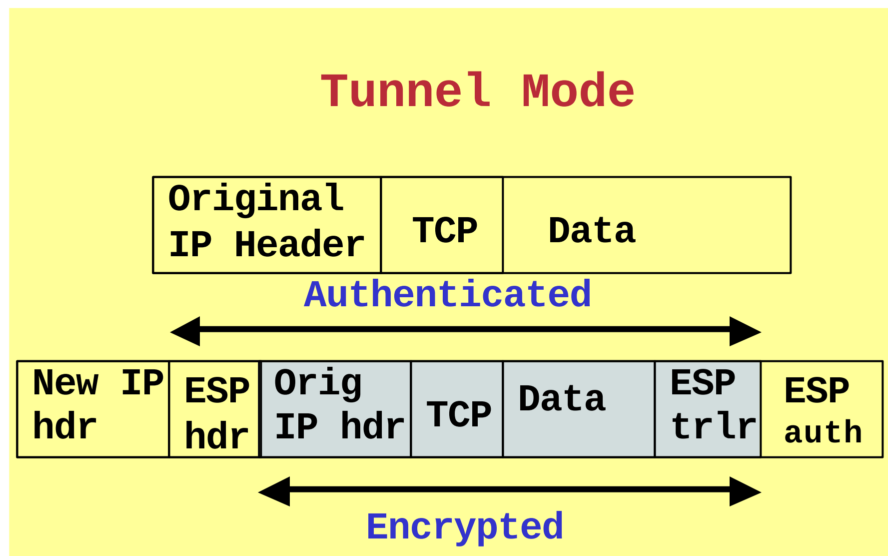
  Sequence no.
  & Sliding window

- Traffic flow confidentiality
- Use IP protocol 50
- Defined in RFC 2406

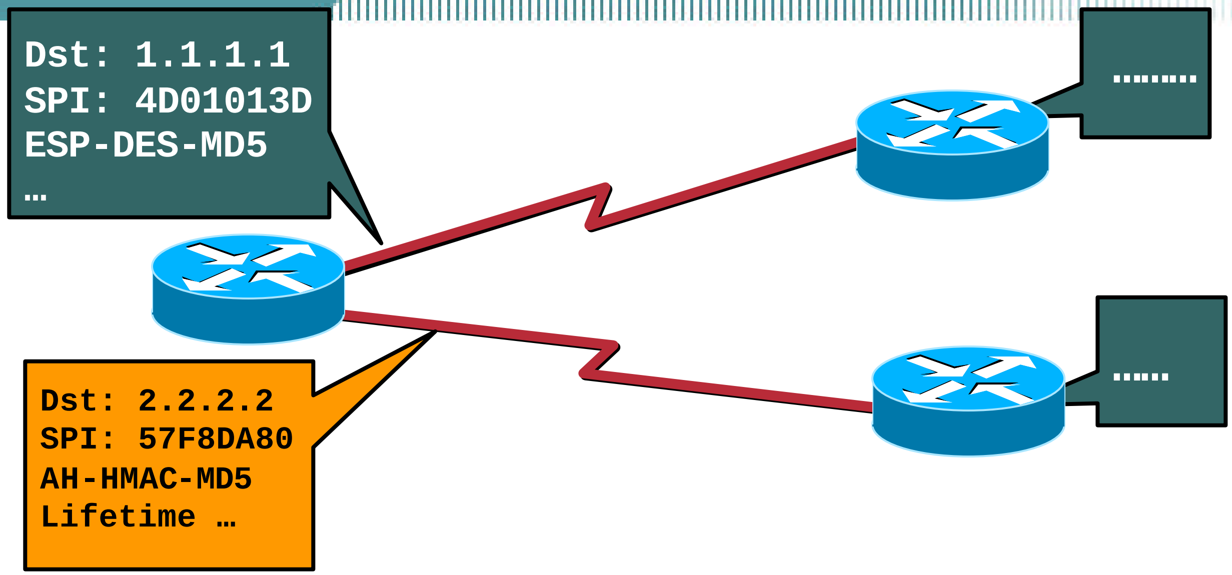
Encapsulating Security Payload (ESP)







Security Association

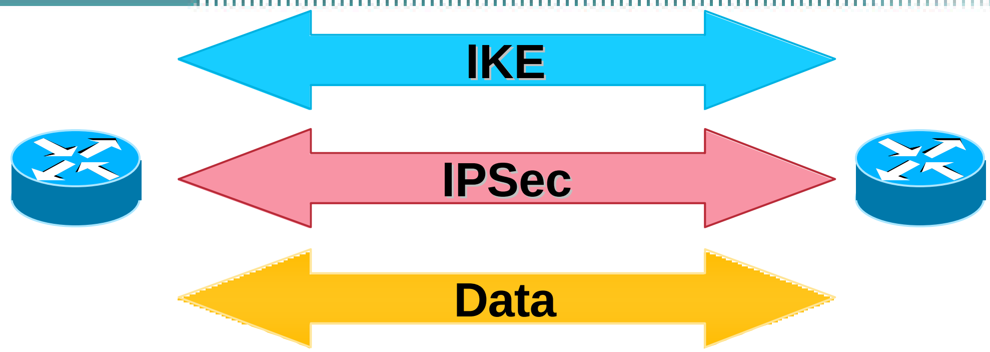


- **Defines one-way relation between IPSec peers which apply security services to the traffic carried.**
- **Two SAs are needed for two-way secure communication.**

Internet Key Exchange (IKE)

- Hybrid protocol: combination of ISAKMP, Oakley Key exchange and SKEME protocols.
- Define the mechanism to derive authenticated keying material and negotiate security associations (used for AH, ESP)
- Uses UDP port 500
- Defined in RFC 2409

IKE (Two-Phase Protocol)



- **Two-phase protocol:**

  – **Phase I exchange: two peers establish a secure, authenticated channel with which to communicate. Main mode or aggressive mode accomplishes a phase I exchange.**

  – **Phase II exchange: security associations are negotiated on behalf of IPSec services. Quick mode accomplishes a phase II exchange.**

- **Each phase has its SAs: ISAKMP SA (phase I) and IPSec SA (phase II).**

IKE Authentication

What are authenticated ?

- Device or host identity authentication.
- Extended Authentication (Xauth) add legacy user authentication.

IKE Authentication Methods

- **Pre-shared secret**
  - Easy to deploy, not scalable
- **Public-key signatures (rsa-signature)**
  - Most secure, require infrastructure.
- **Public-key encryption (rsa-nonce)**
  - Similar security to rsa-sig, requires prior knowledge of peer's public key, limited support.

ISAKMP

- **ISAKMP: Internet Security Association and Key Management Protocol.**
- **Define procedure and packet format to establish, negotiate, modify and delete security association:**
  - **Standardized payload**
  - **Exchange types**
  - **Payload Processing rules**
- **Domain of Interpretation defines the syntax and semantics.**
- **Defined in RFC 2408.**

IPSEC Functionality Flow Chart

Interesting traffic received

↓

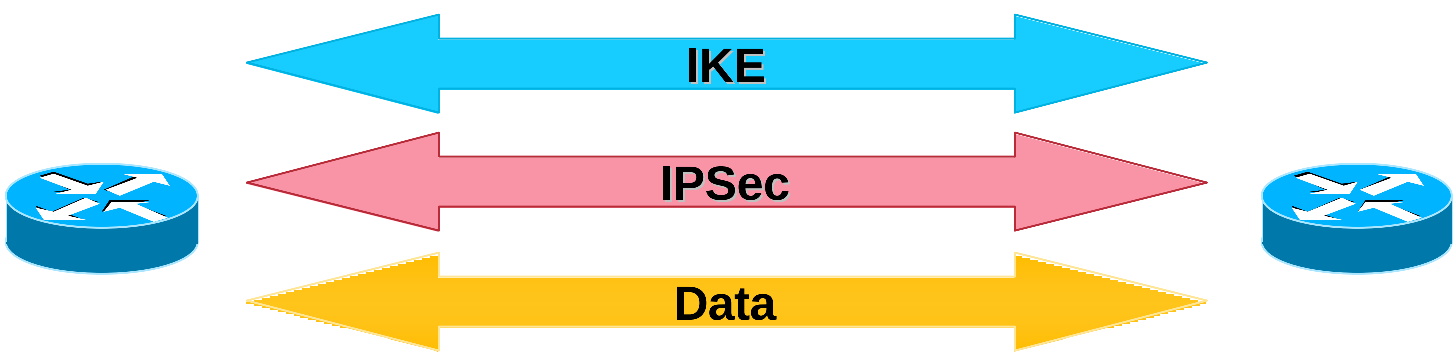
Main Mode IKE negotiation

↓

Quick Mode negotiation

↓

Establishment of tunnel

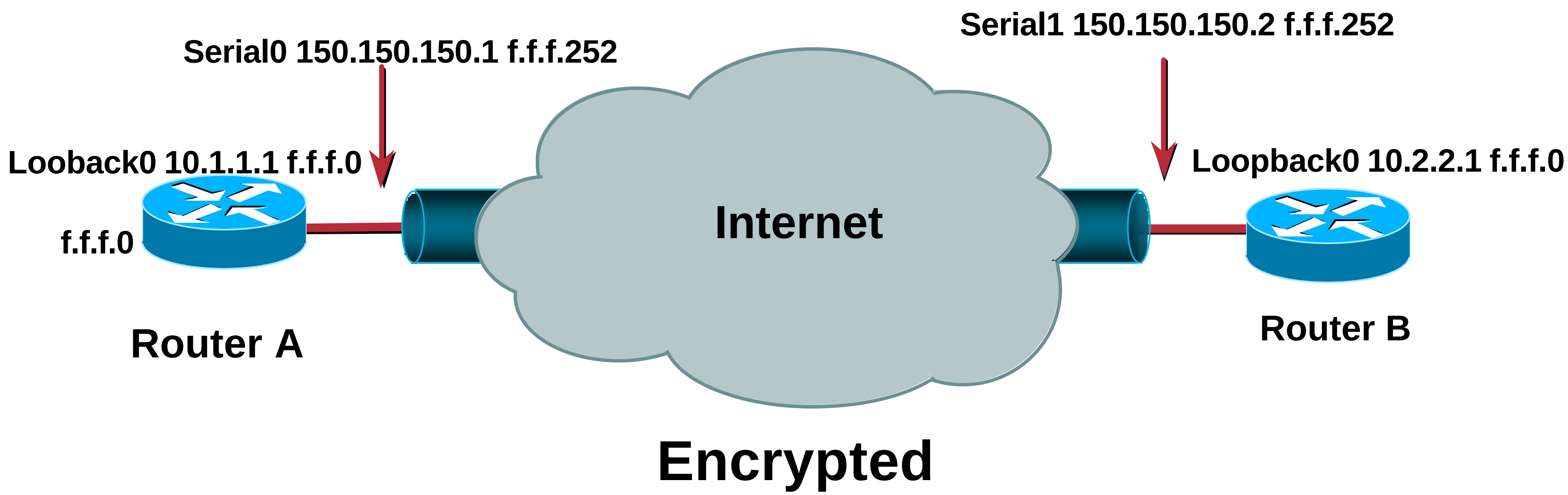


How IPSEC works

IPSEC is implemented in the following five stages:

- **Decision to use IPSEC between two end points across internet**
- **Configuration of the two gateways between the end points to support IPSEC**
- **Initiation of an IPSEC tunnel between the two gateways due to ‘interesting traffic’**
- **Negotiation of IPSEC/IKE parameters between the two gateways**
- **Passage of encrypted traffic**

Layout


Serial0 150.150.150.1 f.f.f.252
Serial1 150.150.150.2 f.f.f.252
Looback0 10.1.1.1 f.f.f.0
f.f.f.0
Internet
Loopback0 10.2.2.1 f.f.f.0
Router A
Router B
Encrypted

Router B configurations

```
Current configuration
Version 12.0
hostname RouterB
Crypto isakmp policy 10
hash md5
Authentication pre-share
Crypto isakmp key cisco address 150.150.150.1
!
Crypto ipsec transform-set set esp-des esp-md5-hmac
!
Crypto map vpn 10 ipsec-isakmp
Set peer 150.150.150.1
Set transform-set set
match address 120
```

Router B configurations

Cisco.com

```
interface Loopback0
ip address 10.2.2.1 255.255.255.0
!
interface Serial 1
ip address 150.150.150.2 255.255.255.252
crypto map vpn
!
ip route 0.0.0.0.0.0.0.0 150.150.150.1
!
access-list 120 permit ip 10.2.2.0.0.0.0.255
10.1.1.0.0.0.0.255
```

Router A configurations

Cisco.com

```
Version 12.0
hostname RouterA

Crypto isakmp policy 10
hash md5
Authentication pre-share
Crypto isakmp key cisco address 150.150.150.2
!
Crypto ipsec transform-set set esp-des esp-md5-hmac
!
Crypto map vpn 10 ipsec-isakmp
Set peer 150.150.150.2
Set transform-set set
Match address 120
```

Router A configurations


```
interface Loopback0
ip address 10.1.1.1 255.255.255.0
!
interface Serial0
ip address 15.150.150.1 255.255.255.252
crypto map vpn
ip classless
ip route 0.0.0.0 0.0.0.0 150.150.150.2
!
Access-list 120 permit ip 10.1.1.0 0.0.0.255
10.2.2.0 0.0.0.255
```

IPSEC debugs and show commands

Cisco.com

Debugs

- Debug crypto isakmp
- Debug crypto ipsec
- Debug crypto engine

Show commands

- Show crypto isakmp sa
- Show crypto ipsec sa
- Show crypto map

How to read an IPSEC config

- *The router can be visualized as going through the IPSEC router config as follows:*

- **Route the traffic to the outgoing interface**

- **If the interface has a crypto map configured on it, go to that crypto map**

- **Go to the access list specified by that crypto map**

- **If the traffic matches that access list then negotiate an IPSEC tunnel with the peer specified in the crypto map based on the configured transform set and ISAKMP policy**

- **Send traffic out the IPSEC tunnel**

Some useful URLs

http://www.cisco.com/warp/public/707/index.shtml

http://www.cisco.com/warp/public/cc/techno/protocol/ipsecur/ipsec/prodlit/dplip_in.htm

http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fipsenc/index.htm

Cisco Systems

Empowering the Internet Generation