Departamento de Tecnología Electrónica

VIRTUAL PRIVATE NETWORK (VPN)

Tecnologías Avanzadas de la Información

Bibliografía

- Markus Feilner, OpenVPN Building and Integrating Virtual Private Networks. Packt Publishing. ISBN 1-904811-85-X
- Stephen A. Thomas, SSL and TLS Essentials, Wiley, ISBN 0-471-38354-6

Índice

- Introducción y conceptos básicos
- Túneles
- VPN en diferentes capas
- OpenVPN
- TINC

Introducción

- Objetivo: Interconexión segura de equipos
  - Solución 1: Líneas dedicadas
  - Solución 2: Uso de red pública con cifrado
- Definición: VPN, Red de datos privada sobre red pública
  - Virtual
  - Private
  - Network

Introducción

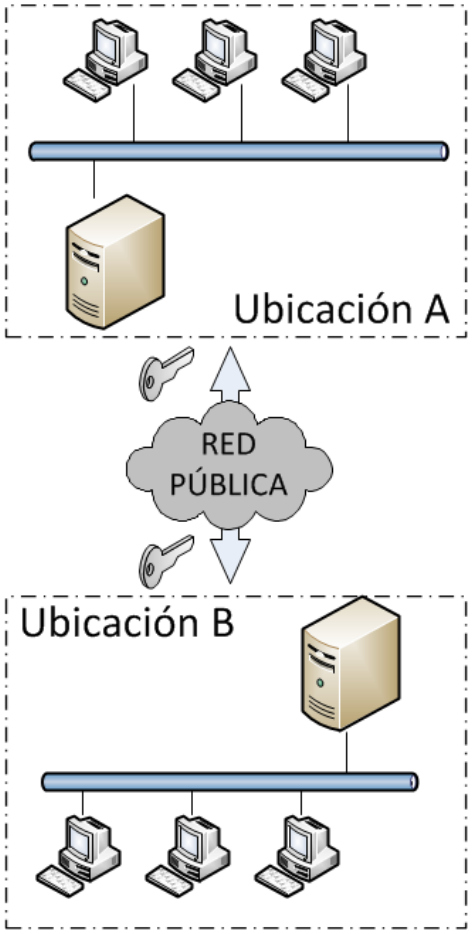
- Virtual: No es una línea dedicada, opera sobre una conexión ya existente
- Privada: Aunque los datos se transmiten por canales compartidos/públicos, serán visibles/ capturables pero no se deben poder descifrar
- Network: Se debe comportar de forma transparente para los equipos de red independiente de su ubicación

Introducción

- Requisitos VPN:
  - **Privacidad:** Sólo los equipos autorizados están conectados.
  - **Integridad:** La información intercambiada no puede ser alterada.
  - **Disponibilidad:** La conexión debe estar disponible cuando se necesite.

Introducción

- Escenarios de uso:
  - Interconexión de varias localizaciones remotas usando una red pública
  - Conexión de equipos remotos a red interna
  - Conexión de proveedores
- Se dispone de una red IP propia distribuida geográficamente



Conceptos básicos

- Privacidad = Criptografía: Se consigue cifrando el tráfico
- Criptografía: disciplina amplia (investigación, desarrollo, etc.) con fuerte componente matemático
- Criptografía en T.A.I:
  - Clave simétrica
  - Clave asimétrica
  - Certificados digitales

Túneles

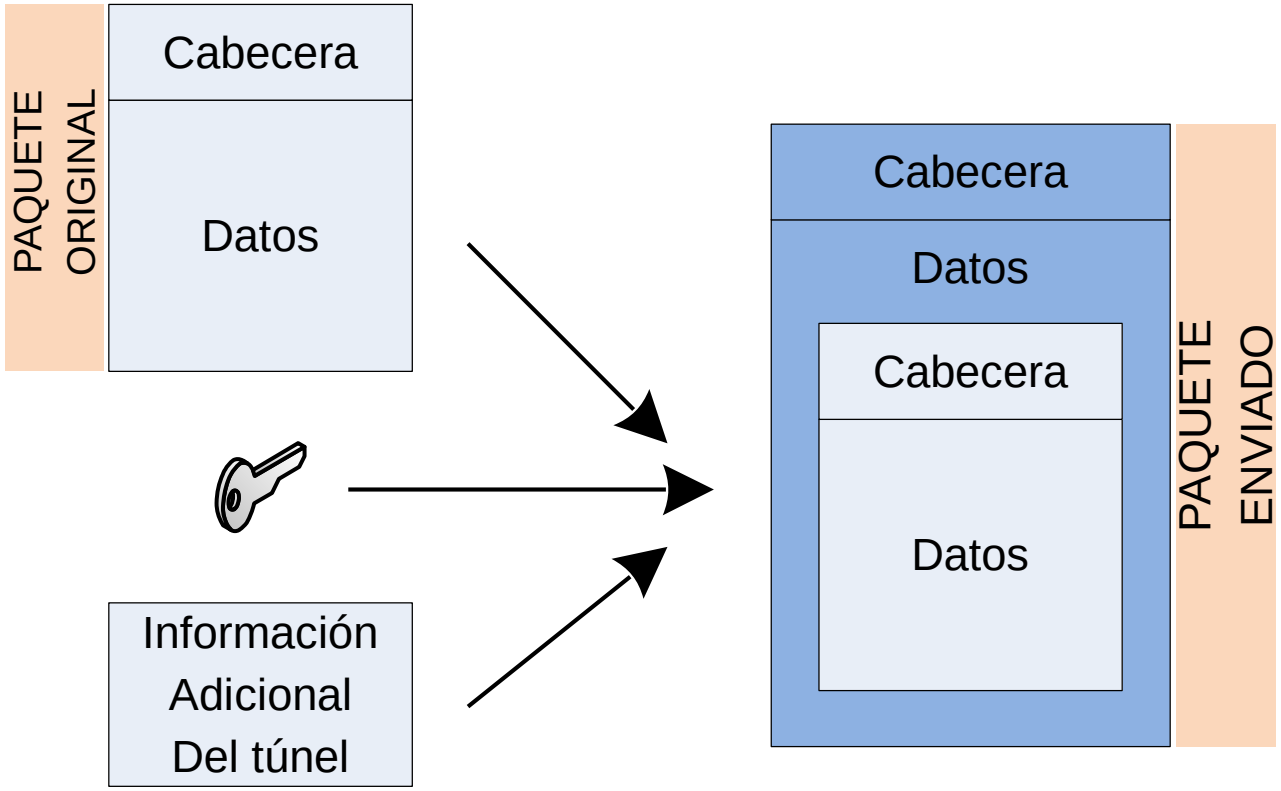
- Túnel: Canal de comunicación usado encapsulando un protocolo en otro.
  - Los datos se pueden cifrar antes de enviarse por un túnel.
  - El paquete original de red se encapsula dentro de un nuevo paquete, pero cifrado.
  - El paquete que se envía sólo tiene «visible» el destino y el origen del mismo

Túneles

- Encapsulación: Consistente en empaquetar una trama como datos en otra una trama de nivel superior.
- Ejemplos:
  - PPPoE / PPPoA: ADSL
  - MLPS: Relacionada con QoS (próximo tema)
  - Etc.

Túneles

- Desventaja: La envoltura produce sobrecarga en el tráfico (50% en muchas implementaciones)



Túneles

- Nos centraremos en túneles IP
- Existen estándares para implementación de túneles:
  - IPIP: IP in IP [RFC 1853]
  - GRE: General Routing Encapsulation: Desarrollado por Cisco y estandarizado [RFC 1701]
- Un túnel puede ser hecho en diferentes capas del modelo OSI

VPN en OSI capa 2

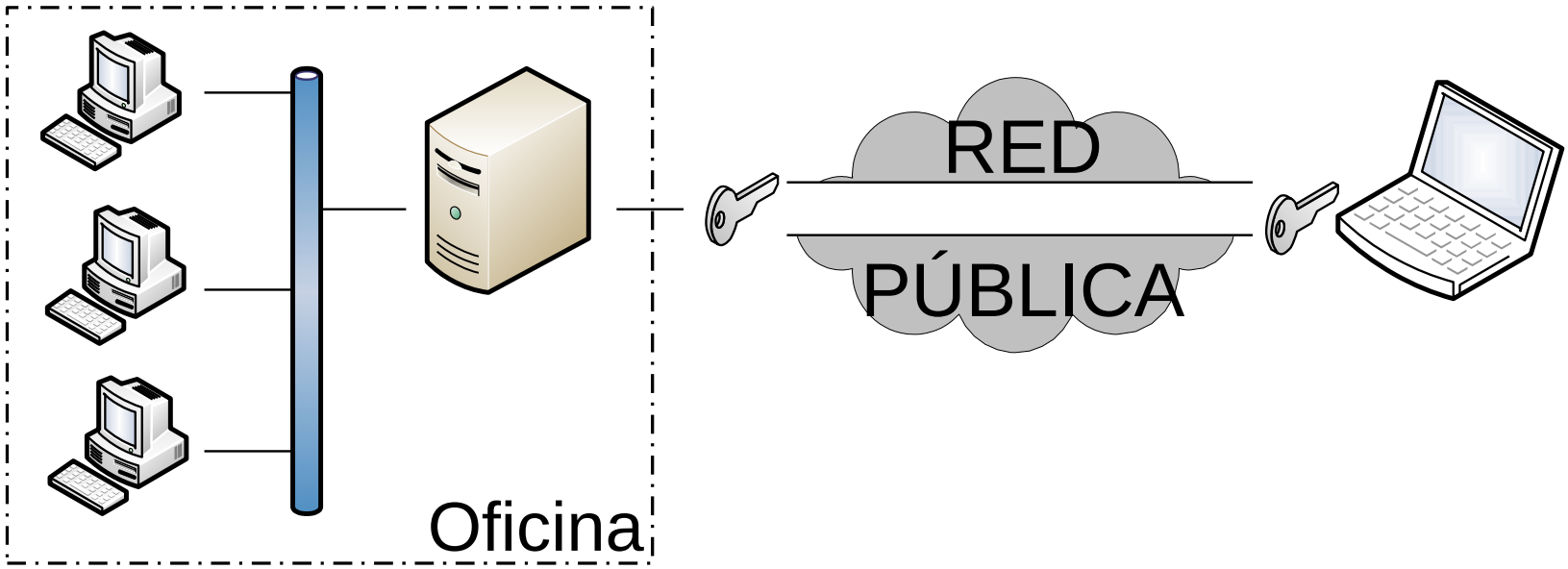
- Encapsular en la capa 2 permite transferir protocolos no-IP dentro del protocolo IP.
- Tecnologías VPN en la capa 2:
  - Point to Point (PPTP)
  - Layer 2 Forwarding (L2F)
  - Layer 2 Tunneling Protocol (L2TP)
  - Layer 2 Security Protocol (L2Sec)

VPN en OSI capa 2
PPTP

- PPTP: Protocolo de túnel punto a punto (PPTP)
  - Protocolo diseñado y desarrollado por 3Com, Microsoft Corporation, Ascend Communications y ECI Telematics, y definido en IETF [RFC 2637]
  - Se emplea en acceso virtual seguro de usuarios remotos a red privada
  - Emplea mecanismo de túneles para envío de datos desde cliente a servidor
  - Es una expansión de PPP, encapsula las tramas del PPP en datagramas IP
  - Usa GRE para encapsular
  - Desventaja: sólo se permite un túnel simultáneamente
  - Vulnerabilidades: No se recomienda su uso bajo ciertas condiciones [Microsoft Security Advisory – 2743314]

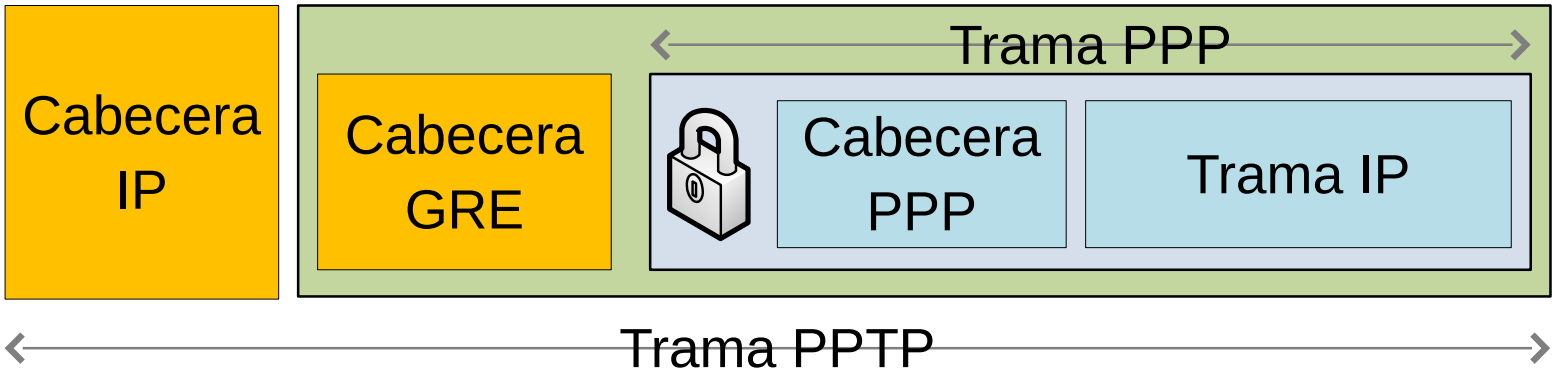
VPN en OSI capa 2
PPTP

- PPTP:
  - El servidor posee una IP real
  - El servidor es un puente para los clientes remotos



VPN en OSI capa 2
PPTP

- Trama PPTP:
  - Incluye una trama PPP encapsulada en un paquete IP usando GRE
  - GRE se define en la cabecera IP (protocolo 47)



VPN en OSI capa 2
PPTP

- PPP: Protocolo punto a punto [RFC 1661]
  - Capaz de transportar múltiples protocolos
  - Usado para conectar con ISP mediante una línea telefónica (modem) o RDSI
  - Versiones para banda ancha (PPPoE y PPPoA)
  - Establecer, mantener y finalizar conexión pto-pto
  - Mecanismos de autenticación de usuarios: PAP y CHAP
  - Crear tramas cifradas

VPN en OSI capa 2
PPTP

- Autenticación PPTP, emplea los mismos mecanismos que PPP:
  - PAP (Password Authentication Protocol)
    - Muy simple: envío de nombre y contraseña en claro
  - CHAP (Challenge Handshake Authentication Protocol)
    - Mecanismo desafío-respuesta
    - Clave secreta compartida
    - Cliente genera una huella a partir del desafío recibido: HASH + SALTO
    - Envíos de varios desafíos para revalidar identidad, el desafío nunca debe repetirse.

VPN en OSI Capa 2

- Características de estas tecnologías:
  - Disponen de métodos de autenticación
  - Disponen de NAT
  - Asignación de IP dinámica en los extremos del túnel
  - Soporte para PKI (Public Key Infrastructures)

VPN en OSI Capa 2
Layer 2 Forwarding (L2F)

- Layer 2 Forwarding (L2F) desarrollado por varias compañías como Cisco [RFC2341]
- Ofrece más posibilidades que PPTP:
  - No depende del protocolo IP puede trabajar sobre otros como ATM
  - Los túneles pueden tener más de una conexión

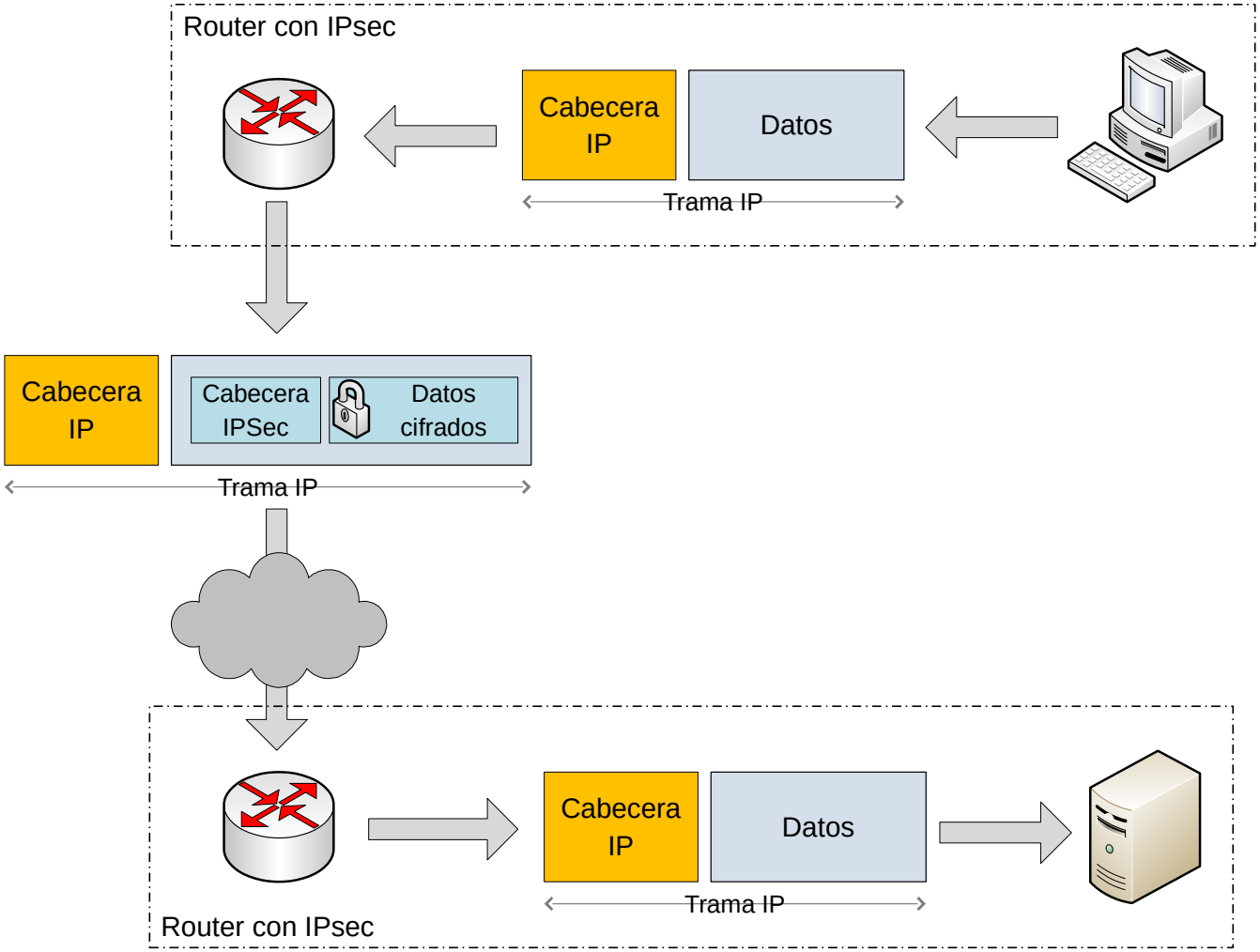
VPN en OSI Capa 2
Layer 2 Tunneling Protocol

- **Layer 2 Tunneling Protocol (L2TP)**: aprobado por IETF ante el protocolo propietario de Microsoft PPTP.
- Aceptado como estándar y ampliamente usado por todos los fabricantes.
- Combina ventajas de L2F y PPTP eliminando las desventajas de PPTP
- No proporciona mecanismos propios de autenticación se pueden usar: CHAP, EAP

VPN en OSI Capa 3

- IPsec: Una de las tecnologías más usadas
  - Estandarizado por IETF (1995)
  - No es un simple protocolo
  - Es un conjunto de protocolos y estándares
  - Protocolo IP 50 y 51
- IPsec funciona principalmente en modo túnel o en modo transporte
- Desventajas IPsec:
  - Muy complejo
  - Existen muchas implementaciones diferentes
  - No se pueden encapsular protocolos de bajo nivel

VPN en OSI Capa 3



VPN en OSI Capa 3

- Open VPN:
  - Es una solución basada en SSL/TLS
  - Implementa conexiones en la capa 2 o capa 3
  - Se estudiará posteriormente y se utilizará en el laboratorio
- TINC
  - VPN Distribuida frente a OpenVPN
  - Utiliza cifrado asimétrico y simétrico simultaneamente

VPN en OSI Capa 4

- Es posible establecer un túnel VPN en el nivel de aplicación: SSL y TLS
- Ventajas:
  - Solución simple para el usuario, la conexión comienza entrando con el navegador en una página web segura https://...
  - Ejemplo: TINC sobre HTTP o HTTPS o DNS

Privacidad

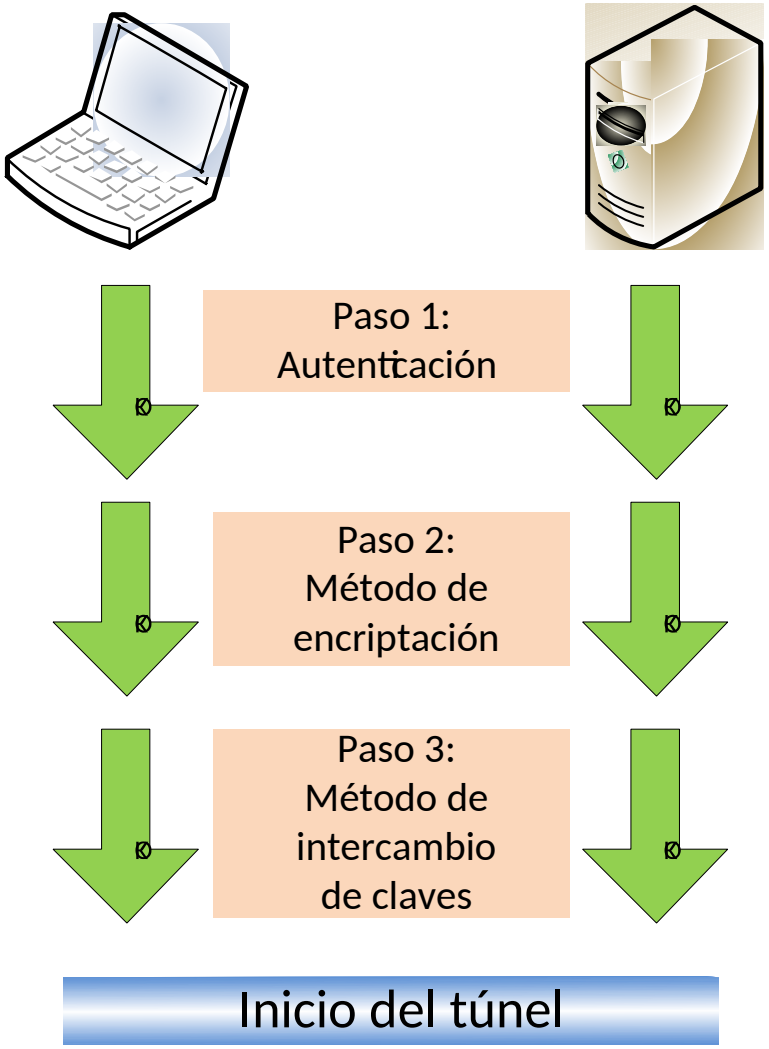
- **Privacidad:** Una VPN sin seguridad no es privada
- La privacidad en VPN se consigue mediante técnicas criptográficas
- Utilizaremos técnicas criptográficas ampliamente utilizadas y estudiadas:
  - Clave simétrica
  - Clave asimétrica

Privacidad: cifrado simétrico

- Soluciones con cifrado simétrico:
  - IPSec cambia la clave cada cierto periodo de tiempo (tiempo de vida)
  - El tiempo de vida debe ser menor que el tiempo requerido/estimado para descifrar la clave
- Se requiere un método de intercambio de claves seguro:
  - Complejo
  - Eslabón débil
  - Ejemplo: Algoritmo Diffie-Hellman

Privacidad: cifrado simétrico

- Esquema de autenticación en VPN clásicas en tres pasos
- Se negocian parámetros entre cliente y servidor:
  - Algoritmos de cifrado
  - Compresión
  - Dirección IP
  - …



Privacidad: Cifrado asimétrico

- Cifrado asimétrico:
  - Clave pública / privada sin firma digital: TINC
  - PKI con certificados digitales: OpenVPN

OPENVPN

http://openvpn.net

OpenVPN

- Es una solución basada en SSL / TLS
- Implementa conexiones en la capa 2 o capa 3
- Ventajas: Despliegue rápido e infraestructura simple, bajo coste.
- Desventajas: Existen pocas soluciones hardware

OpenVPN

- Requisitos:
  - TUN/TAP drivers
  - OpenSSL
  - LZO: Compresión en tiempo real
- Soportado:
  - Linux
  - Mac
  - Windows
  - Android

OpenVPN

- Modos de funcionamiento:
  - Sobre TCP
  - Sobre UDP
  - Soporte para proxy
- Tipo de seguridad:
  - Clave simétrica (no recomendado)
  - Clave asimétrica (RSA)
- Tipos de túneles
  - Túnel IP
  - Puente ethernet

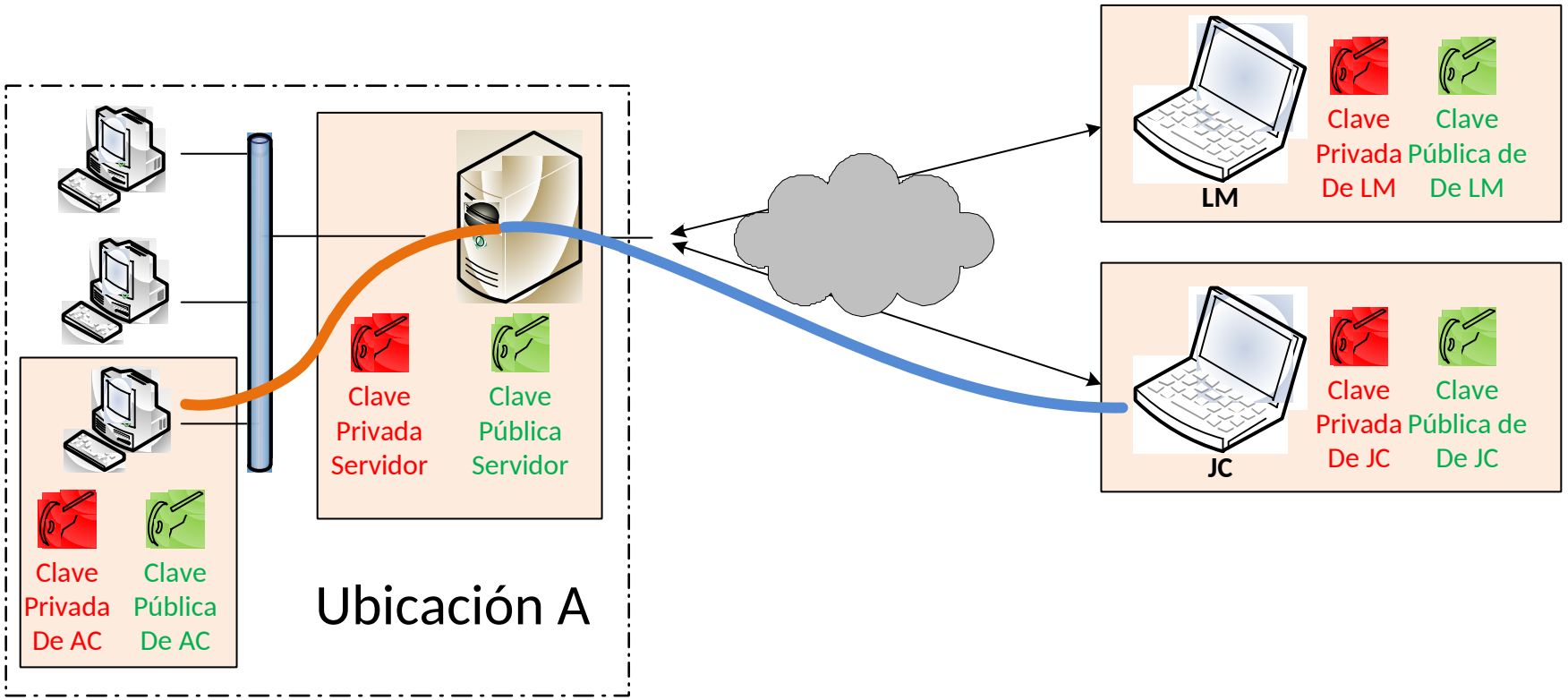
OpenVPN

- Túnel IP:
  - Uso habitual
  - Usado para tráfico IP punto-a-punto sin broadcast
  - Bastante más eficiente que un puente ethernet
  - Más fácil de configurar

OpenVPN

- Puente ethernet:
  - Aplicaciones específicas
  - Se pueden usar para encapsular tanto protocolos IP como no-IP.
  - Apropiado para aplicaciones que se comunican utilizando difusión (broadcast), red de Windows y juegos de área local (LAN).
  - Son bastante más difíciles de configurar.

OpenVPN



Esquema OPENVPN con cifrado asimétrico

Departamento de
Tecnología Electrónica

TINC

http://tinc-vpn.org/

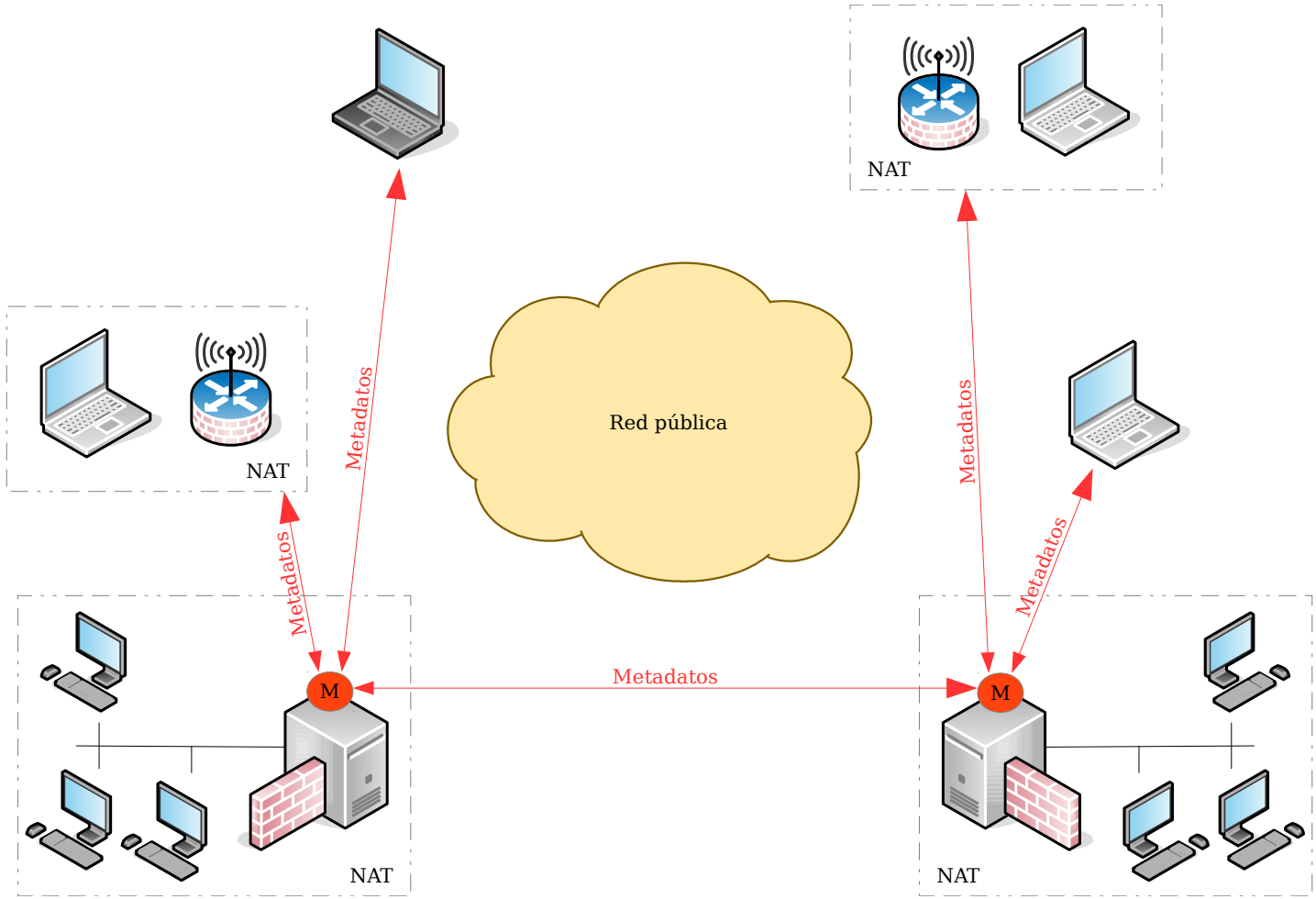
TINC

- Mesh VPN: Sistema distribuido
- No hay un servidor central
- Sólo es necesario configurar puntos de entrada que actúan como nodos maestros
- Usa TCP y UDP:
- Aplicaciones específicas
  - TCP: Intercambio de metadatos
  - UDP: Intercambio de datos

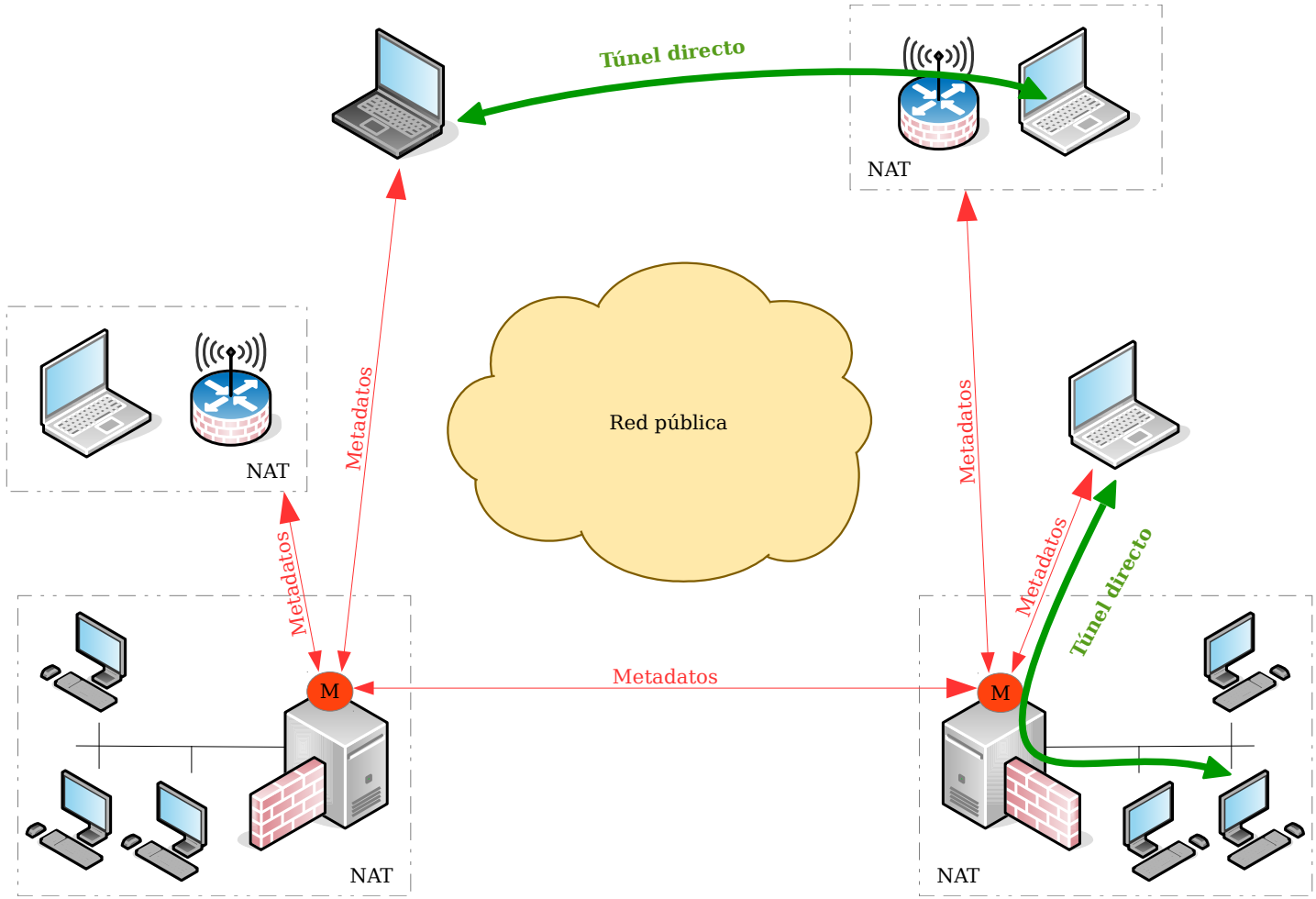
TINC

- TINC Intenta salvar las siguientes barreras:
  - Equipos detrás de NAT:
    - Usa STUN si es posible
    - Si no puede hace relay
  - Nodos maestros caídos
  - Limitación de conexión: puede hacer túneles sobre HTTP, HTTPS, ICMP y DNS.

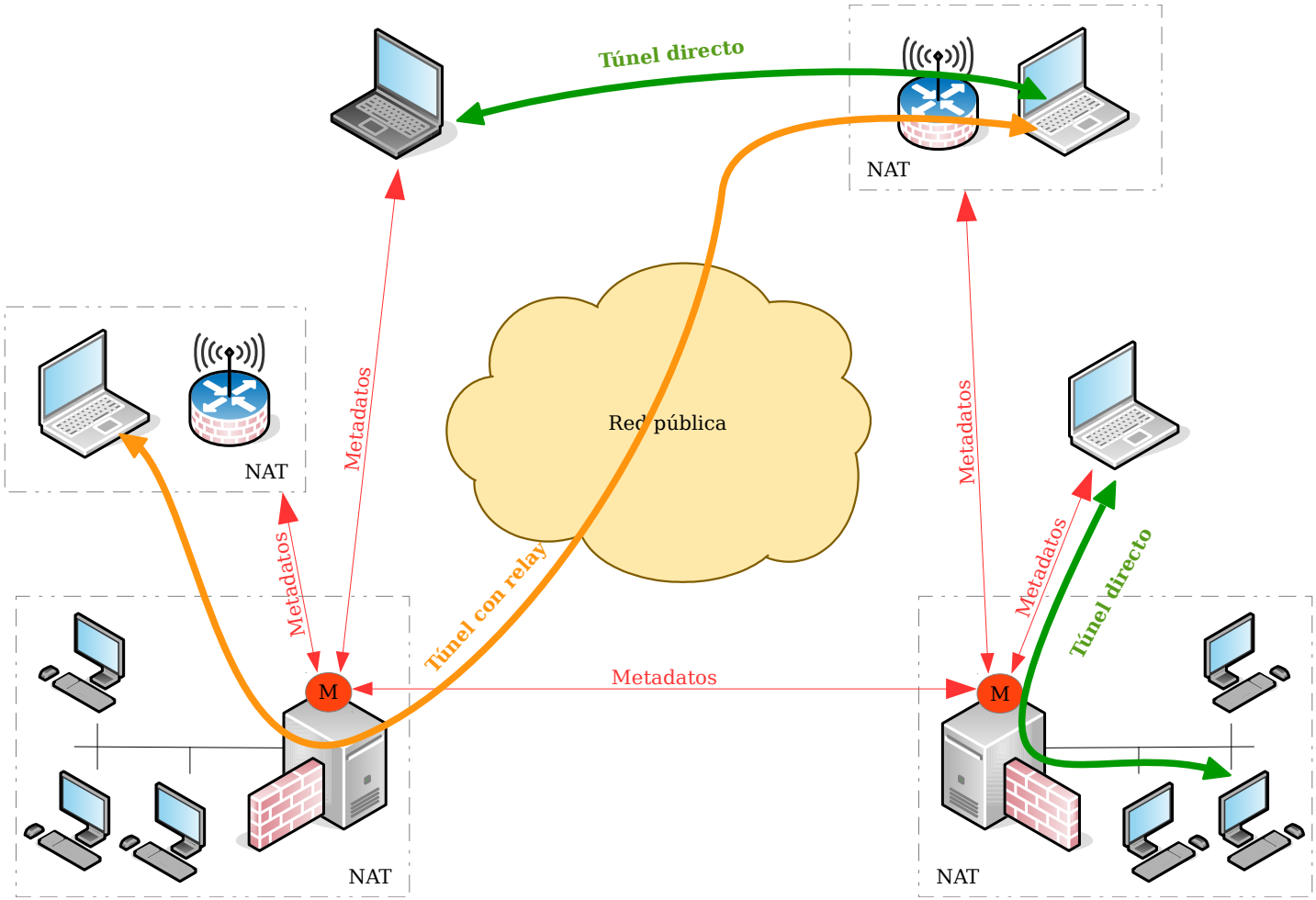
TINC
Conexión de nodos



TINC
Transferencia de datos



TINC
Transferencia de datos



TINC
Autenticación

- Cada nodo:
  - Indica quien és
  - Y quien está permitido a conectarse a él (nodo maestro)
- Método:
  - Clave publica / privada
  - Certificados digitales X.509
  - Claves PGP