

Configuration Guide



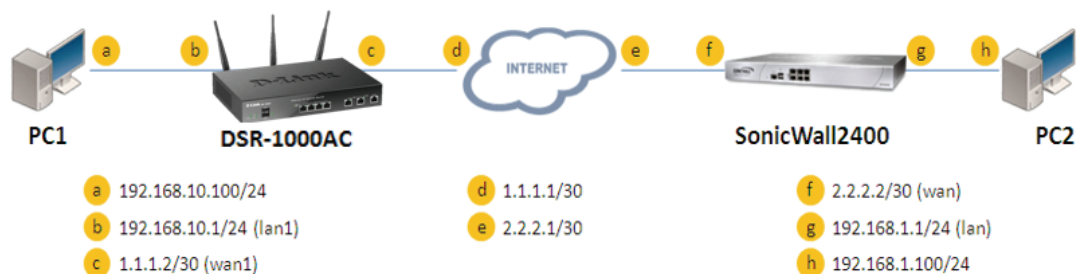
How to set up the IPSec site-to-site Tunnel between the D-Link DSR Router and the SonicWall Firewall

Overview

This document describes how to implement IPsec with pre-shared secrets establishing a site-to-site VPN tunnel between the D-Link DSR-1000AC and the Sonicwall NSA 2400. The screenshots in this document are from firmware version 3.10 of the DSR-1000AC and firmware version 5.9.1.7 (Released in August 2016) of the Sonicwall NSA 2400. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see in your browser.

Situation note

Site-to-site VPNs can be implemented in an enterprise to allow access and the exchange of data between two or more geographically separated sites or offices. Once the site-to-site VPN has been set up, the clients in the groups of the different sites can communicate as if they are on the same internal network. Because companies may have other gateway appliances that are not D-Link products, this document can be used to create IPsec VPN tunnels between the DSR router and other existing gateway appliances.



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: **28800 sec**

Configuration Step

DSR Settings

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

Operation Succeeded

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.

IPv4 WAN1 Settings

WAN1 Setup

Connection Type Static IP

Enable VLAN Tag OFF

Static IP

IP Address

IP Subnet Mask

Gateway IP Address

Domain Name System (DNS) Servers

Primary DNS Server

Secondary DNS Server

MAC Address

MAC Address Source
 Use Default MAC
 Clone your PC's MAC
 Use this MAC

Port Setup

MTU Size Default Custom

Port Speed

Save
Cancel

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

Press the “Add New IPsec Policy” button to create a new policy. In the General section, fill in the relevant information. The IP address of the **Remote Endpoint** refers to the external connection point of the SonicWall NSA 2400, which is shown as the point “f” in the topology. The internal IP Address range, which is indicated by **Local Start IP Address**, is the IP range allowed access to the remote network over the VPN, and the remote network range indicated by the **Remote Start IP Address**, is the IP range reachable through the VPN tunnel with the SonicWall NSA 2400.

Logged in as: admin (ADMIN) | Language: English [US] | Logout
Serial: 539X1G1000007 | Firmware: 3.10_VWV
Wizard | System Search...

VPN > IPsec VPN > Policies

This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
Note: Policy with "*" represents a Client Policy.

IPsec Policies List

Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPsec Mode	Local	Remote	Auth	Encr
No data available in table								

Showing 0 to 0 of 0 entries

First Previous Next Last

Add New IPsec Policy

IPsec Policy Configuration

General

Policy Name: IPsec1

Policy Type: Auto Policy

IP Protocol Version: IPv4

IKE Version: IKEv1

L2TP Mode: None

IPsec Mode: Tunnel Mode

Select Local Gateway: Dedicated WAN

Remote Endpoint: IP Address

IP Address / FQDN: 2.2.2.2

Enable Mode Config: OFF

Save

IPSec Policy Configuration

OFF Enable Mode Config
 OFF Enable NetBIOS
 OFF Enable RollOver
 Protocol: ESP
 OFF Enable DHCP
 Local IP: Subnet
 Local Start IP Address:
 Local Subnet Mask:
 Remote IP: Subnet
 Remote Start IP Address: 192.168.1.0
 Remote Subnet Mask: 255.255.255.0
 OFF Enable Keepalive

Save

In the Phase 1 section, fill in the relevant information. Please notice that the **Pre-shared Key** must be the same as the pre-shared key that will be entered into the SonicWall NSA 2400 later.

IPSec Policy Configuration

Phase1(IKE SA Parameters)

Exchange Mode: Main
 Direction / Type: Both
 Nat Traversal: ON
 NAT Keep Alive Frequency: 20 Seconds
 Local Identifier Type: Local Wan IP
 Remote Identifier Type: Remote Wan IP

Encryption Algorithm

OFF DES 3DES ON
 OFF AES-128 AES-192 OFF
 OFF AES-256
 OFF BLOWFISH

Save

IPSec Policy Configuration

Authentication Algorithm

OFF MD5 SHA-1 ON
 OFF SHA2-256 SHA2-384 OFF
 OFF SHA2-512

Authentication Method: Pre-Shared Key
 Pre-Shared Key: 12345678 [Length: 8 - 49]
 Diffie-Hellman (DH) Group: Group 2 (1024 bit)
 SA-Lifetime: 28800 [Range: 300 - 2147483647] Seconds
 OFF Enable Dead Peer Detection
 Extended Authentication: None

Phase2-(Auto Policy Parameters)

SA Lifetime: 3600 Seconds

Save

In the Phase 2 section, fill in relevant information.

IPSec Policy Configuration X

Phase 2-(Auto Policy Parameters)

SA Lifetime Seconds ▾

Encryption Algorithm

DES <input type="checkbox"/> OFF	None <input type="checkbox"/> OFF	
3DES <input checked="" type="checkbox"/> ON	AES-128 <input type="checkbox"/> OFF	
AES-192 <input type="checkbox"/> OFF	AES-256 <input type="checkbox"/> OFF	
TWOFISH (128) <input type="checkbox"/> OFF	TWOFISH (192) <input type="checkbox"/> OFF	
TWOFISH (256) <input type="checkbox"/> OFF		
BLOWFISH <input type="checkbox"/> OFF		
CAST128 <input type="checkbox"/> OFF		

Integrity Algorithm

MD5 <input type="checkbox"/> OFF	SHA-1 <input checked="" type="checkbox"/> ON	
----------------------------------	--	--

Save

Click the **“Save”** button to complete the IPSec Policy settings.

VPN >> IPSec VPN >> Policies ? ↻

This page shows the list of configured IPSec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPSec VPN policies from this page.
Note: Policy with ™ represents a Client Policy.

IPSec Policies List

Show 10 entries [Right click on record to get more options] 🔍

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
Enabled	IPSec1	None	Auto Policy	Tunnel Mode	192.168.10.0/255.255.255.0	192.168.1.0/255.255.255.0	SHA1	3DES

Showing 1 to 1 of 1 entries
⏪ First
⏩ Previous
1
Next
⏪ Last

Add New IPSec Policy

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

The activity will be shown in the list as the tunnel is established with the other side.

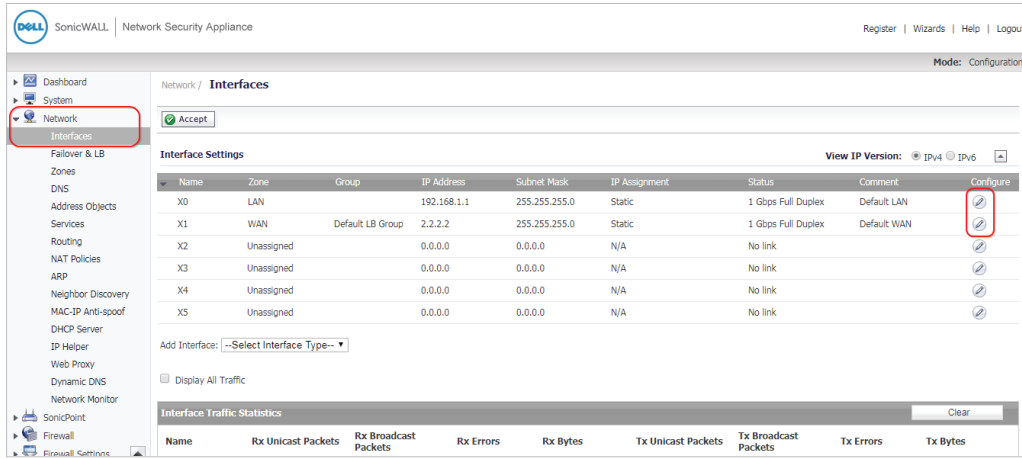
The screenshot displays the D-Link Unified Services Router (DSR-1000AC) web interface. The top navigation bar includes 'Status', 'Wireless', 'Network', 'VPN', 'Security', and 'Maintenance'. The 'Status' menu is expanded to show 'Active VPNs', which is further expanded to 'IPsec SAs'. Below this, there are tabs for 'IPsec SAs', 'SSL VPN Connections', 'PPTP VPN Connections', 'Open VPN Connections', 'L2TP VPN Connections', and 'GRE Tunnel Status'. The main content area shows a message: 'This page lists current established IPsec Security Associations.' Below this is the 'Active IPsec SAs List' section, which includes a search bar and a table with the following data:

Policy Name	Endpoint	tx (KB)	tx (Packets)	State
IPSec1	2.2.2.2	7.77	71	IPsec SA Established

At the bottom of the table, it says 'Showing 1 to 1 of 1 entries' and provides navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'.

Sonicwall NSA 2400 Settings

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



The screenshot displays the SonicWall NSA 2400 web interface. The left sidebar shows the navigation menu with 'Network > Interfaces' selected. The main content area shows the 'Interfaces' configuration page. A table lists the interfaces, with the 'X1' WAN interface highlighted. The 'Configure' icon for the X1 interface is circled in red.

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.1.1	255.255.255.0	Static	1 Gbps Full Duplex	Default LAN	
X1	WAN	Default LB Group	2.2.2.2	255.255.255.0	Static	1 Gbps 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		

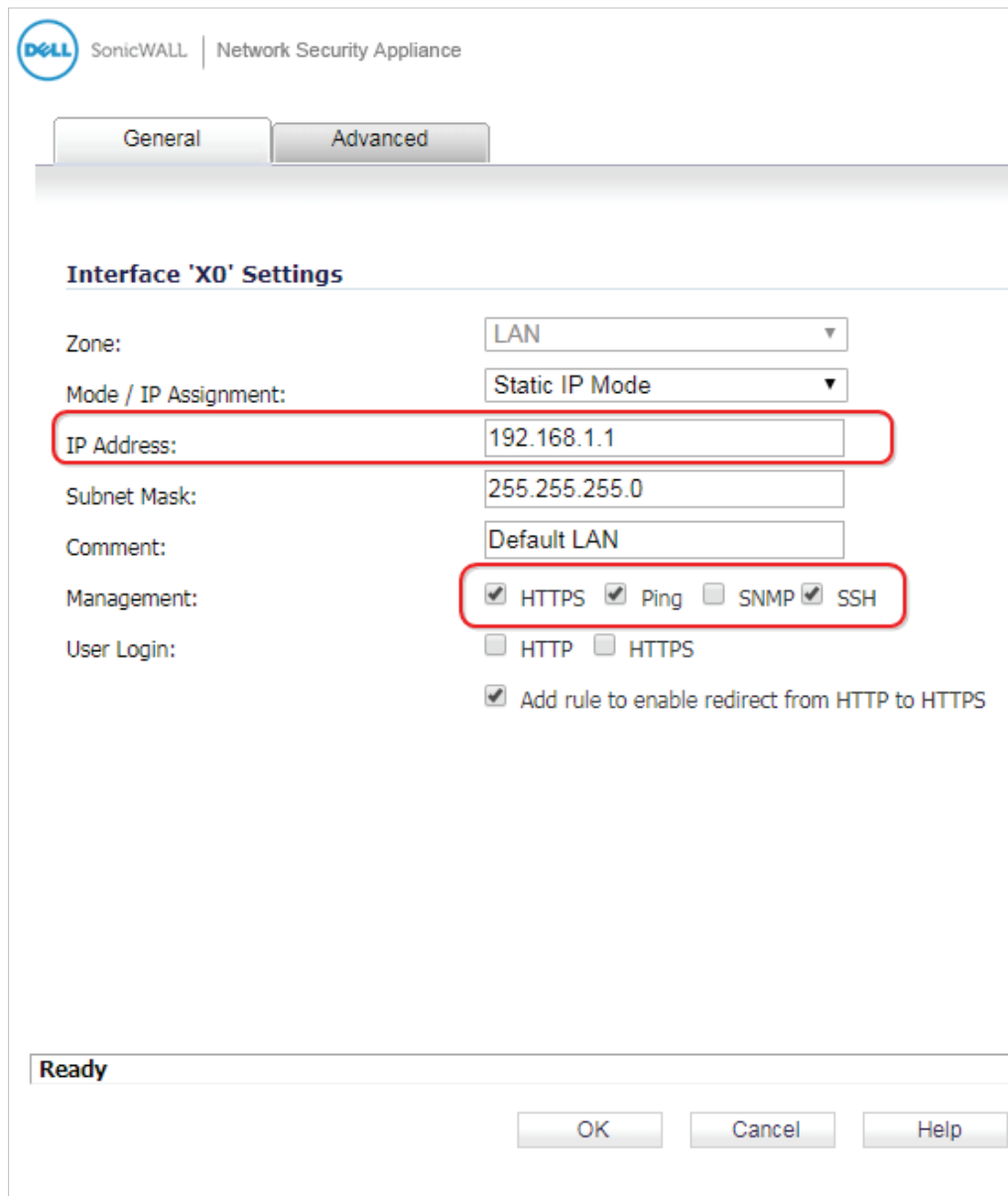
Add Interface: --Select Interface Type--

Display All Traffic

Interface Traffic Statistics Clear

Name	Rx Unicast Packets	Rx Broadcast Packets	Rx Errors	Rx Bytes	Tx Unicast Packets	Tx Broadcast Packets	Tx Errors	Tx Bytes
------	--------------------	----------------------	-----------	----------	--------------------	----------------------	-----------	----------

Fill in the relevant information for the LAN interface configuration as below. The IP Address of the General tab is the **IP address** of internal network connection, which is shown as point “g” in the topology.



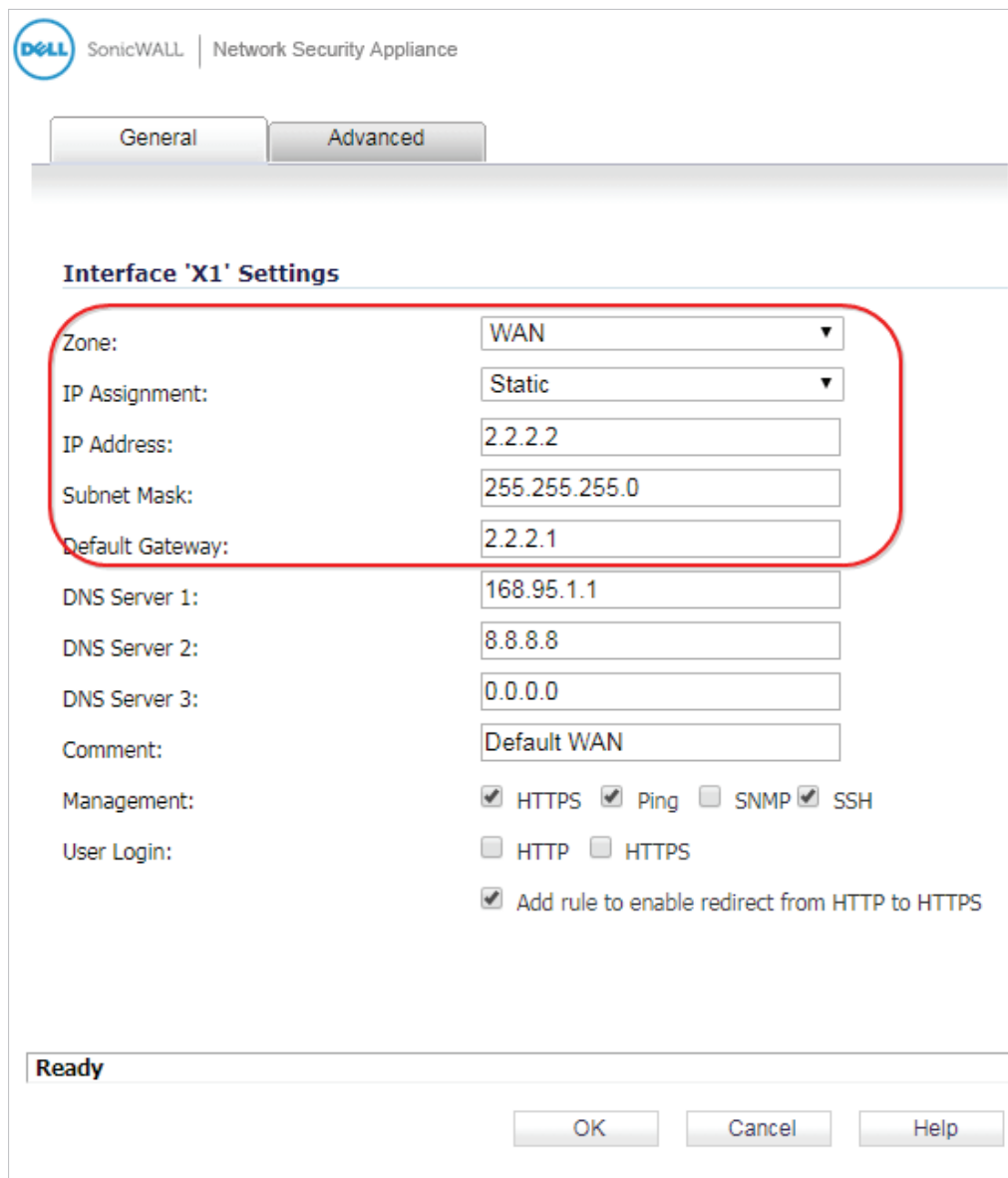
The screenshot shows the SonicWall Network Security Appliance configuration interface. At the top left is the SonicWALL logo and the text "SonicWALL | Network Security Appliance". Below this are two tabs: "General" (selected) and "Advanced". The main section is titled "Interface 'X0' Settings".

The configuration fields are as follows:

- Zone: LAN (dropdown menu)
- Mode / IP Assignment: Static IP Mode (dropdown menu)
- IP Address: 192.168.1.1 (text input field, highlighted with a red box)
- Subnet Mask: 255.255.255.0 (text input field)
- Comment: Default LAN (text input field)
- Management: HTTPS Ping SNMP SSH (checkboxes, highlighted with a red box)
- User Login: HTTP HTTPS
- Add rule to enable redirect from HTTP to HTTPS

At the bottom left, there is a status indicator that says "Ready". At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

Fill in the relevant information for the WAN interface as below. The **IP Address** of the General tab is the IP address of external network connection, which is shown as point "f" in the topology.



SonicWALL | Network Security Appliance

General Advanced

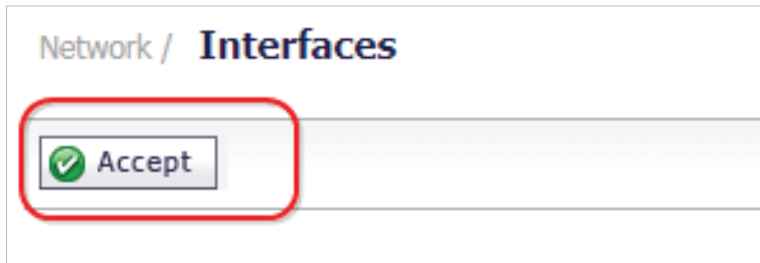
Interface 'X1' Settings

Zone:	WAN
IP Assignment:	Static
IP Address:	2.2.2.2
Subnet Mask:	255.255.255.0
Default Gateway:	2.2.2.1
DNS Server 1:	168.95.1.1
DNS Server 2:	8.8.8.8
DNS Server 3:	0.0.0.0
Comment:	Default WAN
Management:	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Ping <input type="checkbox"/> SNMP <input checked="" type="checkbox"/> SSH
User Login:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
	<input checked="" type="checkbox"/> Add rule to enable redirect from HTTP to HTTPS

Ready

OK Cancel Help

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



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



Configure the relevant settings as below.

Mode: Configuration

Prioritize routes by metric within route classes

Route Policies

Items 1 to 6 (of 6)

View Style: All Policies Custom Policies Default Policies

View IP Version: IPv4 Only IPv6 Only IPv4 and IPv6

#	Source	Destination	Service	TOS / Mask	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
1	Any	255.255.255.255/32	Any	Any	0.0.0.0	X0	20	2			
2	Any	X1 Default Gateway	Any	Any	0.0.0.0	X1	20	3			
3	Any	X0 Subnet	Any	Any	0.0.0.0	X0	20	4			
4	Any	X1 Subnet	Any	Any	0.0.0.0	X1	20	5			
5	X1 IP	Any	Any	Any	X1 Default Gateway	X1	20	6			
6	Any	0.0.0.0/0	Any	Any	2.2.2.1	X1	20	7			

Apply the following metric to IPv6 default routes learned through router advertisement: 50 Change

3. Set up the IPsec Tunnel. Navigate to: **VPN > Settings**.

Press the **"Add"** button.

The screenshot shows the SonicWall configuration interface. The left sidebar has the 'VPN' menu item highlighted with a red box. The main content area is titled 'VPN / Settings' and includes the following sections:

- VPN Global Settings:**
 - Enable VPN
 - Unique Firewall Identifier: 0017C511849C
- VPN Policies:**
 - View IP Version: IPv4 IPv6
 - Refresh Interval (secs): 10
 - Items per page: 50
 - Items: 1 to 2 (of 2)

#	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"/>	

 - Buttons: Add, Delete, Delete All
- Currently Active VPN Tunnels:**
 - Refresh Interval (secs): 10
 - Items per page: 50
 - Items: 0 to 0 (of 0)

#	Created	Name	Local	Remote	Gateway
---	---------	------	-------	--------	---------

Summary statistics at the bottom of the VPN Policies section:

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

In the **General** tab, fill in the name, IPsec primary and secondary gateways, and shared secret. The **IPsec Primary Gateway Name or Address** is the IP address of external network connection of the DSR-1000AC, which is shown as point **c** in the topology. Insert the **Shared Secret** that is the same as the **Pre-shared Key** previously entered in the DSR-1000AC.

The screenshot shows the configuration page for a Security Policy on a SonicWall Network Security Appliance. The interface includes a top navigation bar with the Dell and SonicWALL logos, and tabs for General, Network, Proposals, and Advanced. The 'General' tab is selected. The 'Security Policy' section contains the following fields:

- Policy Type: Site to Site (dropdown)
- Authentication Method: IKE using Preshared Secret (dropdown)
- Name: IPSec_1 (text input)
- IPsec Primary Gateway Name or Address: 1.1.1.2 (text input)
- IPsec Secondary Gateway Name or Address: 0.0.0.0 (text input)

The 'IKE Authentication' section contains the following fields:

- Shared Secret: [masked with dots] (text input)
- Confirm Shared Secret: [masked with dots] (text input)
- Mask Shared Secret (checkbox)
- Local IKE ID: IPv4 Address (dropdown) [empty text input]
- Peer IKE ID: IPv4 Address (dropdown) [empty text input]

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

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

SonicWALL | Network Security Appliance

General **Network** Proposals Advanced

Local Networks

Choose local network from list LAN Subnets

Any address

Remote Networks

Use this VPN Tunnel as default route for all Internet traffic

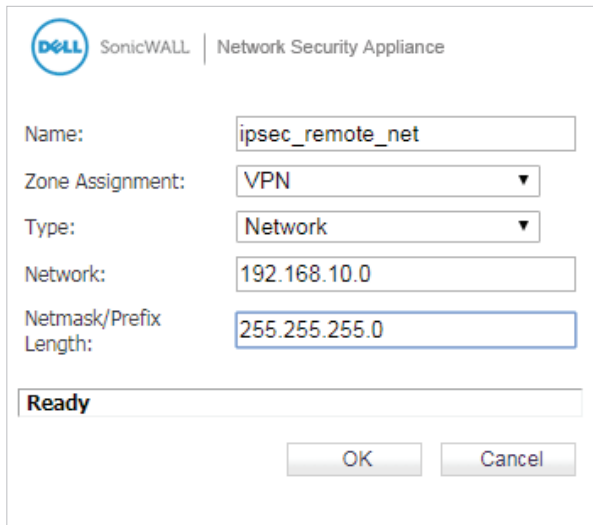
Choose destination network from list create a new address object

Use IKEv2 IP Pool --Select IP Pool Network--

Ready

OK Cancel Help

Configure a new address object to define the IP address of the remote range reachable through the VPN with the DSR-1000AC.



The screenshot shows the configuration window for a new address object in the SonicWall Network Security Appliance. The window title is "SonicWALL | Network Security Appliance". The configuration fields are as follows:


Name:	ipsec_remote_net
Zone Assignment:	VPN
Type:	Network
Network:	192.168.10.0
Netmask/Prefix Length:	255.255.255.0

At the bottom of the configuration area, there is a status field containing the text "Ready". Below the status field are two buttons: "OK" and "Cancel".

Click **OK** and choose the object as a destination.

The screenshot shows a configuration window with four tabs: General, Network, Proposals, and Advanced. The Network tab is active. Under the 'Local Networks' section, the radio button 'Choose local network from list' is selected, and the dropdown menu shows 'LAN Subnets'. Under the 'Remote Networks' section, the radio button 'Choose destination network from list' is selected, and the dropdown menu shows 'ipsec_remote_net'. At the bottom, there is a status bar with the text 'Ready' and three buttons: 'OK', 'Cancel', and 'Help'.

Click the **Proposals** tab. Select the relevant settings as below.

 SonicWALL | Network Security Appliance

General Network **Proposals** Advanced

IKE (Phase 1) Proposal

Exchange:	Main Mode
DH Group:	Group 2
Encryption:	3DES
Authentication:	SHA1
Life Time (seconds):	28800

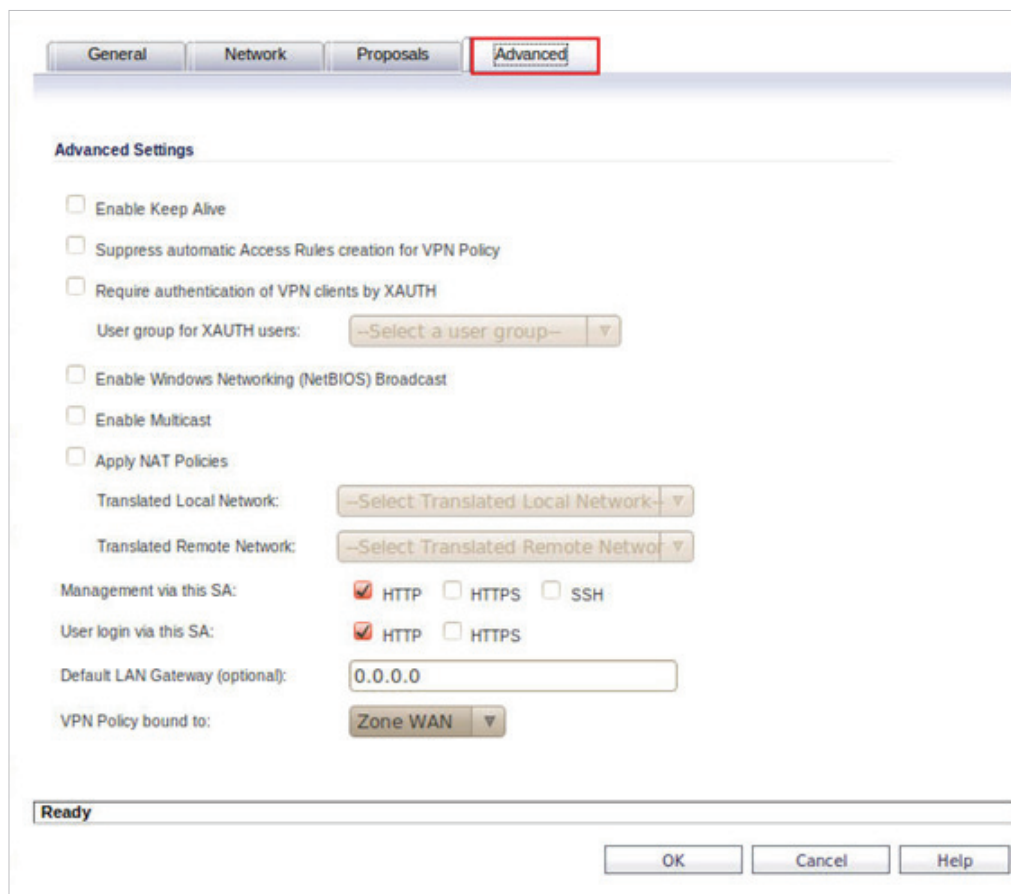
IPsec (Phase 2) Proposal

Protocol:	ESP
Encryption:	3DES
Authentication:	SHA1
<input type="checkbox"/> Enable Perfect Forward Secrecy	
Life Time (seconds):	28800

Ready

OK Cancel Help

Click the “**Advanced**” tab. Select the relevant settings as below.



The screenshot shows the 'Advanced' tab selected in a configuration window. The 'Advanced Settings' section contains the following options:

- 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, a status bar shows 'Ready' and three buttons: 'OK', 'Cancel', and 'Help'.

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

The screenshot shows the SonicWall Network Security Appliance configuration page. The left sidebar contains a navigation menu with options like Dashboard, System, Network, SonicPoint, Firewall, and VPN. The main content area is titled "VPN Policies" and "Currently Active VPN Tunnels".

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
Group/VPN Policies: 2 Policies Defined, 0 Policies Enabled, 8 Maximum Policies Allowed

Currently Active VPN Tunnels

#	Created	Name	Local	Remote	Gateway	
1	06/30/2017 01:27:39	IPSec_1	192.168.1.0 - 192.168.1.255	192.168.10.0 - 192.168.10.255	1.1.1.2	X1 Renegotiate

1 Currently Active VPN Tunnels

Check the statistics to make sure the tunnel is working.

The screenshot shows a "VPN Tunnel Statistics" dialog box with the following information:

- Create Time: 06/30/2017 01:27:39
- Tunnel valid until: 06/30/2017 09:27:39
- Packets In: 31
- Packets Out: 31
- Bytes In: 1860
- Bytes Out: 1860
- Fragments In: 0
- Fragments Out: 0

The dialog box is overlaid on the configuration page, and a mouse cursor is pointing to the "Renegotiate" button.

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 © 2017 D-Link Corporation. All Rights Reserved.