What Is IPSec?

- Network layer encryption and authentication
- Open standards for ensuring secure private communications
- Provides a necessary component of a standards-based, flexible solution for deploying a Network-wide security policy

Security Architecture for IP

Målet med IPsec ar att tillhandahålla olika säkerhetstjänster på IP-nivå. Denna typ av skydd, ofta kallat "VPN" (Virtual Private Network), har hittills varit leverantörsbundet. Del nya med IPsec ar att del ar en leverantörsoberoende öppen säkerhetsarkitektur, som kommer från standardiseringsorganisationen IETF. IPsec har etablerat sig som en branschstandard för VPN-teknik, med vars hjälp även leverantörsoberoende VPN-lösningar ska kunna realiseras.

Med IPsec kan ett datorsystem välja hur skyddet ska utformas. Detta sker genom att välja krypterings- och autenticeringsalgoritmer. Idag finns två säkerhetsprotokoll definierade: Authentication Header (AH) och Encapsulating Security Payload (ESP). AH erbjuder möjligheten att verifiera avsändarens identitet och kontrollera att meddelandet 9r akta. ESP erbjuder förutom detta även sekretess.

Säkerhetsprotokollen är inte bundna till en specifik krypton- eller auteticeringsalgoritm, utan de kan användas med olika algoritmer.
IPsec erbjuder även möjligheten att automatiskt utbyta krypteringsnycklar mellan två parter. Idag tillhandahålls denna tjänst med protokollet IKE (The Internet Key Exchange).

Benefits of IPSec

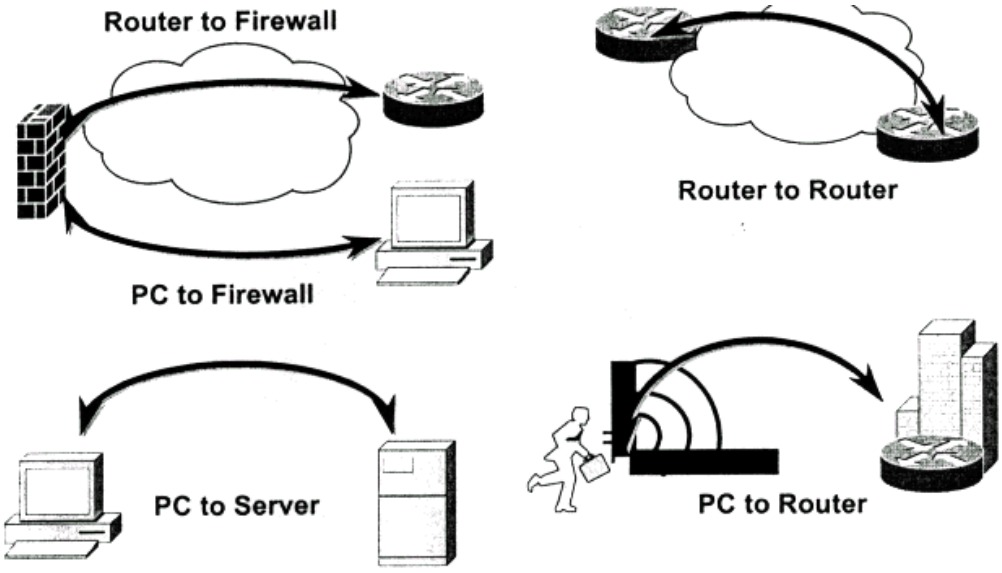
- Standard for privacy, integrity and authenticity for networked commerce
- Implemented transparently in the Network infrastructure . End-to-end security solution including routers, firewalls, PCs

IPsec
IPsec kan erbjuda trafiken följande säkerhetstjänster på IP-nivå:

Sekretessen:
Verifiering av avsändarens identitet
Kontroll av meddelandet äkthet

Trafikfiltrering:
Avvisning av återuppspelad trafik
IPsec kan användas av alla IP-baserade protokoll, t ex TCP, UDP och ICPM.

IPsec Everywhere!



Transport och Tunnel mode

Säkerhetsprotokollen AH och ESP kan köras i "transport mode" eller "tunnel mode".

I tunnel mode kapslas hela del IP-datagram som ska skyddas, inklusive IP-headern, in i ettnytt IP-datagram.

I transport mode används den ursprungliga IP-headern, dvs det är de högre nivåernas protokoll, over IP-nivån, som skyddas.

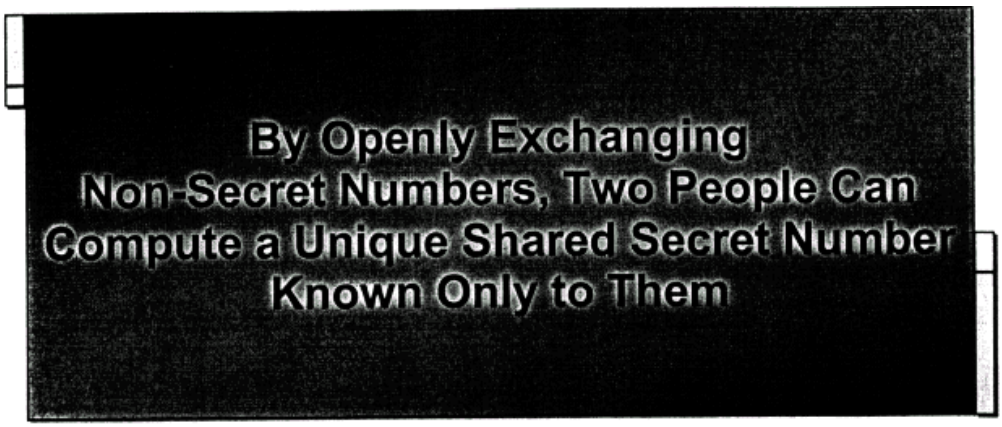
En SG (Security Gateway) arbetar endast i Tunnel mode, dvs trafiken till och från en SG använder sig av den yttre IP-headern, medan adressering av den slutliga källan och destinationen sker med den inre IP-headern (den inkapslade IP-headern).

En Host-implementation ska kunna hantera bade transport och tunnel mode.

Keyed Hashing for Authentication

Secret key and message is hashed together with a hash function.
Recomputation of **digest** verifies that **message** originated **with peer** and that **message was** not altered in transit

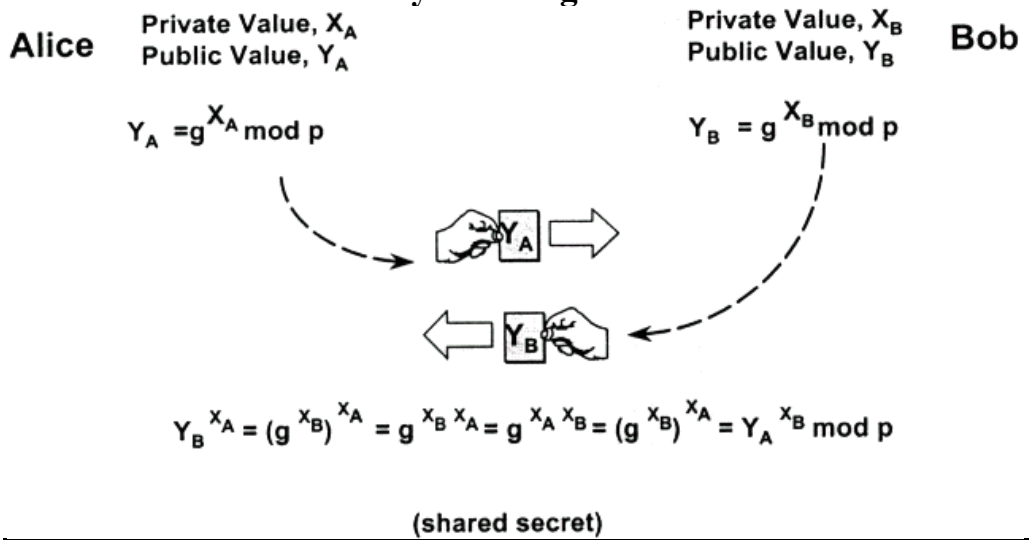
Diffie-Hellman Key Exchange (1976)



Basics of Diffie-Hellman

- One large prime number g Is made public
- Computing g^R is fast
- Computing R from g^R is much more difficult
- Modular arithmetic (mod p) actually used => nearly impossible to get back R

Diffie-Hellman Public Key Exchange



IKE och Diffie-Hellman-algoritmen
IKE använder Diffie-Hellman-algoritmen for att beräkna en gemensam hemlighet, vilken i sin tur används för att generera nycklar.

Observera att talen; G, P, A och B ej är hemliga. Talen G och P kan vara publik information, medan A och B sänds i klartext mellan parterna.

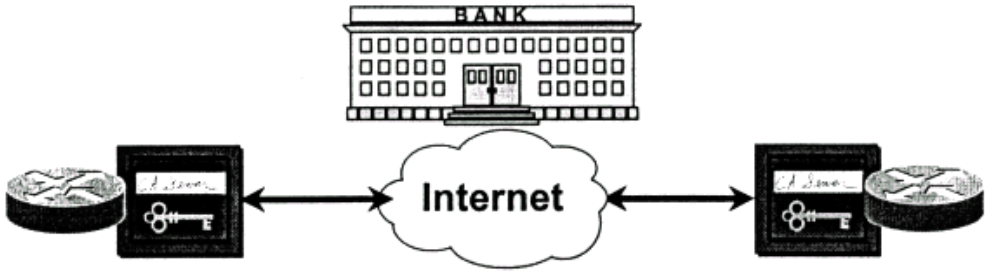
I IKE är talen G och P förutbestämda och definieras i olika grupper, där varje grupp har sitt förbestämda värde for G och P. Två olika grupper, som bygger pa "Classical Diffie-Hellman Modular Exponential Groups", firms defenierade i IKE (grupp 1 - 2).

Även varianten av Diffie-Hellman som använder sig av beräkning av elliptiska kurvor (polynom) kan användas av IKE.

De olika fördefinierade "grupperna" för Diffie-Hellman-algoritmen är:

.A modular exponentiation group with a 768 bit modulus
.A modular exponentiation group with a 1024 bit modulus
.An elliptic curve group over GF[2^155]
.An elliptic curve group over GF [2^185]

Using Certificates

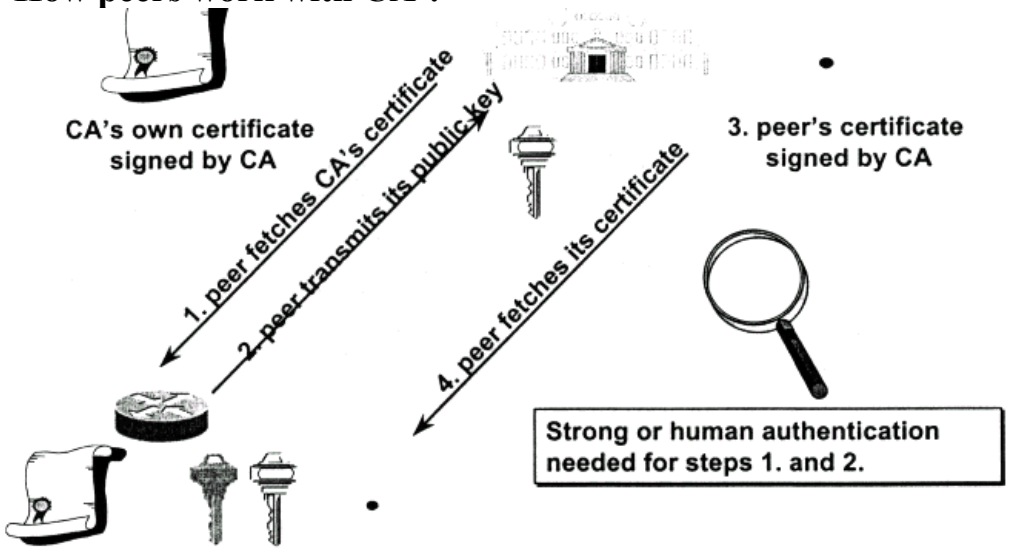


- Certificate Authority (CA) verifies identity
- CA signs digital certificate containing device public key
- Certificate equivalent to an ID card

Digital Certificate

- A digital certificate contains:
- Serial number of the certificate
- Issuer algorithm information .Valid to/from date
- User public key information
- Signature of Issuing authority

How peers work with CA ?



0. peer generates **public/private** key pair

Certification Authority

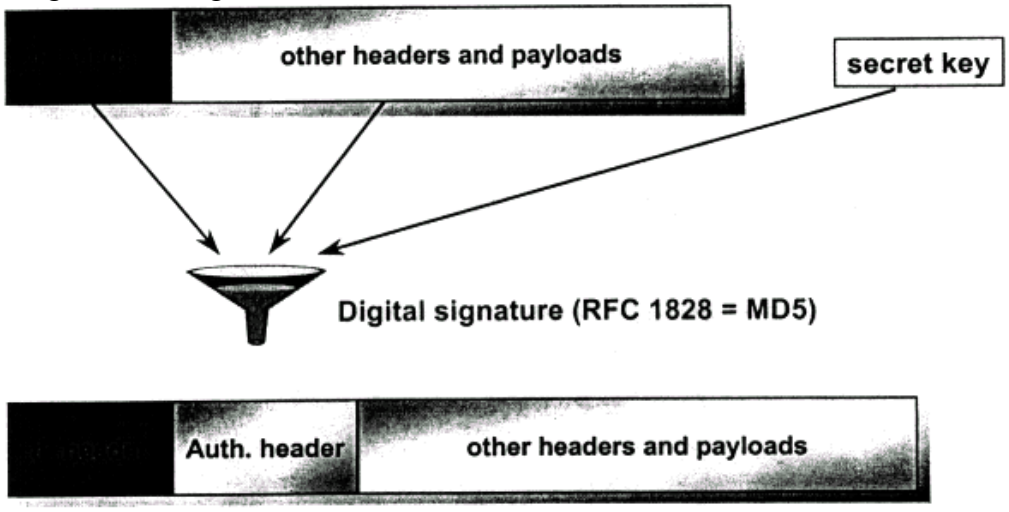
- CA is *a* software
- main purpose of CA = sign certificates after valid authentication
- private key of CA is the 'most secret' key .
- CA can be offline or online
- CA is used only:
    - on Installation
    - public key changes
    - renewal of certificates

IPsec: Authentication Header

- RFC 1826 Aug '95 without anti-replay
- RFC 2085 Feb '97 with anti-replay
- Authentication Header, AH
- additional header inside the IP datagram
- MD5 can be used (RFC 1828),
- or... (currently IETF drafts)

IPsec AH (Cont.)

Original IP datagram



Authenticated IP datagram

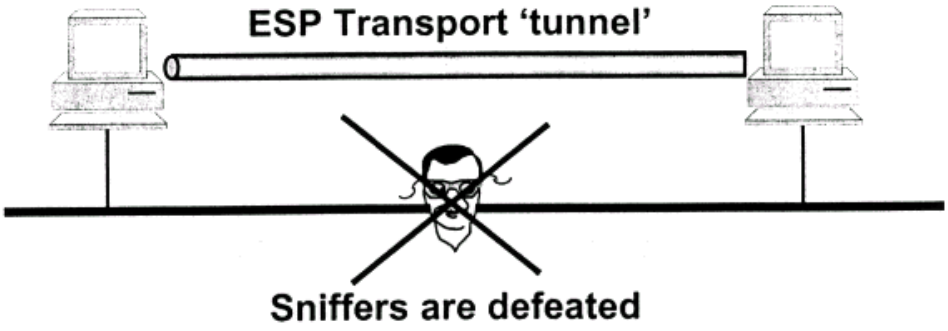
ESP packet

IPsec Encapsulating Security Payload

- RFC 1827 Aug '95
- Encapsulation Security Payload, ESP
- confidentiality of whole IP datagram (tunnel)
  - TCP or UDP payload only (transport) .
- DEScan be used (RFC1829)
- or... (currently IETF drafts) also with authentication in ESP

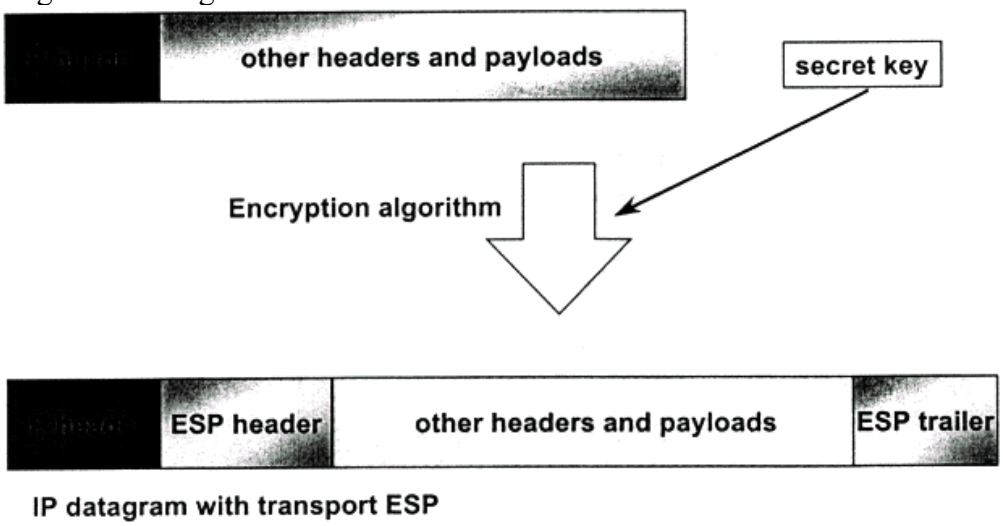
IPsec ESP Transport

Can be used end to end, between host



IPsec ESP Transport

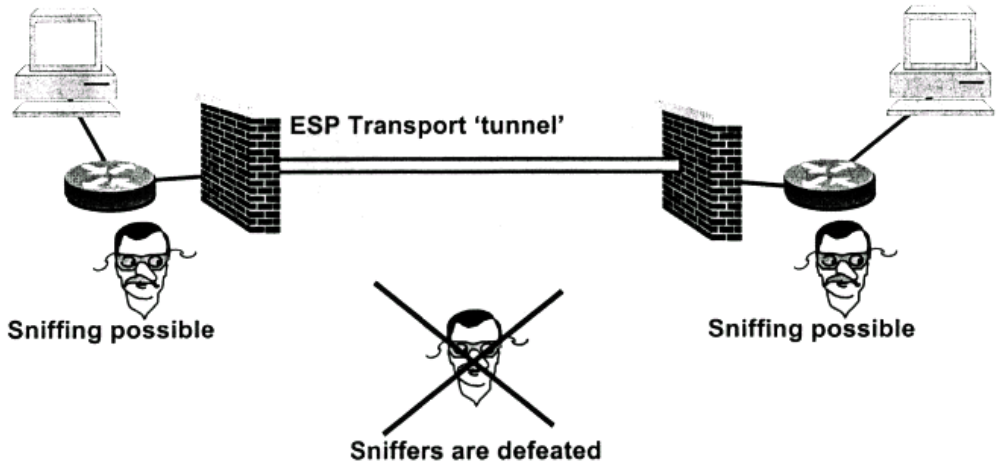
Original IP datagram



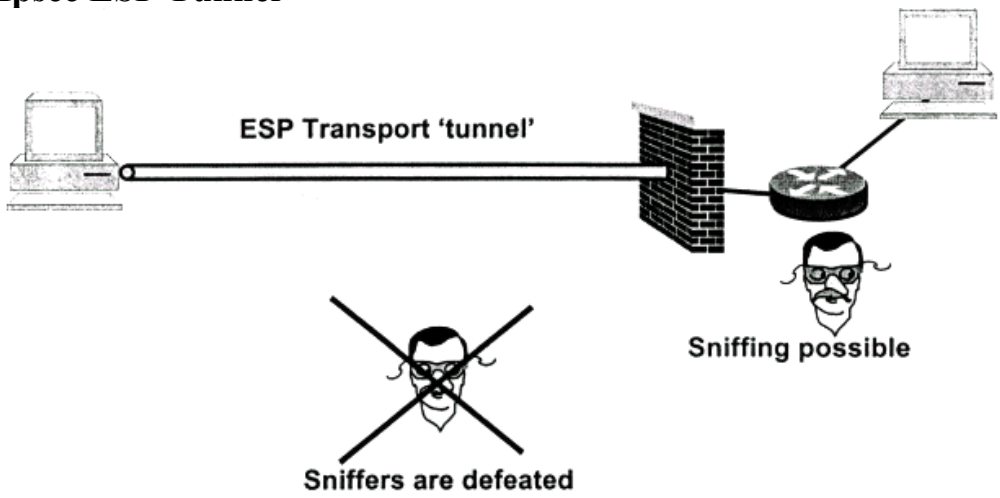
IP datagram with transport ESP

IPsec ESP Tunnel

Usually between firewalls for VPN



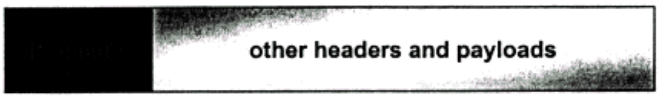
Ipsec ESP Tunnel

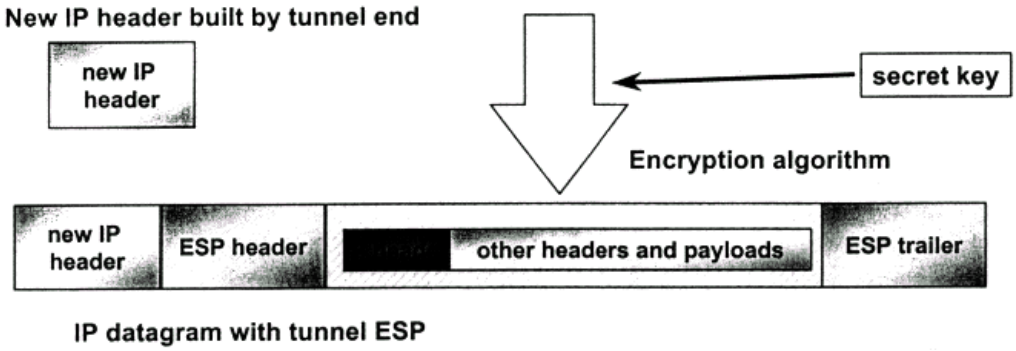


Between client and Firewall, often for VPDN.

IPsec ESP Tunnel

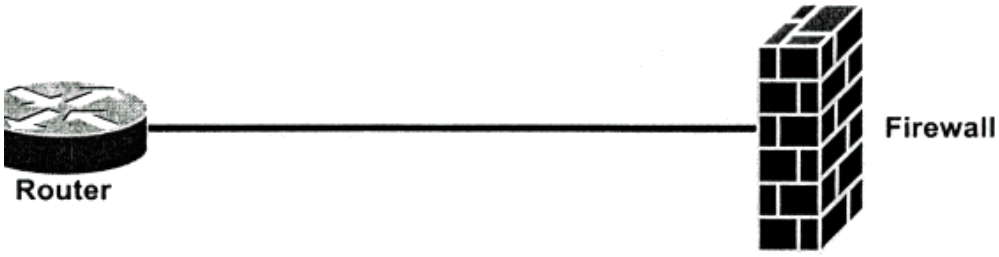
Original IP datagram





IP datagram with tunnel ESP

Security Association (SA)

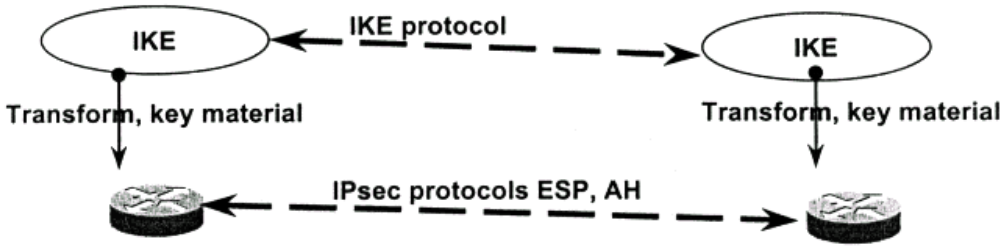


- Agreement between two entitles based on a security policy, including:
    - Encryption algorithm
    - Authentication algorithm
    - Shared session keys
    - SA lifetime
- Unidirectional. Two-way communication consists of two SA's

IKE

- Negotiates policy to protect communication
- Authenticated Diffie-Hellman key exchange
- Negotiates {possibly multiple) security associations for IPSec

IPsec needs IKE



IPsec SA needs for all peers:
- which transform
- which key

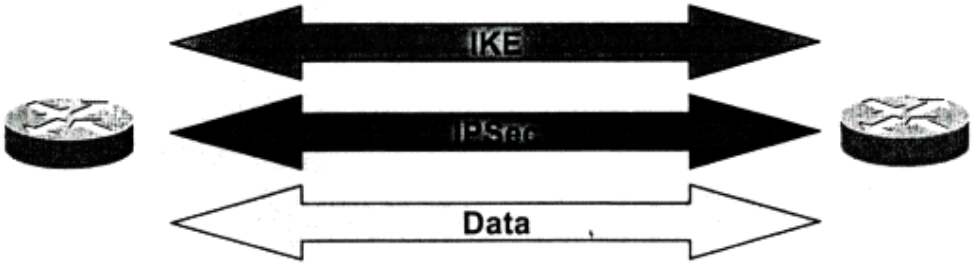
Perfect Forward Secrecy (PFS)

- Compromise of a single key will permit access to only data protected by that particular key.
- IKE provides PFS if required by using Diffie-Hellman for each rekey
- If PFS not required, can refresh key material without using Diffie Hellman

IKE Authentication

- Signatures
- Encrypted nonce's
- Pre-shared key

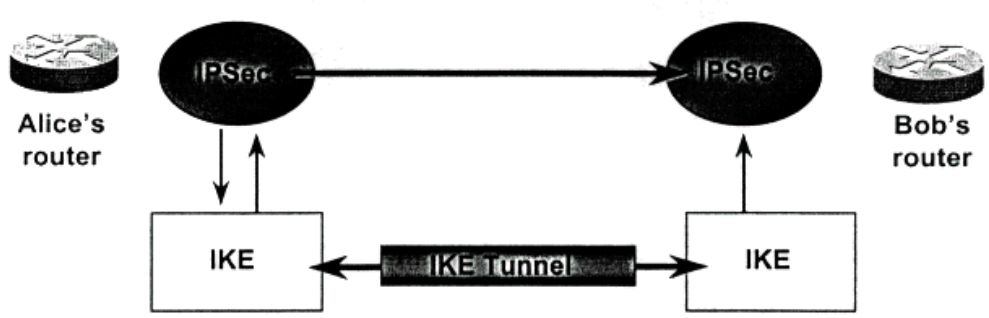
Initiating New Connections



- Establish IKE SA—"Main mode"
- Establish IPSec SA—"Quick mode"
  Multiple quick modes for each main mode
- Send protected data

How IPSec Uses IKE

1. Outbound packets from Alice Bob, no IPSec SA.



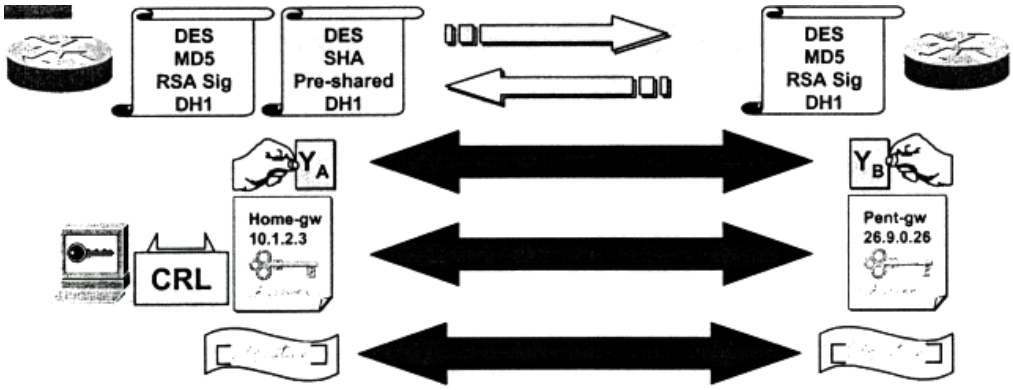
2. Alice's IKE begins negotiation Bob's.
.

3. Negotiation complete. with Alice and Bob now have complete set of SAs in place

4. Packets sent from Alice to protected by IPSec SA

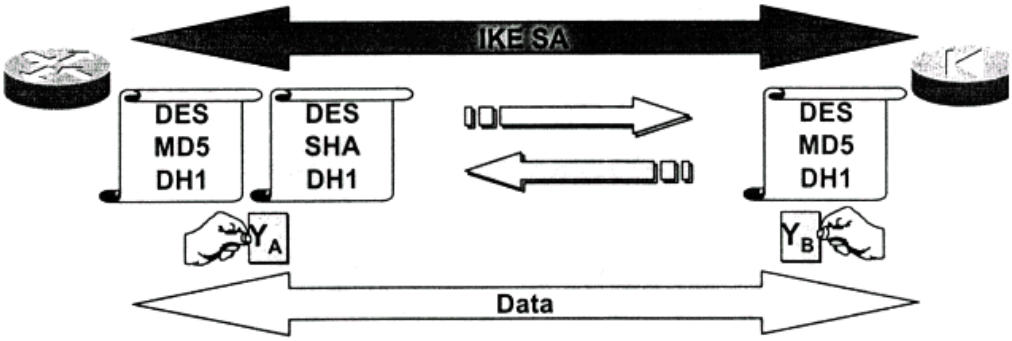
Creating an IKE SA

>>>



- Negotiate IKE parameters
- Exchange DH Numbers
- Exchange Certificates and check CRL
- Exchange signed data for authentication

Creating IPSec SA—Quick Mode

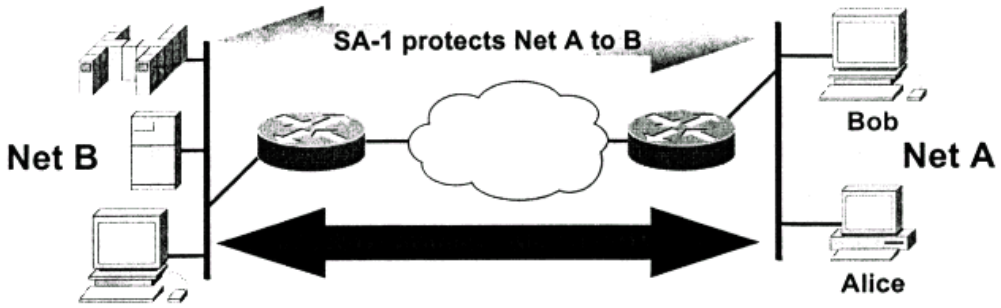


- Requires IKE SA to be in place
- Negotiate IPSec parameters
- Create shared session key

Local policy:

Exchange DH numbers for PFS or Exchange nonces for quick rekey.

Overlapping Security Associations

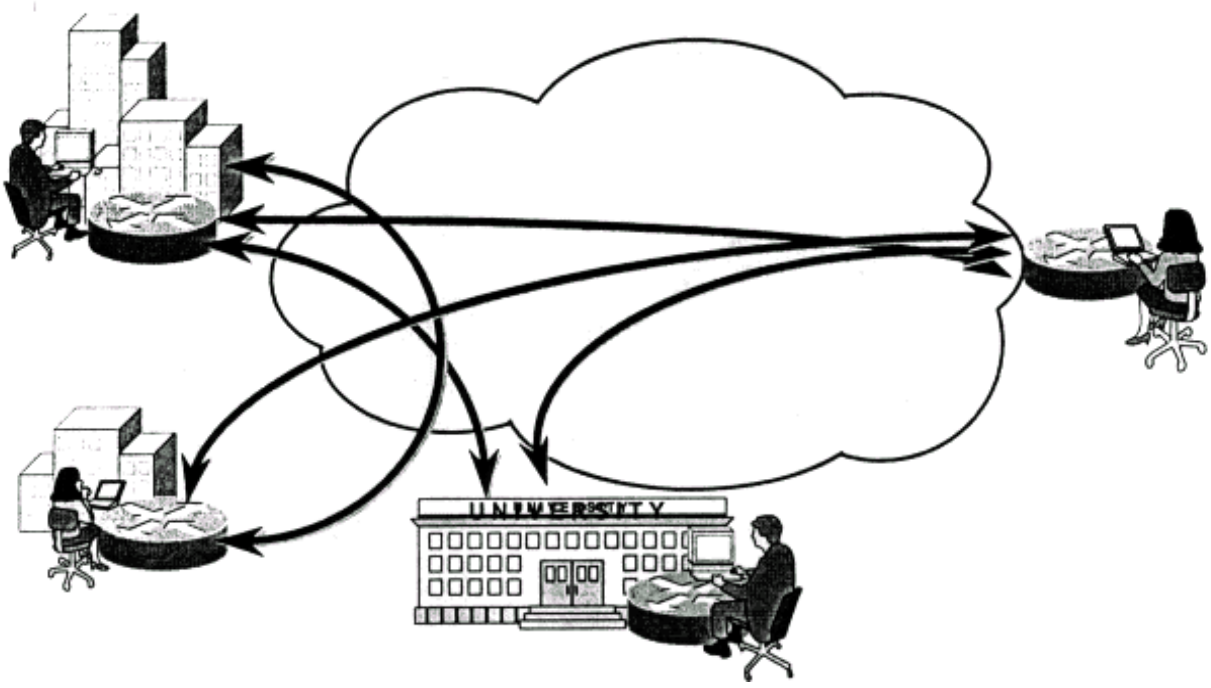


- Multiple, overlapping security associations
- Selectable with extended access lists

Dynamic Crypto Maps

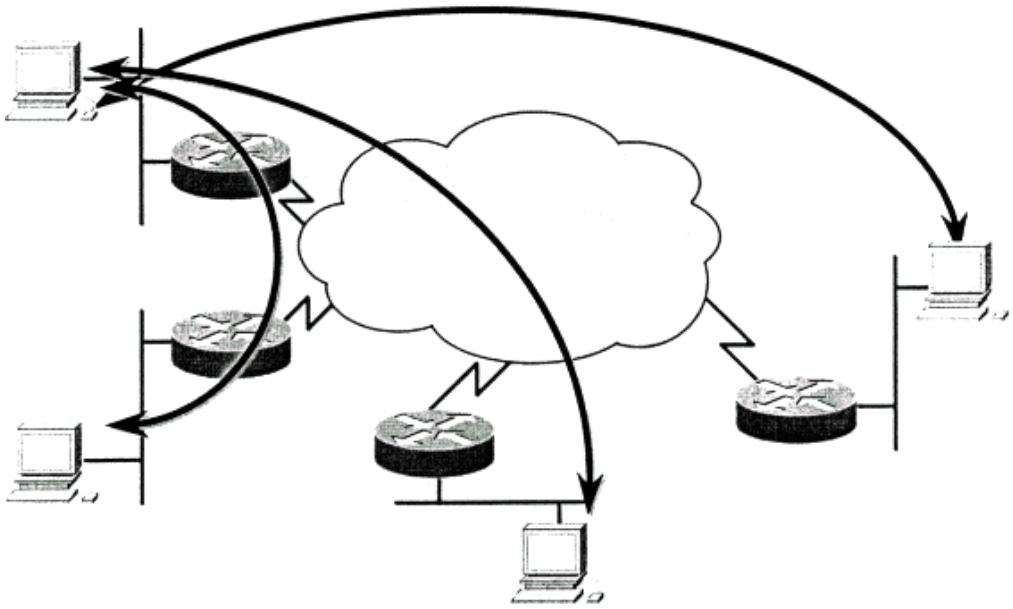
- **Enables easy configuration for remote clients**
- **Crypto map template created without defining a peer**
- **If incoming IPSec SA request is accepted, then a temporary cryptomap entry is created**

Different Keys Everywhere

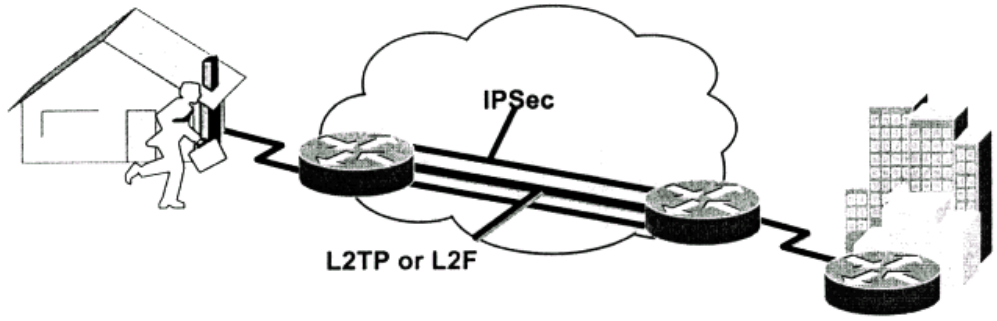


Ensure Confidential Communications in an unsecured Network!

Define Sensitive Traffic for Each “situation”



Enable Mobile Users with L2TP and IPSec



- IPSec protects traffic from remote sites to the enterprise using any application
- IPSec may be combined with L2TP or L2F
- Travelers can access the Network as securely as they would In the office

Other Issues

- QoS
  IPSec copies IP type of service bits from original IP header
  IETF working on additional solutions
- Compression
  IP Packet Compression Protocol (IPPCP)
  Compress data packet by packet

- Chaining and tunneling
  SSH
  SSL