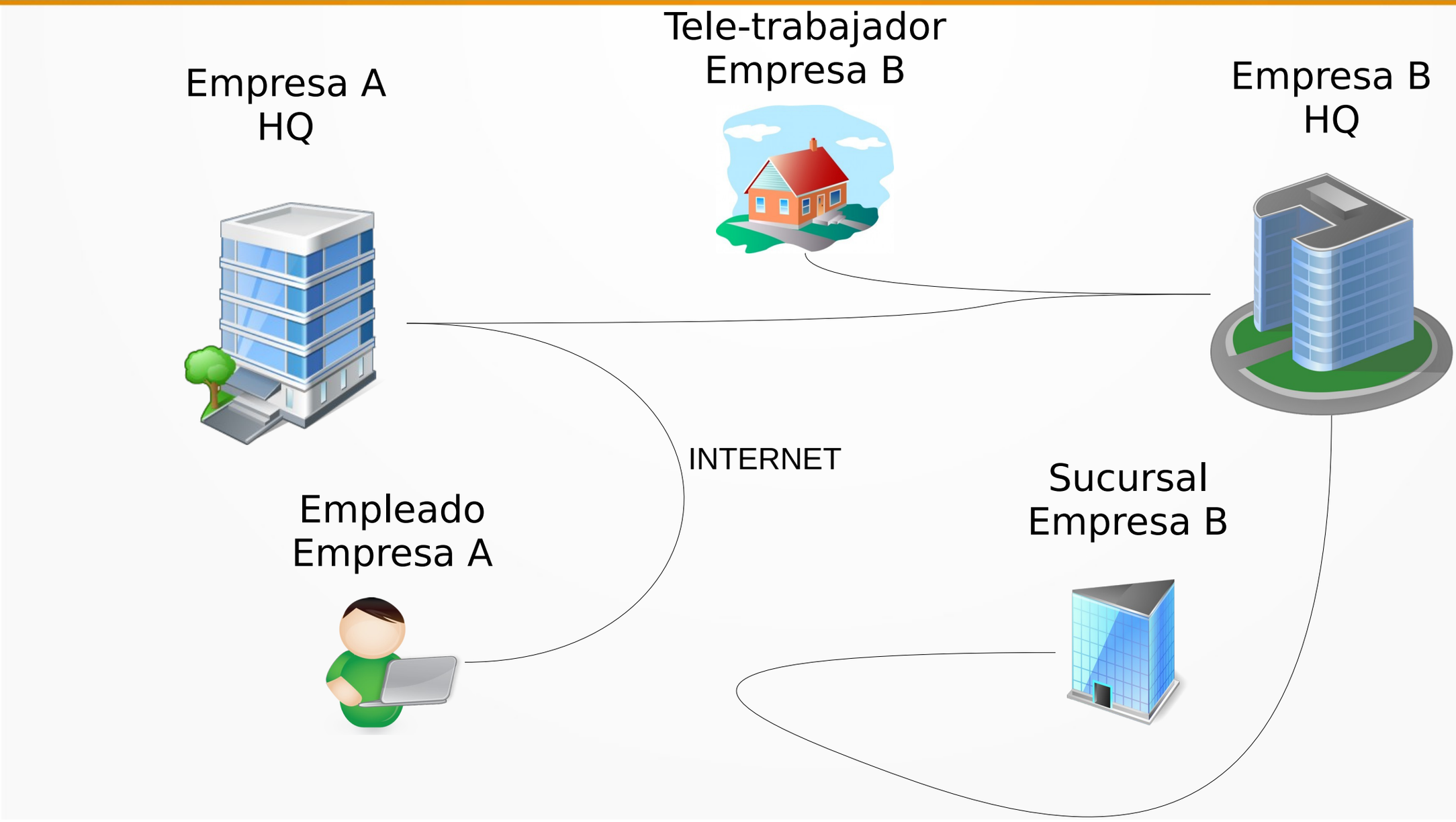
VPN IPsec

- **Requerimientos**
- **Configuración**

VPN


Tele-trabajador
Empresa B
Empresa A
HQ
Empresa B
HQ
INTERNET
Empleado
Empresa A
Sucursal
Empresa B

VPN (Cont.)

- Ahorro en costos de implementación
  - VS lineas dedicadas
  - Utilización de diferentes tecnologías y capacidades de acceso a internet
- Seguridad
  - Decisiones caso x caso: largos llaves, algoritmos, acceso a recursos
- Escalabilidad
  - Sin necesidad de agregar infraestructura significativa

Proveedor vs Empresarial

- **VPN empresariales:** solución común para proteger el tráfico empresarial a través de Internet. Las VPN de sitio a sitio y de acceso remoto son creadas y administradas por la empresa mediante Ipsec, OpenVpn, etc.

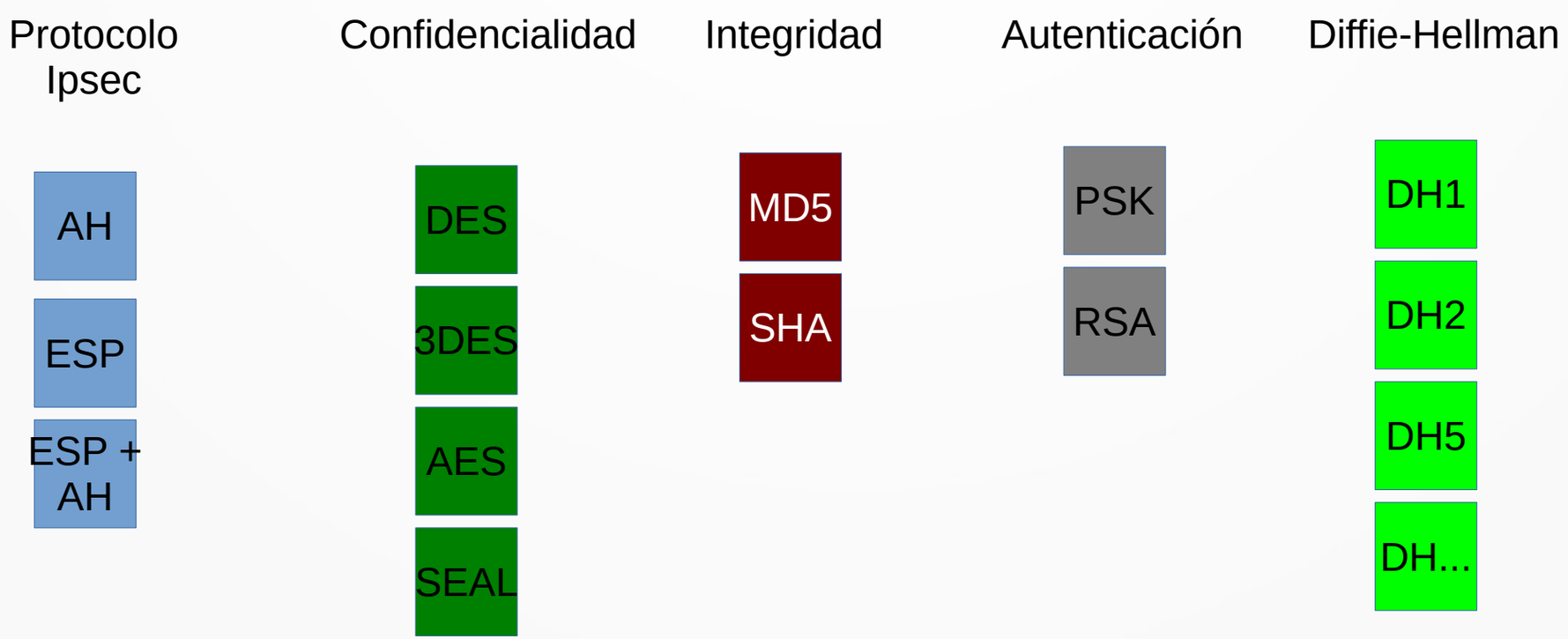
- **VPN de proveedores de servicios:** creadas y administradas por la red del proveedor. Puede utilizar MPLS (Multi-Protocol Label Switching) en la capa 2 o la capa 3 para crear canales seguros entre los sitios de una empresa, separando el tráfico de otro tráfico de clientes.

VPN (Cont.)

- Implementación en Capa 3
  - Punto a Punto
    - GRE (Cisco usado en conjunto con IPsec)
    - EoIP (MikroTik Basado en GRE)
    - TLS (OpenVPN)
    - **Ipsec**
  - Multipunto
    - MPLS (Proveedor de servicio)
    - Hub-to-Spoke - Spoke-to-Spoke

IPsec

- Framework de estandares abiertos que definen las reglas para lograr la comunicación segura



IPsec (con.)

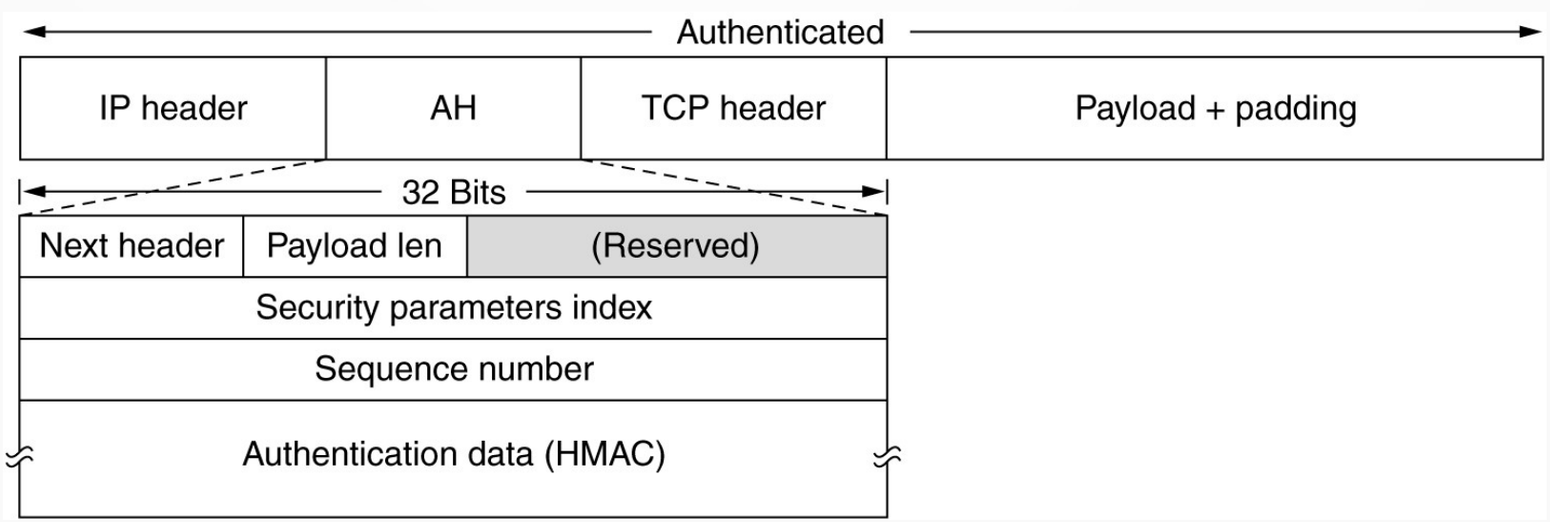
- DH Group
  - Confidencialidad simétrica, intercambio seguro de llaves
  - DH 1,2,5: key size 768, 1024, 1536 bits (DES, 3DES, no recomendados hoy dia)
  - DH 14,15,16: key size 2048, 3072, 4096 bits (AES)
  - DH 19,20,24: Elliptical Curve, key size 256, 384, 2048 bits (preferidos)

IPsec (cont.)

- Protocolo Ipsec
  - AH: Authentication Header
    - IP protocol 51
    - Provee Autenticidad, Integridad
  - ESP: Encapuslating Security Payload
    - IP protocol 50
    - Provee Confidencialidad, Autenticidad + Integridad

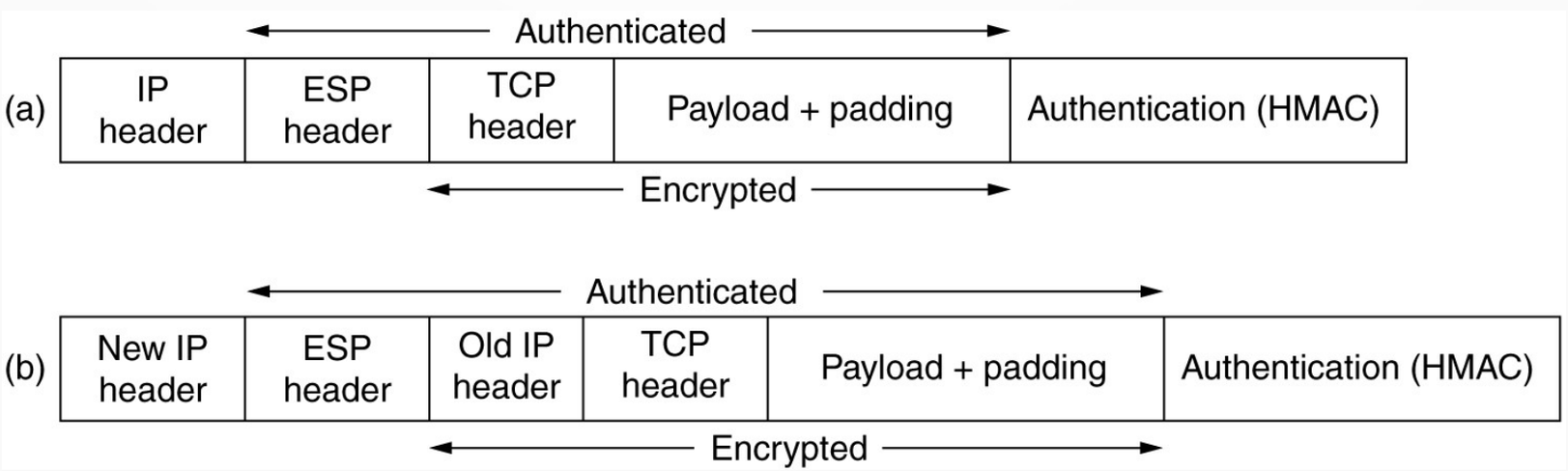
IPsec (cont)

- Paquete con AH
  - Se hace un hash del encabezado IP y el payload
  - Se implementa en un nuevo encabezado AH que se inserta en el paquete original
  - Problema si existe NAT, ya que cambia el encabezado



IPsec (cont)

- Paquete con ESP
  - a) modo transporte
    - Provee seguridad solo para capa de transporte
  - b) modo tunel
    - El paquete original completo es cifrado



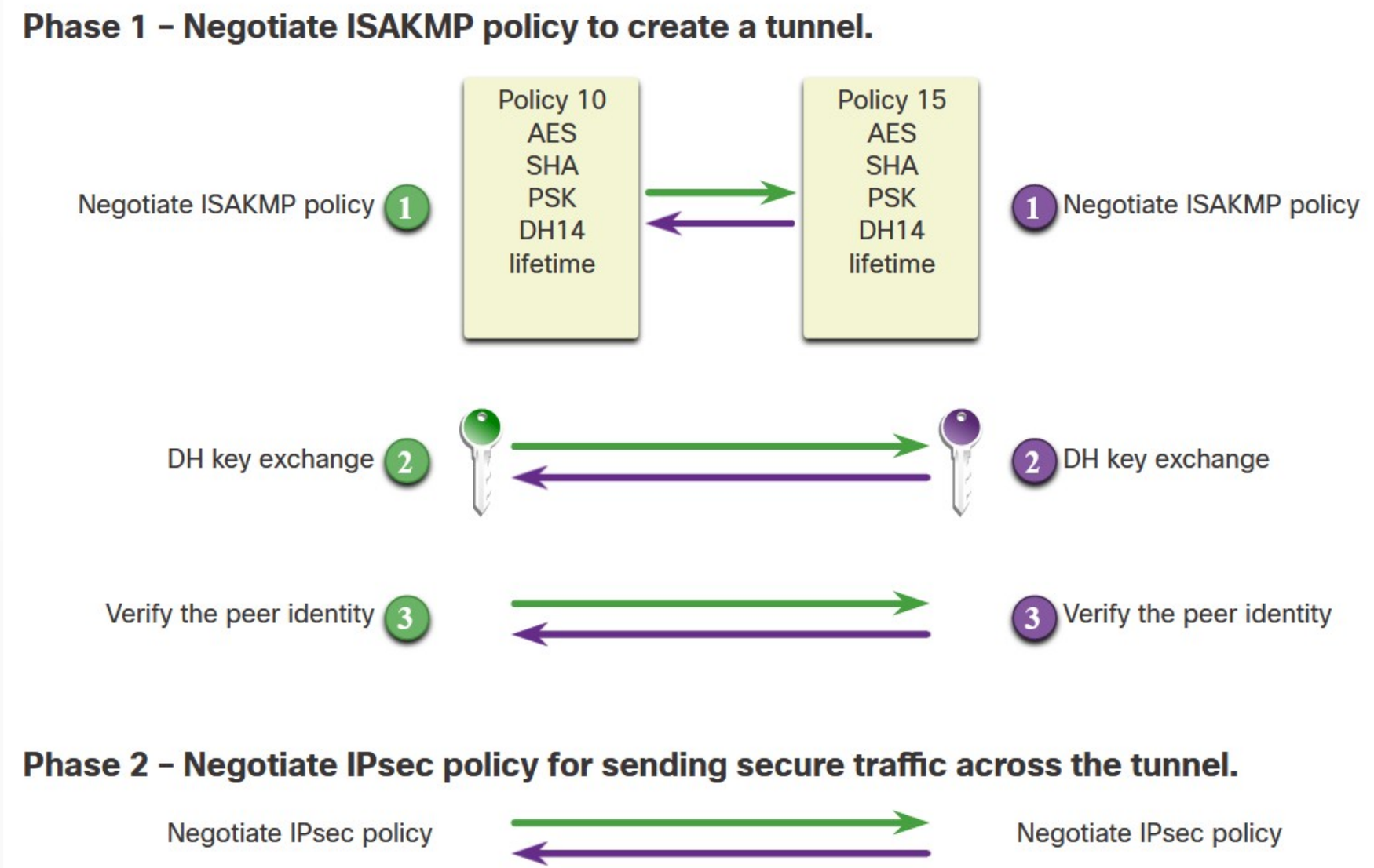
IPsec (cont)

- SA: Security Association
  - Comprende los parámetros negociados entre dos dispositivos
    - Parámetros de intercambio de llaves
    - Establecimiento de llave compartida
    - Autenticación del par
    - Parámetros de cifrado

IPsec (cont)

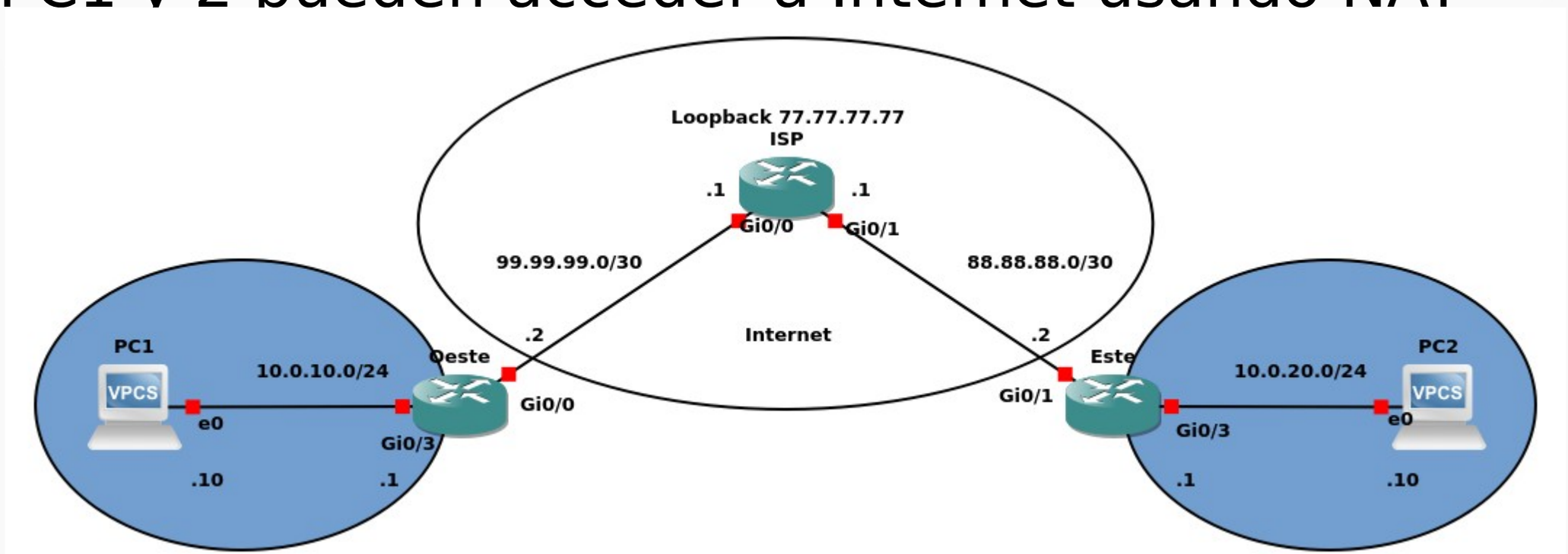
- IKE: Internet Key Exchange
  - UPD puerto 500
  - Fase 1: Negociar los conjuntos de politicas ISAKMP (Internet Security Association and Key Management Protocol), autenticar pares, establecer un canal seguro entre pares
    - Main mode (mas largo)
    - Agressive mode (mas corto)
  - Fase 2: Negocia IPsec transform sets (parametros de seguridad), establece SAs unidirieccionales (uno por cada combinacion de protocolo y algoritmo), renegocia periodicamente las SAs para reforzar la seguridad, opcionalmente puede realizar intercambio adicional de DH
    - Quick mode

IKEv1


Phase 1 – Negotiate ISAKMP policy to create a tunnel.
Policy 10
AES
SHA
PSK
DH14
lifetime
Policy 15
AES
SHA
PSK
DH14
lifetime
Negotiate ISAKMP policy 1
1 Negotiate ISAKMP policy
DH key exchange 2
2 DH key exchange
Verify the peer identity 3
3 Verify the peer identity
Phase 2 – Negotiate IPsec policy for sending secure traffic across the tunnel.
Negotiate IPsec policy
Negotiate IPsec policy

Topologia de Laboratorio

- Se debe configurar un tunel IPsec para comunicar de manera segura las redes LAN de Este/Oeste las cuales están conectadas a Internet
- PC1 y 2 pueden acceder a Internet usando NAT



Config IPsec

Requerimientos de Seguridad

- Cifrar el trafico con AES 256
- Integridad con SHA.
- Autenticar con PSK.
- Intercambio de llaves con DH grupo 24.
- Tiempo de vida de 1 hora para el tunel ISAKMP.
- Usar ESP en el tunel IPsec con un tiempo de vida de 15 minutos

Tareas de configuración:

1) Configurar la Politica de ISAKMP para la Fase 1 de IKE
2) Configurar la Politica de IPsec (Transform-Set) para la Fase 2
3) Configurar un Crypto Map para la politica de IPsec
4) Aplicar la politica de IPsec
5) Verificar que el tunel funciona

Politicas ISAKMP preconfiguradas

- Cisco trae preconfiguradas varias políticas de ISAKMP por defecto

```
Router#show crypto isakmp default policy

Default IKE policy
Default protection suite of priority 65507
        encryption algorithm:     AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:           Secure Hash Standard
        authentication method:    Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:     #5 (1536 bit)
        lifetime:                 86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:     AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:           Secure Hash Standard
        authentication method:    Pre-Shared Key
        Diffie-Hellman group:     #5 (1536 bit)
        lifetime:                 86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:     AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:           Message Digest 5
        authentication method:    Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:     #5 (1536 bit)
        lifetime:                 86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:     AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:           Message Digest 5
      authentication method:      Pre-Shared Key
        Diffie-Hellman group:     #5 (1536 bit)
        lifetime:                 86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:     Three key triple DES
        hash algorithm:           Secure Hash Standard
        authentication method:    Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:     #2 (1024 bit)
        lifetime:                 86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:     Three key triple DES
        hash algorithm:           Secure Hash Standard
        authentication method:    Pre-Shared Key
        Diffie-Hellman group:     #2 (1024 bit)
        lifetime:                 86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:     Three key triple DES
        hash algorithm:           Message Digest 5
        authentication method:    Rivest-Shamir-Adleman
Signature
        Diffie-Hellman group:     #2 (1024 bit)
        lifetime:                 86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:     Three key triple DES
      hash algorithm:             Message Digest 5
        authentication method:    Pre-Shared Key
        Diffie-Hellman group:     #2 (1024 bit)
        lifetime:                 86400 seconds, no volume limit
```

Configurar politica ISAKMP

```
Router(config)# crypto isakmp policy ?
  <1-10000>  Priority of protection suite

Router(config)# crypto isakmp policy 1
Router(config-isakmp)#?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

Configurar Politica ISAKMP (cont)

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#hash sha
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 24
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#lifetime 3600

Router#sh crypto isakmp policy
Global IKE policy
Protection suite of priority 1
  encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
  hash algorithm:    Secure Hash Standard
  authentication method:Pre-Shared Key
  Diffie-Hellman group: #24 (2048 bit, 256 bit subgroup)
  lifetime:  3600 seconds, no volume limit
```

Configurar Pre-Shared Key

- Debemos definir que llave utilizamos para autenticar el otro extremo del tunel

```
Router(config)#crypto isakmp key contraseña address dir.ip.otro.extremo
```

Definir trafico interesante

- Crear una ACL para definir que trafico levanta el tunel Ipsec. Esta lista se utilizará en la configuración del crypto map
- Ej:

```
Router(config)# access-list 101 permit ip 10.0.10.0 0.0.0.255 10.0.20.0 0.0.0.255
```

Configurar el IPsec Transform Set

```
Router(config)#crypto ipsec transform-set ?
  WORD  Transform set tag
Router(config)#crypto ipsec transform-set este-oeste ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  ah-sha256-hmac   AH-HMAC-SHA256 transform
  ah-sha384-hmac   AH-HMAC-SHA384 transform
  ah-sha512-hmac   AH-HMAC-SHA512 transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-3des         ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes          ESP transform using AES cipher
  esp-des          ESP transform using DES cipher (56 bits)
  esp-gcm          ESP transform using GCM cipher
  esp-gmac         ESP transform using GMAC cipher
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-null         ESP transform w/o cipher
  esp-seal         ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac  ESP transform using HMAC-SHA512 auth
```

El Transform-set representa una cierta combinación de protocolos y algoritmos de seguridad.
Durante la negociación de IPsec SA, los pares acuerdan utilizar un Transform-set especifico para proteger un flujo de datos en particular.

```
Router(config)#crypto ipsec transform-set este-oeste esp-aes esp-sha-hmac
```

Configurar Crypto Map

- Necesitamos enlazar todas las configuraciones en un crypto map: la ACL, el transform-set, la IP del otro extremo, el grupo DH y el tiempo de vida del tunel Ipsec

Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp**

```
Router(config)# crypto map mapa-este-oeste 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
  and a valid access list have been configured.
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set transform-set este-oeste
Router(config-crypto-map)#set peer 88.88.88.2
Router(config-crypto-map)#set pfs group24
Router(config-crypto-map)#set security-association lifetime seconds 900
```

- Aplicamos el Crypto Map en la interfaz que implementa el tunel

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#crypto map mapa-este-oeste
```

Verificación en IOS

```
Router#show crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst             src             state          conn-id status

88.88.88.2      99.99.99.2      QM_IDLE           1001 ACTIVE
```

```
Router#sh crypto map

Crypto Map IPv4 "mapa-este-oeste" 10 ipsec-isakmp
    Peer = 88.88.88.2
    Extended IP access list 101
        access-list 101 permit ip 10.0.10.0 0.0.0.255 10.0.20.0
0.0.0.255
    Current peer: 88.88.88.2
    Security association lifetime: 4608000 kilobytes/900 seconds
    Responder-Only (Y/N): N
    PFS (Y/N): Y
    DH group:  group24
    Mixed-mode : Disabled
    Transform sets={
        este-oeste:  { esp-aes esp-sha-hmac  } ,
    }
    Interfaces using crypto map mapa-este-oeste:
        GigabitEthernet0/0
```

Verificación en IOS

```
Router#sh crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: mapa-este-oeste, local addr 99.99.99.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.20.0/255.255.255.0/0/0)
   current_peer 88.88.88.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 99.99.99.2, remote crypto endpt.: 88.88.88.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0xCCE7411A(3437707546)
     PFS (Y/N): Y, DH group: group24

     inbound esp sas:
      spi: 0xD51CA81B(3575425051)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5, flow_id: SW:5, sibling_flags 80004040, crypto map: mapa-este-oeste
        sa timing: remaining key lifetime (k/sec): (4185110/868)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCCE7411A(3437707546)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 6, flow_id: SW:6, sibling_flags 80004040, crypto map: mapa-este-oeste
        sa timing: remaining key lifetime (k/sec): (4185110/868)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```


STAR WARS DAY
MAY THE 4TH
BE WITH YOU