Richart Rojas

INOVA Networks

Ecuador
2013

MUM

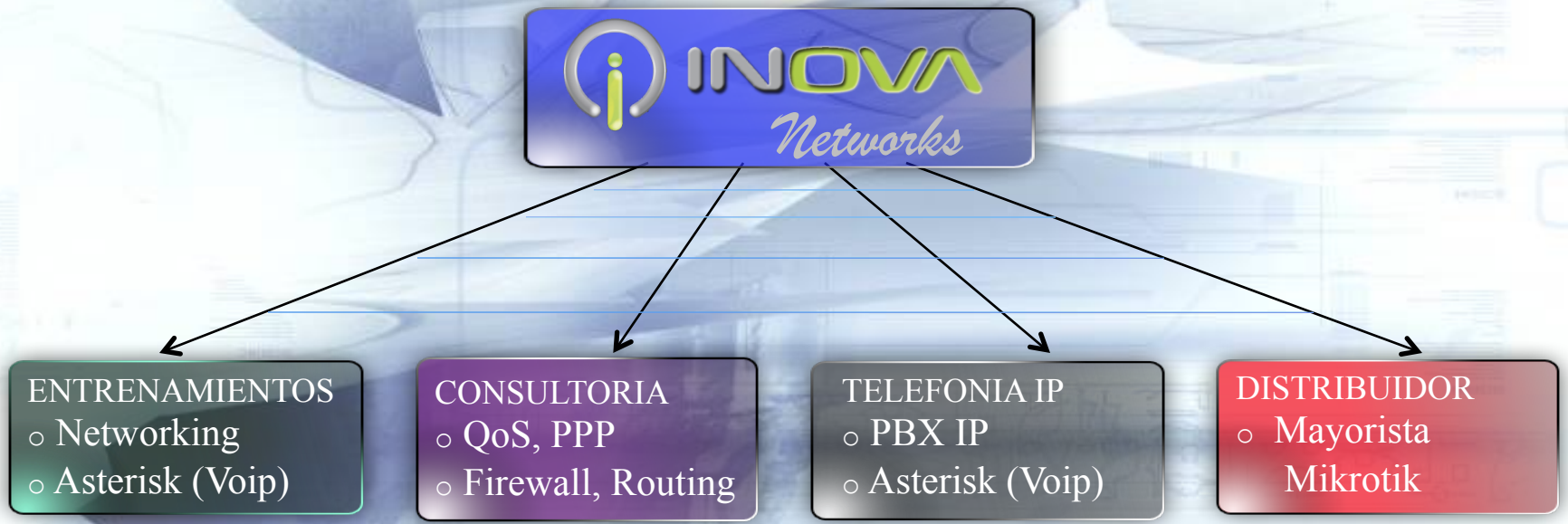
routerOS en entonos gubernamentales
Caso de éxito VPNs

Agenda

- Presentacion
- Area de Trabajo
- Una historia comun
- Entrada de Mikrotik
- Multiples Soluciones
- VPNs y caso de Exitos IPSEC

Presentacion

- **Richart W. Rojas**
- **Mikrotik Certified Consultant**
  (MTCNA, MTCWE, MTCTE, MTCRE, MTCUME, MTCINE)



Area de trabajo

Como empesar?

Motorola

Andrew

Radwin

Una historia común

INOVA

Como empesar?

Una historia común

INOVA

Resignarse???....como seguimos?

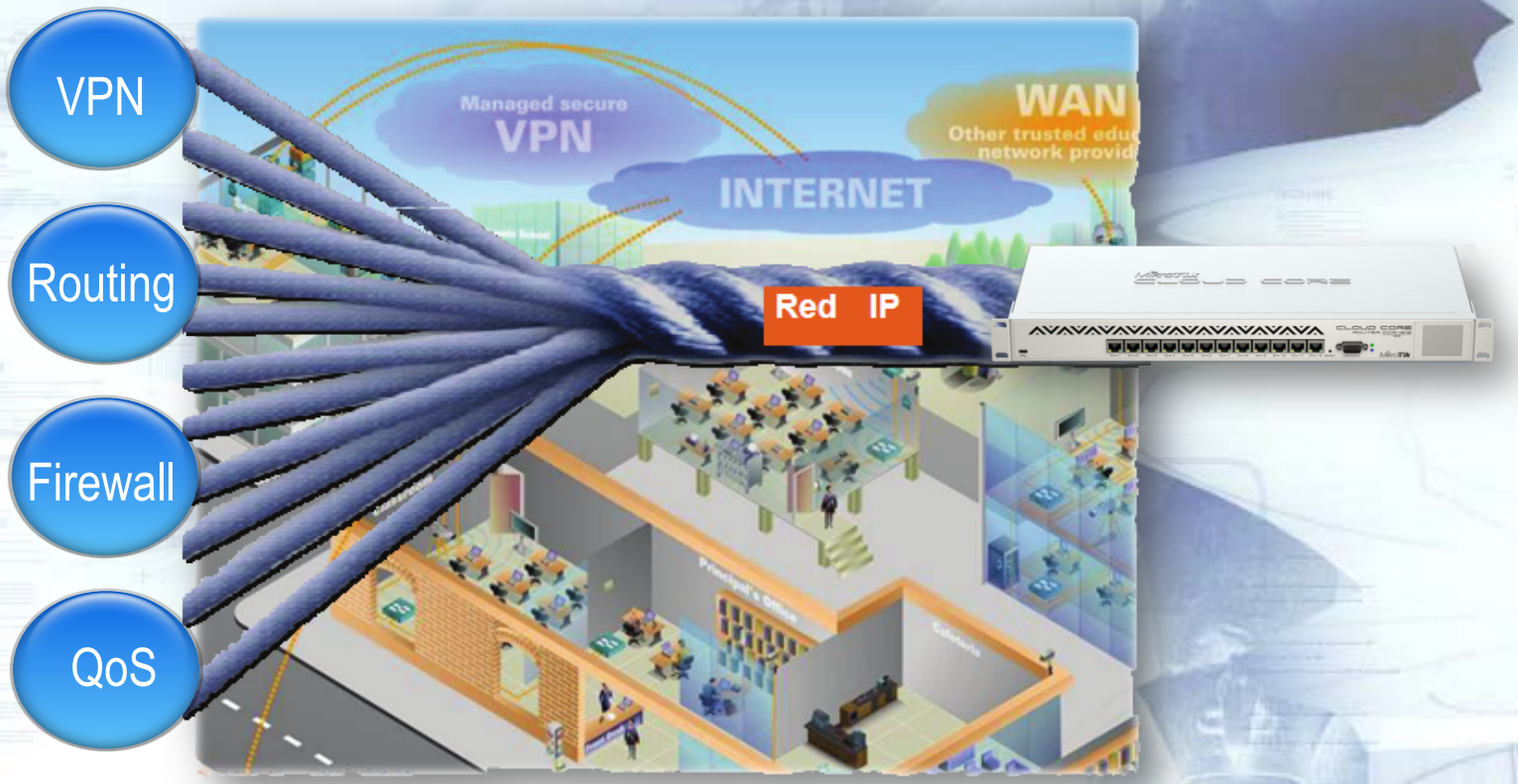
LO QUE ENCONTRAMOS EN MIKROTIK

INOVA

LO QUE ENCONTRAMOS EN MIKROTIK

* Estabilidad
* Flexibilidad
* Herramientas
* Desarrollo continuo
* Compatibilidad -RFC
* Precio/Calidad

Multiples Soluciones



Múltiples soluciones con Mikrotik (Conectividad Completa VPNs, Seguridad, balanceo de carga, Redundancia, QoS. Esa es potencialidad que tiene Mikrotik…tantos beneficios en una solución...)

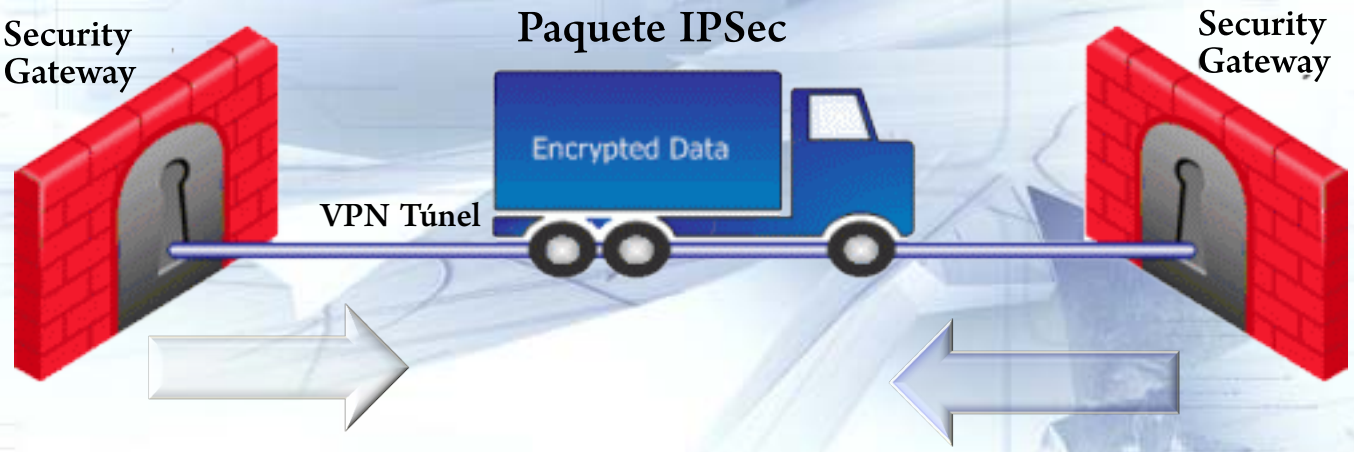
Ahora donde esta MK?

Tuneles & VPN

VPN

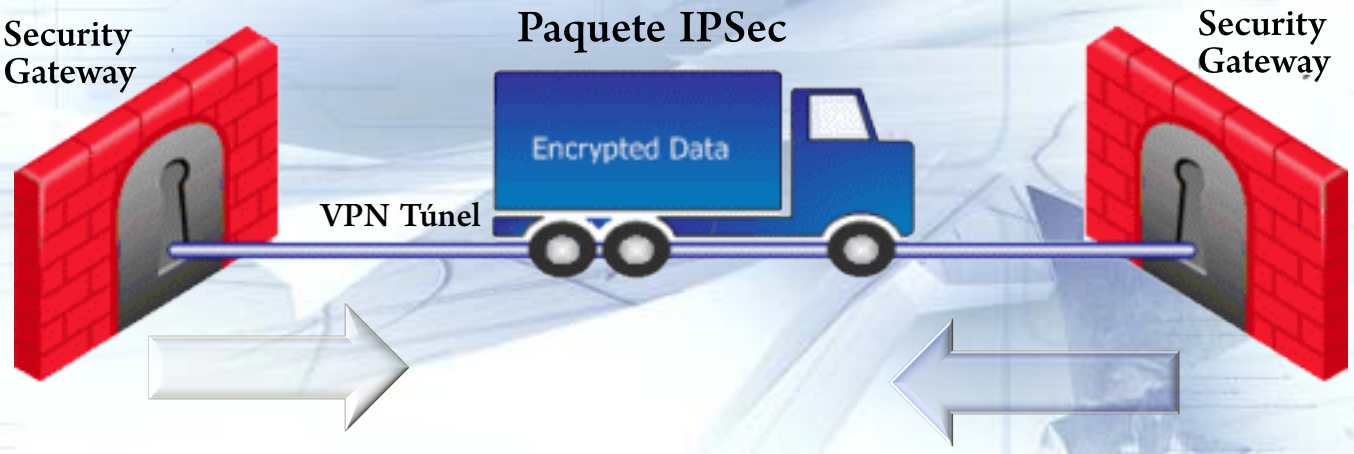
•VPN Red IP Privada y segura que pasa a través de otra red IP no segura normalmente Internet.
PPTP, L2TP,IPIP,EOIP, IPSEC,OpenVPN

IPSec



IPSec es un conjunto de estandares de IETF que proporciona servicios de seguridad a la capa de RED

IPSec



IPSec, tiene como finalidad integrar en IP, funciones de seguridad basadas en criptografia, proporcionando Confidencialidad, Integridad y Autenticidad de paquetes IP atraves del uso de un conjunto de algoritmos de encriptacion

Componentes principales IPSec

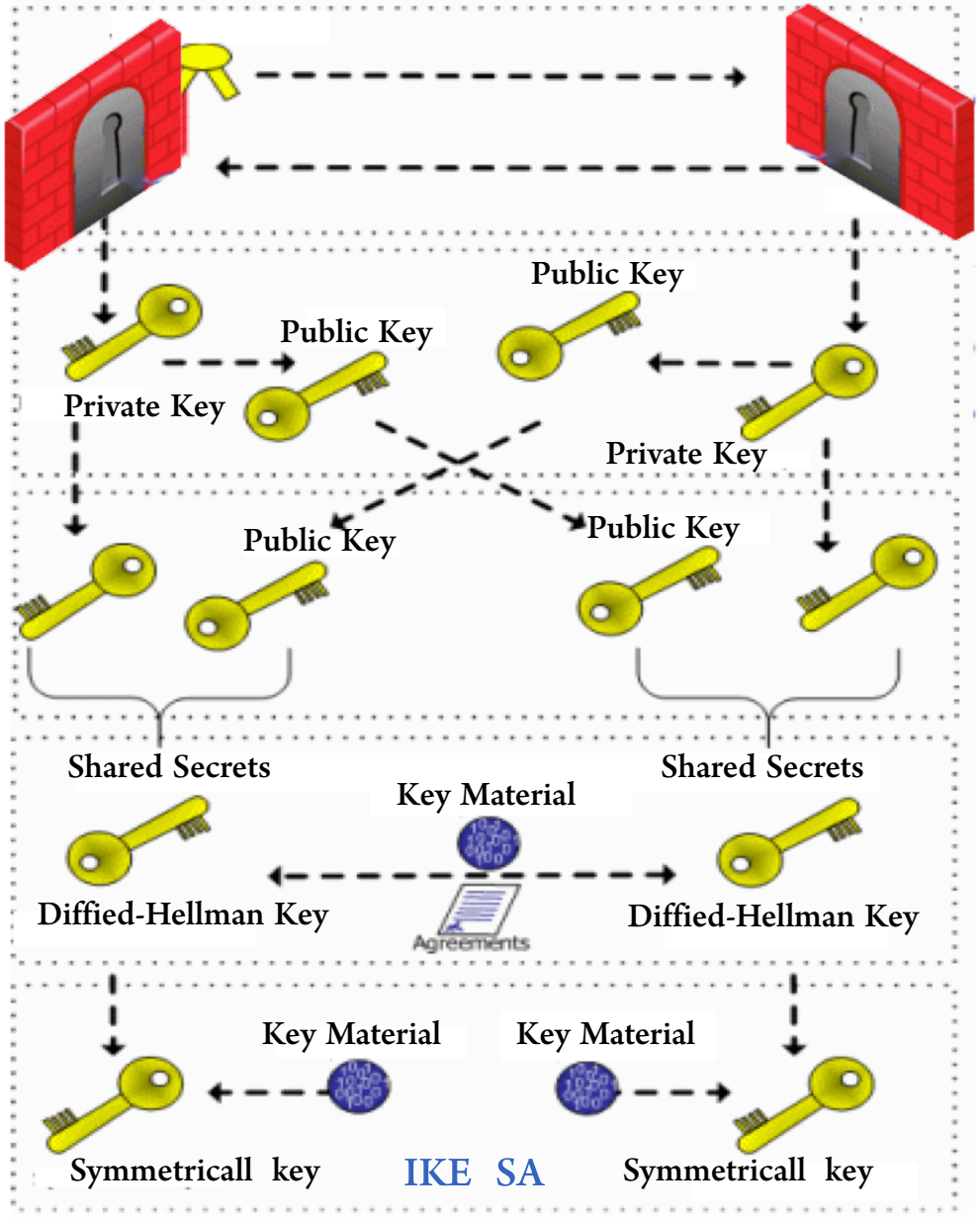
- **IKE (Internet Key Exchange)** RFC 4302
- **AH (Authentication Header)** RFC 4302
- **ESP (Encapsulating Security Payload)**

Fases de la negociación IKE

Fase 1 Ambos nodos establecen un canal seguro

Fase 2 El canal seguro IKE es usado para negociar los parámetros de seguridad

Internet Protocol Security



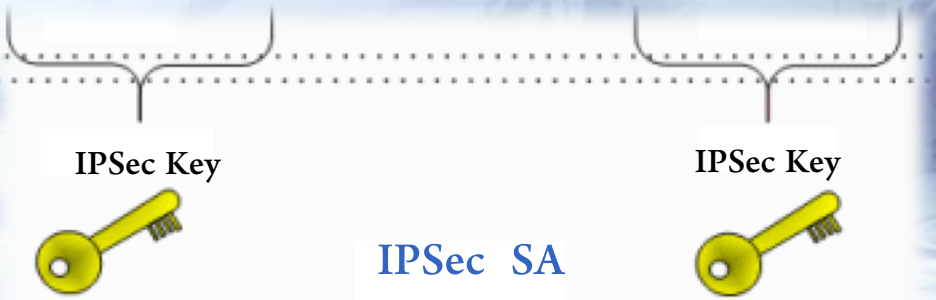
- Autenticacion usando certificados o llaves pre compartidas

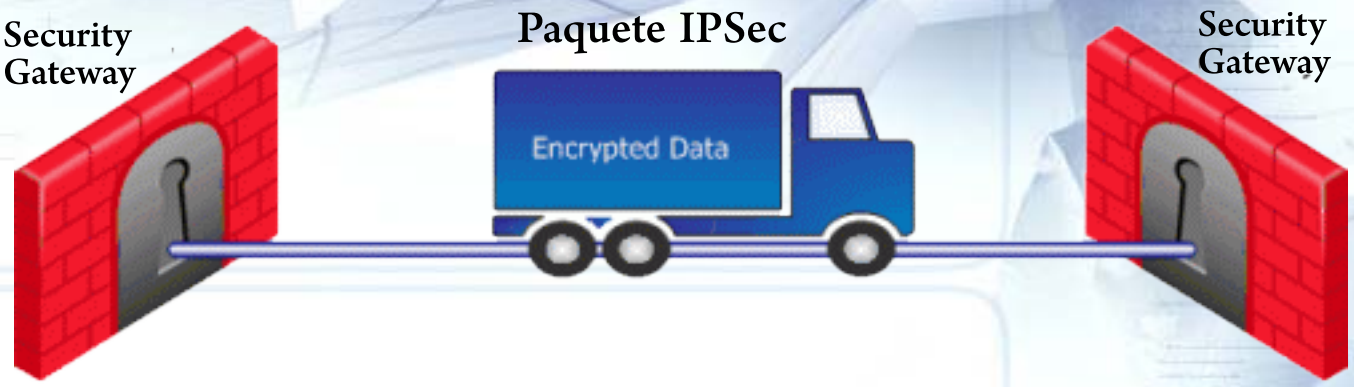
- De un grupo aleatorio, de cada lado produce una clave privada DH
- Cada par se deriva una clave pública DH de su clave privada
- Claves públicas se intercambian

- Cada lado produce un secreto compartido a partir de su clave privada y la clave pública del otro
- Secreto compartido es la clave DF

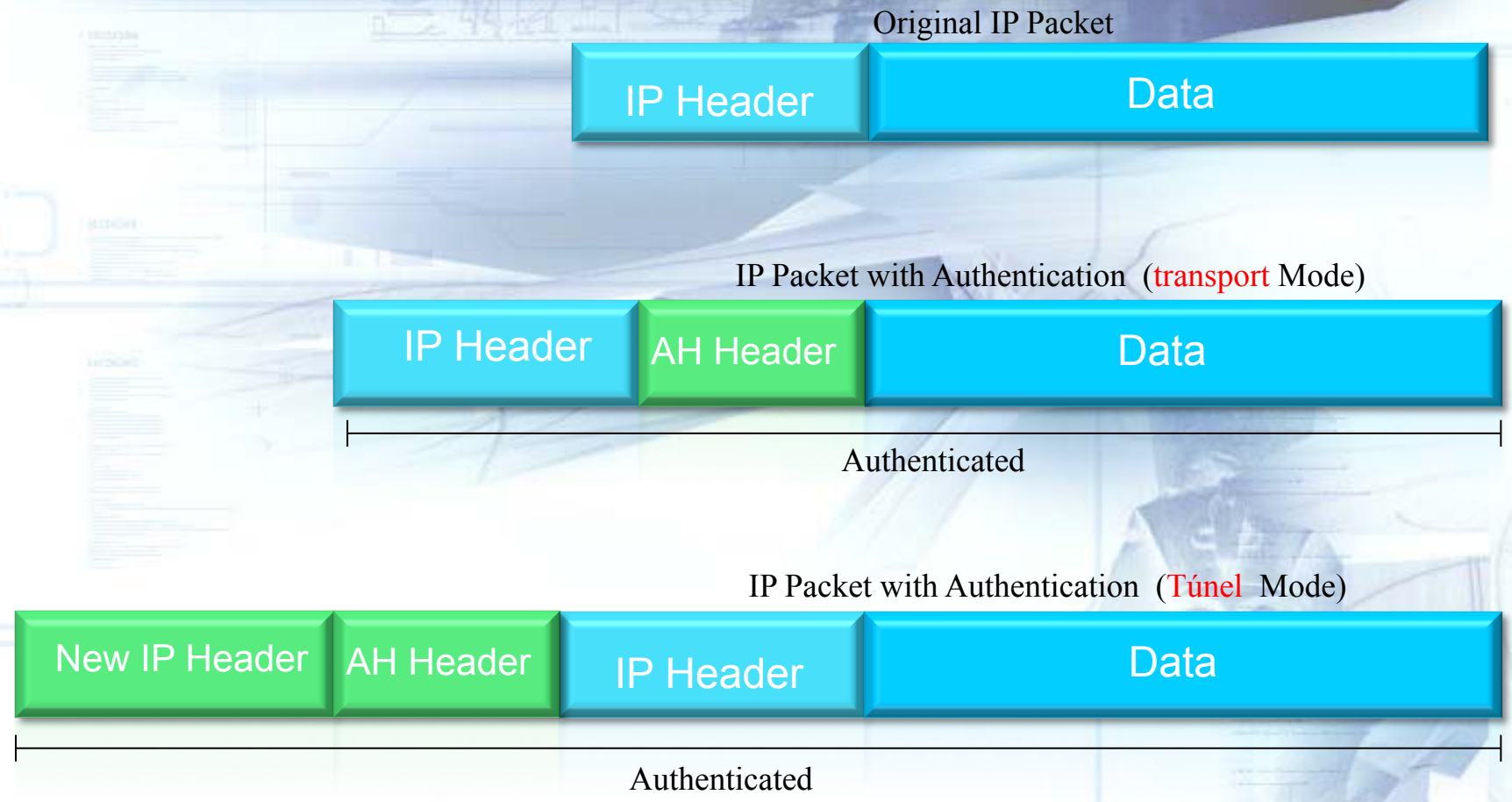
- DH clave utilizada para el intercambio de material clave (bits aleatorios y otros datos matemáticos)
- Acuerdo sobre los métodos de cifrado e integridad de IKE de fase II
- Cada lado de forma independiente genera una clave simétrica sobre la base de la clave DH y el material intercambiado entre ellas

Internet Protocol Security

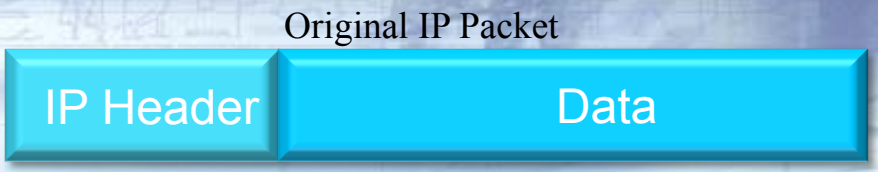


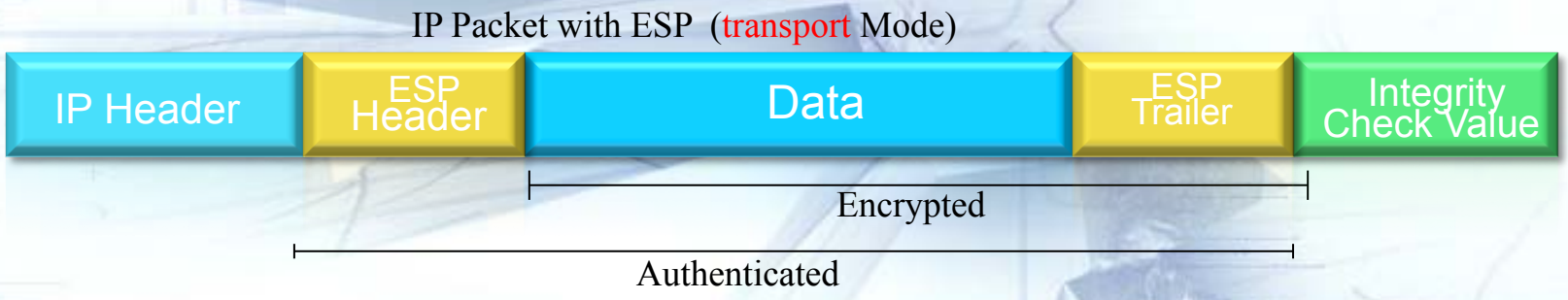


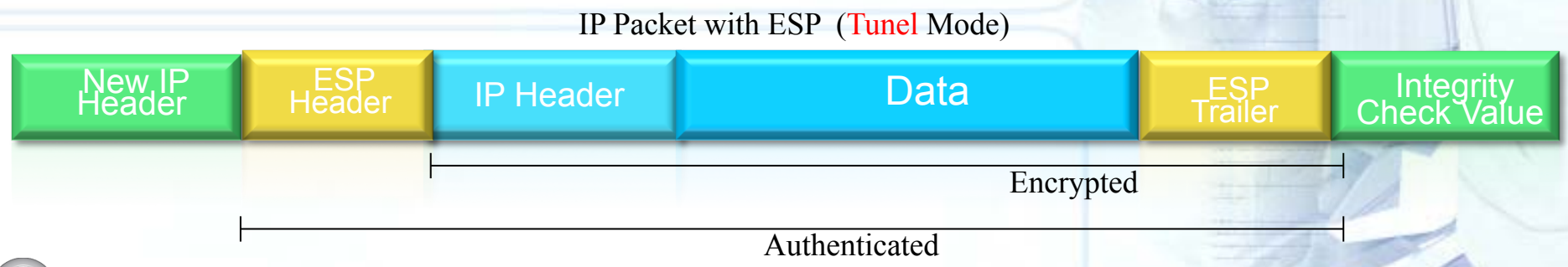
Authentication Heder



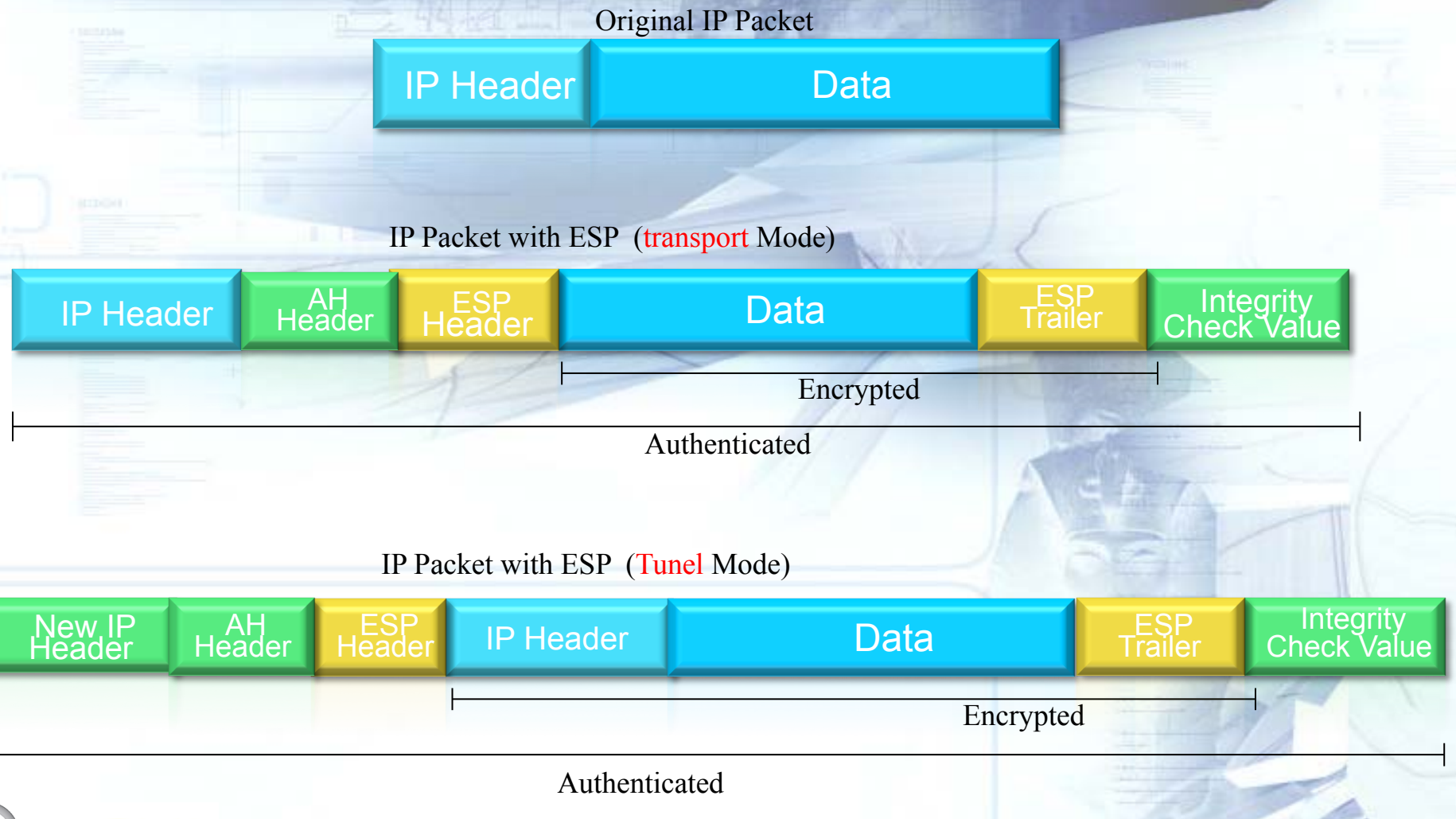
Encapsulating Security Payload







Encapsulating Security Payload



Estado Plurinacional de Bolivia
Ministerio de Economía y Finanzas Públicas

Dirección General de Sistemas de Gestión de Información Fiscal(DGSGIF)

"HISTORIA.- El SIGMA se basa en el trabajo constante del Gobierno de la República de Bolivia desde la aprobación de la Ley 1178 en Julio de 1990. Los diferentes sistemas antecesores del SIGMA desde ese entonces abarcan, entre otros, al SIIF (Sistema Integrado de Información Financiera), el SICOPRE (Sistema Integrado de Contabilidad y Presupuestos) y el SIEF (Sistema de Información Económico Financiero).

Una historia común

INOVA

Una historia común

INOVA

Una historia común

INOVA

Presupuesto Solución Básica.

Precios de la tabla en Dolares US. (2013)

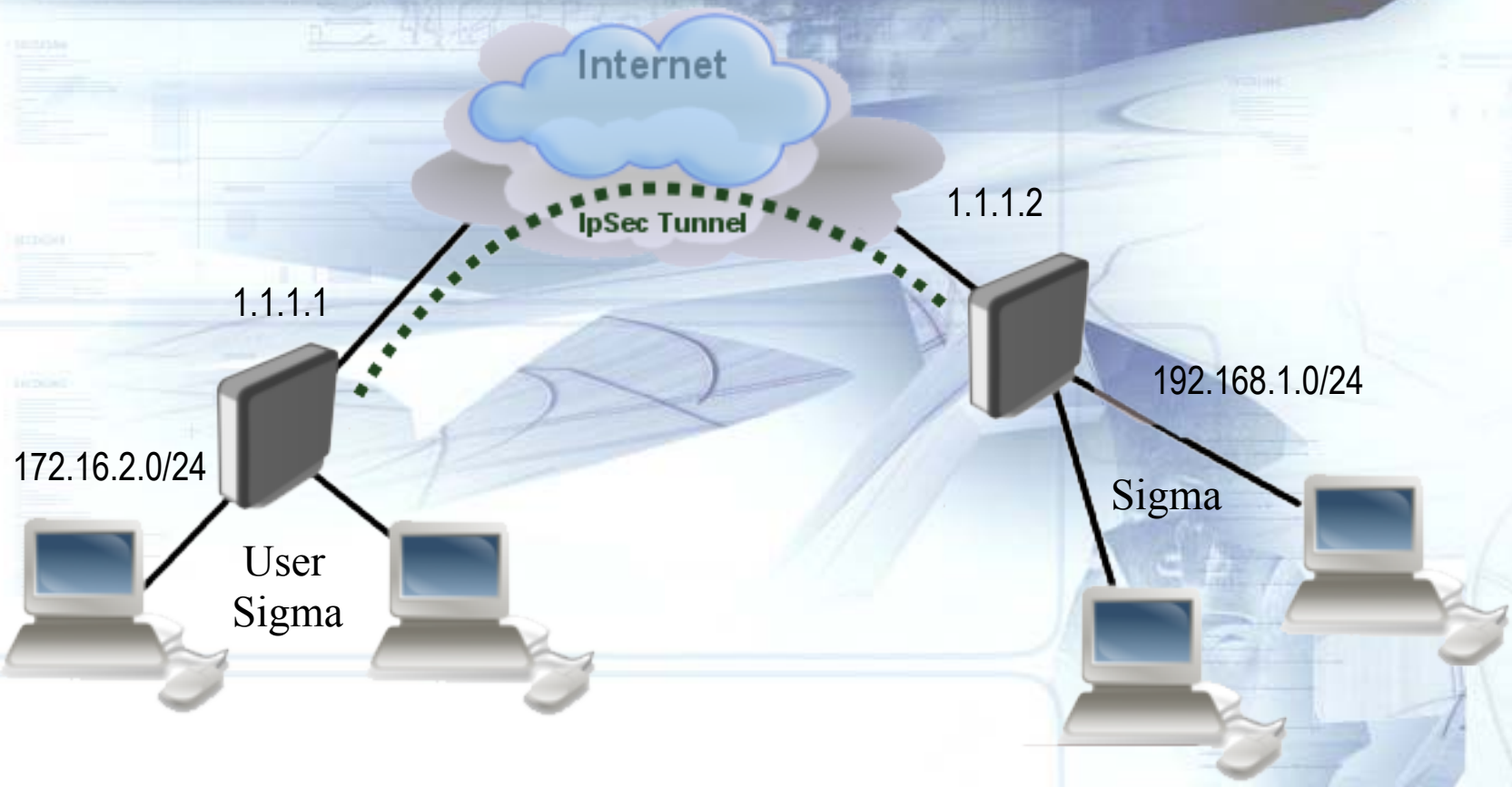
Mikrotik

Cant.	Descripción	Costo
1	RouterOS (RB 450GL)	$ 250,00
1	CRS125-24G-1S-RM	$ 155,00
1	Access Point MK RB2011	$ 190,00
1	Mano Obra	$ 900,00
	Total	$ 1.495,00

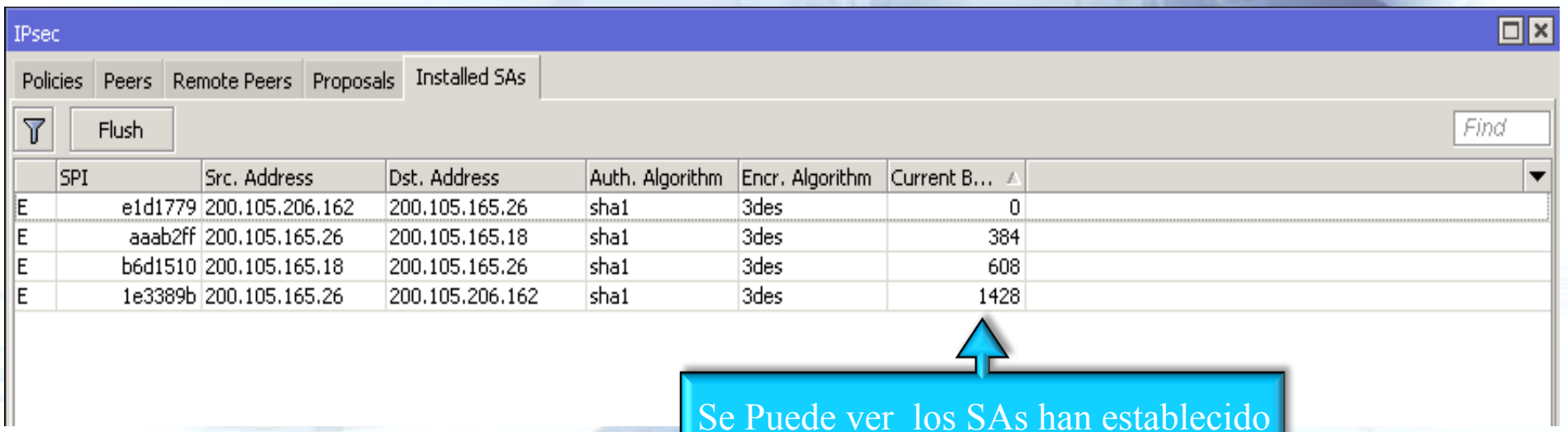
Juniper

Cant.	Descripción	Costo
1	RSX100	$ 1.350,00
1	Switch 2960 24 ptos	$ 1.295,00
1	AP1250	$ 900,00
1	Mano Obra	$ 600,00
	Total	$ 4.145,00

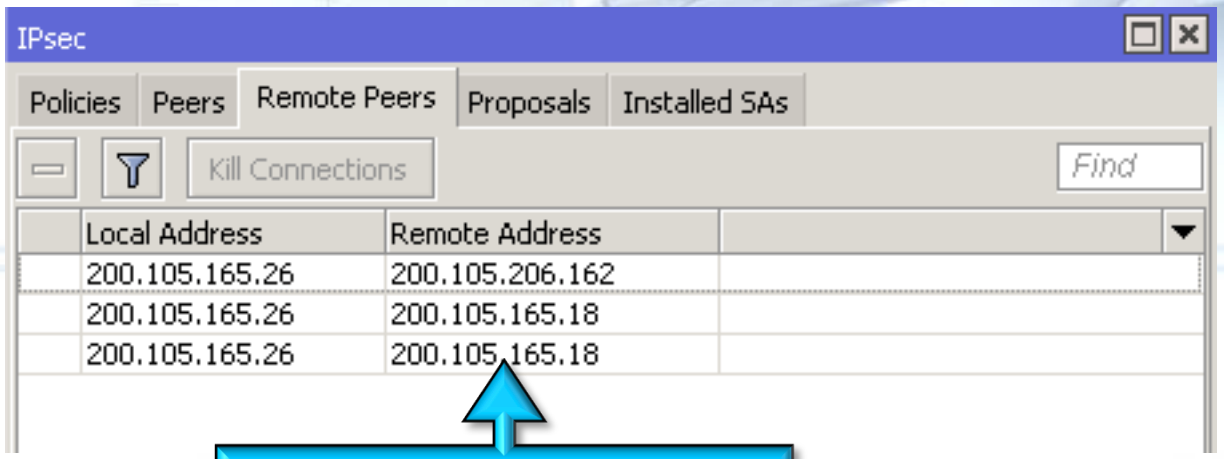
LAB


Internet
IpSec Tunnel
1.1.1.1
1.1.1.2
172.16.2.0/24
User
Sigma
192.168.1.0/24
Sigma

LAB

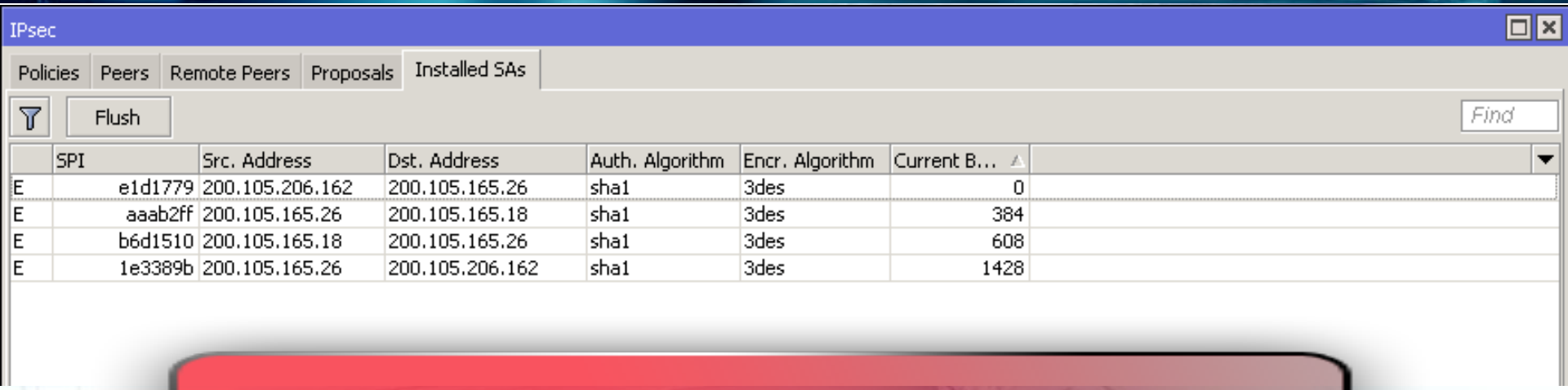


Se Puede ver los SAs han establecido



Se Puede ver los remotos Peers conectados

LAB



	SPI	Src. Address	Dst. Address	Auth. Algorithm	Encr. Algorithm	Current B...
E	e1d1779	200.105.206.162	200.105.165.26	sha1	3des	0
E	aaab2ff	200.105.165.26	200.105.165.18	sha1	3des	384
E	b6d1510	200.105.165.18	200.105.165.26	sha1	3des	608
E	1e3389b	200.105.165.26	200.105.206.162	sha1	3des	1428

La Comprensión de las 2 fases del proceso de la negociación IPSEC no es necesario, pero puede ayudar a diagnosticar los problemas

INOVA

GRACIAS POR SU ATENCION!!!!

Contactos

Mail: wrojas@inova.com.bo
Web: www.inova.com.bo
Tel: 591-2-2906508
Cel: 591-72540809
Ciudad: La Paz / Santa Cruz - Bolivia