VPN IPSec Site-to-Multisite

MUM ARGENTINA, NOVIEMBRE 2015

EMPRESA: WRITEL BOLIVIA SRL

PAÍS: BOLIVIA

EXPOSITOR: ING. JOSE MIGUEL CABRERA / **INSTRUCTOR MIKROTIK #TR0337**

Agenda

La exposición dura en total 45 minutos incluyendo ronda de preguntas

La exposición incluye: teoría, demostración y preguntas.

Acerca del Expositor

Nombre: Jose Miguel Cabrera Dalence

Profesión: Ing. en Redes y Telecomunicaciones (UTEPSA)

PostGrado: Especialista en Educación Superior Tecnológica (UAGRM)

Experiencia:

- Gerente de Proyectos en Writel Bolivia SRL (2015 a la fecha)
- Jefe Nacional de Telecomunicaciones en Banco Fassil (2010-2015)
- Docente Universitario en Utepsa y UAGRM (2011 a la fecha)
- **Instructor Mikrotik #TR0337**
- Certificaciones Mikrotik (MTCNA/MTCWE/MTCRE/Instructor)
- Certificaciones Cisco (CCNP Security/CCNA Routing and Switching)

Acerca de Writel Bolivia SRL

Writel Bolivia SRL es una empresa Boliviana ubicada en Santa Cruz de la Sierra, fue fundada en 2010. Los socios de Writel notan que existe un mercado desatendido en nuevas tecnologías digitales que otros países vecinos ya venían disfrutando, o que no encontraban lo que realmente buscaban dentro del mercado local.

Unidades de negocios:

- Entrenamientos de Mikrotik
- Distribución de equipos
- Proyectos y consultorías

Algunos clientes de Writel Bolivia SRL

Alianzas estratégicas

academy xperts

IMEKA LIMITADA

SUPRA networks

MEGATEL S.R.L.

INTEGRADORES DE SOLUCIONES EN COMUNICACION

Writel Bolivia SRL

Representante legal / CEO : Ing. Jose Alfredo Garcia Davalos jagarcia@writelbolivia.com

Telf. (+591 3)359 6671 (+591) 71092870 (+1) 305 810 8871

Oficina Central: Av. Radial 17 ½ 6to anillo, Santa Cruz Bolivia

Sucursal y Show Room: Comercial Abilcar Oficina N# 1-4. Av. 3er anillo interno entre Radial 19 y Av. Roca y Coronado, Santa Cruz Bolivia

Importaciones: 8333 NW 66 Street, Miami, FL 33166 - US

Ing. Jose Miguel Cabrera

(+591) 710 92871

jmcabrera@writelbolivia.com

WRiTEL Bolivia S.R.L

Conocimientos Previos requeridos

Para un buen entendimiento el publico deberá tener conceptos acerca de:

- Operación básica de RouterOS
- Ruteo
- Sumarizacion
- Subredes
- VPN

¿Qué es una VPN?

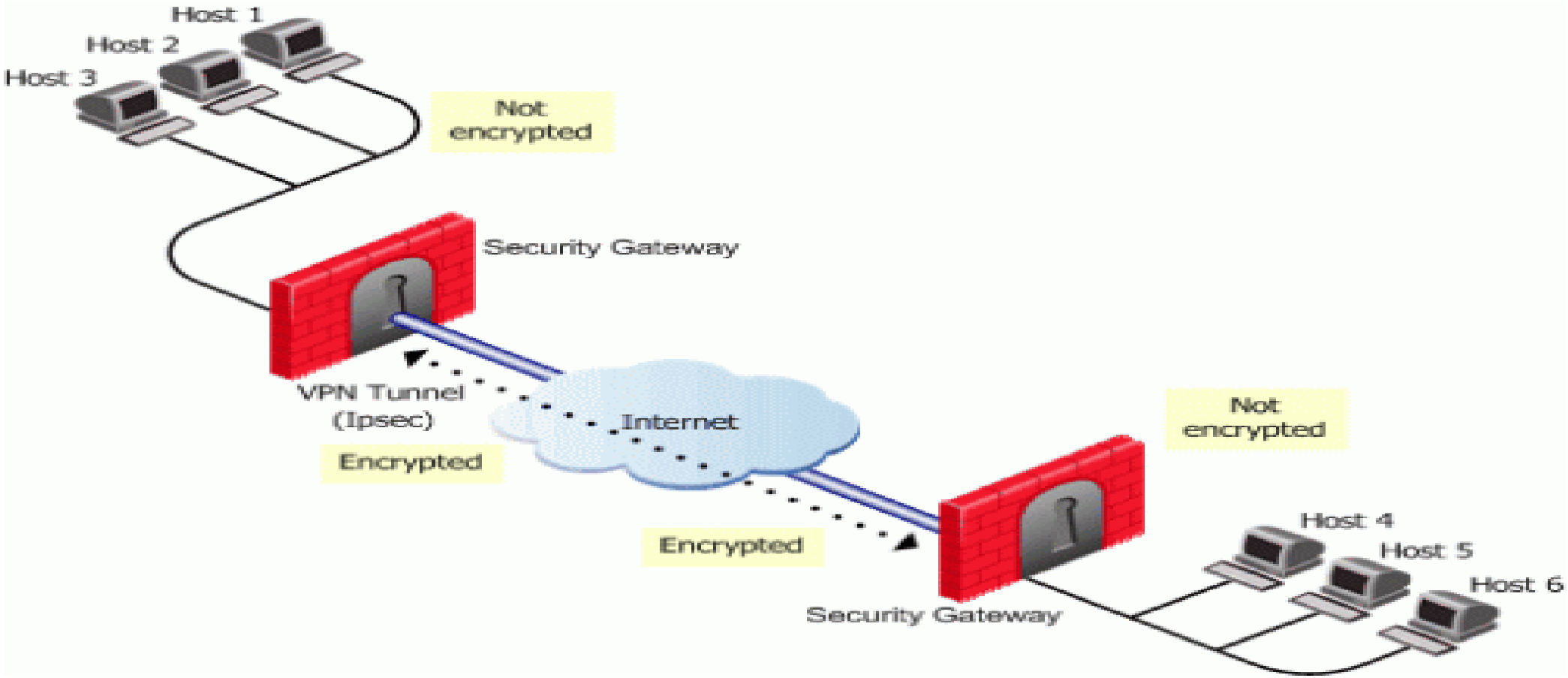
Red Privada Virtual (VPN):

- Virtual: No existe físicamente. Se establece sobre una insfresturctura física publica(Internet) o privada(puede ser wireless).
- Privada: La información se encripta, de manera que solo es visible por los participantes de la VPN.

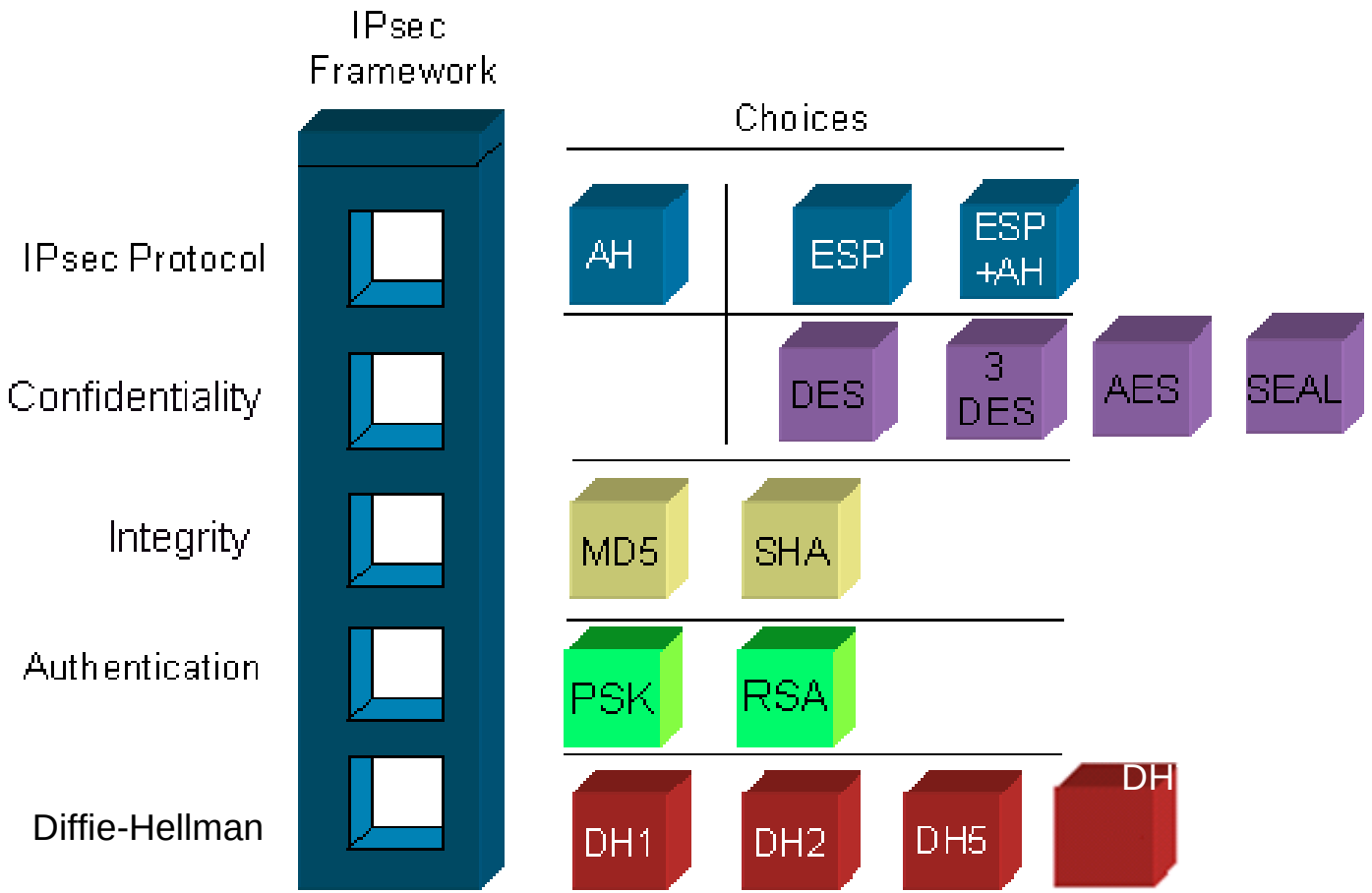
IPSec es un protocolo estandar para establecer VPN. Muchos fabricantes lo soportan.

Es posible establecer IPSec entre marcas distintas siempre y cuando estén correctamente configurados.

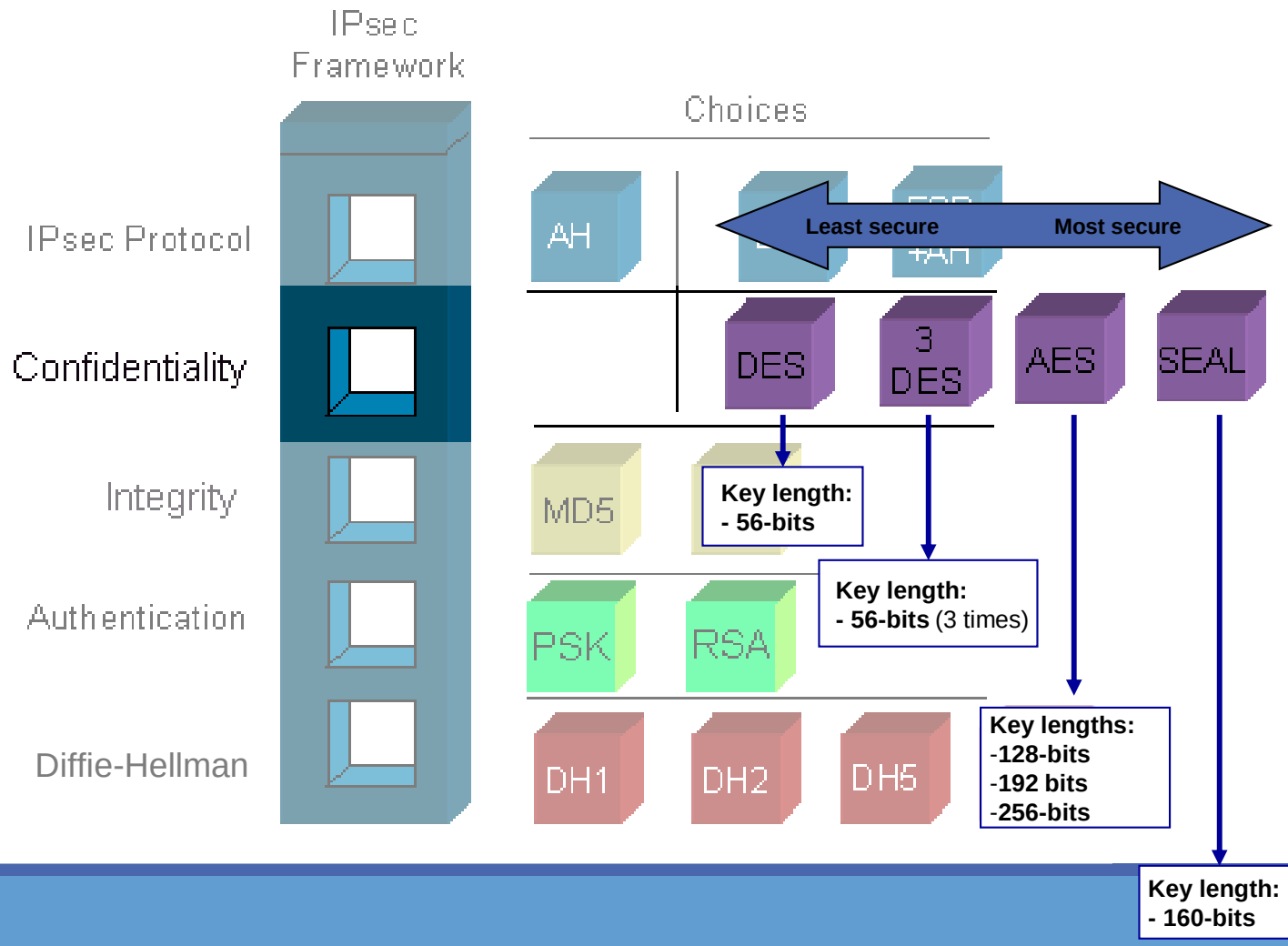
Implementación Típica IPSec VPN



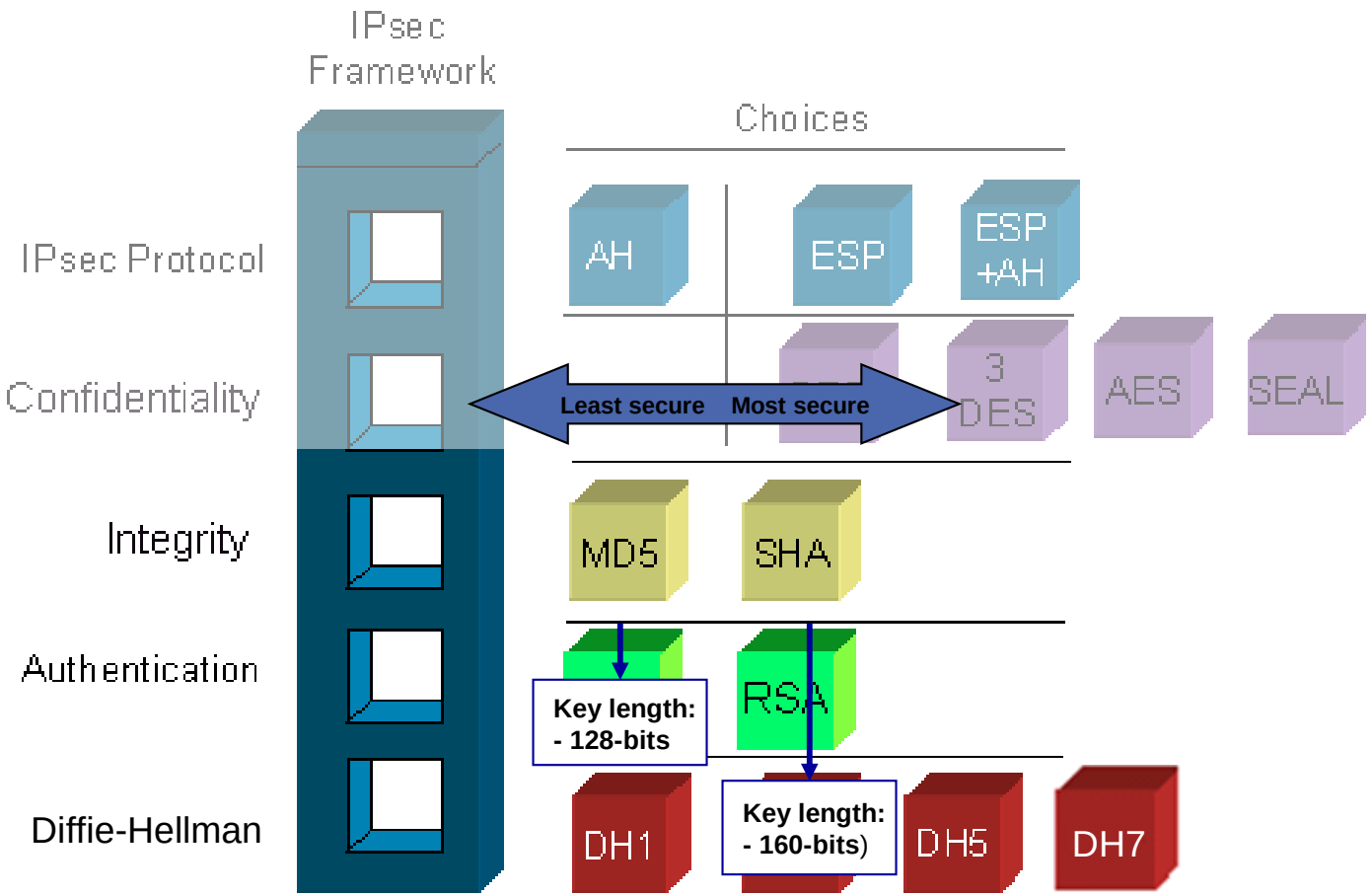
IPSec Framework



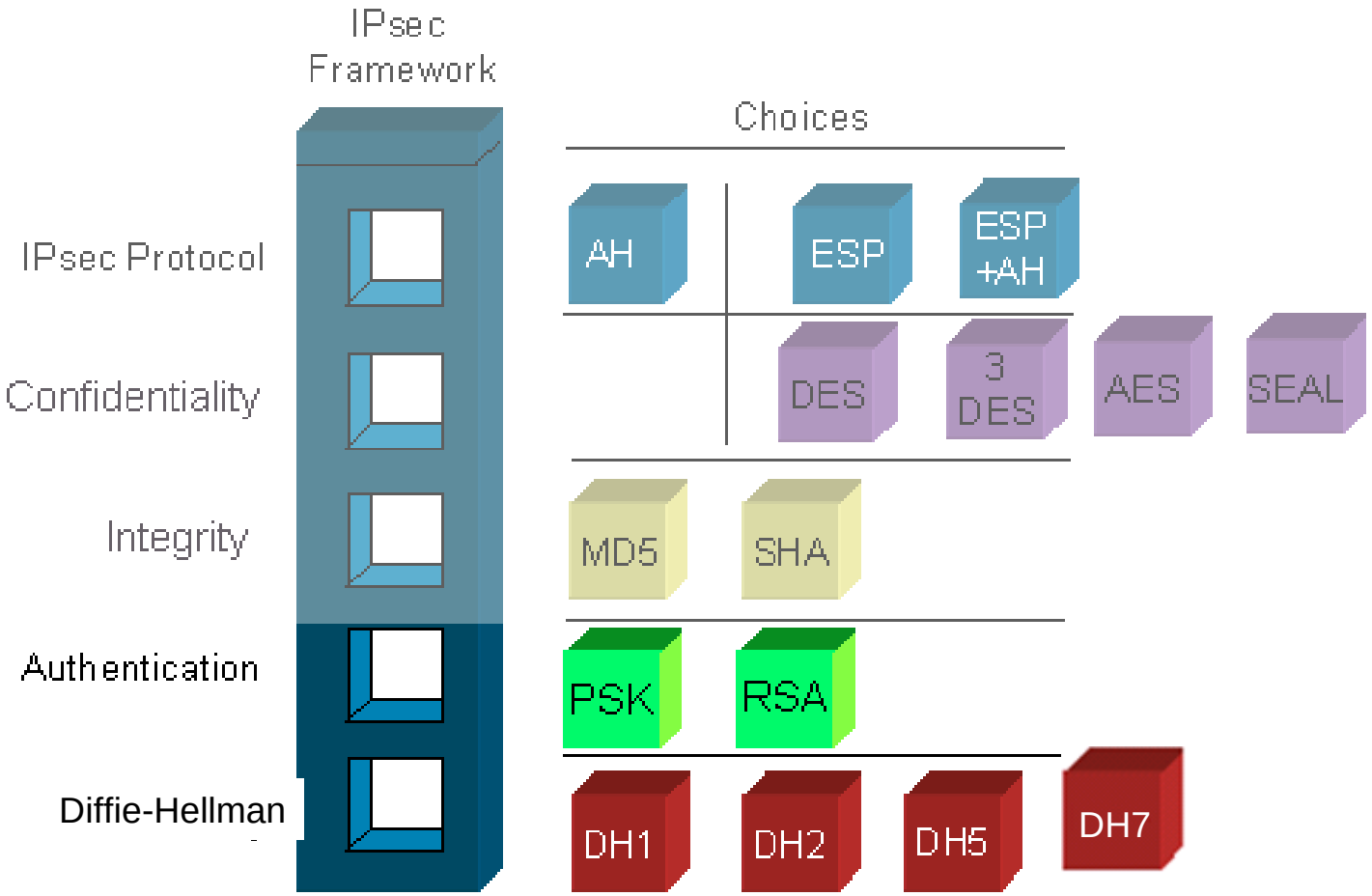
Confidentiality



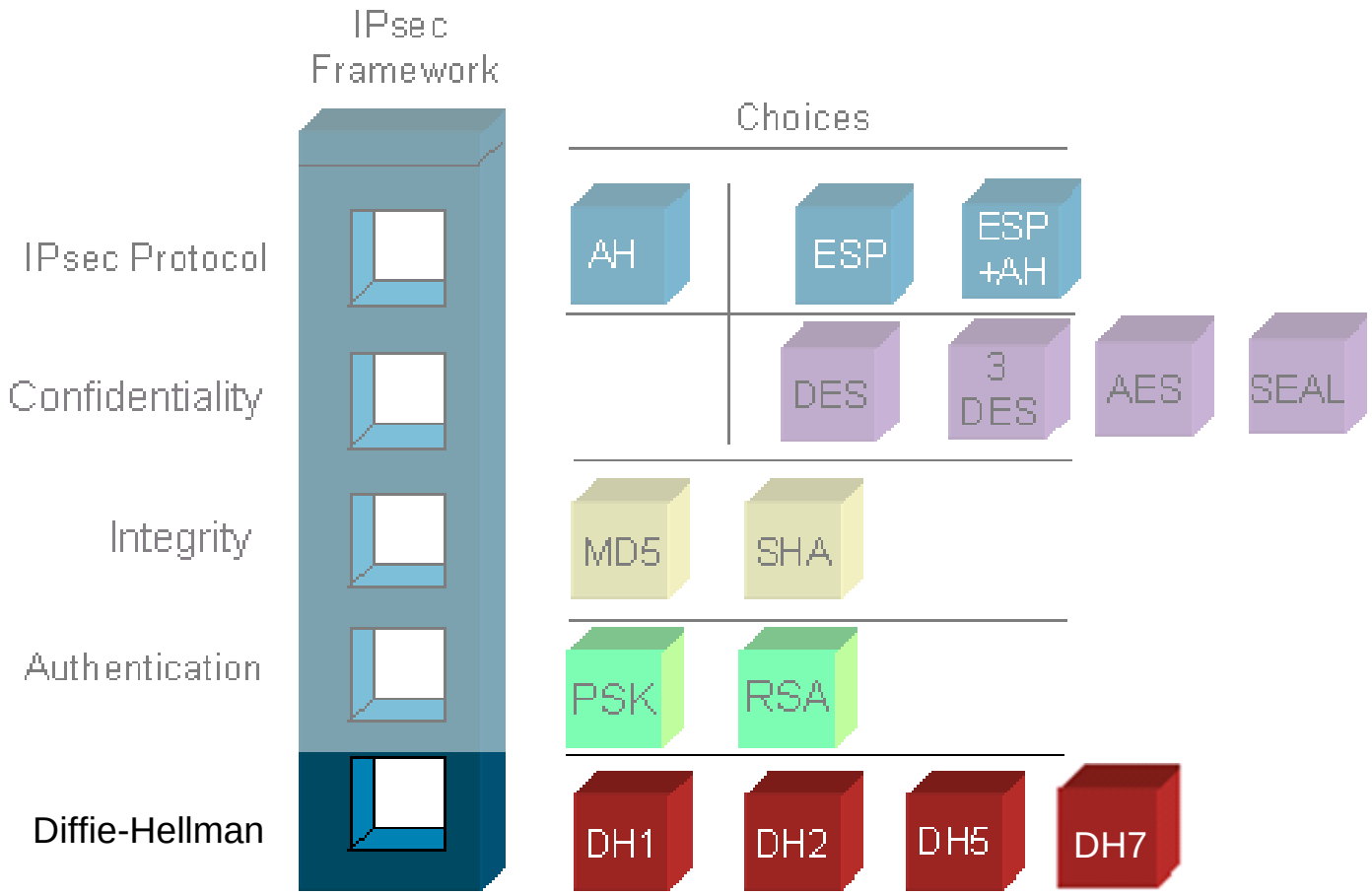
Integrity


IPsec Framework
Choices
IPsec Protocol
Confidentiality
Integrity
Authentication
Diffie-Hellman
AH
ESP
ESP +AH
Least secure
Most secure
3 DES
AES
SEAL
MD5
SHA
Key length: - 128-bits
RSA
DH1
Key length: - 160-bits)
DH5
DH7

Authentication



Secure Key Exchange



VPN Sitio - Multisitio

Normalmente estamos acostumbrados a trabajar IPSec como tuneles punto a punto ó sitio a sitio. Si queremos hacer un enlace entre una Oficina Central y 6 Sucursales, estableces 6 IPSec Policies. Pero esto solo te da comunicación entre la Oficina Central y la Sucursal.

Entre las Sucursales no pueden comunicarse. ¿Cómo lo solucionas? Creas IPSec Policies entre ellos. En 7 router suman 42 IPSec Policies a crearse.

¿Te imaginas hacerlo con 380 sucursales?

Son 144 400 IPSec Policies y ni hablar del mantenimiento

Caso de éxito – Banco en Bolivia

El escenario de implementación es el siguiente:

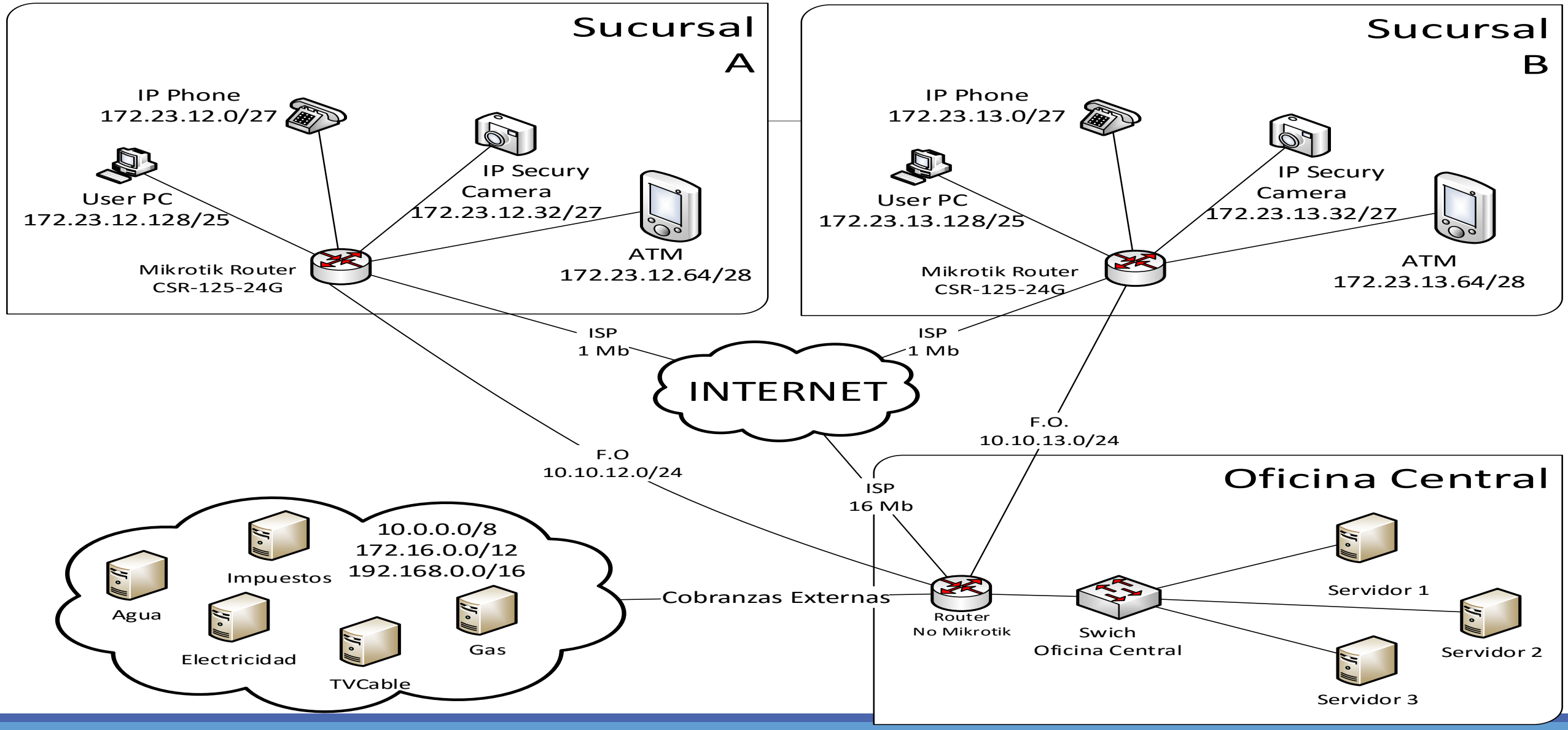
- Se necesita establecer un túnel que alcance **multiples subredes. En distintos segmentos de red**

- Se necesita comunicación entre sucursales para la Telefonia IP, Personal de soporte, Personal de vigilancia, etc.

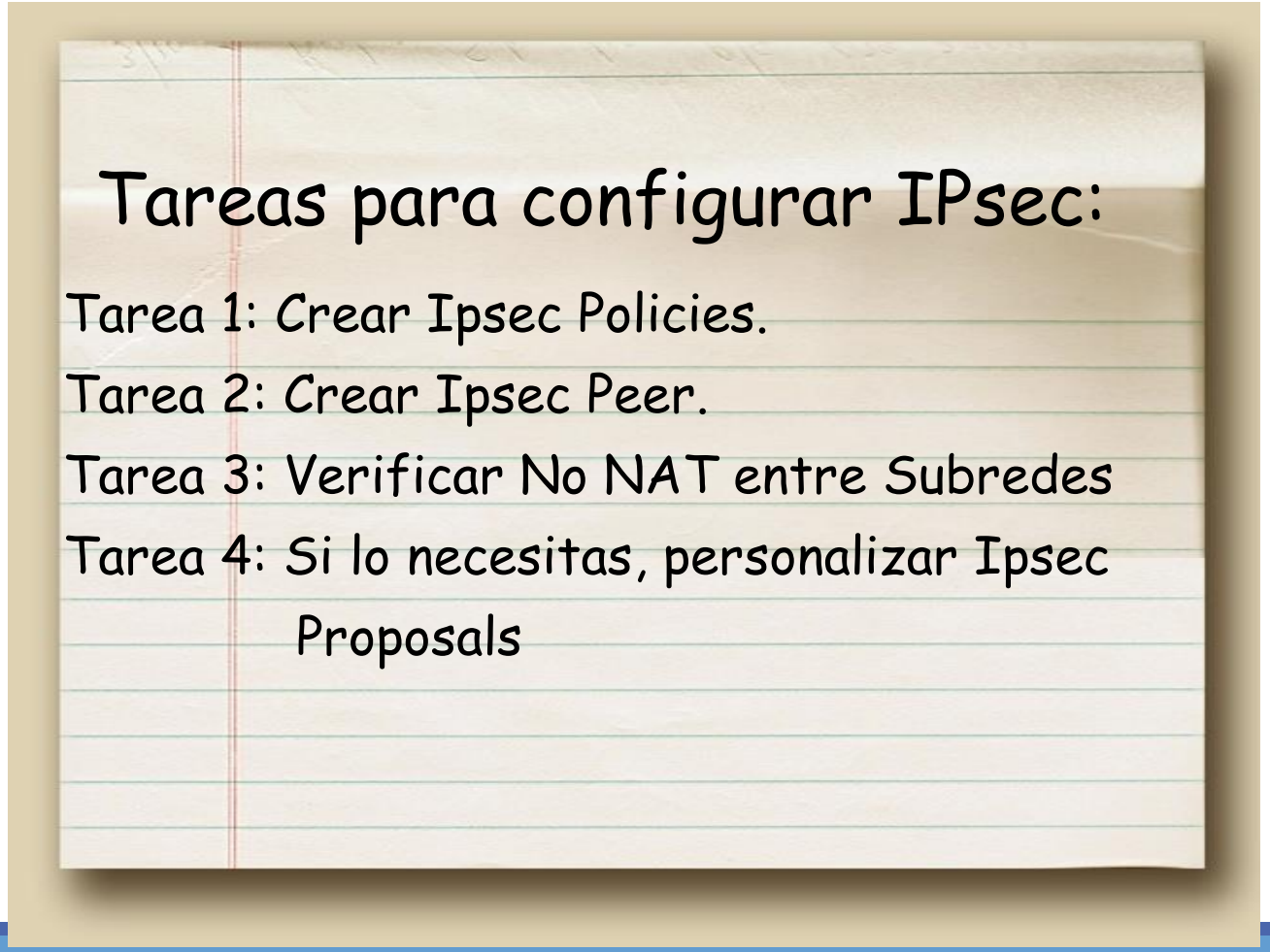
- Cada sucursal tiene una red /24 que es subneteada para diferentes grupos de dispositivos: usuarios, cámaras de vigilancia, cajero automático (ATM) y telefonía IP.

- **Failover, para utilizar un segundo enlace** en caso que el principal falle.

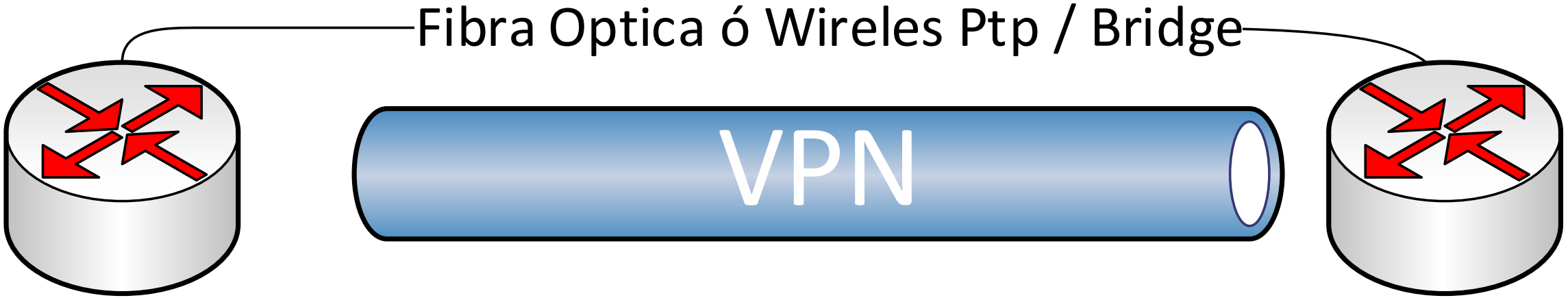
Esquema de conexión



Configurar IPSec VPN



Ejemplo Sencillo



CENTRAL
WAN: 10.10.12.1/24
LAN: 172.23.0.0/24

Sucursal A
WAN: 10.10.12.12/24
LAN: 172.23.12.0/24

Creando IPSec Policie

Router Central

```
/ip ipsec policy
set 0 disabled=yes
add src-address=172.23.0.0/24 dst-address=172.23.12.0/24 \
    sa-src-address=10.10.12.1 sa-dst-address=10.10.12.12 \
    tunnel=yes
```

Router Sucursal A

```
/ip ipsec policy
set 0 disabled=yes
add src-address=172.23.12.0/24 dst-address=172.23.0.0/24 \
    sa-src-address=10.10.12.12 sa-dst-address=10.10.12.1 \
    tunnel=yes
```

Creando IPSec Peer

Router Central

```
/ip ipsec peer
add address=10.10.12.12/32 nat-traversal=no secret=Pass123**
```

Router Sucursal A

```
/ip ipsec peer
add address=10.10.12.1/32 nat-traversal=no secret=Pass123**
```

Creando una regla de NO NAT

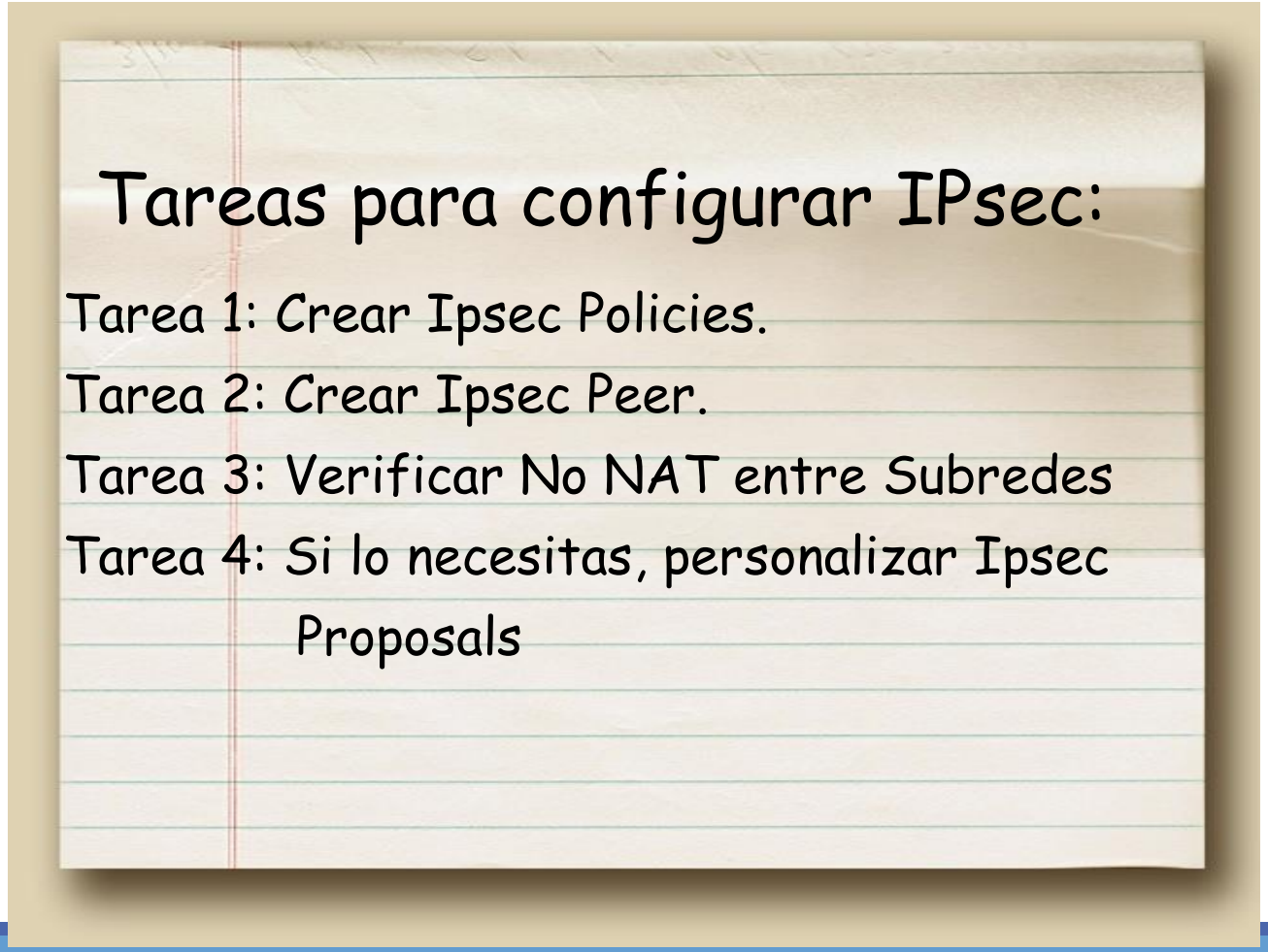
Router Central

```
/ip firewall nat
add action=accept chain=srcnat \
    src-address=172.23.0.0/24 dst-address=172.23.12.0/24
```

Router Sucursal

```
/ip firewall nat
add action=accept chain=srcnat \
    src-address=172.23.12.0/24 dst-address=172.23.0.0/24
```

Repaso

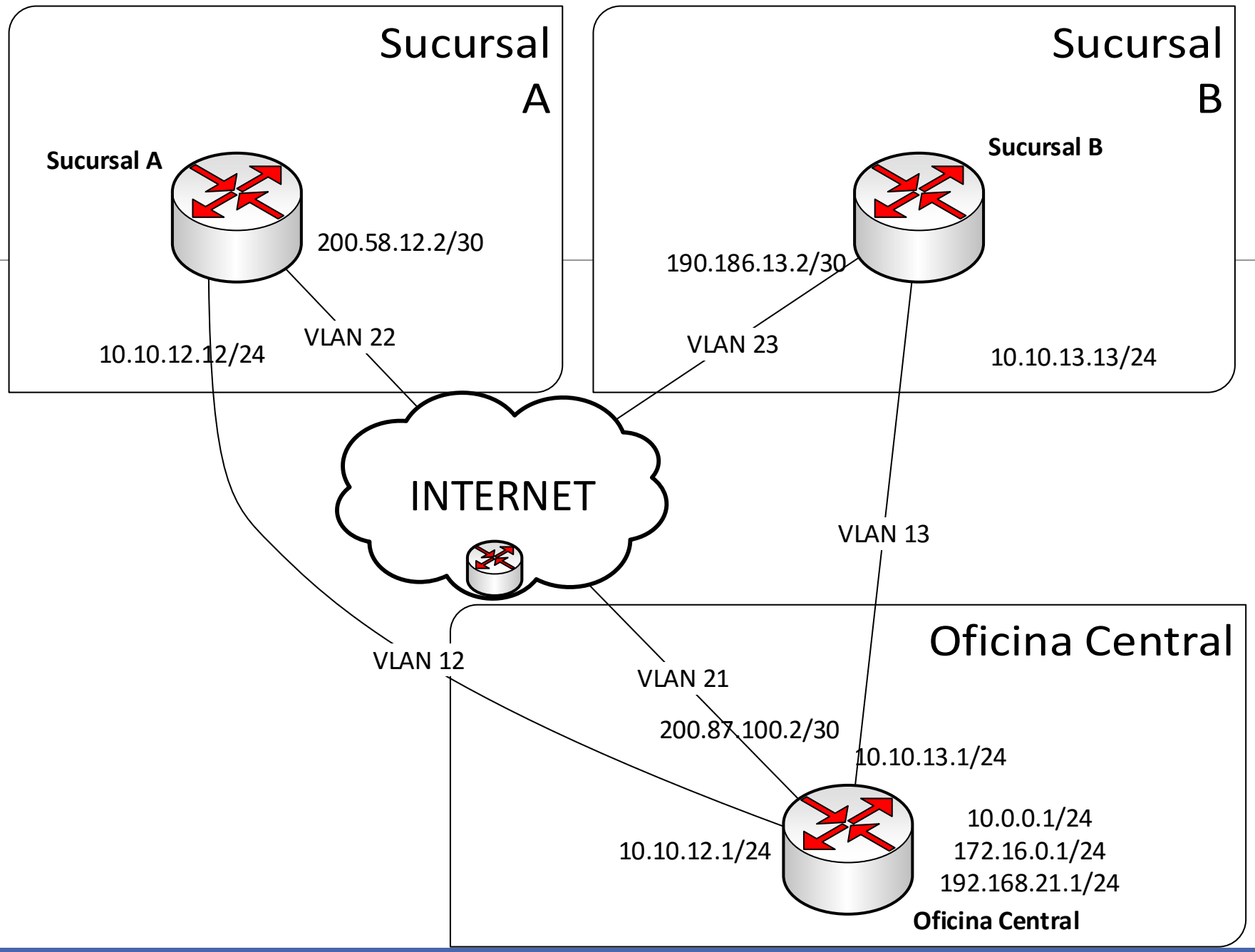

Tareas para configurar IPsec:
Tarea 1: Crear Ipsec Policies.
Tarea 2: Crear Ipsec Peer.
Tarea 3: Verificar No NAT entre Subredes
Tarea 4: Si lo necesitas, personalizar Ipsec
Proposals

Failover IPSec

Utilizando /tool netwatch

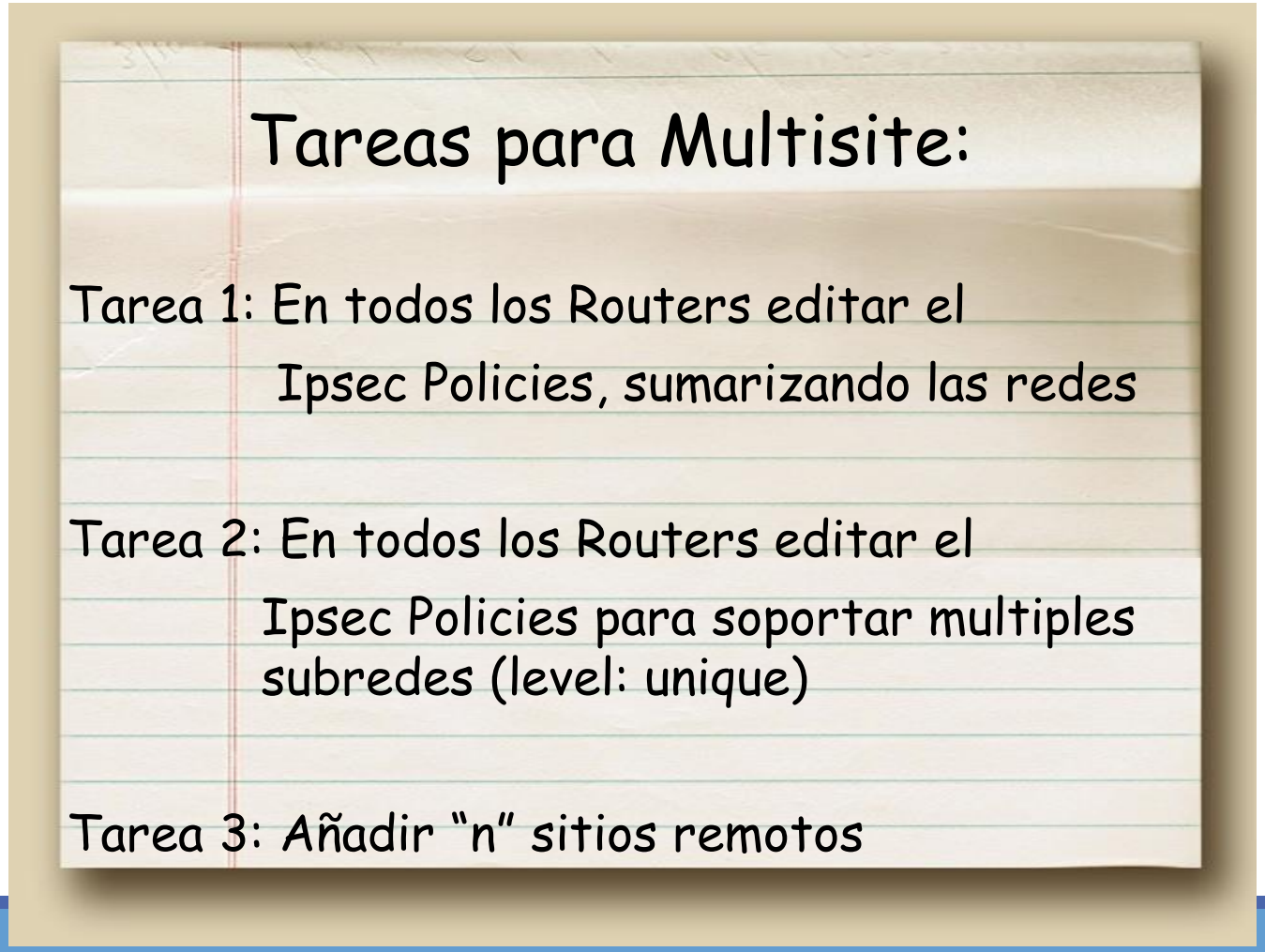
Podemos hacer que ciertos policies del IPSec se habiliten o deshabiliten, además de habilitar y deshabilitar Ipsec Peer. Un ejemplo es el siguiente:

```
/tool netwatch
add host=10.10.12.1 interval=20s \
down-script="ip ipsec policy disable numbers=1\r\
    \nip ipsec policy disable numbers=2\r\
    \nip ipsec policy disable numbers=3\r\
    \nip ipsec peer disable numbers=0\r\
    \n:delay 3\r\
    \nip ipsec policy enable numbers=4\r\
    \nip ipsec policy enable numbers=5\r\
    \nip ipsec policy enable numbers=6\r\
    \nip ipsec peer enable numbers=1" \
up-script="ip ipsec policy disable numbers=4\r\
    \nip ipsec policy disable numbers=5\r\
    \nip ipsec policy disable numbers=6\r\
    \nip ipsec peer disable numbers=1\r\
    \n:delay 3\r\
    \nip ipsec policy enable numbers=1\r\
    \nip ipsec policy enable numbers=2\r\
    \nip ipsec policy enable numbers=3\r\
    \nip ipsec peer enable numbers=0"
```



Esquema de conexión - Demostración

Tareas para Multisite



Demostración

¿Preguntas?

GRACIAS POR SU ATENCION

Writel Bolivia SRL

Representante legal / CEO : Ing. Jose Alfredo Garcia Davalos jagarcia@writelbolivia.com

Telf. (+591 3)359 6671 (+591) 71092870 (+1) 305 810 8871

Oficina Central: Av. Radial 17 ½ 6to anillo, Santa Cruz Bolivia

Sucursal y Show Room: Comercial Abilcar Oficina N# 1-4. Av. 3er anillo interno entre Radial 19 y Av. Roca y Coronado, Santa Cruz Bolivia

Importaciones: 8333 NW 66 Street, Miami, FL 33166 - US

Ing. Jose Miguel Cabrera / Instructor Mikrotik #TR0337

(+591) 710 92871

jmcabrera@writelbolivia.com

WRiTEL Bolivia S.R.L

ANEXOS – EXPORT DE DEMOSTRACION

Si quieres ver el archivo export de los routers de la demostración

http://notepad.cc/share/JDa0EVTAvA