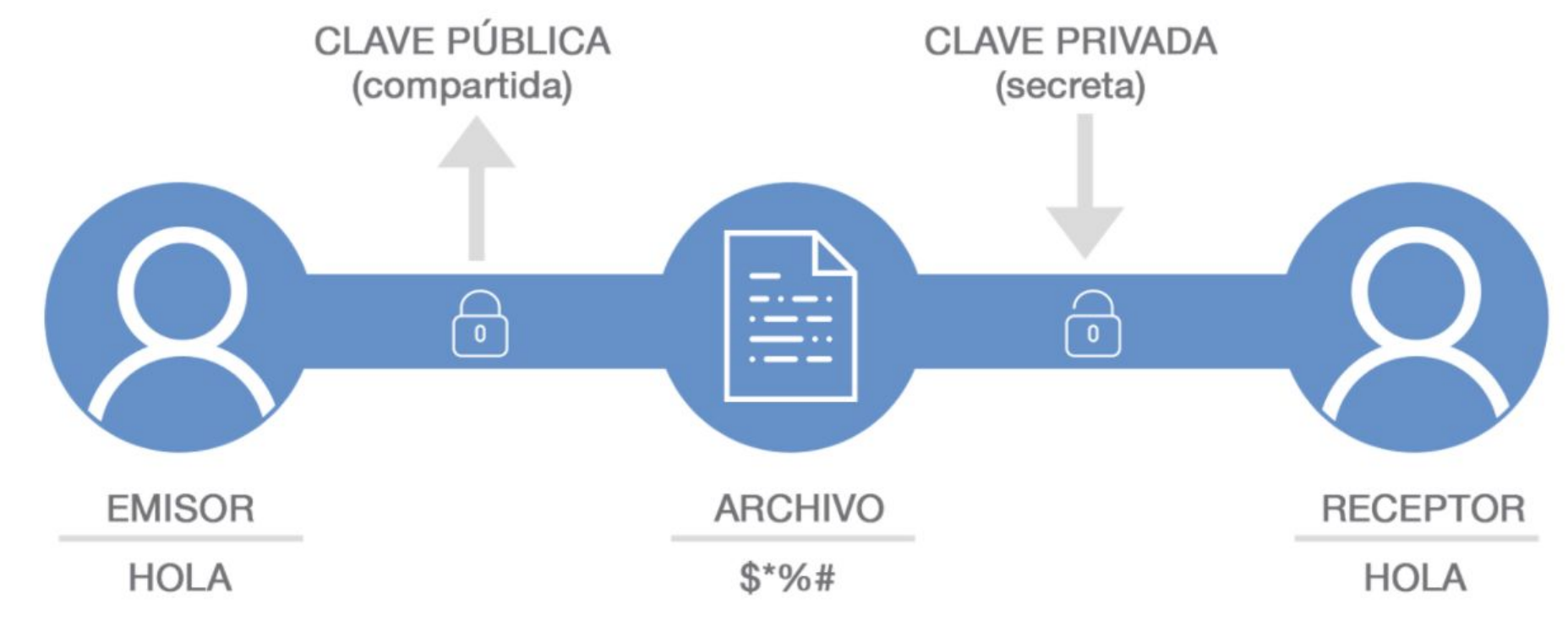
Algoritmos de encriptación

Conceptos generales

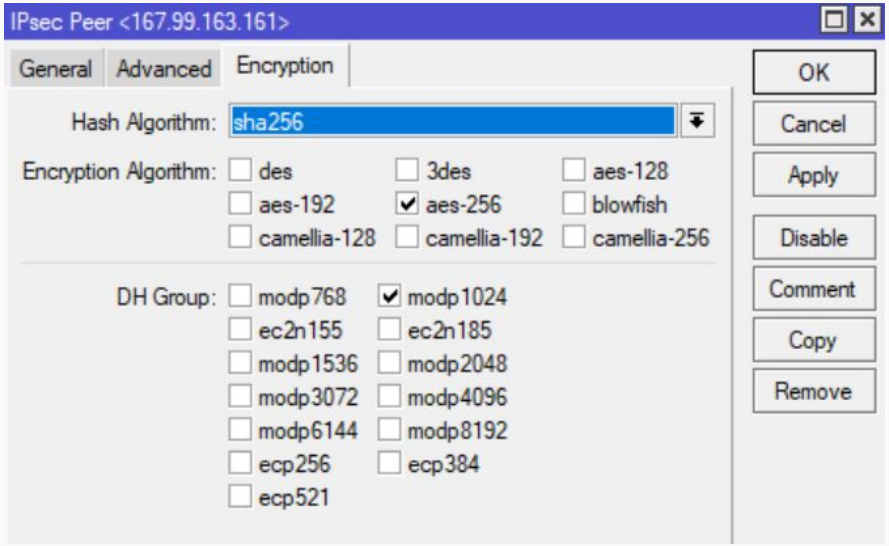
Encriptación



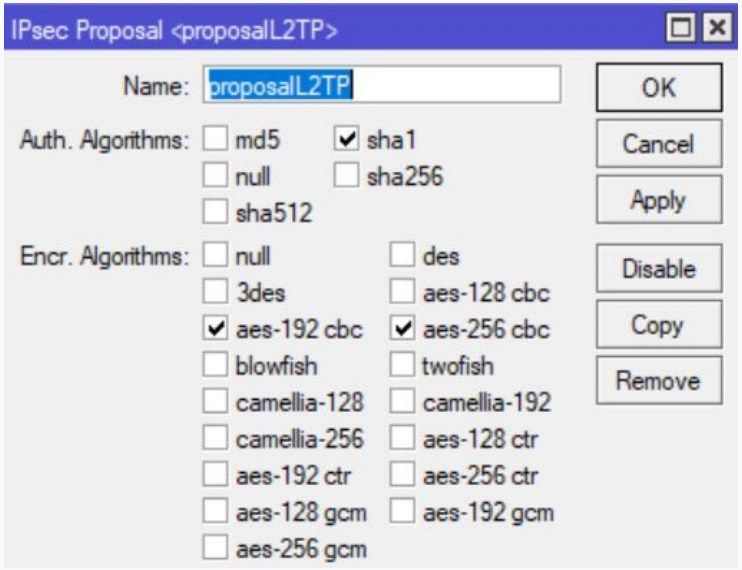
CANÓ ACADEMY

Encriptación IPSEC Mikrotik

PEER



PROPOSAL



CANÓ ACADEMY

Tipos de algoritmos de encriptación Mikrotik

Mikrotik soporta varios tipos de algoritmos de encriptación. Estos algoritmos son utilizados en combinaciones distintas dependiendo de los fabricantes al que nos vayamos a conectar o simplemente la elección que hagamos en nuestro túnel.

Los utilizados son:

- DES
- AES
- Camelia
- Blowfish
- Twofish

CANÓ ACADEMY

DES (Data Encription Standar)

El algoritmo DES usa una clave simétrica de 64bits, los 56 primeros bits son empleados para el cifrado, y los 8 bits restantes se usan para comprobación de errores durante el proceso. La clave efectiva es de 56 bits, por tanto, tenemos 2^{56} combinaciones posibles, por lo que la fuerza bruta se hace casi imposible.

DES(Data Encription Standar)

Ventajas:

- Es uno de los sistemas más empleados y extendidos, por tanto es de los más probados.
- Implementación sencilla y rápida.

Desventajas

- No se permite una clave de longitud variable, es decir, no se puede aumentar para tener una mayor seguridad.
- Es **vulnerable al criptoanálisis diferencial** (2^{47} posibilidades) siempre que se conozco un número suficiente de textos en claro y cifrados.
- La longitud de clave de 56 bits es demasiado corta, y por tanto vulnerable. **Actualmente DES ya no es un estándar,** debido a que en **1999** fue roto por un ordenador.

3DES (Triple Data Encription Standar)

Se basa en aplicar el algoritmo DES tres veces, la clave tiene una longitud de 128 bits. Si se cifra el mismo bloque de datos dos veces con dos llaves diferentes (de 64 bits), aumenta el tamaño de la clave. El 3DES parte de una llave de 128 bits, que es divida en dos llaves, A y B.

Al recibir los datos, aplicamos el algoritmo DES con la llave A, a continuación se repite con la llave B y luego otra vez con la llave A (de nuevo).

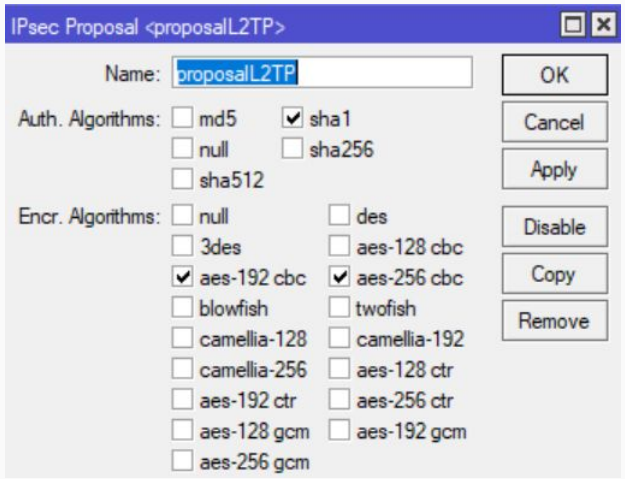
3DES aumenta de forma significativa la seguridad del sistema de DES, pero requiere más recursos del ordenador.

AES(Advance Encription Standar)

Este algoritmo es el más conocido entre los usuarios de routers, ya que WPA opera con AES como método de cifrado. Este cifrado puede implementar tanto en sistemas hardware como en software. El sistema criptográfico AES opera con bloques y claves de longitudes variable, hay AES de 128bits, de 192 bits y de 256 bits.

Existen varios tipos:

- CBC (Cipher-block chaining)
- CRT(Counter)
- GCM(Galois/Counter Mode)



CANÓ ACADEMY

Blowfish

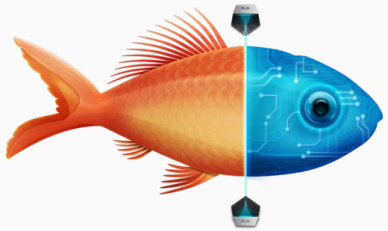
Es un codificador de bloques simétricos de **64 bits AES** y claves que van desde los **32 bits** hasta **448 bits**, incluido en un gran número de conjuntos de codificadores y productos de cifrado. Es un codificador de 16 rondas y usa llaves que dependen de las Cajas-S, En total, el algoritmo de cifrado Blowfish correrá 521 veces para generar todas las subclaves, y cerca de 4KB de datos son procesados.

- Longitud de clave: Variable: de 32 a 448 bits.
- Tamaño de bloque: 64 bits.

Twofish

Es un algoritmo simétrico con cifrado por bloques de tipo **AES**. El tamaño de bloque es de 128 bits y el tamaño de clave puede llegar hasta 256 bits. Las características distintivas de Twofish son el uso de S-boxes pre-computadas con llaves dependientes, y una llave-horario relativamente compleja. Es levemente más lento que **Rijndael** (el algoritmo elegido para AES) para las llaves de **128 bits**, pero algo más rápido para las llaves de 256 bits y **en muchas ocasiones es más seguro que AES.**

- Longitud de clave: Variable, hasta 256 bits.
- Tamaño de bloque: 128 bits.



CANÓ ACADEMY

Camellia

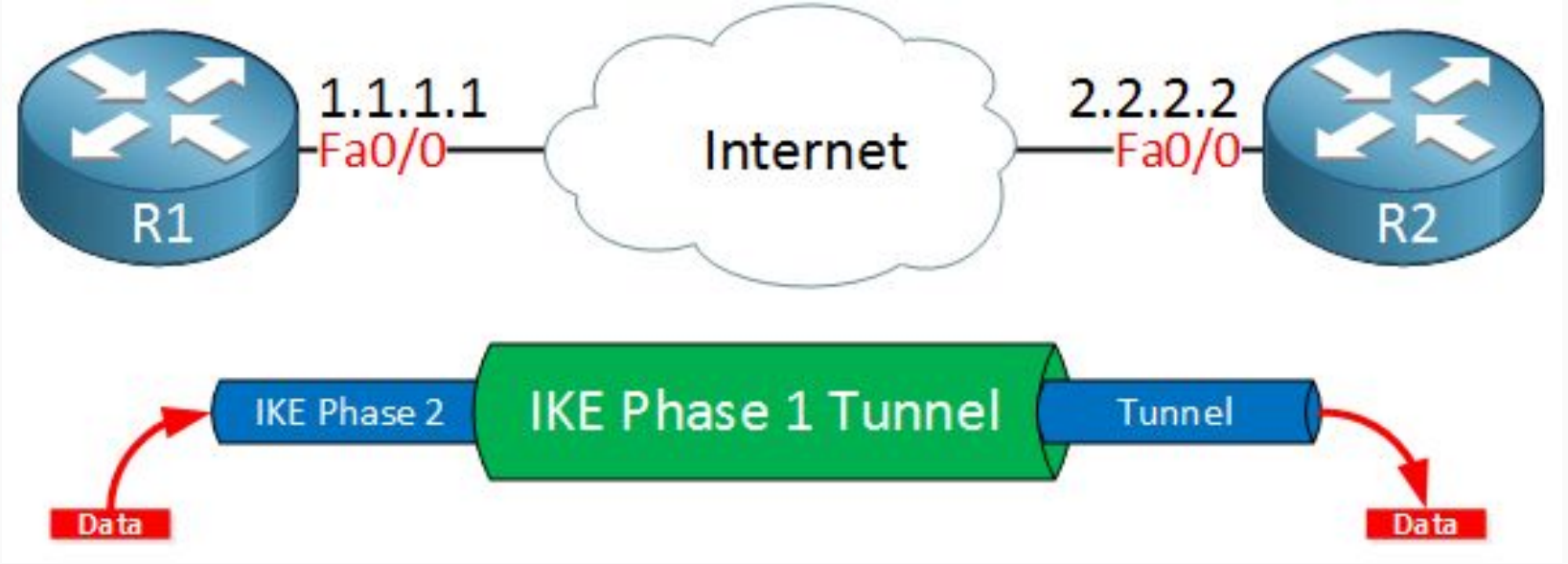
Es un algoritmo de cifrado simétrico desarrollado en el año 2000 por la compañía telefónica de Japón y la Corporación eléctrica Mitsubishi para implementarse en hardware y software.

Es considerado un estándar criptográfico en Europa y en las oficinas gubernamentales de Japón para el uso de políticas de IPSEC.

Camellia es un cifrador de bloques de tamaño dijo de 128, 192 0 256 efectuando rondas tipo Feitsel.

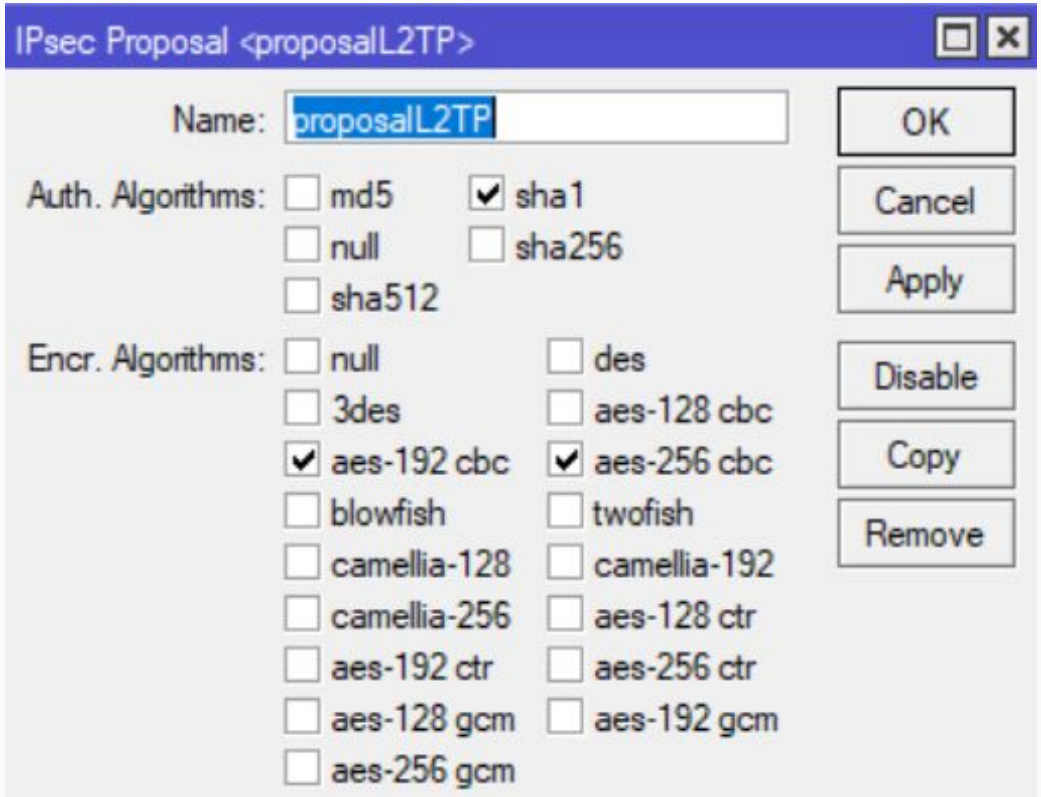
Si Japón lo considera para sus oficinas gubernamentales, ya usted sabe!

IPSEC



CANÓ ACADEMY

Resumen de algoritmos de encriptación para IPSEC - Mikrotik



CANÓ ACADEMY

Laboratorios IPSEC

Ahora vamos a configurar los laboratorios de IPSEC Site to Site.

Atención especial a estos laboratorios que tienen muchos detalles.

MikroTik

CANÓ ACADEMY