Administración y Gestión de Redes
Lic. en Sistemas de Información

Laboratorio de REDES
Recuperación de Información
y Estudios de la Web

Seguridad en Redes de Datos
Redes Privadas Virtuales (VPNs)

Equipo docente:

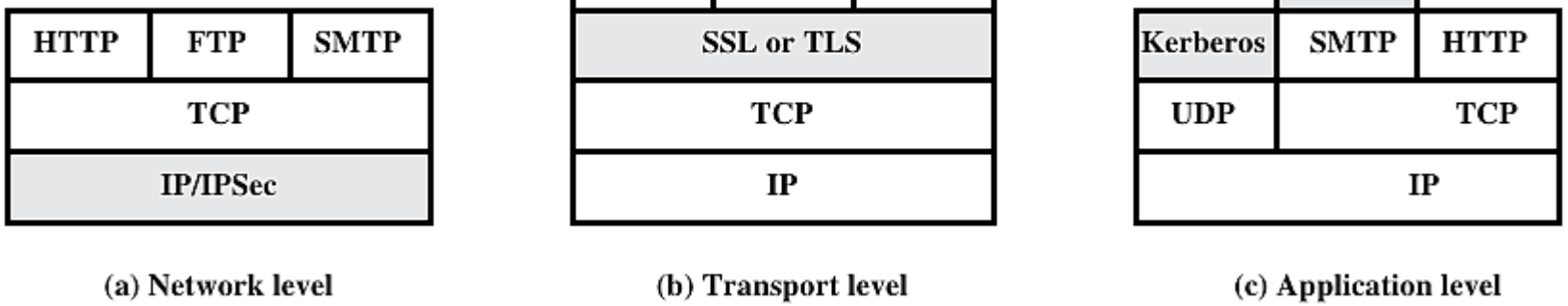
Fernando Lorge (florge@unlu.edu.ar)
Santiago Ricci (sricci@unlu.edu.ar)
Alejandro Iglesias (aaiglesias@unlu.edu.ar)
Mauro Meloni (maurom@unlu.edu.ar)
Patricio Torres (ptorres@unlu.edu.ar)

- 2025 -

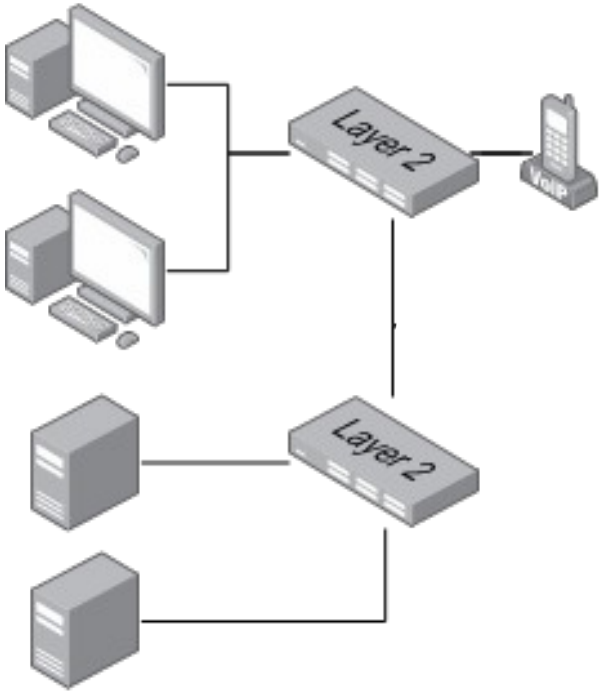
¿Cómo proteger la info en tránsito?

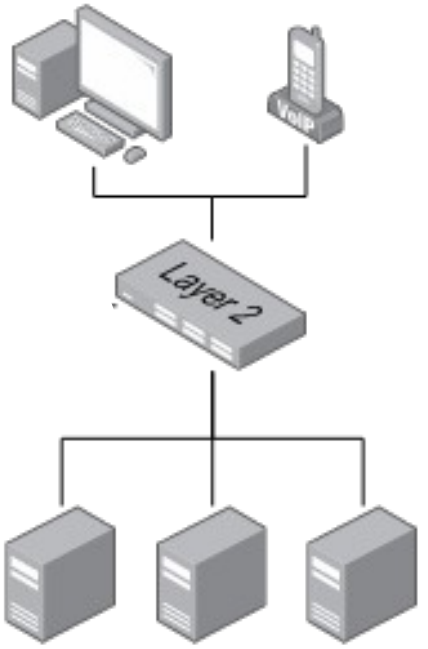
Un acercamiento válido es introduciendo protocolos y mecanismos en una o varias capas del modelo OSI, pudiendo brindar diferentes soluciones a diferentes niveles.

- End-to-end – Link-level – Network-level - Transport level - Application level
- PGP, S/MIME, Secure Shell (ssh), Transport Layer Security (TLS), IPSec, L2TP, user-space VPNs

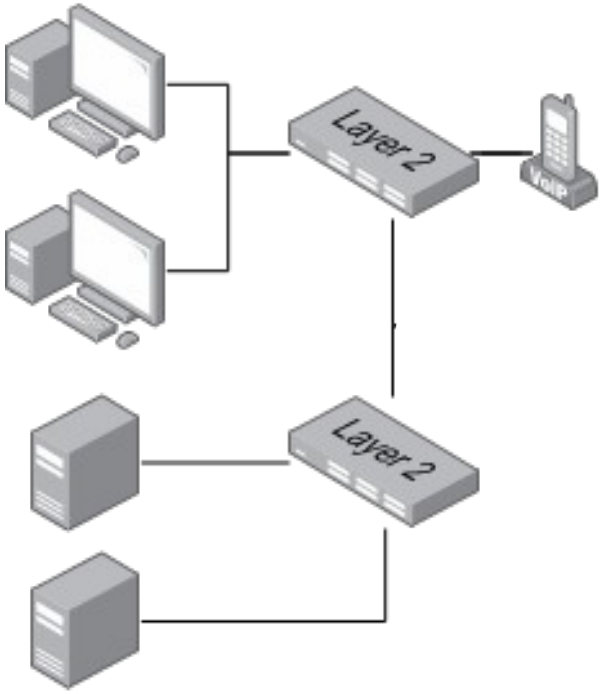


Conectividad hace unos años





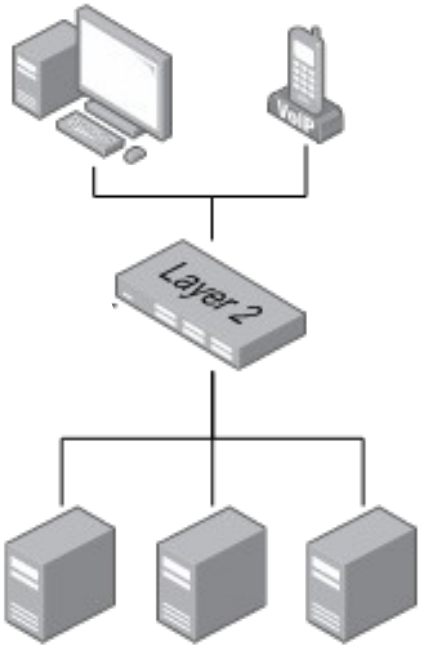
Conectividad hace unos años



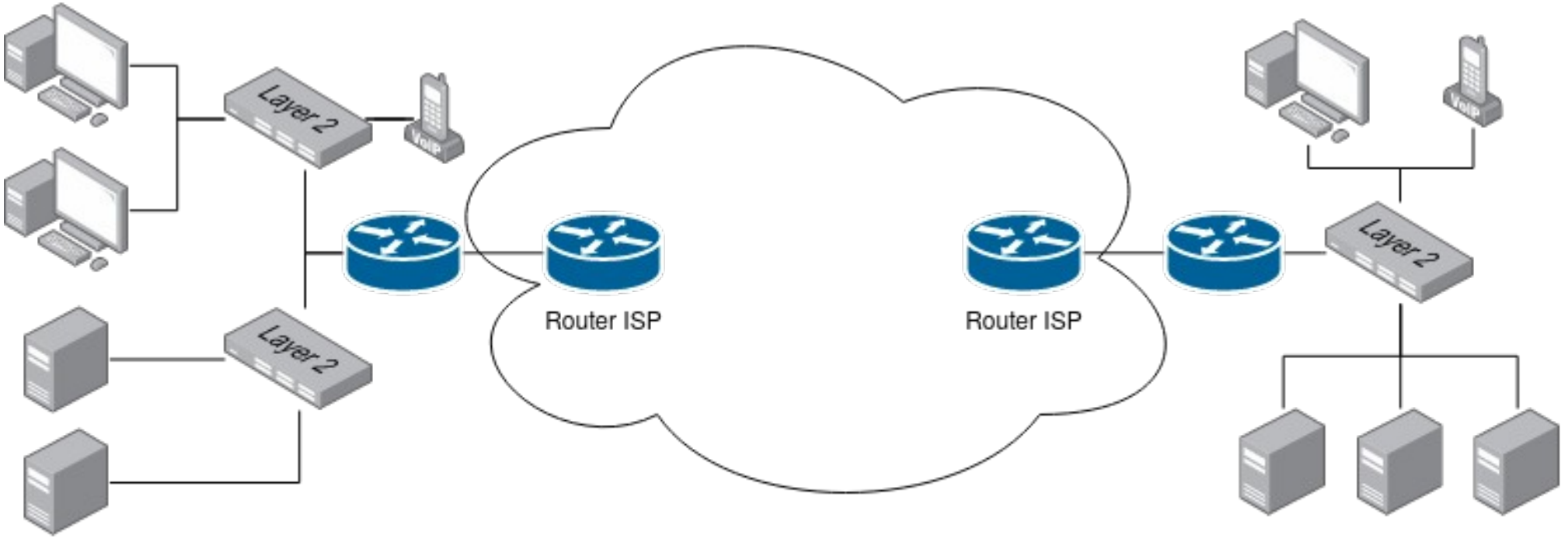
SATELITAL / INALÁMBRICO

DIAL-UP UTILIZANDO PSTN

ENLACE P-2-P CONTRATADO



Conectividad hace unos años



Redes Privadas Virtuales (VPNs)

Una VPN es un conjunto de herramientas que permite a redes de diferentes lugares conectarse de forma segura, utilizando una red pública como capa de transporte".

-- James Yonan: The User-Space VPN and OpenVPN

¿Para qué sirven?

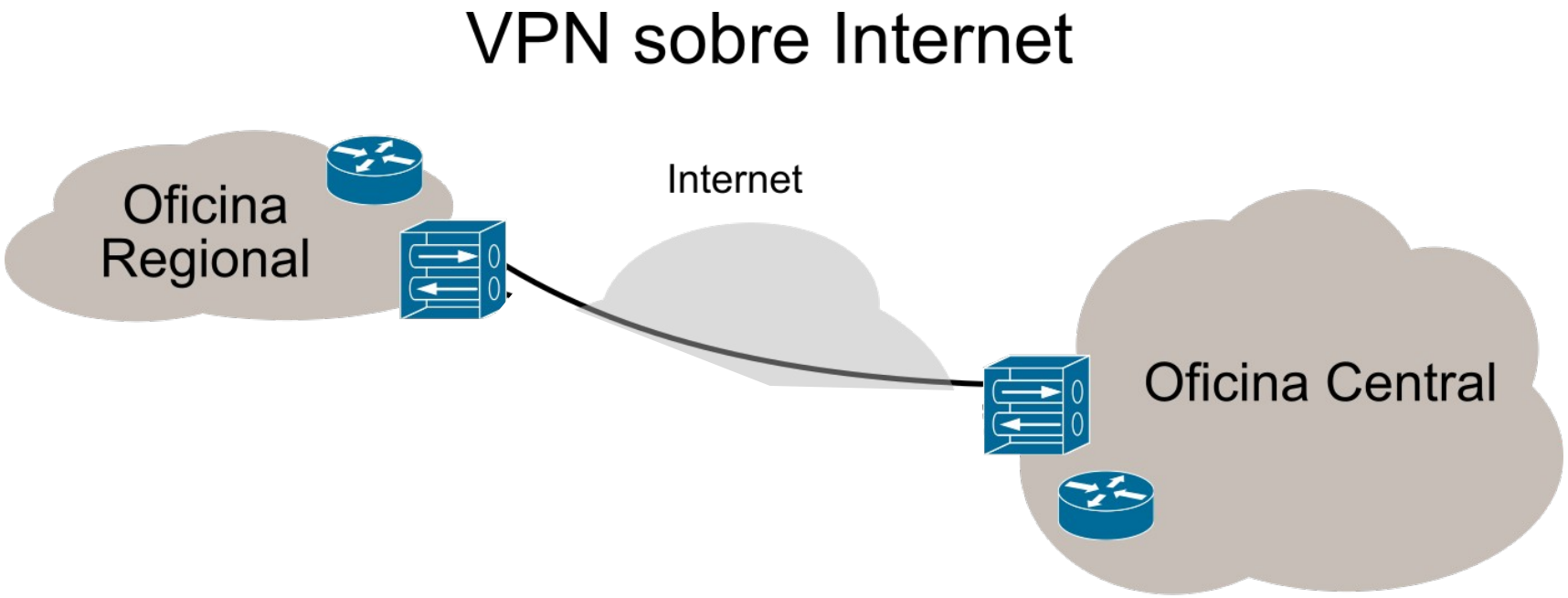
- Proveen un medio de establecer comunicaciones seguras sobre redes públicas o inseguras.
- Utilizan cifrado para proveer confidencialidad, autenticidad e integridad.

Redes Privadas Virtuales (VPNs)

Objetivos / Casos de Uso comunes

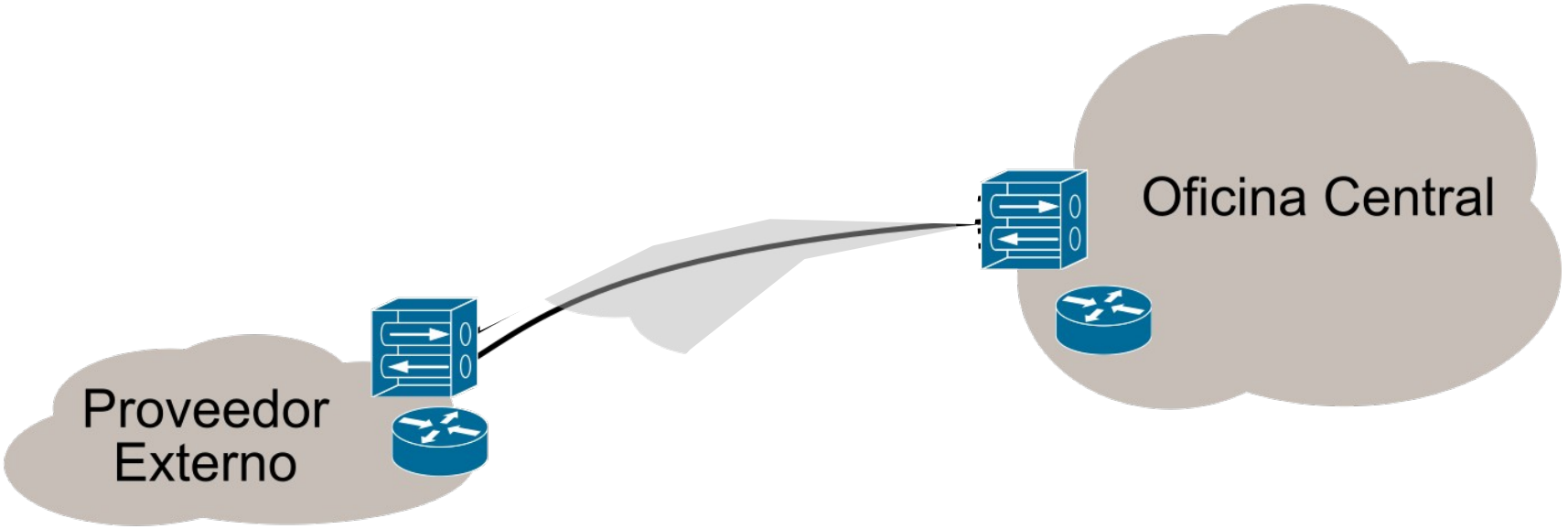
- **Acceso remoto**
  - Conectar usuarios de forma segura a sus redes empresariales.
- **Intranet**
  - Vincular sucursales con una red empresarial.
- **Extranet**
  - Ampliar la existente infraestructura de red de una organización para incluir socios, proveedores y clientes.

Redes Privadas Virtuales



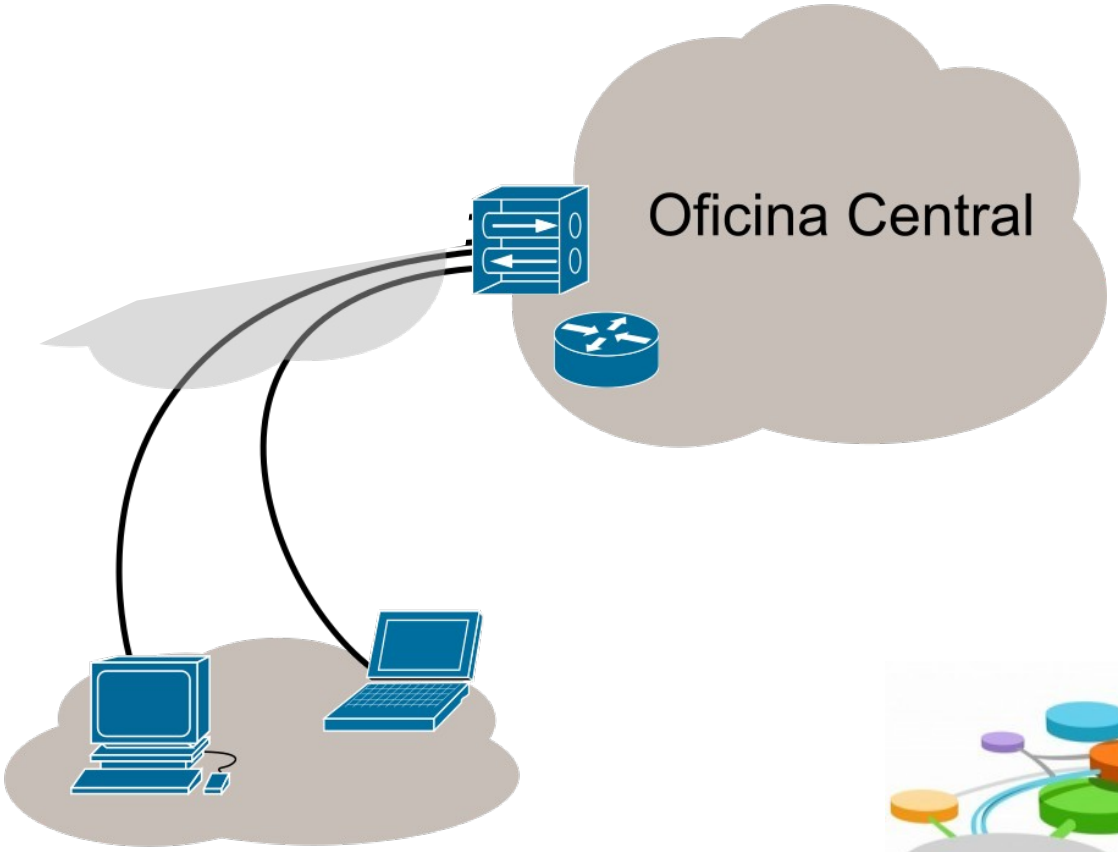
Redes Privadas Virtuales

VPN sobre Internet

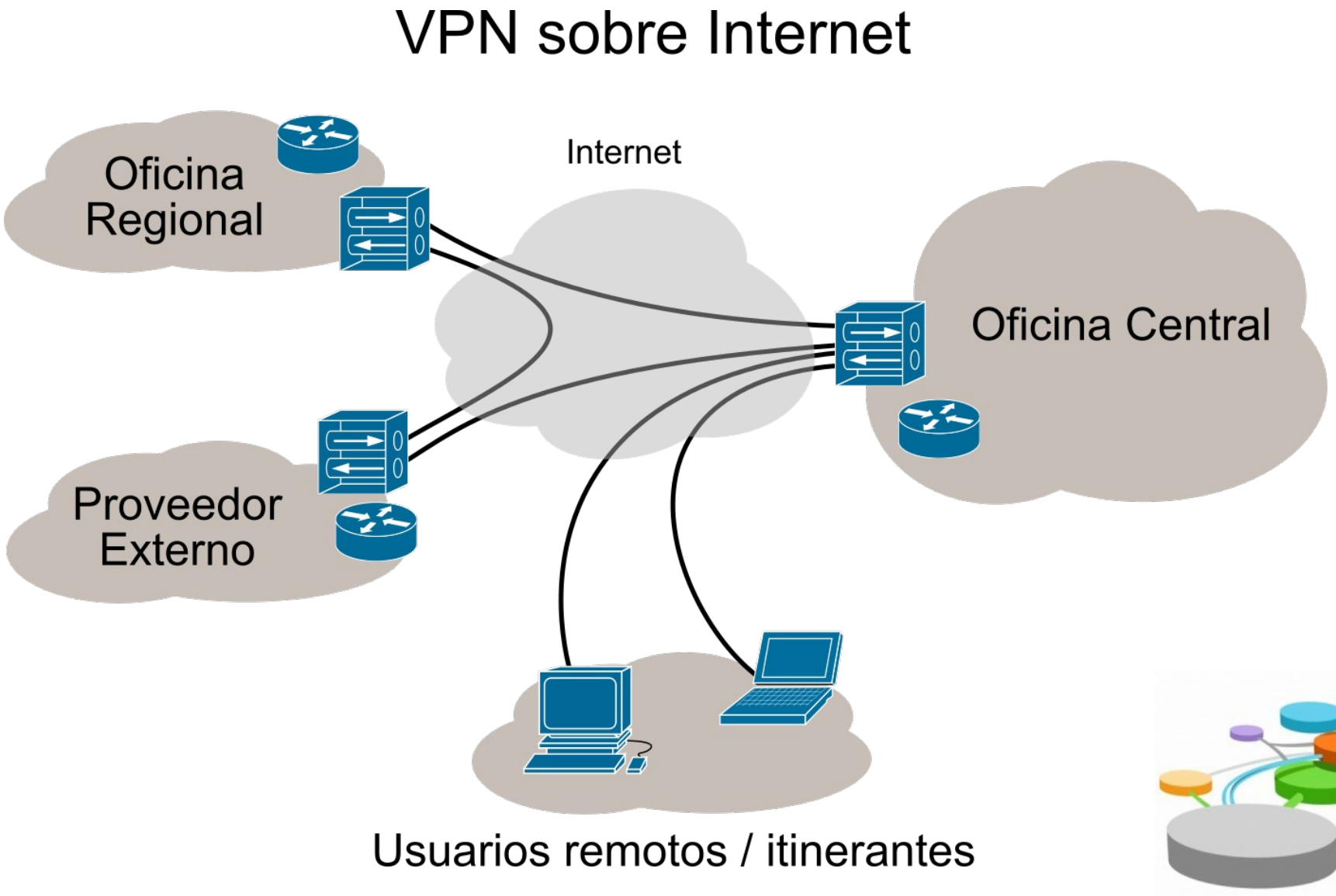


Redes Privadas Virtuales

VPN sobre Internet



Redes Privadas Virtuales



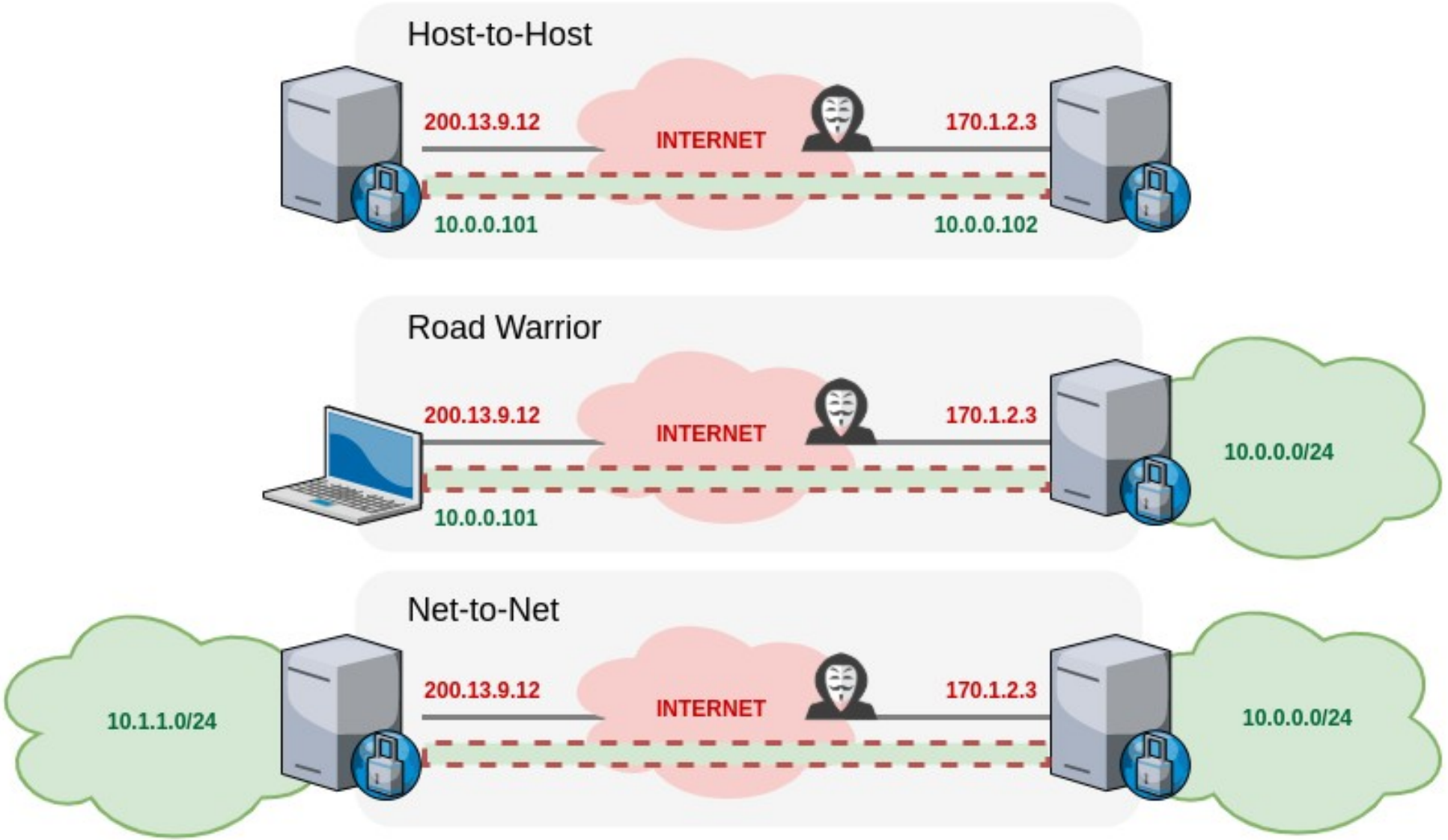
Servicios requeridos (I)

- **Cifrado de datos**
  Los datos transmitidos sobre la infraestructura de red pública deberían ser ilegibles para clientes no autorizados de la VPN.
- **Enrutamiento y Encapsulamiento**
  La tecnología VPN debe encapsular los datos privados agregando una cabecera adicional que permita a estos transitar por la red pública (mediante un *túnel*) y por la red remota hasta arribar al host destino.
- **Soporte a múltiples protocolos**
  Proveer soporte para los protocolos utilizados en la red pública.

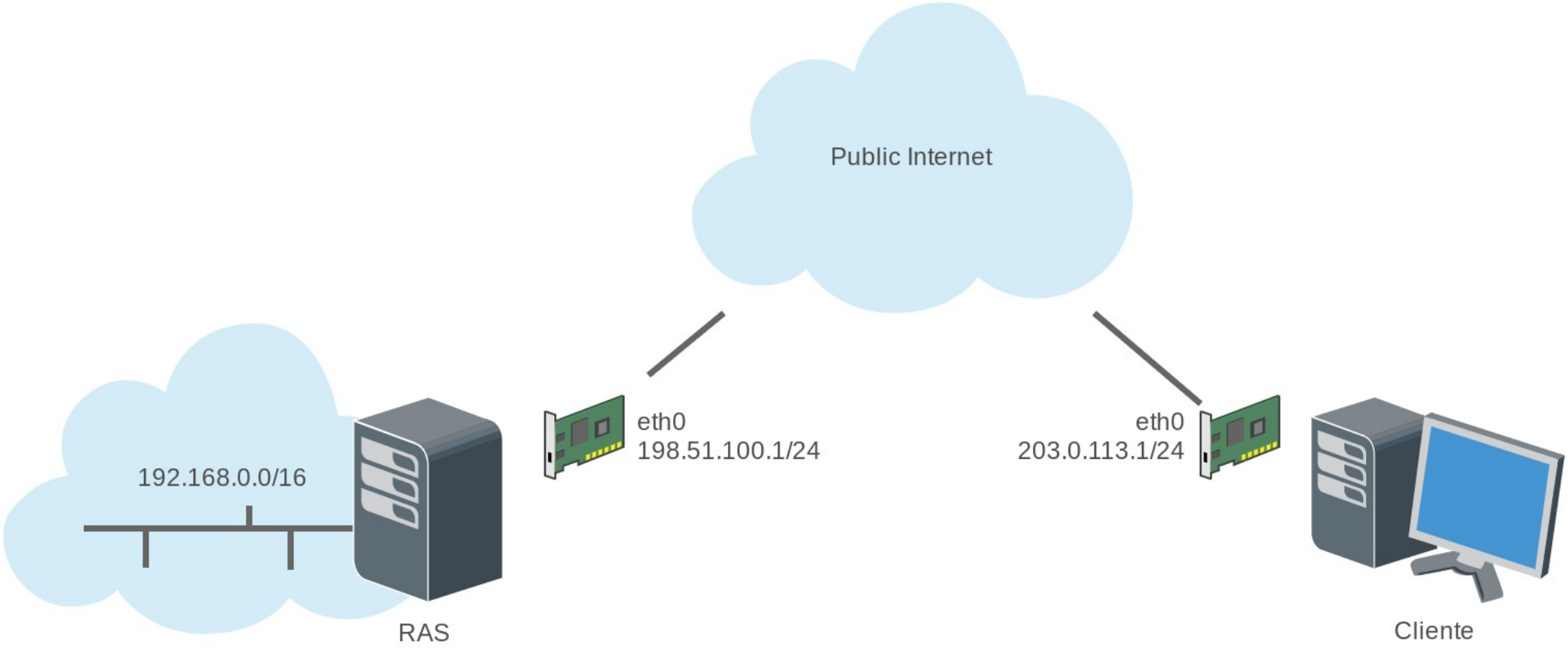
Servicios requeridos (II)

- **Autenticación de usuarios y paquetes**
  Solamente usuarios autorizados pueden tener acceso a la VPN. También debería autenticarse cada paquete de datos.
- **Administración de claves**
  Se deben generar y actualizar las claves de cifrado para los clientes VPN y el servidor VPN.
- **Administración de direcciones**
  Se deben asignar a los clientes de la VPN las direcciones IP dentro de la red corporativa y asegurar que dichas direcciones se mantengan privadas.

Tipos de VPN

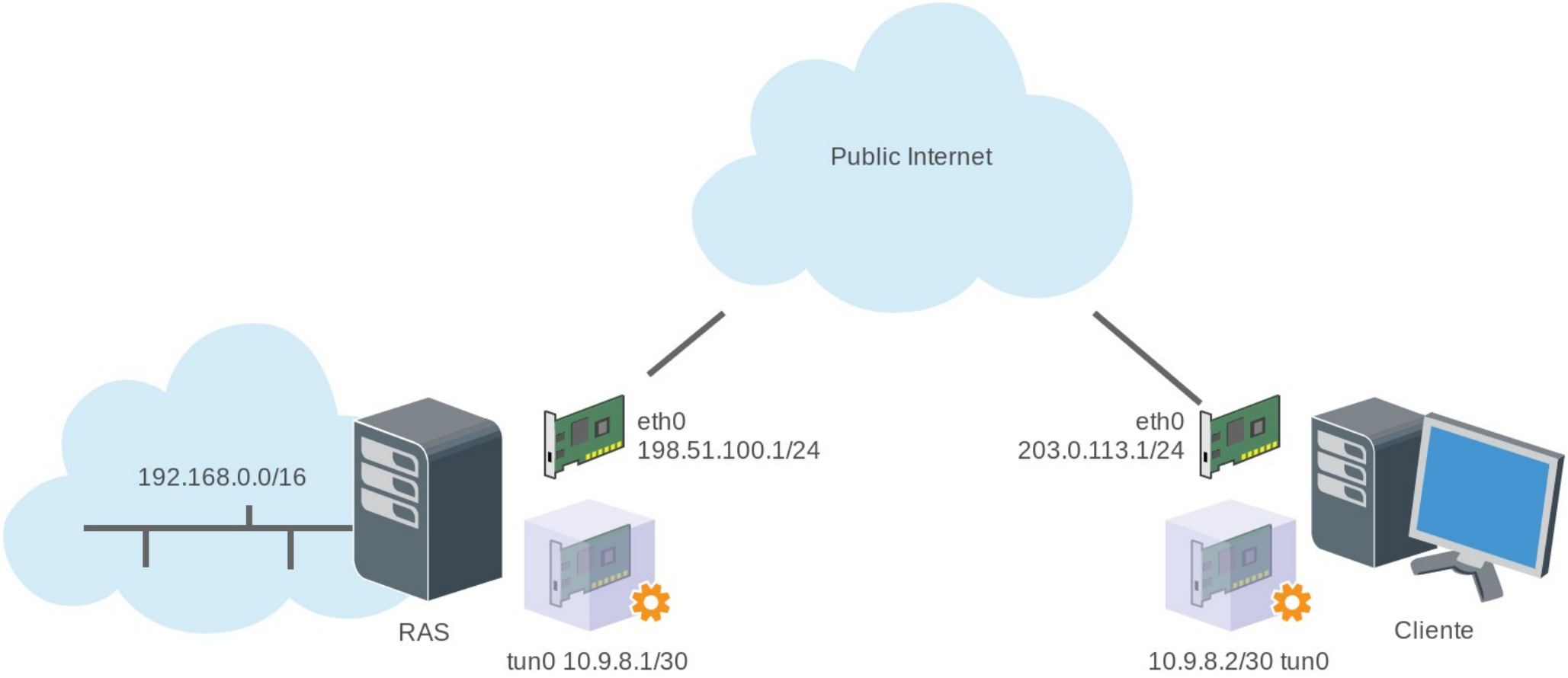

Host-to-Host
200.13.9.12
INTERNET
170.1.2.3
10.0.0.101
10.0.0.102
Road Warrior
200.13.9.12
INTERNET
170.1.2.3
10.0.0.0/24
10.0.0.101
Net-to-Net
10.1.1.0/24
200.13.9.12
INTERNET
170.1.2.3
10.0.0.0/24

Esquema de funcionamiento



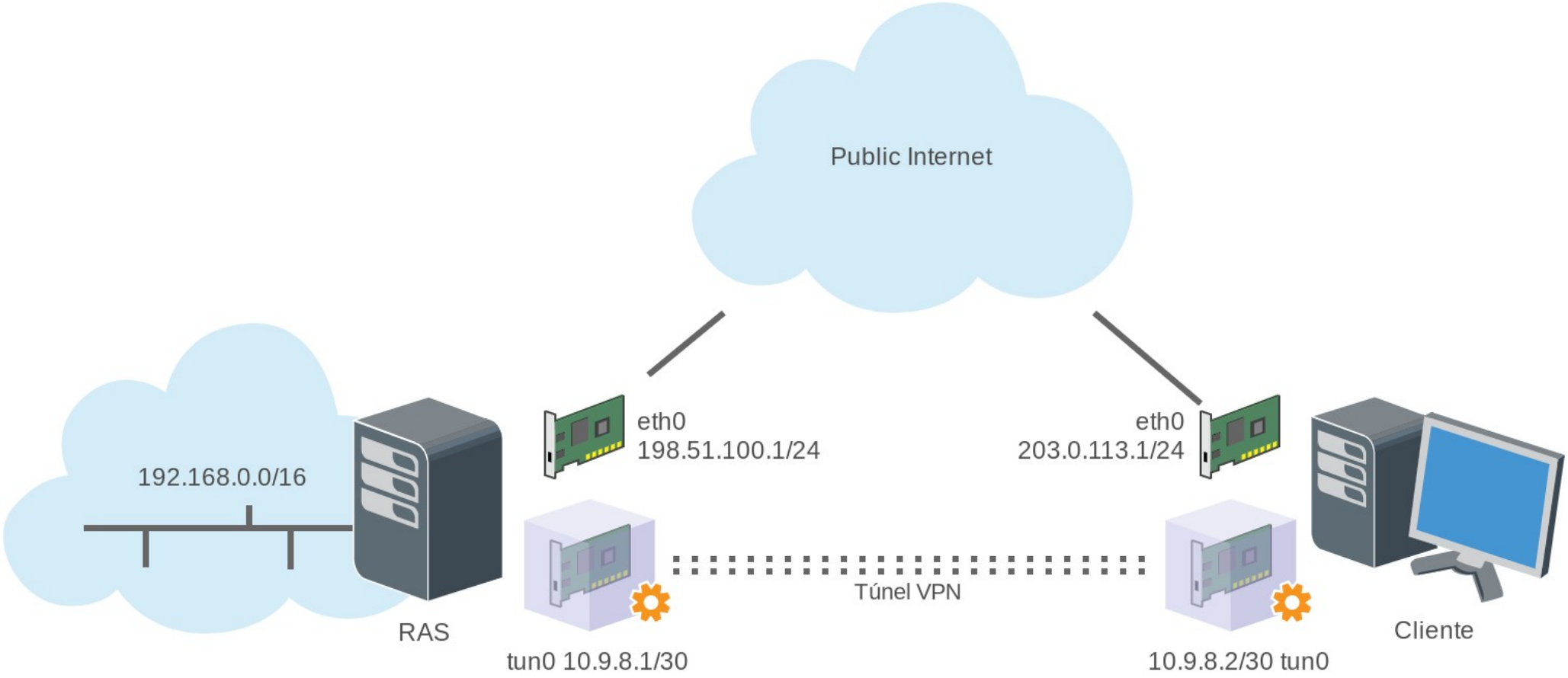
Sin VPN establecida

Esquema de funcionamiento



Creación de interfaces virtuales **tunN**

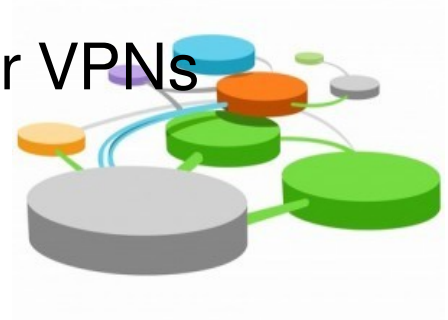
Esquema de funcionamiento



Establecimiento del túnel (conexión y autenticación)

Implementaciones

- **OpenVPN**
  Una de las implementaciones VPN más utilizadas.
- **Microsoft PPTP / SSTP**
  PPTP hoy se considera inseguro y fue reemplazado por SSTP.
- **IPSec, IKE/IPSec, L2TP/IPSec**
  El estándar más conocido, aunque complejo de implementar.
- **Wireguard**
  Surgida hace pocos años. Aparentemente performante y segura.
- **MPLS**
  Se ha utilizado y se utiliza actualmente para proveer VPNs intra-proveedor net-to-net, pero NO provee cifrado.



Administración y Gestión de Redes
Lic. en Sistemas de Información

Laboratorio de REDES
Recuperación de Información
y Estudios de la Web

IPSec

- 2025 -

IPSec - Generalidades

- Desarrollado en los '90, originalmente obligatorio en IPv6, luego recomendado. Opcional en IPv4.
- Última actualización 2005 (RFC 4301).
- 2 Modos de Operación:
  - **Transporte**
  - **Túnel**
- Servicio de Autenticación
  - **Authentication Header** (RFC 4302)
- Servicio de Confidencialidad y/o Integridad:
  - **IP Encapsulating Security Payload** (RFC 4303)
- IPSec es una tecnología compleja.

IPSec - Conceptos principales

- Protocolo de Encabezado de Autenticación
  Authentication Header Protocol (AH)
- Protocolo de “Encapsulamiento de Seguridad”
  Encapsulating Security Protocol (ESP)
- Asociaciones de Seguridad
  Security Associations (SAs)
- Base de datos de Asociaciones de Seguridad
  Security Association Database (SADB)
- Base de datos de Políticas de Seguridad
  Security Policy Database (SPD)

IPSec - “Subprotocolos”

AH (Authentication Header) Protocol

- Provee autenticación, integridad y protección frente a reenvíos.
- Asegura la carga de un paquete IP y porciones del header IP.
- NO brinda confidencialidad.

ESP (Encapsulating Security Payload) Protocol

- Puede proveer autenticación, integridad, protección frente a reenvíos y, además, confidencialidad.
- Asegura tanto headers como carga de un paquete IP.

IKE (Internet Key Exchange) Protocol

- Utilizado para distribuir las Asociaciones de Seguridad y las claves entre los nodos.

Security Associations (SAs)

Describen exactamente cómo se alcanzará la protección deseada para cada sentido de cada conexión (cada SA es unidireccional).

- Algunos parámetros típicos de una SA incluyen:
  - Algoritmo de cifrado, algoritmo de hash, clave de cifrado, clave de autenticación, tiempo de vida de claves, valores de inicialización.
- Seteo manual o automático (ISAKMP, IKE, etc.).
- Identificada por la tripla *(spi, ip_destino, ipsec_proto_id)*
  - Security Parameter Index (SPI)
  - IP destino
  - Security Protocol Identifier (AH o ESP)

Security Association Database (SADB)

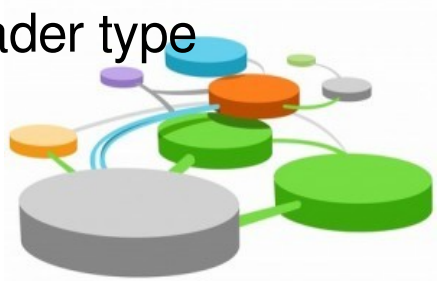
Define los parámetros asociados a cada SA:

- Security Parameter Index
- Sequence Number Counter
- Sequence Counter Overflow
- Anti-Reply Window
- AH Information
- ESP Information
- Lifetime
- IPSec Protocol Mode
- Path MTU
- DSCP values
- Tunnel header IP source and destination address...

Security Policy Database (SPD)

Definen cómo se aplica IPSec al tráfico transmitido o recibido.

- Opciones de procesamiento: DISCARD, BYPASS, PROTECT
- En las entradas se utilizan “Selectores”:
  - Local Address,
  - Remote Address,
  - Next Layer Protocol,
  - Local Port, or ICMP message type/code or Mobility Header type (depending on the next layer protocol)
  - Remote Port, or ICMP message type/code or Mobility Header type (depending on the next layer protocol)



SADB y SPD

Security Associations Database

SPI	DEST IP ADDR	PROTO	HASH ALGO	CIPH ALGO	MODE	AUTH KEY	CIPH KEY	...
33	13.135.30.1	AH	HMAC-SHA2	AES-GCM	Transp	0xd6ef...	0xc3a1...	
61	200.119.7.4	ESP	HMAC-SHA1	3DES-CBC	Transp	0xab11...	0xa45f...	
172	**170.210.96.37**	**ESP**	HMAC-SHA2	AES-GCM	Túnel	0x543d...	0x773d...	
...	...							

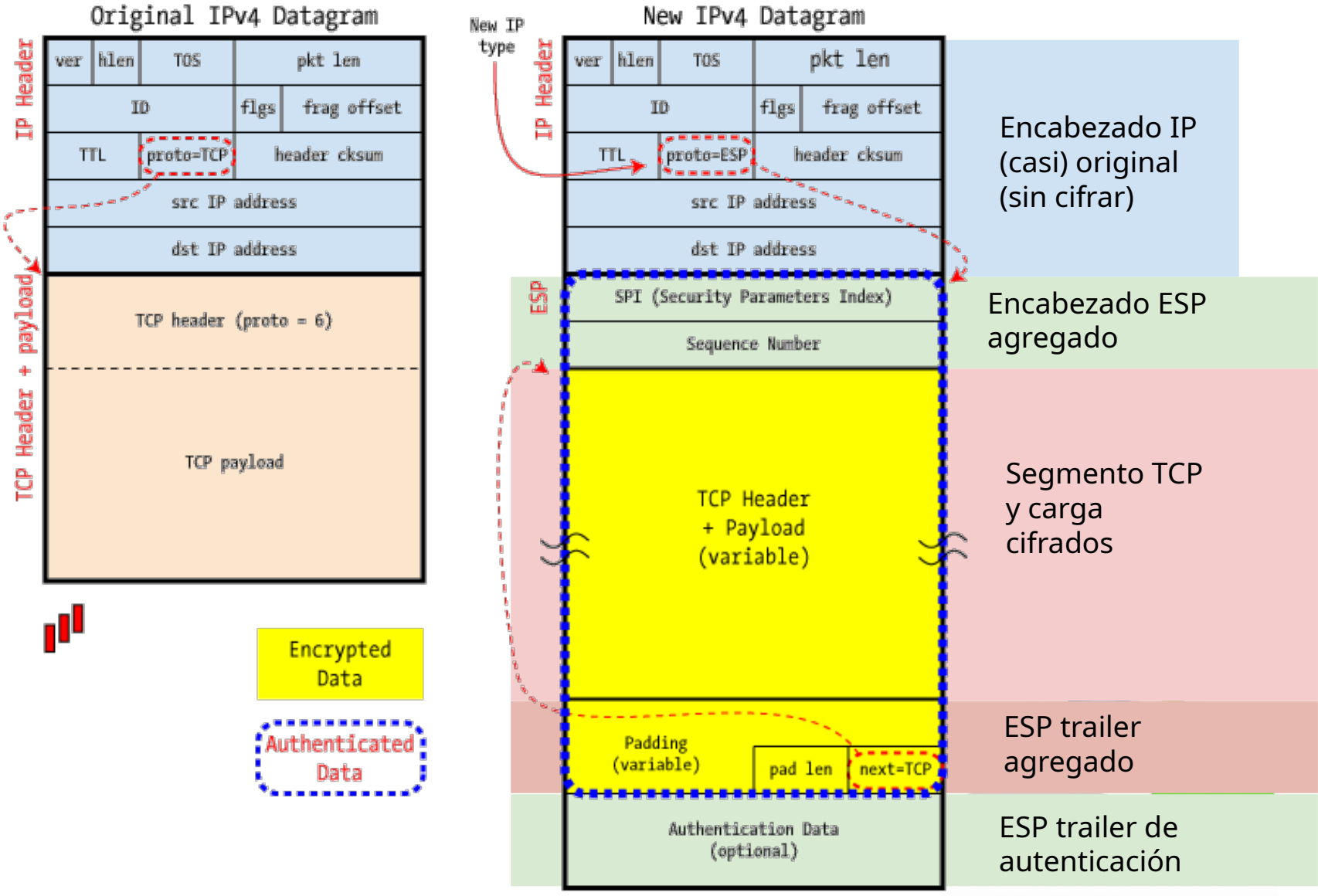
Security Policy Database

PROTO	IP LOCAL	LOCAL PORT	REMOTE IP	REM PORT	SPI	PROCESAMIENTO
UDP	45.12.3.4	500	*	1025	---	BYPASS
TCP	45.12.3.4	*	13.135.30.1	80	33	PROTECT
TCP	45.12.3.4	3321	170.210.96.37	21	172	PROTECT
*	*	*	8.8.8.8	*	---	DISCARD

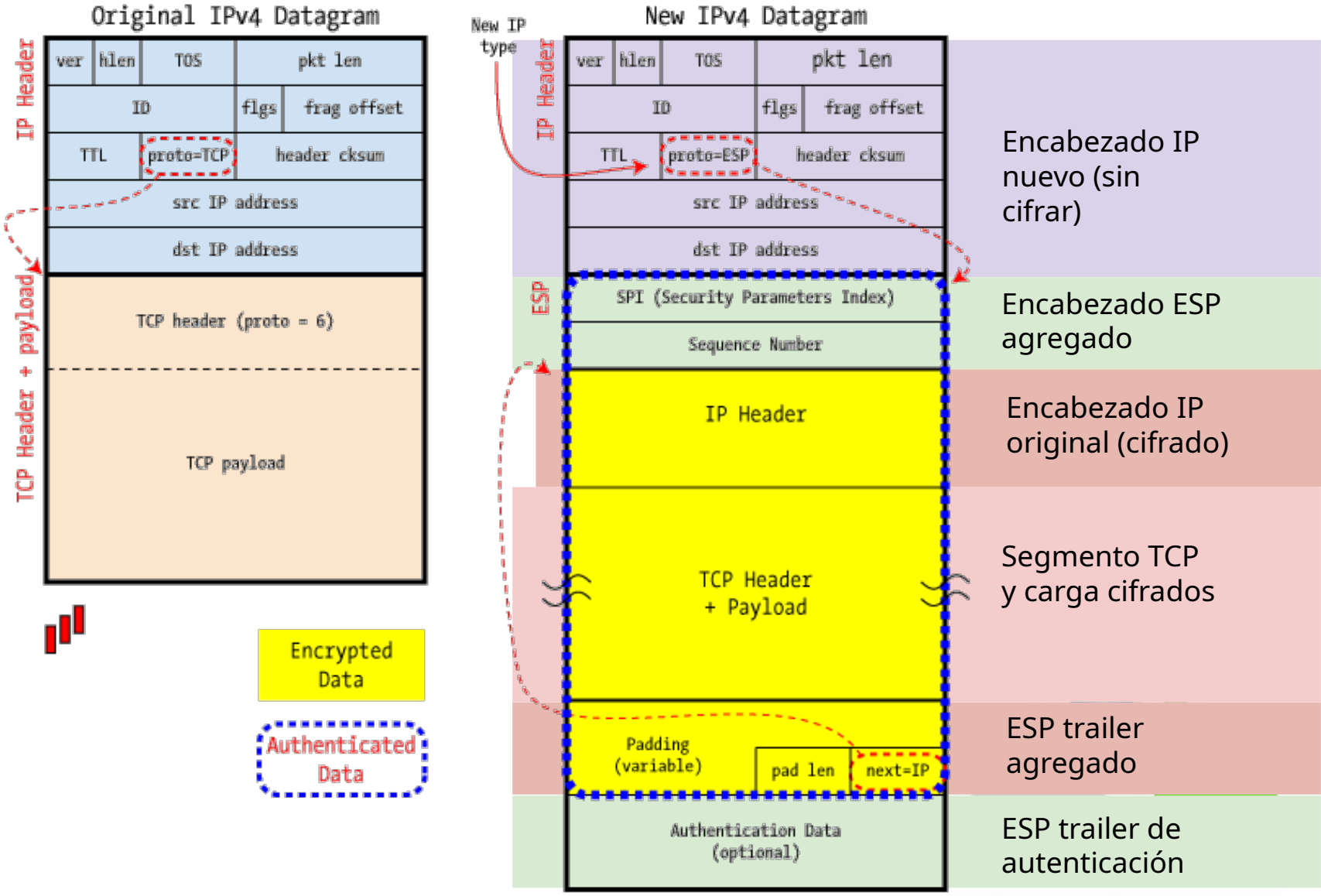
Internet Key Exchange (IKE)

- En los inicios, las claves de cifrado se distribuían off-line (y todavía hoy en algunos casos se distribuyen así).
- El protocolo IKE utiliza criptografía asimétrica, certificados X.509 y el intercambio de claves Diffie-Hellman para **distribuir Security Associations y claves en forma segura** entre los actores que intervienen en una implementación IPSec.
  Es un protocolo complejo que integra varios otros protocolos.
- Opera sobre transporte UDP en puerto 500 (ISAKMP).
- Hay implementaciones privativas y libres (*swan).

IPSec in IPv4 ESP Transport Mode



IPSec in IPv4 ESP Tunnel Mode



Administración y Gestión de Redes
Lic. en Sistemas de Información

Laboratorio de REDES
Recuperación de Información
y Estudios de la Web

OpenVPN

- 2025 -

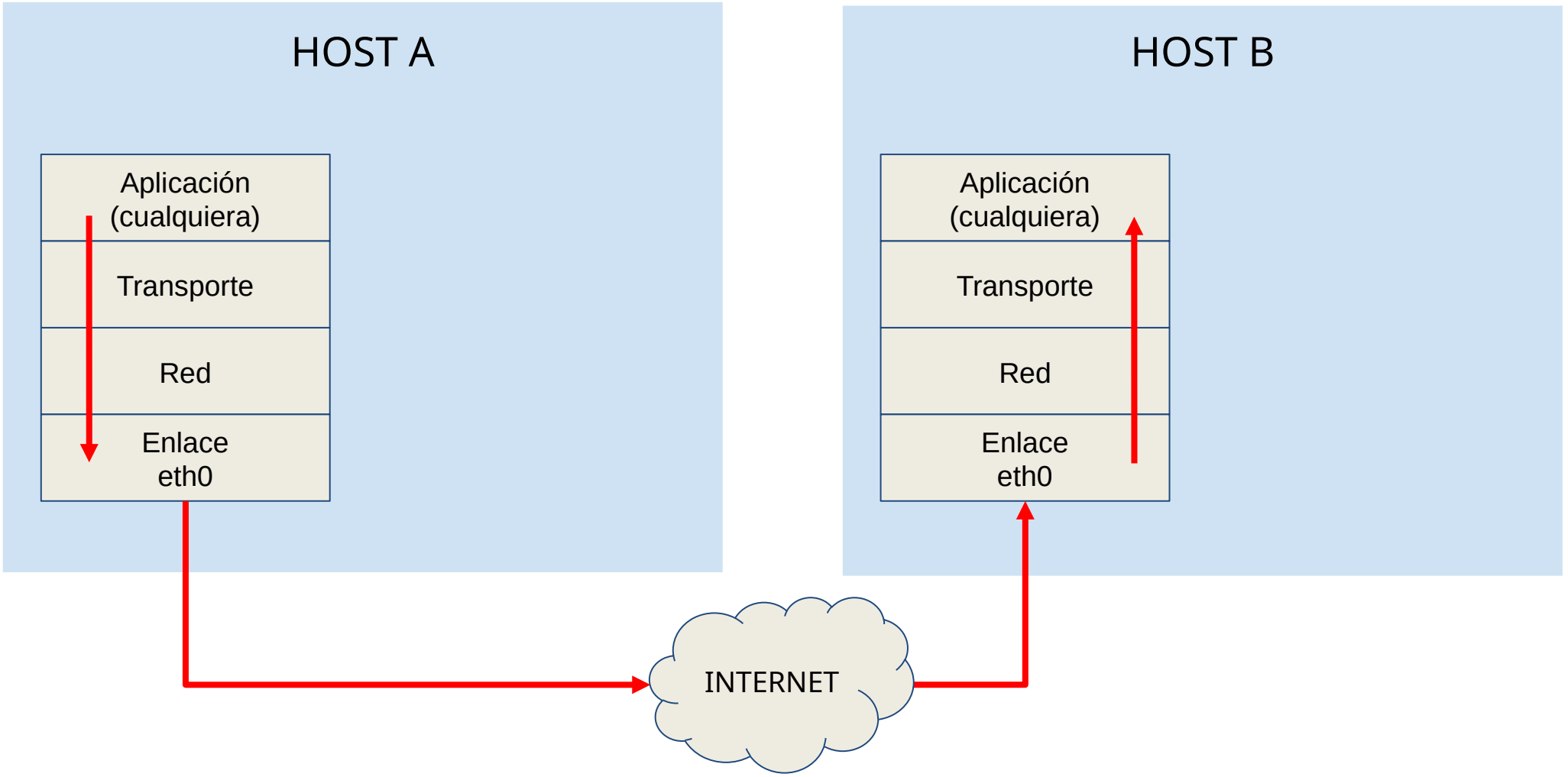
OpenVPN

- A diferencia de IPSec, que está implementado en el Kernel de Linux y de otros sistemas operativos, OpenVPN es básicamente una “aplicación”, por lo que es independiente del S.O.
- Crea una interfaz de red virtual (habitualmente *tun0*).
- Todo lo que el stack TCP/IP envíe a través de la interfaz virtual es enviado al proceso OpenVPN. Ese proceso agrega los encabezados propios, opcionalmente cifra el paquete y luego lo envía por la interfaz real hasta el otro extremo del túnel, que lo descifra, autentica y pasa al stack TCP/IP “como un paquete recién llegado”.

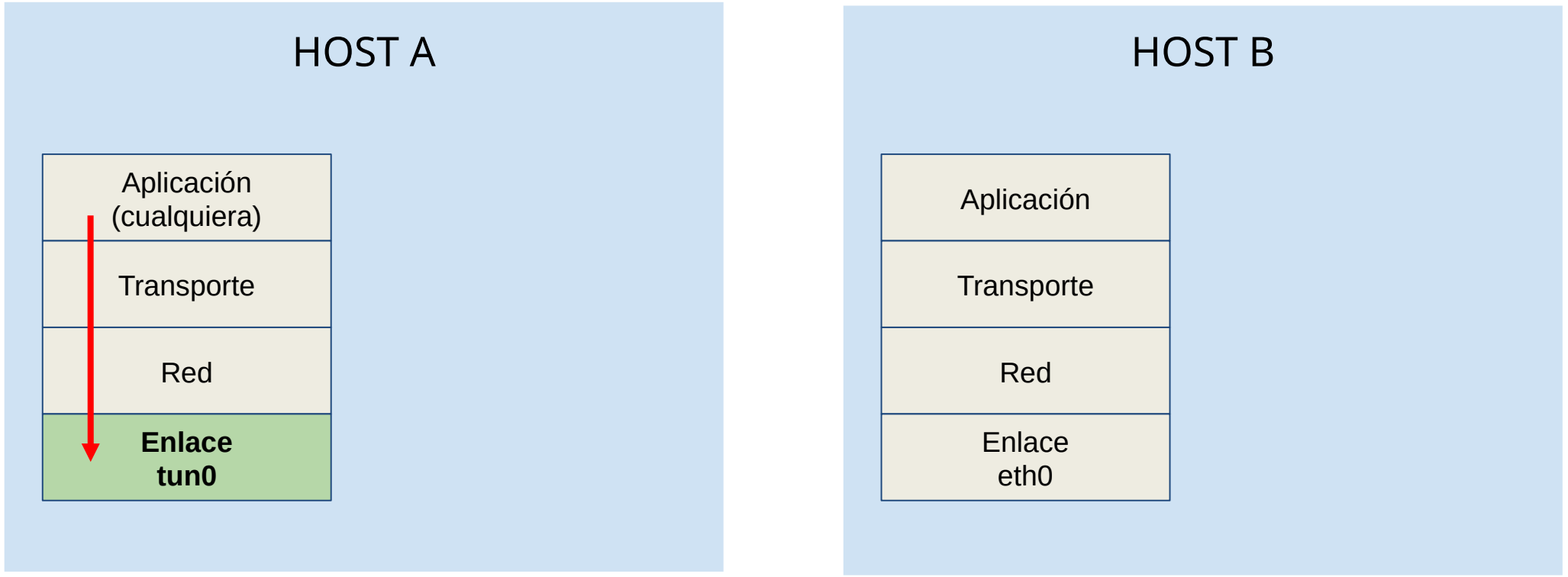
OpenVPN

- Respecto a la confidencialidad, puede operar...
  - sin cifrado,
  - con cifrado simétrico.
- Respecto a la autenticación de clientes, puede operar...
  - sin autenticación,
  - con autenticación basada en clave secreta precompartida,
  - con autenticación basada en usuario y clave,
  - con autenticación basada en claves asimétricas, certificados X.509 y cero, una o más Autoridades de Certificación (como en TLS).

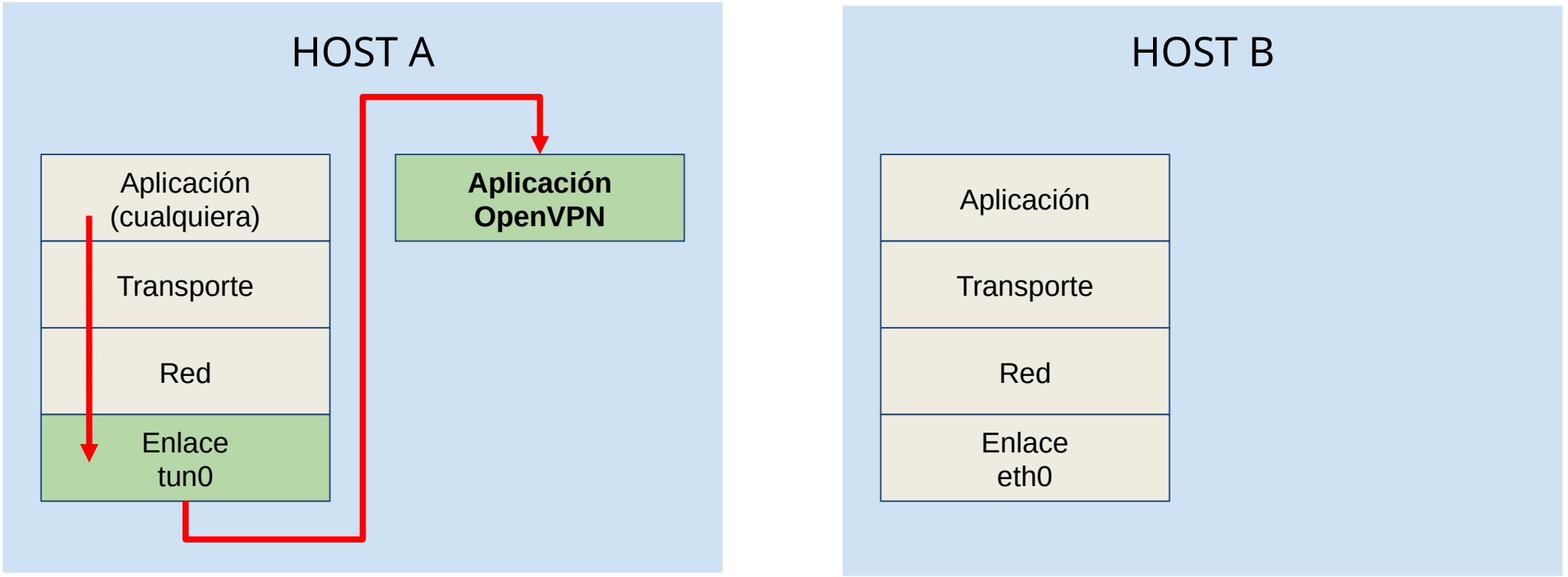
Comunicación tradicional

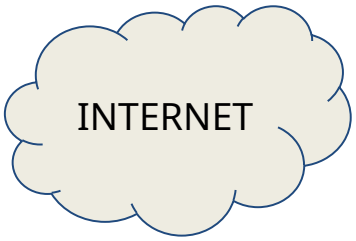


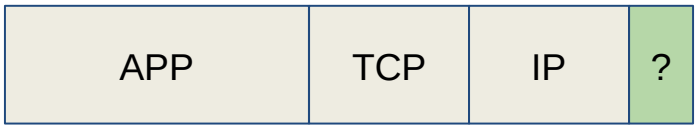
OpenVPN


HOST A
Aplicación (cualquiera)
Transporte
Red
Enlace tun0
HOST B
Aplicación
Transporte
Red
Enlace eth0
INTERNET
APP
TCP
IP
?

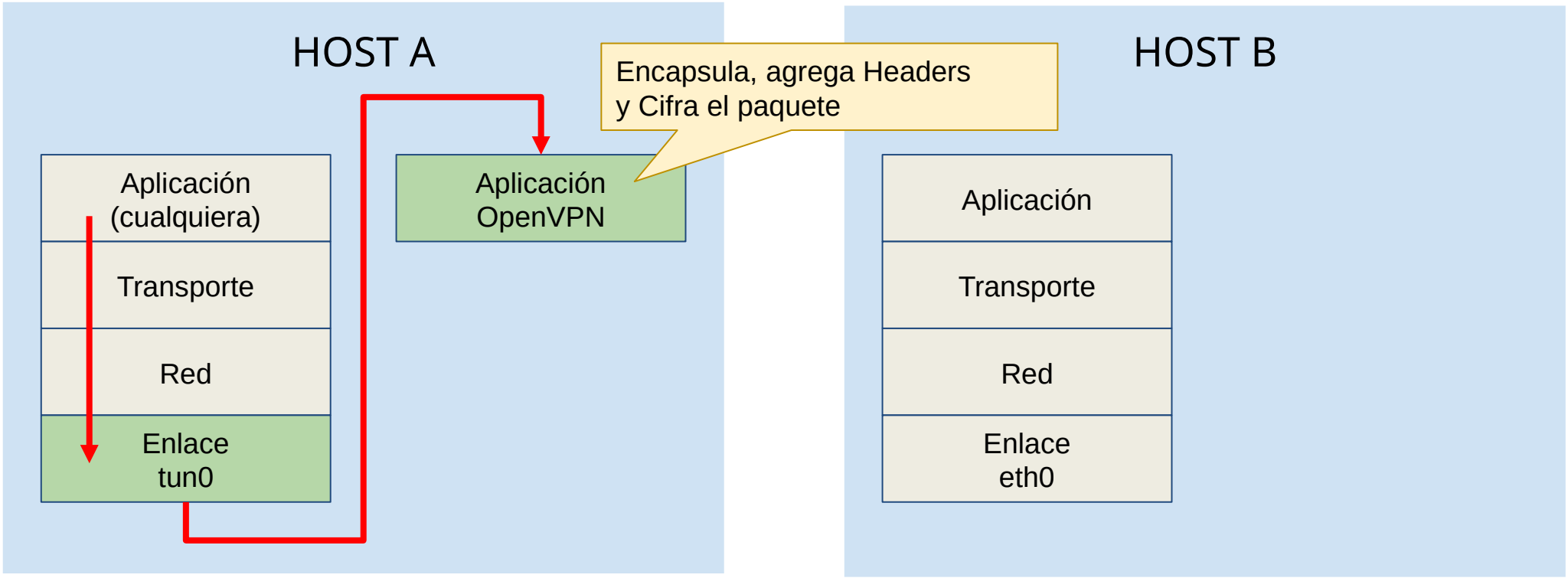
OpenVPN

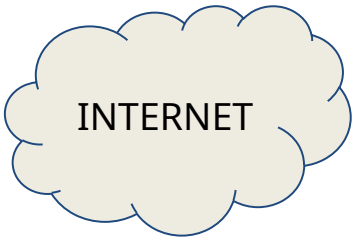

HOST A
Aplicación (cualquiera)
Transporte
Red
Enlace tun0
Aplicación OpenVPN
HOST B
Aplicación
Transporte
Red
Enlace eth0


INTERNET


APP
TCP
IP
?

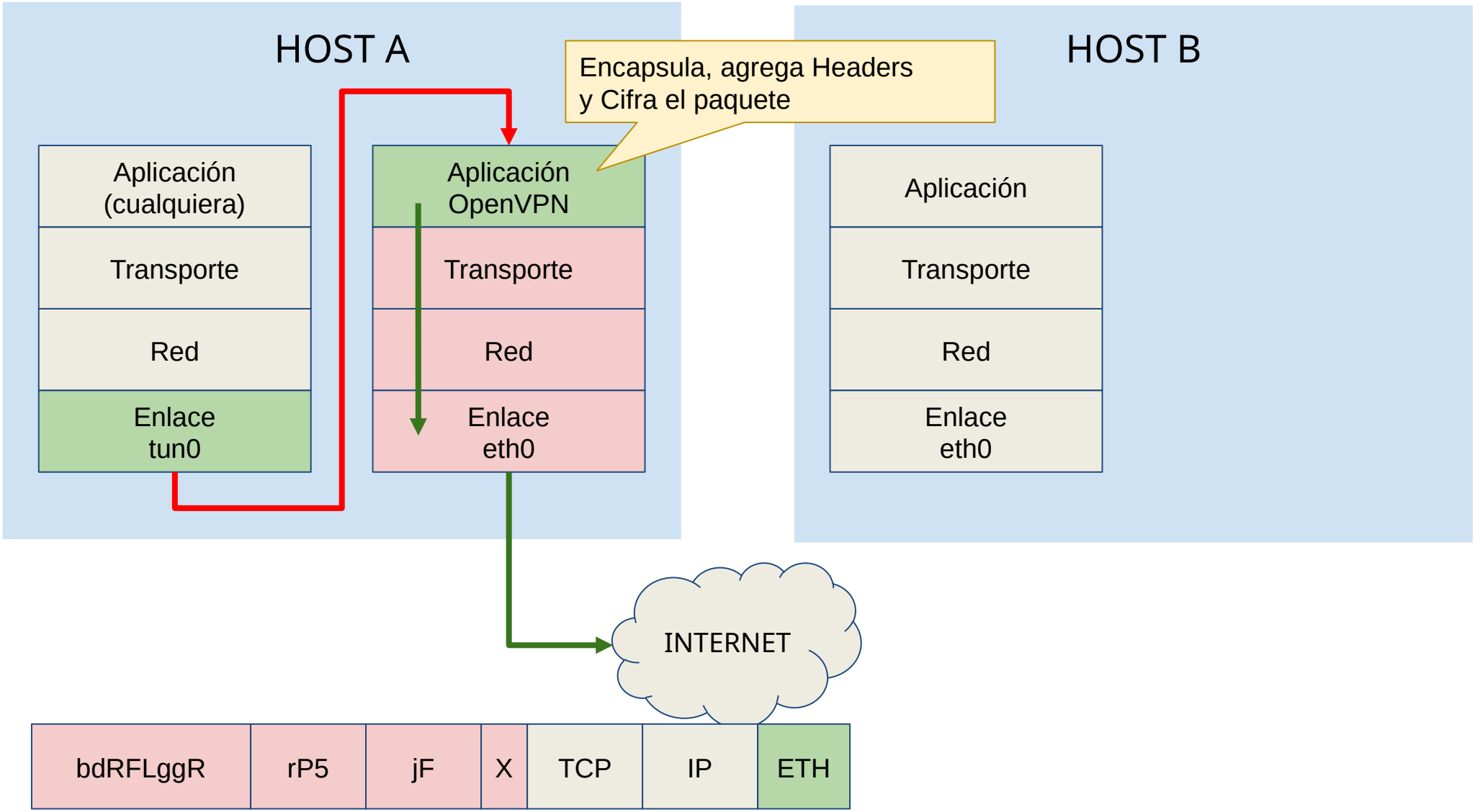
OpenVPN



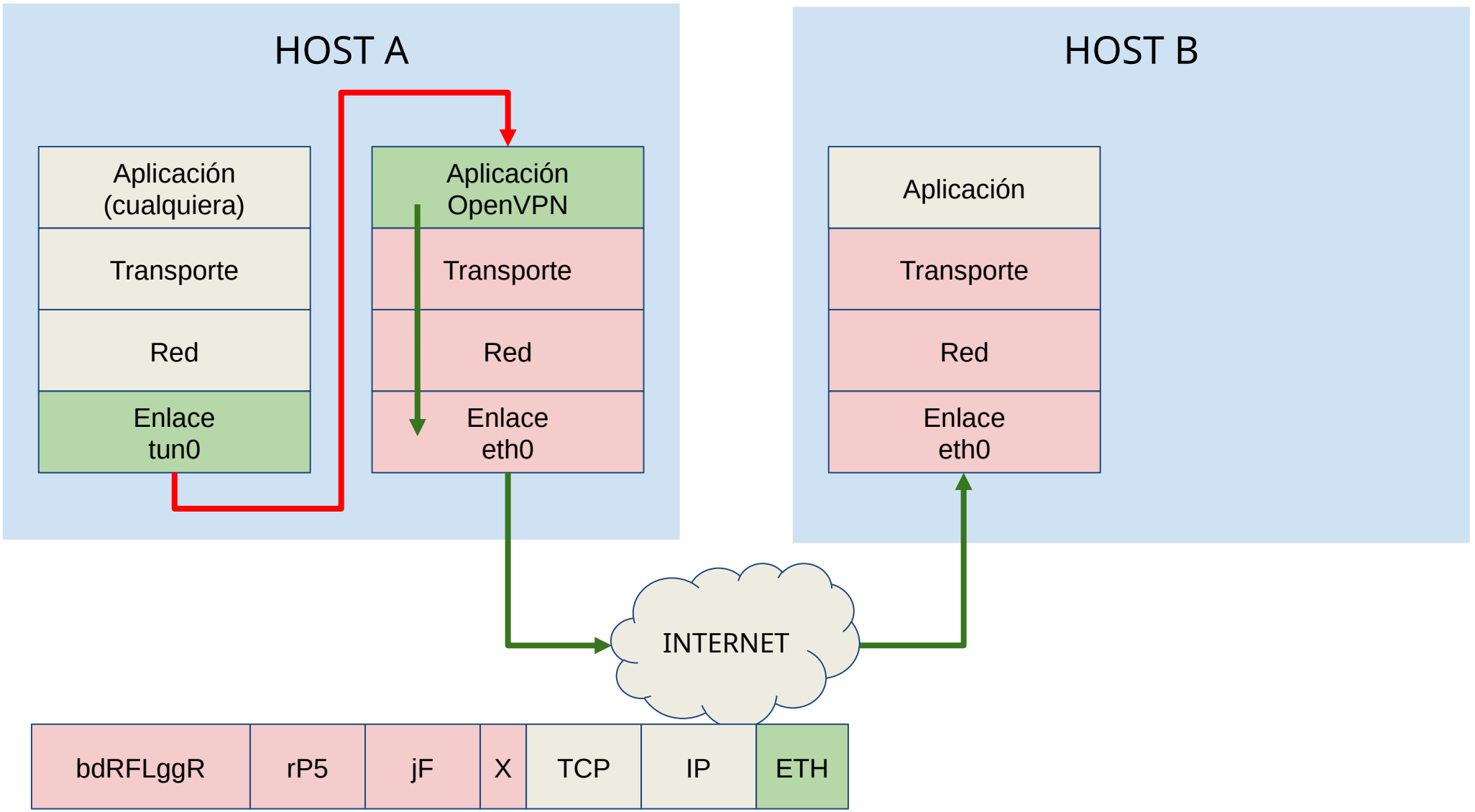


bdRFLggR	rP5	jF	X

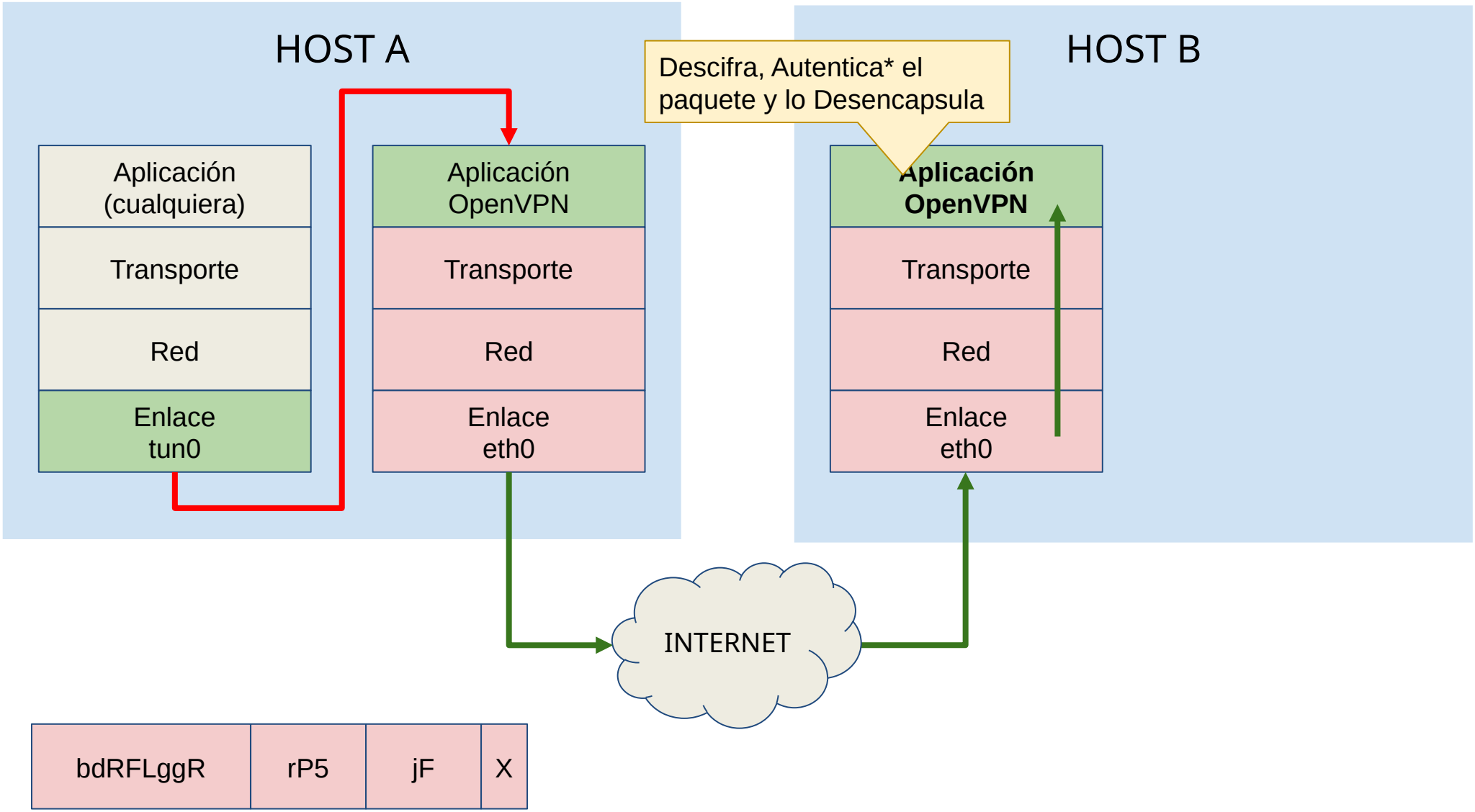
OpenVPN


HOST A
Encapsula, agrega Headers
y Cifra el paquete
HOST B
Aplicación
(cualquiera)
Transporte
Red
Enlace
tun0
Aplicación
OpenVPN
Transporte
Red
Enlace
eth0
Aplicación
Transporte
Red
Enlace
eth0
INTERNET
bdRFLggR
rP5
jF
X
TCP
IP
ETH

OpenVPN

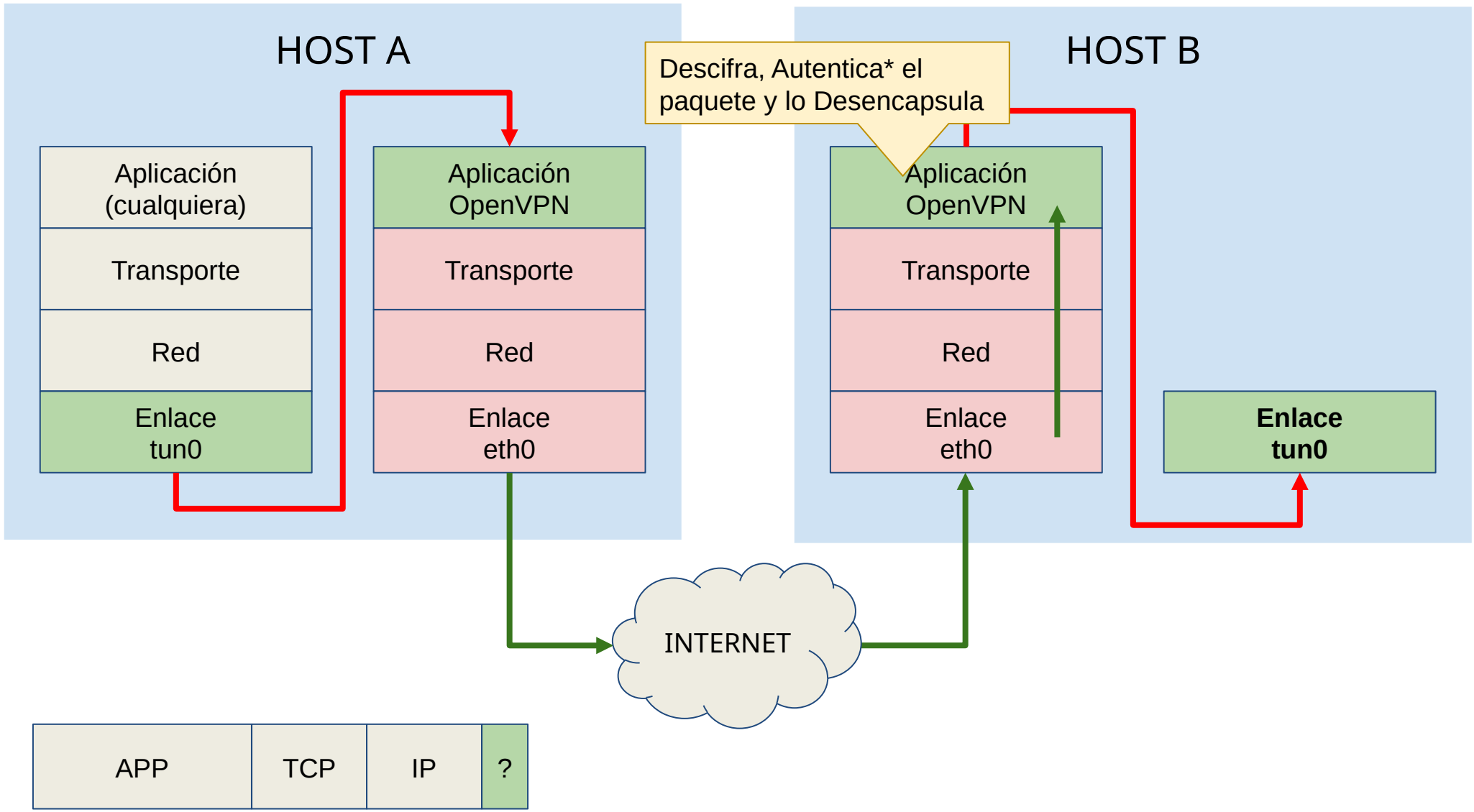

HOST A
Aplicación (cualquiera)
Transporte
Red
Enlace tun0
Aplicación OpenVPN
Transporte
Red
Enlace eth0
HOST B
Aplicación
Transporte
Red
Enlace eth0
INTERNET
bdRFLggR
rP5
jF
X
TCP
IP
ETH

OpenVPN



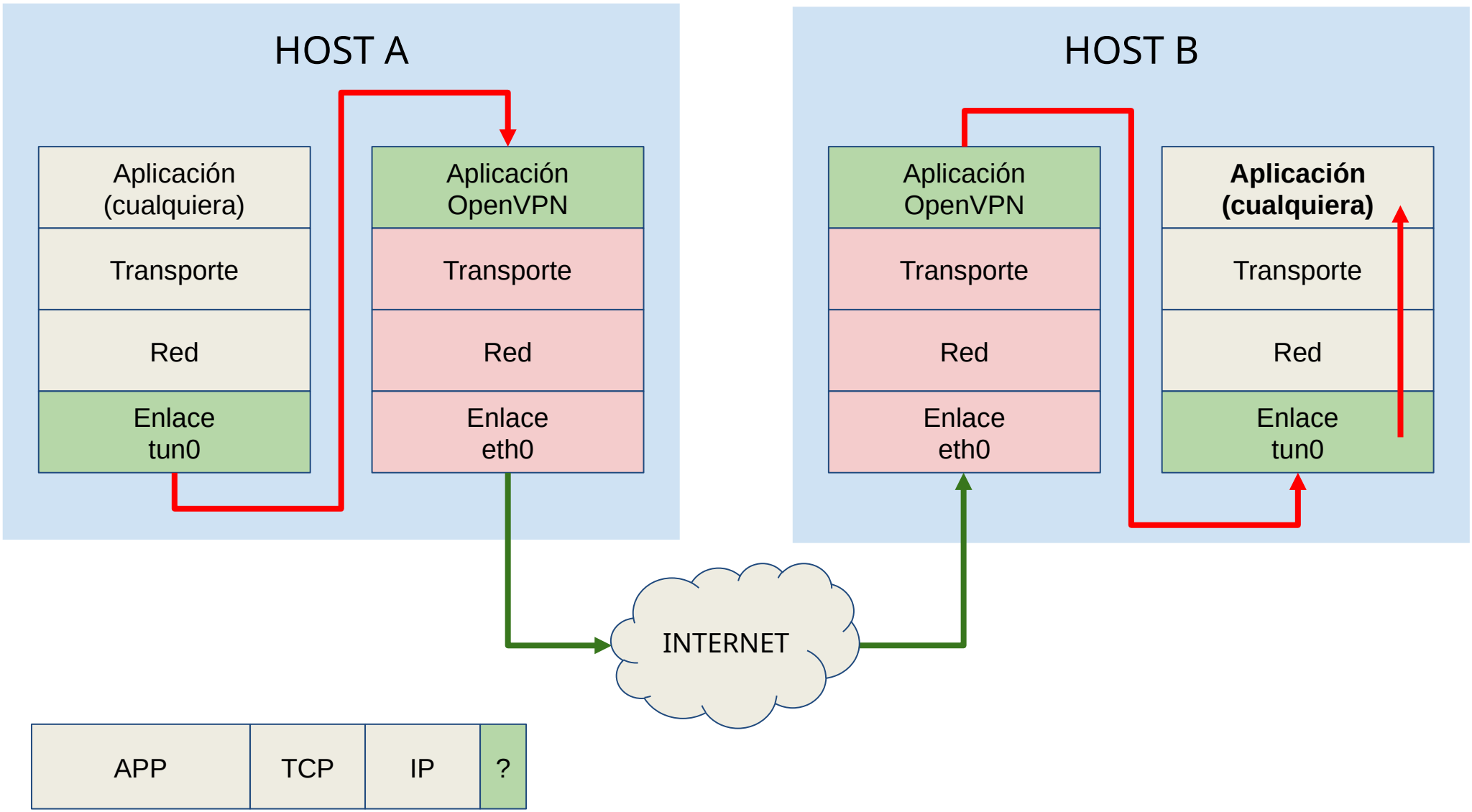
* dependiendo de la configuración, puede que autentique antes de descifrar el paquete

OpenVPN

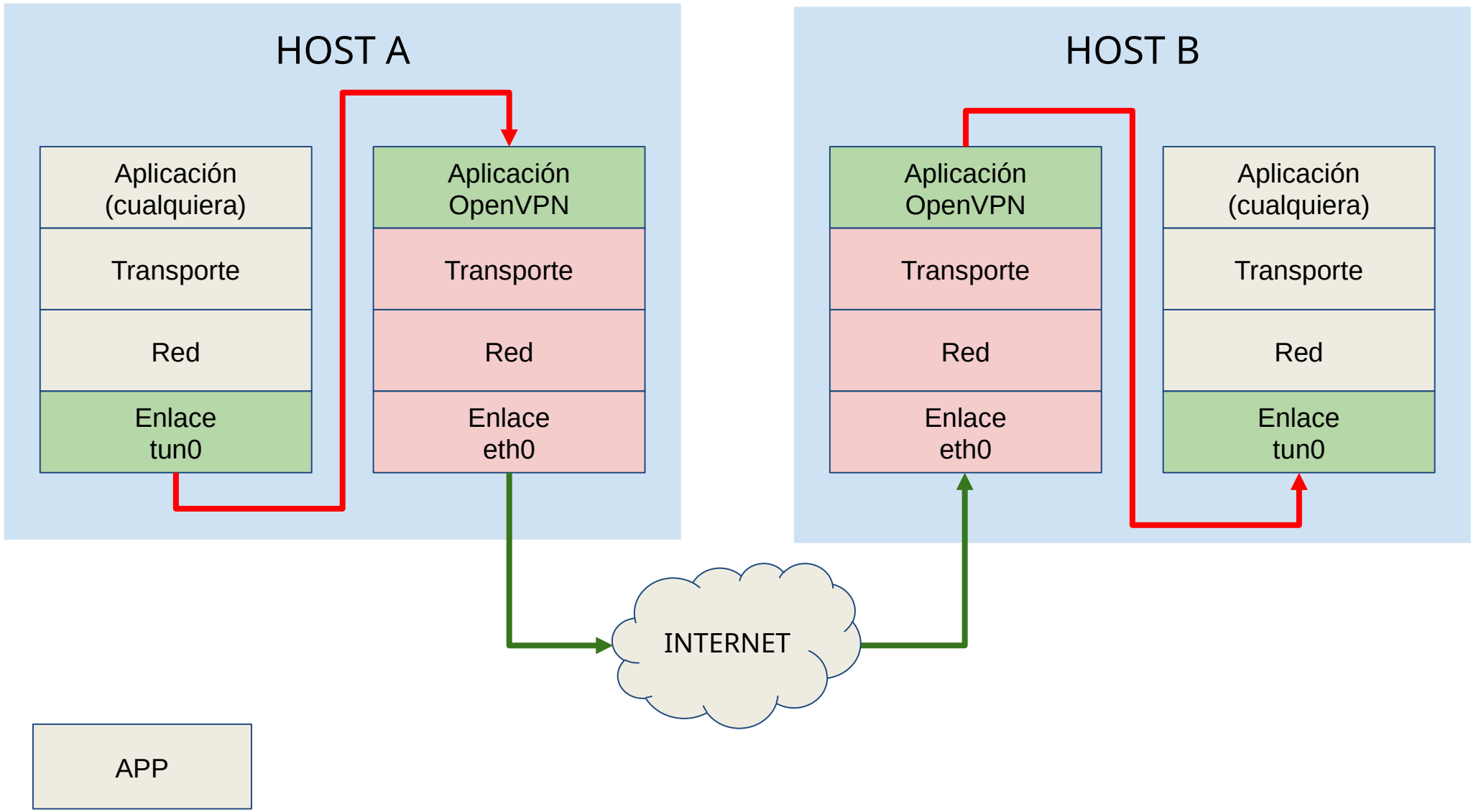


* dependiendo de la configuración, puede que autentique antes de descifrar el paquete

OpenVPN


HOST A
Aplicación (cualquiera)
Transporte
Red
Enlace tun0
Aplicación OpenVPN
Transporte
Red
Enlace eth0
HOST B
Aplicación OpenVPN
Transporte
Red
Enlace eth0
Aplicación (cualquiera)
Transporte
Red
Enlace tun0
INTERNET
APP
TCP
IP
?

OpenVPN


HOST A
Aplicación (cualquiera)
Transporte
Red
Enlace tun0
Aplicación OpenVPN
Transporte
Red
Enlace eth0
HOST B
Aplicación OpenVPN
Transporte
Red
Enlace eth0
Aplicación (cualquiera)
Transporte
Red
Enlace tun0
INTERNET
APP

TCP sobre IP sobre TCP sobre IP...

Nótese que hay encapsulamiento:

- PDU de App (cualquiera) sobre PDU de Transporte
- PDU de Transporte sobre PDU Red
- PDU de Red sobre PDU de Enlace Virtual (opcional)
- PDU de Enlace (opc) sobre PDU de App (OpenVPN)
- PDU de App (OpenVPN) sobre PDU de Transporte
- PDU de Transporte sobre PDU Red
- PDU de Red sobre PDU de Enlace (real)

TCP sobre IP sobre TCP sobre IP...

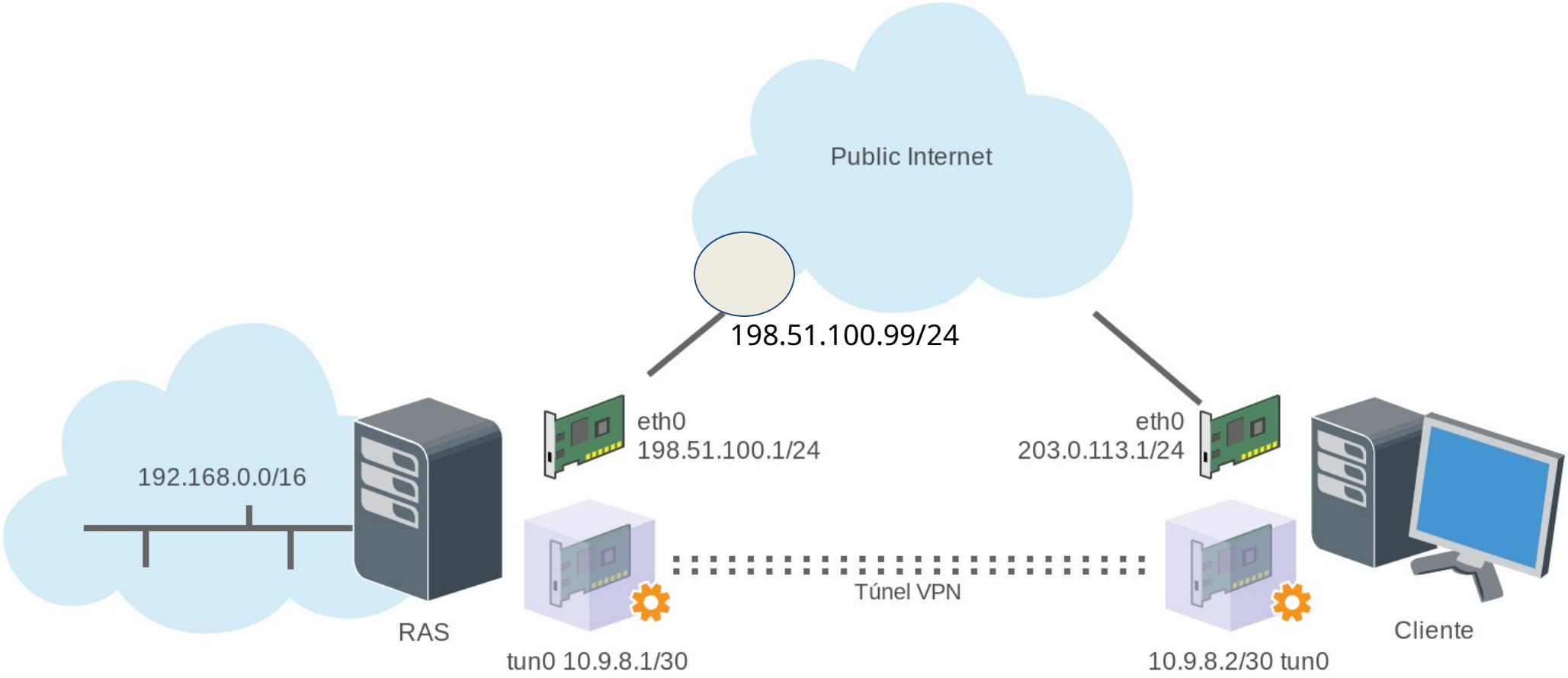
Nótese que hay encapsulamiento:

- PDU de App (cualquiera) sobre PDU de Transporte
- PDU de Transporte sobre PDU Red
- PDU de Red sobre PDU de Enlace Virtual (opcional)
- PDU de Enlace (opc) sobre PDU de App (OpenVPN)
- PDU de App (OpenVPN) sobre PDU de Transporte
- PDU de Transporte sobre PDU Red
- PDU de Red sobre PDU de Enlace (real)

TCP sobre IP sobre TCP sobre IP...

- Utilizar TCP sobre IP sobre ... sobre TCP sobre IP conlleva problemas de performance pues se duplica:
  - Control de errores
  - Control de congestión
  - Timers
  - Buffers
- Por ello, se recomienda que las PDU de OpenVPN se transporten sobre UDP (puerto 1194).
- No adiciona demasiado overhead y no posee entrega asegurada (al igual que IP).

Esquema de funcionamiento



Establecimiento del túnel (conexión y autenticación)

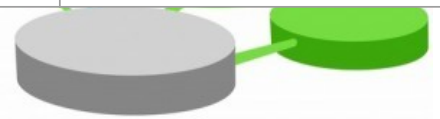
Antes de establecer el túnel

Tabla de Rutas -- Servidor de Acceso Remoto

DESTINO	MÁSCARA	GATEWAY	INTERFAZ	COMENTARIO
198.51.100.0	/24	*	eth0	enlace hacia el ISP
192.168.0.0	/16	*	eth1	hacia red propia
*	*	198.51.100.99	eth0	hacia Internet

Tabla de Rutas -- Cliente de Acceso Remoto

DESTINO	MÁSCARA	GATEWAY	INTERFAZ	COMENTARIO
203.0.113.0	/24	*	eth0	enlace hacia el ISP
*	*	203.0.113.99	eth0	hacia Internet



Luego de establecer el túnel

Tabla de Rutas -- Servidor de Acceso Remoto

DESTINO	MÁSCARA	GATEWAY	INTERFAZ	COMENTARIO
198.51.100.0	/24	*	eth0	enlace hacia el ISP
192.168.0.0	/16	*	eth1	hacia red propia
10.9.8.0	/30	*	**tun0**	túnel cifrado
*	*	198.51.100.99	eth0	hacia Internet

Tabla de Rutas -- Cliente de Acceso Remoto

DESTINO	MÁSCARA	GATEWAY	INTERFAZ	COMENTARIO
203.0.113.0	/24	*	eth0	enlace hacia el ISP
10.9.8.0	/30	*	**tun0**	túnel cifrado
192.168.0.0	/16	10.9.8.1	**tun0**	hacia red organiz.
*	*	203.0.113.99	eth0	hacia Internet

Luego de establecer el túnel

Tabla de Rutas -- Servidor de Acceso Remoto

DESTINO	MÁSCARA	GATEWAY	INTERFAZ	COMENTARIO
198.51.100.0	/24	*	eth0	enlace hacia el ISP
192.168.0.0	/16	*	eth1	hacia red propia
10.9.8.0	/30	*	**tun0**	túnel cifrado
*	*	198.51.100.99	eth0	hacia Internet

Tabla de Rutas -- Cliente de Acceso Remoto

DESTINO	MÁSCARA	GATEWAY	INTERFAZ	COMENTARIO
203.0.113.0	/24	*	eth0	enlace hacia el ISP
10.9.8.0	/30	*	**tun0**	túnel cifrado
192.168.0.0	/16	10.9.8.1	**tun0**	hacia red organiz.
*	*	203.0.113.99	eth0	hacia Internet

¿Qué tráfico va por la VPN y qué tráfico no?
¿Podría salir todo el tráfico por la VPN?

Modos de networking en OpenVPN

Routing mode (Layer 3 VPN tun0)

- En el modelo que vimos de OpenVPN, se utiliza una red IP nueva para el túnel entre el cliente y el servidor.
- De esta forma, el servidor VPN actúa como “router” e interconecta dos redes de capa 3: la que lleva al cliente y la de la organización.

Bridging mode (Layer 2 VPN tap0)

- Alternativamente, OpenVPN puede configurarse para “extender” una red existente de capa 2 (LAN) tal como si fuera un switch.
- En este modo, el cliente VPN obtiene una dirección IP de la red remota y puede operar en ella como un local (utilizando ARP, DHCP, etc).

Administración y Gestión de Redes
Lic. en Sistemas de Información

Laboratorio de REDES
Recuperación de Información
y Estudios de la Web

Wireward

- 2025 -

Wireward

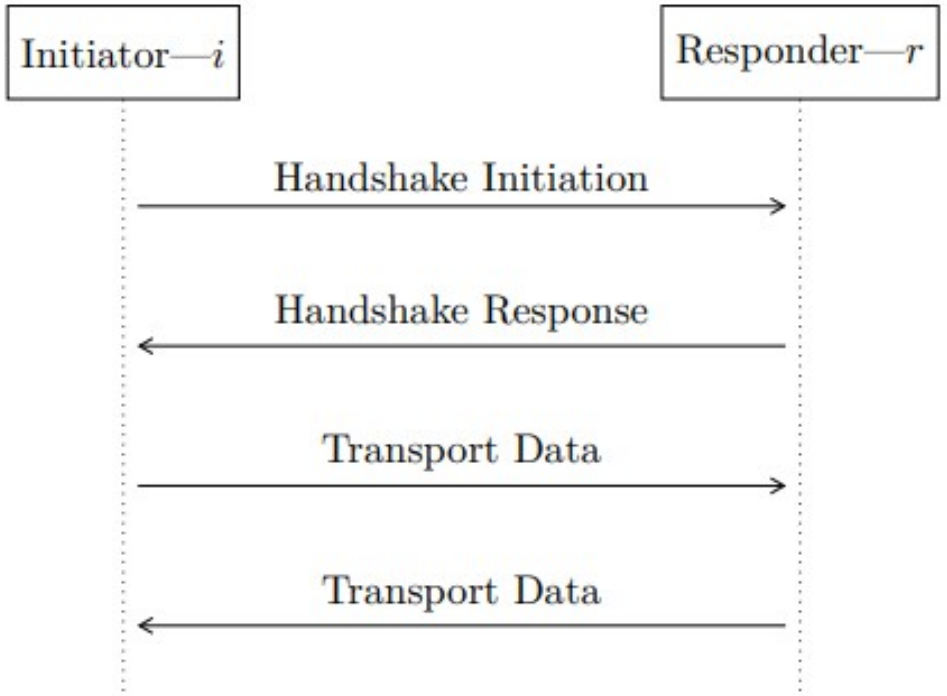
- Alternativa moderna a IPSec y OpenVPN.
- Diseñado para ser simple y rápido.
- Implementado en Kernel (Linux, macOS, BSD, iOS, Android) y de código reducido.
- Reconección automática y posibilidad de roaming
- Crea una interfaz de red virtual (habitualmente wg*X*).
- El tráfico se envía por el túnel cifrado utilizando UDP (Puerto por default 51820)

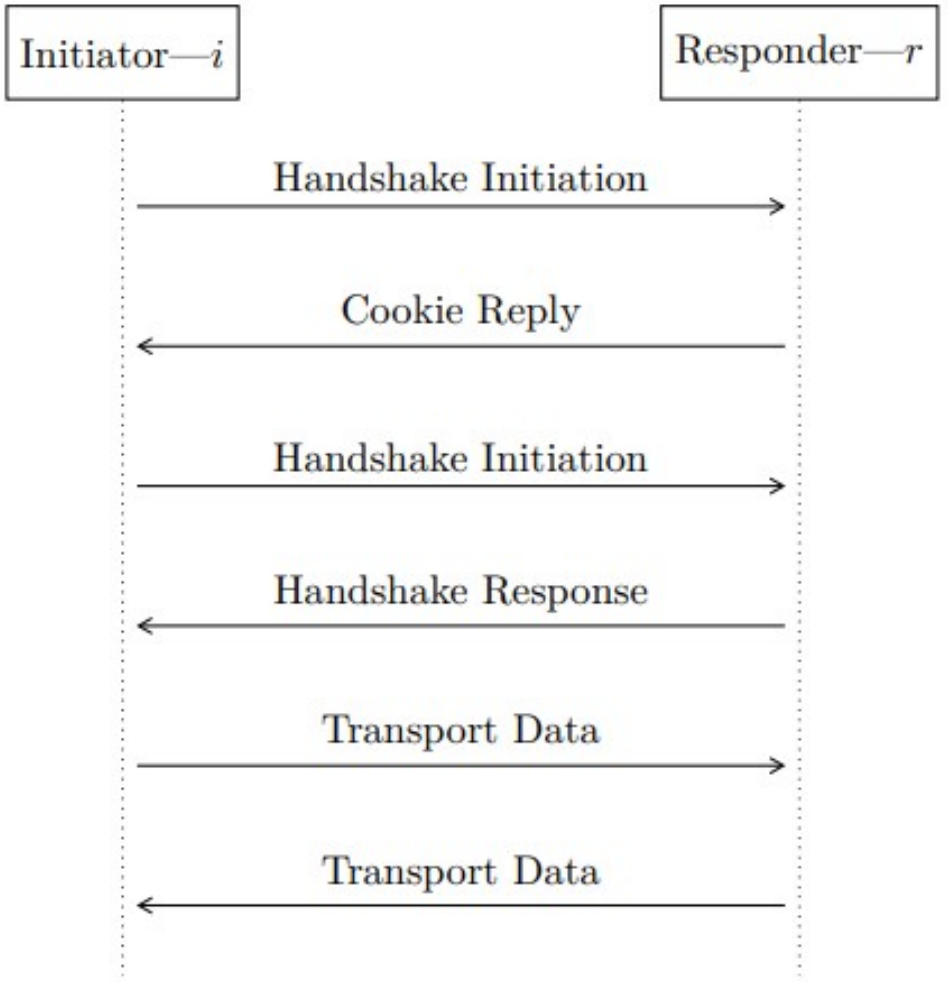
Wireward

- Modo de operación de WireGuard
  - Cada dispositivo (servidor y cliente) genera su propio par de claves públicas y privadas.
  - Las claves públicas deben intercambiarse para la autenticación mutua (método fuera de banda).
  - Mediante un proceso de “handshake” eficiente se establecen las sesiones seguras (túnel).
  - Una vez establecido el túnel, todo el tráfico de datos que viaja entre los dispositivos se cifra y envía encapsulado en UDP.
  - Tambiés es posible utilizar claves simétricas precompartidas en lugar de claves públicas.

Wireward

Sólamente 4 tipos de mensajes:





Bibliografía

- STALLINGS, W. 2011. *Cryptography and Network Security: Principles and Practice* (5th ed). Prentice Hall.
  - Capítulo 19: IP Security
- GORALSKI, W. 2017. *The Illustrated Network (2nd ed)*. Morgan Kaufmann.
  - Capítulo 27: Securing Sockets with SSL
  - Capítulo 33: IP Security
- YONAN J. 2003. *The User-Space VPN and OpenVPN* https://es.slideshare.net/guestb9d7f98/blug-talk-presentation
- HERTZOG, R.; MAS, R. 2015. *El manual del Administrador de Debian*. Freexian.
  - Capítulo 10. Sección 2: "Red privada virtual"