

Laboratorio: Configuración de IPsec Server Xauth PSK

Objetivo: Configurar un VPN IPsec server Xauth PSK para Roadwarriors





CONFIGURACIÓN DE LA FASE 1

 Paso 1: Vamos a crear un pool de IPs con el rango que ustedes prefieran. Este pool será utilizado para asignarle a cada cliente conectado.En mi caso, utilizaré 10.5.6.2-10.5.6.10.

IP Pool <xauth></xauth>										
Name: XAut	h		OK							
Addresses: 10.5.	6.2-10.5.6.10	•	Cancel							
Next Pool: none	₹.	▲	Apply							
			Comment							
			Сору							
			Remove							

Paso 2: Vamos a la menú IP-IPsec, una vez allí vamos a la pestaña Mode
 Configs y le damos al boton de + . Una vez pulsado nos saldrá un una ventana en la cual configuraremos los siguientes parámetros.

Name: Nombre el modo de configuración.

Address Pool: Pool de direcciones creado anteriormente.

Split Include: Redes a las cuales nuestros clientes tendrán acceso. System DNS: Añade los DNS existente a nuestros clientes una vez se conecten.

IPsec									
Policies Propos	als Groups	Peers	Identities	Profiles	Active Peers	Mode Confi	igs Installed SAs	Keys	
+ - 7									
Name	∆ Respo	Addres	s Pool	Addre	ss	Address Pre	fi Split Include		System D
XAUTH	yes	XAuth					24 10.90.1.0/24		yes
* reques IPsec N	lode Config <	XAUTH	>						
	Nam	e: XAL	JTH				ОК		
	L L	> 🗸 F	lesponder				Cancel		
	Address Po	ol: XAu	ith			₹▲	Apply		
	Addres	s:				_	Сору		
Addres	s Prefix Leng	th: 24					Remove		
	Split Incluc	le: 10.9	0.1.0/24			\$			
	Split DN	S:				•			
		> 🗸 S	ystem DN	S					



 Paso 3: Luego vamos a Groups para crear una plantilla de configuración especial e independiente de cualquier otra configuración. Hacemos click en el signo de + y le ponemos el nombre XAUTH.

IPsec							
Policies Propo	sals Groups	Peers	Identities	Profiles	Activ	e Peers	Mode (
+ - 7							
Name	Δ						
XAUTH							
* default	IPsec Group	<xaut< td=""><td>H></td><td></td><td></td><td></td><td></td></xaut<>	H>				
	Name: 🔀	UTH				OK	
						Cance	1
						Apply	
						Сору	
						Remov	e

• **Paso 4**: Ahora vamos a la pestaña **Profile** para empezar con lo que sera la **fase 1** de nuestro server y configuraremos los siguiente parámetros:

IPsec Profile <xauth> Name IPSEC1 Xauth default Incryption Algorithms: sha1 icancel Encryption Algorithm: des icancel icanel<th>Policies</th><th>Propo</th><th>sals</th><th>Groups</th><th>Peers</th><th>Identities</th><th>Profiles</th><th>Active Peers</th><th>Mode (</th><th>Configs</th><th>Installed SA</th></xauth>	Policies	Propo	sals	Groups	Peers	Identities	Profiles	Active Peers	Mode (Configs	Installed SA
Name Name: Xauth IPSEC1 Kauth Xauth IHash Algorithms: default Encryption Algorithm: default ecryption ecryption Algorithm: des default ecryption ecryption ecryption camellia-128 camellia-192 camellia-256 DH Group: DH Group: modp768 modp1024 ecryption ecryption ecryption modp3072 modp4096 modp6144 modp8192 ecryption ecryption Lifebytes: v VAT Traversal DPD Interval: DPD Interval: 120 proposal Check: s	+ -	7	IPsec	c Profile <>	Kauth>						
Xauth Hash Algorithms: sha1 Cancel Image: Hash Algorithms: des 3 des Apply Image: Encryption Algorithm: des 3 des Image: I	Name IPSEC	1			Nam	ne: Xauth					ОК
Certaint Encryption Algorithm: des 3 des Apply aes-128 aes-192 Copy aes-256 blowfish Remove camellia-128 camellia-192 camellia-192 camellia-128 camellia-192 camellia-192 camellia-256 DH Group: modp768 modp1024 DH Group: modp768 modp1024 modp1024 ec2n155 ec2n185 modp4096 modp6144 modp8192 ecp521 Proposal Check: obey Lifetime: 1d 00:00:00 Lifebytes: NAT Traversal DPD Interval: 120 s DPD Maximum Failures: 5 Image: Simple state stat	Xauth			Hash A	lgorithn	ns: sha1			+	0	Cancel
Image: Section of the seccccccccccccccccccccccccccccccccccc	derault		E	incryption	Algorith	m: 🔄 des		3des			Apply
aes-256 blowfish Remove camellia-128 camellia-192 camellia-256 DH Group: modp768 DH Group: modp768 modp1024 ec2n155 ec2n185 modp1536 modp2048 modp6144 modp8192 ecp256 ecp384 ecp521 Proposal Check: obey V NAT Traversal V DPD Intervat: 120 DPD Maximum Failures: 5					5	> ▼ aes-	128	aes-192			Сору
□ camellia-128 □ camellia-192 □ camellia-256 DH Group: modp768 □ modp768 □ modp1024 □ ec2n155 □ ec2n185 □ modp1536 modp2048 □ modp6144 modp8192 □ ecp256 □ ecp384 □ ecp521 Proposal Check: Proposal Check: obey □ Lifebytes: ▼ □ PD Interval: 120 □ PD Maximum Failures: 5						aes-2	256	blowfish		R	emove
camellia-256 DH Group: modp768 modp1024 ec2n155 ec2n185 modp1536 modp3072 modp6144 modp8192 ecp256 ecp384 ecp521 Proposal Check: obey ifetime: 1d 00:00:00 ifetime: 1d 00:00:00 ifebytes: VNAT Traversal DPD Interval: 120 S DPD Maximum Failures: 5						came	ellia-128	camellia-	192		
DH Group: modp768 ✓ modp1024 ec2n155 ec2n185 modp1536 modp2048 modp3072 modp4096 modp6144 modp8192 ecp256 ecp384 ecp521 ✓ Proposal Check: obey Lifetime: 1d 00:00:00 Lifebytes: ✓ DPD Interval: 120 DPD Maximum Failures: 5						came	ellia-256				
Image: state sta				[)H Grou	ıp: 🗌 mod	p768	✓ modp1024			
3 items modp1536 modp2048 modp3072 modp4096 modp6144 modp8192 ecp256 ecp384 ecp521 Proposal Check: obey Lifetime: 1d 00:00:00 Lifebytes: • DPD Interval: 120 • DPD Interval: 5						ec2n	155	ec2n185			
3 items modp3072 modp4096 modp6144 modp8192 ecp256 ecp384 ecp521 Proposal Check: obey Lifetime: 1d 00:00:00 Lifebytes: NAT Traversal DPD Interval: 120 F DPD Maximum Failures: 5						mod	p1536	modp2048			
3 items modp6144 modp8192 ecp256 ecp384 ecp521 Proposal Check: obey Lifetime: 1d 00:00:00 Lifebytes: NAT Traversal DPD Interval: 120 F DPD Maximum Failures: 5						mod	p3072	modp4096			
3 items ecp256 ecp384 ecp521 Proposal Check: obey ▼ Lifetime: 1d 00:00:00 ▼ Lifebytes: ▼ Image: Comparison of the com	0.11					mod	p6144	modp8192			
ecp521 Proposal Check: obey	5 items					ecp2	56	ecp384			
Proposal Check: obey						ecp5	21				
Lifetime: 1d 00:00:00 Lifebytes: V NAT Traversal DPD Interval: 120 V S DPD Maximum Failures: 5				Propos	sal Che	ck: obey			₹		
Lifebytes: NAT Traversal DPD Interval: 120 DPD Maximum Failures: 5					Lifetim	ne: 1d 00:0	0:00				
DPD Interval: 120 Traversal DPD Maximum Failures: 5					Lifebyte	es:			•		
DPD Interval: 120 To s DPD Maximum Failures: 5						▼ NAT	Traversal				
DPD Maximum Failures: 5				DP	D Interv	al: 120			▼ S		
			DPE) Maximun	n Failure	es: 5					



 Paso 5: Ahora vamos a la pestaña Peer para asignar el perfil y colocar las direcciones que permitimos conectar a nuestro VPN:

Nombre = Remotos: Es un identificador de los clientes a conectar.
 Address = 0.0.0.0/0: Para establecer la negociación con cualquier dirección que solicite. Al completar este paso se visualizará ::/0 como en la imagen.
 Passive= yes: Esto nos sirve para que nuestro túnel se mantenga a la espera de un tráfico inicial.

Exchange Mode = Main: Es nuestro intercambio inicial de llaves IKEv1 en modo Main. Luego de completar el laboratorio vamos a cambiar a IKEv2

IPsec									
Policies Proposals Groups Peers Identi	ties Profiles Active Peers	Mode Configs Ir							
IPsec Peer <remotos></remotos>									
Name: Remotos		ОК							
Address: ::/0	▲	Cancel							
Port:	•	Apply							
Local Address:	▼	Disable							
Profile: Xauth	•	Comment							
Exchange Mode: main	₹	Сору							
✓ Passive		Remove							
✓ Send INITIAL_CONTACT									
enabled	responder								



• Paso 6: Vamos a Identities configuraremos los siguientes parámetros:

Peer: Seleccionamos creado en el paso anterior llamado Remotos Auth Method: Seleccionamos el modo de autorización pre shared key xauth Secret: Es el secret IPSEC general

Username: Es el usuario que configuraremos en el cliente para conectarnos **Password:** Contraseña para el usuario anterior.

Mode Configuration: Seleccionamos el modo de configuración XAUTH Generate Policy: Port strict

IPs	ec				
Po	olicies Proposals Grou	ps Peers Iden	tities Profiles	Active Pee	ers Mode Configs
÷	- 🗸 🗠 🦷	Settings			
#	Peer	Auth. Method	Username	Remote	ID Mode
	IPsec Identity <remotos< th=""><th>></th><th></th><th></th><th></th></remotos<>	>			
	Peer:	Remotos		₹	ОК
	Auth. Method:	pre shared key x	auth	Ŧ	Cancel
	Secret:	Cano.123			Apply
	Username:	Cano			Disable
	Password	Cano 123			Comment
					Сору
	Policy Template Group:	default		₹	Remove
	Notrack Chain:			₹	
	My ID Type:	auto		₹	
2 if	Remote ID Type:	auto		₹	
	Match By:	remote id		₹	
	Mode Configuration:	XAUTH	•	F 🔺	
	Generate Policy:	port strict		Ŧ	
	enabled				





CONFIGURACIÓN DE LA FASE 2

• Paso 7: Vamos a configurar el Proposals con los siguientes algoritmos de autenticación, encriptación, lifetime y PFS group.

IPse									
Po	licies	Proposals	Groups	Peers	Identities	Profiles	Activ	ve Peers	Mode Cor
÷	-	× × .	T						
	IPse	c Proposal <	Xauth>						
		Name	: Xauth					C	ĸ
* (Aut	h. Algorithms	s: 🔄 md5		sha1			Car	ncel
			null		sha256			Ар	ply
			sha5	512				Dis	able
	End	r. Algorithms	s: 🗌 null		des			Co	
			3des	;	🖌 aes-	128 cbc		Ren	nove
			aes-	192 cbc	aes-	256 cbc			
			blow	fish	twof	ish			
			came	ellia-128	cam	ellia-192			
			came	ellia-256	aes-	128 ctr			
3 ite			aes-	192 ctr	aes-	256 ctr			-
			aes-	128 gcm	aes-	192 gcm			
			aes-	256 gcm	1		_		
		Lifetime	e: 00:30:0	0			▲		
		PFS Group	none				₹		
	enat	bled							



• Paso 8: Nos dirigimos a la pestaña Policies. Lo primero que debemos hacer es dar click en Template, luego veremos la configuración como la imagen.

El **Src. Address:** 0.0.0.0/0 representa cualquier dirección entrante, ya que nuestros clientes se conectarán desde cualquier IP pública.

El **Dst. Address**: será el rango del pool designado para nuestra VPN. Al conectarse el cliente, vamos a recibir una de estas IPs del pool.

Por último, agregamos el Group XAUTH creados por nosotros anteriormente.

IPsec											
Policies Proposals Groups Peers Identities Profiles Active Peers Mode	Configs	Installed SA									
🛨 🗕 🖌 🗶 🖾 🍸 Statistics											
# Door Tumpel Cro. Addresso Cro. Dott Addresso I IPsec Policy <0.0.0.0/0:0->10.5.6.0/24:0> I											
General Action Status	0	ĸ									
Src. Address: 0.0.0.0/0	Can	cel									
Src. Port:	Ар	ply									
Dst. Address: 10.5.6.0/24	Disa	ble									
Dst. Port:	Comr	nent									
Protocol: 255 (all)	Со	ру									
Template	Rem	ove									
Group: XAUTH											
enabled Template Active											

Hacemos click en Action para configurar el resto



• **Paso 9:** Aquí vamos a seleccionar la acción de encriptar con el proposal creado y como protocolo IPSEC elegimos ESP para mejor seguridad.

IPsec										
Policies Proposals Groups Peers Identities Profiles Active Peers Mod	le Configs Installed S									
F - V X C Y Statistics										
# Dear Turnel Cro. Address / Cro. Best Det Address IPsec Policy <0.0.0/0:0->10.5.6.0/24:0> IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII										
General Action Status	ОК									
Action: encrypt	Cancel									
IPsec Protocols: esp	Apply									
Proposal: Xauth	Disable									
	Comment									
	Сору									
	Remove									
a enabled Template Active										

- Paso 10: Configurar un cliente para este VPN en su celular.
 Para crear el cliente debe ir al menú de VPNs y elegir IPSEC XAUTH.
 Aquí debe configurar con los siguientes parámetros:
 - IP Pública de su servidor IPSEC
 - Secret del IPSEC
 - Usuario
 - Contraseña

Al completar, vamos a active peers y probamos tráfico a la red que ha permitido en el túnel VPN. La mía ha sido 10.90.1.0/24. Prueba haciendo Ping a la VLAN tuya.

IPsec												
Policies	Proposals	Groups	Peers	Identities	Profiles	Active Peers	Mode Configs	Installed SAs	Keys			
- 7	Kill Conne	ections									Fin	d
ID	State	e	Local	Address	Remo	te Address	Dynamic Address	Side	Uptime	F	H2 Total	T₂▼
	esta	blished	155.1	38.164.46	45.77.	219.87	0.0.0.0	responder		00:17:24		
Cano	esta	blished	155.1	38.164.46	148.1	03.138.84	10.5.6.7	responder		00:00:26		1
•												•
2 items												

Laboratorio IPSEC y clientes XAUTH – Canó Academy 2020. RouterOS: 6.47.1