

Laboratorio IPSEC: Configuración site to site MikroTik-MikroTik.

Objetivo: configurar un VPN IPsec site to site entre routers Mikrotik.





Router-A:

FASE 1

Paso 1: Nos dirijimos al menú IP y luego vamos a IPSEC.

Dentro del menú IPSEC vamos a Profiles:

🗡 Quick Set							
CAPsMAN	IPsec						
Interfaces	Poli	ies Proposals	Groups Peers Id	lentities Profiles Active	Peers Mode Configs Ir	stalled SAs Keys	
Wireless	+	- 7					Find
👯 Bridge	Na	ne	Hash Algorithms	Encryption Algorithm	DH Group	Proposal C	
🏣 PPP	* def	ault	sha1	3des aes-128	modp1024 modp2048	obey	
Mesh							
P IP	\square						
Ø MPLS	\square						
🎩 Routing	\square						
😂 System	\square						
Queues							
QueuesFiles							
P Queues Files	-						

Agregamos un nuevo perfil llamado **IPSEC1** y configuramos de la siguiente forma:

IPsec Profile <ipsec1></ipsec1>				
Name:	IPSEC1			OK
Hash Algorithms:	sha1		₹	Cancel
Encryption Algorithm:	des	3des		Apply
-	aes-128	aes-192		Сору
L	✓ aes-256	blowfish		Remove
	camellia-12	8 camellia-192	2	
	camellia-25	6		
DH Group:	modp768	✓ modp1024		
	ec2n155	ec2n185		
	modp1536	modp2048		
	modp3072	modp4096		
	modp6144	modp8192		
	ecp256	ecp384		
	ecp521			
Proposal Check:	obey		∓	
Lifetime:	08:00:00			
Lifebytes:			•	
		sal	_	
DPD Interval:	120		s	
DPD Maximum Failures:	5			



Paso 2: Nos dirigimos a Peer y **colocamos la IP** de nuestro cliente junto al **profile** que hemos creado recientemente llamado **IPSEC1**.

IPsec											
Policies	Proposals	Groups	Peers	Identities	Profiles	Active	Peers	Mode Configs	Installed	SAs Keys	
+ -		7									
#	Name		Address	Lo	cal Addre	SS	Profile)	Exchange .		
0	Cliente		45.77.21	9.87			IPSEC	21	main		
IPsec Pe	er <cliente></cliente>] ×
	Name: Cli	iente								ОК	
A	Address: 45	.77.219.8	7							Cancel	
	Port:								~	Apply	
Local A	Address:								•	Disable	
	Profile: IP:	SEC1							₹	Comment	
Exchang	e Mode: ma	ain							₹	Сору	
		Passive								Remove	
	✓	Send INI	TIAL_CO	NTACT							
enabled					r	esponde	r				

Paso 3: Ahora vamos a configurar el método de autenticación. Para eso vamos a **Identities.** Elegimos el Peer y el Policy Template IPSEC. Luego elegimos el método de **pre share Key** y colocamos la clave **Curso!!123!!\$** en secret.

IPsec Identity <cliente></cliente>			
Peer:	Cliente T	[ОК
Auth. Method:	pre shared key		Cancel
Secret:	Curso!!123!!\$		Apply
		٦	Disable
Policy Template Group:	default 🔸		Comment
Notrack Chain:	₹		Сору
My ID Type:	auto 두		Remove
Remote ID Type:	auto 두		
Match By:	remote id 두		
Mode Configuration:	•		
Generate Policy:	no 두		



FASE 2

Paso 4: Nos dirigimos al menú Proposal y configuramos de la siguiente forma. Algoritmo de autenticación sha1, algoritmo de encriptación aes-256cbc, lifetime 30 minutos y PFS Group modp1024.

IPsec	IPsec Proposal <pro-ipsec1></pro-ipsec1>	
Policies Proposals Grout	Name: PRO-IPSEC1	ОК
	Auth. Algorithms:md5 🛛 🗹 sha1	Cancel
Name 🛆 Auth. Algor	null sha256	Apply
PRO-IPSE sha1	sha512	Disable
" default sha i	Encr. Algorithms: null des	Сору
	3des aes-128 cbc	Remove
	aes-192 cbc	
	blowfish twofish	
	camellia-128 camellia-192	
	camellia-256 aes-128 ctr	
	aes-192 ctr aes-256 ctr	
	aes-128 gcm aes-192 gcm	
	aes-256 gcm	
	Lifetime: 00:30:00	
	PFS Group: modp1024	
	enabled	



Paso 5: Configuración del **Policies** o política de IPSEC. Aquí es donde definimos que nuestro IPSEC va a trabajar en modo túnel con el peer indicado. El **source address** es la red local y el dst address es la red remota del cliente.

IPsec					
Policies Proposals Grou	os Peers Identities	Profiles Active Peers	Mode Configs Installed S	SAs Key	/s
+-~~~	Statistics				
# Peer	Tunnel Src. Ad	ldress 🛆 Src. P	ort Dst. Address	Dst. Po	rt Proto Action
1 Cliente	yes 10.90.1	.0/24	192.168.11.0/24		255 (encrypt
0 *T IPsec Policy	<10.90.1.0/24:0->192.	.168.11.0/24:0>			
General Ac	tion Status				ОК
Pee	Cliente		₹	•	Cancel
	✓ Tunnel				Apply
Src. Addres	: 10.90.1.0/24 Ac	quí colocas tu red	local o VLAN		Disable
Src. Por	t:] 🗸 📔	Comment
Dst. Addres	: 192.168.11.0/24	Aquí colocas la red	l local o VLAN del cli	iente	Сору
Dst. Por	t:			•	Remove
Protoco	l: 255 (all)			₹	
	Template				
enabled		Template	Active		

Para completar la configuración vamos al menú **Action** de nuestra política IPSEC. Aquí elegimos el protocolo **esp** y el **proposal** para nuestra fase 2. La encriptación será requerida ya que trabajaremos un túnel seguro esp.

IPsec			
Policies Proposals Groups Peer	rs Identities Profiles Active	Peers Mode Configs Installed S	SAs Keys
🛨 🖃 🖉 Statist	tics		
# Peer Tu	Innel Src. Address	Src. Port Dst. Address	Dst. Port Proto Action
1 Cliente ye	es 10.90.1.0/24	192.168.11.0/24	255 (encrypt
0 *T IPsec Policy <10.90.1	.0/24:0->192.168.11.0/24:0>		
General Action Sta	atus		ОК
Action: end	crypt		▼ Cancel
Level: req	luire		Apply
IPsec Protocols: esp	o		▼ Disable
Proposal: PR	O-IPSEC1		▼ Comment
			Сору
			Remove
enabled	Template	Active	



Paso 6: configuración de regla de NAT

Ahora vamos a aceptar el tráfico de la red local y la red remota. Esta regla debe colocarse en la primera posición para aceptar el tráfico entre las dos redes que vamos a compartir por IPSEC. Sin esta regla no hay tráfico y por eso es muy importante colocarla en el orden correcto.

Primero colocamos la red local(src-address) y luego la red remota(dst-address).

🌽 Quick Set		NAT Rule <10.90.1.0/24->192.168.11.0/24>		
CAPsMAN		General Advanced Extra Action Statistic	s	ОК
Interfaces	Firewall	Chain: srcnat	Ŧ	Cancel
T Wireless	Filter Rules NAT Mangle	Src. Address: 10.90.1.0/24		Apply
💥 Bridge	+ - / x - 7	Dst. Address: 192.168.11.0/24		Disable
	# Action Chain			Comment ut
	> 0	Protocol:		Сору
	1 1 mas srcnat	Src. Port:		Bemove
Pouting		Dst. Port:	•	Poset Countere
System		Any. Port:		
		In. Interface:	•	Reset All Counters
Files		Out. Interface:	-	
		In. Interface List:] 🗸	

Debemos repetir estos pasos en el cliente teniendo en cuenta que intercambiaremos las redes locales y remotas. Lo demás es igual. Tras completar los pasos vamos a tener un túnel establecido completamente.

IPsec Policy <10.90.1.0/24:0->192.168.11.0/24:0>	
General Action Status	ОК
PH2 Count: 1	Cancel
PH2 State: established	Apply
SA Src. Address: 155.138.164.46	Disable
SA Dst. Address: 45.77.219.87	Comment
	Сору
	Remove
enabled Template Active	



Paso 7: Probar la conexión entre las redes via IPSEC.

Como realizaremos la prueba desde nuestro propio router, debemos especificar nuestro src-address, simulando un ping desde la IP 10.90.1.1. Si no lo hacemos así, el router intentará realizar un ping por la ruta por defecto.

Terminal	
[Tab]	Completes the command/word. If the input is ambiguous, a second [Tab] gives possible options
/	Move up to base level
/command	Use command at the base level
[admin@SERVER-V	PN] > ping 192.168.11.1 src-address=10.90.1.1
SEQ HOST	SIZE TTL TIME STATUS
0 192.168.1	1.1 56 64 22ms
1 192.168.1	1.1 56 64 21ms
2 192.168.1	1.1 56 64 22ms
3 192.168.1	1.1 56 64 21ms
4 192.168.1	1.1 56 64 22ms
5 192.168.1	1.1 56 64 21ms
6 192.168.1	1.1 56 64 21ms
7 192.168.1	1.1 56 64 22ms
8 192.168.1	1.1 56 64 21ms
9 192.168.1	1.1 56 64 21ms
10 192.168.1	1.1 56 64 21ms
11 192.168.1	1.1 56 64 21ms
sent=12 rec	eived=12 packet-loss=0% min-rtt=21ms avg-rtt=21ms max-rtt=22ms
[admin@SERVER-V	PN] >

Cabe destacar que en IPSEC no utilizamos enrutamiento. Las rutas se comparten en el IPSEC Policy.