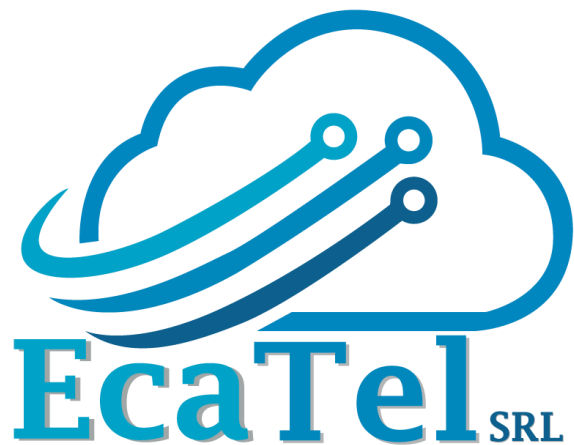




MUM – Chile 2019

How to IPsec

Por: Ing. José Miguel Cabrera
Ecatel SRL



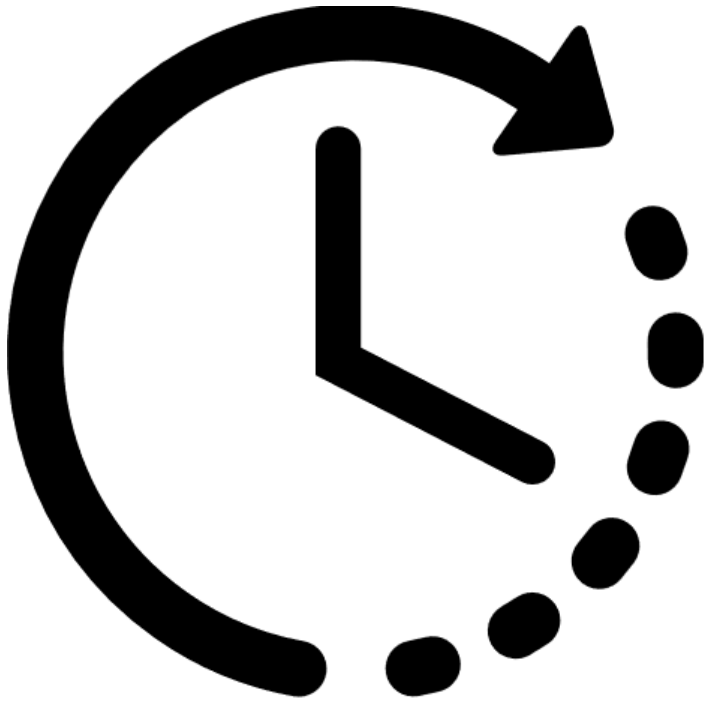
Resumen

Ipsec es el protocolo para VPN considerado más seguro en la actualidad, aprender a implementarlo es indispensable.

Vamos a analizar paso a paso como funciona este protocolo, mostraremos como configurarlo y por su puesto una demostración en vivo de su implementación.



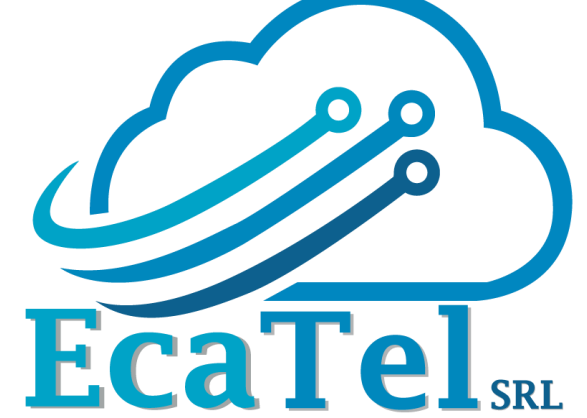
Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de IPsec
- Como implementar IPSec
- Demostración



Acercas de la empresa



Es una empresa que se dedica a la **implementación de proyectos** integrando principalmente equipos de la marca MikroTik, si es necesario combinados con otras marcas.

Brindamos **capacitaciones de MikroTik**.



Contáctenos

info@ecatel.com.bo

+591 776 25848



facebook.com/EcatelSRL



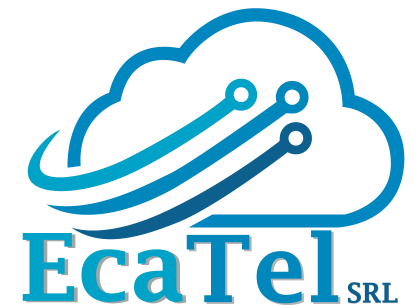
Acerca del disertante

- **Nombre:** Jose Miguel Cabrera Dalence
- **Nacionalidad:** Boliviano 
- **Profesión:** Ing. en Redes y Telecomunicaciones (UTEPSA)
- **Posgrado:** Especialista en Educación Superior Tecnológica (UAGRM)



Experiencia Laboral:

- Gerente de Proyectos en Ecatel SRL (2015 a la fecha)
- Instructor Mikrotik (2015 a la fecha)
- Jefe Nacional de Telecomunicaciones Banco Fassil (2010-2015)
- Docente Universitario en Utepsa y UAGRM (2011-2016).



Acercas del disertante

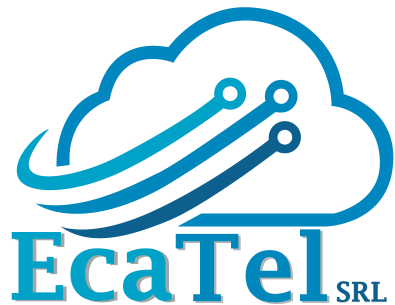
Certificaciones:



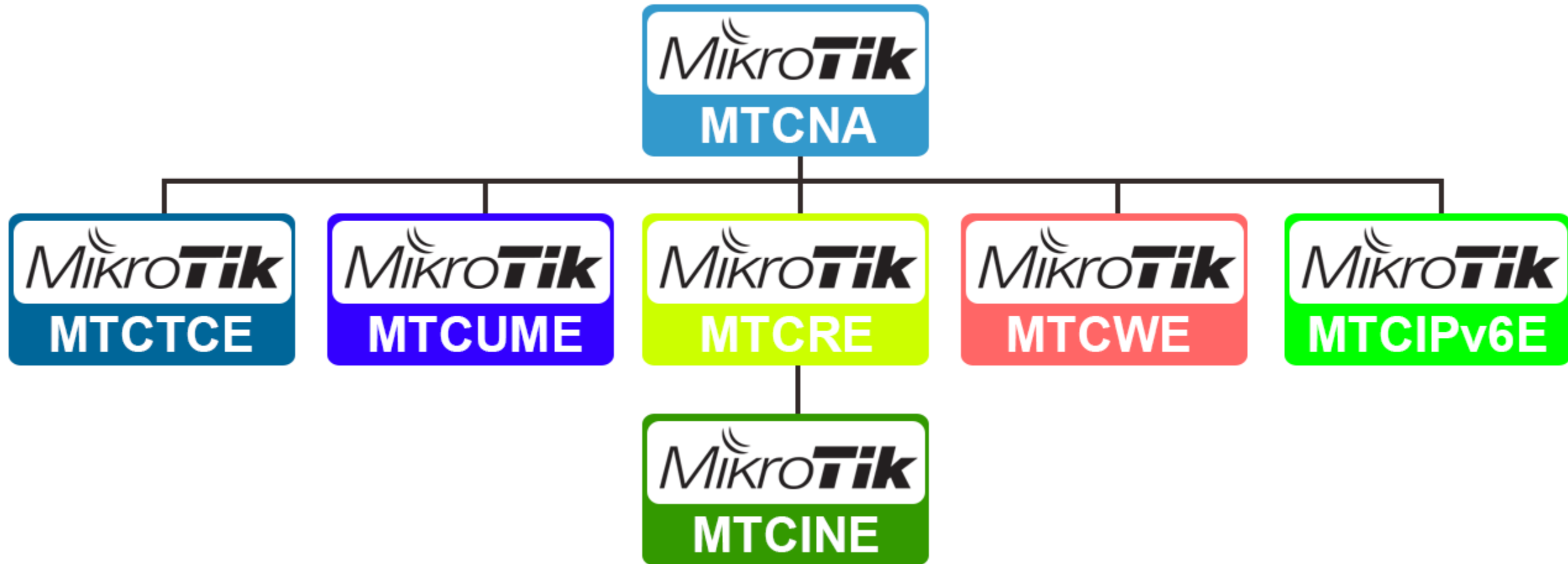
- **Mikrotik:** MTCNA, MTCWE, MTCRE, MTCINE, MTCUME, MTCTE, MTCIPv6E, Trainer
- **Cisco:** CCNP Security, CCNA R&S, CCNA Security

Conferencias y Capacitaciones:

- **Conferencista:** Argentina, Chile, Bolivia, México, Paraguay, Perú y Uruguay.
- **Se capacitó en:** Bolivia, Perú, Ecuador y Estados Unidos
- **Entrenador MikroTik:** Bolivia, Chile, México, Paraguay, Perú y Uruguay



Programa de Certificaciones



Santiago, Chile

CURSOS OFICIALES

MikroTik MTCNA

12, 13 y 14 de Febrero 2019

Desde las 09:00 am - 06:00pm



Santiago, Chile

CURSOS OFICIALES

MTCUME

18 y 19 de Marzo 2019

09:00 am - 06:00pm

MTCTCE

20 y 21 de Marzo 2019

09:00 am - 06:00pm

MTCRE

22 y 23 de Marzo 2019

09:00 am - 06:00pm



MTCNA
Network Associate

MikroTik

Agosto 2018



SISTEK MikroTik - MTCNA
Innovaciones Tecnológicas Unificadas MikroTik Certified Network Associate



MTCNA
Network Associate

MikroTik

Noviembre 2018





Objetivos Del Curso **MTCNA**

- Proporcionar una visión general del software RouterOS y los productos RouterBoard
- Obtener destrezas prácticas en configuración, mantenimiento y resolución de problemas básicos para dispositivos MikroTik RouterOS

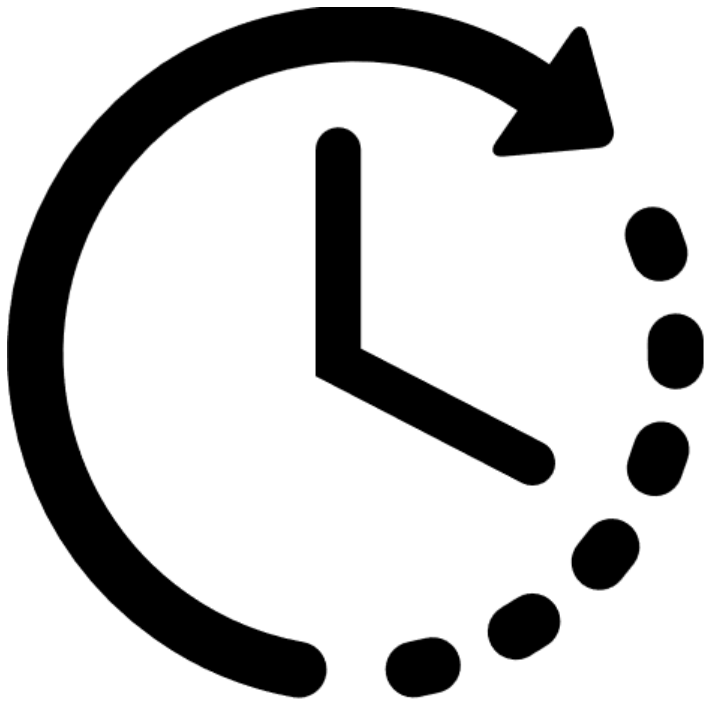


Contenido del **MTCNA**

- Capitulo 1: Introducción
- Capitulo 2: DHCP
- Capitulo 3: Bridging
- Capitulo 4: Routing
- Capitulo 5: Wireless
- Capitulo 6: Firewall
- Capitulo 7: QoS
- Capitulo 8: Tuneles VPN
- Capitulo 9: Herramientas



Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- **Conceptos de IPsec**
 - Como implementar IPsec
 - Demostración





Version del RouterOS

En esta exposición vamos a mostrar comandos y pantallas aplicables en la **versión 6.43 de RouterOS**

En versiones más antiguas o futuras las opciones pueden ser diferentes.



IPSec =



Cebolla



IPSec

- IPSec al igual que una cebolla tienes muchas capas
- Una cebolla te hace llorar, pues IPSec también lo hará
- **¡Pero tranquilo!** No empieces a llorar aún.
- **¡Presta mucha atención!** y lograrás entender IPSec



IPSec

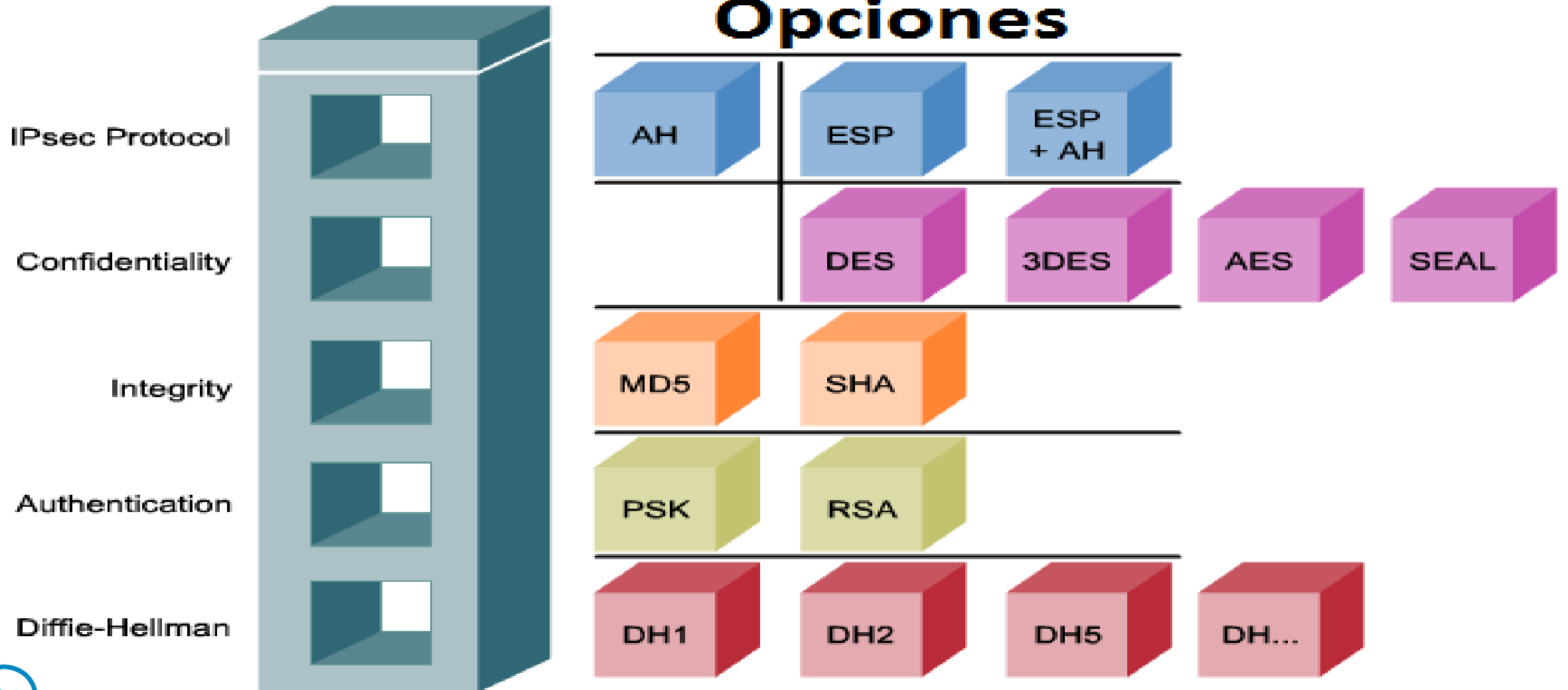
Internet **P**rotocol **S**ecurity

Es un conjunto de protocolos definidos por el IETF (Internet Engineering Task Force) para asegurar el intercambio de paquetes sobre redes IP / IPv6 no protegidas, como Internet



Arquitectura de IPSec

Opciones



Fase 1 (IKE)

Peers + Peer Profiles

Fase 1 (Phase 1): Los nodos se ponen de acuerdo en los algoritmos que usarán en los siguientes mensajes IKE (negocian) y se autenticarán. También se genera e intercambia la llave (key) para todas las SA.



Fase 1 (IKE)

Peers + Peer Profiles

Esta fase debe coincidir con las siguientes configuraciones:

- authentication method
- exchange mode
- hash algorithm
- encryption algorithm
- DH group
- NAT-T
- Lifetime (opcional)
- DPD (opcional)



Fase 2 (IKE)

Policies + Policy Proposals

Fase 2 (Phase 2): Los nodos establecen una o más SA que serán utilizadas por IPsec para cifrar datos. Todas las SA tendrán valores de tiempo de vida, después de lo cual SA se convertirá en inválido.



Fase 2 (IKE)

Policies + Policy Proposals

Esta fase debe coincidir con las siguientes configuraciones:

- Ipsec protocol
- mode (tunnel or transport)
- authentication method
- PFS (DH) group
- lifetime



DH Groups

Diffie-Hellman

El protocolo de intercambio de claves Diffie-Hellman (DH) permite a dos partes sin ningún secreto compartido inicial crear uno de manera segura.

RouterOS soporta: Modular Exponential (MODP) y Elliptic Curve (EC2N), este ultimo conocido tambien como "Oakley".



DH Groups

Diffie-Hellman

| DH Group | Mikrotik DH Group |
|----------|----------------------|
| Group 1 | 768 bit MODP group |
| Group 2 | 1024 bits MODP group |
| Group 5 | 1536 bits MODP group |
| Group 14 | 2048 bits MODP group |
| Group 15 | 3072 bits MODP group |
| Group 16 | 4096 bits MODP group |
| Group 17 | 6144 bits MODP group |



DH Groups

Diffie-Hellman

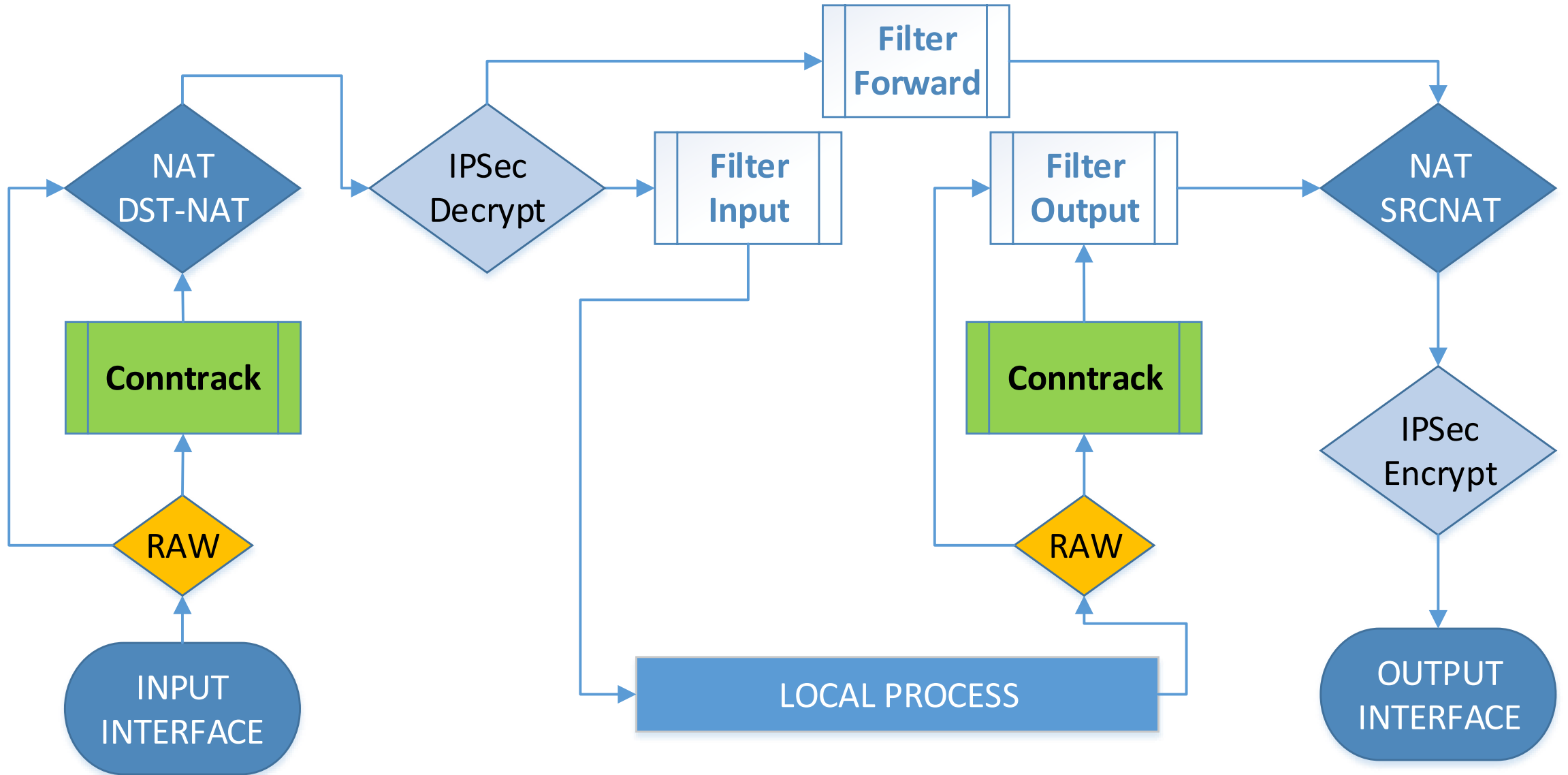
| DH Group | Mikrotik DH Group |
|----------|-------------------------------------|
| Group 3 | EC2N group on GP(2 ¹⁵⁵) |
| Group 4 | EC2N group on GP(2 ¹⁸⁵) |



¡Ya casi terminamos!



IPSec Encryption / Decryption





RECOMENDACIÓN FINAL

IPsec es un estándar, muchos fabricantes lo implementan. Si va a establecer una vpn con otro fabricante tome especial cuidado con:

- En Fase 1: Lifetime y DPD
- En Fase 2: Lifetime y PFS



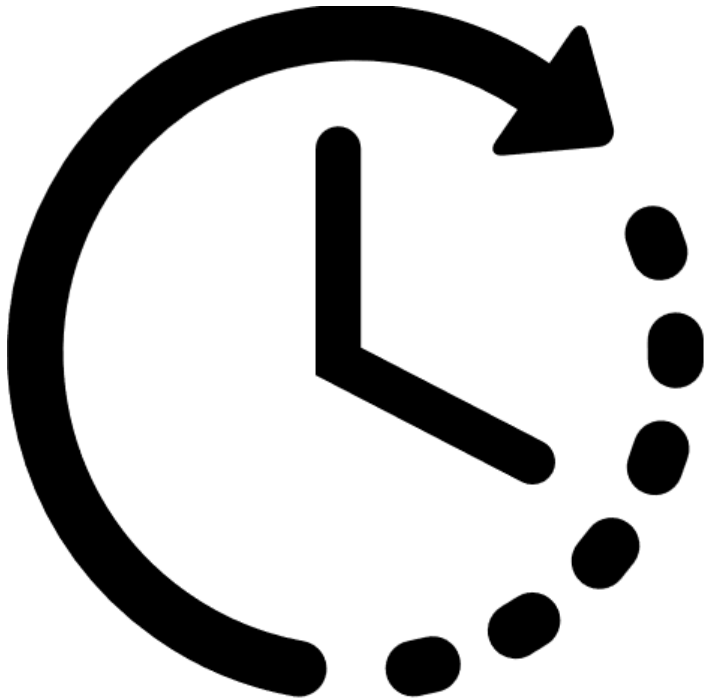


RECOMENDACIÓN FINAL

- Necesitas tener una IP Publica fija en ambos extremos del túnel
- Si no tienes IP Publica en un extremo, puedes utilizar túneles L2tp con IPSec



Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de IPsec
- **Como implementar IPsec**
- Demostración





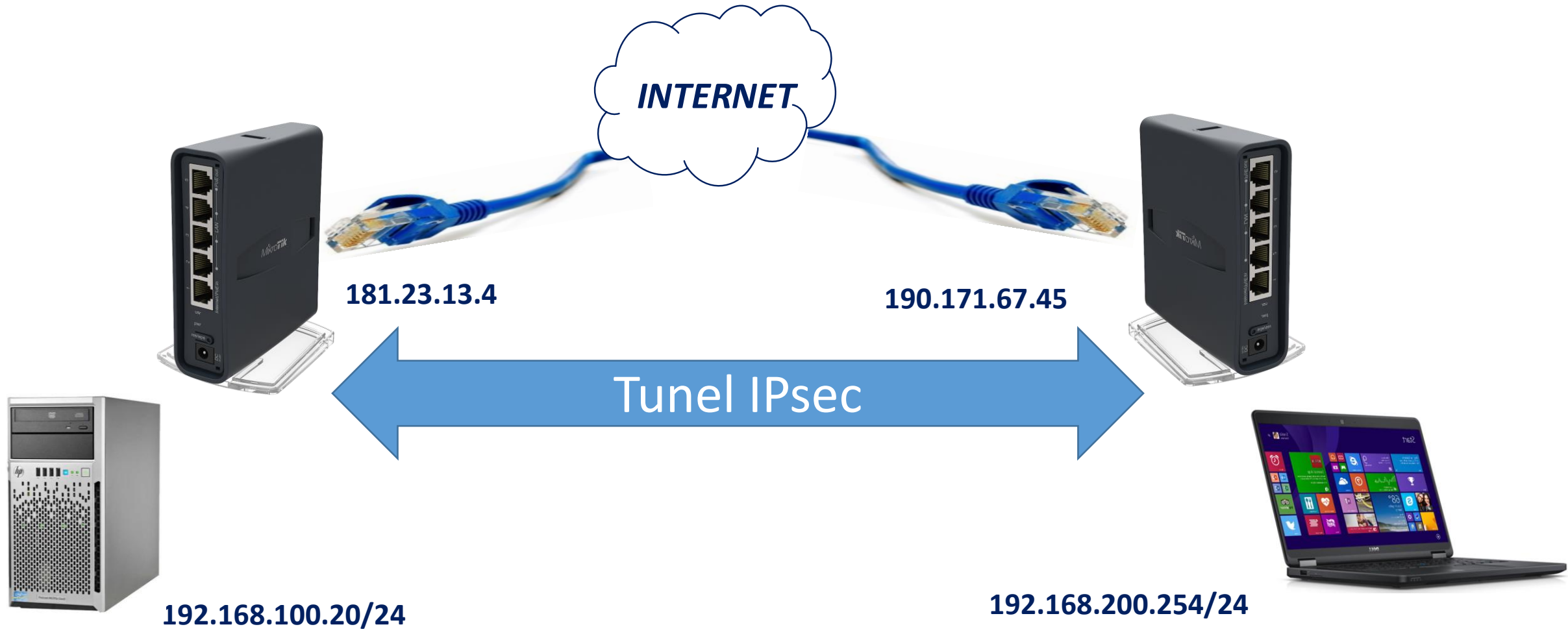
Version del RouterOS

En esta exposición vamos a mostrar comandos y pantallas aplicables en la **versión 6.43 de RouterOS**

En versiones más antiguas o futuras las opciones pueden ser diferentes.



Ipsec - Escenario



Configurar IPSec VPN

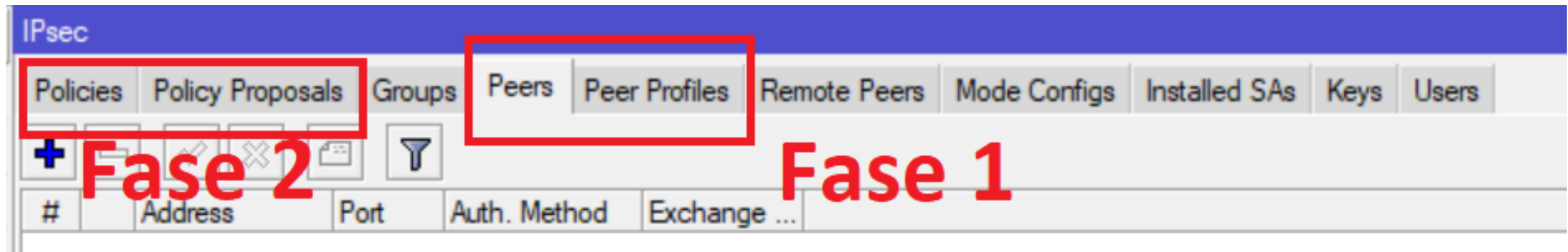
Tareas para configurar IPsec:

- Paso 1: Crear Ipsec Peers (Fase 1)
- Paso 2: Crear Ipsec Policies (Fase 2)
- Paso 3: Ajustar el Proposals si es necesario (Fase 2)
- Paso 4: Verificar No NAT entre Subredes



¿CÓMO CONFIGURO?

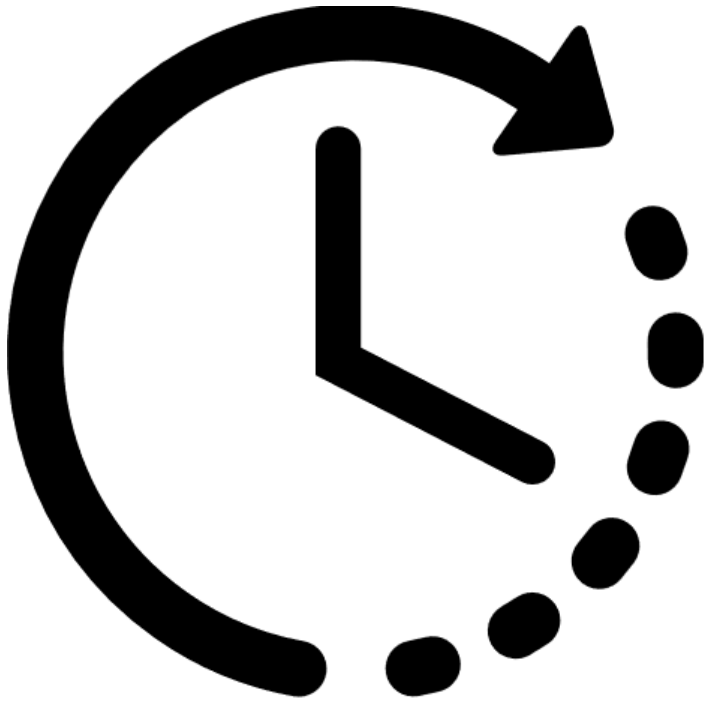
Recuerde la teoría, ahora configure los parámetros donde corresponda.



The screenshot shows the IPsec configuration interface. The menu bar includes: Policies, Policy Proposals, Groups, Peers, Peer Profiles, Remote Peers, Mode Configs, Installed SAs, Keys, and Users. The 'Peers' and 'Peer Profiles' items are highlighted with a red box and labeled 'Fase 1'. Below the menu bar, there are several icons: a plus sign, a minus sign, a checkmark, an 'X', a speech bubble, and a funnel. The plus sign icon is highlighted with a red box and labeled 'Fase 2'. Below the icons, there is a table with columns: #, Address, Port, Auth. Method, and Exchange ...



Scheduler

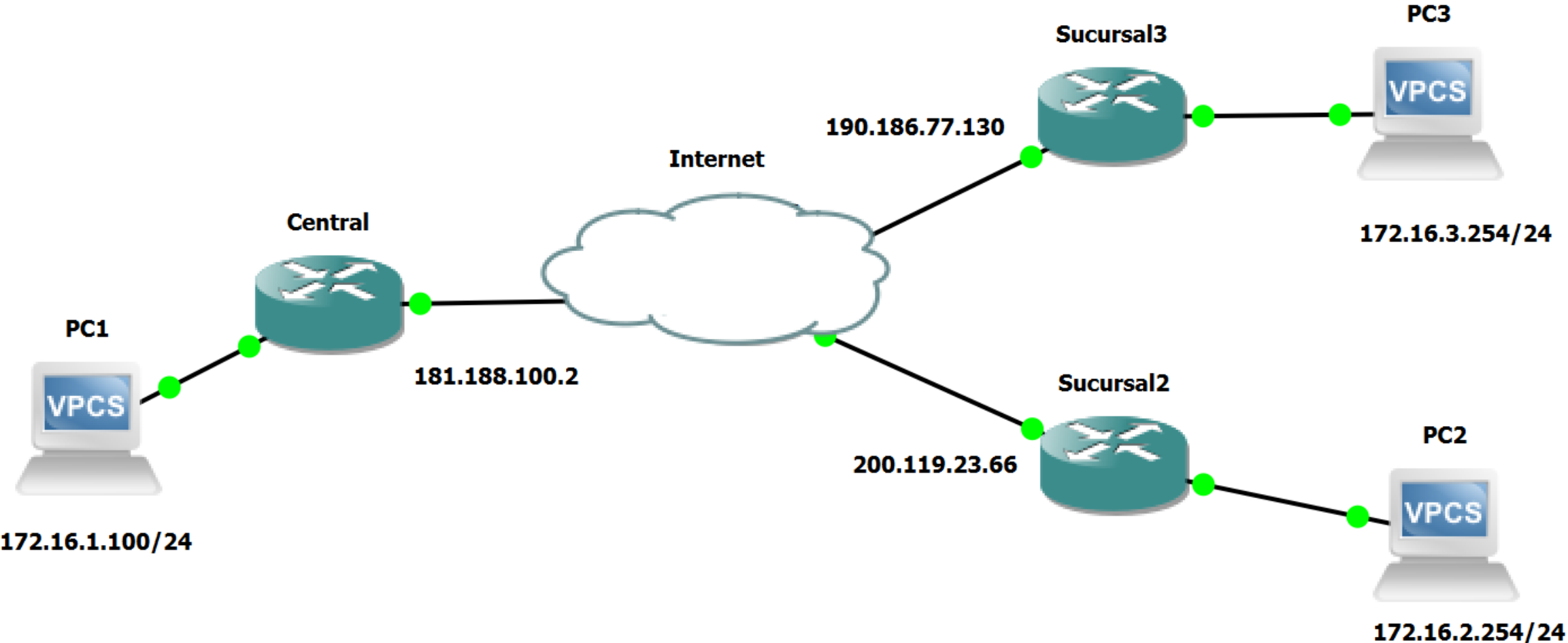


- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de IPsec
- Como implementar IPsec

- **Demostración**

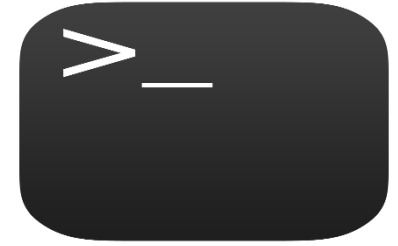


Laboratorio – IPSec Multisite



COMANDOS

Central



```
/ip ipsec peer
```

```
add address=0.0.0.0/0 dh-group=modp1024 secret=123456789
```

```
/ip ipsec policy
```

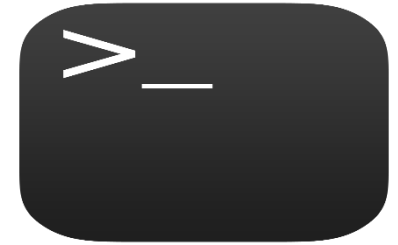
```
add src-address=172.16.0.0/16 dst-address=172.16.3.0/24 \  
sa-src-address=181.188.100.2 sa-dst-address=190.186.77.130 \  
tunnel=yes
```

```
add src-address=172.16.0.0/16 dst-address=172.16.2.0/24 \  
sa-src-address=181.188.100.2 sa-dst-address=200.119.23.66 \  
tunnel=yes
```



COMANDOS

Sucursal 2



```
/ip ipsec peer
```

```
add address=181.188.100.2/32 dh-group=modp1024 secret=123456789
```

```
/ip ipsec policy
```

```
add src-address=172.16.2.0/24 dst-address=172.16.0.0/16 \  
sa-src-address=200.119.23.66 sa-dst-address=181.188.100.2 \  
tunnel=yes
```



COMANDOS

Sucursal 3



```
/ip ipsec peer
```

```
add address=181.188.100.2/32 dh-group=modp1024 secret=123456789
```

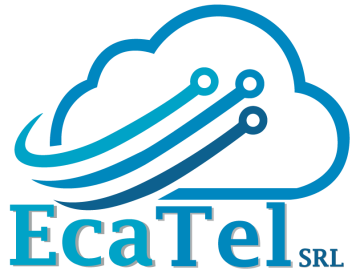
```
/ip ipsec policy
```

```
add src-address=172.16.3.0/24 dst-address=172.16.0.0/16 \  
sa-src-address=190.186.77.130 sa-dst-address=181.188.100.2 \  
tunnel=yes
```





***¡SHOW TIME!
DEMOSTRACION***



¡Gracias!

¿PREGUNTAS?

