UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN COMPUTACIÓN

INFORME TÉCNICO: REDES PRIVADAS VIRTUALES (VPN)

Materia: Criptografía y seguridad de la información

Integrantes (Grupo #05):

- Cevallos Michael
- Enriquez Jhon
- Pereguez Luis

1. Definición y Fundamentos Tecnológicos

Una **Red Privada Virtual (VPN)** se define como una tecnología de red que permite la extensión de una red de área local (LAN) sobre una red pública no controlada, típicamente Internet. Su objetivo fundamental es crear un "túnel" de comunicación seguro que garantice que los datos transmitidos mantengan las propiedades de una red privada, a pesar de transitar por una infraestructura pública insegura [1].

El funcionamiento de una VPN se rige por la garantía de la **Tríada de Seguridad (CIA)** en tránsito:

1. **Confidencialidad:** Se asegura mediante algoritmos de cifrado simétrico, impidiendo que actores malintencionados (Man-in-the-Middle) puedan leer el contenido de los paquetes interceptados .
2. **Integridad:** Se garantiza mediante funciones hash y códigos de autenticación de mensajes (HMAC), asegurando que los datos no hayan sido alterados o corrompidos durante el trayecto.
3. **Autenticación:** Verifica rigurosamente la identidad de los extremos de la comunicación (cliente y servidor o gateway-gateway) mediante certificados digitales o claves precompartidas (PSK) [2].

Existen dos topologías predominantes en la industria:

- **Acceso Remoto (Remote Access):** Conecta un dispositivo individual (endpoint) a la red corporativa. Es la base del teletrabajo moderno.
- **Sitio a Sitio (Site-to-Site):** Interconecta redes enteras (ej. Sede Central con Sucursal) de manera transparente para los usuarios finales, utilizando gateways dedicados [3].

2. Algoritmos Criptográficos Implementados

La seguridad de una VPN no reside en el protocolo de transporte per se, sino en la robustez de las primitivas criptográficas que emplea.

2.1. Cifrado Simétrico (Confidencialidad del Payload)

Es utilizado para cifrar el flujo de datos real debido a su eficiencia computacional.

- **AES (Advanced Encryption Standard):** Específicamente en modo **GCM (Galois/Counter Mode)**. Es el estándar industrial actual. Ofrece confidencialidad y autenticación de datos simultánea. Se beneficia de la aceleración por hardware (instrucciones AES-NI) en procesadores modernos [1].
- **ChaCha20:** Un cifrado de flujo moderno desarrollado por Daniel J. Bernstein. A diferencia de AES, ChaCha20 es extremadamente rápido en software, lo que lo hace ideal para dispositivos móviles o IoT que carecen de aceleración de hardware para AES [4].

2.2. Cifrado Asimétrico (Intercambio de Claves)

Se utiliza únicamente durante la fase de negociación (Handshake) para establecer un canal seguro inicial.

- **RSA:** Basado en la dificultad de factorizar grandes números enteros. Requiere claves de gran longitud (2048 o 4096 bits) para ser seguro hoy en día [1].
- **ECDH (Elliptic Curve Diffie-Hellman):** Una variante del protocolo Diffie-Hellman que utiliza la matemática de curvas elípticas. Permite acordar claves simétricas con claves públicas mucho más pequeñas y eficientes que RSA.

2.3. Funciones Hash (Integridad)

- **SHA-2 (Secure Hash Algorithm 2):** En sus variantes de 256 o 512 bits, es el estándar para firmas digitales y verificaciones HMAC en IPSec.
- **Poly1305:** Un generador de código de autenticación de mensajes (MAC) de alta velocidad. Se utiliza casi exclusivamente en conjunto con ChaCha20 (en la suite ChaCha20-Poly1305) dentro del protocolo WireGuard [4].

3. Protocolos Criptográficos de Red

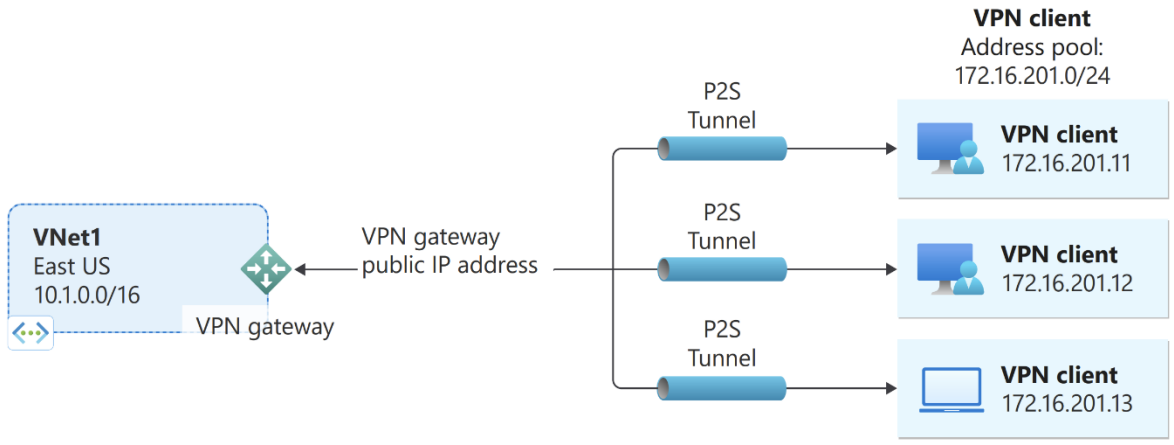
Los algoritmos anteriores se orquestan mediante protocolos de red que operan en distintas capas del modelo OSI.

Protocolo	Capa OSI	Descripción Técnica
IPSec (IKEv2)	Capa 3 (Red)	Es una suite de protocolos, no uno solo. IKEv2 maneja la negociación y movilidad (MOBIKE), mientras que ESP maneja el cifrado de datos. Es el estándar corporativo por excelencia debido a su interoperabilidad [5].
WireGuard	Capa 3 (Red)	Protocolo de nueva generación diseñado con el concepto de "Versionado Criptográfico". No negocia algoritmos (lo que evita ataques de downgrade), sino que usa un conjunto fijo: ChaCha20, Poly1305 y Curve25519. Es considerablemente más ligero (4,000 líneas de código) que IPSec[4].

Protocolo	Capa OSI	Descripción Técnica
OpenVPN	Capa 7 (App)	Opera en espacio de usuario y utiliza la librería OpenSSL. Su mayor ventaja es la flexibilidad: puede operar sobre TCP o UDP y utilizar el puerto 443 para disfrazarse de tráfico HTTPS, evadiendo firewalls estrictos [6].

4. Arquitectura y Diseño Esquemático

El funcionamiento técnico de una VPN se basa en el proceso de **encapsulación**.



4.1. Diseño del Paquete (Modo Túnel IPSec)

En una VPN Site-to-Site, el paquete IP original (privado) es "tragado" por un nuevo paquete. La estructura resultante es:

1. **Nueva Cabecera IP:** Contiene las IPs públicas de los gateways VPN (origen y destino en Internet) [2].
2. **Cabecera ESP:** Contiene información de seguridad (SPI y número de secuencia).
3. **Paquete Original Cifrado:** Todo el datagrama original (IP privada + Payload) se vuelve ilegible.
4. **ESP Trailer/Auth:** Contiene el relleno (padding) y la firma de integridad (ICV).

4.2. Flujo de Establecimiento (Handshake IKEv2)

Para establecer el túnel, se sigue una secuencia lógica descrita en el RFC 7296 [5]:

1. **IKE_SA_INIT:** Los pares intercambian "nonces" y valores Diffie-Hellman. Se crea un canal cifrado, pero aún no autenticado.
2. **IKE_AUTH:** Dentro del canal seguro anterior, los pares intercambian identidades (Certificados o Claves) y negocian los selectores de tráfico.
3. **Creación de Child SA:** Se generan las claves finales para el protocolo ESP.

4. **Rekeying:** Periódicamente, el sistema destruye las claves antiguas y genera nuevas para garantizar Perfect Forward Secrecy (PFS), asegurando que, si una clave futura es comprometida, el tráfico pasado permanezca seguro.

5. Escenarios de Uso Frecuente

1. **Teletrabajo y Acceso Remoto Seguro:**
    - Contexto: Empleados conectándose desde redes Wi-Fi domésticas o cafeterías.
    - Utilidad: Evita el "sniffing" de credenciales corporativas. Se recomienda el uso de Split-Tunneling inverso para cifrar solo el tráfico hacia la empresa, optimizando el ancho de banda [1].
2. **Interconexión de Sedes (Site-to-Site):**
    - Contexto: Una empresa con oficinas en Quito y Guayaquil necesita compartir bases de datos.
    - Utilidad: Reemplaza las costosas líneas dedicadas (MPLS) utilizando Internet como medio de transporte, reduciendo costos operativos drásticamente sin sacrificar la confidencialidad [3].
3. **Ámbito Académico y de Investigación:**
    - Contexto: Estudiantes que requieren acceso a repositorios como IEEE Xplore o JSTOR que validan por IP institucional.
    - Utilidad: Las universidades implementan VPNs (generalmente SSL/TLS) que otorgan al estudiante una IP institucional temporal, permitiendo el acceso a recursos bibliográficos desde casa.

6. Banco de Preguntas

A continuación, se presentan preguntas de reactivo para validar el conocimiento técnico expuesto.

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

Respuesta: c

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
- b) Telnet
- c) RSA
- d) SHA-2
- e) POP3

Respuestas: a, b, d

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

Conceptos:

WireGuard

IKEv2

SSL VPN

PFS

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.

Respuesta: 1-C, 2-A, 3-D, 4-E, 5-B

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

Respuesta: Split-Tunneling

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

- Verdadero
- Falso

Respuesta: Verdadero

7. Referencias Bibliográficas:

[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**.