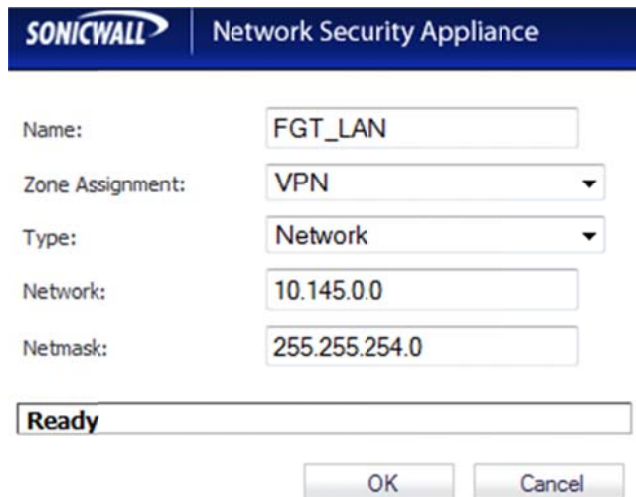


Route-Based (Interface Mode) IPSec VPN from FortiGate to SonicWALL

Configuration on SonicWALL

1. Create Address Object for remote location LAN



The screenshot shows the SonicWALL Network Security Appliance configuration interface. At the top, there is a blue header with the SonicWALL logo and the text "Network Security Appliance". Below the header, there are several configuration fields:

- Name:** FGT_LAN
- Zone Assignment:** VPN (selected from a dropdown menu)
- Type:** Network (selected from a dropdown menu)
- Network:** 10.145.0.0
- Netmask:** 255.255.254.0

Below these fields, there is a status bar that says "Ready". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

NOTE: Please select "**VPN**" Zone Assignment ; SonicWALL has a predefined LAN Subnet address object, there is no need to create an address object for the LAN.

2. Creation of IPSec VPN policy

SONICWALL | Network Security Appliance

General | Proposals | Advanced

Security Policy

Policy Type: Tunnel Interface

Authentication Method: IKE using Preshared Secret

Name: toFGT

IPsec Primary Gateway Name or Address: 192.168.146.15

IKE Authentication

Shared Secret: fortinet

Confirm Shared Secret: fortinet Mask Shared Secret

Local IKE ID: IP Address

Peer IKE ID: IP Address

Ready

OK Cancel Help

Note: Please select “**Tunnel Interface**” for Policy Type

3. Phase 1 and Phase 2 Proposal please leave it as Default

SONICWALL | Network Security Appliance

General | **Proposals** | Advanced

IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipssec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Ready

OK Cancel Help

- General
- Proposals
- Advanced

Advanced Settings

- Enable Keep Alive
- Allow Advanced Routing
- Enable Transport Mode
- Enable Windows Networking (NetBIOS) Broadcast
- Enable Multicast
- Permit TCP Acceleration

Management via this SA:

- HTTP
- HTTPS
- SSH

User login via this SA:

- HTTP
- HTTPS

VPN Policy bound to:

Interface X1

Ready

OK

Cancel

Help

VPN-> Advanced

VPN /

Advanced

AcceptCancel

Advanced VPN Settings


- Enable IKE Dead Peer Detection
 - Dead Peer Detection Interval (seconds)
 - Failure Trigger Level (missed heartbeats)
 - Enable Dead Peer Detection for Idle VPN sessions
 - Dead Peer Detection Interval for Idle VPN sessions (seconds)
- Enable Fragmented Packet Handling
 - Ignore DF (Don't Fragment) Bit
- Enable NAT Traversal
- Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address
- Preserve IKE Port for Pass Through Connections
- Enable OCSP Checking
- Send VPN Tunnel Traps only when tunnel status changes
- Use RADIUS in MSCHAP MSCHAPv2 mode for XAUTH (allows users to change expired passwords)

IKEv2 Settings

- Send IKEv2 Cookie Notify
- IKEv2 Dynamic Client Proposal

NOTE: SonicWALL will create the firewall policy automatically once the Phase1 and Phase 2 are configured.

Creating Static Route on SonicWALL

 Network Security Appliance

General

Route Policy Settings

Source: LAN Subnets

Destination: FGT_LAN

Service: Any

Gateway: 0.0.0.0

Interface: toFGT

Metric: 1

Comment:

Disable route when the interface is disconnected

Permit TCP acceleration

Auto-add Access Rules

Probe: None

Disable route when probe succeeds

Probe default state is UP

Ready


OK Cancel Help

Configuration on FortiGate

1. Creating address objects

Edit Address

Address Name

Color  [Change]


Type

Subnet / IP Range

Interface


Tags

Applied tags

Add tags 

Edit Address

Address Name

Color  [Change]


Type

Subnet / IP Range

Interface

Tags

Applied tags

Add tags 

2. IPsec Phase 1 configuration

Edit Phase 1

Name	<input type="text" value="TZ105"/>
Remote Gateway	<input type="text" value="Static IP Address"/>
IP Address	<input type="text" value="192.168.1.69"/>
Local Interface	<input type="text" value="mgmt1(WAN)"/>
Mode	<input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)
Authentication Method	<input type="text" value="Preshared Key"/>
Pre-shared Key	<input type="text" value="....."/>
Peer Options	
	<input checked="" type="radio"/> Accept any peer ID (XAUTH, NAT Traversal, DPD)
<input type="button" value="Advanced..."/>	
<input checked="" type="checkbox"/> Enable IPsec Interface Mode	
IKE Version	<input checked="" type="radio"/> 1 <input type="radio"/> 2
Local Gateway IP	<input type="radio"/> Main Interface IP <input type="radio"/> Specify <input type="text" value="0.0.0.0"/>
P1 Proposal	
	1 - Encryption <input type="text" value="3DES"/> Authentication <input type="text" value="SHA1"/>
DH Group	<input type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input type="checkbox"/> 5 <input type="checkbox"/> 14
Keylife	<input type="text" value="28800"/> (120-172800 seconds)
Local ID	<input type="text"/> (optional)
XAUTH	
	<input checked="" type="radio"/> Disable <input type="radio"/> Enable as Client <input type="radio"/> Enable as Server
NAT Traversal	<input type="checkbox"/> Enable
Keepalive Frequency	<input type="text" value="10"/> (10-900 seconds)
Dead Peer Detection	
	<input checked="" type="checkbox"/> Enable

NOTE: "Enable IPsec Interface Mode" must be selected

3. IPSec Phase 2 configuration

Edit Phase 2

Name

Phase 1

Advanced...

P2 Proposal 1- Encryption: 3DES Authentication: SHA1

Enable replay detection

Enable perfect forward secrecy(PFS).

DH Group 1 2 5 14

Keylife: Seconds (Seconds) (KBytes)

Autokey Keep Alive Enable

Quick Mode Selector

Source address	<input type="radio"/> Specify	<input type="text" value="0.0.0.0/0"/>
	<input type="radio"/> Select	<input type="text" value="-----Address-----"/>
Source port		<input type="text" value="0"/>
Destination address	<input type="radio"/> Specify	<input type="text" value="0.0.0.0/0"/>
	<input type="radio"/> Select	<input type="text" value="-----Address-----"/>
Destination port		<input type="text" value="0"/>
Protocol		<input type="text" value="0"/>

4. Static Route Configuration

Edit Static Route

Destination IP/Mask

Device

Gateway

Comments 0/63

5. Firewall Policy Creation

Edit Policy

Source Interface/Zone

Source Address +

Destination Interface/Zone

Destination Address +

Schedule

Service +

Action ✓

Log Allowed Traffic

Enable web cache

Enable NAT

Enable Identity Based Policy

Resolve User Names Using FSSO Agent

UTM

Traffic Shaping

Enable Endpoint Security






Tags

Applied tags

Add tags +

Comments 0/63

Edit Policy

Source Interface/Zone	<input type="text" value="mgmt2 (LAN)"/>
Source Address	<input type="text" value="FGT_LAN"/> 
Destination Interface/Zone	<input type="text" value="TZ105"/>
Destination Address	<input type="text" value="SonicWALL_LAN"/> 
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ANY"/> 
Action	<input type="text" value="ACCEPT"/> 
<input checked="" type="checkbox"/> Log Allowed Traffic	
<input type="checkbox"/> Enable web cache	
<hr/>	
<input type="checkbox"/> Enable NAT	
<hr/>	
<input type="checkbox"/> Enable Identity Based Policy	
<input type="checkbox"/> Resolve User Names Using FSSO Agent	
<hr/>	
<input type="checkbox"/> UTM	
<input type="checkbox"/> Traffic Shaping	
<input type="checkbox"/> Enable Endpoint Security <input type="text" value="[Please Select]"/>	
Tags	
Applied tags	
Add tags <input type="text"/> 	
Comments	<input type="text" value="Write a comment..."/> 0/63

OK

Cancel

Verifying the VPN Tunnel is Up

Name	Type	Remote Gateway	Remote Port	Username	Timeout	Proxy ID Source	Proxy ID Destination	Status	Incoming Data	Outgoing Data
TZ105	Static IP or Dynamic DNS	192.168.1.69	0		19126	0.0.0.0/0	0.0.0.0/0	Bring Down	198448 B	33452 B

VPN Policies

Refresh Interval (secs) 10 Items per page 50 Items 1 to 3 (of 3)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
<input type="checkbox"/>	1	WAN GroupVPN		ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input type="checkbox"/>	2	WLAN GroupVPN		ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	3	toFGT	192.168.146.15	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

Add... Delete Delete All

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 5 Maximum Policies Allowed
 GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 25 Maximum Policies Allowed

Currently Active VPN Tunnels

Refresh Interval (secs) 10 Items per page 50 Items 1 to 1 (of 1)

#	Created	Name	Local	Remote	Gateway	
1	10/10/2012 09:47:55	toFGT	0.0.0.0 - 255.255.255.255	0.0.0.0 - 255.255.255.255	192.168.146.15	Renegotiate

1 Currently Active VPN Tunnels