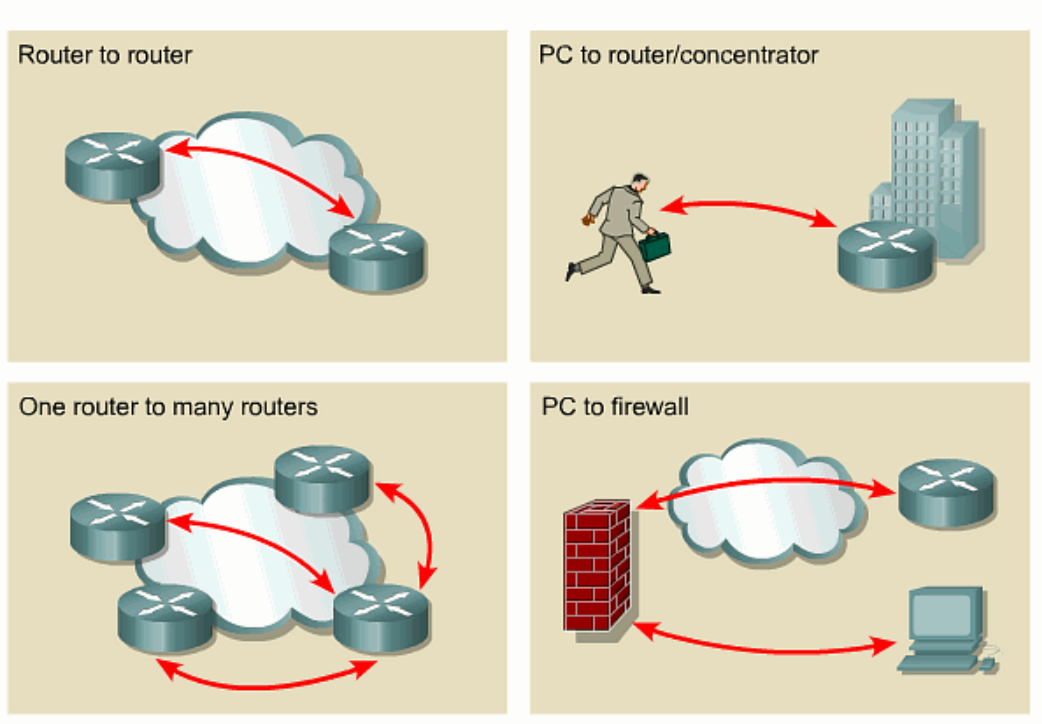


VPN

Olga Torstensson

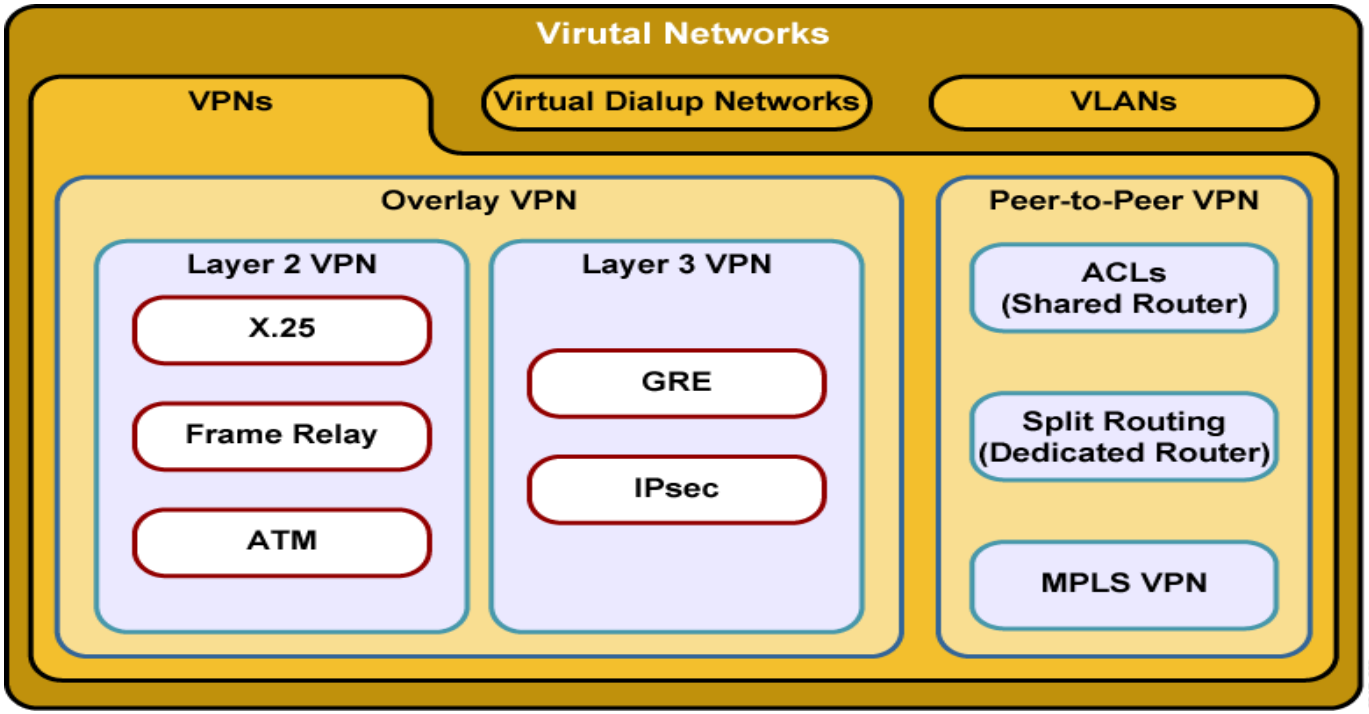
IDE

Halmstad University

What is a VPN?

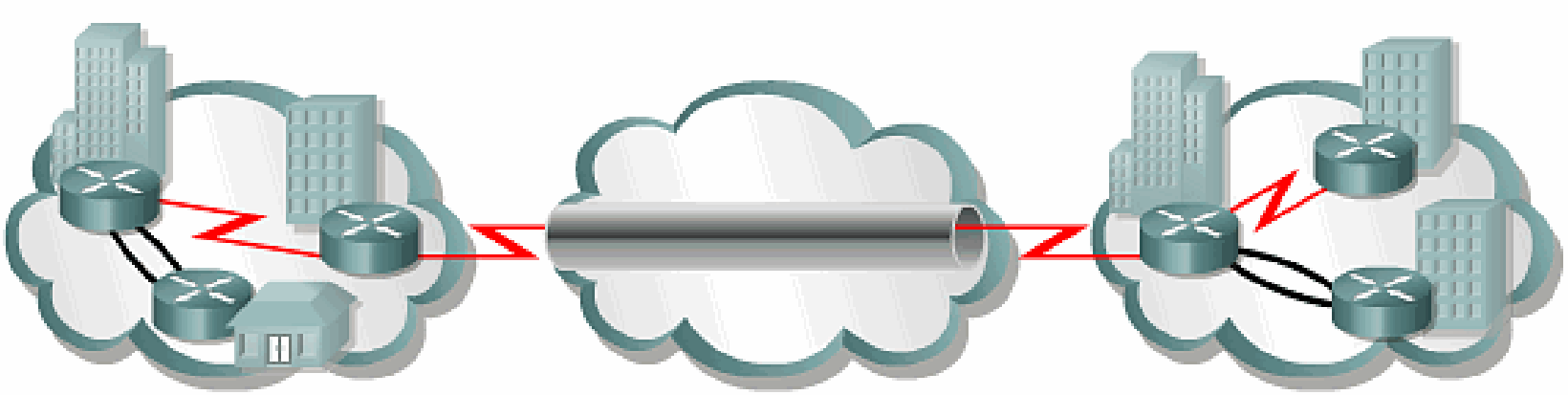
- ***A Virtual Private Network (VPN) is*** defined as network connectivity deployed on a shared infrastructure with the same policies and security as a private network.

VPN Taxonomy



- Overlay VPNs—Service providers provide virtual point-to-point links.
- Peer-to-peer VPNs—Service providers participate in the customer routing.

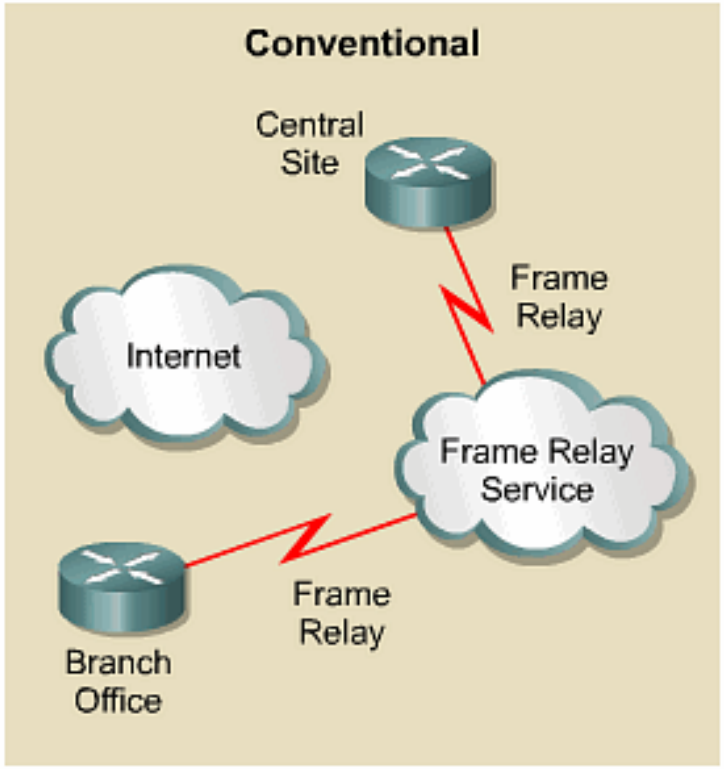
Virtual Private Networks (VPNs)

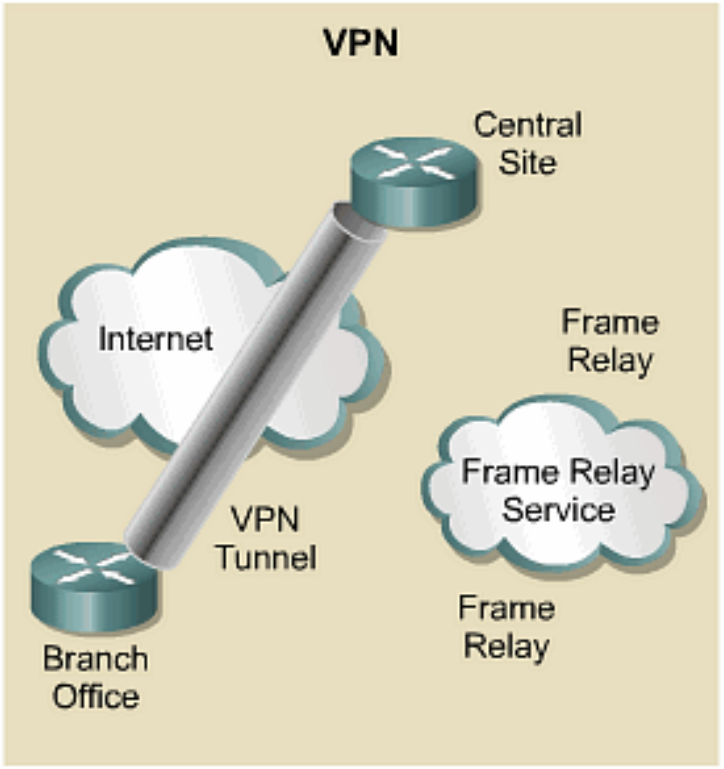


A VPN carries private traffic over a public network using advanced encryption and tunnels to protect:

- Confidentiality of information
- Integrity of data
- Authentication of users

Why Have VPNs?

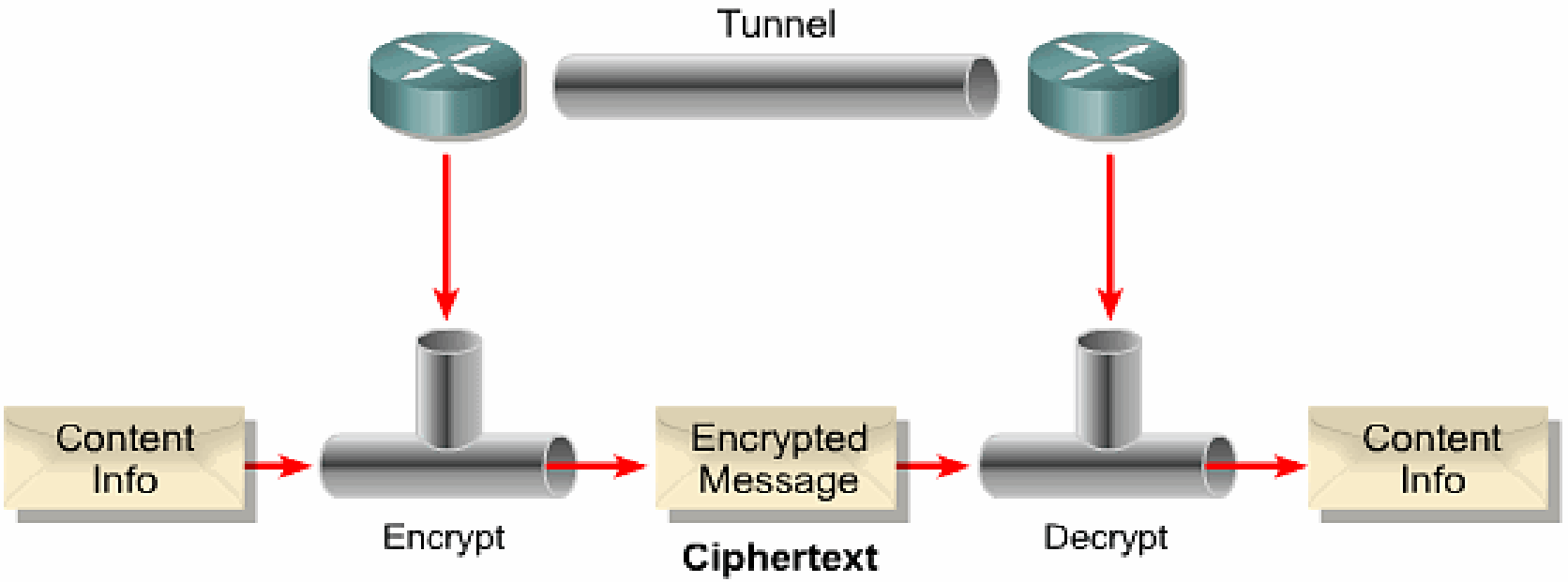




- Higher cost
- Less flexible
- WAN management
- Complex topologies

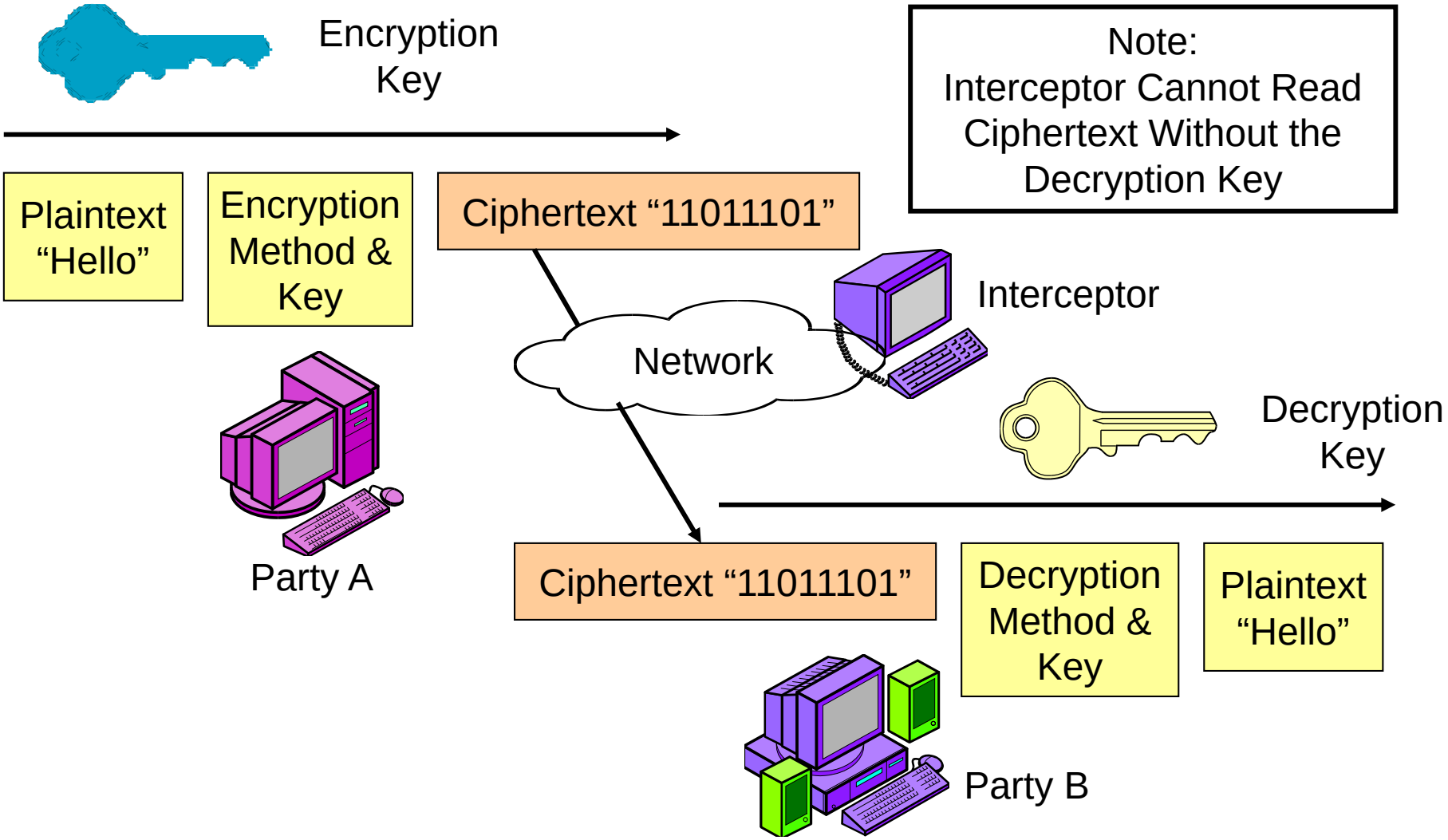
- Lower cost
- More flexible
- Simpler management
- Tunnel topology

Tunneling and Encryption

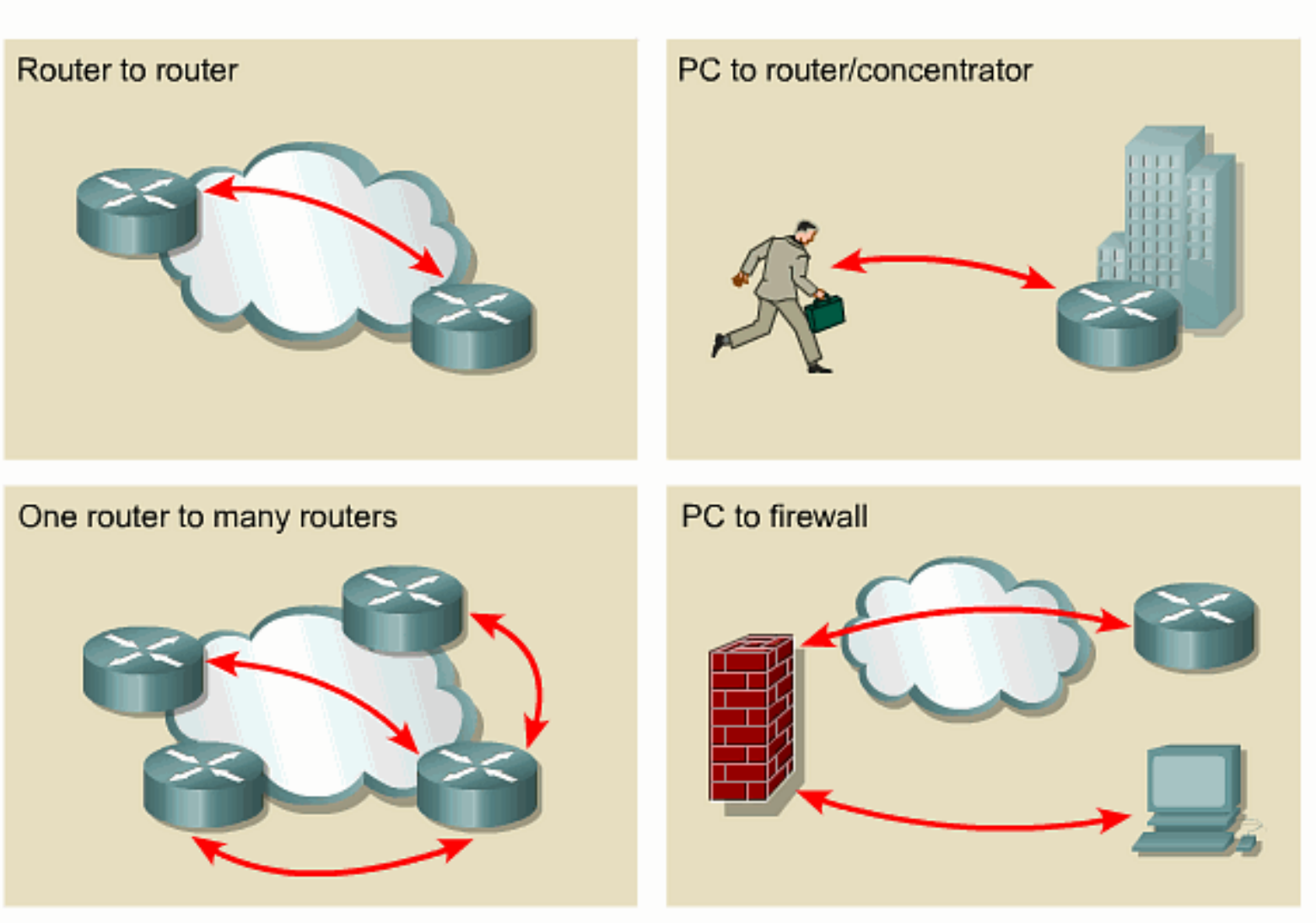


- A tunnel is a virtual point-to-point connection
- A tunnel carries one protocol inside another protocol
- Encryption transforms content information into ciphertext
- Decryption restores content information from ciphertext

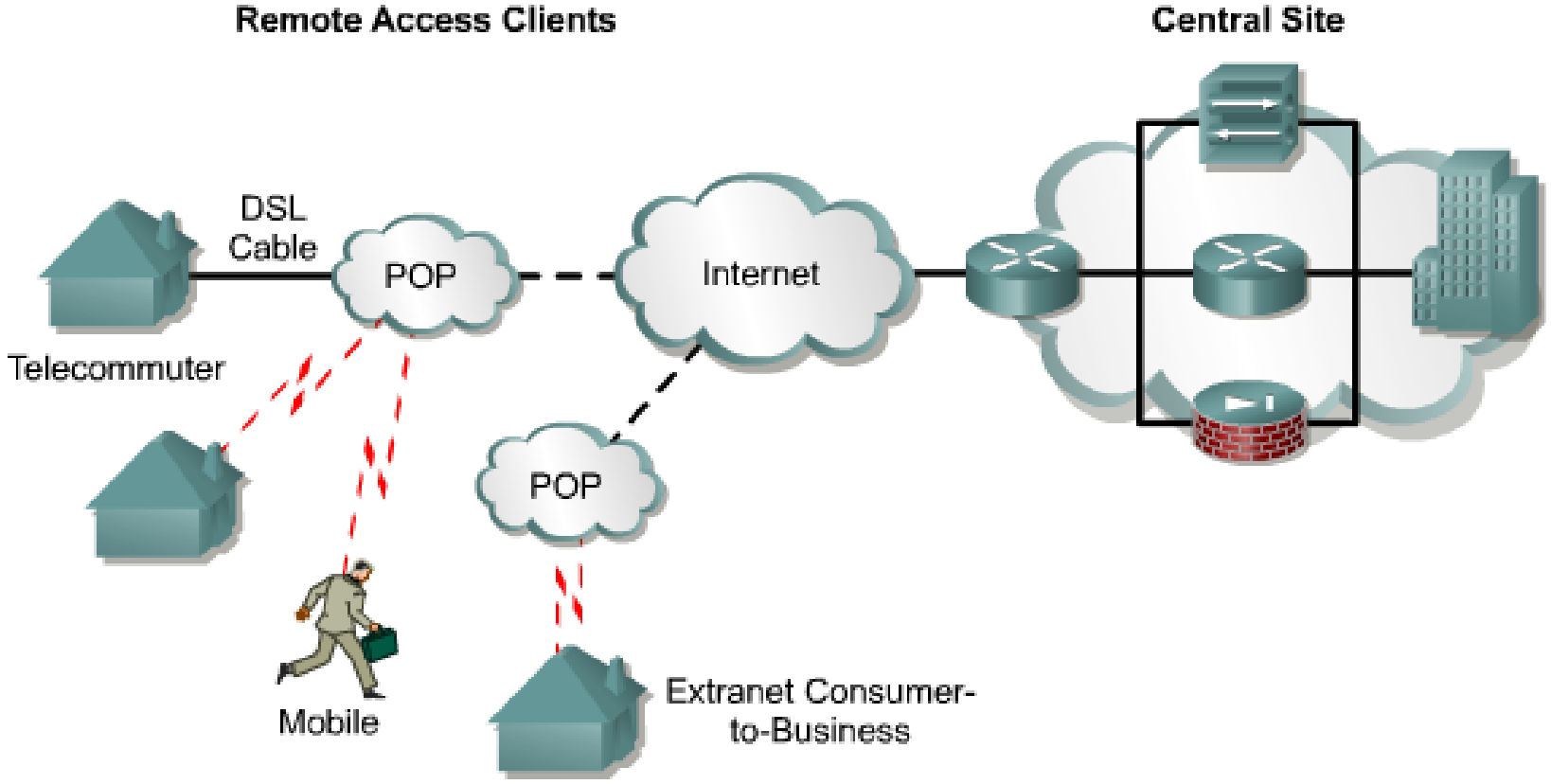
Plaintext, Encryption, Ciphertext, and Decryption



Use VPNs with a Variety of Devices

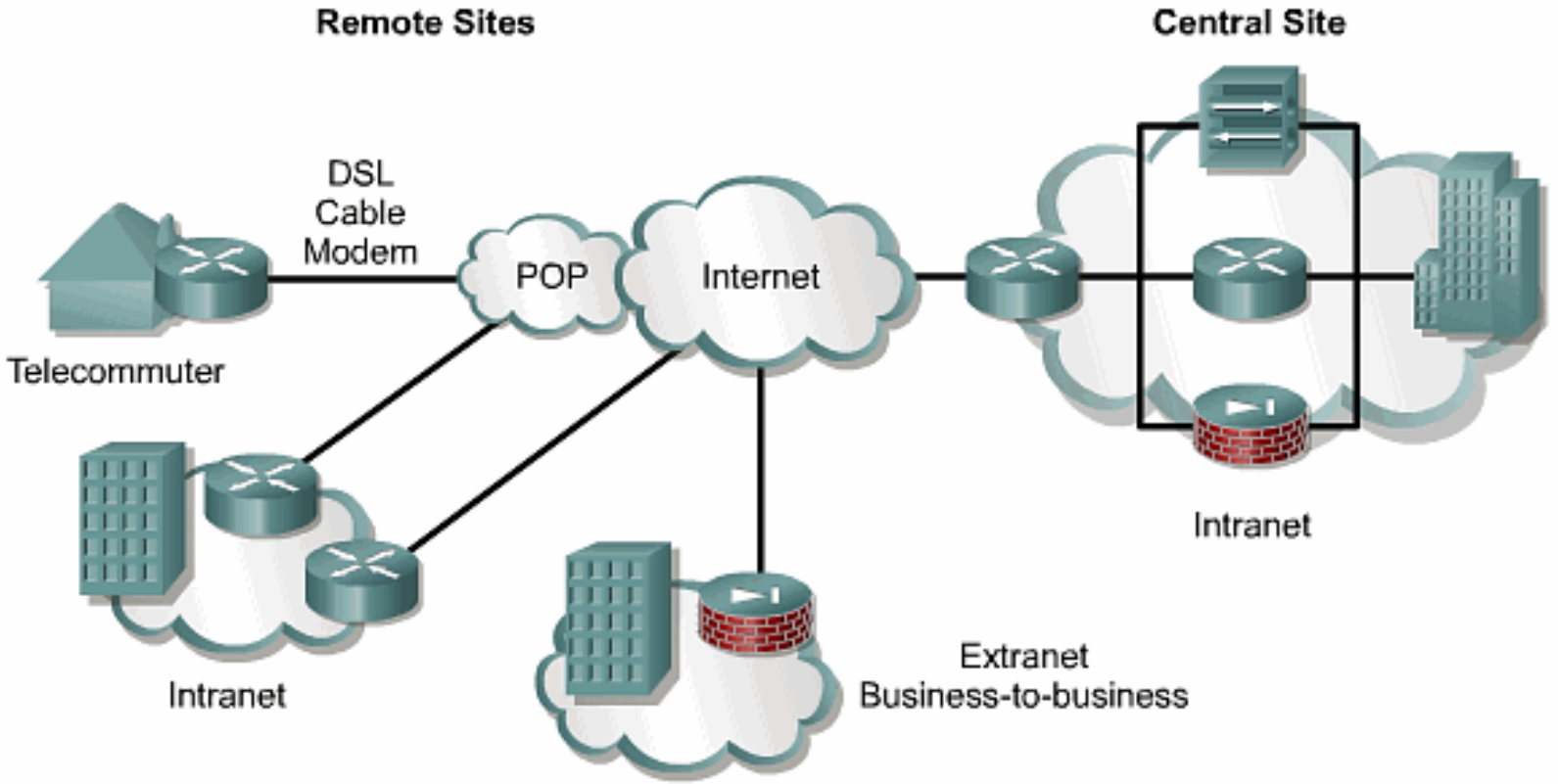


VPN Types
Remote Access VPN Solutions



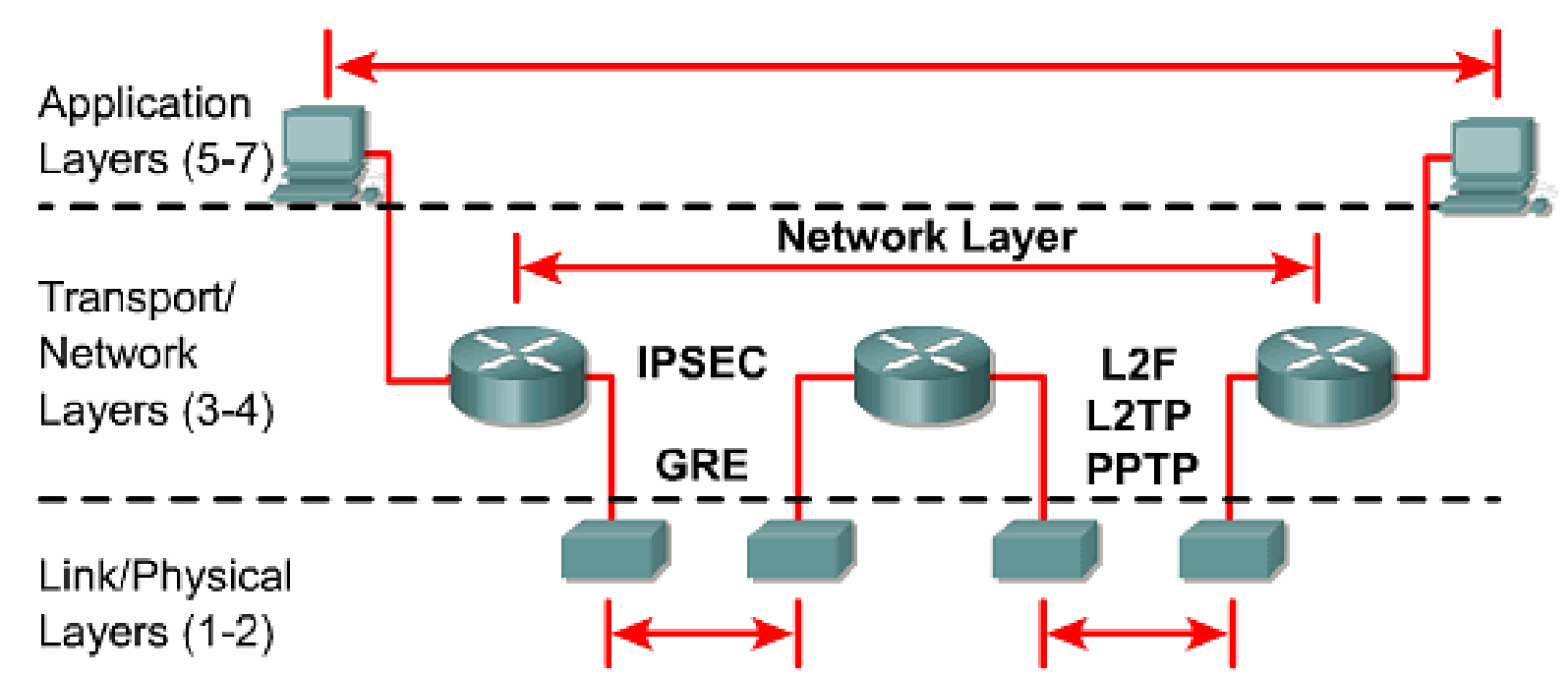
Extension of classic WAN

Site-to-Site VPN Solutions



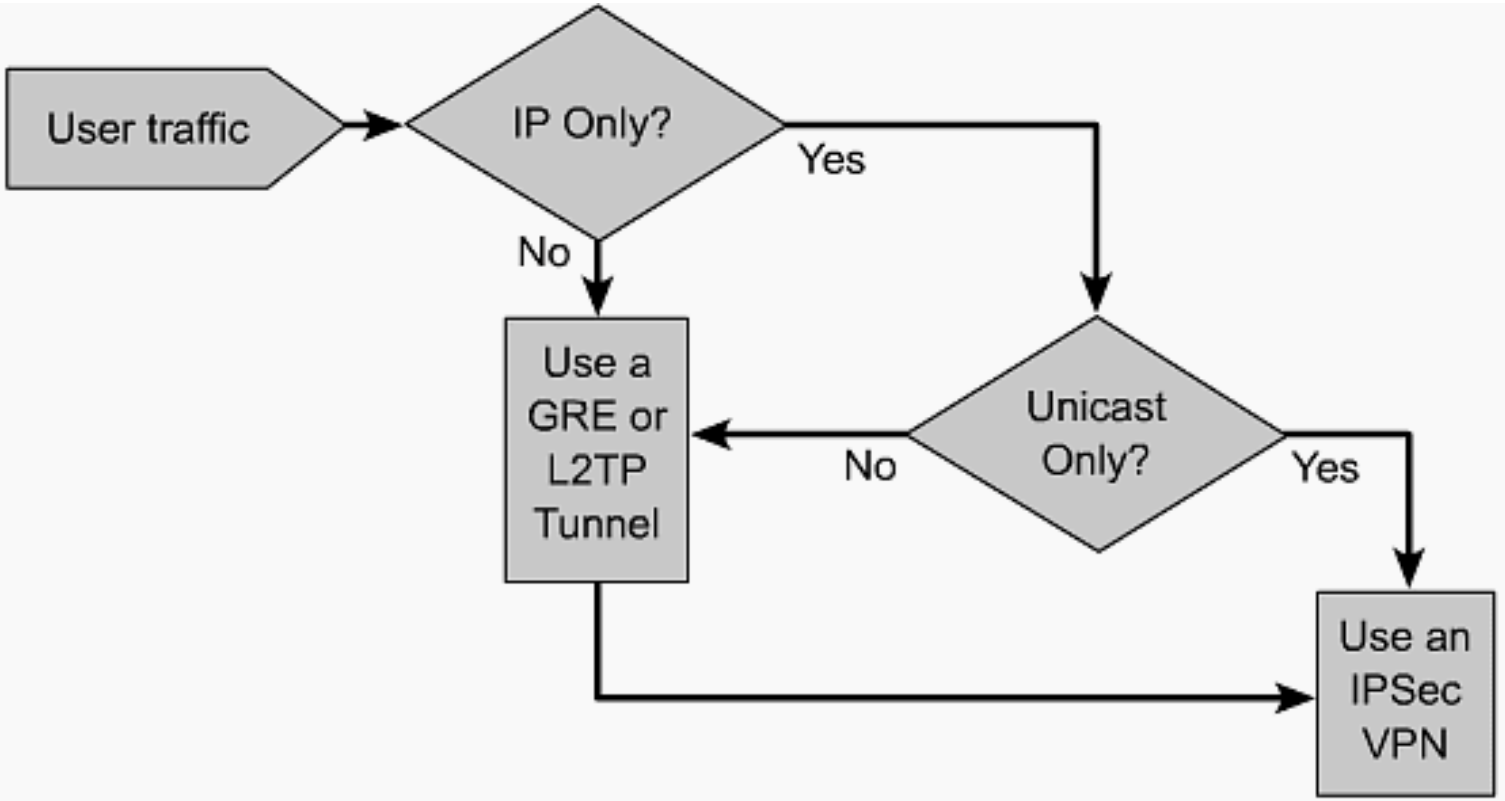
Extension of classic WAN

Tunneling Protocols



VPN Protocols	Description	Standard
L2TP	Layer 2 Tunneling Protocol	RFC 2661
GRE	Generic Routing Encapsulation	RFC 1701 and 2784
IPSec	Internet Protocol Security	RFC 2401

Selecting Layer 3 VPN Tunnel Options



Note: For multiple traffic types use VPN option combinations.

Identifying VPN and IPSec Terms

- **Tunnel**
- **Encryption/Decryption**
- **Cryptosystem**
- **Hashing**
- **Authentication**
- **Authorization**
- **Key Management**
- **Certificate of Authority Service**

Identifying VPN and IPSec Terms

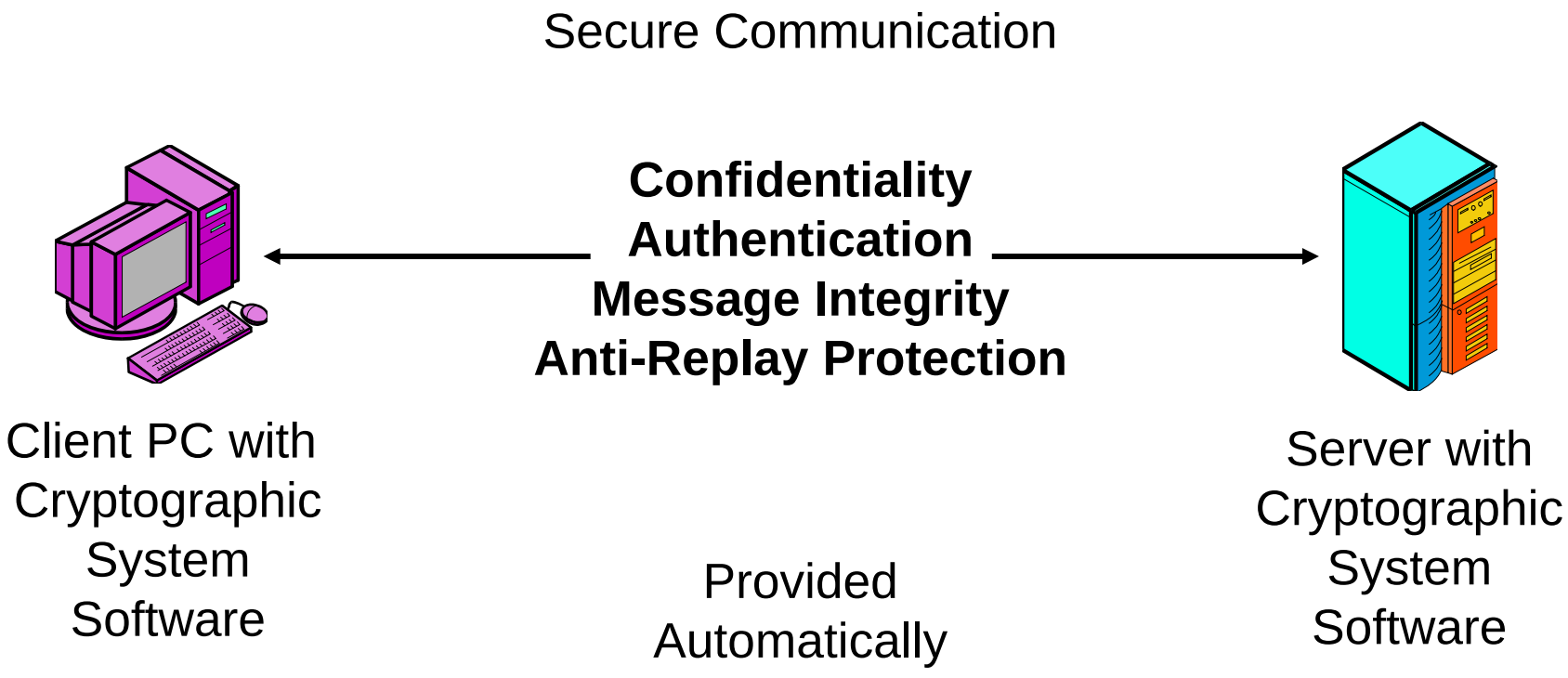
IPSec main protocols are used to provide protection for user data:

- **Authentication Header – AH**
- **Encapsulating Security Payload – ESP**

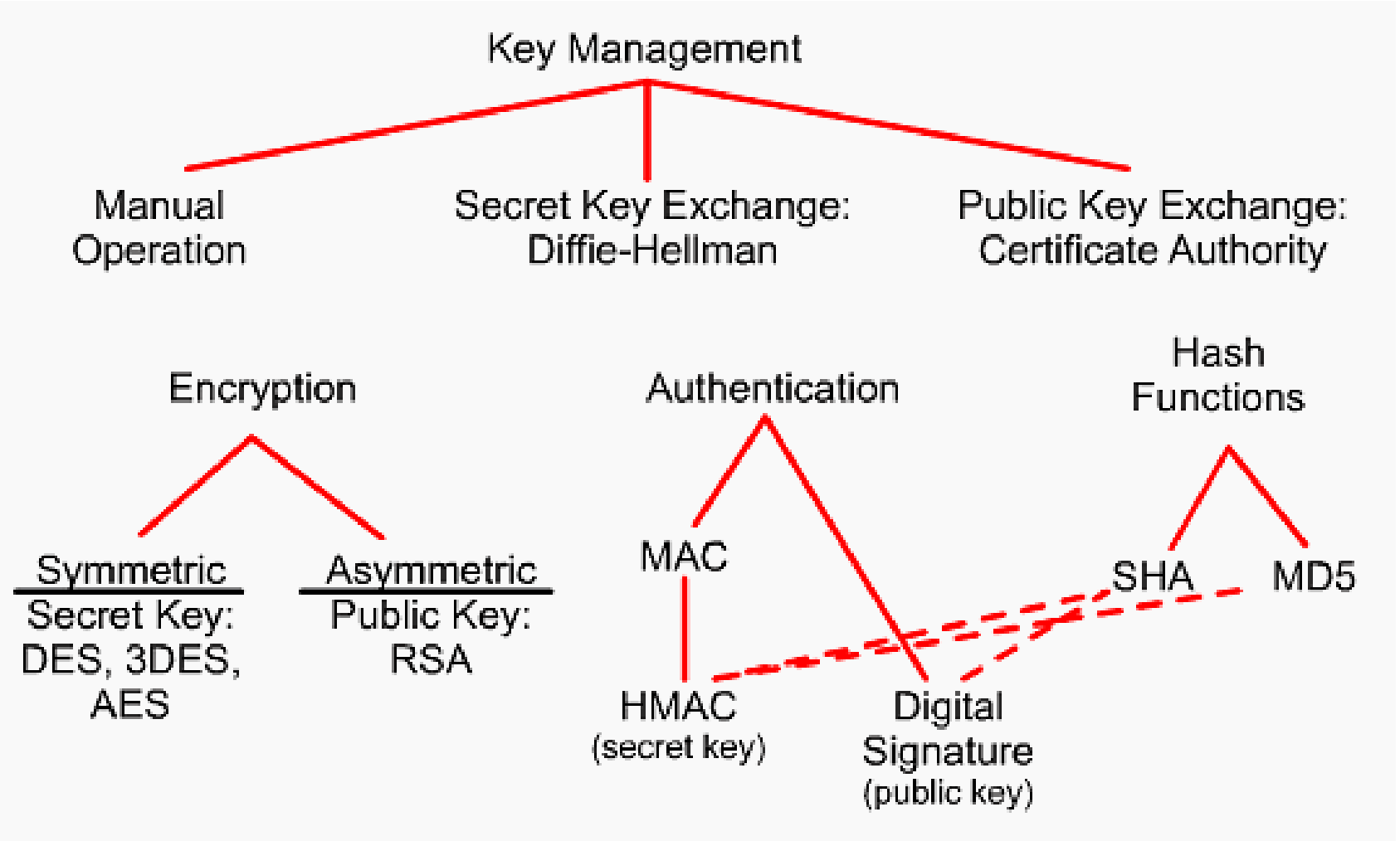
Internet Key Exchange – IKE

Internet Security Association Key Management Protocol – ISAKMP

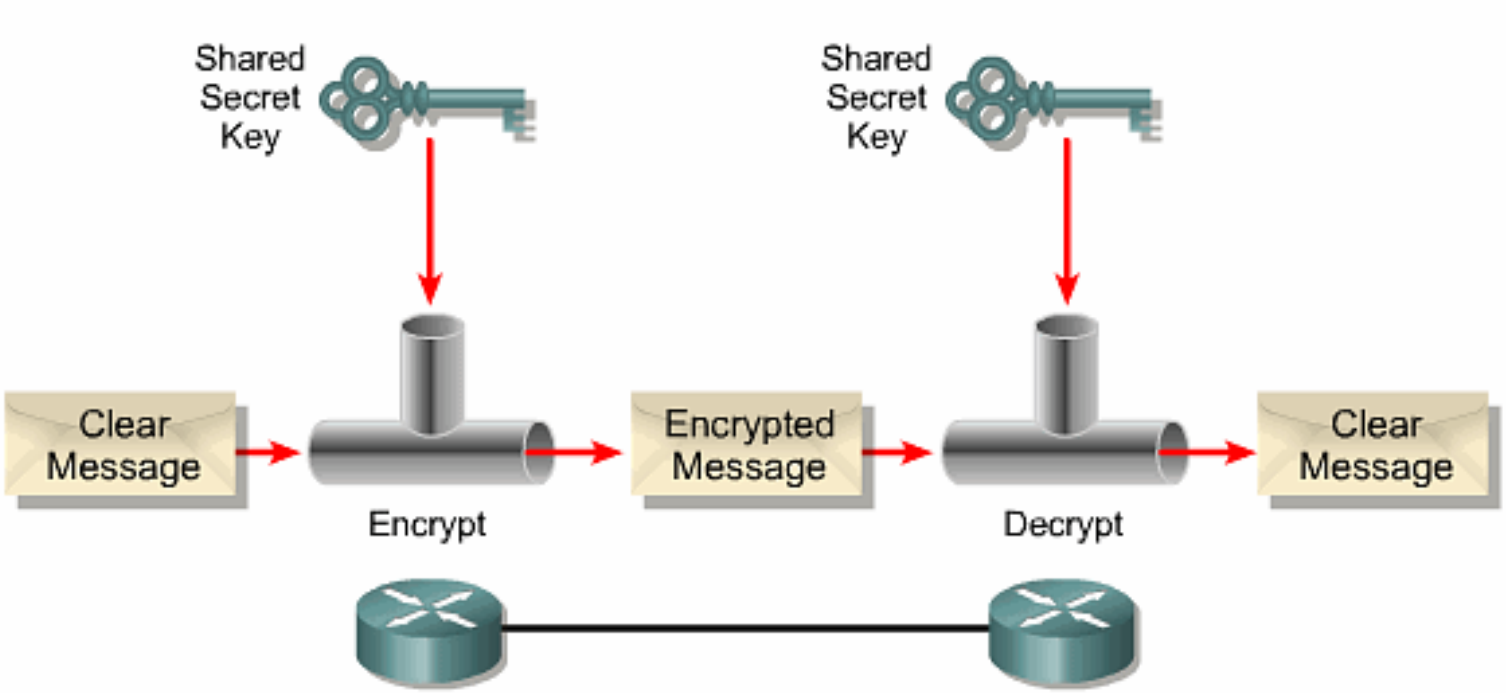
Cryptographic System



Cryptosystem Overview

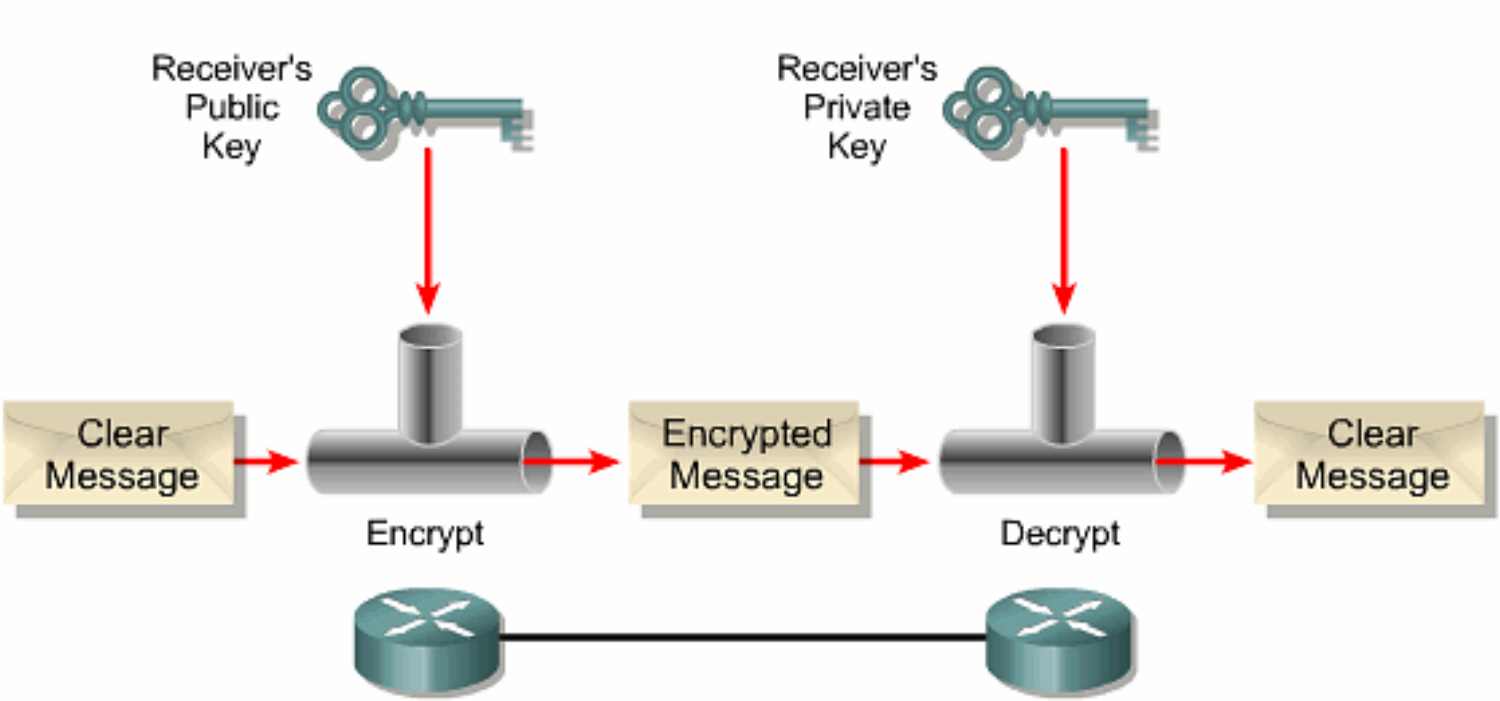


Symmetric Encryption



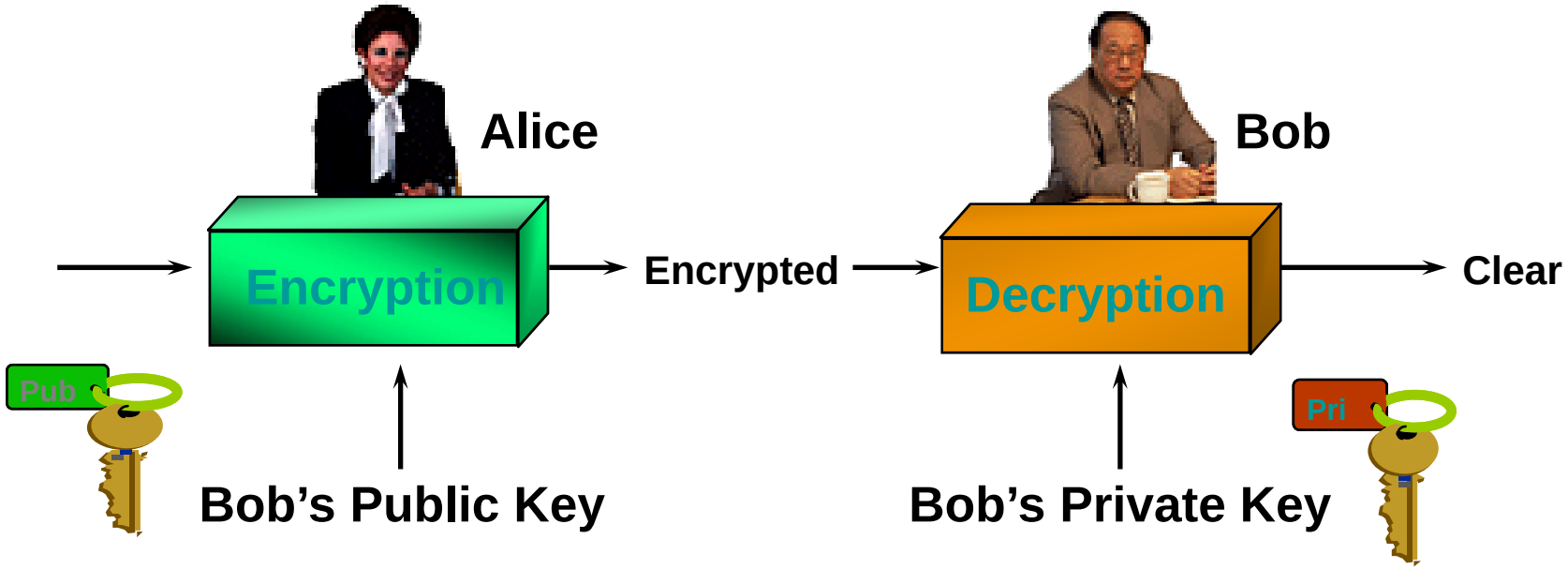
- Encryption turns clear text into ciphertext
- Decryption restores clear text from ciphertext
- Keys enable encryption and decryption

Asymmetric Encryption



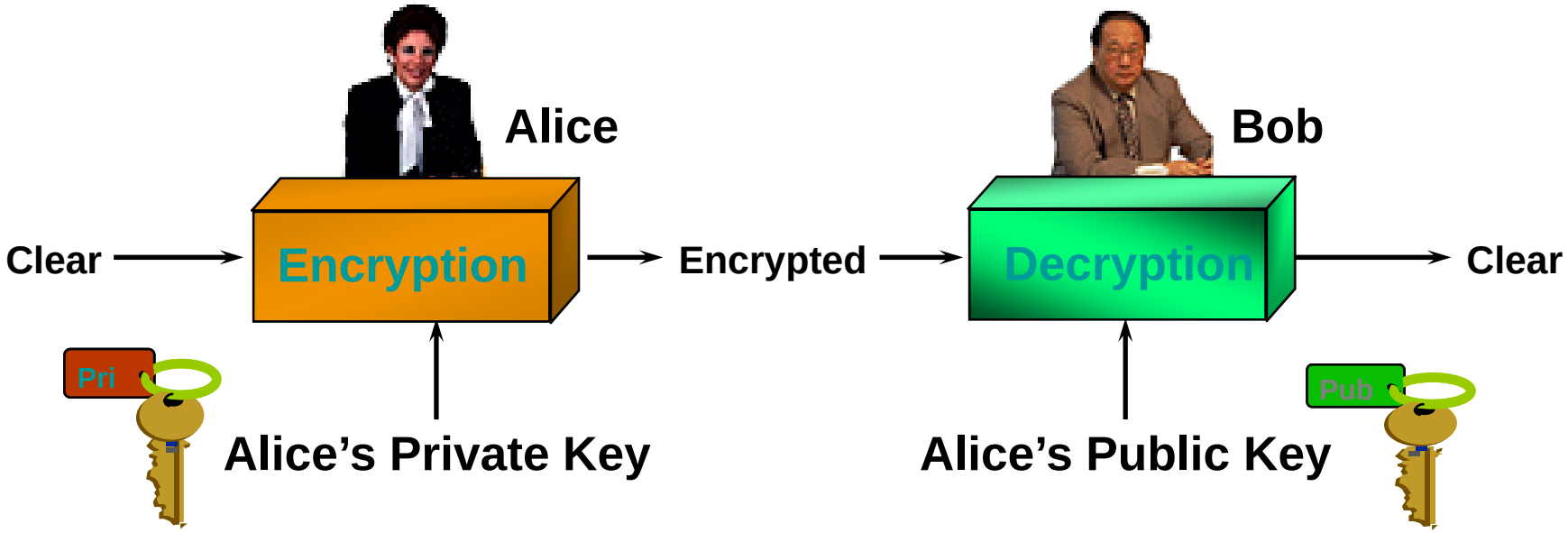
- Private key is known only to receiver
- Public key is known to public
- Public key distribution is not a secret operation

RSA encryption (privacy)



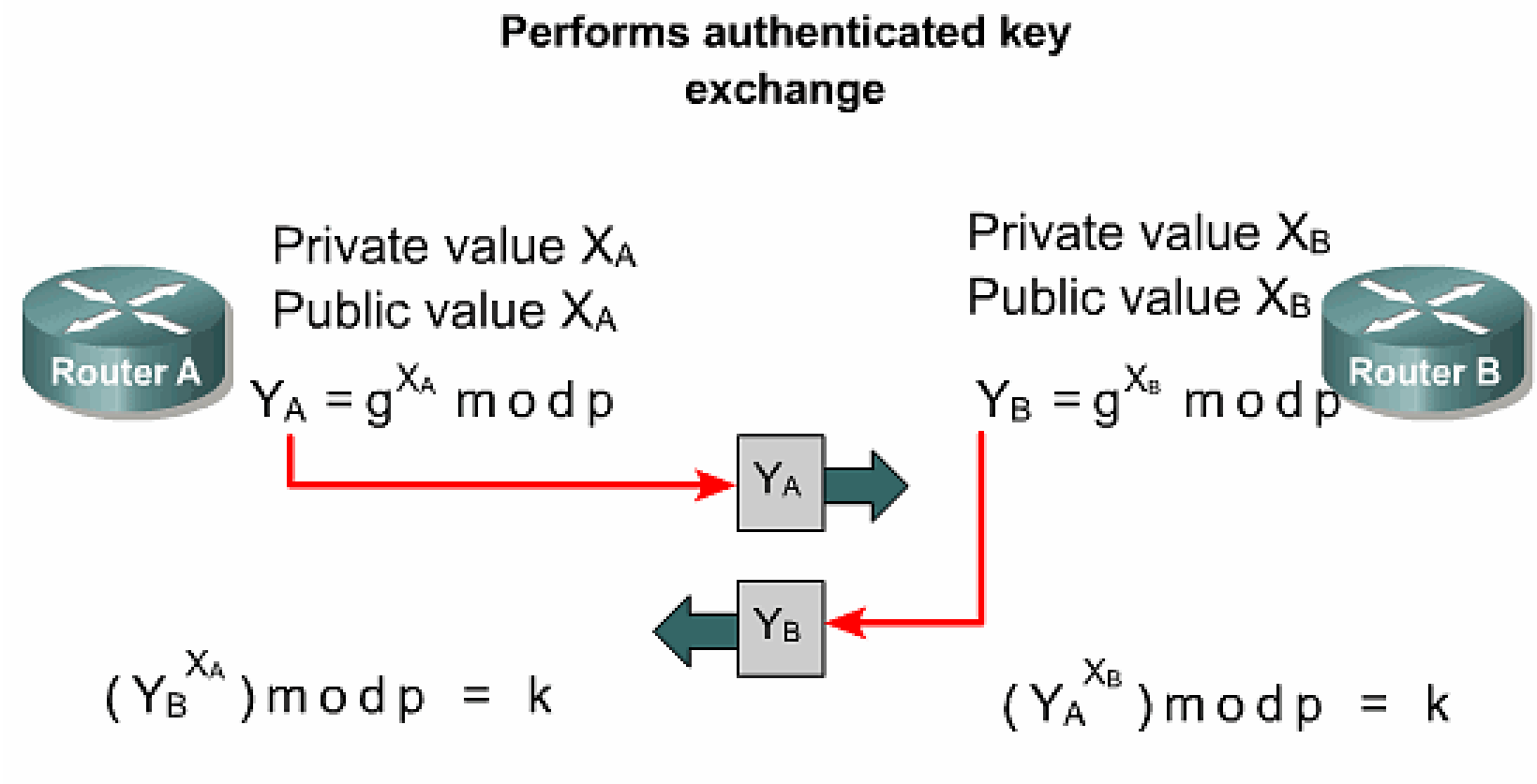
- Alice gets Bob's public key
- Alice encrypts message with Bob's public key
- Bob decrypts message using his private key

RSA signatures (authentication)

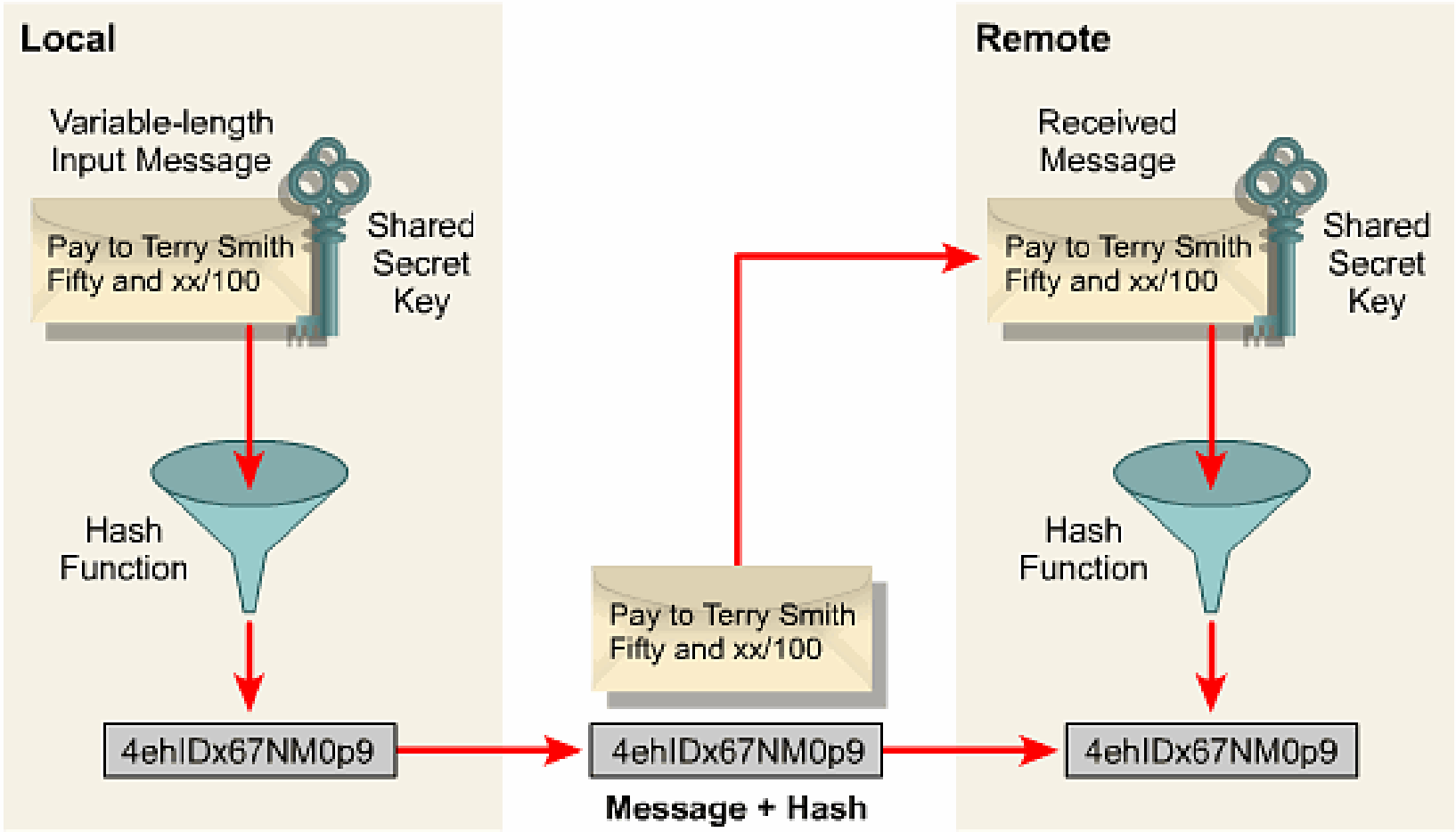


- **Alice encrypts message with her private key**
- **Bob gets Alice's public key**
- **Bob decrypts message using Alice's public key**

Key Exchange – Diffie-Hellman Algorithm



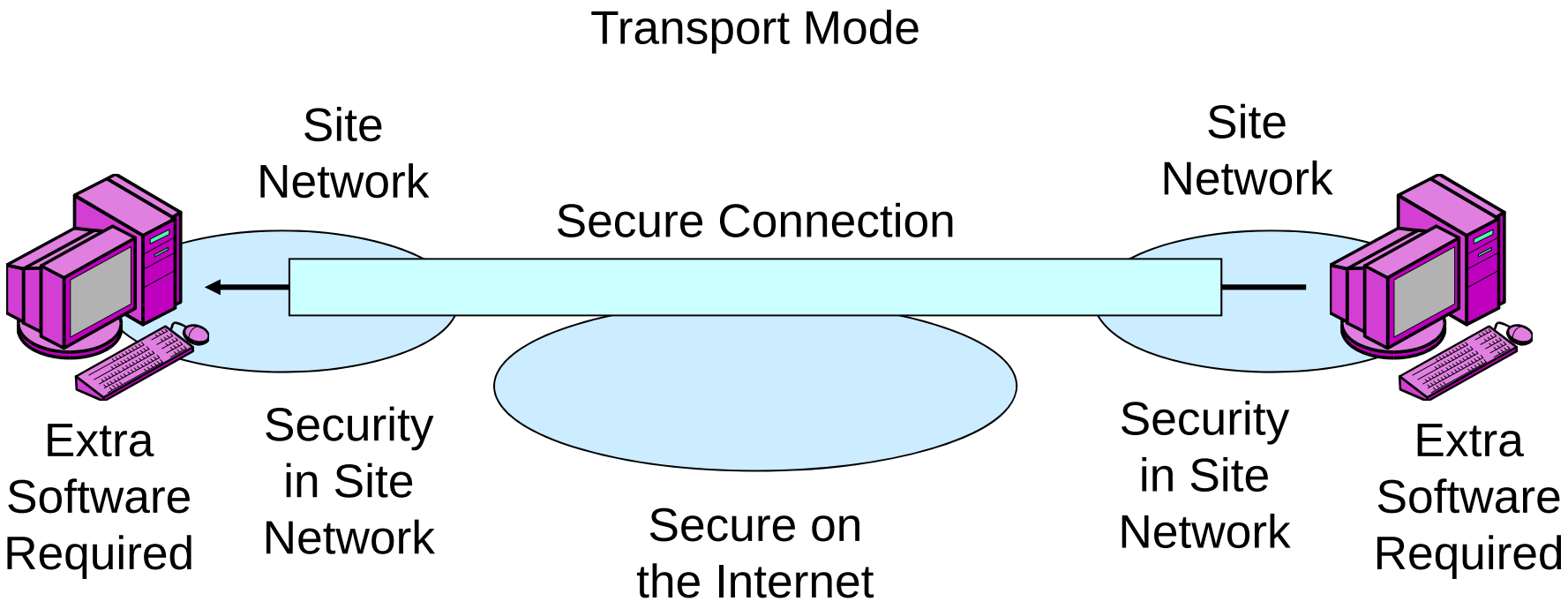
Hashing


Local
Variable-length
Input Message
Pay to Terry Smith
Fifty and xx/100
Shared
Secret
Key
Hash
Function
4ehIDx67NM0p9
Pay to Terry Smith
Fifty and xx/100
4ehIDx67NM0p9
Message + Hash
Remote
Received
Message
Pay to Terry Smith
Fifty and xx/100
Shared
Secret
Key
Hash
Function
4ehIDx67NM0p9

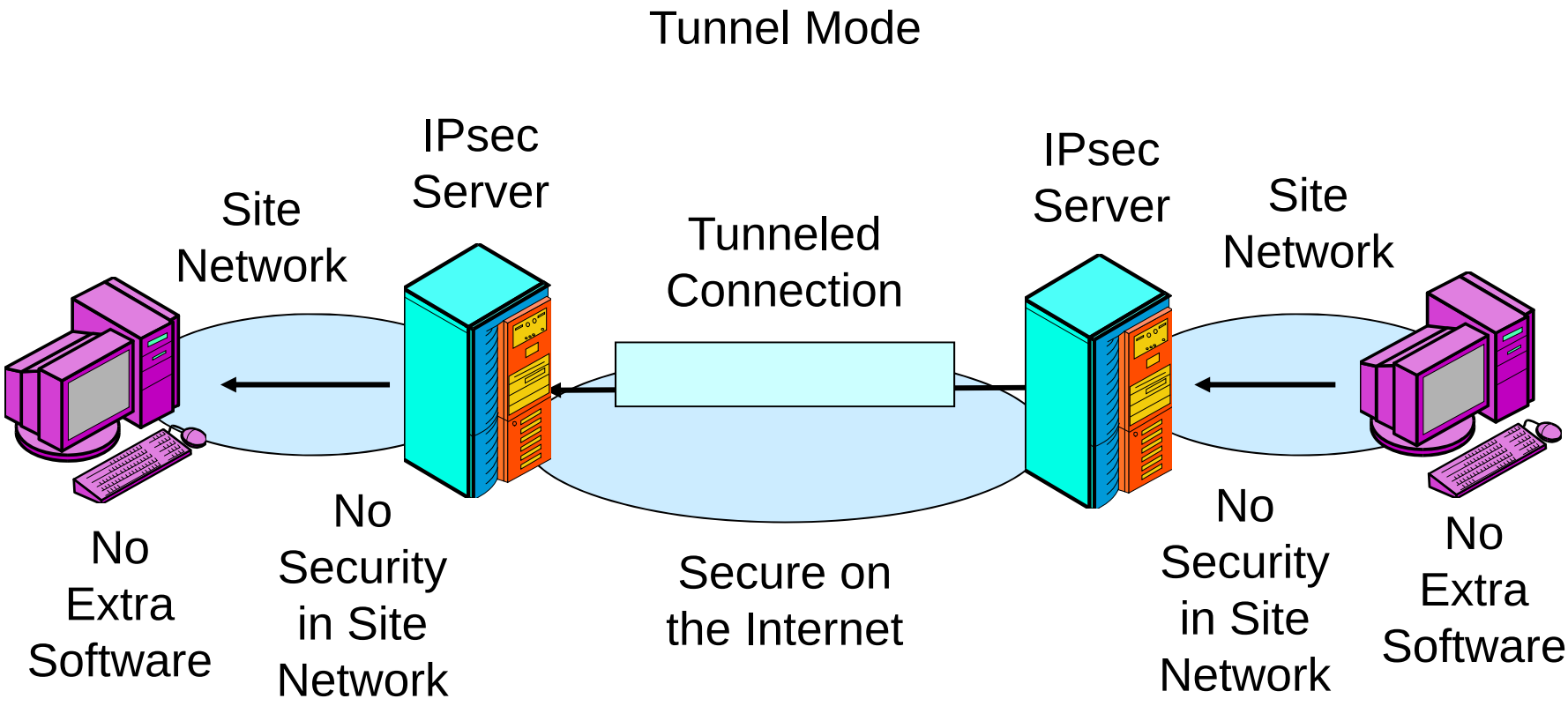
Encryption Versus Hashing

	Encryption	Hashing
Use of Key	Uses a key as an input to an encryption method	Key is usually added to text; the two are combined, and the combination is hashed
Length of Result	Output is similar in length to input	Output is of a fixed short length, regardless of input
Reversibility	Reversible; ciphertext can be decrypted back to plaintext	One-way function; hash cannot be “de-hashed” back to the original string

IPsec Operation: Tunnel and Transport Modes



IPsec Operation: Tunnel and Transport Modes



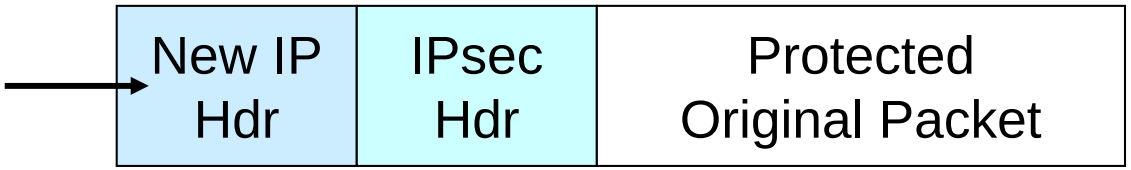
IPsec Operation: Tunnel and Transport Modes

Transport Mode

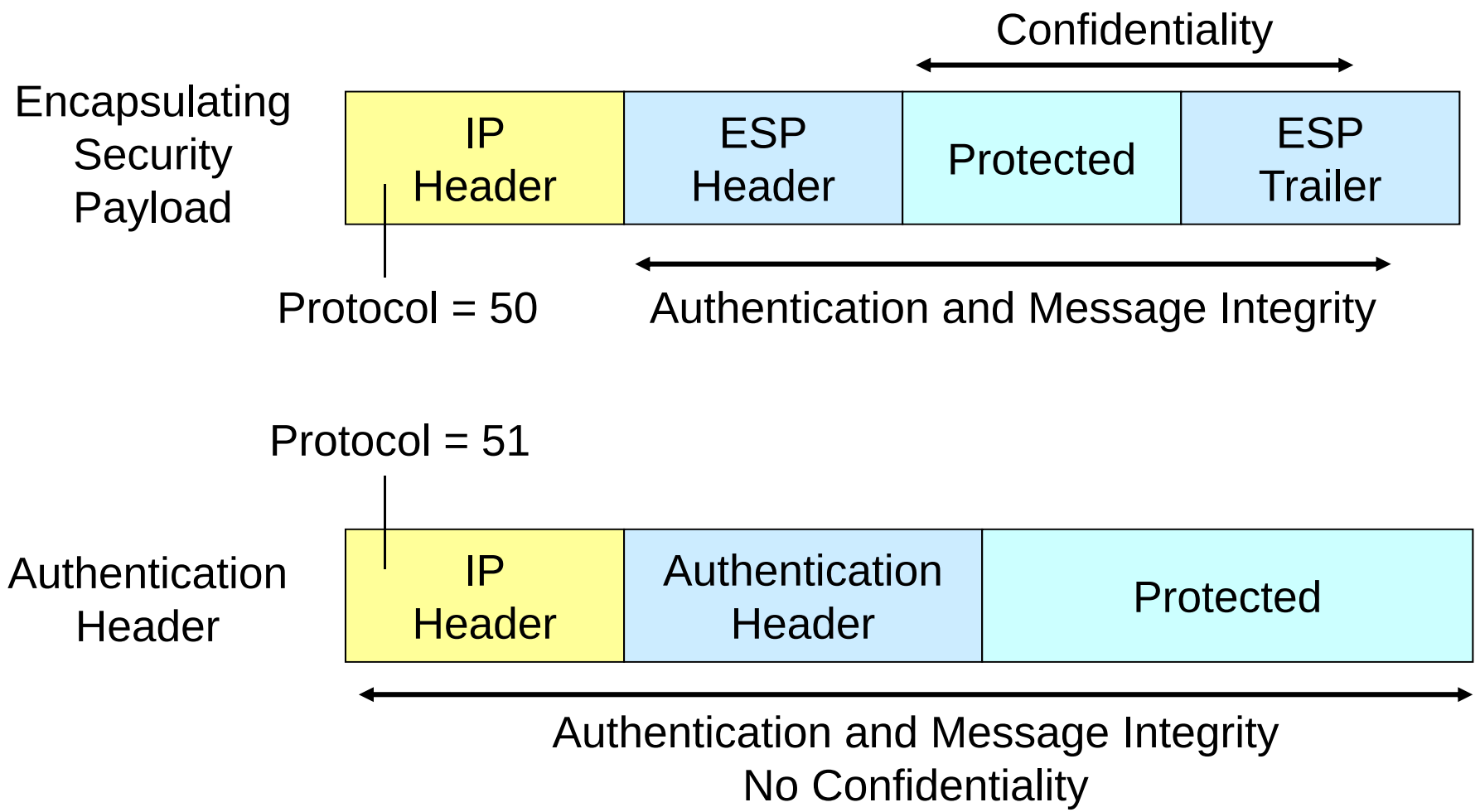
Destination IP Address
Is Actual Address;
Vulnerable to Scanning

Tunnel Mode

Destination IP Address is
IPsec Gateway Address
Host IP Address
Is not Revealed

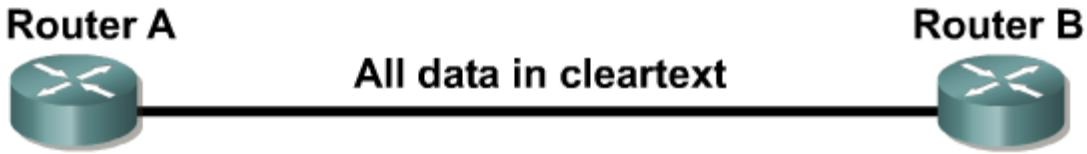


IPsec ESP and AH Protection



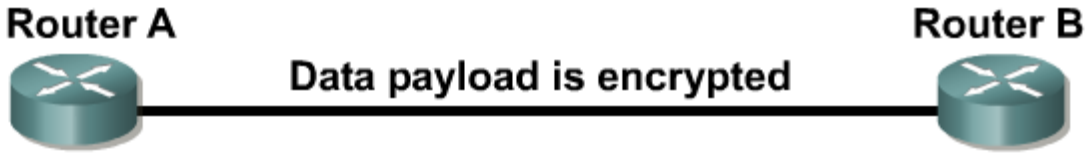
IPSec Security Protocols

Authentication Header



- Ensures data integrity
- Provides origin authentication - ensures packets definitely came from peer router
- Uses keyed-hash mechanism
- Does NOT provide confidentiality (no encryption)
- Provides optional replay protection

Encapsulating Security Payload



- Data confidentiality (encryption)
- Limited traffic flow confidentiality
- Data integrity
- Optional data origin authentication
- Anti-replay protection
- Does not protect IP header

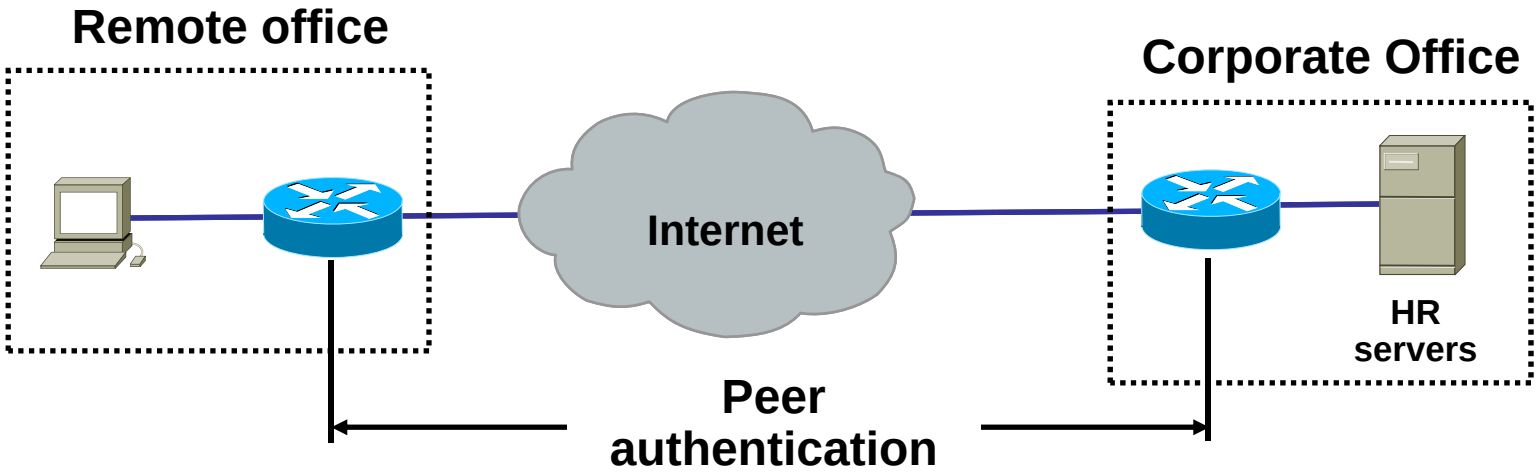
IPSEC Concepts

- Peers
- Transform sets
- Security Associations
- Transport and Tunnel modes
- Authentication Header (AH) & Encapsulating Security Payload (ESP)

Peers

A *peer* of an IPSEC device is another device participating in IPSEC. A peer can be a router, firewall, server or some remote *PC* with IPSEC support.

***Peering* between two IPSEC device is usually a point to point relationship**



- Peer authentication methods:
  - Pre-shared keys
  - RSA signatures

Peer Authentication

Transform Sets

- A *transform set is a list of IPsec protocols and cryptographic algorithms that a peer can accept. Because IPsec allows for the use of different protocols and algorithms, a peer needs to declare and negotiate with other peers what it can support.*

- *Peers communicate the protocols and algorithms they support by exchanging transform sets. For two peers to communicate successfully, they must share a common transform set, otherwise peering fails.*

A Transform Set

- An IPsec security protocol, *AH* or *ESP* or both
- An integrity/Authentication algorithm

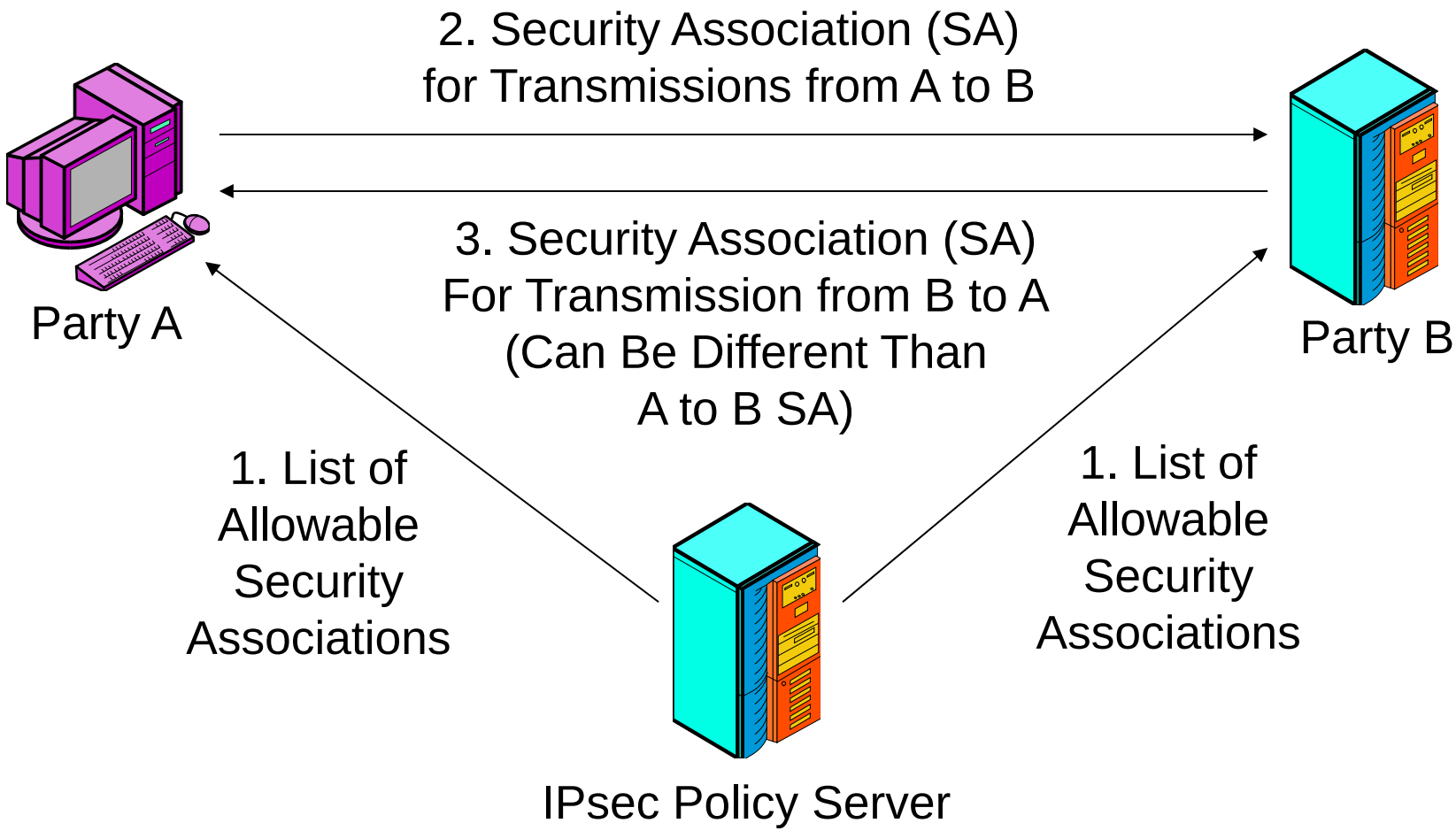
  ie MD5 HMAC or SHA-1 HMAC
- An encrypting algorithm DES, 3DES.

  A null encryption algorithm is also supported.

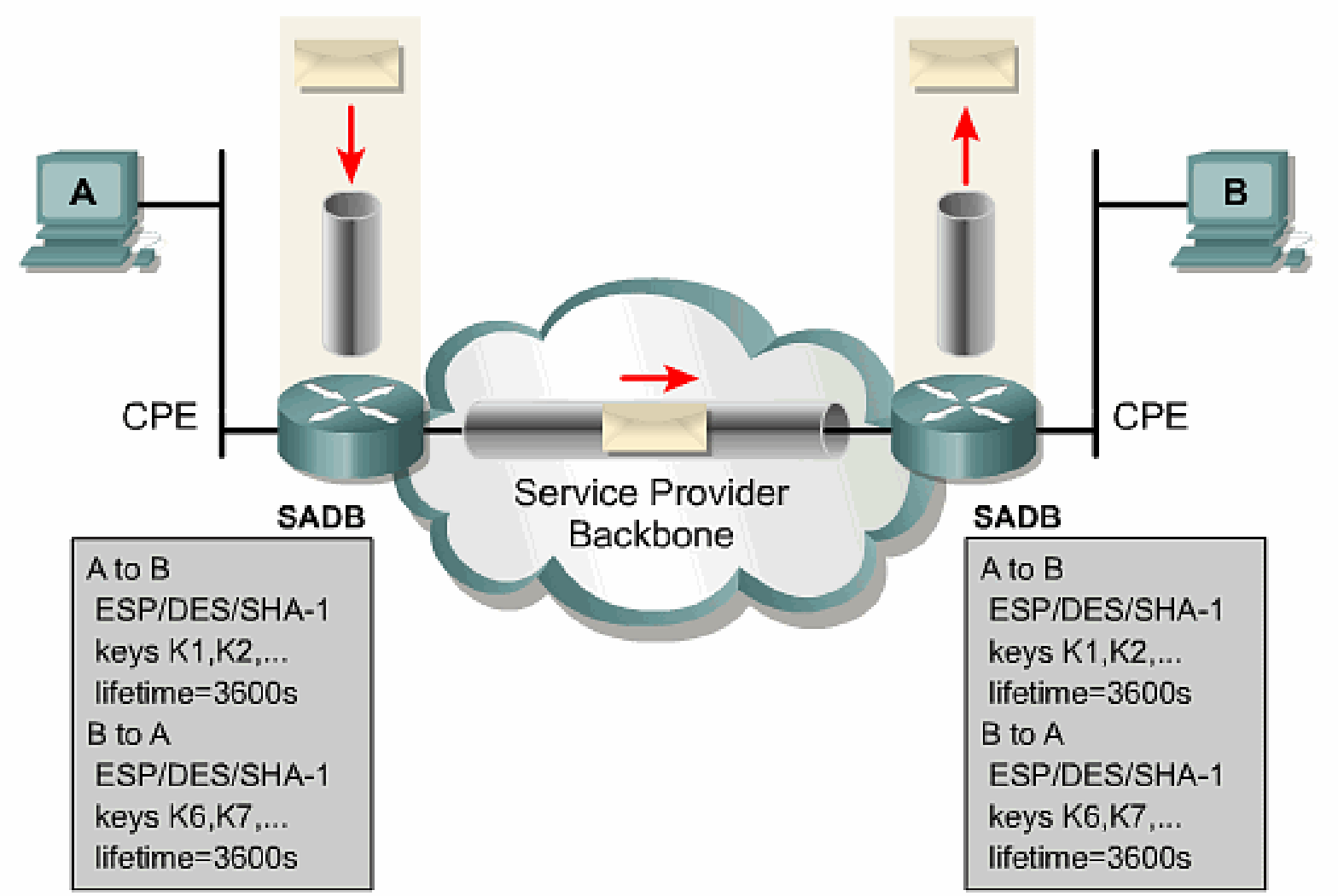
Security Association

- A *Security Association (SA)* is a logical connection that provides data flowing from one peer to another by using a transform set. Security associations are like logical tunnels between peers. Traffic entering an *SA* is protected and transported to the other side.

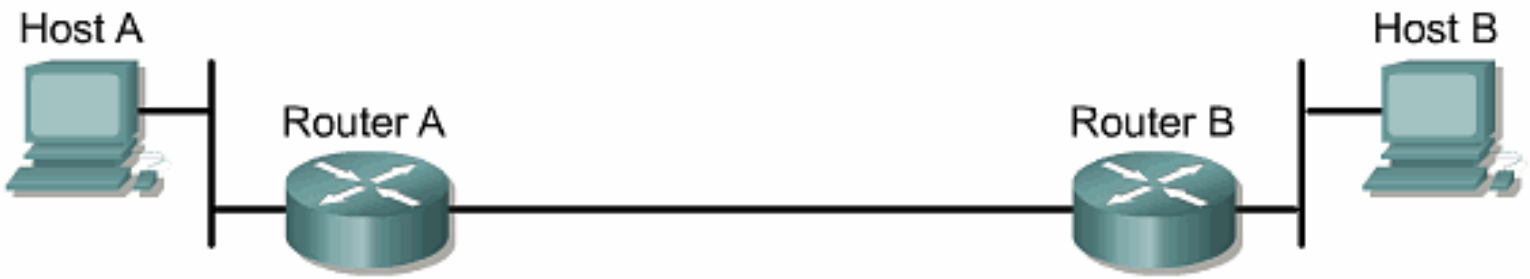
IPsec Security Associations



Security Association

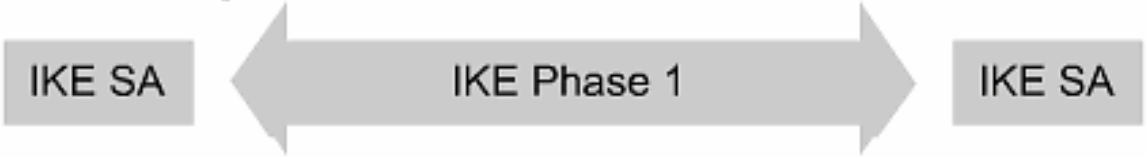


Five steps of IPSec



1. Host A sends interesting traffic to Host B.

2. Router A and B negotiate an IKE Phase 1 session.

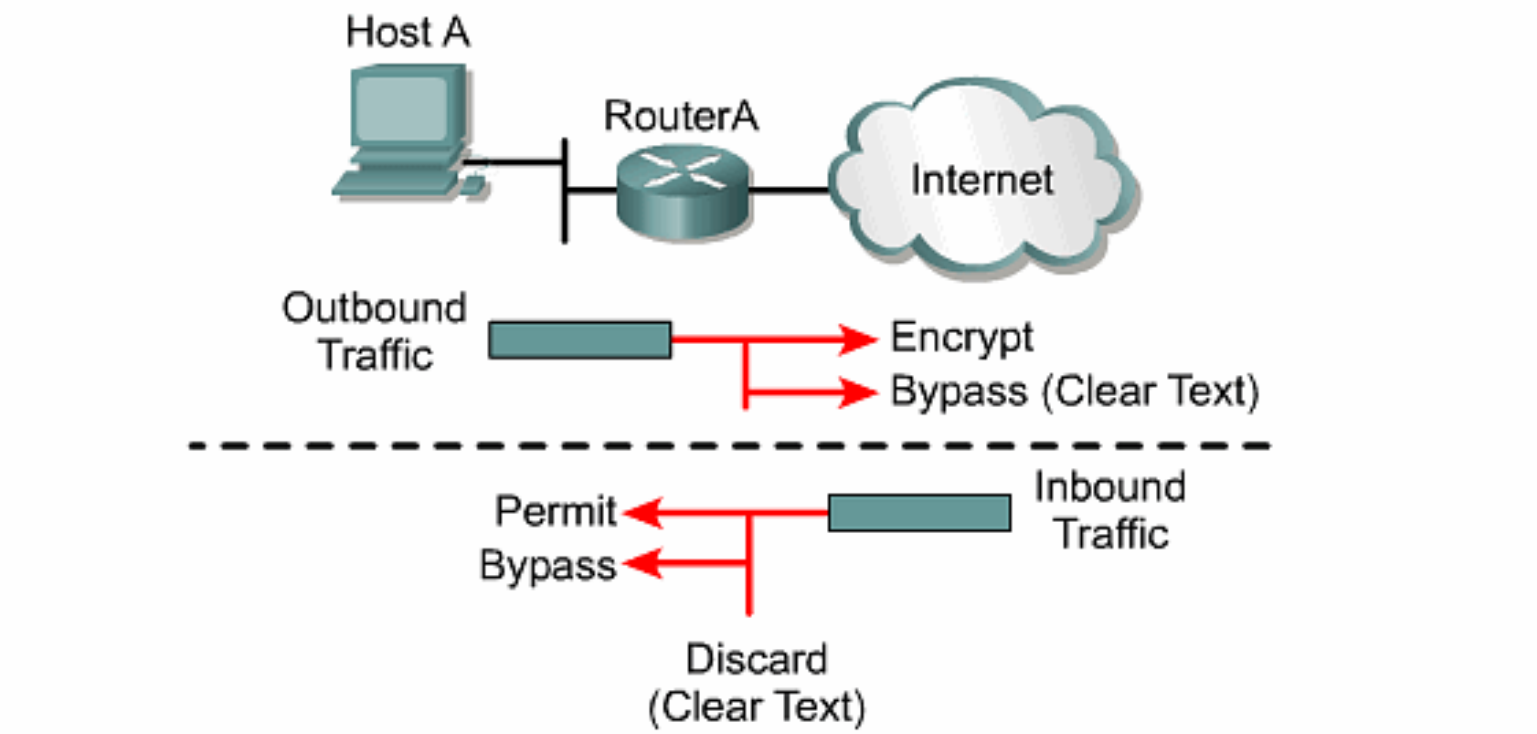


3. Router A and B negotiate an IKE Phase 2 session.

4. Information is exchanged via the IPSec tunnel.

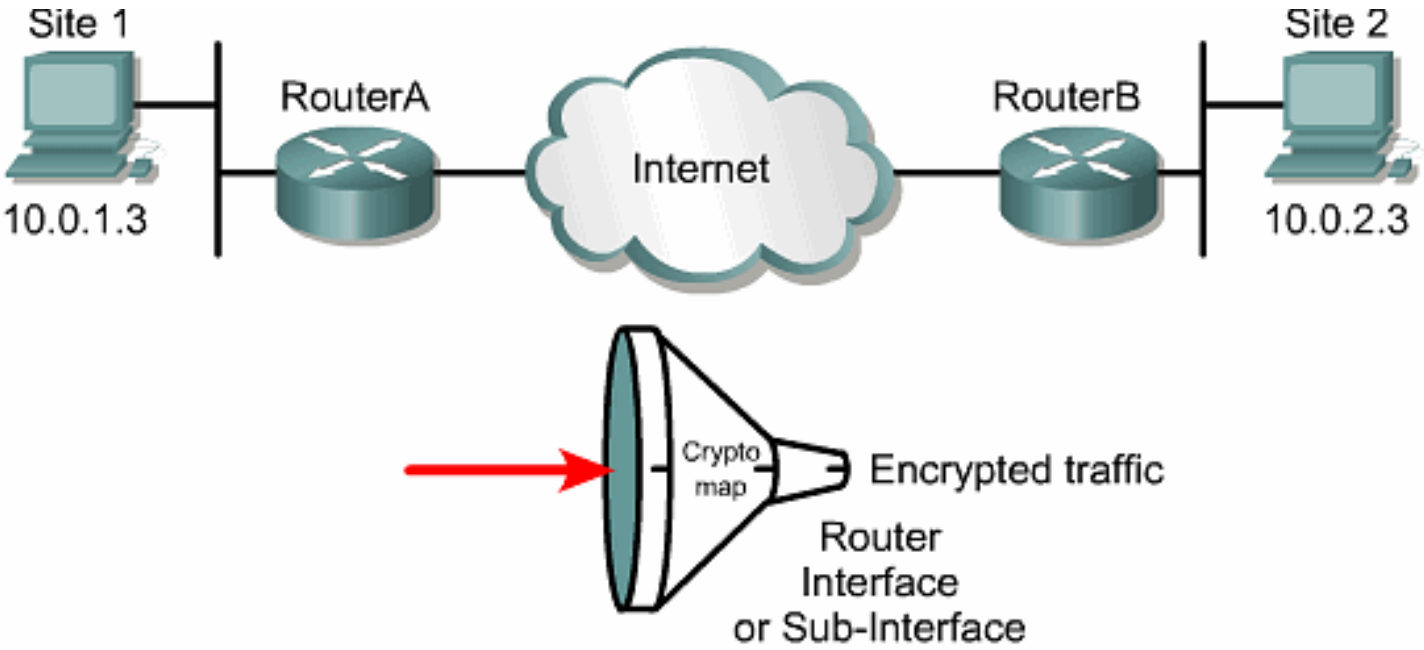
5. The IPSec tunnel is terminated.

Purpose of Crypto ACLs



- Outbound access lists indicate the data flow to be protected by IPSec
- Inbound access lists filter out and discard traffic that should have been protected by IPSec

Crypto Map Parameters



Crypto maps define the following:

- The access list to be used
- Remote VPN peers
- Transform set to be used
- Key management method
- Security association lifetimes

IPSec Configuration Examples


```
RouterA#show running config
crypto ipsec transform-set mine
esp-des
!
crypto map mymap 10 ipsec-isakmp
set peer 172.30.2.2
set transform-set mine
match address 110
!
interface Ethernet 0/1
ip address 172.30.1.2 255.255.255.0
no ip directed-broadcast
crypto map mymap
!
access-list 110 permit tcp 10.0.1.0
0.0.0.255 10.0.2.0 0.0.0.255
```

```
RouterB#show running config
crypto ipsec transform-set mine
esp-des
!
crypto map mymap 10 ipsec-isakmp
set peer 172.30.1.2
set transform-set mine
match address 110
!
interface Ethernet 0/1
ip address 172.30.2.2 255.255.255.0
no ip directed-broadcast
crypto map mymap
!
access-list 110 permit tcp 10.0.2.0
0.0.0.255 10.0.1.0 0.0.0.255
```

Test and Verify IPSec

- Display configured IKE policies.
  - `show crypto isakmp policy`
  - (`show isakmp policy` on a PIX)
- Display configured transform sets.
  - `show crypto ipsec transform-set`
- Display phase | security associations.
  - `show crypto isakmp sa`
  - (`show isakmp sa` on a PIX)

Generic Routing Encapsulation GRE

- GRE is an OSI Layer 3 tunneling protocol:
  - Encapsulates a wide variety of protocol packet types inside IP tunnels
  - Creates a virtual point-to-point link to Cisco routers at remote points over an IP internetwork
  - Uses IP for transport
  - Uses an additional header to support any other OSI Layer 3 protocol as payload (for example, IP, IPX, AppleTalk)

Reasons for using GRE over IPsec

- To pass multicast and broadcast traffic across the tunnel securely
- To pass non-IP traffic securely
- To provide resiliency
- To assist in saving memory and CPU cycles in the router, by reducing the number of SA that need to be set up

Secure GRE Tunnels

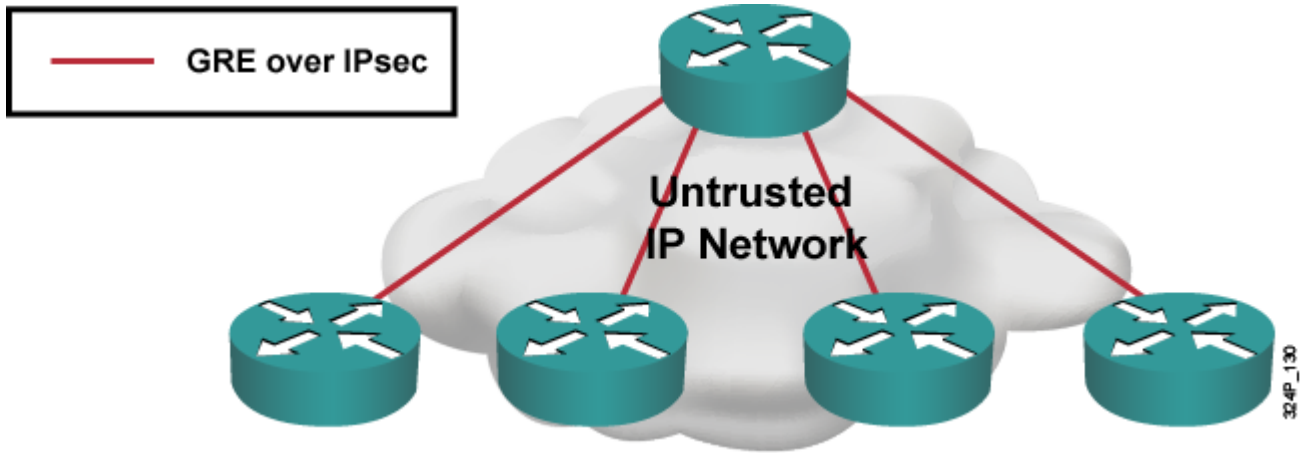
IPsec provides what GRE lacks:

- Confidentiality through encryption using symmetric algorithms
- Data source authentication using HMACs Data integrity verification using HMACs

IPsec is not perfect at tunneling:

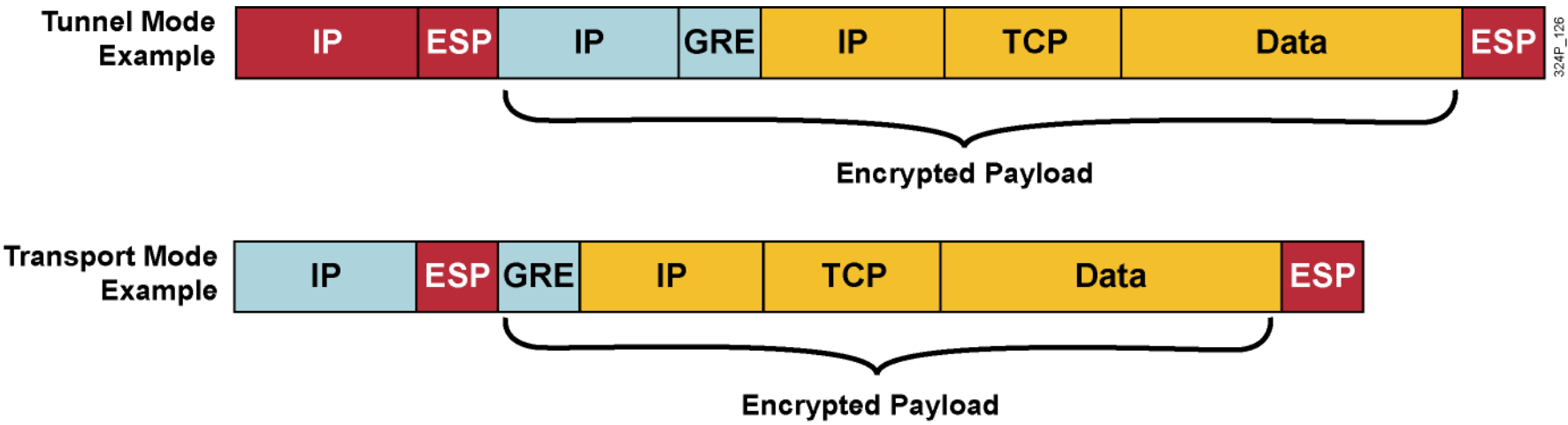
- Older IOS versions do not support IP multicast over IPsec
- IPsec was designed to tunnel IP only (no multiprotocol support)
- Using crypto maps to implement IPsec does not allow the use of routing protocols across the tunnel
- IPsec does not tunnel IP protocols; GRE does

GRE over IPsec



- **GRE over IPsec is typically used to do the following:**
  - **Create a logical hub-and-spoke topology of virtual point-to-point connections**
  - **Secure communication over an untrusted transport network (e.g. the Internet)**

GRE over IPsec Encapsulation



- GRE encapsulates an arbitrary payload.
- IPsec encapsulates unicast IP packet (GRE):
  - Tunnel mode (default): IPsec creates a new tunnel IP packet
  - Transport mode: IPsec reuses the IP header of the GRE (20 bytes less overhead than tunnel mode)