

Data Security Firewall

How to configure L2TP over IPSec on your firewall

How to configure L2TP over IPSec on your firewall

This section contains information about the parameters required to define the VPN tunnel.

Default Policy will by default be pre-configured with factory settings. You'll have to create a new policy for L2TP.

1. L2TP VPN Policy Settings

Go to VPN --> IPSec --> Policy

GAJSHIELD	D						🐥 陆 DSF Dashboard Da	chibeard Wicard Repo				
Definitione 4												
Configuration 4	Policy Tunnels VPN Failover Gro	oup Local IPsec Key Reserved IPs Advanced Setup	Restart VPN									
Management 4		Add Policy VEB Boley										
Discussion of	VPN Policy											
Unagnosia •	Policy Name*			12tp								
Firewall 4	Allow Re-keying*			🖲 Yes 💿 N	10							
VPN >	Key Negotiation Tries*			3	0 (0 means infinite	key negotiation retries)						
Psec ISL VPN 2TP	Pass Data In Compressed Format ^a			O Yes 🔍 🖲 N	lo							
PTP ocal User	Phase 1											
Enterprise Cloud	Encryption Algorithm*	3DES	v	Authentication Algorithm*		MD5	~					
AntiSpam	Encryption Algorithm	3DES	-	Authentication Algorithm		SHA1	-					
APP Filtor	Encryption Algorithm	3DES	~	Authentication Algorithm		SHA1	~					
DLP 4												
Beporta 4	DH Group*			1 2 3 2 14 15 16	5							
	Key Life*			3600	Seconds							
Browsing 4	Rekey Margin*			120	Seconds							
PS	Randomize Re-Keying Margin By*			0	96							
ogout	Enable Dead Peer Detection				0							
	Check Peer After Every				Seconds							
	Wait For Response Upto				120 Seconds							
	Action When Peer Is Not Active											
	Phase 2											
	Encryption Algorithm*	3DES	~	Authentication Algorithm*		MD5	~)					
	Encryption Algorithm	3DES	~	Authentication Algorithm		SHA1	~					
	Encryption Algorithm	3DES	v	Authentication Algorithm		SHA1	v					
	000 0 ······ 8											
	Pro Group*			● None () 1 () 2 () 5 () 14 ()	15 () 16							
	Key Life"			18000	peconds							

Note – Policy configuration is required to setup a L2TP tunnel. You can configure L2TP with both ISPs

2. L2TP VPN Tunnel Configuration

Go to VPN --> IPSec --> Tunnels

Policy	Tunnels	VPN Failover Group	Local IPsec Key	Reserved IPs	Advanced Setup	Restart V	PN			
						Add Tu	nnel			0
Tunnel Name							L2TPTunnel			
Automatic Fir	ewall Rules:									
Automatic Fir	ewall Rule Lo	gs:								
VPN Details										
Policy						l2tp	~			
Action on Re	start						Passive	~		
VPN Type							L2TP	~		
IKE Version							IKEv1	~		
Local Netwo	rk Details									
Local Server							fwip-WAN	~	<u> </u>	Firewall WAN IP
Gateway of I	ocal Server						GAJSHIELD	~		Gateway of WAN
Local ID							X.509DN	~		Interface
Local ID			Add Tunnel							
Remote Net	wo <mark>rk</mark> Details									
Remote Host							Any	~		
Romoto ID							X.509DN	v		
Kenioce 10										
Authenticati	on Details									
Authenticatio	in Type						Preshared Key	~		
Remote Certificate										
Descharadiv										
Presnared K	IZp on Restart pe pe ision restore Revork Details erer o o factore sprear (GASHIELD o o o ce Network Details e Network Details a lo o e Network Details e Retwork Details e Control									
Save	Cance	el								

Note- You'll have to select L2TP in VPN type option since the configuration is L2TP over IPSec.

3. L2TP Configuration

Go to VPN -> L2TP -> L2TP Options

E GAJS	HIELD	9	La 20 22 E 2 € Difumbourd Databourd Databourd Based The
2* Definitions			
Configuration		L2TP Options Restart L2TP	-
A Management	4		Add L2TP Option (2)
		Server Name	Iztp
Q Diagnosis	٩	Server IP	fwip-LAN ~
Firewall	- 4		Start IP:
-		IP Pappa	192.168.5.12
VPN ·		, nonge	End IP:
IPsec SSI VPN			11.121.120
LZTP	Local IP	192.168.2.167 Firewall LAN IP	
PPTP Local User		Authentication Type	Local
Enterprise Clo	Enterprise Cloud		Primary DNS Server:
		DNE Server (Optional)	8.8.8.8
AntiSpam		Dive Server (Optional)	Secondary DNS Server:
Y APP Filter			4.2.2.2
			Primary WINS Server:
Ø, DLP	Ø, DLP 4	WINS Server (Optional)	Consider WINE Constr.
B Reports	1		אישע איז
Browsing	4	Save Cancel	
A IPS			
G Logout			

Specify the following fields:

Server IP: Public IP of Firewall.

IP Range: When Users connect through VPN, that time users get the IP address from the above defined range.

Local IP: Firewall local LAN IP.

	L2TP Options R	estart L2TP									
Sea	Irch in All	✓ for		۹						6	900
	Server Name 11	Server IP ↓↑	Start IP ↓†	End IP ↓↑	Local IP ↓↑	Authentication Type 1	Primary DNS Server $\downarrow \uparrow$	Secondary DNS Server 11	Primary WINS Server ↓↑	Secondary WINS Server ↓↑	Tasks
	12tp	fwip-LAN	192.168.5.12	192.168.5.16	192.168.2.167	Local	8.8.8.8	4.2.2.2			\$
	Delete										

4. Create a VPN User

Go to VPN -> Local User -> VPN Users

≡	GAJSHIEL	_D	elp
ß	Definitions		_
	Configuration	VPN Users	
		Add VPN User Settings (2)	
-	Management	Username test	
۹	Diagnosis	Pasword	
•	Firewall	Confirm Password	
1	* VPN	Local N/w IP (Optional) 192.168.2.200	
	IPsec SSL VPN	Save Cancel	
	L2TP		
	Local User		
٩	Enterprise Cloud		
8	AntiSpam		
т	APP Filter		
۵.	DLP		
в	Reports		
	Browsing		
6	IPS		
64	Logout		

You can create a new user or modify an existing VPN user

VPN Users										
Search in All	✓ for Q.		•00							
	Username ↓↑	Local N/w IP (Optional)	Tasks							
	test	192.168.2.200	夺 亩							
Delete										

5. Rules for L2TP VPN Go to Firewalls -> Policies -> Rules

JSHIELD)												DSF Dashboard	Cashboard	Ward H	6	2
ns 4		_															
ion 🔅 斗		Rules	Port Forv	varding DoS Settings	MAC Binding	MAC Filtering	Install Policies										
4		Group Search	1	All Rules v Zone	All	✓ To All	~ D	Hide Inactive R	ules							•?	0
4		Rule No.	IP Version	Direction	Source	Destination	Service	User Sense	Users and Groups	Action	Schedule	Policies	QoS		Tasks		
							CI	IS Exception	on Firewall Rule	s							
								No Rec	cords Found								
								Global Pre	Firewall Rules								
							This Firmwa	re Version is n	ot Compatible with CN	IS Global							
					NAC Diament NAC Statemant Totala Position *Section NAC Statemant Totala Position Nace Nace												
								No Rei	cords Found								
								Local Fi	ewall Rules								
		1	IPv4	LAN to LAN	fwnel-LAN	twip-LAN	GajAccess	no		accept	AllTime				¢ 90)	(🖞 🗘	
ЧС.		2	IPv4	Any to Any	twip-LAN	ADServer	AD			accept	AllTime				¢ ₽₀ \$	(to \$	
•		3	IPv4	WAN to LAN	Any	twip-WAN J GAJSHIELD	Remote-Login			accept	AllTime				¢ 90 \$	《 団 ¢	
4		4	IPv4	Any to Any	snmpserver	fwnet-LAN	srimp			accept	AllTime				¢ 901	< ± ¢	
		5	IPv4	LAN to Any	twnet-LAN	Any	smtp-virus-spam-scan			accept	AllTime				¢ -	< to \$	
		6	IPv4	Any to Any	cloudnetwork	internet	Browse		-	accept	blockonofficehr	Uri Filter Policy: blockinotticehrs SSL Deep Inspect: on	Route Failove	er: GLOBAL	¢ @	4 m ¢	
		7	IPv4	WAN to WAN	Any L Loopback NAT	twip-WAN ↓ GAJSHIELD	GajAccess	no		accept	AlTime				¢ 🔁	(m ¢	
	0	8	IPv4	WAN to Any	Any	twip-WAN I GAJSHIELD	GajAccess	no	5	accept	AlTime				¢ ¶o \$	(th ¢	
		9	IPv4	Any to Any	internet	fwnet-WAN	12tp		-3	accept	AllTime	-	-		¢ ₽₀ 3	< to \$	
		10	IPv4	Any to Any	GAJSHIELD	twip-LAN	Any			accept	AllTime				¢ 10	< 10 ¢	
		11	IPv4	Any to Any	test1	fwnet-LAN	Any			accept	AllTime				¢ 001	< to \$	
		12	IPv4	LAN Zone to INTERNET Zone	Minel-LAN	Any	Browse	yes	testgroup	accept	Arnme	Un Filter Policy: Open SSL Deep Inspect: off	*		₽ 40)	0	
		13	IPv4	LAN Zone to INTERNET Zone	twnet-LAN	Any	Browse	no		accept	AlTime	Uri Filter Policy: blockinofficehrs SSL Deep Inspect: off			¢ 🔁	2	

Configure the 3 rules as specified above.

NOTE: If a user has 2 ISPs, he'll have to configure 2 tunnels, second time with the second ISP as the destination. (If user wants to configure L2TP with both the ISPs)