

How to Configure IPSec VPN on your Firewall



TABLE OF CONTENTS

- VPN Policy..... 3
- VPN Policy Settings..... 3
- VPN Tunnel Details..... 4
- VPN Tunnel Configuration..... 4
- Required Rules for VPN Connectivity..... 5

How to Configure IPsec VPN on your Firewall

In this document, we are going to understand the steps to configure Site-to-Site VPN using pre-shared Key



The following steps need to be followed to configure Site to Site VPN using pre shared key.

- Creation of Policy
- Creation of Tunnel
- Required to add Rules
- Restart VPN Service

VPN Policy

Policy Tunnels VPN Failover Group Local IPsec Key Reserved IPs Advanced Setup Restart VPN

Search in All for

<input type="checkbox"/>	Policy Name ↓↑	Allow Re-keying ↓↑	Key Negotiation Tries ↓↑	Pass Data In Compressed Format ↓↑	Encryption Algorithm ↓↑	Authentication Algorithm ↓↑	Encryption Algorithm ↓↑	Authentication Algorithm ↓↑	Tasks
<input type="checkbox"/>	Default	y	3	n	3DES	MD5	3DES	MD5	 

Delete

This section contains information about parameters required to define VPN Tunnels. Default Policy will come with factory settings. If you want you can create your own policy.

VPN Policy Settings

Policy Tunnels VPN Failover Group Local IPsec Key Reserved IPs Advanced Setup Restart VPN

Add Policy

VPN Policy

Policy Name* IPsec

Allow Re-keying* Yes No

Key Negotiation Tries* 3 (0 means infinite key negotiation retries)

Pass Data In Compressed Format* Yes No

Phase 1

Encryption Algorithm* 3DES Authentication Algorithm* MD5

DH Group* 1 2 5 14 15 16

Key Life* 3600 Seconds

Rekey Margin* 120 Seconds

Randomize Re-Keying Margin By* 0 %

Enable Dead Peer Detection

Check Peer After Every 60 Seconds

Wait For Response Upto 600 Seconds

Action When Peer Is Not Active Restart

Phase 2

Encryption Algorithm* 3DES Authentication Algorithm* MD5

PFS Group* None 1 2 5 14 15 16

Key Life* 28800 Seconds

Save Cancel

Note - This is default Policy Configuration required to setup an IPSec Tunnel

VPN Tunnel Details

Policy	Tunnels	VPN Failover Group	Local IPsec Key	Reserved IPs	Advanced Setup	Restart VPN						
Search in All for <input type="text"/>							⊕ ? ⓘ					
<input type="checkbox"/>	Tunnel Name	Action on Restart	Policy	VPN Type	Local Server	Gateway of Local Server	Local Internal Network	Remote Host	Remote Internal Network	Authentication Type	Status	Tasks
No records found												

VPN Tunnel Configuration

Add Tunnel ⓘ					
Tunnel Name	<input type="text" value="Test"/>				
Automatic Firewall Rules:	<input type="checkbox"/>				
Automatic Firewall Rule Logs:	<input type="checkbox"/>				
VPN Details					
Policy	IPsec				
Action on Restart	Active				
VPN Type	IPSec				
IKE Version	IKEv1				
Local Network Details					
Connection Type	Net to Net				
Local Server	fwip-WAN				
Gateway of Local Server	WAN_GW				
Local Internal Network	<table border="1"><tr><td>Available Local Internal Network</td><td>Selected Local Internal Network</td></tr><tr><td>ADServer CCTV_IP GAJSHIELD Sourabh WAN_GW fwip-Airtel fwip-DMZ fwip-LAN fwip-WAN</td><td>fvnet-LAN</td></tr></table>	Available Local Internal Network	Selected Local Internal Network	ADServer CCTV_IP GAJSHIELD Sourabh WAN_GW fwip-Airtel fwip-DMZ fwip-LAN fwip-WAN	fvnet-LAN
Available Local Internal Network	Selected Local Internal Network				
ADServer CCTV_IP GAJSHIELD Sourabh WAN_GW fwip-Airtel fwip-DMZ fwip-LAN fwip-WAN	fvnet-LAN				
Local ID	X.509DN				
Remote Network Details					

Policy		Tunnels	VPN Failover Group	Local IPsec Key	Reserved IPs	Advanced Setup	Restart VPN			
Local ID	X.509DN									
Remote Network Details										
Remote Host	Remote StaticIP									
Remote Internal Network	<table border="1"><tr><td>Available Remote Internal Network</td><td>Selected Remote Internal Network</td></tr><tr><td>fwip-Airtel fwip-DMZ fwip-LAN fwip-WAN fvnet-LAN internet fvnet-DMZ fvnet-Airtel fvnet-WAN</td><td>Remote_Network</td></tr></table>						Available Remote Internal Network	Selected Remote Internal Network	fwip-Airtel fwip-DMZ fwip-LAN fwip-WAN fvnet-LAN internet fvnet-DMZ fvnet-Airtel fvnet-WAN	Remote_Network
Available Remote Internal Network	Selected Remote Internal Network									
fwip-Airtel fwip-DMZ fwip-LAN fwip-WAN fvnet-LAN internet fvnet-DMZ fvnet-Airtel fvnet-WAN	Remote_Network									
Remote ID	X.509DN									
Authentication Details										
Authentication Type	Preshared Key									
Remote Certificate	Enable Xauth: <input type="checkbox"/>									
Preshared Key	Show Preshared Key: <input type="checkbox"/>									
<input type="button" value="Save"/> <input type="button" value="Cancel"/>										

Required Rules for VPN Connectivity

Rules Port Forwarding DoS Settings MAC Binding MAC Filtering Install Policies

Rule No.	IP Version	Direction	Source	Destination	Service	UserSense	Users and Groups	Action	Schedule	Policies	QoS	Tasks
1	IPv4	WAN to WAN	fwip-WAN	Remote_StaticIP	IPSec-VPN		-	accept	AllTime	-	-	} VPN Connectivity
2	IPv4	WAN to WAN	Remote_StaticIP	fwip-WAN	IPSec-VPN		-	accept	AllTime	-	-	
3	IPv4	LAN to Any	fwnet-LAN ↓ No NAT	Remote_Network	Any		-	accept	AllTime	-	-	} VPN Access
4	IPv4	Any to LAN	Remote_Network	fwnet-LAN	Any		-	accept	AllTime	-	-	

Rule No 1 and 2 are for VPN Connectivity.

Rule No 3 and 4 are for Access of Lan. Once all the Configuration is done do restart VPN by going to VPN > IPSec > Restart VPN.

Thus, we have successfully configured IPSec VPN on your firewall.