

VPN'S FÁCILES Y SEGURAS

Creación de enlaces PPTP/L2TP
incorporando IPSec

LSC. David Ricardo López Aldret
Íntegra Communications.
Miahuatlán, Oaxaca, México

MUM MÉXICO 2013

Acerca de



Nombre: LSC. David Ricardo López Aldret
MTCNA

Empresa: Íntegra Comunicaciones.
Propietario.
Partner de MKE en México para capacitaciones oficiales e implementaciones/soluciones llave en mano.

Ubicación: Miahuatlán, Oaxaca, México

Actividades: Wisp Local, Implementaciones externas.

Mail: contacto@internetmiahuatlan.com.mx

URL: www.internetmiahuatlan.com.mx

Objetivo:

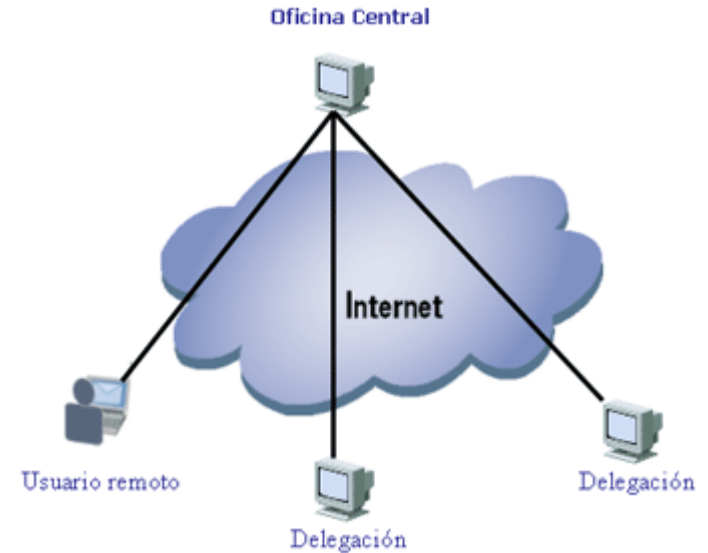


Presentación de una guía simple, fácil y resumida para la implementación de una o mas VPN's sobre PPTP o L2TP con un cifrado superior utilizando IPSEC.

Se obvian configuraciones iniciales para dar mayor fluidez a la misma.

Definamos VPN:

Redes locales que se extienden a través de una red pública mediante túneles virtuales cifrados. Facilita que los equipos conectados en extremos distantes interactúen y se comuniquen como si estuvieran ubicados en una sola red.



Funcionales en Mikrotik:



PPP

PPTP

SSTP

L2TP

OVPN

PPPOE

EOIP

Algunas trabajan en capa 2, otras en capa 3

Definamos IPSec

Internet Protocol Security.

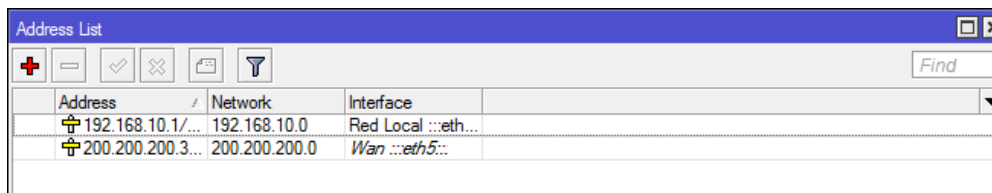
Conjunto de protocolos que aseguran las comunicaciones mediante el cifrado/descifrado previo intercambio de una llave común.

Muy robusto, presenta algoritmos de cifrado desde “simples” hasta grado militar: 3des, camelia-256, aes-128.

¡A mayor complejidad de cifrado mayor consumo de CPU!

Empezamos

Configuración servidor:



Address	Network	Interface
192.168.10.1/...	192.168.10.0	Red Local ::eth...
200.200.200.3...	200.200.200.0	Wan ::eth5...

Red local: 192.168.10.0/24

IP Wan: 200.200.200.3/29

Creando el servidor:

Interface <juanito>

General Status Traffic

Name: juanito

Type: L2TP Server

L2 MTU:

User: juanito

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave Status: connected



New PPP Secret

Name: juanito

Password: juanito

Service: l2tp

Caller ID:

Profile: default-encryption

Local Address: 10.254.254.1

Remote Address: 10.254.254.2

Routes:

Limit Bytes In:

Limit Bytes Out:

OK Cancel Apply Disable Comment Copy Remove

enabled



L2TP Server

Enabled

Max MTU: 1460

Max MRU: 1460

MRRU:

Keepalive Timeout: 30

Default Profile: default-encryption

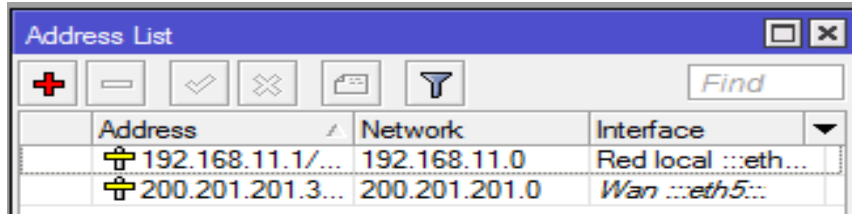
- Authentication

pap chap

mschap1 mschap2

OK Cancel Apply

Configuración lado cliente:

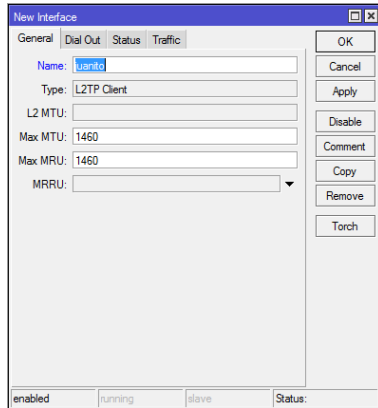


Address	Network	Interface
192.168.11.1/...	192.168.11.0	Red local ::eth...
200.201.201.3...	200.201.201.0	Wan ::eth5::

Red local: 192.168.11.0/24

IP Wan: 200.201.201.3/29

Creando el cliente:



New Interface

General Dial Out Status Traffic

Name:

Type: L2TP Client

L2 MTU:

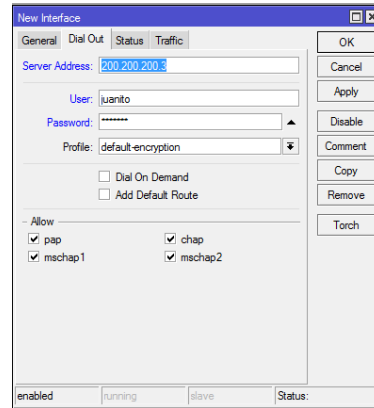
Max MTU: 1460

Max MRU: 1460

MRRU:

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave Status:



New Interface

General Dial Out Status Traffic

Server Address:

User:

Password:

Profile: default-encryption

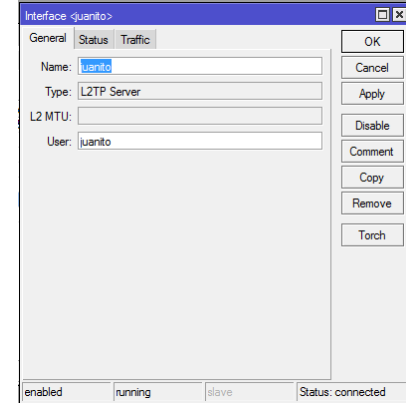
Dial On Demand
 Add Default Route

- Allow

pap chap
 mschap1 mschap2

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave Status:



Interface <juanito>

General Status Traffic

Name:

Type: L2TP Server

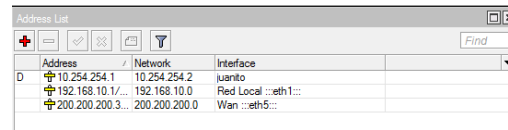
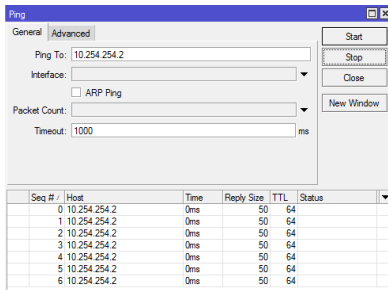
L2 MTU:

User:

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave Status: connected

Conexión creada a nivel VPN:



Ciframos con IPSec

Servidor

IPsec Policy <192.168.10.0/24:0->192.168.11.0/24:0>

General Action

Src. Address: 192.168.10.0/24

Src. Port: [v]

Dst. Address: 192.168.11.0/24

Dst. Port: [v]

Protocol: 255 (all) [v]

OK
Cancel
Apply
Disable
Comment
Copy
Remove

enabled



IPsec Policy <192.168.10.0/24:0->192.168.11.0/24:0>

General Action

Action: encrypt [v]

Level: require [v]

IPsec Protocols: esp [v]

Tunnel

SA Src. Address: 10.254.254.1

SA Dst. Address: 10.254.254.2

Proposal: default [v]

Priority: 0

OK
Cancel
Apply
Disable
Comment
Copy
Remove

enabled

Ciframos con IPSec

Cliente

IPsec Policy <192.168.11.0/24:0->192.168.10.0/24:0>

General Action

Src. Address: 192.168.11.0/24

Src. Port:

Dst. Address: 192.168.10.0/24

Dst. Port:

Protocol: 255 (all)

OK
Cancel
Apply
Disable
Comment
Copy
Remove

enabled



IPsec Policy <192.168.11.0/24:0->192.168.10.0/24:0>

General Action

Action: encrypt

Level: require

IPsec Protocols: esp

Tunnel

SA Src. Address: 10.254.254.2

SA Dst. Address: 10.254.254.1

Proposal: default

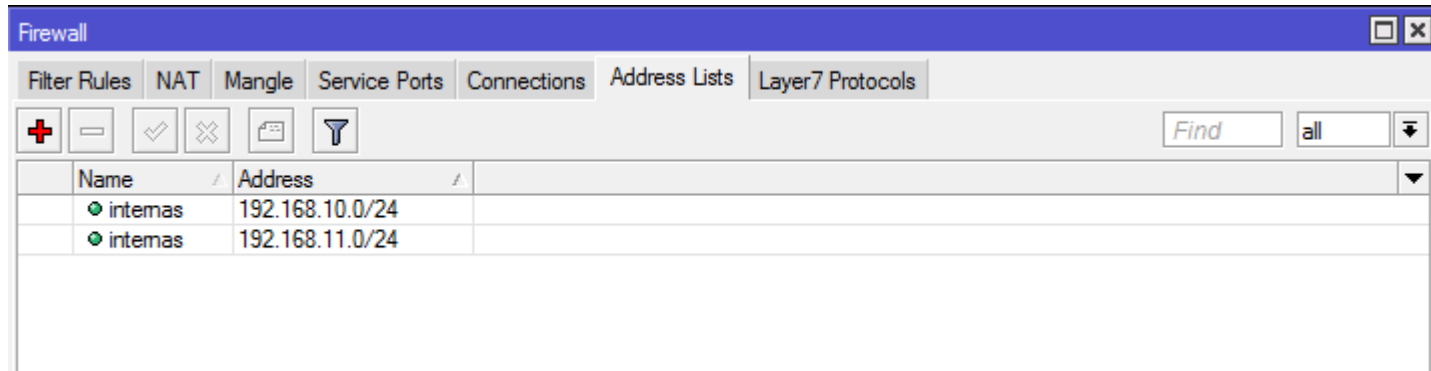
Priority: 0

OK
Cancel
Apply
Disable
Comment
Copy
Remove

enabled

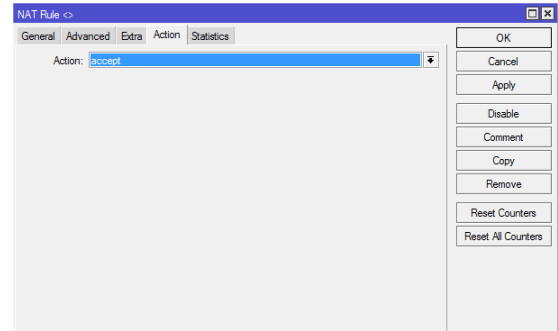
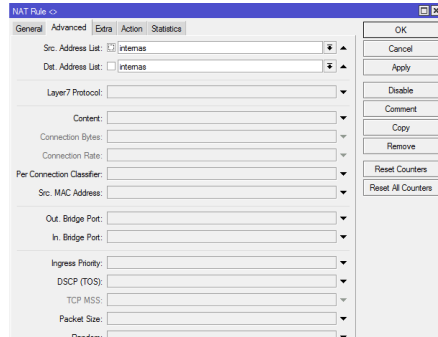
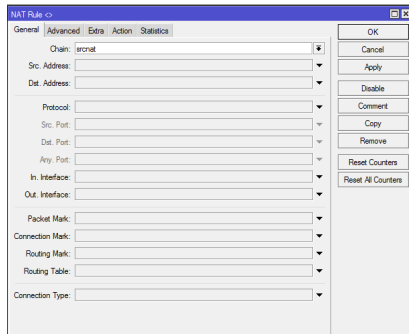
Definimos address-list

En ambos extremos



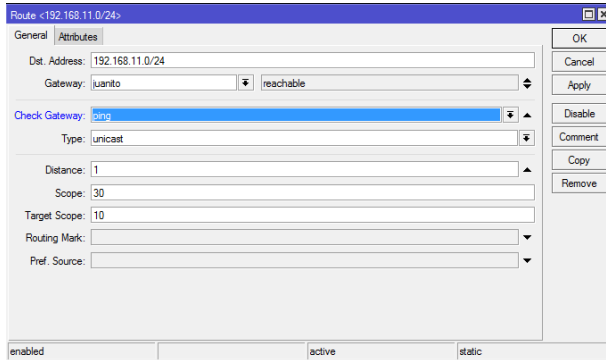
Aceptamos el tráfico interno

En ambos extremos



Definimos rutas estáticas

Lado servidor



The screenshot shows a network configuration window titled "Route <192.168.11.0/24>". The window has two tabs: "General" and "Attributes". The "General" tab is active, showing the following fields:

- Dest. Address: 192.168.11.0/24
- Gateway: lanito (with a dropdown arrow) and reachable (with a dropdown arrow)
- Check Gateway: ping (with a dropdown arrow)
- Type: unicast (with a dropdown arrow)
- Distance: 1 (with a dropdown arrow)
- Scope: 30 (with a dropdown arrow)
- Target Scope: 10 (with a dropdown arrow)
- Routing Mark: (with a dropdown arrow)
- Pref. Source: (with a dropdown arrow)

On the right side of the window, there are several buttons: OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom of the window, there are three checkboxes: "enabled" (checked), "active" (checked), and "static" (checked).

Definimos rutas estáticas

Lado cliente

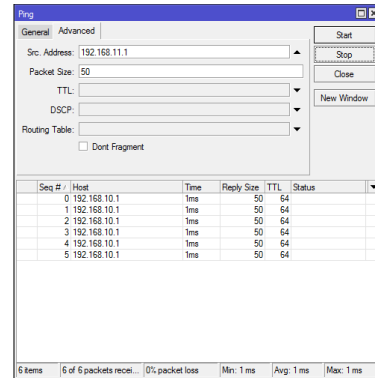
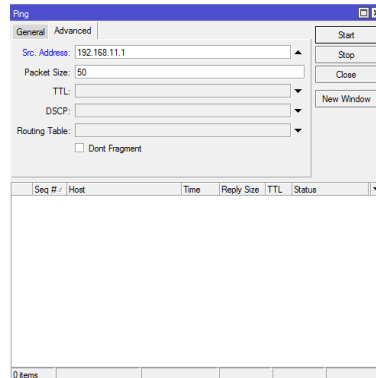
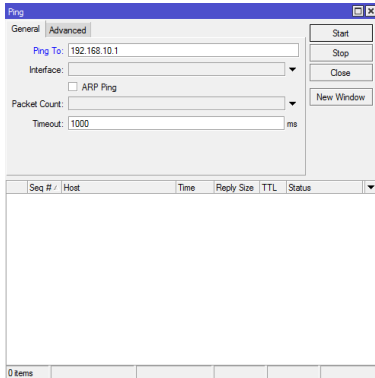
The image shows a network configuration window titled "Route <192.168.10.0/24>". The window has two tabs: "General" and "Attributes". The "General" tab is active. The configuration fields are as follows:

- Dist. Address: 192.168.10.0/24
- Gateway: juanito (selected) | reachable (dropdown)
- Check Gateway: ping (dropdown)
- Type: unicast (dropdown)
- Distance: 1
- Scope: 30
- Target Scope: 10
- Routing Mark: (empty dropdown)
- Pref. Source: (empty dropdown)

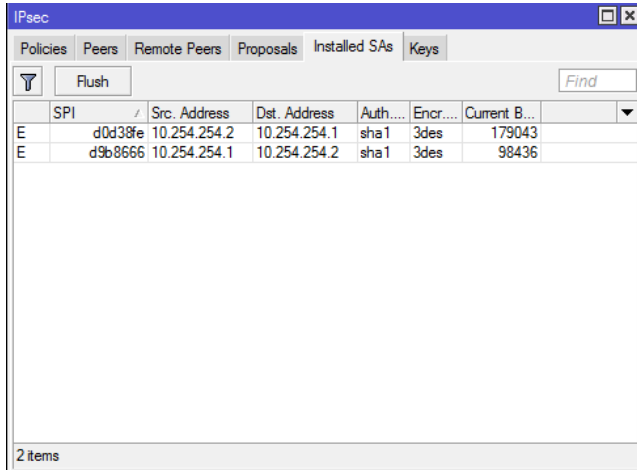
On the right side of the window, there are several buttons: OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom of the window, there are three status indicators: "enabled", "active", and "static".

Generamos tráfico

Al generar tráfico INTERNO forzamos la instalación de la llave entre equipos



La llave se ha intercambiado



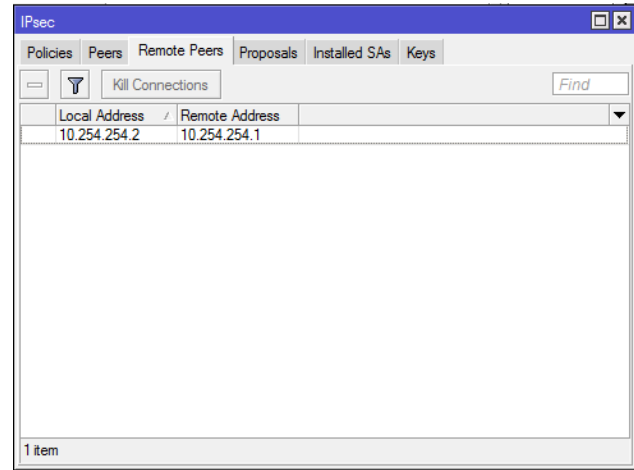
IPsec

Policies Peers Remote Peers Proposals Installed SAs Keys

Flush Find

SPI	Src. Address	Dst. Address	Auth....	Encr....	Current B...
E d0d38fe	10.254.254.2	10.254.254.1	sha1	3des	179043
E d9b8666	10.254.254.1	10.254.254.2	sha1	3des	98436

2 items



IPsec

Policies Peers Remote Peers Proposals Installed SAs Keys

Kill Connections Find

Local Address	Remote Address
10.254.254.2	10.254.254.1

1 item

¿PREGUNTAS?

Creación de enlaces PPTP/L2TP
incorporando IPSec

LSC. David Ricardo López Aldret
Íntegra Communications.
Miahuatlán, Oaxaca, México

MUM MÉXICO 2013

GRACIAS

Creación de enlaces PPTP/L2TP
incorporando IPSec

LSC. David Ricardo López Aldret
Íntegra Communications.
Miahuatlán, Oaxaca, México

MUM MÉXICO 2013