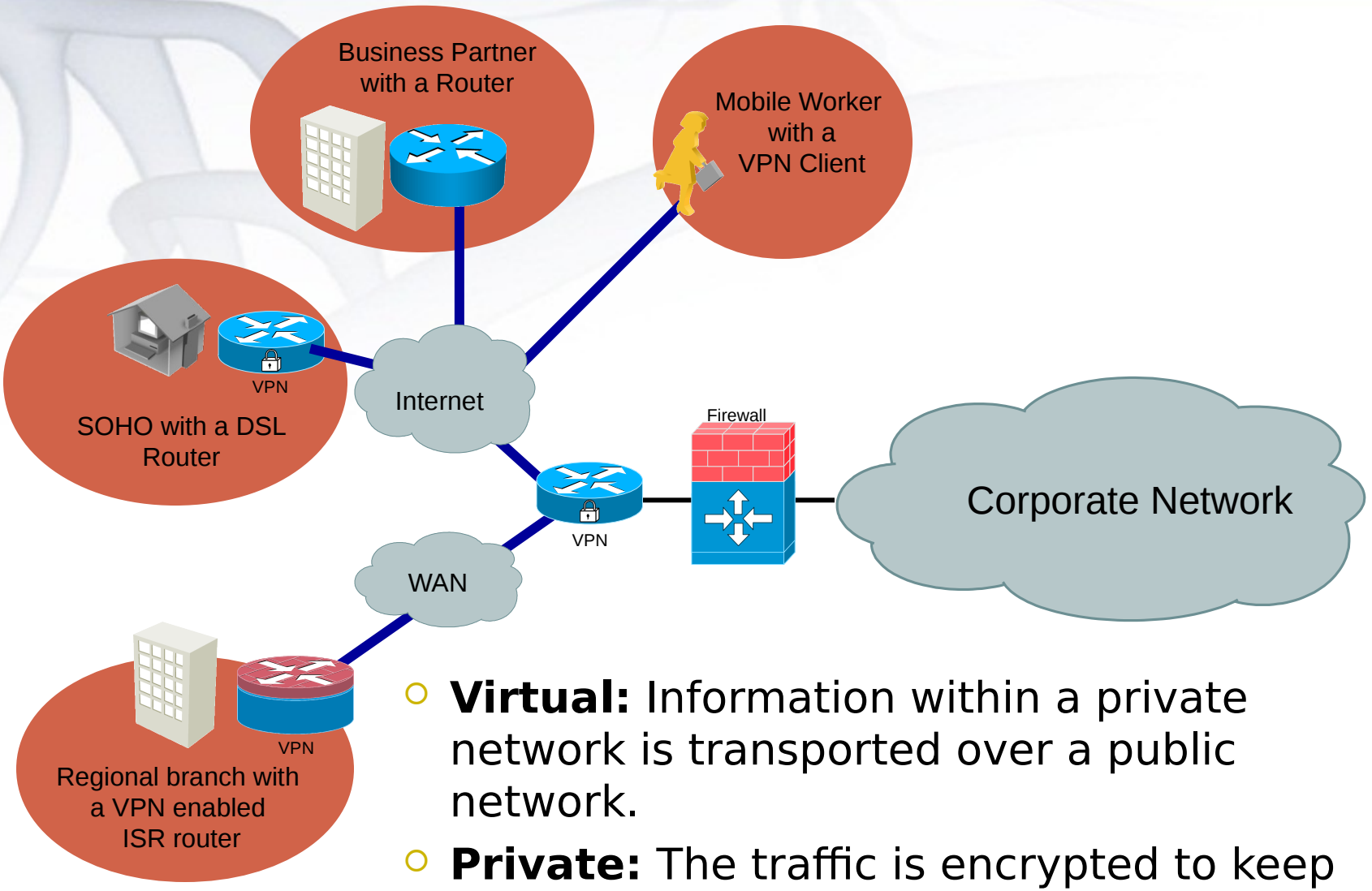
Lecture Seven

Implementing VPN

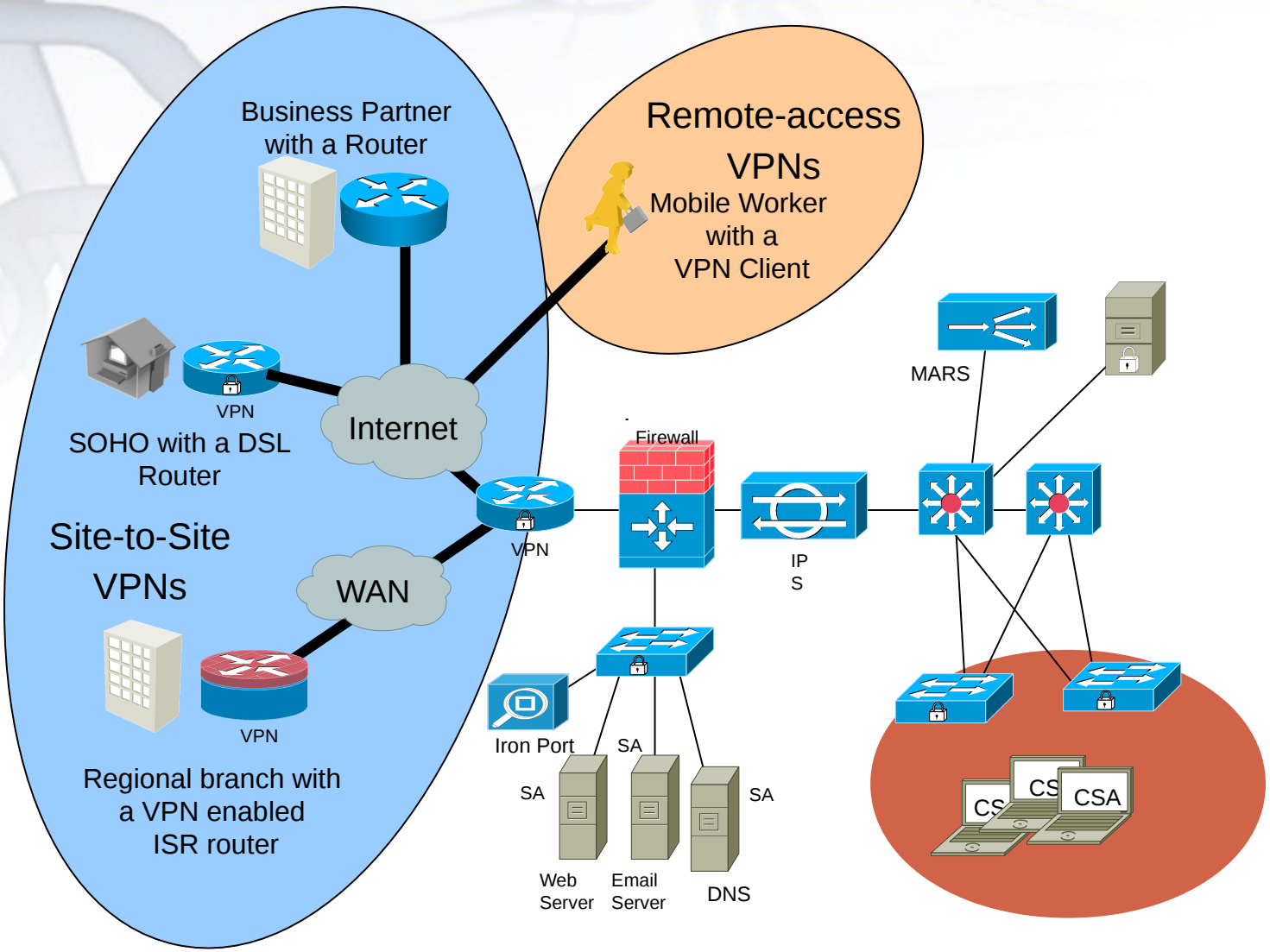
© Dr. M. Mahfuzul Islam
Professor, Dept. of CSE, BUET

What is VPN?

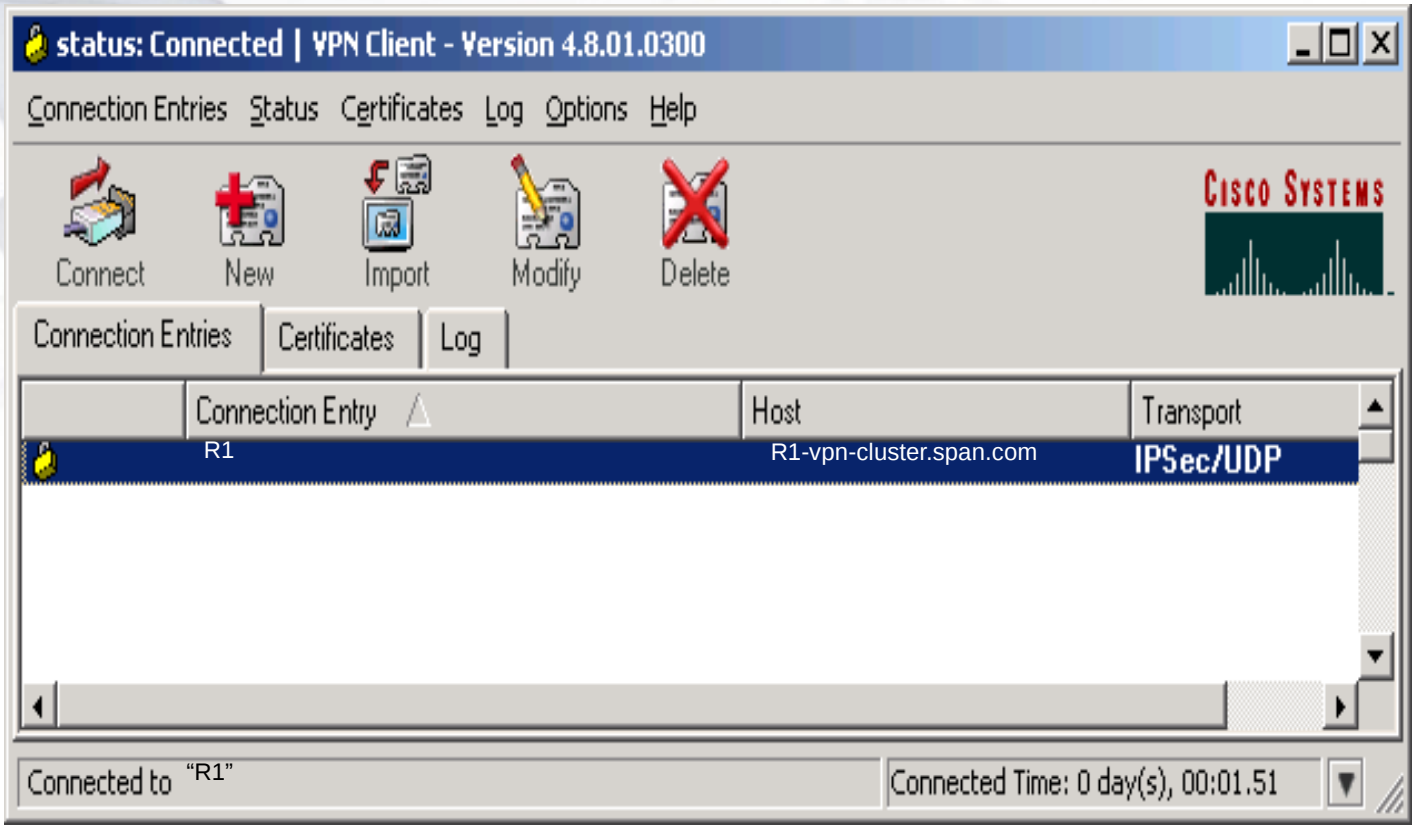


- **Virtual:** Information within a private network is transported over a public network.
- **Private:** The traffic is encrypted to keep the data confidential.

Types of VPNs



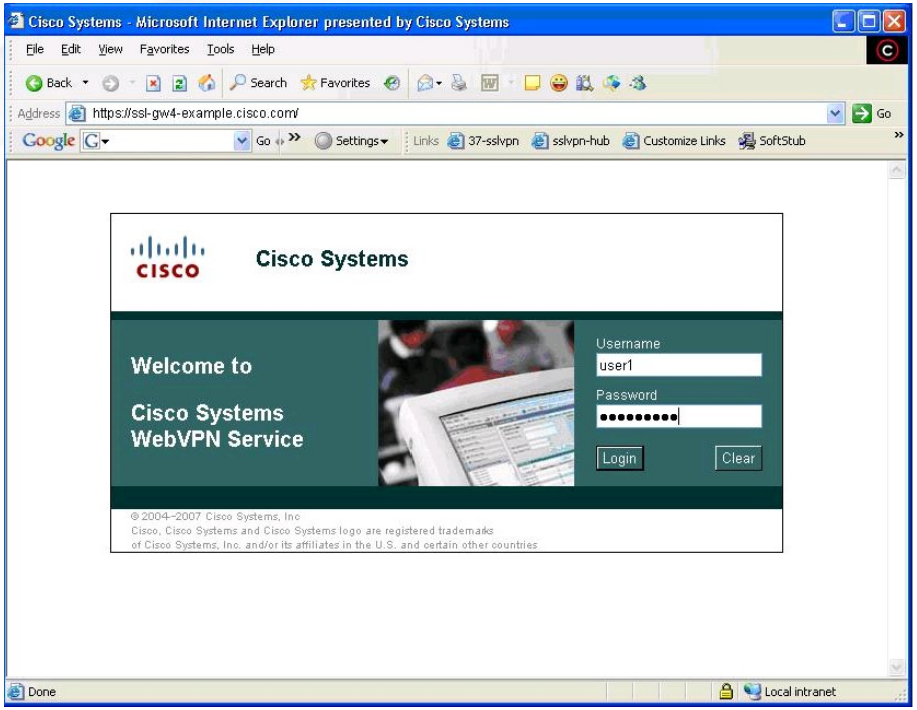
VPN Client Software



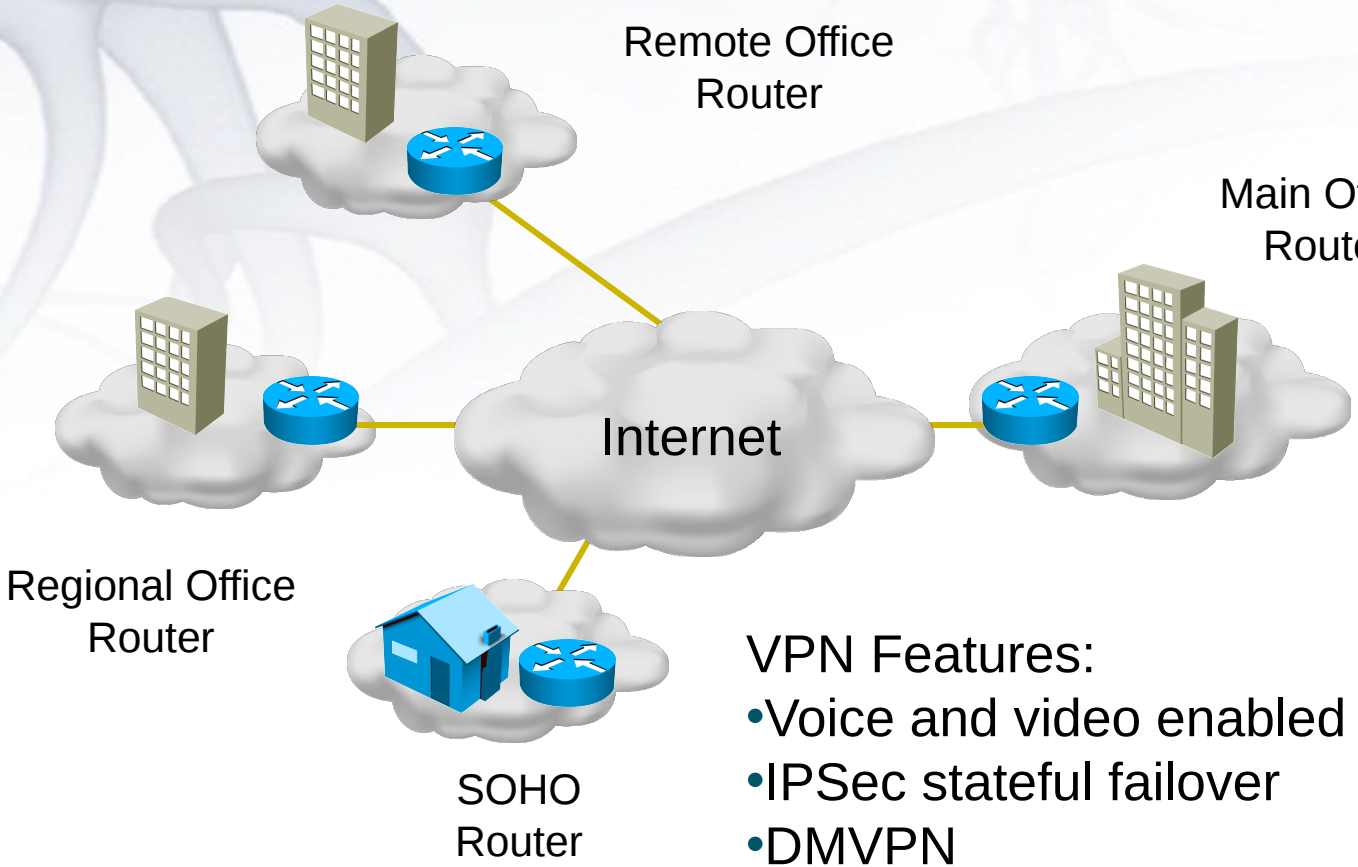
In a remote-access VPN, each host typically has VPN Client software

IOS SSL VPN

- Provides remote-access connectivity from any Internet-enabled host
- Uses a web browser and SSL encryption
- Delivers two modes of access:
  - Clientless
  - Thin client



VPN Optimized Routers



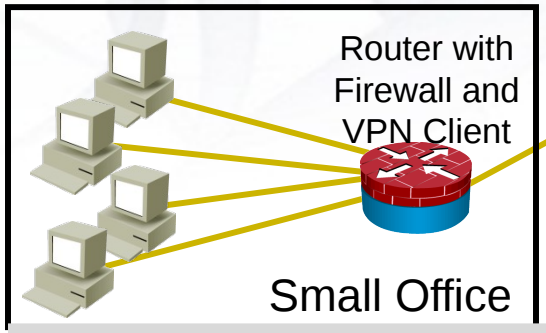
VPN Features:

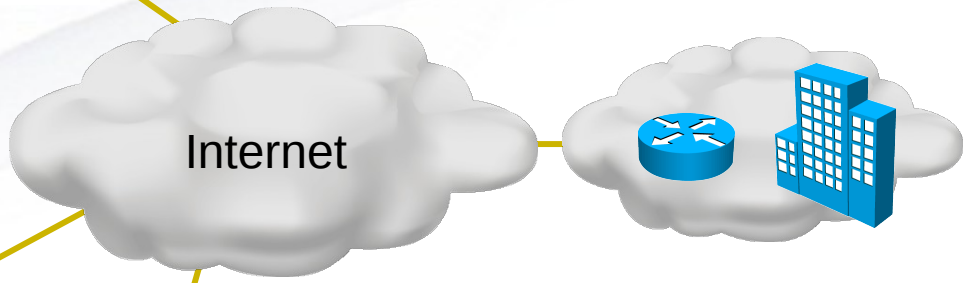
- Voice and video enabled VPN (V3PN)
- IPSec stateful failover
- DMVPN
- IPSec and Multiprotocol Label Switching (MPLS) integration
- Cisco Easy VPN

IPSec Clients

Certicom PDA IPsec VPN Client

A wireless client that is loaded on a PDA



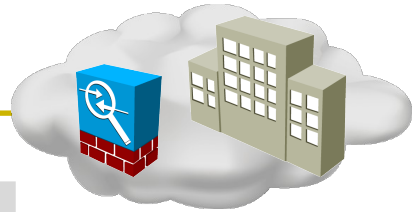


VPN Software Client

Software loaded on a PC

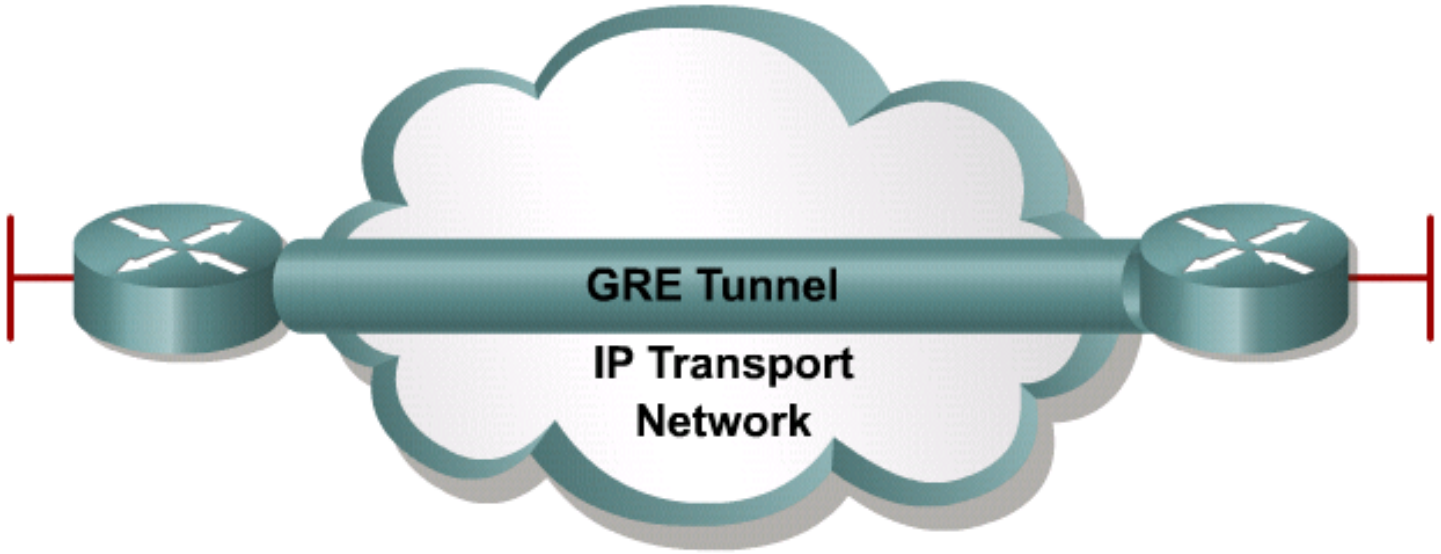
A network appliance that connects SOHO LANs to the VPN

AnyConnect VPN Client



Provides remote users with secure VPN connections

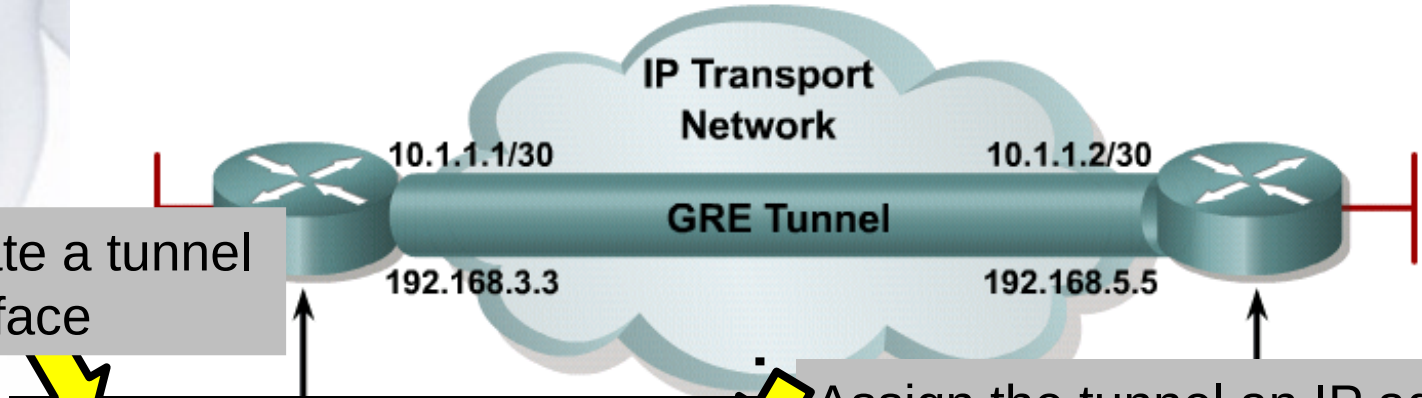
GRE VPN Overview



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)

Configuring GRE Tunnels



Create a tunnel interface

Assign the tunnel an IP address

```
R1(config)# interface tunnel 0
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# tunnel source serial 0/0
R1(config-if)# tunnel destination 192.168.5.5
R1(config-if)# tunnel mode gre ip
R1(config-if)#
```

```
R2(config-if)# tunnel mode gre ip
```

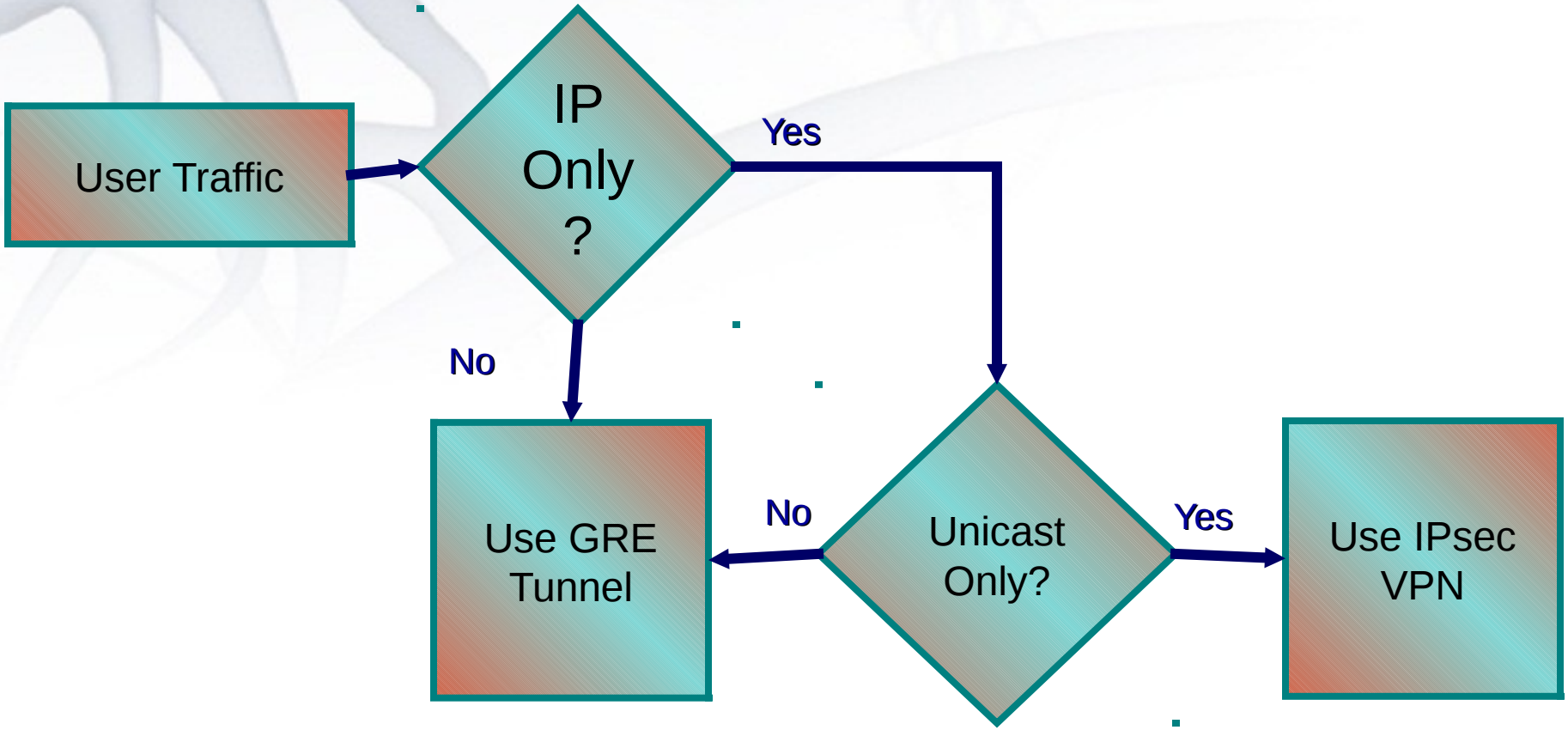
Identify the source tunnel interface

Identify the destination of the tunnel

Configure what protocol GRE will encapsulate

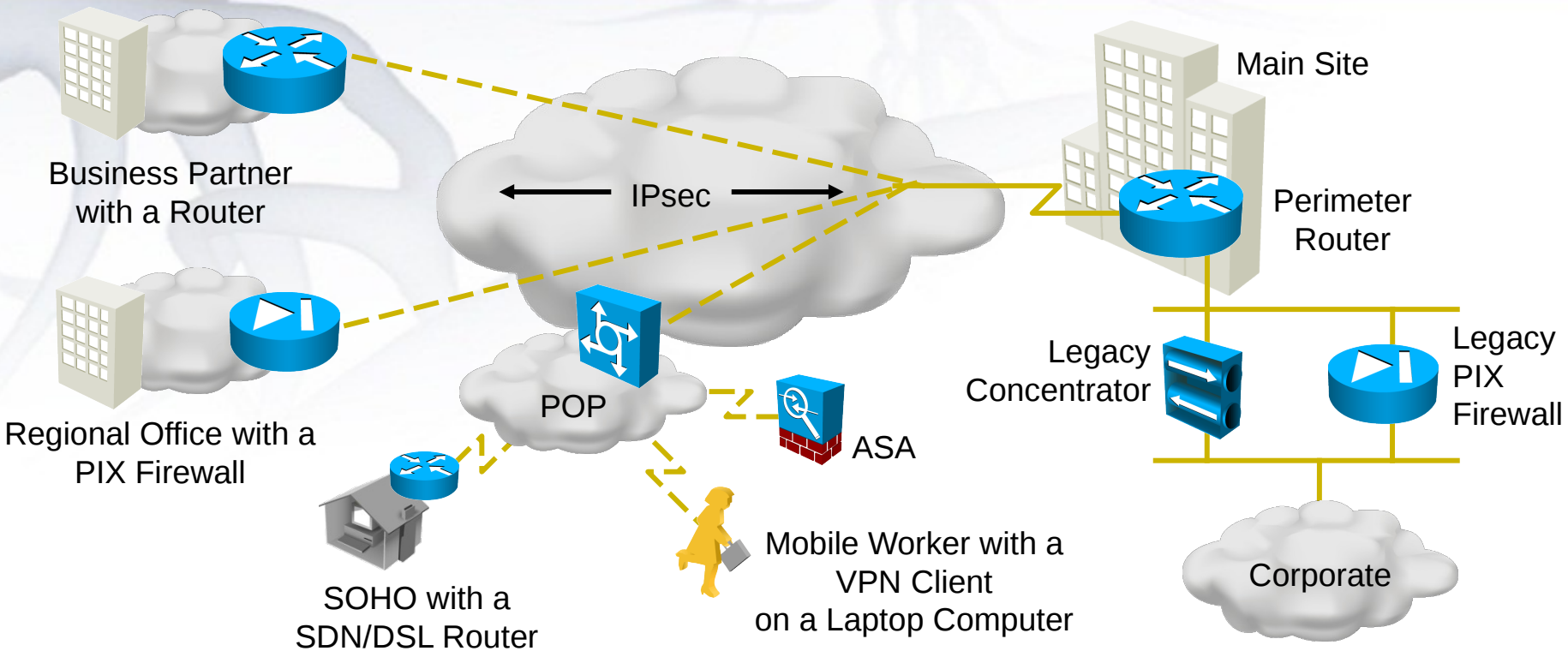
- GRE tunnel is up and the protocol is up if:
  - Tunnel source and destination are configured
  - Tunnel destination is in routing table
  - GRE keepalives are received (if used)
- GRE is the default tunnel mode.

Using GRE



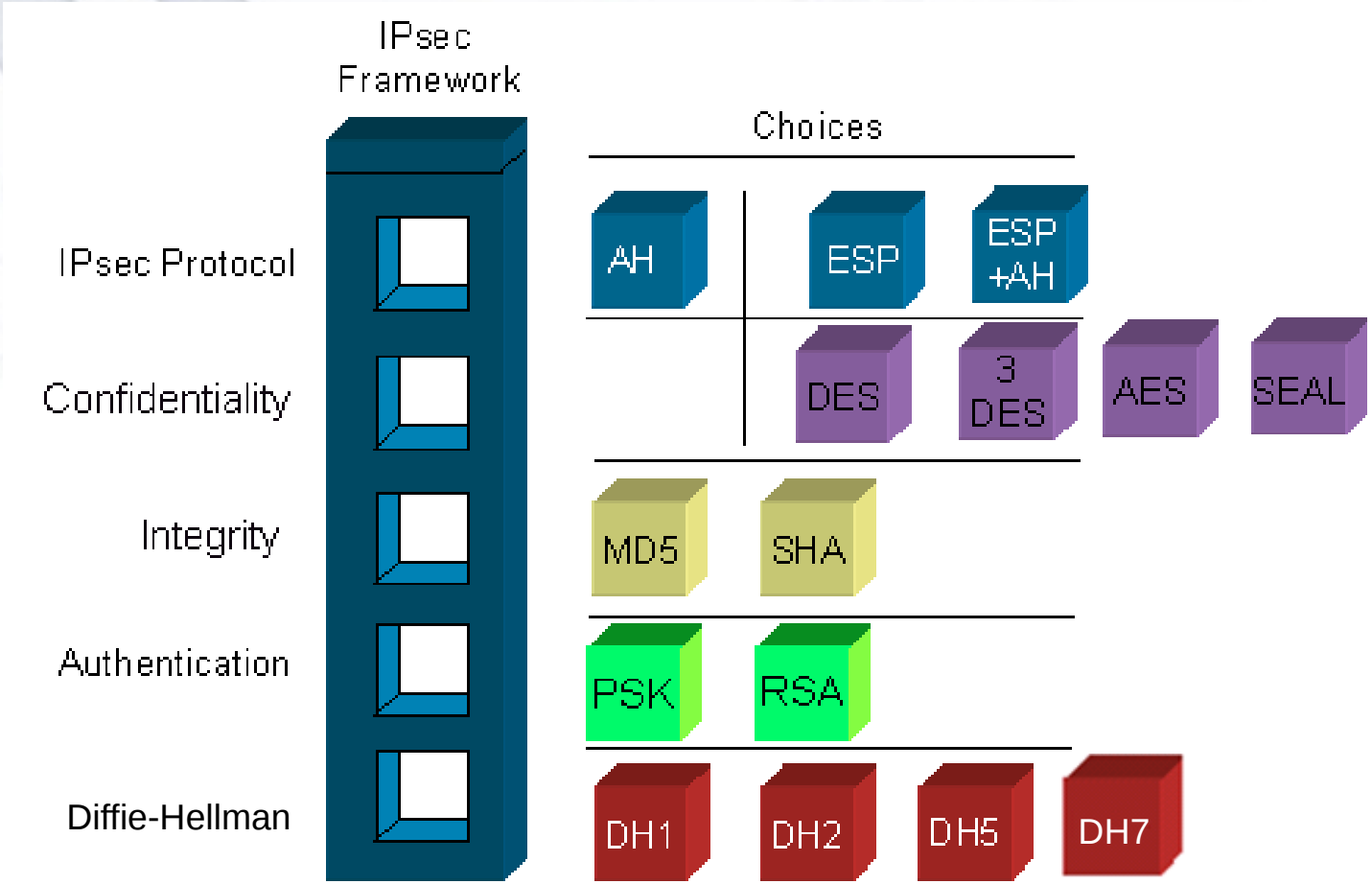
GRE does not provide encryption

IPSec Technology

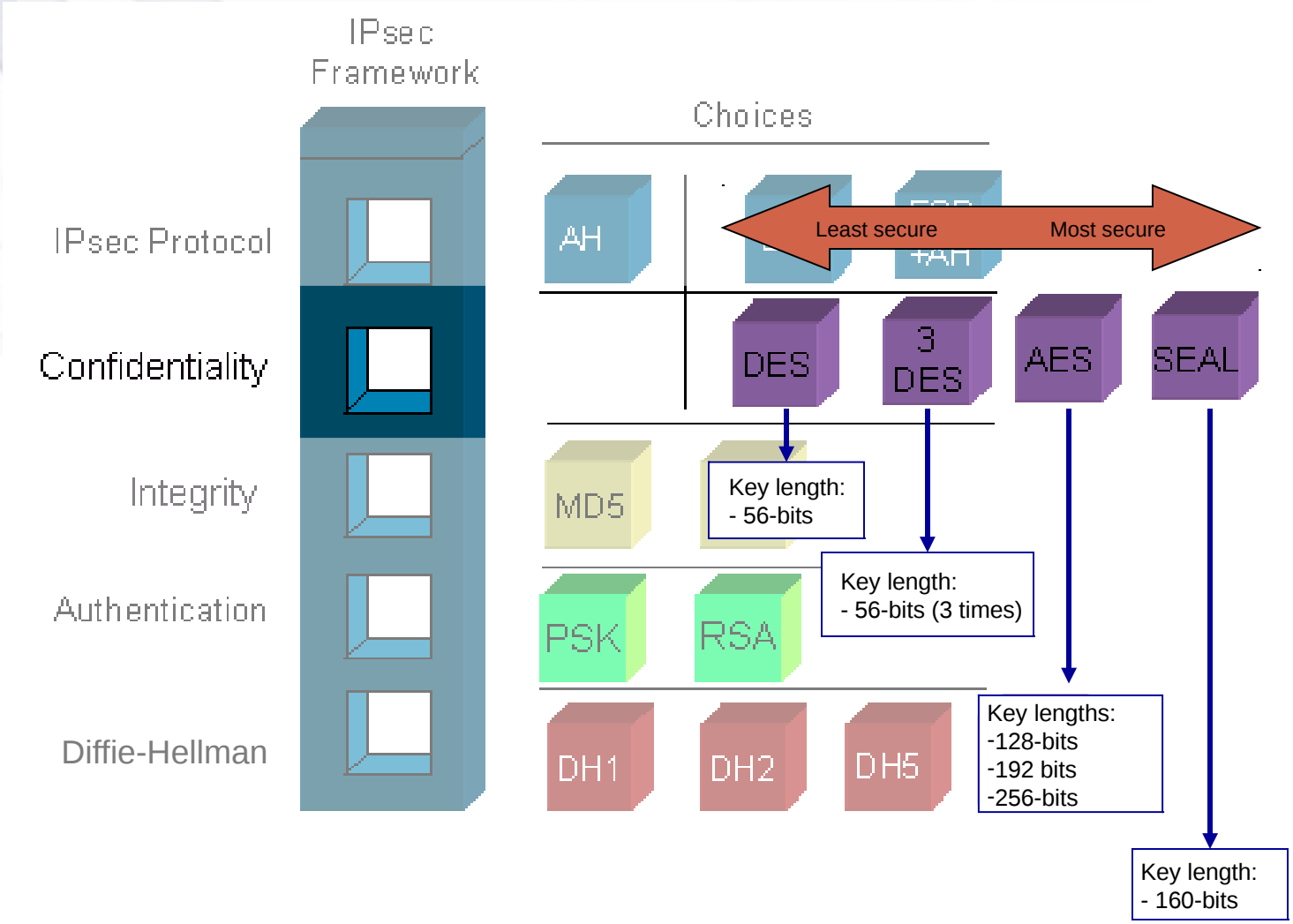


- Works at the network layer, protecting and authenticating IP packets.
  - It is a framework of open standards which is algorithm-independent.
  - It provides data confidentiality, data integrity, and origin authentication.

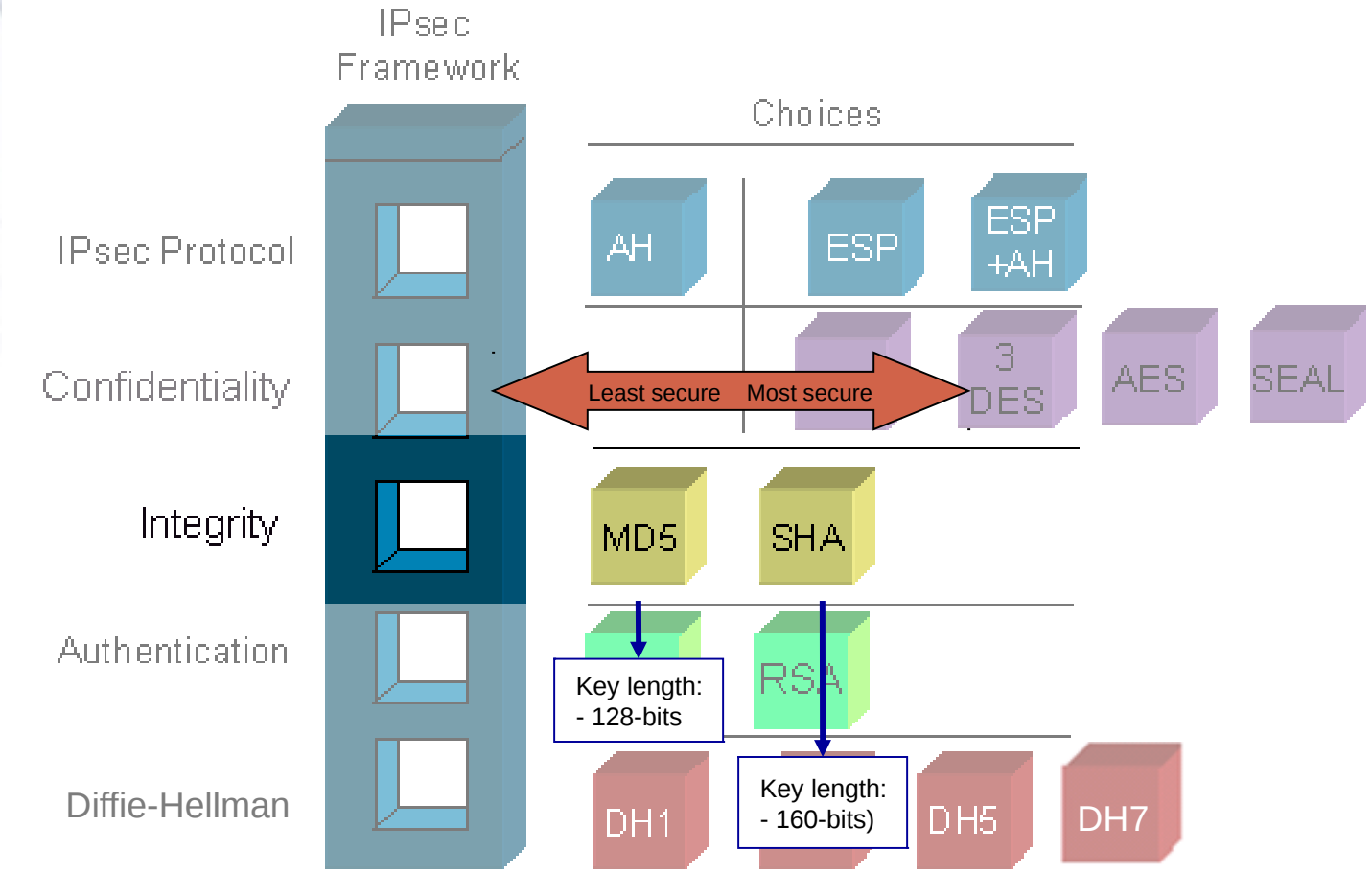
IPSec Framework



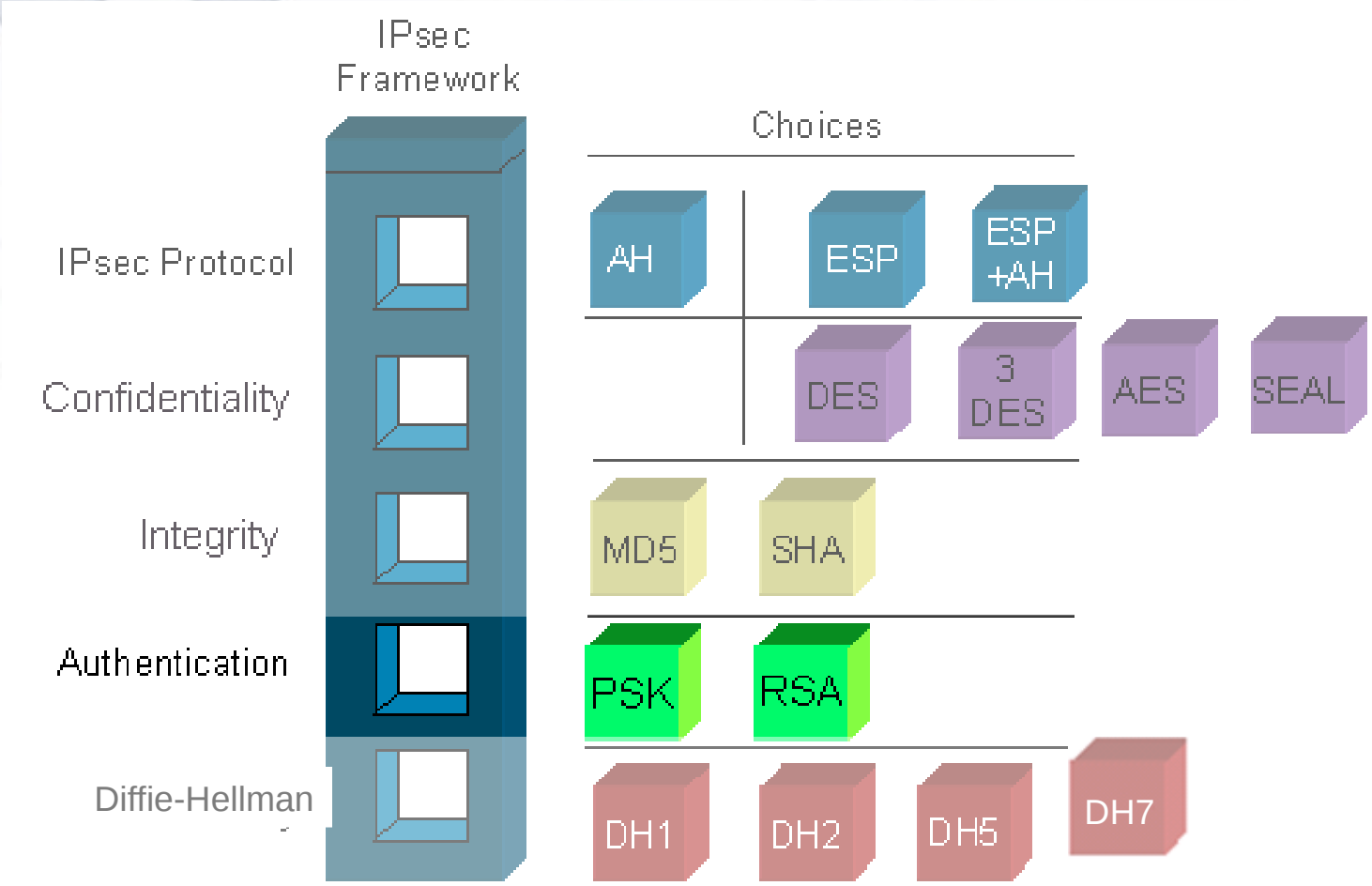
Confidentiality



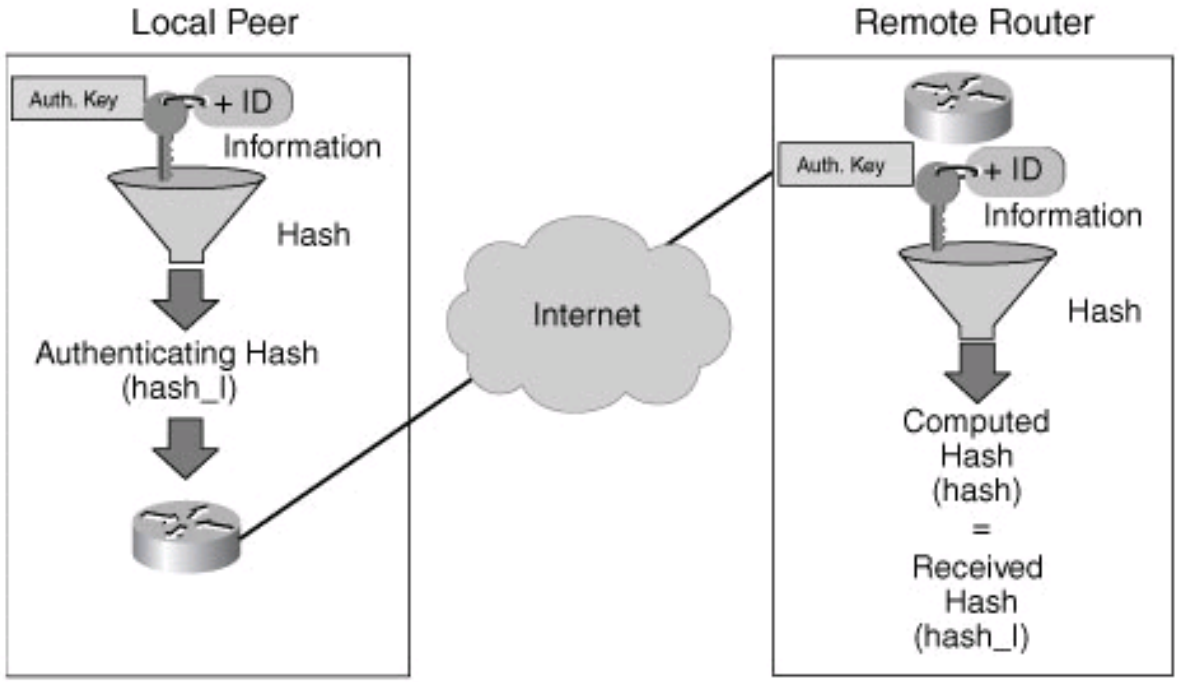
Integrity


IPsec Framework
Choices
IPsec Protocol
Confidentiality
Integrity
Authentication
Diffie-Hellman
AH
ESP
ESP +AH
Least secure
Most secure
3 DES
AES
SEAL
MD5
SHA
Key length:
- 128-bits
RSA
Key length:
- 160-bits)
DH1
DH5
DH7

Authentication



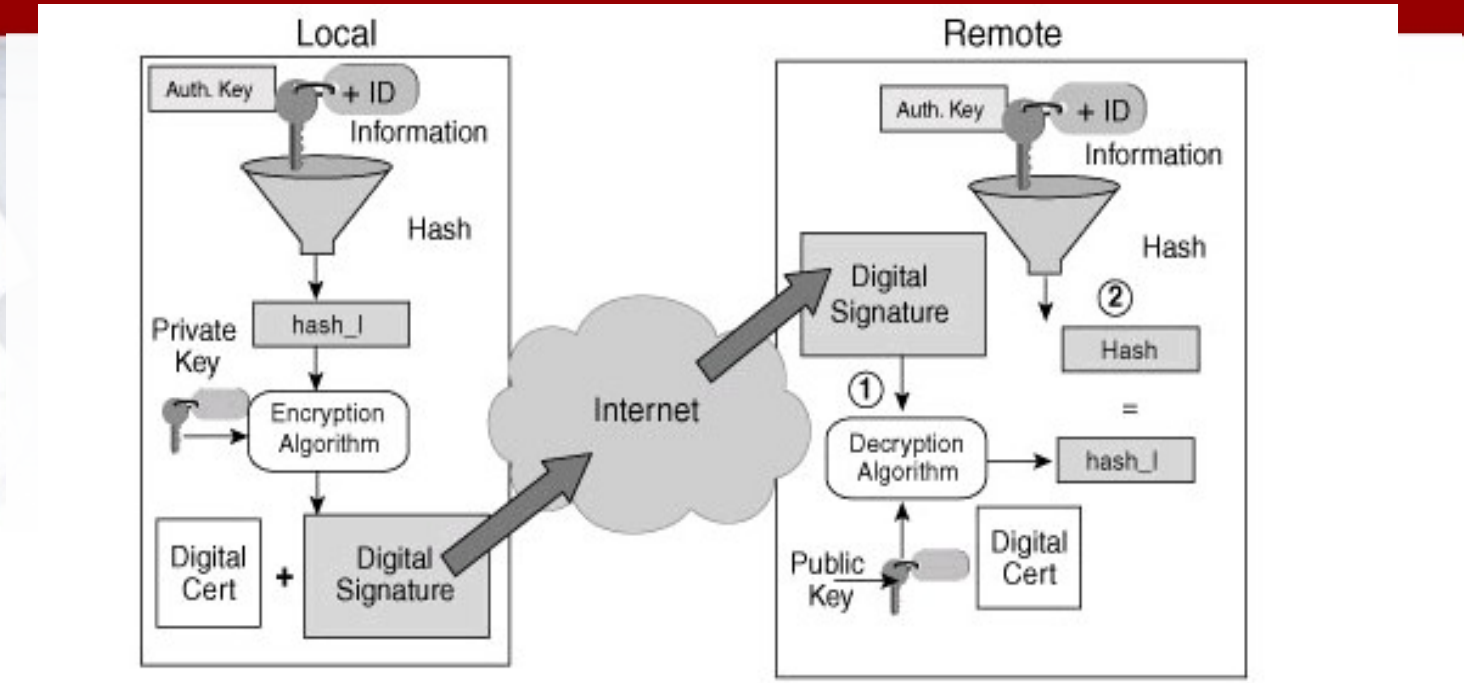
Pre-shared Key (PSK)



•At the local device, the authentication key and the identity information (device-specific information) are sent through a hash algorithm to form hash_I. One-way authentication is established by sending hash_I to the remote device. If the remote device can independently create the same hash, the local device is authenticated.

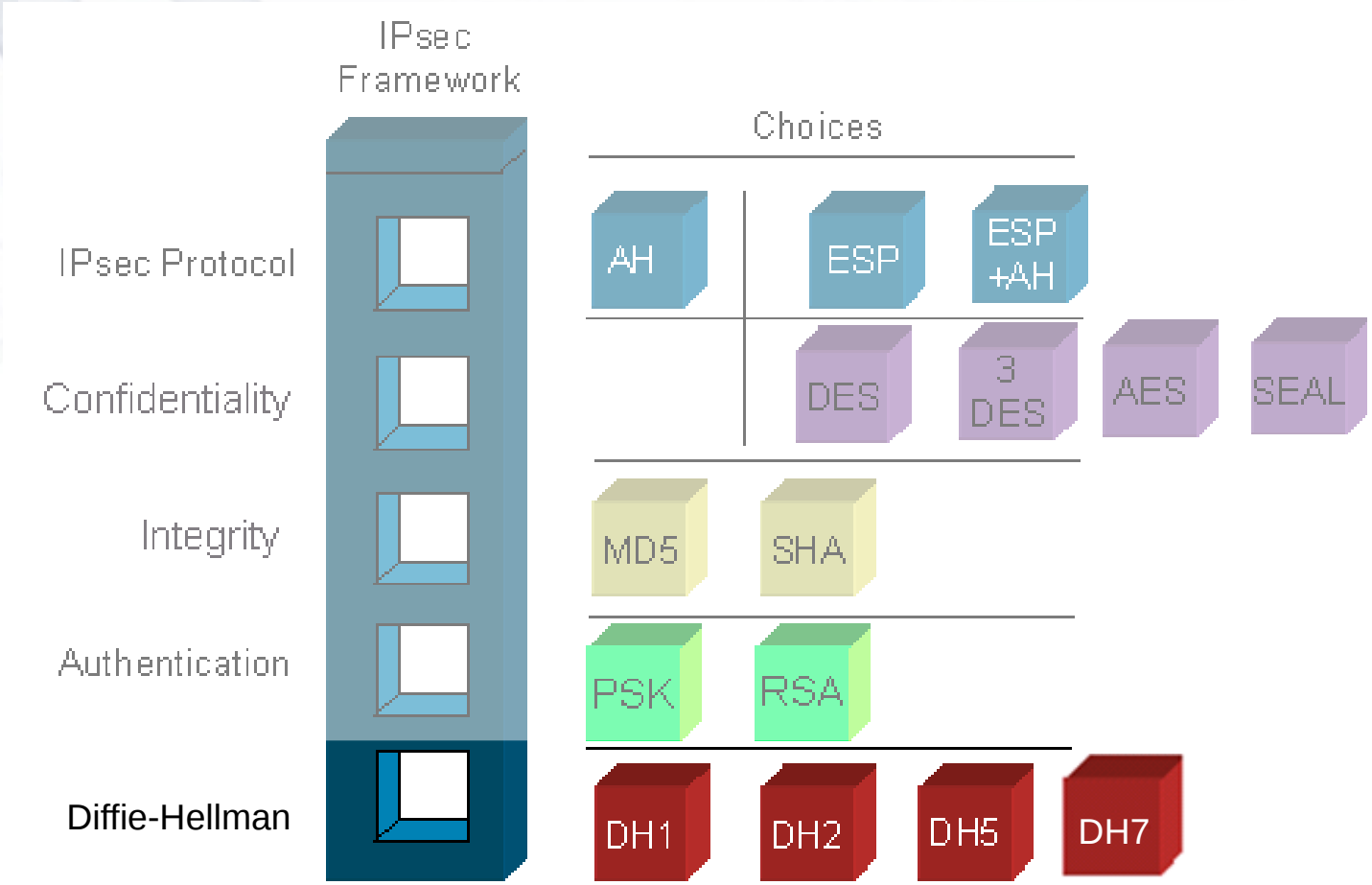
• The authentication process continues in the opposite direction. The remote device combines its identity information with the preshared-based authentication key and sends it through the hash algorithm to form hash_R. hash_R is sent to the local device. If the local device can independently create the same hash, the remote device is authenticated.

RSA Signatures



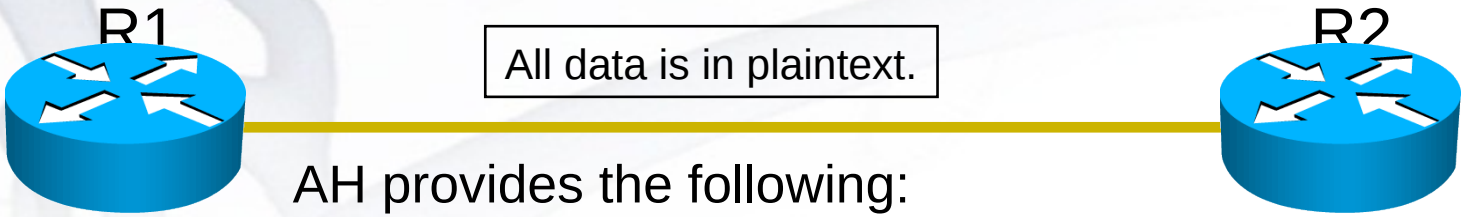
- At the local device, the authentication key and identity information (device-specific information) are sent through the hash algorithm forming hash_I. hash_I is encrypted using the local device's private encryption key creating a digital signature. The digital signature and a digital certificate are forwarded to the remote device. The public encryption key for decrypting the signature is included in the digital certificate. The remote device verifies the digital signature by decrypting it using the public encryption key. The result is hash_I.
- Next, the remote device independently creates hash_I from stored information. If the calculated hash_I equals the decrypted hash_I, the local device is authenticated. After the remote device authenticates the local device, the authentication process begins in the opposite direction and all steps are repeated from the remote device to the local device.

Secure Key Exchange



IPSec Framework Protocols

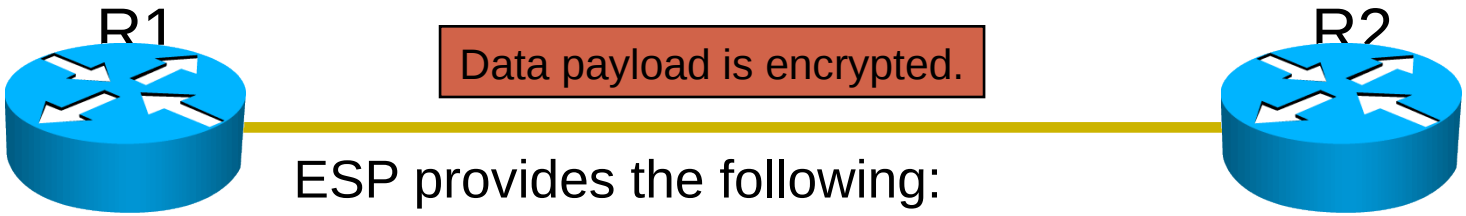
Authentication Header



AH provides the following:

- Authentication
- Integrity

Encapsulating Security Payload



ESP provides the following:

- Encryption
- Authentication
- Integrity

Authentication Header (AH)

1. The IP Header and data payload are hashed

IP Header + Data + Key

Hash

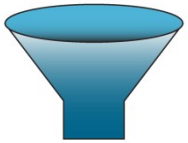
Authentication Data
(00ABCDEF)

2. The hash builds a new AH header which is prepended to the original packet

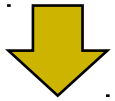
3. The new packet is transmitted to the IPSec peer router

R2

IP Header + Data + Key



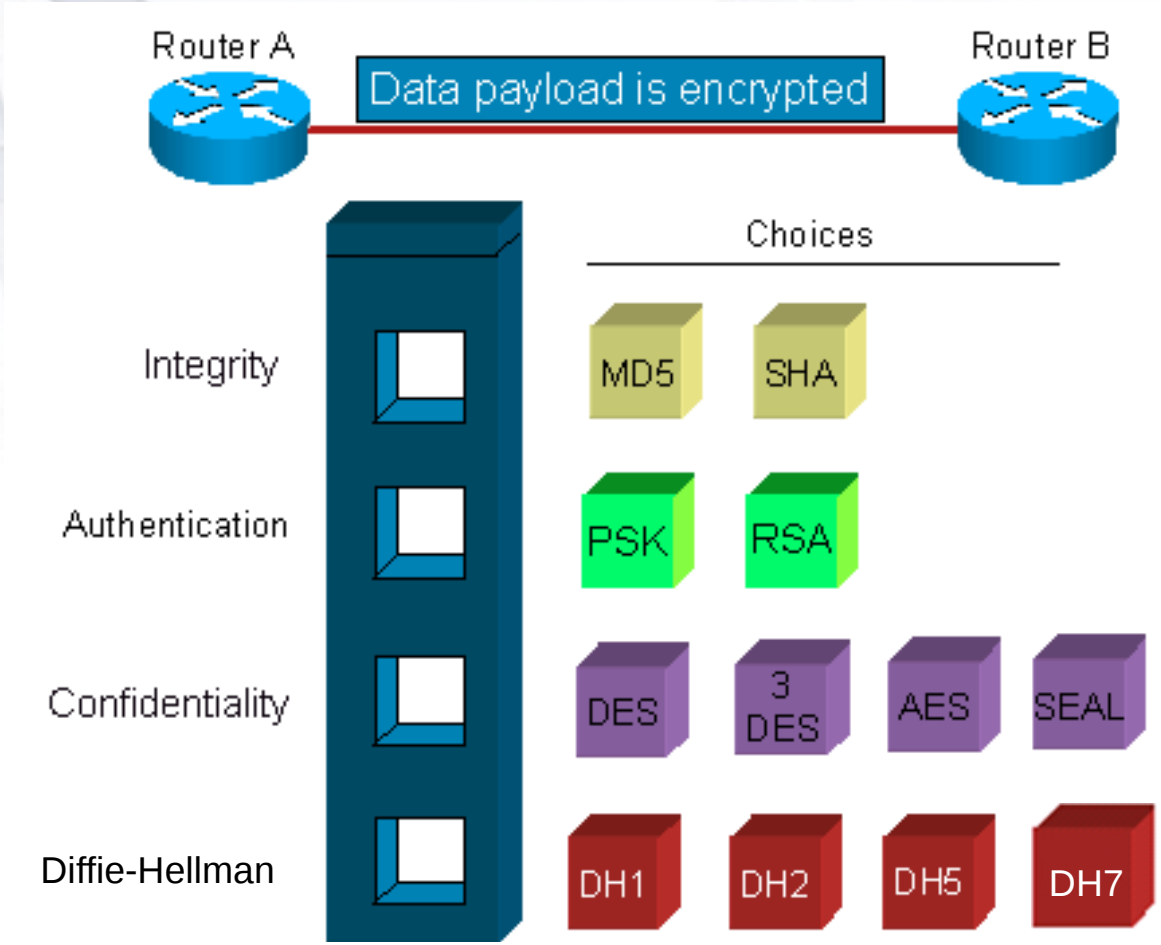
Hash



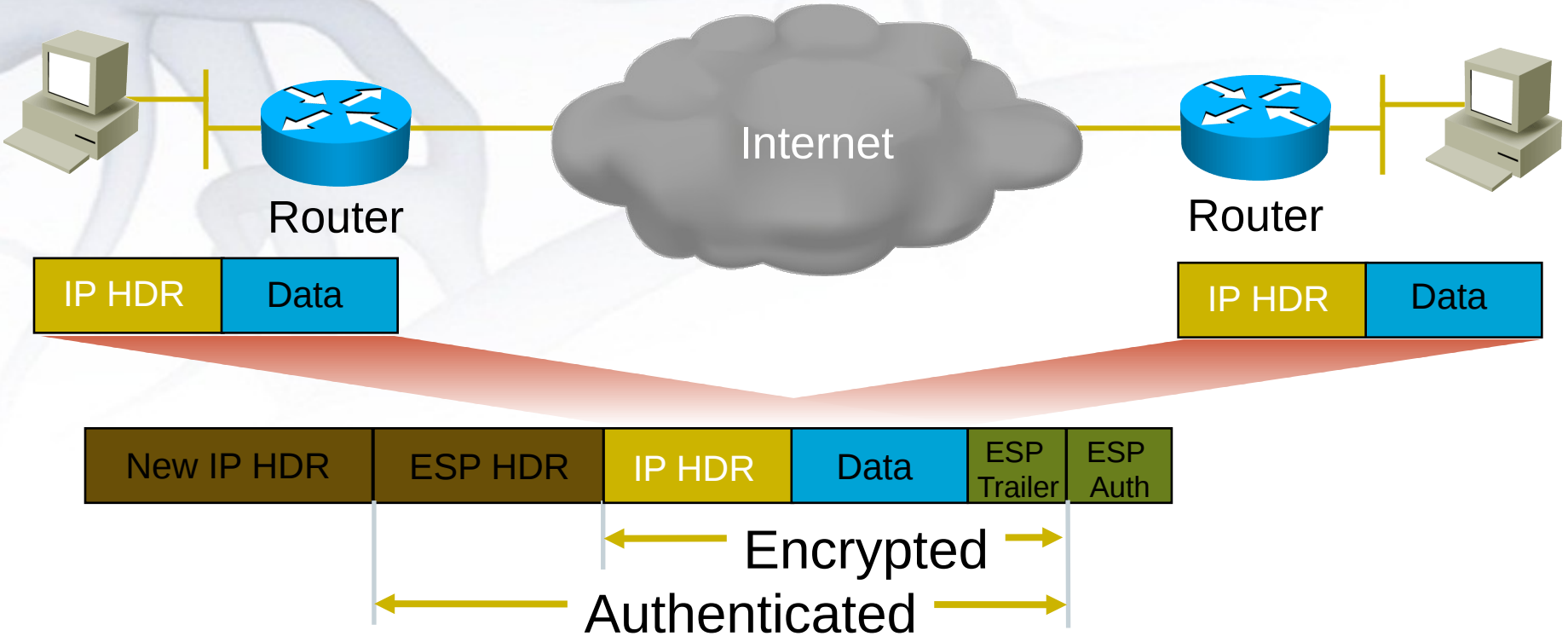
Recomputed Hash (00ABCDEF) = Received Hash (00ABCDEF)

4. The peer router hashes the IP header and data payload, extracts the transmitted hash and compares

Encapsulating Security Payload (ESP)



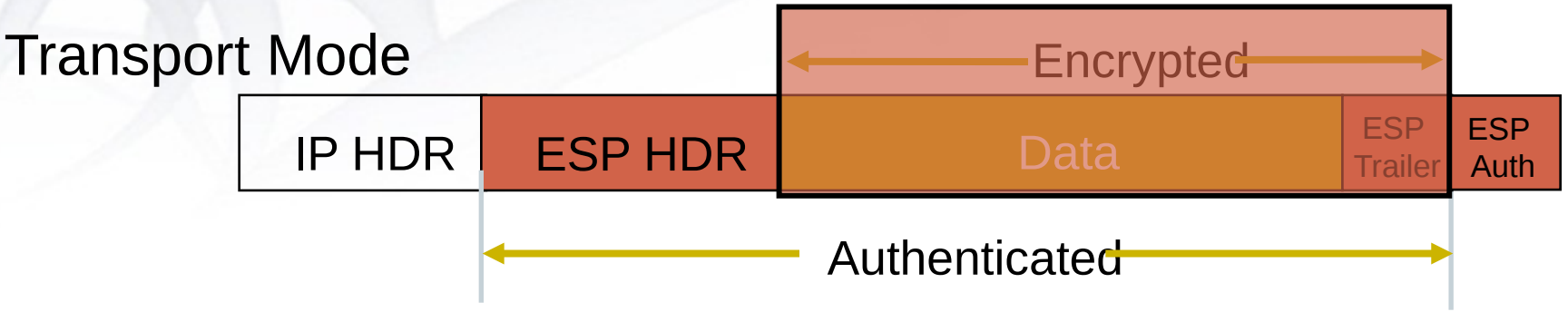
Function of ESP

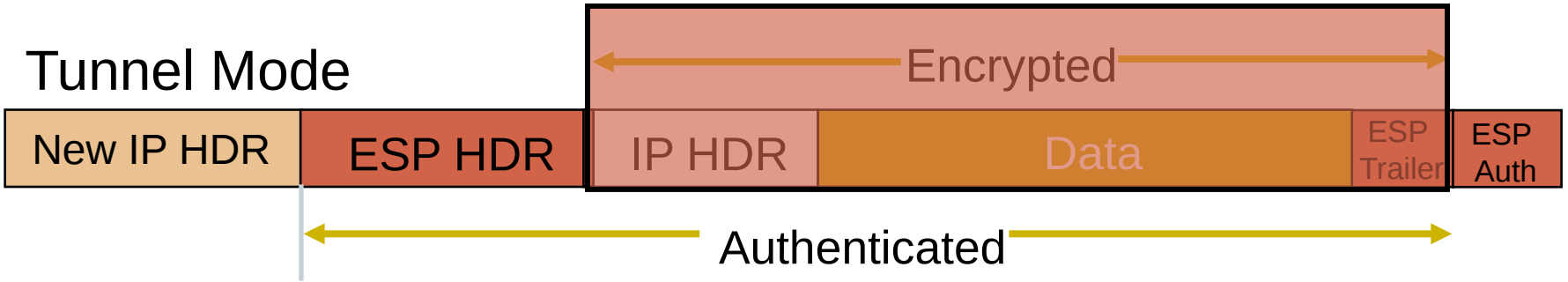


- Provides confidentiality with encryption
- Provides integrity with authentication

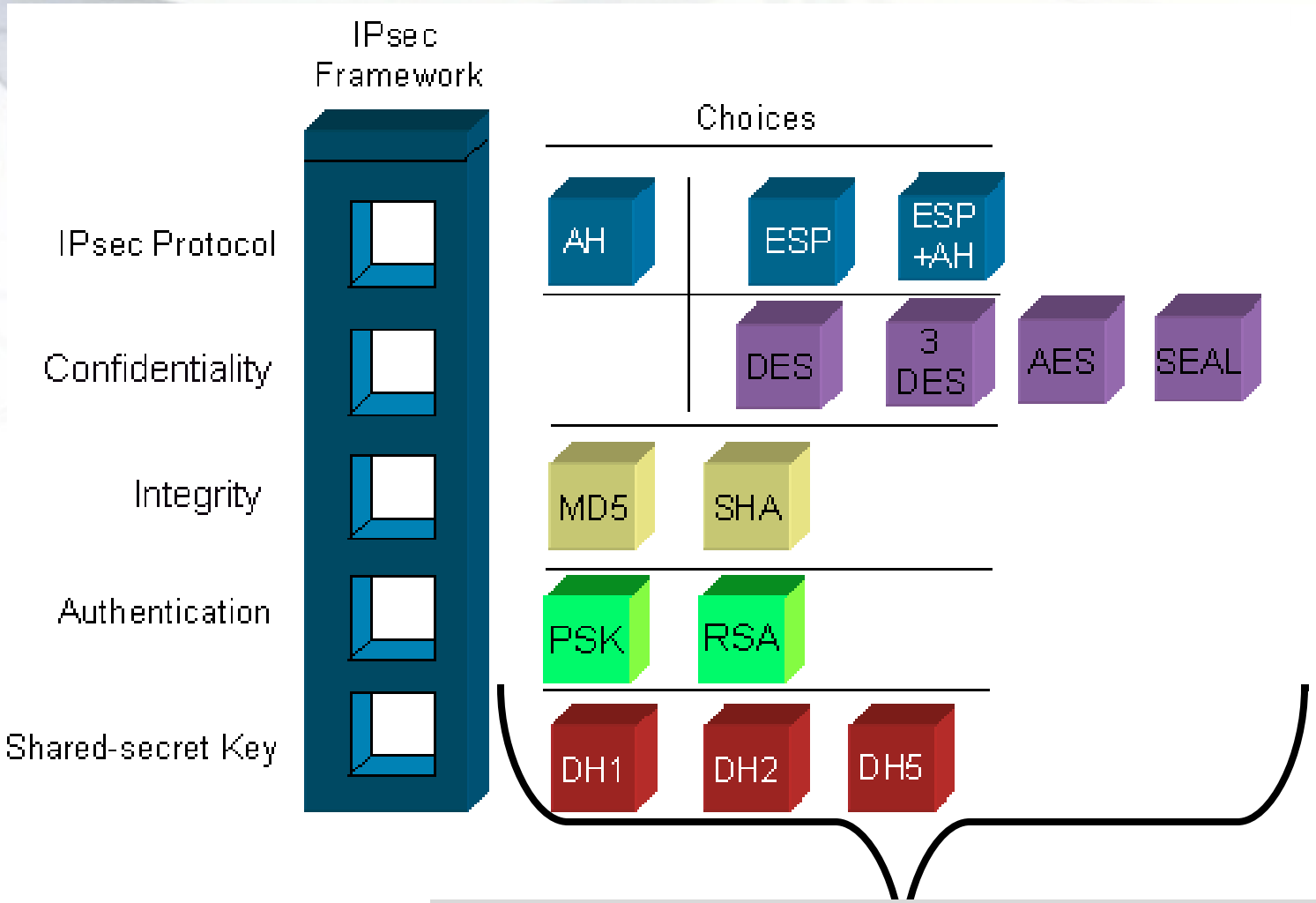
Mode Type

Original data prior to selection of IPSec protocol mode





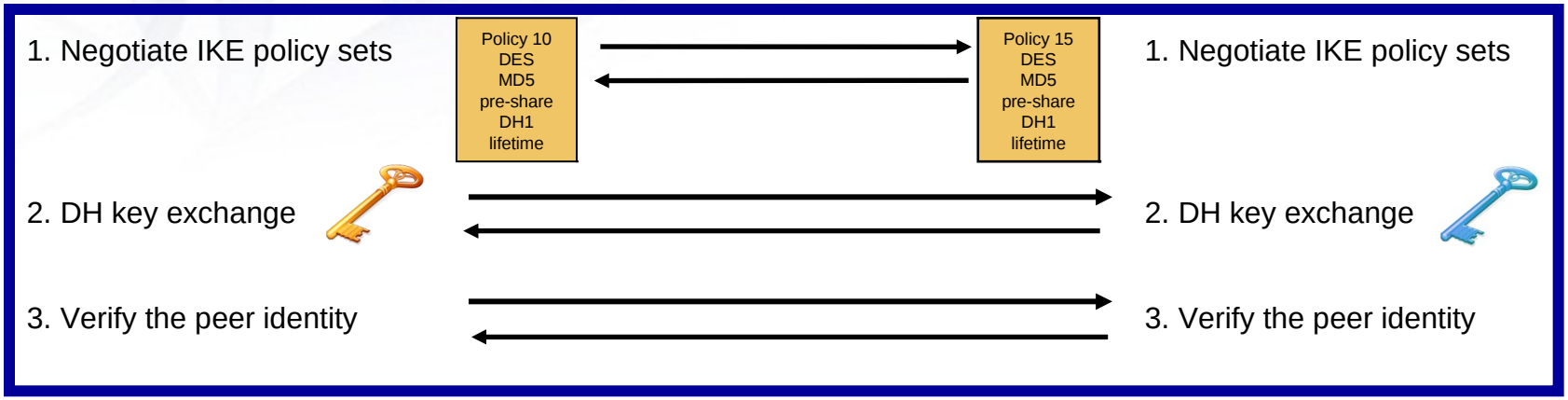
IPSec Associations



IPSec parameters are configured using IKE

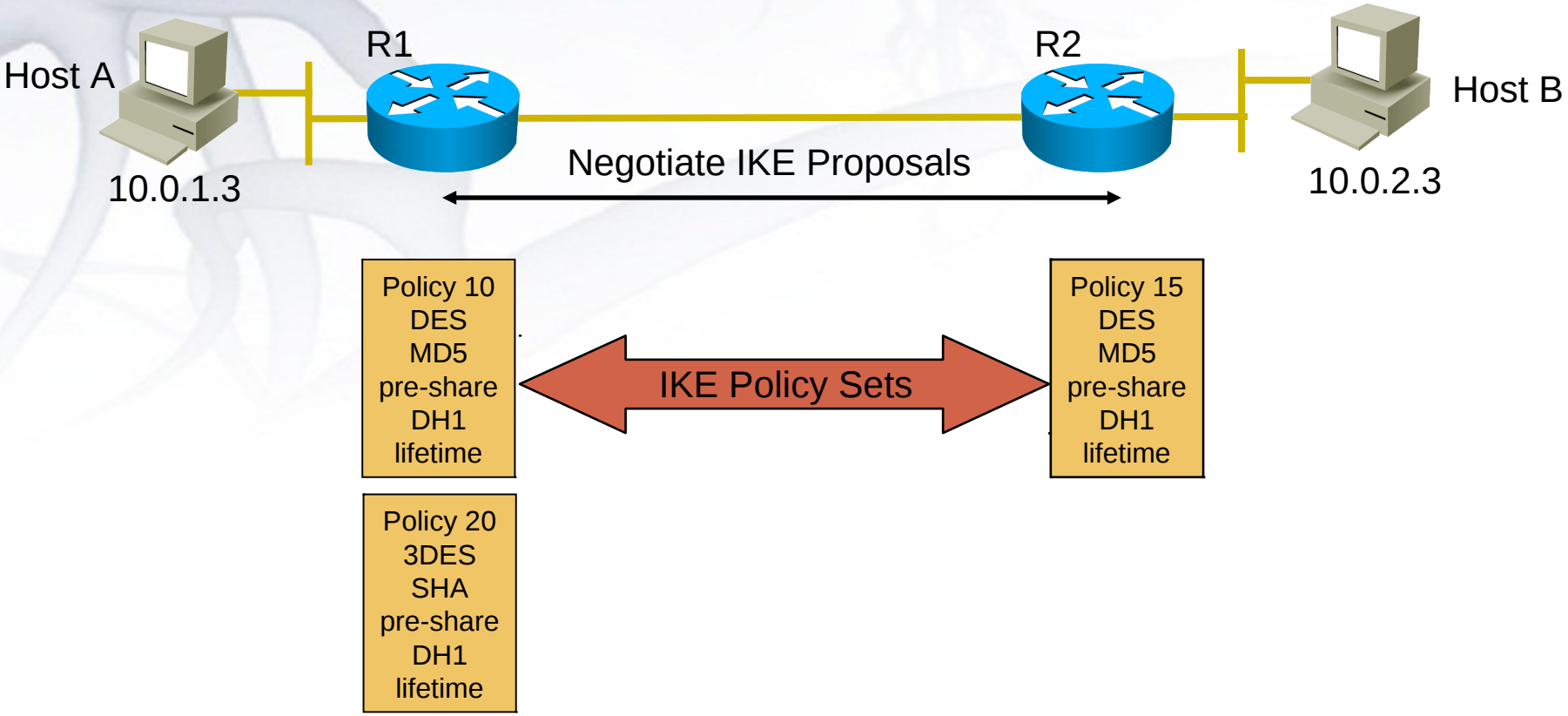
Internet Key Exchange (IKE) Phases

IKE Phase 1 Exchange



IKE Phase 2 Exchange

IKE Phase 1 – First Exchange



Negotiates matching IKE policies to protect IKE exchange

IKE Phase 1 – Second Exchange

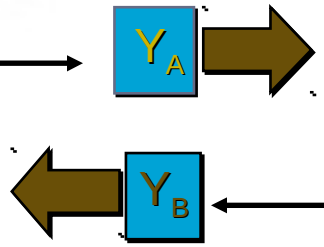
Establish Diffie-Hellman(DH) Key

Alice

Private value, X_A

Public value, Y_A

$Y_A = g^{X_A} \bmod p$



Private value, X_B

Public value, Y_B

$Y_B = g^{X_B} \bmod p$

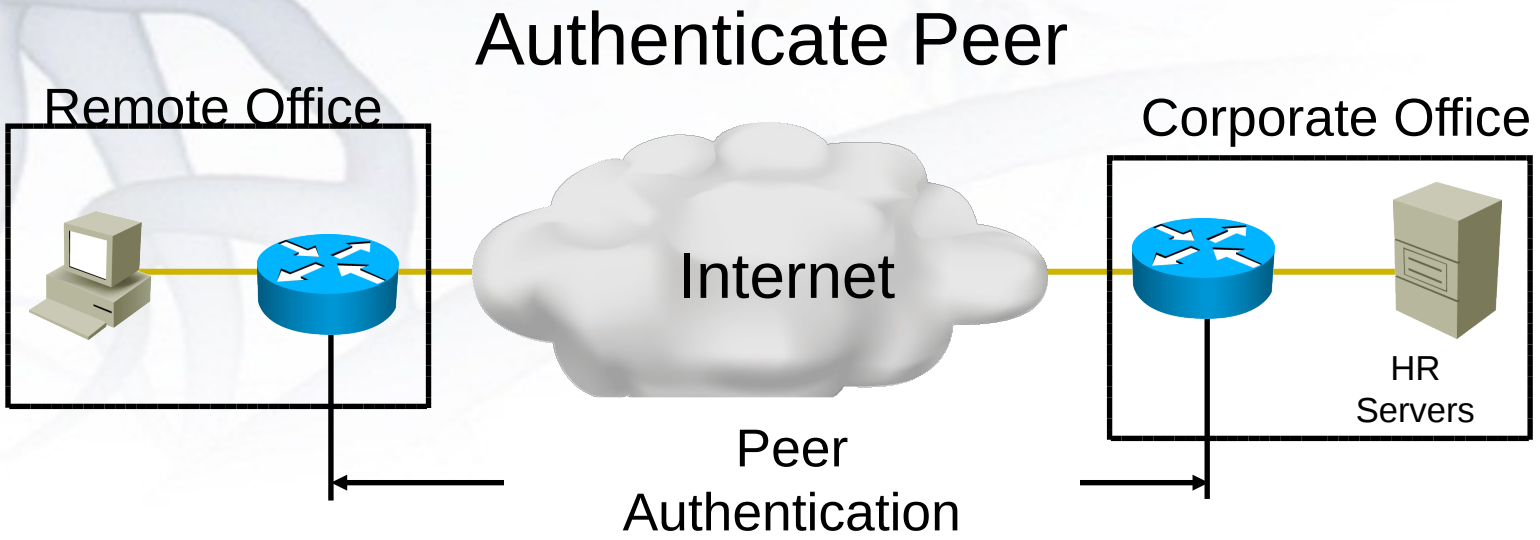
Bob

$(Y_B)^{X_A} \bmod p = K$

$(Y_A)^{X_B} \bmod p = K$

A DH exchange is performed to establish keying material.

IKE Phase 1 – Third Exchange



Peer authentication methods

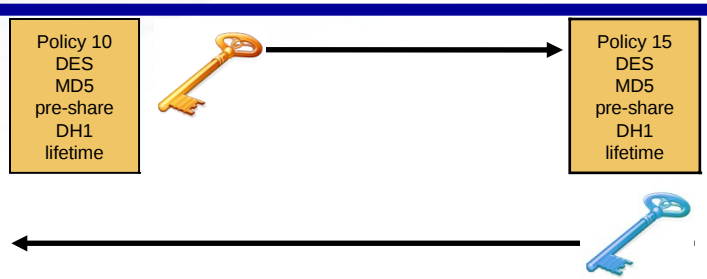
- PSKs
- RSA signatures
- RSA encrypted nonces

A bidirectional IKE SA is now established.

IKE Phase 1 – Aggressive Mode

IKE Phase 1 Aggressive Mode Exchange

1.Send IKE policy set and R1's DH key



2. Confirm IKE policy set, calculate shared secret and send R2's DH key

3.Calculate shared secret, verify peer identify, and confirm with peer

4. Authenticate peer and begin Phase 2.

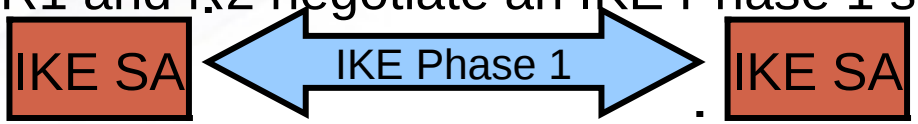
IKE Phase 2 Exchange

IKE Phase 2

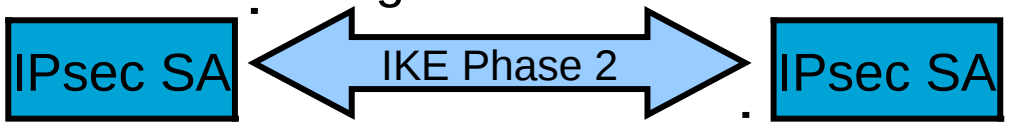
- IKE negotiates matching IPsec policies.
- Upon completion, unidirectional IPsec Security Associations(SA) are established for each protocol and algorithm combination.

IPSec VPN Negotiation

1. Host A sends interesting traffic to Host B.
2. R1 and R2 negotiate an IKE Phase 1 session.



3. R1 and R2 negotiate an IKE Phase 2 session.

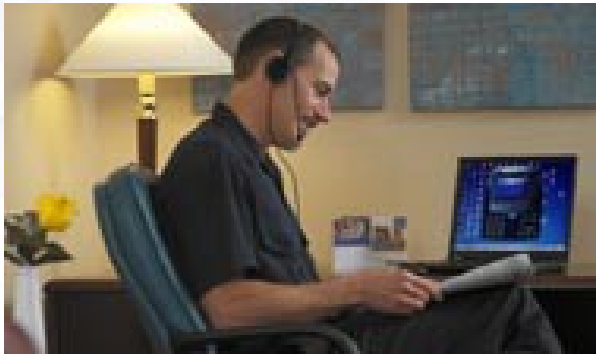


4. Information is exchanged via IPsec tunnel.

5. The IPsec tunnel is terminated.

Telecommuting

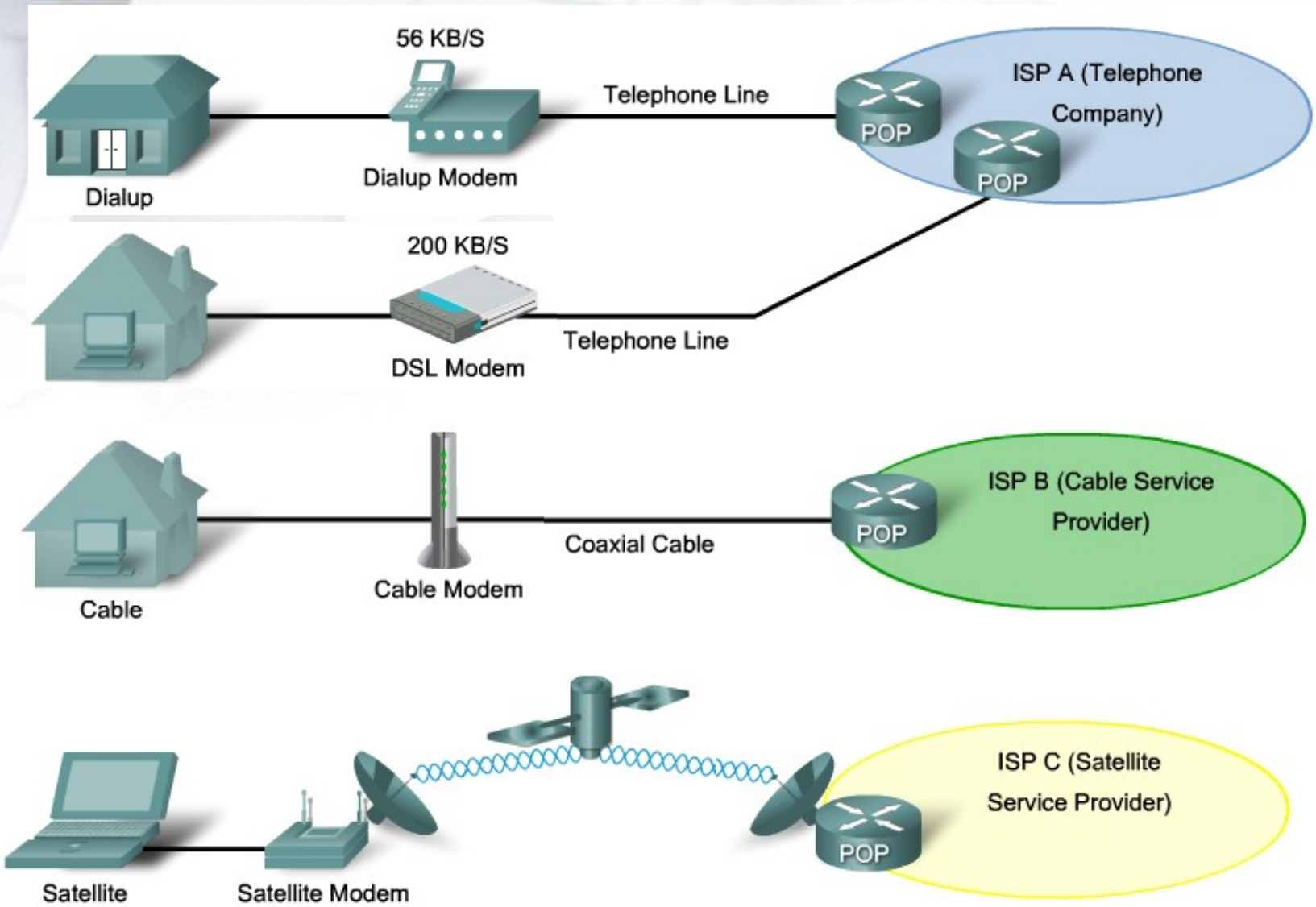
- Flexibility in working location and working hours
- Employers save on real-estate, utility and other overhead costs
- Succeeds if program is voluntary, subject to management discretion, and operationally feasible



Telecommuting Benefits

- Organizational benefits:
  - Continuity of operations
  - Increased responsiveness
  - Secure, reliable, and manageable access to information
  - Cost-effective integration of data, voice, video, and applications
  - Increased employee productivity, satisfaction, and retention
- Social benefits:
  - Increased employment opportunities for marginalized groups
  - Less travel and commuter related stress
- Environmental benefits:
  - Reduced carbon footprints, both for individual workers and organizations

Implementing Remote Access

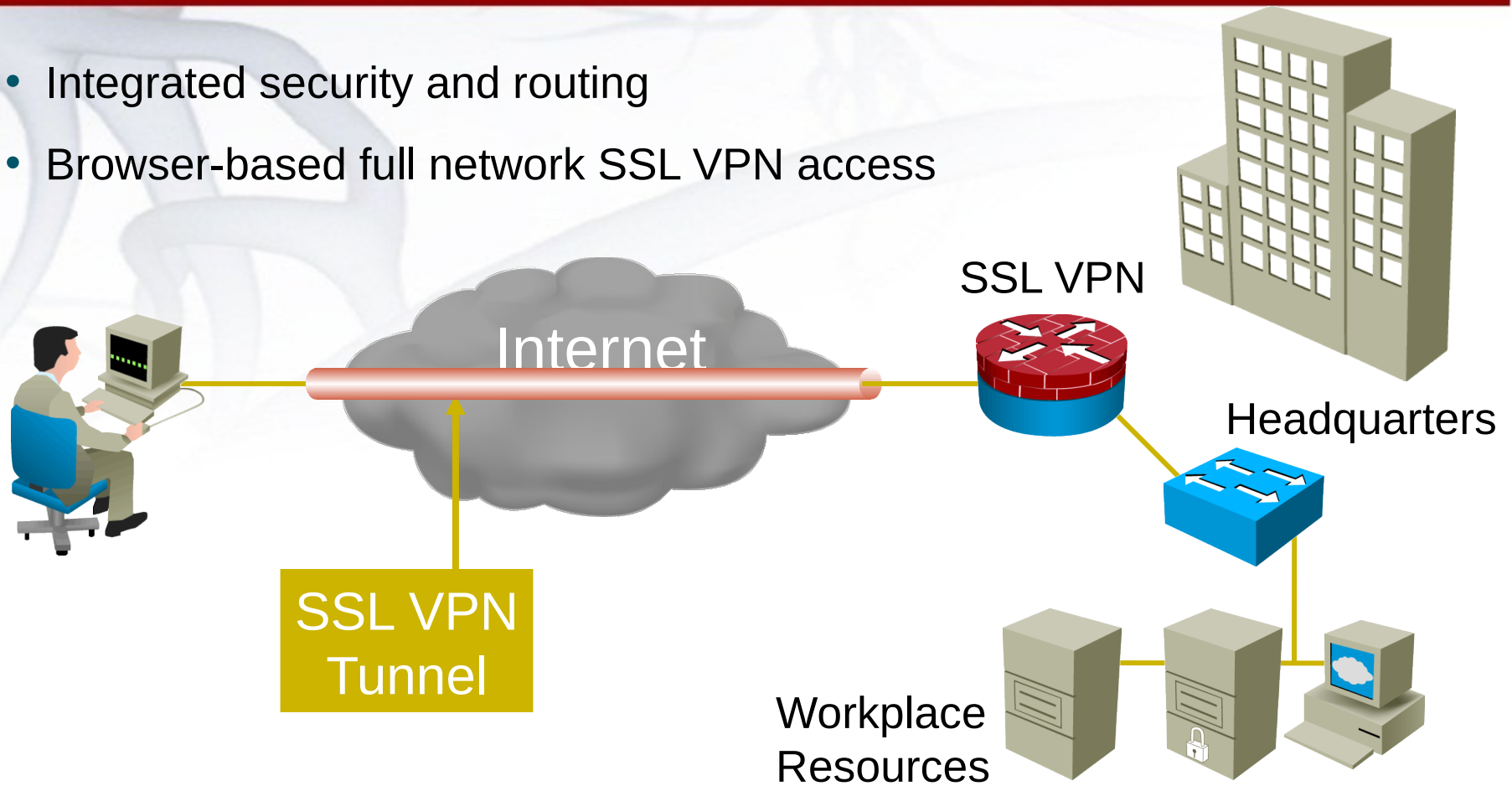


Comparison of SSL and IPSec

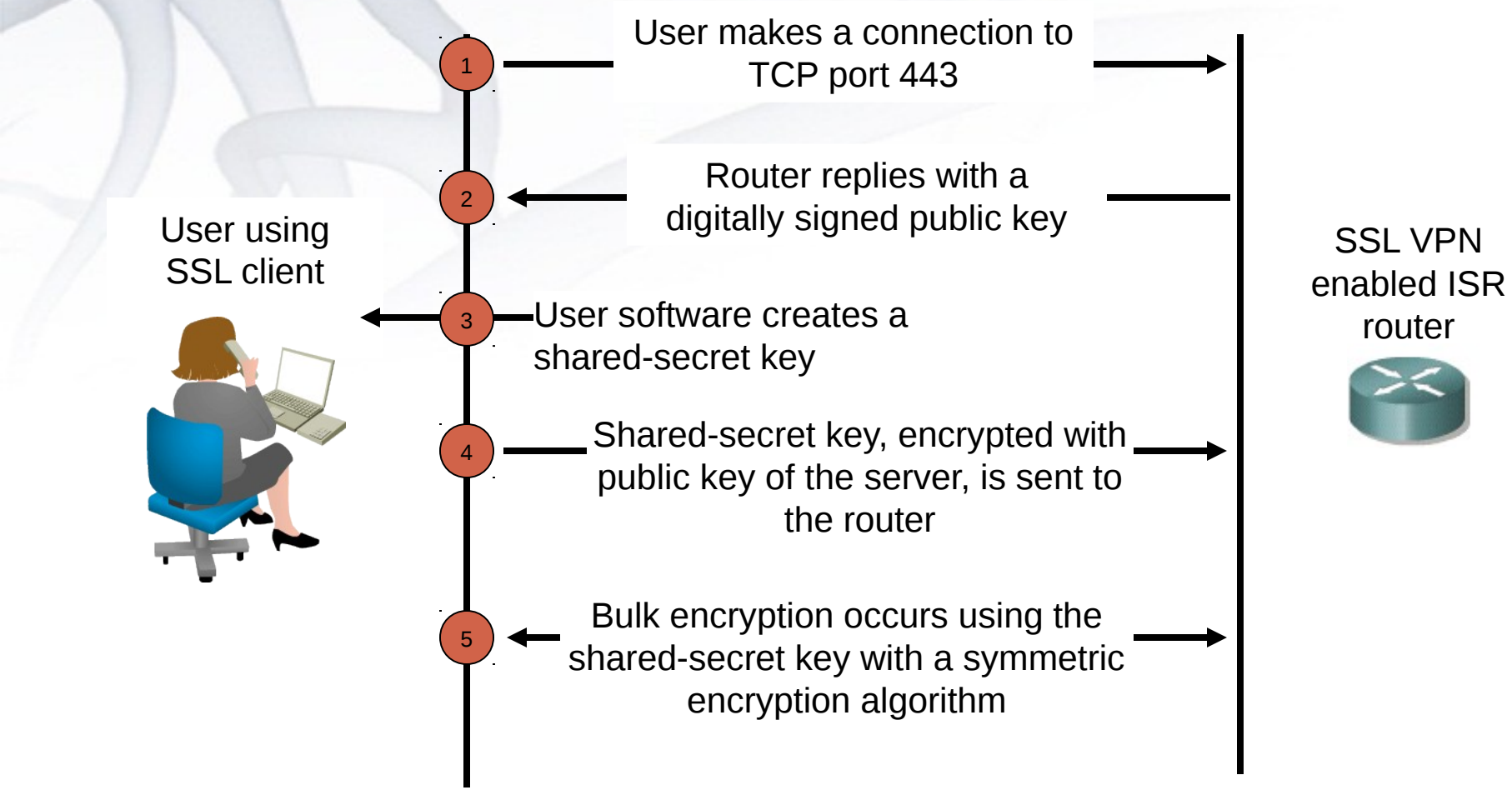
	SSL	IPsec
Applications	Web-enabled applications, file sharing, e-mail	All IP-based applications
Encryption	**Moderate** Key lengths from 40 bits to 128 bits	**Stronger** Key lengths from 56 bits to 256 bits
Authentication	**Moderate** One-way or two-way authentication	**Strong** Two-way authentication using shared secrets or digital certificates
Ease of Use	**Very high**	**Moderate** Can be challenging to nontechnical users
Overall Security	**Moderate** Any device can connect	**Strong** Only specific devices with specific configurations can connect

SSL VPN

- Integrated security and routing
- Browser-based full network SSL VPN access



Establishing SSL session

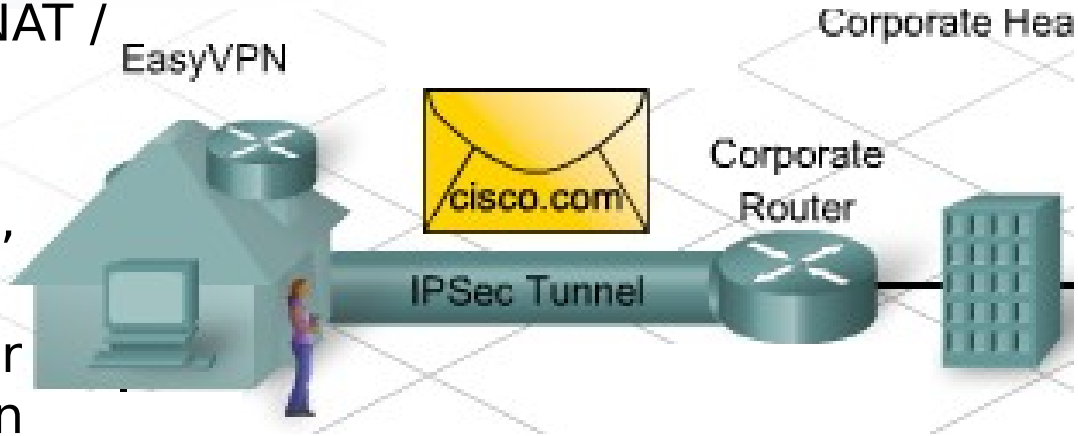


SSL VPN Design Considerations

- User connectivity
- Router feature
- Infrastructure planning
- Implementation scope

Cisco Easy VPN

- Negotiates tunnel parameters
- Establishes tunnels according to set parameters
- Automatically creates a NAT / PAT and associated ACLs
- Authenticates users by usernames, group names, and passwords
- Manages security keys for encryption and decryption
- Authenticates, encrypts, and decrypts data through the tunnel



Securing the VPN