Redes Privadas Virtuales (VPN)

Arquitectura, Protocolos Criptográficos y Seguridad

Grupo #05

Cevallos Michael

Enriquez Jhon

Pereguez Luis

1. Definición y Fundamentos

CONCEPTO TÉCNICO

Una **VPN** es una tecnología de red que crea una conexión segura ("túnel") sobre una red pública (Internet). Permite la extensión lógica de la red local, garantizando que los datos enviados sean indescifrables para intermediarios.

Objetivos de Seguridad (CIA):
1. **Confidencialidad:** Prevención de lectura no autorizada (Cifrado).
2. **Integridad:** Detección de modificaciones en tránsito (Hashing).
3. **Autenticación:** Verificación de identidad de los extremos [6].

TIPOLOGÍA PRINCIPAL

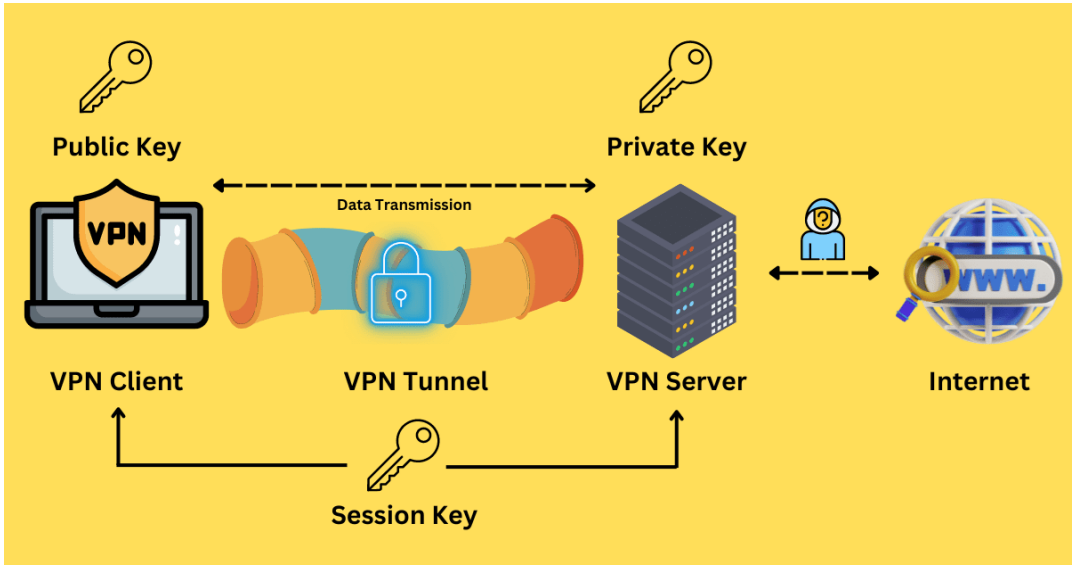
- **Remote Access (Client-to-Site):** Conecta un endpoint (usuario) a la LAN corporativa. Esencial para teletrabajo y movilidad [6].
- **Site-to-Site (LAN-to-LAN):** Interconecta dos redes geográficamente separadas mediante gateways VPN dedicados. Transparente al usuario final.
- **Host-to-Host:** Poco común, usado para asegurar un canal específico entre dos servidores críticos.

Arquitectura de Túnel y Encapsulación

MECÁNICA DE ENCAPSULACIÓN

El proceso fundamental de una VPN es la encapsulación: el paquete original (privado) se envuelve dentro de una nueva cabecera IP (pública) para su enrutamiento en Internet.

- **Interfaz Virtual (TUN/TAP):** El SO ve la VPN como una tarjeta de red más.
- **Punto de Terminación:** Dispositivo que des encapsula, descifra y reenvía el tráfico a la red destino.



2. Algoritmos Criptográficos Involucrados

CIFRADO SIMÉTRICO

Confidencialidad del payload de datos.

- **AES (128/256-GCM):** Advanced Encryption Standard. Estándar de facto, robusto y acelerado por hardware (AES-NI) [2].
- **ChaCha20:** Cifrado de flujo moderno. Más rápido que AES en CPUs sin aceleración dedicada (móviles/IoT) [1].

CIFRADO ASIMÉTRICO

Intercambio de claves y autenticación.

- **RSA:** Basado en factorización de enteros. Claves largas (2048+ bits) [6].
- **ECDH (Elliptic Curve Diffie-Hellman):** Permite acordar claves simétricas sobre un canal inseguro.
- **ECDSA:** Firmas digitales con curvas elípticas. Más eficiente que RSA.

FUNCIONES HASH

Integridad (HMAC) y firmas.

- **SHA-2 (256/512):** Secure Hash Algorithm. Estándar actual.
- **Poly1305:** Generador de MAC de alta velocidad. Generalmente pareado con ChaCha20 en WireGuard [5].

3. Protocolos Criptográficos

Protocolo	Capa (OSI)	Contexto y Uso	Algoritmos Típicos
IPSec (IKEv2)	Capa 3 (Red)	Estándar corporativo para Site-to-Site y Remote Access. Complejo pero interoperable.	AES-GCM, SHA-2, Diffie-Hellman Groups.
WireGuard	Capa 3 (Red)	Nueva generación. Código ligero, "Stateless", fácil auditoría y alto throughput.	ChaCha20, Poly1305, Curve25519, BLAKE2s.
OpenVPN	Capa 7 (App)*	Estándar de código abierto muy flexible. Opera sobre TCP o UDP. Evade firewalls fácilmente.	Librería OpenSSL (AES, RSA, etc.).
SSTP	Capa 7 (App)	Propietario de Microsoft. Usa SSL/TLS sobre puerto 443. Integrado en Windows.	AES, RC4 (Legacy), certificados SSL.

* OpenVPN corre en espacio de usuario pero tuneliza tráfico IP.

Diseño Esquemático: Suite IPSec [7]

COMPONENTES DE LA SUITE

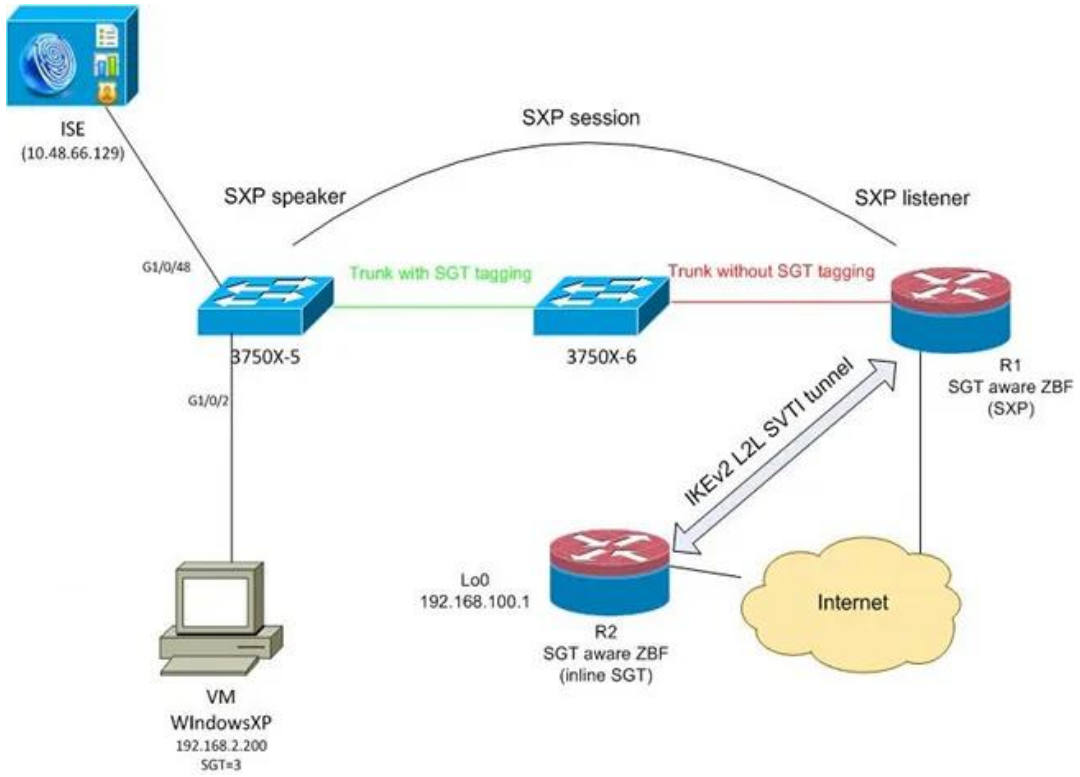
- **IKEv2 (Internet Key Exchange):** Protocolo de plano de control. Negocia las "Security Associations" (SA). Maneja la autenticación y el intercambio de claves.
- **ESP (Encapsulating Security Payload):** Protocolo de plano de datos (IP 50). Transporta la carga útil cifrada. Provee confidencialidad, integridad y anti-replay.
- **AH (Authentication Header):** (IP 51) Solo integridad/autenticación. Incompatible con NAT, uso decreciente.

DIFERENCIA DE MODOS [3]

Modo Transporte (End-to-End):
Cifra solo el payload. La cabecera IP original se mantiene visible.
[IP Orig][ESP Hdr][Datos Cifrados][ESP Trl]

Modo Túnel (Site-to-Site):
Cifra todo el paquete original. Nueva cabecera IP.
[IP Nueva][ESP Hdr][IP Orig Cifrada][Datos Cifrados][ESP Trl]

Flujo de Establecimiento (IKEv2 Handshake)



FASES DE CONEXIÓN [8]

1. **IKE_SA_INIT:** Negociación de algoritmos criptográficos y parámetros Diffie-Hellman. Se establece un canal inicial no autenticado pero cifrado.
2. **IKE_AUTH:** Intercambio de identidades (Certificados o PSK) y creación de la primera *Child SA* (el túnel de datos).
3. **Transferencia de Datos:** Tráfico encapsulado en ESP fluye bidireccionalmente.
4. **Rekeying:** Regeneración periódica de claves para asegurar PFS (Perfect Forward Secrecy).

4. Escenarios de Uso Frecuente

TELETRABAJO SEGURO

Contexto: Empleados accediendo a servidores internos desde Wi-Fi doméstico o público.

Solución: VPN de Acceso Remoto con autenticación MFA. Previene el robo de credenciales corporativas en redes inseguras [6].

INTERCONEXIÓN DE SEDES

Contexto: Conexión de sucursales bancarias con el Data Center central.

Solución: VPN IPSec Site-to-Site. Reemplaza líneas dedicadas (MPLS) reduciendo costos drásticamente mientras mantiene el cifrado [3].

ACCESO ACADÉMICO

Contexto: Estudiantes e investigadores accediendo a bases de datos (IEEE Xplore, JSTOR) restringidas por IP.

Solución: SSL VPN (Portal Web). Permite acceso a recursos bibliotecarios sin instalar clientes complejos.

Ventajas y Limitaciones Técnicas

👍VENTAJAS

- **Coste-Eficiencia:** Usa infraestructura pública compartida en lugar de costosos enlaces dedicados.
- **Geolocalización:** Permite eludir restricciones geográficas y censura.
- **Integridad:** Garantiza que los datos no han sido alterados en ruta (anti-tampering).

⚠LIMITACIONES Y RIESGOS

- **Latencia (Overhead):** El encapsulamiento y cifrado añaden tiempo de procesamiento y reducen el MTU efectivo (fragmentación) [4].
- **Split-Tunneling:** Si se configura mal, permite tráfico directo a internet desde el cliente, exponiendo la red interna a malware.
- **Complejidad:** La gestión de PKI (certificados) en implementaciones masivas es crítica.

Bibliografía:

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Hoboken, NJ: Pearson, 2020.

[2] S. Kent y K. Seo, “Security Architecture for the Internet Protocol”, Internet Engineering Task Force, RFC 4301, dic. 2005. doi: **10.17487/RFC4301**.

[3] S. T. Aung y T. Thein, “Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks”, en *2020 IEEE Conference on Computer Applications (ICCA)*, Yangon, Myanmar: IEEE, feb. 2020, pp. 1–5. doi: **10.1109/ICCA49400.2020.9022848**.

[4] J. A. Donenfeld, “WireGuard: Next Generation Kernel Network Tunnel”, en *NDSS Symposium 2017*, San Diego, CA: Internet Society, 2017. doi: **10.14722/NDSS.2017.23160**.

[5] C. Kaufman, P. Hoffman, Y. Nir y P. Eronen, “Internet Key Exchange Protocol Version 2 (IKEv2)”, Internet Engineering Task Force, RFC 7296, oct. 2014. doi: **10.17487/RFC7296**.

[6] A. Kurniawan, “Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol”, *IEEE Access*, vol. 11, pp. 58912–58925, 2023. doi: **10.1109/ACCESS.2023.3284567**.

5. Evaluación de Conocimientos

1. Pregunta: ¿Cuál de los siguientes modos de operación de IPSec se caracteriza por encapsular **todo** el paquete IP original dentro de una nueva cabecera, siendo el estándar habitual para las conexiones *Site-to-Site*?

a) Modo Transporte

b) Modo IKE_AUTH

c) Modo Túnel

d) Modo Transparente

e) Modo Híbrido

2. Pregunta: Seleccione los tres **(3)** algoritmos criptográficos que se utilizan legítimamente dentro de una arquitectura VPN segura para funciones de cifrado o integridad.

a) AES (Advanced Encryption Standard)

b) Telnet (Teletype Network)

c) RSA (Rivest-Shamir-Adleman)

d) SHA-2 (Secure Hash Algorithm 2)

e) POP3 (Post Office Protocol 3)

5. Evaluación de Conocimientos

3. Emparejamiento

Instrucciones: Relaciona cada número (Concepto) con su letra correspondiente (Definición).

Conceptos:

1. WireGuard
2. IKEv2
3. SSL VPN
4. PFS (Perfect Forward Secrecy)
5. ChaCha20

Definiciones:
A. Protocolo de la suite IPSec encargado de negociar claves y autenticar.

B. Algoritmo de cifrado rápido, ideal para móviles que no soportan AES por hardware.

C. Protocolo moderno, de código ligero y alto rendimiento ("Stateless").

D. Tecnología que permite acceso vía navegador web (Capa 7) sin instalar clientes.

E. Propiedad de seguridad que protege las sesiones pasadas si se roba la clave actual.

5. Evaluación de Conocimientos

4. Pregunta: ¿Qué nombre recibe la técnica de configuración que permite a un usuario de VPN acceder a la red corporativa segura y a Internet local simultáneamente sin enviar todo el tráfico por el túnel?

5. Pregunta: El modo **Transporte** de IPSec cifra únicamente la carga útil (payload) de los datos, manteniendo visible la cabecera IP original para el enrutamiento.

- Verdadero
- Falso