

Tech Note

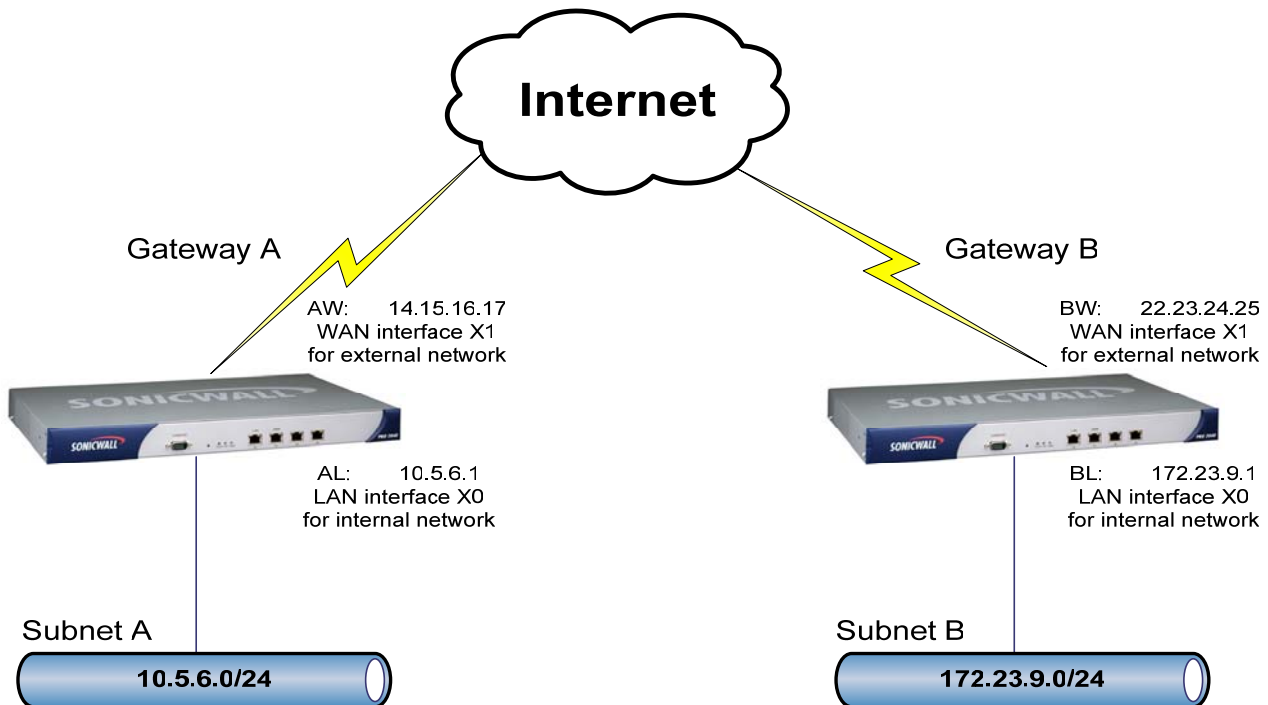
This document describes how to configure a SonicWALL Internet security appliance running SonicOS Enhanced to implement the VPN Consortium IPsec Interoperability specification (<http://www.vpnc.org/InteropProfiles/Interop-01.html>).

This document contains the following sections:

- Gateway-to-Gateway with Preshared Secrets Deployment Scenario Overview
- Setup Process Tasks
- Setup Procedures
- Diagnostics

Scenario 1: Gateway-To-Gateway with Preshared Secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication.



Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

Tech Note

The IKE Phase 1 parameters are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The IKE Phase 2 parameters are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

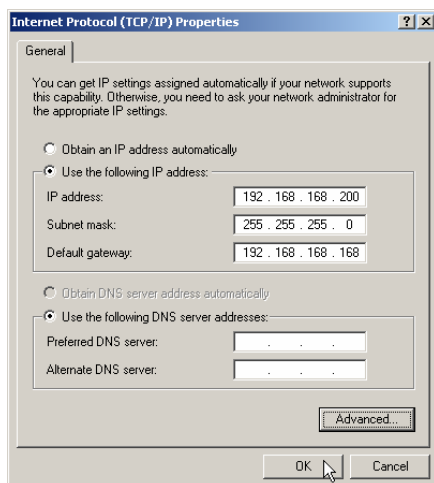
Setup Process Tasks

1. Connect Management Workstation to SonicWALL security appliance Lan Interface (X0)
2. Set IP address of Management Workstation to 192.168.168.200
3. Log into the Management GUI of the SonicWALL security appliance using a current Web browser.
4. Change the IP address of the internal (LAN/X0) interface to 10.5.6.1 and apply the changes
5. Set IP address of Management Workstation to 10.5.6.200 and login again to the SonicWALL security appliance
6. Change the IP address of the external (WAN/X1) interface to 14.15.16.17 and apply the changes
7. Create new VPN Policy
8. Specify Destination Network(s), IKE Phase 1 and Phase 2 properties

Setup Procedures

Connect one end of a CAT5 network cable into the LAN (X0) port of your SonicWALL security appliance. Connect the other end of the cable into the computer you are using to manage the SonicWALL security appliance. If the network card on the management station is not Auto-MDIX (Automatic medium-dependent interface crossover) a crossover type network cable will be required.

Set the IP address of the Management Workstation to:



IP Address: 192.168.168.200
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.168.168

The default network configuration of the SonicWALL security appliance LAN (X0) interface is an IP address of 192.168.168.168 with a 24 bit Subnet Mask (255.255.255.0) Now that both the management workstation and SonicWALL security appliance are configured on the same subnet, it is possible to log into the Management GUI of the SonicWALL security appliance.

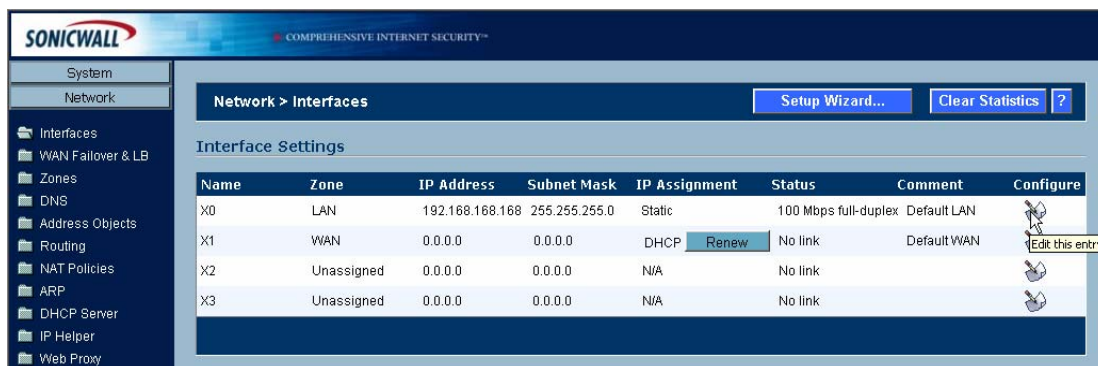


Tech Note

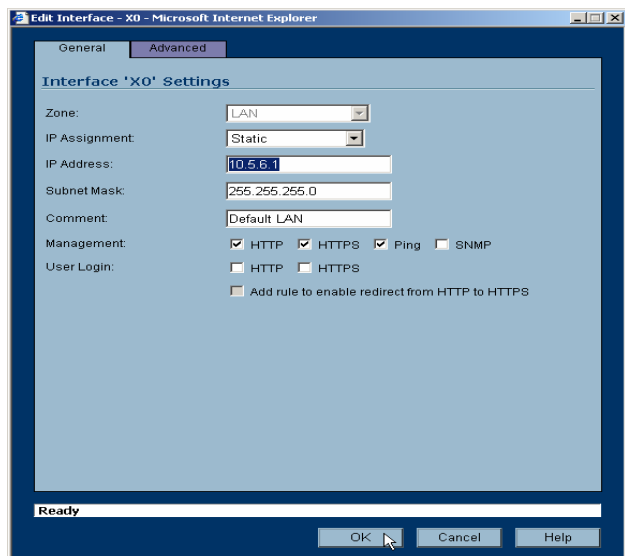
Log into the SonicWALL security appliance's Management GUI using a current Web browser. Open a Web browser and enter https://192.168.168.168 (the default LAN management IP address) in the Location or Address field. The Management Interface displays and prompts you to enter your user name and password. Enter **admin** in the User Name field, **password** in the Password field and press the Login button.



Proceed to the Network > Interfaces page. Under the Interface Settings section, configure the IP Address of the X0 (LAN) port by clicking on the notepad icon. This will bring up the Edit interface dialog page.



On the Edit Interface - X0 - dialog page, enter the IP address of 10.5.6.1 and click ok. Note, this change is immediate and you will lose connectivity to the SonicWALL security appliance.

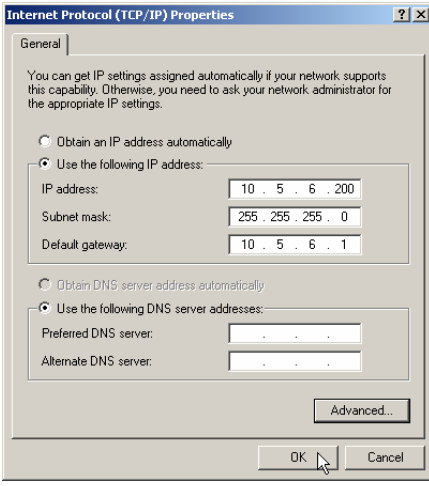


Tech Note

You will see this notice on the bottom of the page to inform you that the browser is now trying to reconnect to SonicWALL security appliance. This will not be possible until you change the IP address of the management PC to match the new IP addressing.

Status: X0 IP address changed. Reconnecting to [10.5.6.1](#).

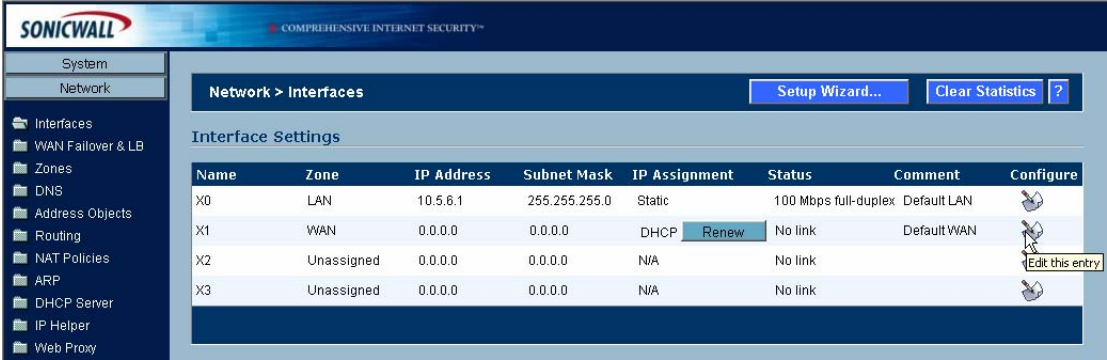
Set the IP address of the Management Workstation to:



IP Address: 10.5.6.200
Subnet Mask: 255.255.255.0
Default Gateway: 10.5.6.1

Now that both the management workstation and SonicWALL security appliance are configured on the same subnet, it is possible to reconnect to the Management GUI of the SonicWALL security appliance.

Log into the SonicWALL security appliance again and go back to the Network > Interfaces page. The X0 LAN interface is now configured and we can now configure the X1 WAN interface by clicking on the notepad icon. This will bring up the Edit interface dialog page.



Tech Note

On the Edit Interface – X1 - dialog page, change the **IP Assignment** to **Static** and enter the **IP address** of **14.15.16.17**.

General Advanced

Interface 'X1' Settings

Zone: WAN

IP Assignment: Static

IP Address: 14.15.16.17

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server 1: 0.0.0.0

DNS Server 2: 0.0.0.0

DNS Server 3: 0.0.0.0

Comment: Default WAN

Management: HTTP HTTPS Ping SNMP

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Ready

OK Cancel Help

The Default Gateway and DNS Servers should also be entered at this time. Also, if desired, you can enable Web management from the WAN on the SonicWALL security appliance by selecting the HTTPS radio button.

Click OK to continue.

The Network > Interfaces page now shows both the LAN and WAN ports correctly addressed. It is now time to create the VPN policy for Gateway B.

Network > Interfaces

Setup Wizard... Clear Statistics ?

Interface Settings

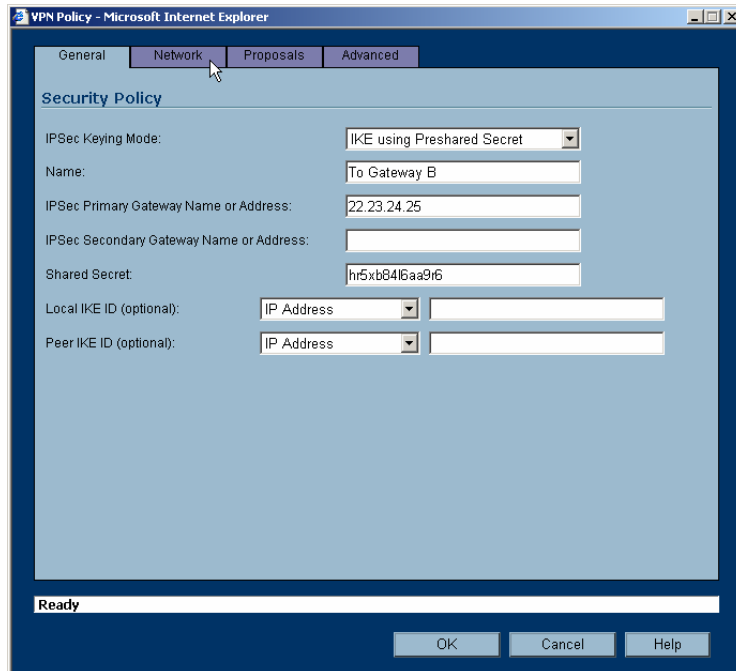
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	10.5.6.1	255.255.255.0	Static	100 Mbps full-duplex	Default LAN	
X1	WAN	14.15.16.17	255.255.255.0	Static	100 Mbps full-duplex	Default WAN	
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

Tech Note

From the navigation bar on the left, click on 'VPN', this will bring up the 'VPN > Settings' page. In the 'VPN Global Settings' section, make sure the 'Enable VPN' radio button is selected. In the 'VPN Policies' section, click on 'Add' to create the new VPN policy for Gateway B.



The 'VPN Policy' window will then appear.



On the 'General' tab page:

Select "**IKE using Preshared Secret**" from the 'IPSec Keying Mode:' dropdown box.

Enter a 'Name:' for the VPN policy. In this example, "**To Gateway B**"

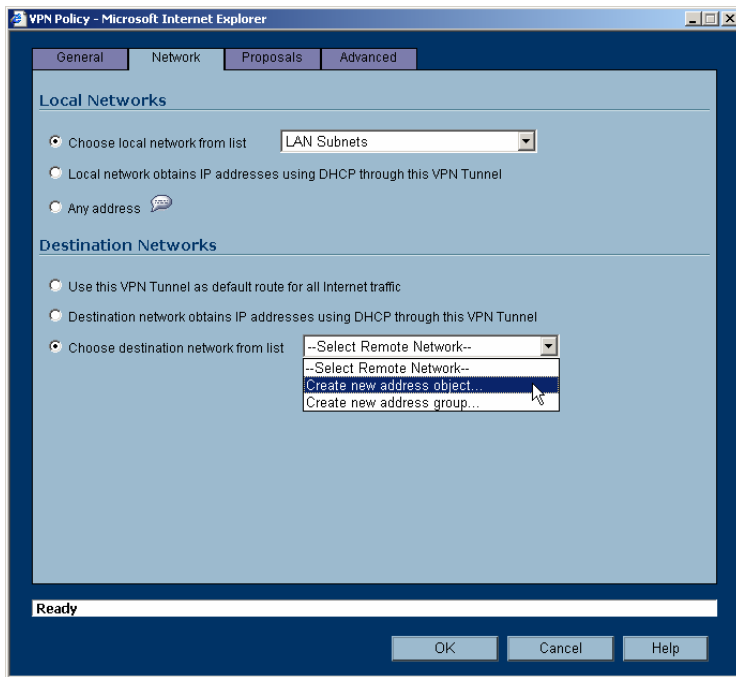
Then enter the IP address of Gateway B in the 'IPSec Primary Gateway Name or Address:' field. In this example, "**22.23.24.25**"

Then enter the preshared secret in the 'Shared Secret:' field. In this example, "**hr5xb84l6aa9r6**".

Next select the 'Network' tab.

Tech Note

On the Network Tab,



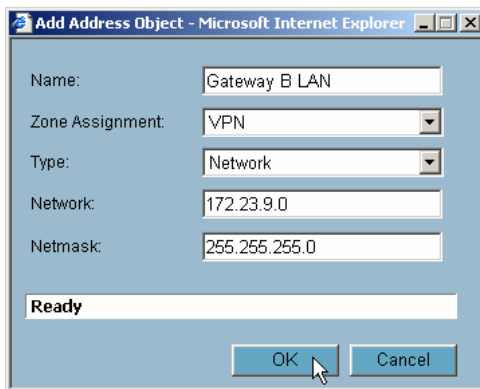
In the 'Local Networks' section,

Select the radio button next to 'Choose local network from list' and select "**LAN Primary Subnet**" from the drop-down box.

In the 'Destination Networks' section,

Select the radio button next to 'Choose destination network from list' and select "**Create New Address object**" from the dropdown box. This will bring up the "Add Address Object" dialog to create the address object for the LAN behind Gateway B.

The address object is for the LAN behind the Gateway B.



The 'Name:' is "**Gateway B LAN**"

The 'Zone Assignment:' is "**VPN**"

The 'Type:' is "**Network**"

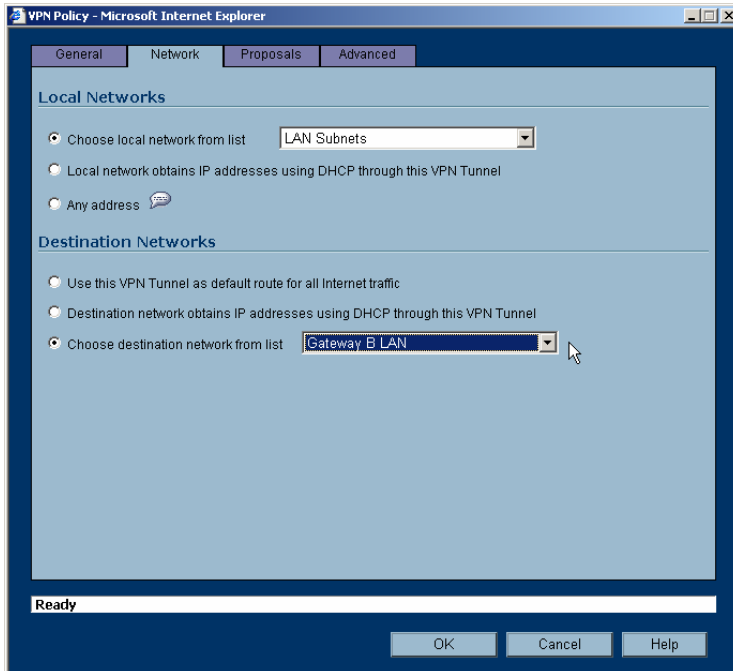
The 'Network:' is "**172.23.9.0**".

The 'Netmask:' is "**255.255.255.0**"

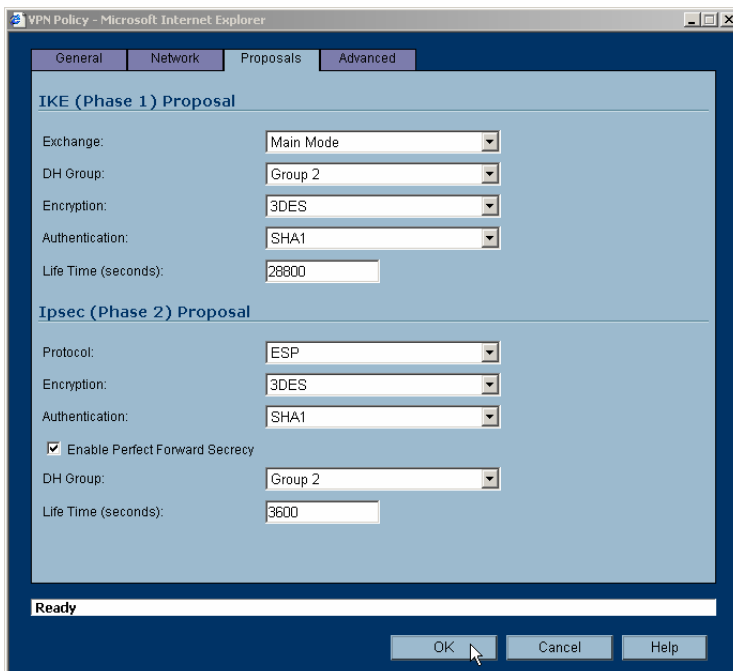
Click 'OK' to finish.

Tech Note

The Networks are now configured with the correct Local and Destination networks. Next, click on the Proposals tab.



On the 'Proposals' tab make sure the correct values are entered for both Phase 1 and 2 proposals.



For the 'IKE (Phase 1) Proposal' section:
'Exchange:' is "**Main Mode**"
'DH Group' is "**Group 2**"
'Encryption' is "**3DES**"
'Authentication' is "**SHA1**"
'Life Time (seconds)' is "**28800**"

For the 'Ipsec (Phase 2) Proposal' section:
'Protocol' is "**ESP**"
'Encryption' is "**3DES**"
'Authentication' is "**SHA1**"
'DH Group' is "**Group 2**"
'Life Time (seconds)' is "**3600**"

Enable Perfect Forward Security checked.

Click 'OK' to finish.

Tech Note

The VPN Policy has now been successfully created.

The screenshot shows the 'VPN > Settings' page in the SonicWall management interface. At the top, there are buttons for 'VPN Policy Wizard...', 'Apply', 'Cancel', and a help icon. Below this is the 'VPN Global Settings' section, which includes a checked 'Enable VPN' option and a 'Unique Firewall Identifier' field containing '0006B111066C'. The 'VPN Policies' section shows a table with three policies:

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	[Icons]
2	WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	[Icons]
3	To Gateway B	22.23.24.25	172.23.9.1 - 172.23.9.255	ESP 3DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	[Icons]

At the bottom of the table are buttons for 'Add...', 'Delete', and 'Delete All'.

Next, from the main navigation bar on the left, click on 'VPN', then 'Advanced' this will bring up the 'VPN > Advanced VPN Settings' page. In the 'Advanced VPN Settings' section, deselect the 'Enable NAT Traversal' radio button. This will disable NAT Traversal and ensure interoperability with devices that use different draft versions of the NAT-T specification. Click **Apply** to update the configuration. The VPN policy configuration is now complete.

The screenshot shows the 'VPN > Advanced VPN Settings' page in the SonicWall management interface. The left sidebar contains a navigation menu with 'VPN' selected. The main content area has the title 'VPN > Advanced VPN Settings' and buttons for 'Apply', 'Cancel', and a help icon. Below the title is the 'Advanced VPN Settings' section with the following options:

- Enable IKE Dead Peer Detection
 - Dead Peer Detection Interval (seconds): 60
 - Failure Trigger Level (missed heartbeats): 3
- Enable Dead Peer Detection for Idle vpn sessions
 - Dead Peer Detection Interval for Idle vpn sessions (seconds): 600
- Enable Fragmented Packet Handling
- Ignore DF (Don't Fragment) Bit
- Enable NAT Traversal (highlighted with a red box)
- 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
 - OCSP Responder URL: [Text Field]
- Send vpn tunnel traps only when tunnel status changes

At the bottom left, the status is 'Ready'.

Tech Note

To activate the VPN Policy, send traffic through the VPN tunnel. When the VPN policy establishes the connection, it will appear in the **Currently Active VPN Tunnels** section and a green dot will be shown in the **VPN Policies** section.









VPN > Settings VPN Policy Wizard... Apply Cancel ?

VPN Global Settings

Enable VPN
Unique Firewall Identifier:

VPN Policies

Items to 3 (of 3) ⏪ ⏩


#	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	To Gateway B	22.23.24.25	● 172.23.9.1 - 172.23.9.255	ESP 3DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	 

Add... Delete Delete All

Site To Site Policies: [1 Policies Defined, 1 Policies Enabled, 50 Maximum Policies Allowed](#)
GroupVPN Policies: [2 Policies Defined, 0 Policies Enabled, 8 Maximum Policies Allowed](#)

Currently Active VPN Tunnels

Items to 1 (of 1) ⏪ ⏩

#	Name	Local	Remote	Gateway	
1	To Gateway B	10.5.6.1 - 10.5.6.255	172.23.9.1 - 172.23.9.255	22.23.24.25	Renegotiate 

[1 Currently Active VPN Tunnels](#)

Tech Note

Diagnostics

The Diagnostic Tools are located on the **System > Diagnostics** page. To test network connectivity you can pick Ping from the list of Diagnostic Tools.

System > Diagnostics

Tech Support Report

VPN Keys ARP Cache
 DHCP Bindings IKE Info

[Download Report](#)

Diagnostic Tools

Diagnostic Tool:

Ping

Ping host or IP address: [Go](#)

System > Diagnostics

Tech Support Report

VPN Keys ARP Cache
 DHCP Bindings IKE Info

[Download Report](#)

Diagnostic Tools

Diagnostic Tool:

Ping

Ping host or IP address: [Go](#)

The Logs are also very useful in troubleshooting the VPN. The logs are located on the **Log > View** page.

Log View Items to 7 (of 7) [↩](#) [⏪](#) [⏩](#) [↪](#)

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	08/23/2005 19:13:22.400	Info	VPN IKE	IKE negotiation complete. Adding IPSec SA. (Phase 2)	14.15.16.17	22.23.24.25		
2	08/23/2005 19:13:22.400	Info	VPN IKE	IKE Initiator: Accepting IPSec proposal (Phase 2)	14.15.16.17	22.23.24.25	10.5.6.0 / 255.255.255.0 -> 172.23.9.0/255.255.255.0	
3	08/23/2005 19:13:22.288	Info	VPN IKE	IKE Initiator: Start Quick Mode (Phase 2).	14.15.16.17, 500	22.23.24.25, 500		
4	08/23/2005 19:13:22.288	Info	VPN IKE	IKE Initiator: Main Mode complete (Phase 1)	14.15.16.17, 500	22.23.24.25, 500	3DES SHA1 Group 2 lifeSeconds=28800	
5	08/23/2005 19:13:22.288	Info	VPN IKE	NAT Discovery : No NAT/NAPT device detected between IPSec Security gateways	14.15.16.17, 500	22.23.24.25, 500		
6	08/23/2005 19:13:22.192	Info	VPN IKE	IKE Initiator: Start Main Mode negotiation (Phase 1)	14.15.16.17, 500	22.23.24.25, 500		
7	08/23/2005 19:13:12.688	Info	Firewall Logging	Log Cleared				