



# Application Guide

Fortigate-Hongdian-IPSec Configuration



## Contents

<b>Contents</b> .....	<b>2</b>
<b>Revision History</b> .....	<b>2</b>
<b>1 Overview</b> .....	<b>3</b>
<b>2 Description</b> .....	<b>3</b>
2.1 Test Topology.....	3
2.2 Fortigate Setup.....	3
2.3 Hongdian Setup.....	7
2.4 Check Ping.....	9

## Revision History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

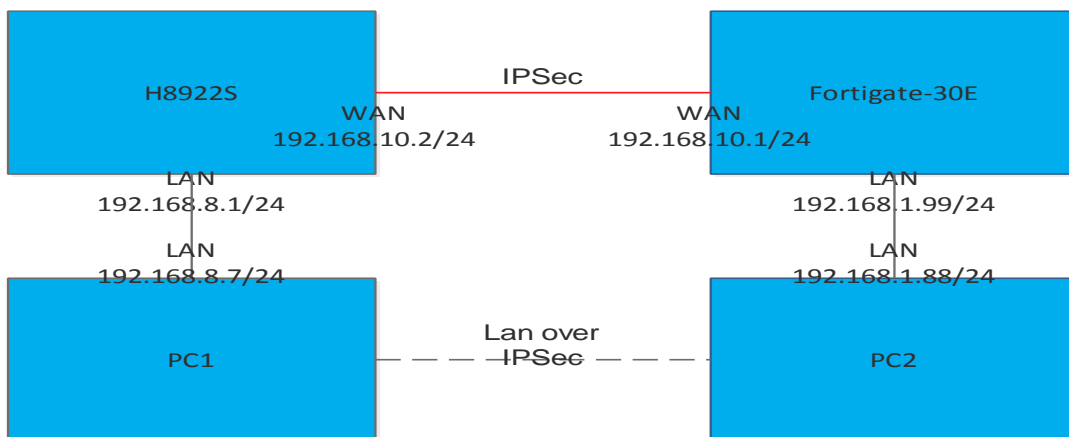
Doc Version	Product	Release Data	Details
V1.0	Hongdian Router	2017.08.23	First Release

# 1 Overview

Hongdian Router support to set up IPSec VPN with Fortigate Firewall, and it acts as the VPN client. Here we take an example for guiding you to build up the IPSec connection between Hongdian Router and Fortigate Firewall. Following we will take Hongdian H8922S Router and Fortigate-30E as the example.

## 2 Description

### 2.1 Test Topology



### 2.2 Fortigate Setup

#### 1. LAN WAN setup: Allow ping via IPSec Test

Status	Name	Members	IP/Netmask	Type	Access	Row
<b>Hardware Switch (1)</b>						
	lan		192.168.1.99.255.255.0	Hardware Switch (4)	PING HTTPS SSH HTTP FMG-Access CAPWAP	3
<b>Physical (2)</b>						
	wan		192.168.10.1.255.255.0	Physical Interface	PING FMG-Access	3
	IPSecTest		0.0.0.255.255.255	Tunnel Interface	PING	4

The screenshot shows the 'Edit Interface' configuration for 'IPSecTest'. The interface is a Tunnel Interface connected to 'wan'. The role is set to 'Undefined'. The addressing mode is 'Manual' with IP and Remote IP both set to 0.0.0.0. Under 'Restrict Access', 'PING' is checked, while 'HTTPS', 'SNMP', 'FMG-Access', 'CAPWAP', and 'SSH' are unchecked. 'DHCP Server' is disabled. 'Admission Control' is set to 'None'. Under 'Miscellaneous', 'Scan Outgoing Connections to Botnet Sites' is set to 'Disable'. The 'Interface State' is 'Enabled'.

## 2. Routing setup: Add static route direct to 192.168.8.0/255.255.255.0 via IPSec Test

The screenshot shows the 'Static Routes' configuration. A new static route is added with destination 192.168.8.0/24, gateway 192.168.10.2, and interface IPSecTest. Below, the 'Routing Monitor' shows the route as 'Connected'.

Destination	Gateway	Interface	Comment
0.0.0.0/0	192.168.10.2	wan	
192.168.8.0/24		IPSecTest	

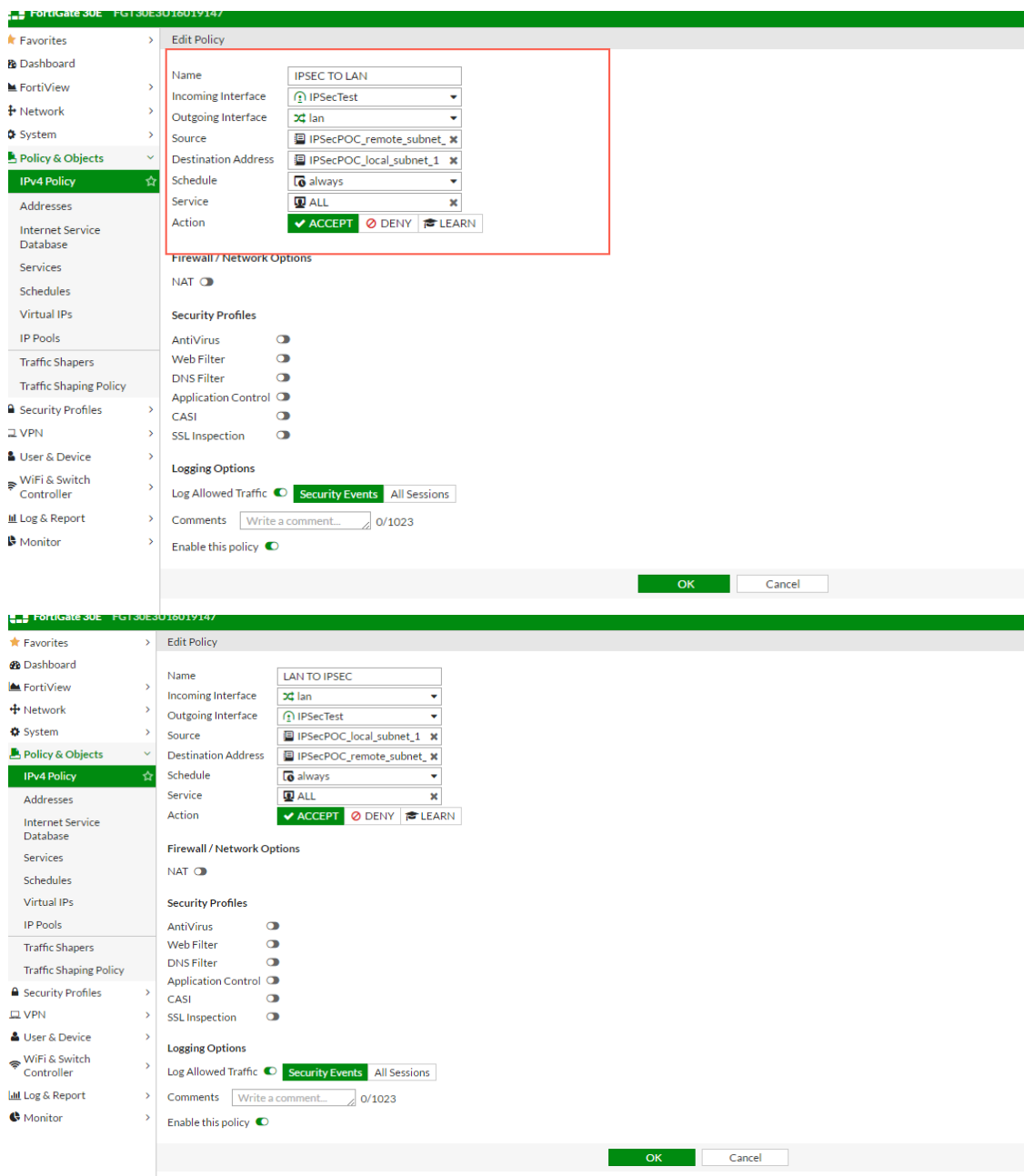
  

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	192.168.10.2	wan	
Connected		192.168.1.0/24	0.0.0.0	lan	
Static		192.168.8.0/24	0.0.0.0	IPSecTest	
Connected		192.168.10.0/24	0.0.0.0	wan	

## 3. Policy setup: Allow IPSec to LAN, LAN to IPSec traffic, please note disable NAT

The screenshot shows the 'Policy & Objects' configuration. Two policies are visible: 'IPSec TO LAN' (Seq # 1) and 'lan -> IPSecTest (2-2)'. Both policies have 'NAT' disabled and 'Action' set to 'ACCEPT'. The 'IPSec TO LAN' policy has source 'IPSecPOC\_remote\_subnet\_1' and destination 'IPSecPOC\_local\_subnet\_1'. The 'lan -> IPSecTest (2-2)' policy has source 'lan' and destination 'IPSecPOC\_remote\_subnet\_1'.

Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	IPSec TO LAN	IPSecPOC_remote_subnet_1	IPSecPOC_local_subnet_1	always	ALL	ACCEPT	Disabled	UTM		170.10 kB
2	lan -> IPSecTest (2-2)	lan	IPSecPOC_remote_subnet_1	always	ALL	ACCEPT	Disabled	UTM		33.00 kB



#### 4. IPsec setup:

> Edit VPN Tunnel

Name: IPSecTest

Comments:  0/255

**Network** Edit

Remote Gateway: Static IP Address, Interface: wan

**Authentication** Edit

Authentication Method: Pre-shared Key  
 IKE Version: 1, Mode: Main (ID protection)  
 Accept Peers: peertype\_

**Phase 1 Proposal** Edit

Algorithms: 3DES-SHA1  
 Diffie-Hellman Group: 5

**XAUTH** Edit

Type: Disabled

**Phase 2 Selectors**

Name	Local Address	Remote Address	
IPSecTest	192.168.1.0/255.255.255.0	192.168.8.0/255.255.255.0	<span>Add</span> <span>Edit</span>

OK Cancel

FortiGate 30E FGT30E3U16019147

Create New Edit Delete Print Instructions

Tunnel	Interface Binding	Template	Status	Ref.
IPSecTest	wan	Custom	1 connections	4

Favorites  
 Dashboard  
 FortiView  
 Network  
 System  
 Policy & Objects  
 Security Profiles  
 VPN  
 IPsec Tunnels  
 IPsec Wizard

## 2.3 Hongdian Setup

**Control Panel** Build time: 170422-183644  
Time: Fri Jun 2 13:14:23 2017

Network Applications **VPN** Forward Security System Status

VPDN Tunnel IPsec OpenVPN

**Phase1**

Policy Name	Encrypt	Hash	Authentication	Operation
POC1	3des	sha1	psk	Mod Del

**Phase2**

Policy Name	Encrypt	Hash	Remote Subnet	Operation
POC2	3des	sha1	192.168.1.0/24	Mod Del

**IPsec Interface**

Interface Name	Encrypt Interface	Destination IP or Domain	Operation
POC3	eth0	192.168.10.1	Mod Del View En Dis

Add Refresh

---

**Control Panel**

Network Applications **VPN** Forward Security System Status

VPDN Tunnel IPsec OpenVPN

**Policy Name**  
The Policy Name identifies an IPsec interface rule. The Policy Name should be unique.

Policy Name: POC1 \* Max length is 12

Initiate Mode: main

Encrypt: 3des

Hash: sha1

Authentication: psk

Pre Share Key: ..... \* Max length is 64

Self Identify: \_\_\_\_\_ Max length is 64

Match identify: \_\_\_\_\_ Max length is 64

IKE Lifetime: 3600 \* 120-86400 s

Group Name: group1536

DPD Service:  Enable  Disable

DPD Delay: 30 1-512 s

DPD Retry Times: 5 1-512 times

Save Return

**宏电®**  
Hongdian Connecting Machine ... Control Panel

Network Applications **VPN** Forward Security System Status

VPDN Tunnel IPsec **OpenVPN**

Policy Name: POC2 \* Max length is 12

Encryption Protocol: esp

Encrypt: 3des

Hash: sha1

PFS: open

Group Name: group1536

Lifetime: 3600 \* 120-86400 s

Local Protoport: : eg. 47:0

Remote Protoport: : eg. 47:0

Transport Mode: tunnel

Local Subnet: 192.168.8.0/24 \* eg. 192.168.8.0/24

Remote Subnet: 192.168.1.0/24 \* eg. 192.168.88.0/24

Save Return

**宏电®**  
Hongdian Connecting Machine ... Control Panel

Network Applications **VPN** Forward Security System Status

VPDN Tunnel IPsec **OpenVPN**

Status: Enable Disable

Interface Name: POC3 \* Max length is 12

Match Phase1: POC1

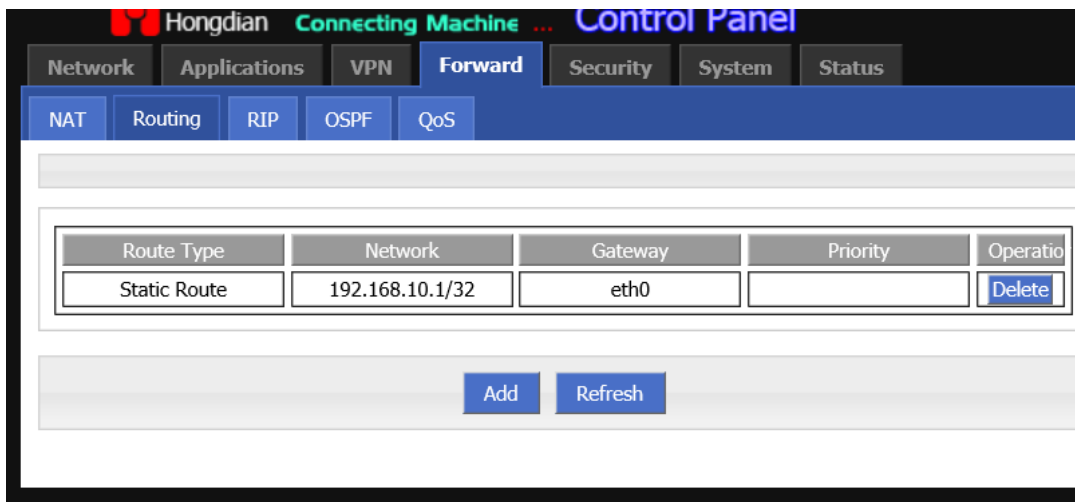
Match Phase2: POC2

Destination IP or Domain: 192.168.10.1 \* Max length is 64

Encrypt Interface: eth0

Save Return





## 2.4 Check Ping

### 1. From Hongdian:

```
C:\WINDOWS\system32\cmd.exe - ping 192.168.1.111 -t
```

```

来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=4ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62
来自 192.168.1.111 的回复: 字节=32 时间=3ms TTL=62

```

### 2. From Fortigate:

```
Administrator: C:\Windows\system32\cmd.exe - ping 192.168.8.240 -t
```

```

Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=4ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62
Reply from 192.168.8.240: bytes=32 time=3ms TTL=62

```

### 3. IPSec traffic monitor:

The screenshot shows the FortiGate web interface. On the left is a navigation menu with categories like Favorites, Dashboard, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, and Monitor. The Monitor section is expanded, showing sub-items: Routing Monitor, DHCP Monitor, WAN Link Monitor, FortiGuard Quota, IPsec Monitor (highlighted with a star), SSL-VPN Monitor, and Firewall User Monitor. The main content area displays a table with a 'Refresh' button and a single data row for 'IPSecTest'. The table has columns for Name, Type, Remote Gateway, Username, Status, Incoming Data, Outgoing Data, and Phase 2 Selectors.

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 2 Selectors
IPSecTest	Custom	192.168.10.2		Up	238.64 kB	123.42 kB	IPSecTest



*Create smart things*



## **Contact us**

---

 F14 - F16, Tower A, Building 14, No.12, Ganli 6th Road, Longgang District, Shenzhen 518112, China.

 +86-755-88864288-5

 +86-755-83404677

 hongdianchina

 [www.hongdian.com](http://www.hongdian.com)

 [sales@hongdian.com](mailto:sales@hongdian.com)

 Hongdian\_China