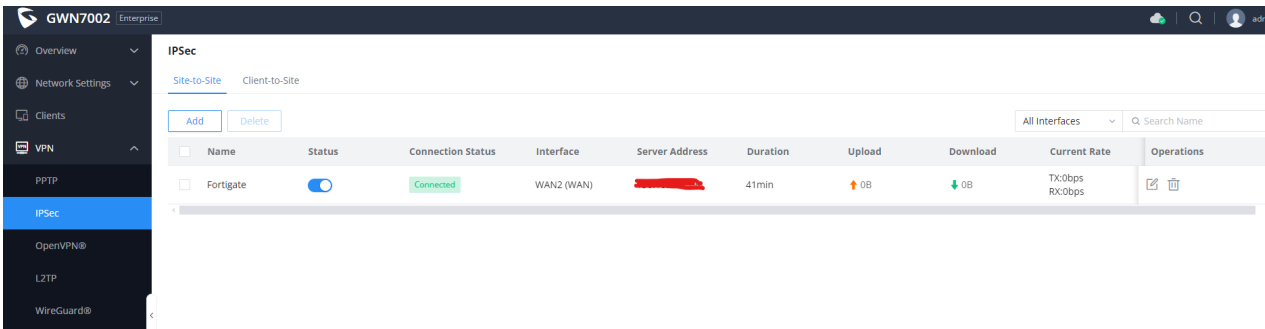
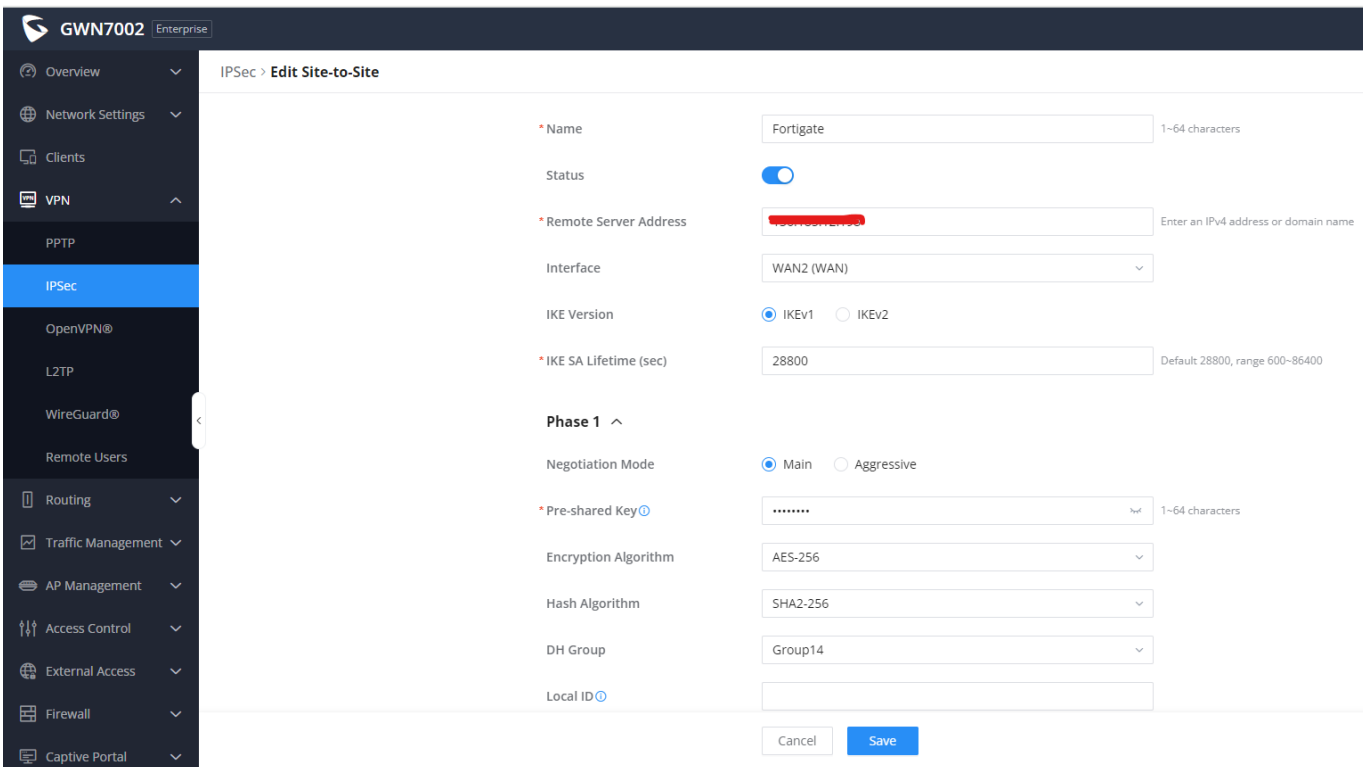


How to configure IPSec VPN Site-to-Site in Grandstream GWN700X router and Fortigate



IPSec										
Site-to-Site Client-to-Site										
Add Delete All Interfaces Search Name										
<input type="checkbox"/>	Name	Status	Connection Status	Interface	Server Address	Duration	Upload	Download	Current Rate	Operations
<input type="checkbox"/>	Fortigate	<input checked="" type="checkbox"/>	Connected	WAN2 (WAN)	[REDACTED]	41min	↑ 0B	↓ 0B	Tx:0bps Rx:0bps	Edit Delete

Step 1: create a IPSec Site-to-Site in GWN700x



IPSec > Edit Site-to-Site

* Name: Fortigate 1~64 characters

Status: ☒

* Remote Server Address: [REDACTED] Enter an IPv4 address or domain name

Interface: WAN2 (WAN)

IKE Version: ☒ IKEv1 ☐ IKEv2

* IKE SA Lifetime (sec): 28800 Default 28800, range 600~86400

Phase 1 ^

Negotiation Mode: ☒ Main ☐ Aggressive

* Pre-shared Key: 1~64 characters

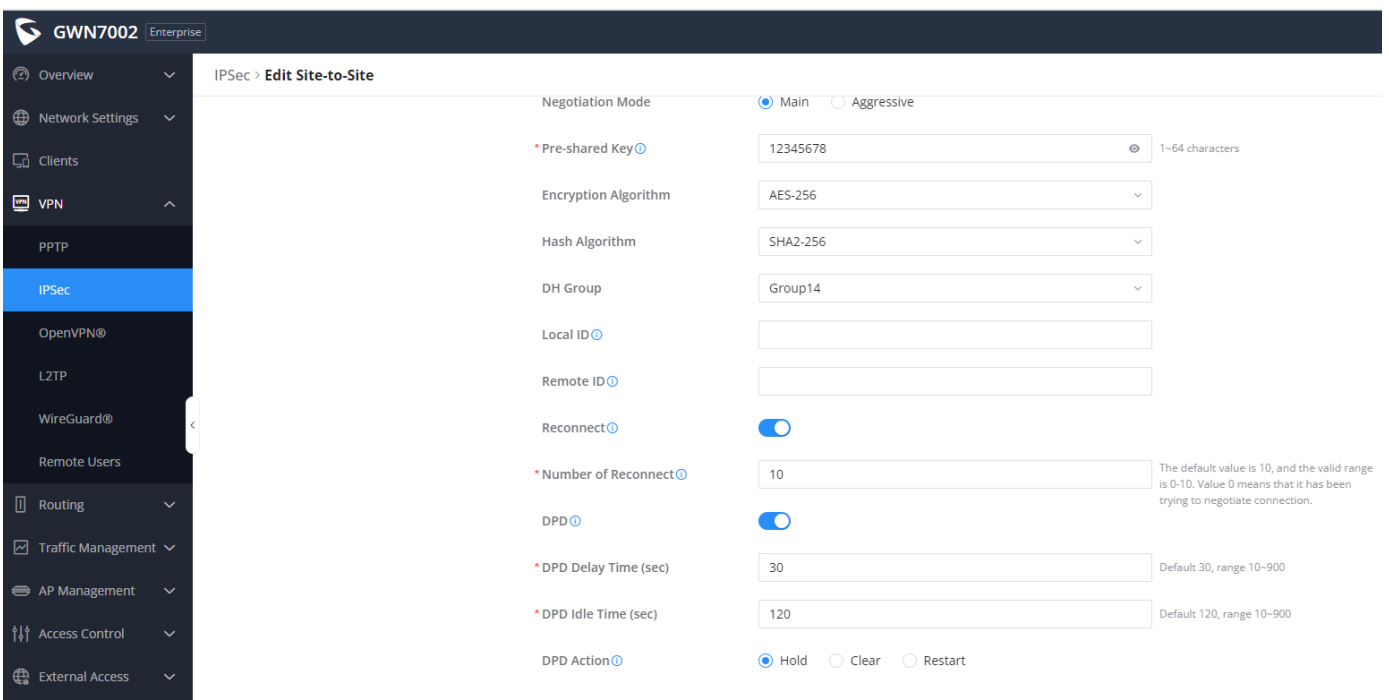
Encryption Algorithm: AES-256

Hash Algorithm: SHA2-256

DH Group: Group14

Local ID:

[Cancel](#) [Save](#)



IPSec > Edit Site-to-Site

Negotiation Mode: ☒ Main ☐ Aggressive

* Pre-shared Key: 12345678 1~64 characters

Encryption Algorithm: AES-256

Hash Algorithm: SHA2-256

DH Group: Group14

Local ID:

Remote ID:

Reconnect: ☒

* Number of Reconnect: 10 The default value is 10, and the valid range is 0-10. Value 0 means that it has been trying to negotiate connection.

DPD: ☒

* DPD Delay Time (sec): 30 Default 30, range 10-900

* DPD Idle Time (sec): 120 Default 120, range 10-900

DPD Action: ☒ Hold ☐ Clear ☐ Restart

← → ↻ Not secure https://192.168.180.1/#/vpn/ipsec

GWN7002 Enterprise

Overview

Network Settings

Clients

VPN

PPTP

IPSec

OpenVPN®

L2TP

WireGuard®

Remote Users

Routing

Traffic Management

AP Management

Access Control

External Access

Firewall

IPSec > Edit Site-to-Site

DPD Action ⓘ
☒ Hold ☐ Clear ☐ Restart

Phase 2 ^

* Local Subnet ⓘ
192.168.180.0 / 24 + +

* Local Source IP Address ⓘ
192.168.180.1

* Remote Subnet ⓘ
172.16.10.0 / 24 + +

* IPSec SA Lifetime (sec)
3600 Default: 3600, range 600-86400

Security Protocol
☒ ESP

ESP Encryption Algorithm
AES-256

ESP Hash Algorithm
SHA2-256

Encapsulation Mode
☒ Tunnel Mode

PFS Group
Disabled

Cancel

Save

Step 2: Create a IPSec Tunnel at the Fortigate

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

+ Create New

Edit

Delete

Show Matching Logs

Search

Tunnel	Interface Binding	Status	Ref.
Custom 1			
Sathish	wan	Up	4

<div><div>Dashboard</div><div>Network</div><div>Policy & Objects</div><div>Security Profiles</div><div>VPN</div><div>Overlay Controller VPN</div><div>IPsec Tunnels</div><div>IPsec Wizard</div><div>IPsec Tunnel Template</div><div>SSL-VPN Portals</div><div>SSL-VPN Settings</div><div>SSL-VPN Clients</div><div>VPN Location Map</div><div>User & Authentication</div><div>WiFi & Switch Controller</div><div>System</div><div>Security Fabric</div><div>Log & Report</div></div>	<div><div>+ Create New</div><div>Edit</div><div>Delete</div><div>Show Matching Logs</div><div>Search</div><div>Q</div></div> <table><tr><th>Tunnel</th><th>Interface Binding</th><th>Status</th><th>Ref.</th></tr><tr><td>Custom 1</td><td></td><td></td><td></td></tr><tr><td>Sathish</td><td>wan</td><td>Up</td><td>4</td></tr></table>	Tunnel	Interface Binding	Status	Ref.	Custom 1				Sathish	wan	Up	4	<div><div>Edit VPN Tunnel</div><div>Name Sathish</div><div>Comments Comments</div><div>Network</div><div>IP Version IPv4</div><div>Remote Gateway Static IP Address</div><div>IP Address 192.168.180.1</div><div>Interface wan</div><div>Local Gateway <input type="checkbox"/></div><div>Mode Config <input type="checkbox"/></div><div>NAT Traversal <input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable <input type="checkbox"/> Forced</div><div>Keepalive Frequency 10</div><div>Dead Peer Detection <input type="checkbox"/> Disable <input checked="" type="checkbox"/> On Idle <input checked="" type="checkbox"/> On Demand</div><div>DPD retry count 3</div><div>DPD retry interval 20 s</div><div>Forward Error Correction Egress <input type="checkbox"/> Ingress <input type="checkbox"/></div><div>+ Advanced...</div></div>
Tunnel	Interface Binding	Status	Ref.											
Custom 1														
Sathish	wan	Up	4											

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

WiFi & Switch Controller

System

Create New

Edit

Delete

Stats

Tunnel

Custom

Sathish

wan

Edit VPN Tunnel

Comments

Network

Remote Gateway : Static IP Address (210.18.182.103) , Interface : wan

Authentication

Method : Pre-shared Key

Pre-shared Key : 12345678

IKE

Version : 1 2

Mode : Aggressive Main (ID protection)

Phase 1 Proposal

Algorithms : AES256-SHA256

Diffie-Hellman Group : 14

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

WiFi & Switch Controller

System

Security Fabric

Log & Report

Create New

Edit

Delete

Stats

Tunnel

Custom

Sathish

wan

Edit VPN Tunnel

Authentication Method : Pre-shared Key (12345678)

IKE Version : 1 , Mode : Main (ID protection)

Phase 1 Proposal

Algorithms : AES256-SHA256

Diffie-Hellman Group : 14

XAUTH

Type : Disabled

Phase 2 Selectors

Name	Local Address	Remote Address
Sathish	172.16.10.0/255.255.255.0	192.168.180.0/255.255.255.0

Edit Phase 2

Name : Sathish

Comments

Local Address : Subnet 172.16.10.0/255.255.25.25

Remote Address : Subnet 192.168.180.0/255.255.255.

Advanced...

Step 3: Verify the Firewall status

Policy & Objects	Name	Source	Destination	Schedule	Service	Action	VPN	Security Profiles	Log	Bytes
Firewall Policy	lan → Sathish									
Addresses	sathish-vpn	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	840 B
Virtual IPs	Sathish → lan									
IP Pools	sathish-in	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B