

Configuration Guide



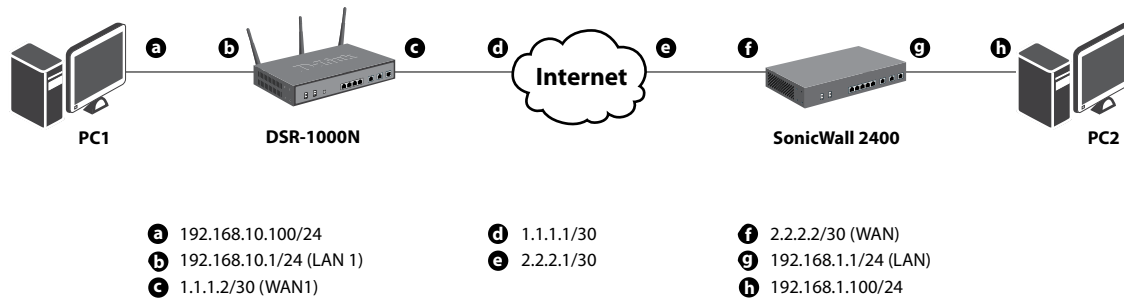
How to set up the IPSec site-to-site Tunnel between the D-Link DSR Router and the Sonicwall Firewall

Overview

This document describes how to implement IPSec with pre-shared secrets establishing site-to-site VPN tunnel between the D-Link DSR-1000N and the Sonicwall 2400. The screenshots in this document is from firmware version 1.03B12 of DSR-1000N and firmware version 3.0 of Sonicwall 2400. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

Situation note

Site-to-site VPN could be implemented in an enterprise allows to access and exchange data among more than two geographical sites or offices. Once the site-to-site VPN set up, the clients in the groups of the different located sites are as in the internal networks. As companies may have other gateway appliances which are not D-Link products, this document will be useful when you intend to create IPSec VPN tunnel between DSR and other existing gateway appliance.



IP addresses

DSR WAN: **1.1.1.2/30**

DSR LAN: **192.168.10.1/24**

FortiGate100 WAN: **2.2.2.2/30**

FortiGate100 LAN: **192.168.1.1/24**

IPSec Parameters

IPSec Mode: **Tunnel Mode**

IPSec Protocol: **ESP**

Phase1 Exchange Mode: **Main**

Phase1 Encryption: **3DES**

Phase1 Authentication: **SHA1**

Phase1 Authentication Method: **Pre-Shared Key**

Diffie-Hellman Group: **G2**
Phase1 Lifetime: **28800 sec**
Phase2 Encryption: **3DES**
Phase2 Authentication: **SHA1**
Phase2 Lifetime: **3600 sec**

Configuration Step

DSR Settings

1. Set up the WAN IP address. Navigate to the [Internet Settings > WAN1 Settings > WAN1 Setup](#).
Fill in relative information based on the settings of topology. The **IP Address** of the field of ISP Connection Type is the IP address of external network connecting point which is shown as the point “c” on the topology. Click the button “save settings” to complete WAN IP address settings.the button “**save settings**” to complete WAN IP address settings.

Wizard	
Internet Settings	
Wireless Settings	
Network Settings	
DMZ Setup	
VPN Settings	
USB Settings	
VLAN Settings	

WAN1 SETUP

LOGOUT

This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Addresses, Account Information etc. This information is usually provided by your ISP or network administrator.

ISP Connection Type

ISP Connection Type:

IP Address:

IP Subnet Mask:

Gateway IP Address:

Domain Name System (DNS) Servers

Primary DNS Server:

Secondary DNS Server:

MAC Address

MAC Address Source:

MAC Address:

2. Set up the IPsec policy. Navigate to the [VPN Settings > IPsec > IPsec Policies](#).

Press the button "Add" to increase a new policy. In General Section, fill in relative information. The IP address of **Remote Endpoint** refers to the external network connecting point of SonicWall 2400 which is shown as the point "f" on the topology. The internal network group, which is indicates the IP information on **Local Start IP Address**, under DSR-1000N allows access to the remote network group, which indicates the IP information on **Remote Start IP Address**, under SonicWall 2400 through VPN tunnel.

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS
Wizard	IPSEC CONFIGURATION LOGOUT			
Internet Settings	This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.			
Wireless Settings	<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>			
Network Settings	General			
DMZ Setup	Policy Name:	<input type="text" value="IPSec1"/>		
VPN Settings	Policy Type:	Auto Policy ▼		
USB Settings	IPsec Mode:	Tunnel Mode ▼		
VLAN Settings	Select Local Gateway:	Dedicated WAN ▼		
	Remote Endpoint:	IP Address ▼		
		<input type="text" value="2.2.2.2"/>		
	Enable Mode Config:	<input type="checkbox"/>		
	Enable NetBIOS:	<input type="checkbox"/>		
	Enable RollOver:	<input type="checkbox"/>		
	Protocol:	ESP ▼		
	Enable DHCP:	<input type="checkbox"/>		
	Local IP:	Subnet ▼		
	Local Start IP Address:	<input type="text" value="192.168.10.0"/>		
	Local End IP Address:	<input type="text"/>		
	Local Subnet Mask:	<input type="text" value="255.255.255.0"/>		
	Remote IP:	Subnet ▼		
	Remote Start IP Address:	<input type="text" value="192.168.1.0"/>		
	Remote End IP Address:	<input type="text"/>		
	Remote Subnet Mask:	<input type="text" value="255.255.255.0"/>		

In Phase 1 Section, fill in relative information. Please notice that the Pre-shared Key must be as same as the Shared Secret which will be inserted on SonicWall 2400 on the later step.

Phase1(IKE SA Parameters)	
Exchange Mode:	Main ▼
Direction / Type:	Both ▼
Nat Traversal:	
On:	<input checked="" type="radio"/>
Off:	<input type="radio"/>
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP ▼
Local Identifier:	
Remote Identifier Type:	Remote Wan IP ▼
Remote Identifier:	
Encryption Algorithm:	3DES ▼
Key Length:	
Authentication Algorithm:	SHA-1 ▼
Authentication Method:	Pre-shared key ▼
Pre-shared key:	1234567890
Diffie-Hellman (DH) Group:	Group 2 (1024 bit) ▼
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	<input type="checkbox"/>
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	None ▼
Authentication Type:	User Database ▼
Username:	
Password:	

In Phase 2 Section, fill in relative information.

Phase2-(Manual Policy Parameters)

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key Length:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Phase2-(Auto Policy Parameters)

SA Lifetime:

Encryption Algorithm:

Key Length:

Integrity Algorithm:

PFS Key Group:

Click the button “save settings” to complete IPsec Policy settings.

3. Check the VPN status. Navigate to the [Status > Active VPNs](#).

The activity will be shown on the list while the tunnel is established with the other side.

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS												
Device Info	<p style="color: red;">Operation succeeded</p> <p style="color: red;">The page will auto-refresh in 10 seconds</p>															
Logs																
Traffic Monitor																
Active Sessions																
Active RunTime Sessions																
Wireless Clients	ACTIVE VPN LOGOUT															
LAN Clients	This page displays the active VPN connections, IPSEC as well as SSL.															
Active VPNs	<div style="background-color: #333; color: white; padding: 2px;">Active IPsec SAs</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Policy Name</th> <th>Endpoint</th> <th>tx (KB)</th> <th>tx (Packets)</th> <th>State</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>IPsec</td> <td>2.2.2.2</td> <td>0.00</td> <td>0</td> <td>IPsec SA Not Established</td> <td style="text-align: center;"><input type="button" value="Connect"/></td> </tr> </tbody> </table>				Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action	IPsec	2.2.2.2	0.00	0	IPsec SA Not Established	<input type="button" value="Connect"/>
Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action											
IPsec	2.2.2.2	0.00	0	IPsec SA Not Established	<input type="button" value="Connect"/>											
<div style="background-color: #333; color: white; padding: 2px;">Active SSL VPN Connections</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>User Name</th> <th>IP Address</th> <th>Local PPP Interface</th> <th>Peer PPP Interface IP</th> <th>Connect Status</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="text-align: center;"> Poll Interval: <input type="text" value="10"/> (Seconds) <input type="button" value="Start"/> <input type="button" value="Stop"/> </td> </tr> </tbody> </table>					User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status	Poll Interval: <input type="text" value="10"/> (Seconds) <input type="button" value="Start"/> <input type="button" value="Stop"/>						
User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status												
Poll Interval: <input type="text" value="10"/> (Seconds) <input type="button" value="Start"/> <input type="button" value="Stop"/>																

Sonicwall 2400 Settings

1. Set up the LAN & WAN IP addresses. Navigate to the **Network > Interfaces**. Click the icon **"Configure"**.

Network Security Appliance

Network / Interfaces

Accept

Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.1.1	255.255.255.0	Static	1000 Mbps full-duplex	Default LAN	
X1	WAN	2.2.2.2	255.255.255.252	Static	100 Mbps full-duplex	Default WAN	
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X4	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X5	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

Add Interface...

Interface Traffic Statistics

Traffic Statistics	X0	X1	X2	X3	X4	X5
Rx Unicast Packets	8275	871	0	0	0	0
Rx Broadcast Packets	280	25	0	0	0	0

Clear

Status: Ready

Fill in the relative information for the settings of LAN as below. The IP Address of General tab is the **IP address** of internal network connecting point which is shown as the point "g" on the topology.

SONICWALL Network Security Appliance

General Advanced

Interface 'X0' Settings

Zone: LAN

IP Assignment: Static

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

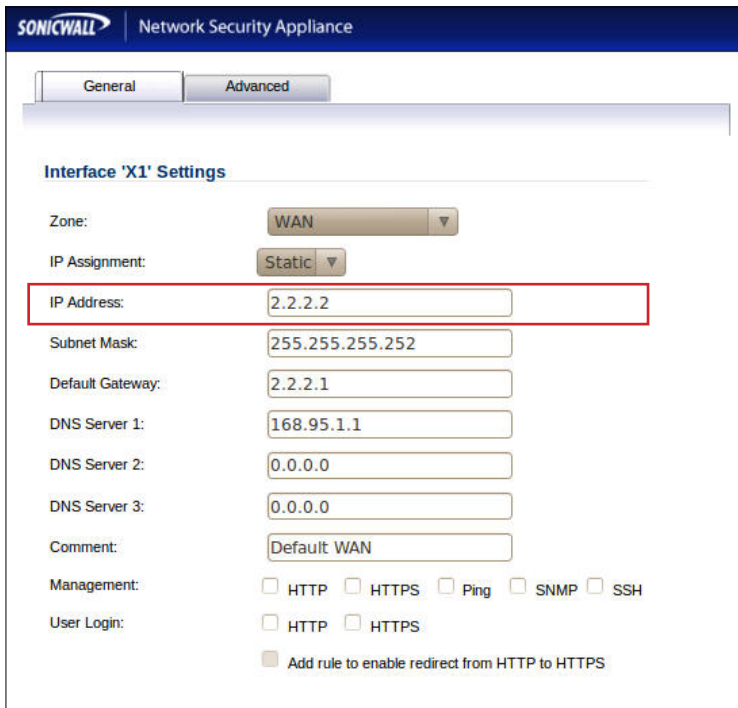
Comment: Default LAN

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Fill in the relative information for the settings of WAN as below. The **IP Address** of General tab is the IP address of external network connecting point which is shown as the point "f" on the topology.



SONICWALL Network Security Appliance

General Advanced

Interface 'X1' Settings

Zone: WAN

IP Assignment: Static

IP Address: 2.2.2.2

Subnet Mask: 255.255.255.252

Default Gateway: 2.2.2.1

DNS Server 1: 168.95.1.1

DNS Server 2: 0.0.0.0

DNS Server 3: 0.0.0.0

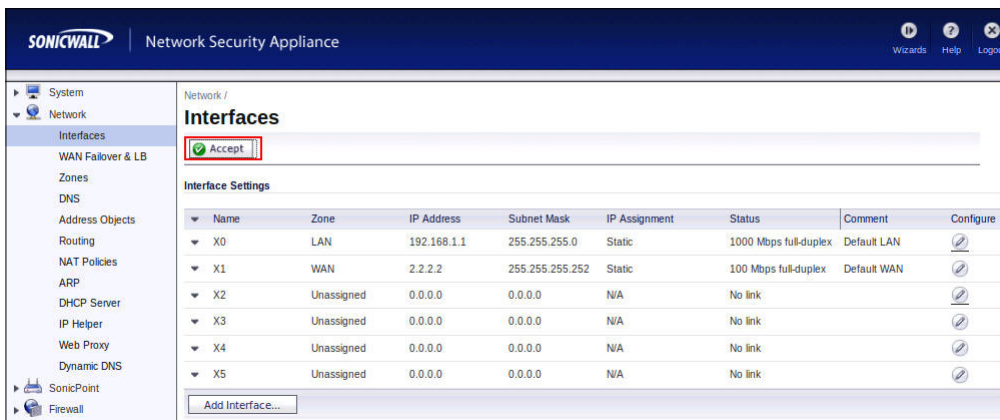
Comment: Default WAN

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Press the button "**Accept**" to confirm the changes.



SONICWALL Network Security Appliance

Wizards Help Logout

System

Network

Interfaces

WAN Fallover & LB

Zones

DNS

Address Objects

Routing

NAT Policies

ARP

DHCP Server

IP Helper

Web Proxy

Dynamic DNS

SonicPoint

Firewall

Network /

Interfaces

Accept

Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.1.1	255.255.255.0	Static	1000 Mbps full-duplex	Default LAN	
X1	WAN	2.2.2.2	255.255.255.252	Static	100 Mbps full-duplex	Default WAN	
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X4	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X5	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

Add Interface...

2. Check the default route. Navigate to **Network > Routing**.

The screenshot shows the SonicWall Network Security Appliance interface. The left sidebar has 'Network' and 'Routing' highlighted with red boxes. The main content area shows the 'Route Policies' configuration page. At the top, there's a section for 'Apply the following metric to default routes received from Advanced Routing protocols:' with a value of '110' and a 'Change' button. Below that, there's a 'Route Policies' section with a table of policies. The 6th policy is highlighted with a red box.

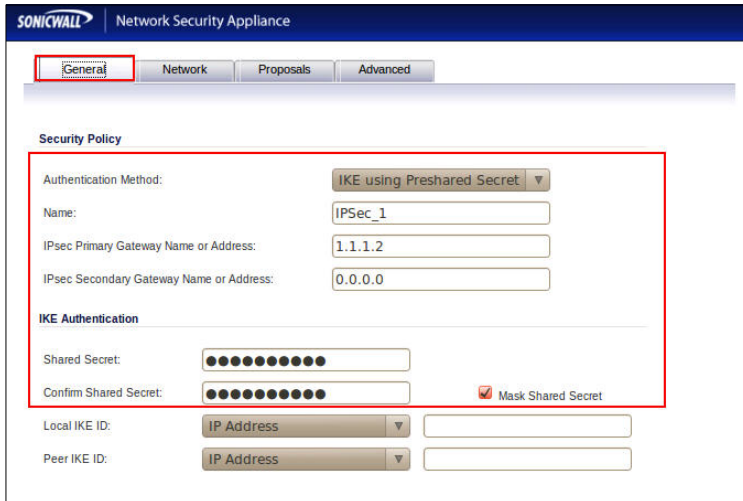
#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	Default Gateway	Any	0.0.0.0	X1	20	1		
2	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	2		
3	Any	X1 Subnet	Any	0.0.0.0	X1	20	3		
4	Any	X0 Subnet	Any	0.0.0.0	X0	20	4		
5	X1 Subnet	Any	Any	Default Gateway	X1	20	5		
6	Any	0.0.0.0/0	Any	2.2.2.1	X1	20	6		

3. Set up the IPSec Tunnel. Navigate to the **VPN > Settings**. Press the button "**Add**".

The screenshot shows the SonicWall Network Security Appliance interface. The left sidebar has 'VPN' and 'Settings' highlighted with red boxes. The main content area shows the 'VPN Settings' configuration page. At the top, there's an 'Accept' button. Below that, there's a 'VPN Global Settings' section with 'Enable VPN' checked and a 'Unique Firewall Identifier' field containing '0017C511849C'. Below that, there's a 'VPN Policies' section with a table of policies. The 'Add...' button at the bottom of the table is highlighted with a red box.

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
3	IPSec_1	1.1.1.2	192.168.10.0 - 192.168.10.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

In the tab "General", fill in the name, IPsec primary and secondary gateway, and shared secret. The **IPsec Primary Gateway Name or Address** is the IP address of external network connecting point of DSR-1000N which is shown as the point "c" on the topology. Insert the **Shared Secret** which is as same as the Pre-shared Key put in DSR-1000N in the previous step.



SONICWALL Network Security Appliance

General Network Proposals Advanced

Security Policy

Authentication Method: IKE using Preshared Secret ▼

Name: IPsec_1

IPsec Primary Gateway Name or Address: 1.1.1.2

IPsec Secondary Gateway Name or Address: 0.0.0.0

IKE Authentication

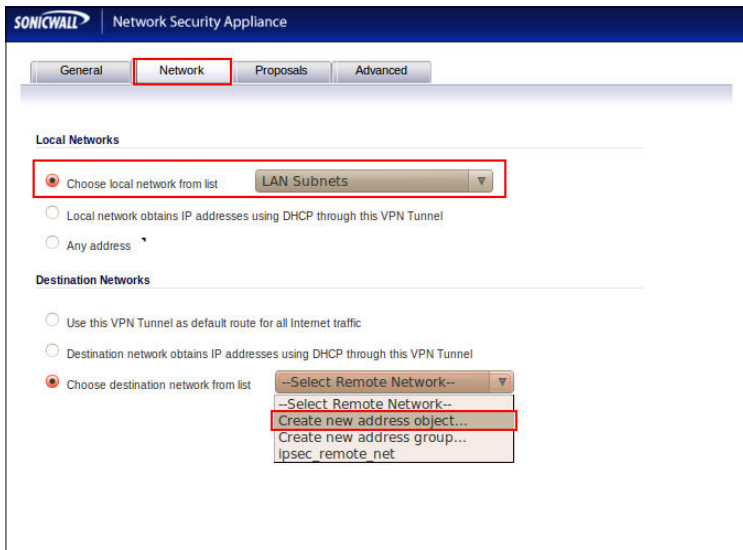
Shared Secret: ●●●●●●●●

Confirm Shared Secret: ●●●●●●●● Mask Shared Secret

Local IKE ID: IP Address

Peer IKE ID: IP Address

Click the tab "Network". In Local Networks section, select **LAN Subnets** as the local network. In Destination Networks, create new address object for destination network.



SONICWALL Network Security Appliance

General Network Proposals Advanced

Local Networks

Choose local network from list LAN Subnets ▼

Local network obtains IP addresses using DHCP through this VPN Tunnel

Any address ▼

Destination Networks

Use this VPN Tunnel as default route for all Internet traffic

Destination network obtains IP addresses using DHCP through this VPN Tunnel

Choose destination network from list

--Select Remote Network--
--Select Remote Network--
Create new address object...
Create new address group...
ipsec_remote_net

Configure a new address object to define the IP address of the remote group which under DSR-1000N.

The screenshot shows the configuration page for a new address object in the Sonicwall Network Security Appliance. The fields are as follows:

- Name: ipsec_remote_net
- Zone Assignment: VPN
- Type: Network
- Network: 192.168.10.0
- Netmask: 255.255.255.0

The status is "Ready" and there are "OK" and "Cancel" buttons at the bottom.

The screenshot shows the configuration page for a VPN tunnel in the Sonicwall Network Security Appliance. The "Network" tab is selected. The configuration is as follows:

- Local Networks:
 - Choose local network from list: LAN Subnets
 - Local network obtains IP addresses using DHCP through this VPN Tunnel
 - Any address
- Destination Networks:
 - Use this VPN Tunnel as default route for all Internet traffic
 - Destination network obtains IP addresses using DHCP through this VPN Tunnel
 - Choose destination network from list: ipsec_remote_net

The status is "Ready" and there are "OK", "Cancel", and "Help" buttons at the bottom.

Click the tab "**Proposals**". Select the relative settings as below.

The screenshot shows the Sonicwall Network Security Appliance configuration interface. The "Proposals" tab is selected and highlighted with a red box. The interface is divided into two sections: "IKE (Phase 1) Proposal" and "Ipssec (Phase 2) Proposal".

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
- DH Group: Group 2
- Life Time (seconds): 28800

At the bottom, there is a "Ready" status bar and three buttons: "OK", "Cancel", and "Help".

Click the tab "**Advanced**". Select the relative settings as below.

The screenshot shows the Sonicwall Network Security Appliance configuration interface. The "Advanced" tab is selected and highlighted with a red box. The interface displays "Advanced Settings" with various options and fields.

Advanced Settings

- Enable Keep Alive
- Suppress automatic Access Rules creation for VPN Policy
- Require authentication of VPN clients by XAUTH
 - User group for XAUTH users: --Select a user group--
- Enable Windows Networking (NetBIOS) Broadcast
- Enable Multicast
- Apply NAT Policies
 - Translated Local Network: --Select Translated Local Network--
 - Translated Remote Network: --Select Translated Remote Network--
- Management via this SA: HTTP HTTPS SSH
- User login via this SA: HTTP HTTPS
- Default LAN Gateway (optional): 0.0.0.0
- VPN Policy bound to: Zone WAN

At the bottom, there is a "Ready" status bar and three buttons: "OK", "Cancel", and "Help".

4. Check the VPN status. Navigate to **VPN > Settings**.

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar shows the navigation menu with 'VPN' selected and 'Settings' expanded. The main content area is titled 'VPN Policies' and shows a table of three policies. The third policy, 'IPSec_1', is highlighted with a red box. Below the table, there are statistics for Site To Site Policies and GroupVPN Policies. At the bottom, the 'Currently Active VPN Tunnels' section shows one active tunnel, 'IPSec_1', also highlighted with a red box. The interface includes a top navigation bar with 'Wizards', 'Help', and 'Logout' buttons, and a 'Unique Firewall Identifier' field at the top left.

Unique Firewall Identifier: 0017C511849C

VPN Policies

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
3	IPSec_1	1.1.1.2	192.168.10.0 - 192.168.10.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 75 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 8 Maximum Policies Allowed

Currently Active VPN Tunnels

#	Created	Name	Local	Remote	Gateway	
1	01/25/2011 17:25:21	IPSec_1	192.168.1.0 - 192.168.1.255	192.168.10.0 - 192.168.10.255	1.1.1.2	Renegotiate

1 Currently Active VPN Tunnels

D-Link[®]

Visit our website for more information
www.dlink.com

D-Link, D-Link logo, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries.
All other third party marks mentioned herein are trademarks of the respective owners.

Copyright © 2011 D-Link Corporation. All Rights Reserved.