Seguridad en Redes y Datos

2021

UNIVERSIDAD ORT
Uruguay

Virtual Private Networks

¿Por qué una VPN?

UNIVERSIDAD ORT Uruguay

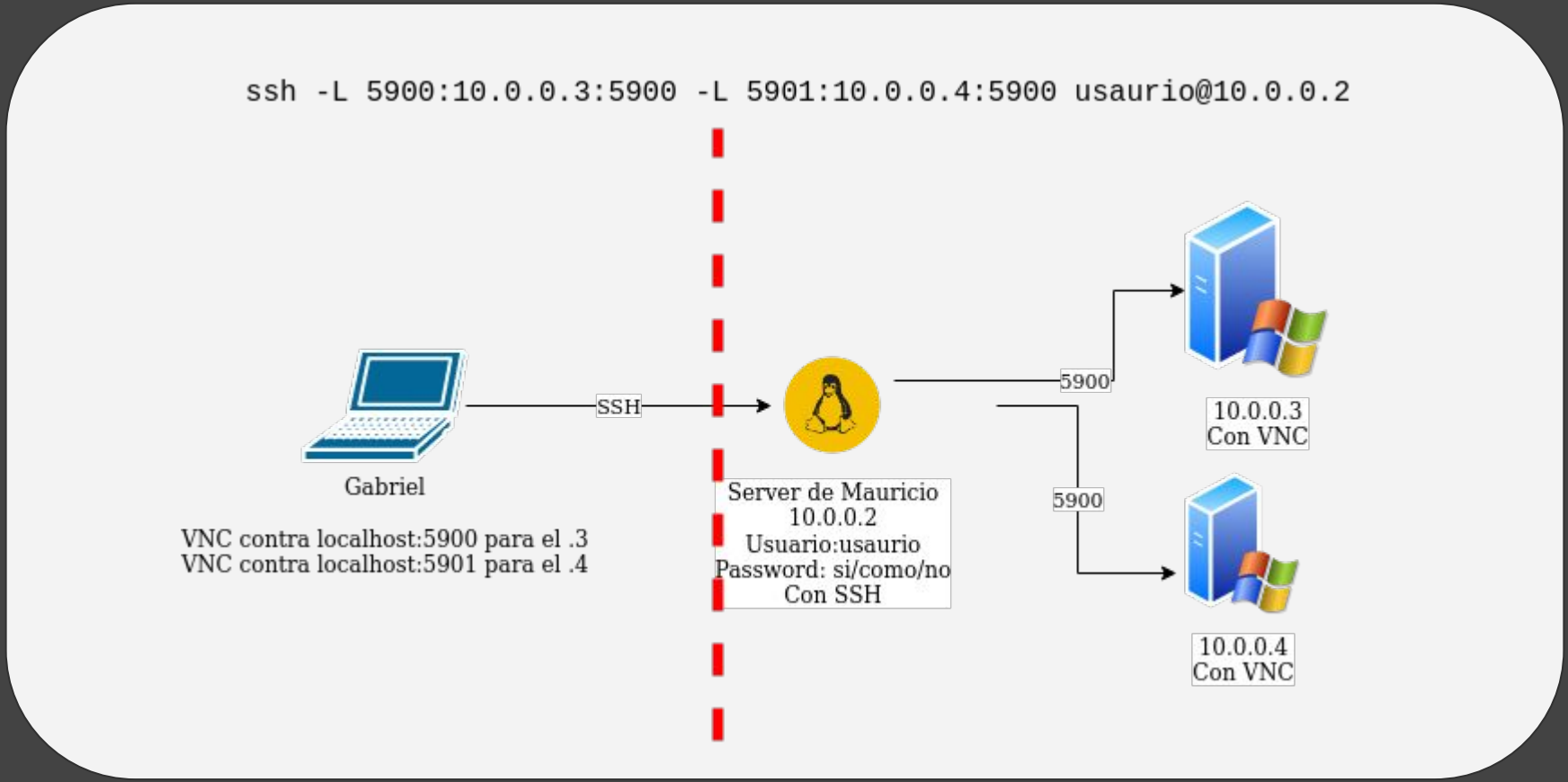
- Canal inseguro
  - Toda transmisión fuera de nuestro dominio de control
  - Toda comunicación con potencial de ser escuchada y/o adulterada
- Cifrado
  - Mecanismo para lograr que una comunicación no sea interpretable
  - Si hablamos de Criptografía entonces también podemos garantizar la integridad
- Redes Privadas Virtuales
  - Implementación tecnológica para permitir una transmisión segura sobre canal inseguro

Tecnologías VPN

UNIVERSIDAD ORT Uruguay

- IPSec
  - Conjunto de protocolos, mandatorio para IPv6 y portado a IPv4
  - IKE/ISAKMP, AH, ESP
  - Robusto, orientado a interconexión de redes
- SSL/TLS
  - Originalmente pensado para transporte web
  - Foco en cliente
  - Fácilmente integrable a otras soluciones
- SSH
  - No se piensa directamente como usable pero lo es
  - Requiere parámetros adicionales (túnel)

Túnel SSH Ejemplo

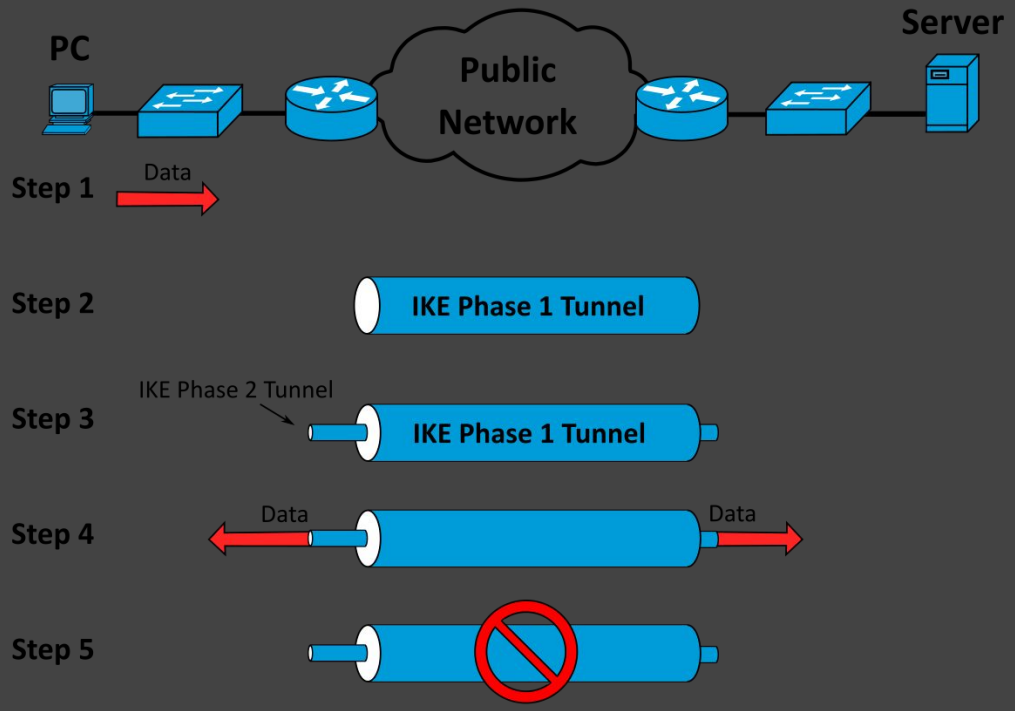


Diferencia IPSec y SSL

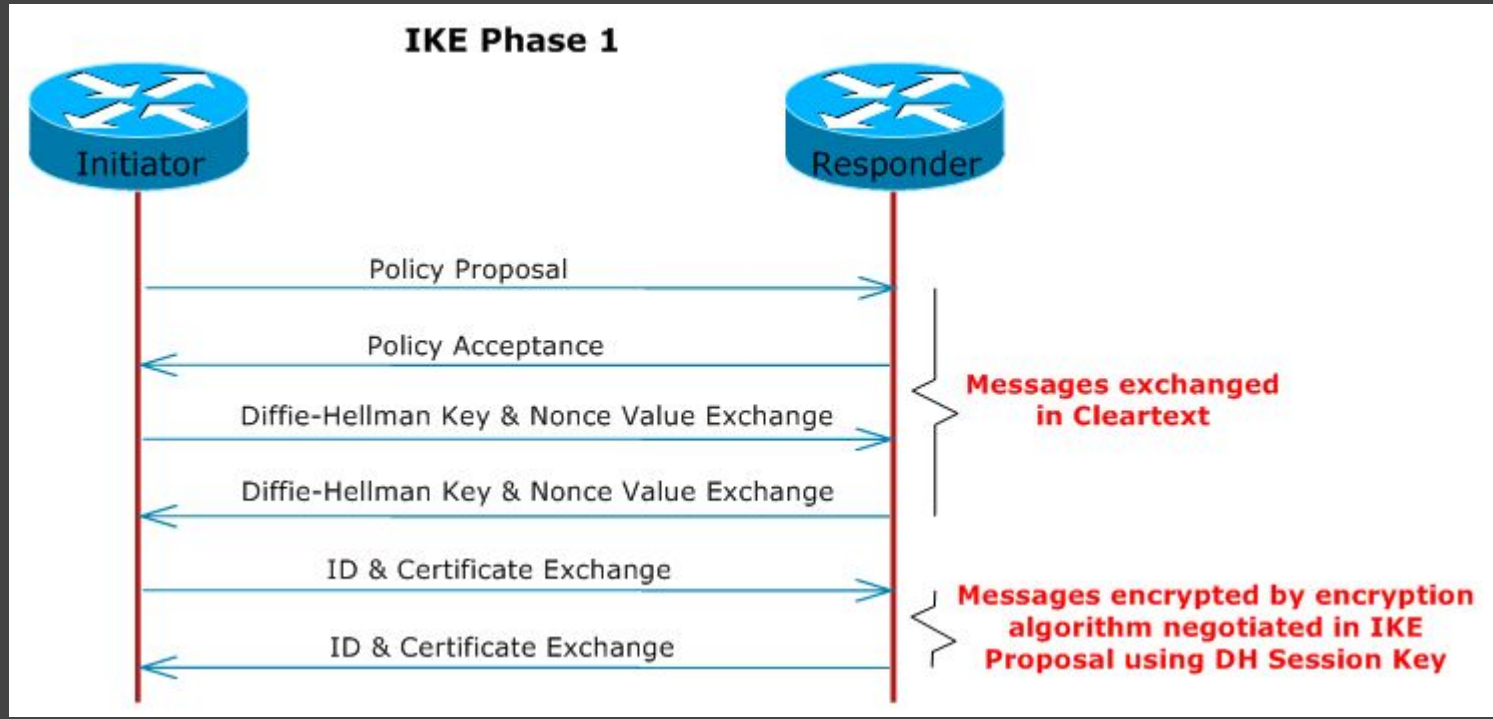
UNIVERSIDAD ORT Uruguay

IPSEC	SSL
Internet protocol security (IPsec) is a set of protocols that provide security for Internet Protocol.	SSL is a secure protocol developed for sending information securely over the Internet.
It Work in Internet Layer of the OSI model.	It Work in Between the transport layer and application layer of the OSI model.
Configuration of IPsec is Complex	Configuration of SSl is Comparatively Simple
IPsec is used to secure a Virtual Private Network.	SSL is used to secure web transactions.
Installation process is Vendor Non-Specific	Installation process is Vendor Specific
Changes are required to OS for implementation. NO Changes are required to application	No changes are required to OS for implementation but Changes are required to application
IPsec resides in operating system space	SSL resides in user space

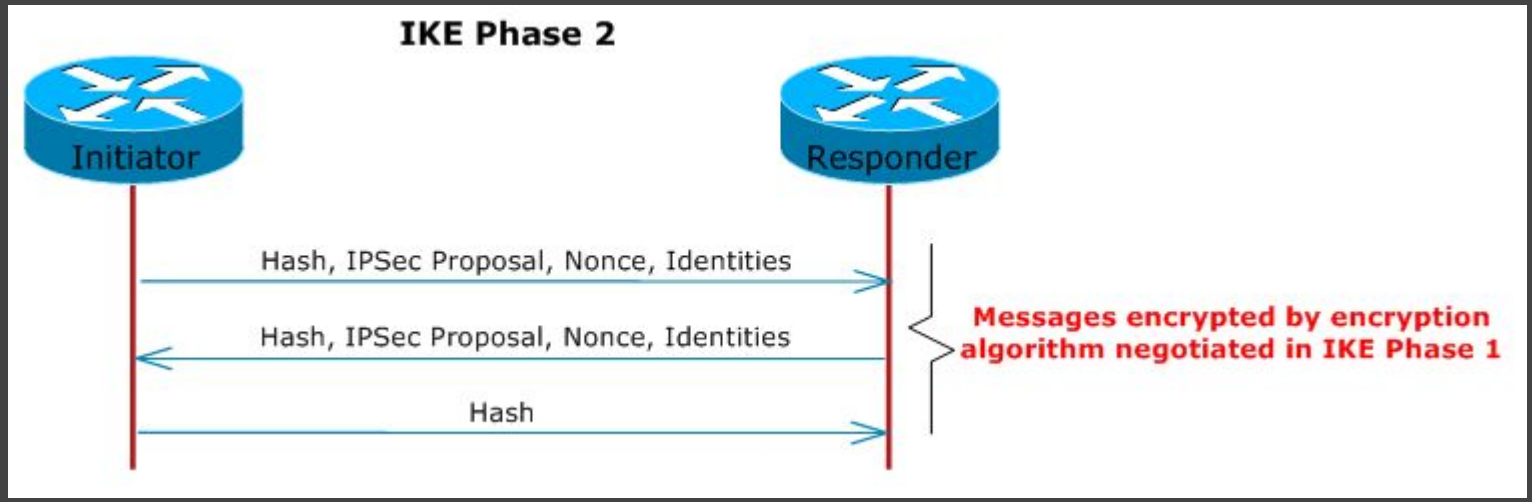
IPSec


PC
Public Network
Server
Step 1
Data
Step 2
IKE Phase 1 Tunnel
Step 3
IKE Phase 2 Tunnel
IKE Phase 1 Tunnel
Step 4
Data
Data
Step 5

IKE Fase 1


IKE Phase 1
Initiator
Responder
Policy Proposal
Policy Acceptance
Diffie-Hellman Key & Nonce Value Exchange
Diffie-Hellman Key & Nonce Value Exchange
ID & Certificate Exchange
ID & Certificate Exchange
Messages exchanged in Cleartext
Messages encrypted by encryption algorithm negotiated in IKE Proposal using DH Session Key

IKE Fase 2


IKE Phase 2
Initiator
Responder
Hash, IPSec Proposal, Nonce, Identities
Hash, IPSec Proposal, Nonce, Identities
Hash
Messages encrypted by encryption algorithm negotiated in IKE Phase 1

IKE

UNIVERSIDAD ORT Uruguay

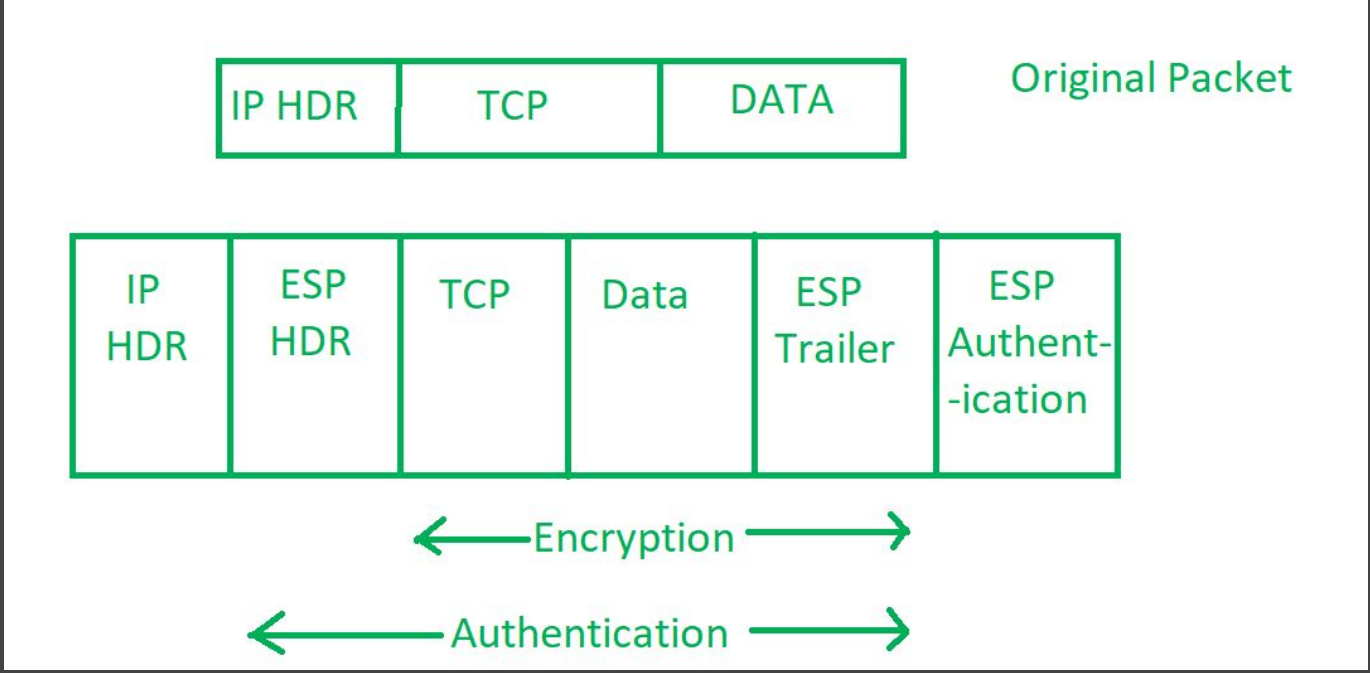
- Modo Principal
  - Tres intercambios
    - Algoritmos IKE
    - Algoritmos DH
    - Identidad
- Modo Agresivo
  - Menos intercambios más compactos
- Modo Rápido
  - Política IPSec
- PFS (Perfect Forward Secrecy)
  - ¿Cómo negociamos nuevas claves?

IPSec Modo Tunnel o Transport

UNIVERSIDAD ORT Uruguay

- Modo Túnel
  - Pensado para red a red
  - El cliente es agnóstico del túnel
  - El paquete original es el payload del paquete IPSec
  - MTU
- Modo Transporte
  - Pensado para clientes
  - Es responsabilidad del cliente encapsular IPSec
  - Usado para conexiones de cliente a red

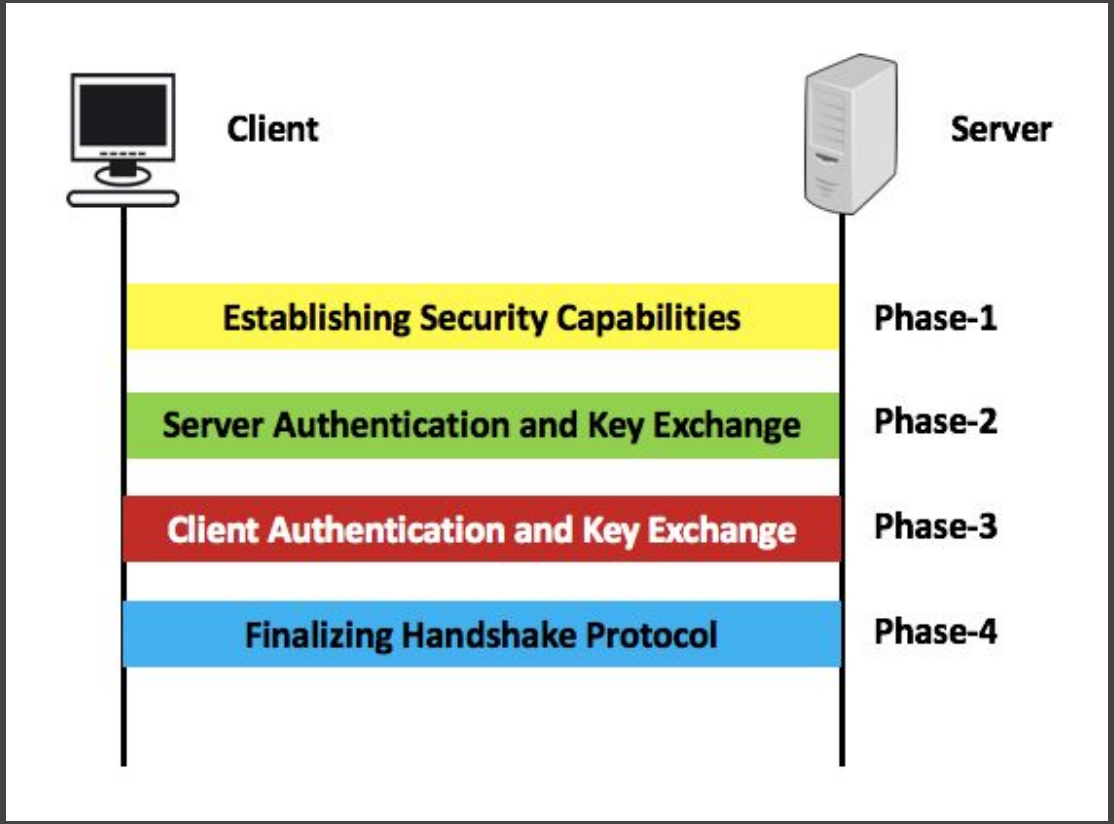
IPSec ESP modo transport



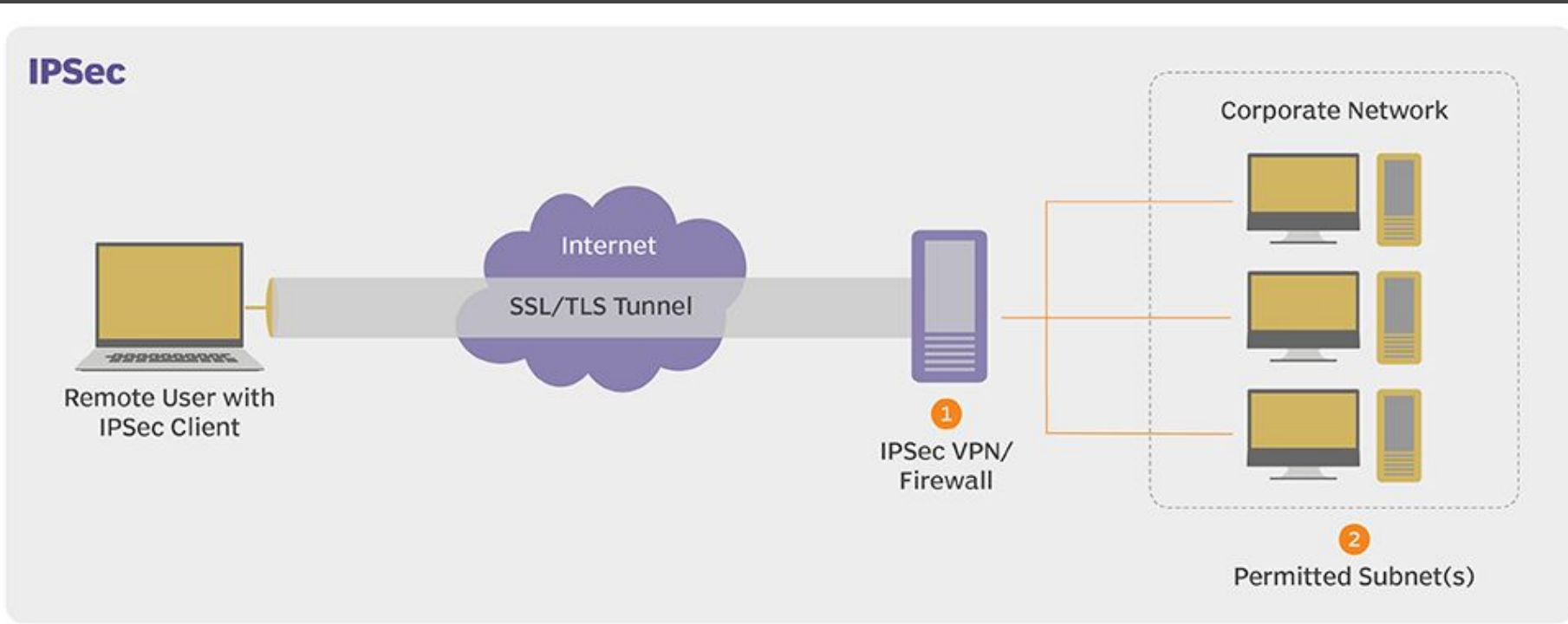
UNIVERSIDAD ORT
Uruguay

SSL VPNs

Protocolo SSL

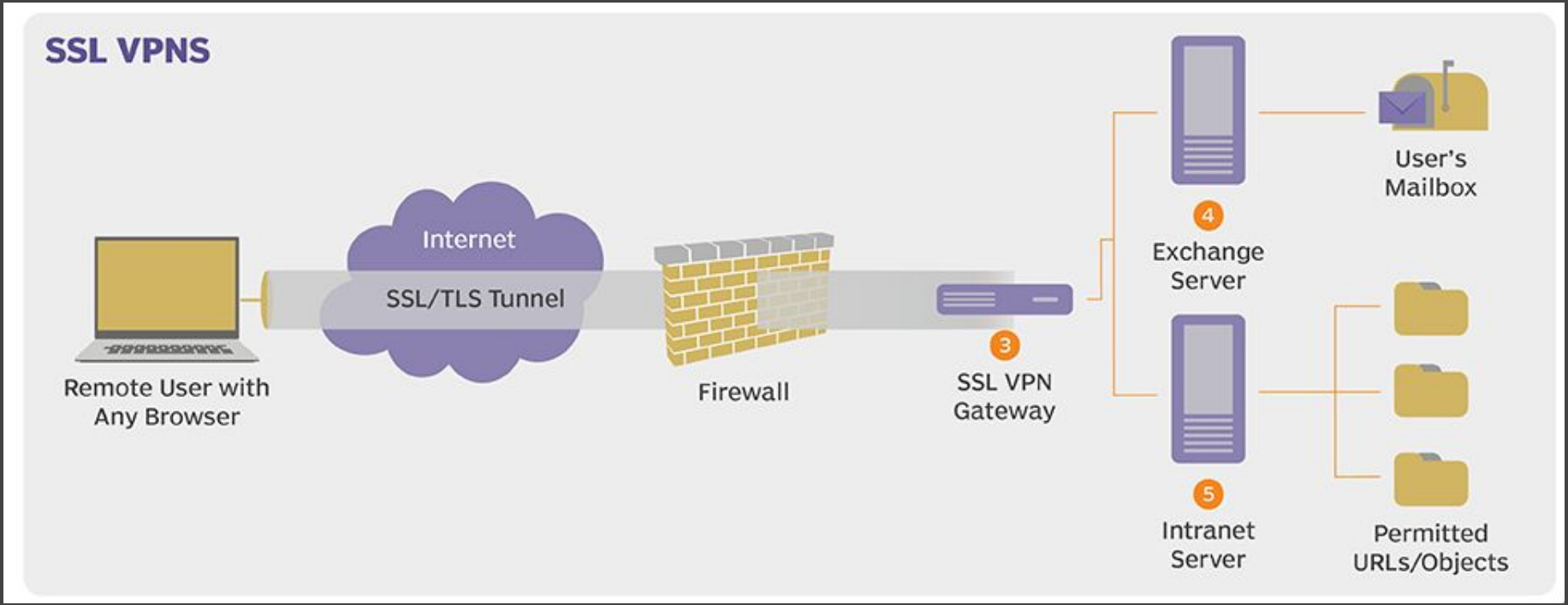


IPsec vs. SSL



https://searchsecurity.techtarget.com/definition/SSL-VPN

IPsec vs. SSL



https://searchsecurity.techtarget.com/definition/SSL-VPN