

## SonicWALL VPN with Raptor PowerVPN 6.5

Prepared by SonicWALL, Inc.  
06/19/2002

### Introduction:

VPN standards are still evolving and interoperability between products is a continued effort. SonicWALL has made progress in this area and is interoperable with Raptor PowerVPN using IKE as shown below. Advanced setups are possible but are not covered in this document.

This tech-note assumes the reader has a working knowledge of Raptor PowerVPN management tools and SonicWALL appliance configuration. This tech-note describes the required steps to set-up a compatible Security Association on both Raptor PowerVPN and SonicWALL products.

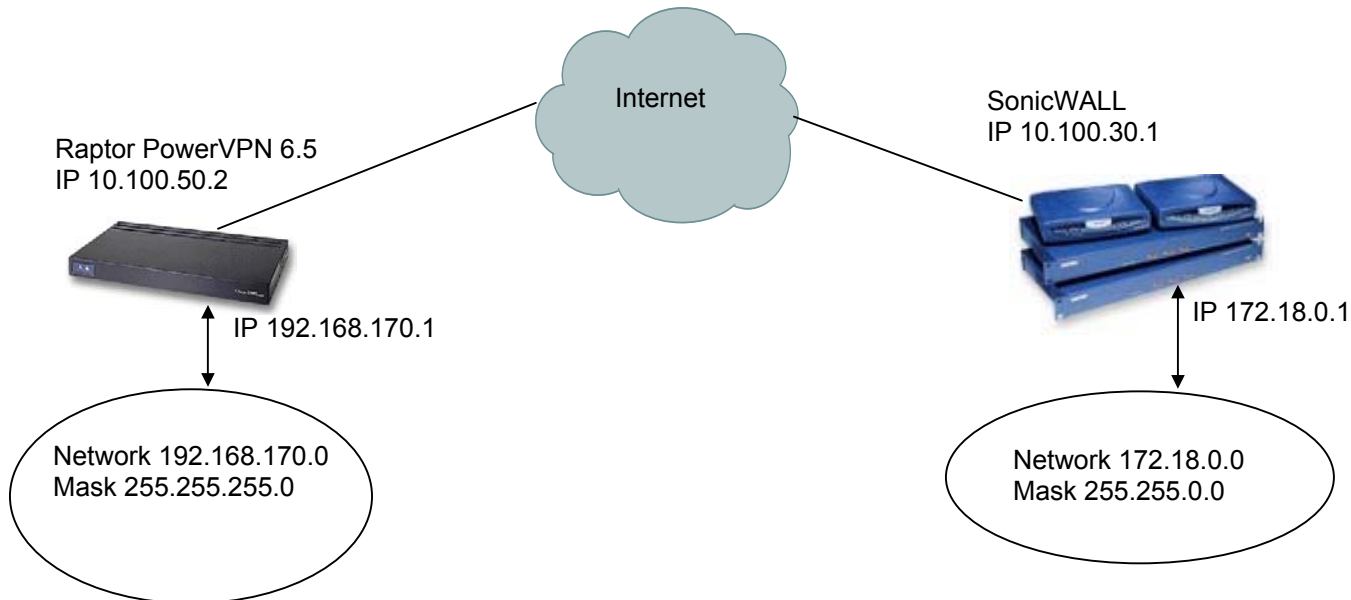
### Technical Notes:

SonicWALL has tested VPN interoperability with Raptor PowerVPN version 6.5 and SonicWALL Pro 300 version 6.3.1.0 using the following VPN Security Association information:

Keying Mode:	IKE
IKE Mode:	Main Mode with No PFS (perfect forward secrecy)
SA Authentication Method:	Pre-Shared key
Keying Group:	DH (Diffie Hellman) – Group 2
Encryption and Data Integrity:	ESP 3DES with SHA1

### EXAMPLE:

The network configuration shown below is used in the example VPN configuration. The example will configure a VPN using 3DES encryption with SHA1 and without PFS.



## SonicWALL VPN with Raptor PowerVPN 6.5

## SonicWALL Configuration

## On the SonicWALL, create an SA

Change the IPSec Keying Mode to IKE using pre-shared secret

Name your SA (In this example, Raptor)

Fill in the IPSec gateway (in this example, 10.100.50.2)

Select Group 2 for Phase 1 DH Group

Select 3DES SHA1 for Phase 1 Encryption/Authentication

Select ESP 3DES HMAC SHA1 for Phase 2 Encryption/Authentication

Enter your Shared Secret, (In this example, passwordpasswordpass)

Fill in the appropriate Destination Network (in this example, 192.168.170.0) and Subnet Mask (in this example, 255.255.255.0)

A Sample Screen shot from SonicWALL firmware version 6.3.1.0 is displayed below

The screenshot shows the SonicWALL configuration interface for adding or modifying an IPSec Security Association (SA). The interface is divided into several sections:

- Summary:** Security Association: Raptor; IPsec Keying Mode: IKE using Preshared Secret; Name: Raptor; Disable This SA: ; IPsec Gateway Address: 10.100.50.2
- Security policy:** Phase 1 DH Group: Group 2; SA Life time (secs): 28800; Phase 1 Encryption/Authentication: 3DES & SHA1; Phase 2 Encryption/Authentication: Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1); Shared Secret: passwordpasswordpass
- Destination Networks:**
  - Use this SA as default route for all Internet traffic
  - Destination network obtains IP addresses using DHCP through this SA
  - Specify destination networks below

Network	Subnet Mask		
192.168.170.0	255.255.255.0		

Buttons: Add New Network..., Advanced Settings..., Delete This SA

At the bottom right, there are buttons for Update and Reset.

## SonicWALL VPN with Raptor PowerVPN 6.5

Click on Advanced Settings  
Select Group 2 for Phase 2 DH Group  
Click OK  
Click Update

A sample screen shot from SonicWALL firmware version 6.3.1.0 is displayed below

### Edit Advanced Settings

Use Aggressive Mode

Enable Keep Alive

Require authentication of local users

Require authentication of remote users

Remote users behind VPN gateway  
 Remote VPN clients with XAUTH

Enable Windows Networking (NetBIOS) broadcast

Apply NAT and firewall rules

Forward packets to remote VPNs

Enable Perfect Forward Secrecy

Phase 2 DH Group

Default LAN Gateway

VPN Terminated at  LAN  DMZ  LAN/DMZ

*Note that after clicking OK you must click Update on the main page to save changes made here.*

## Raptor PowerVPN 6.5 Configuration

### Create Raptor Gateway

Open up base components


Right click on Network Entities, select New, and select Security Gateway

Name the gateway(in this example, Raptor)

Make sure Type is Security Gateway

**raptortest\Network Entity\Raptor Properties** ? X

General | **Security Gateway** | In Use By

 Please enter a name and description and select the Network Entity type.

Name:

Description:

Type:

OK Cancel Help

## SonicWALL VPN with Raptor PowerVPN 6.5

**Select the Security Gateway Tab**

- Select the WAN IP address of the raptor firewall from the IP Address pull down menu
- Check Enable IKE
- Make sure Phase 1 ID is left blank
- Click OK

The screenshot shows the 'raptortest\Network Entity\Raptor Properties' dialog box with the 'Security Gateway' tab selected. The dialog contains the following elements:

- General** | **Security Gateway** | In Use By
- Icon of a globe and computer with the text: "Please enter the address of the Security Gateway and complete the IKE information."
- IP Address: 10.100.50.2 (dropdown menu)
- Enable IKE (Internet Key Exchange / ISAKMP)
- IKE Parameters section:
  - Phase1 ID: (empty text box)
  - (Leave Phase1 ID blank to use IP Address)
  - Certificate
  - Shared Secret: (empty text box) [Reveal]
- Buttons: OK, Cancel, Help

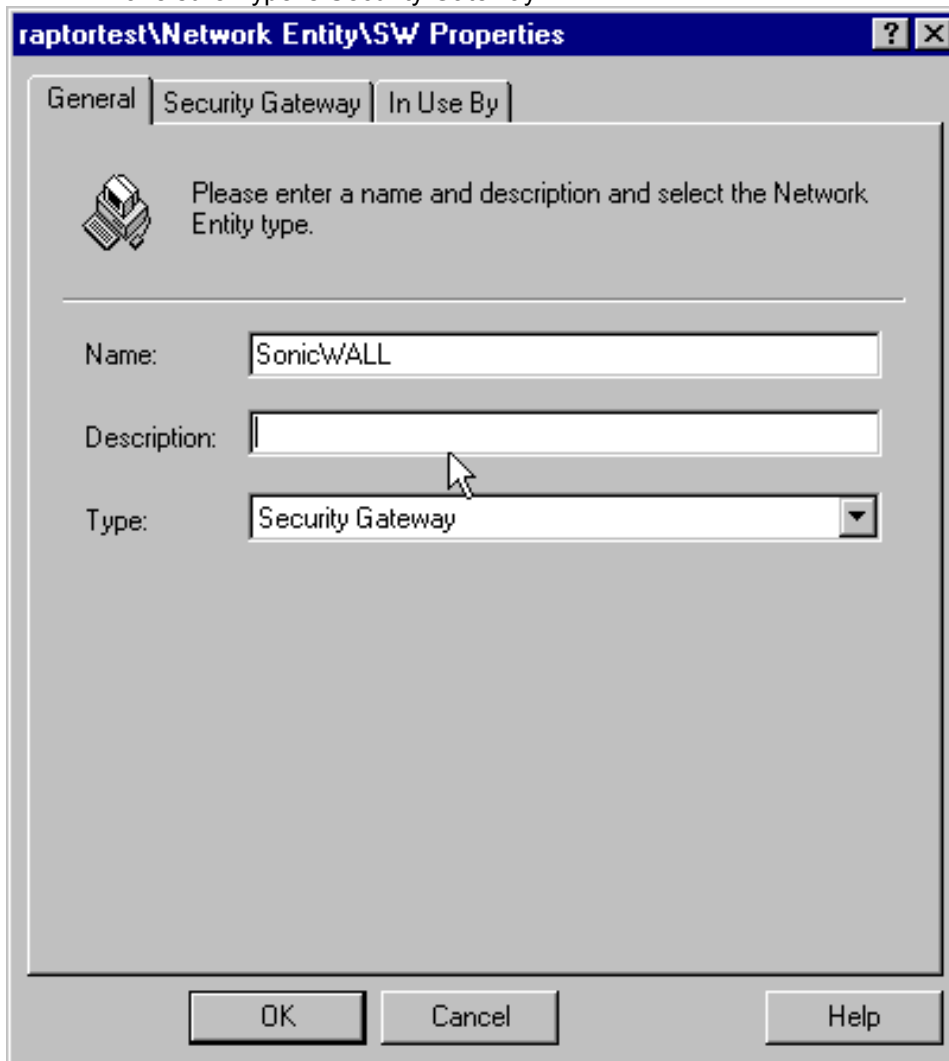
## SonicWALL VPN with Raptor PowerVPN 6.5

**Create SonicWALL Gateway**

Right click on Network Entities, select New, and select Security Gateway

Name the gateway(In this example, SonicWALL)

Make sure Type is Security Gateway



The screenshot shows a Windows-style dialog box titled "raptortest\Network Entity\SW Properties". It has three tabs: "General", "Security Gateway", and "In Use By". The "General" tab is active. Inside the dialog, there is a message: "Please enter a name and description and select the Network Entity type." Below this message are three input fields: "Name:" with the text "SonicWALL", "Description:" which is empty, and "Type:" which is a dropdown menu currently showing "Security Gateway". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

## SonicWALL VPN with Raptor PowerVPN 6.5

**Select the Security Gateway Tab**

Select the WAN IP address of the SonicWALL from the IP Address pull down menu

Check Enable IKE

Make sure Phase 1 ID is left blank

Select Shared Secret

Enter the same secret you entered on the SonicWALL

*Note: Raptor requires this to be at least 20 characters long*

Click OK

The screenshot shows a Windows-style dialog box titled "raptortest\Network Entity\SW Properties". It has three tabs: "General", "Security Gateway", and "In Use By". The "Security Gateway" tab is selected. The dialog contains the following elements:

- A globe icon and the text: "Please enter the address of the Security Gateway and complete the IKE information."
- An "IP Address:" label followed by a dropdown menu containing "10.100.30.1".
- A checked checkbox labeled "Enable IKE (Internet Key Exchange / ISAKMP)".
- An "IKE Parameters" section containing:
  - A "Phase1 ID:" label followed by an empty text box, with the instruction "(Leave Phase1 ID blank to use IP Address)".
  - Two radio buttons: "Certificate" (unselected) and "Shared Secret" (selected).
  - A "Shared Secret:" label followed by a text box containing "passwordpasswordpass" and a "Hide" button.
- At the bottom, there are three buttons: "OK", "Cancel", and "Help".

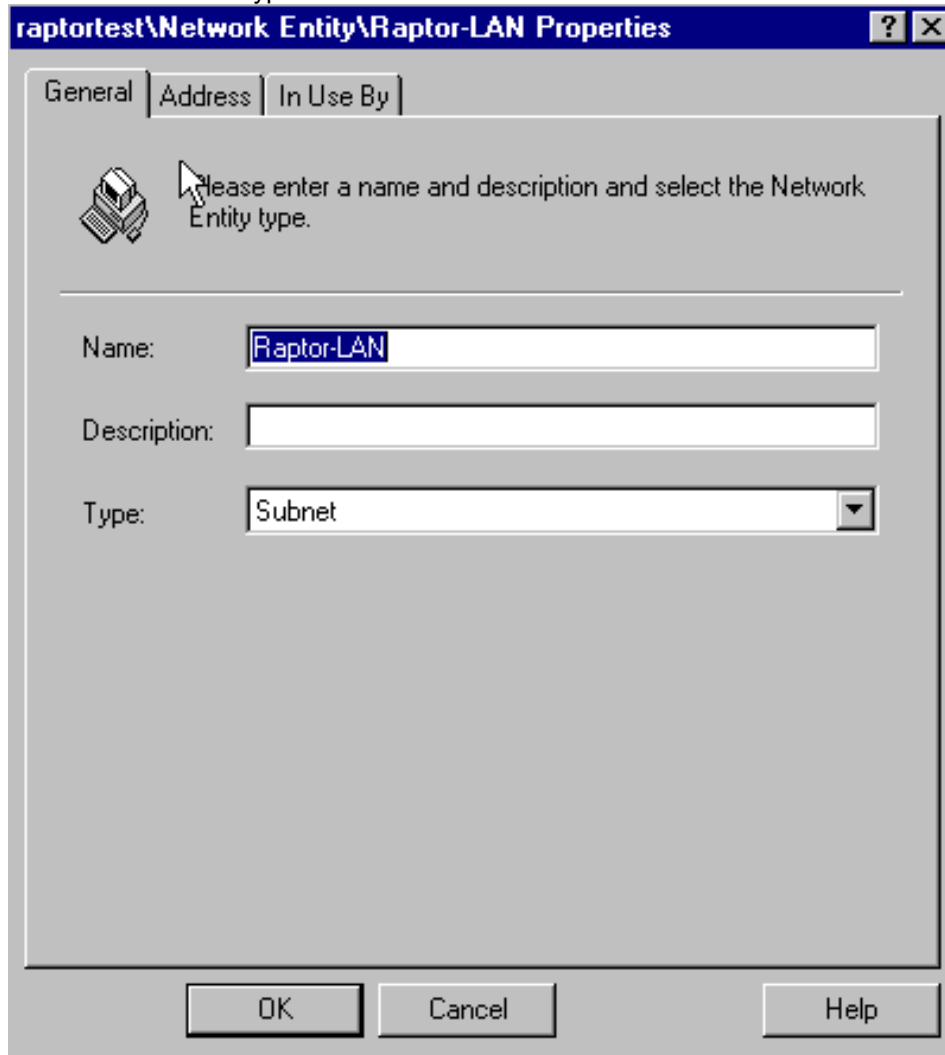
## SonicWALL VPN with Raptor PowerVPN 6.5

**Create Raptor Subnet**

Right click on Network Entities, select New, and select Subnet


Enter a Name for the Subnet

Make sure Type is Subnet



**raptortest\Network Entity\Raptor-LAN Properties** ? X

General | Address | In Use By

 Please enter a name and description and select the Network Entity type.

Name:

Description:

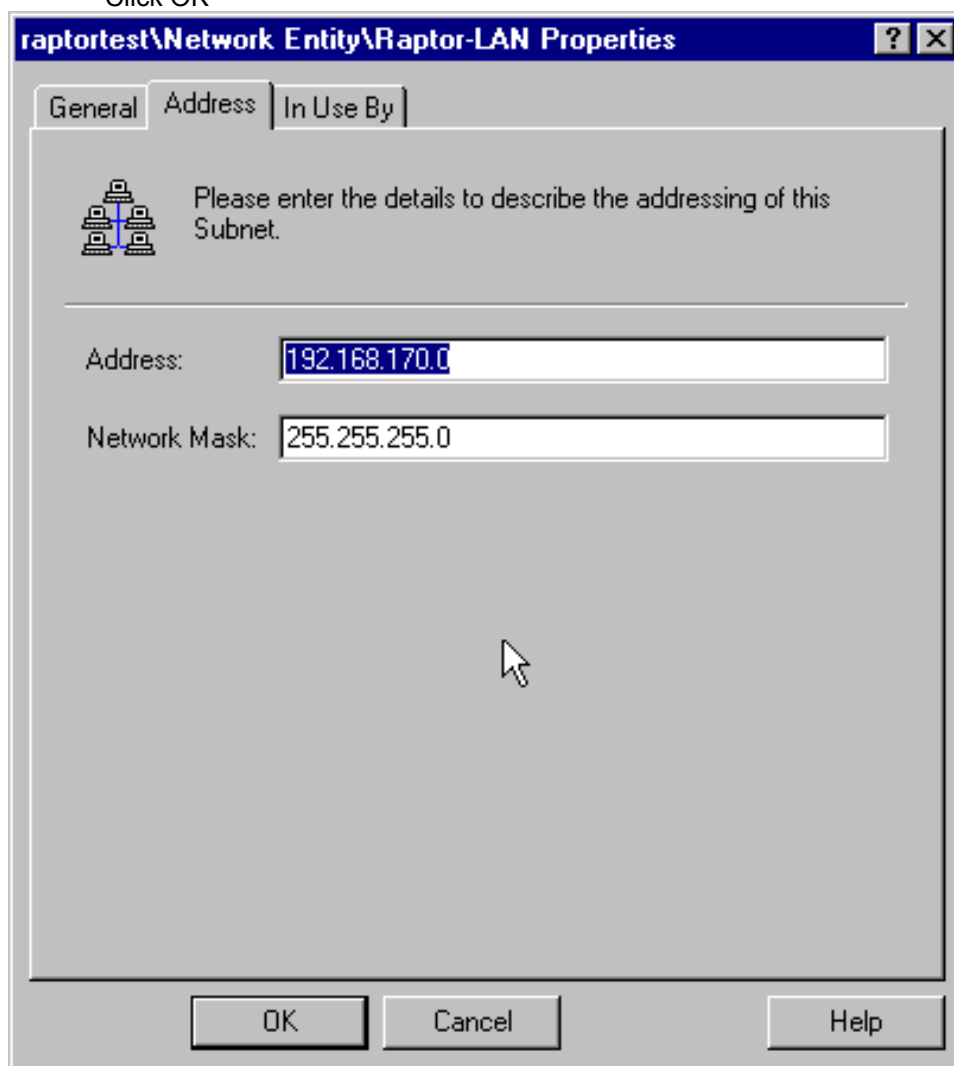
Type:

OK Cancel Help

## SonicWALL VPN with Raptor PowerVPN 6.5

**Click on the Address Tab**

Enter the LAN network and subnet mask which is behind the Raptor  
Click OK



The screenshot shows a dialog box titled "raptortest\Network Entity\Raptor-LAN Properties". It has three tabs: "General", "Address", and "In Use By". The "Address" tab is selected. The dialog contains a message: "Please enter the details to describe the addressing of this Subnet." Below this message are two input fields: "Address:" with the value "192.168.170.0" and "Network Mask:" with the value "255.255.255.0". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

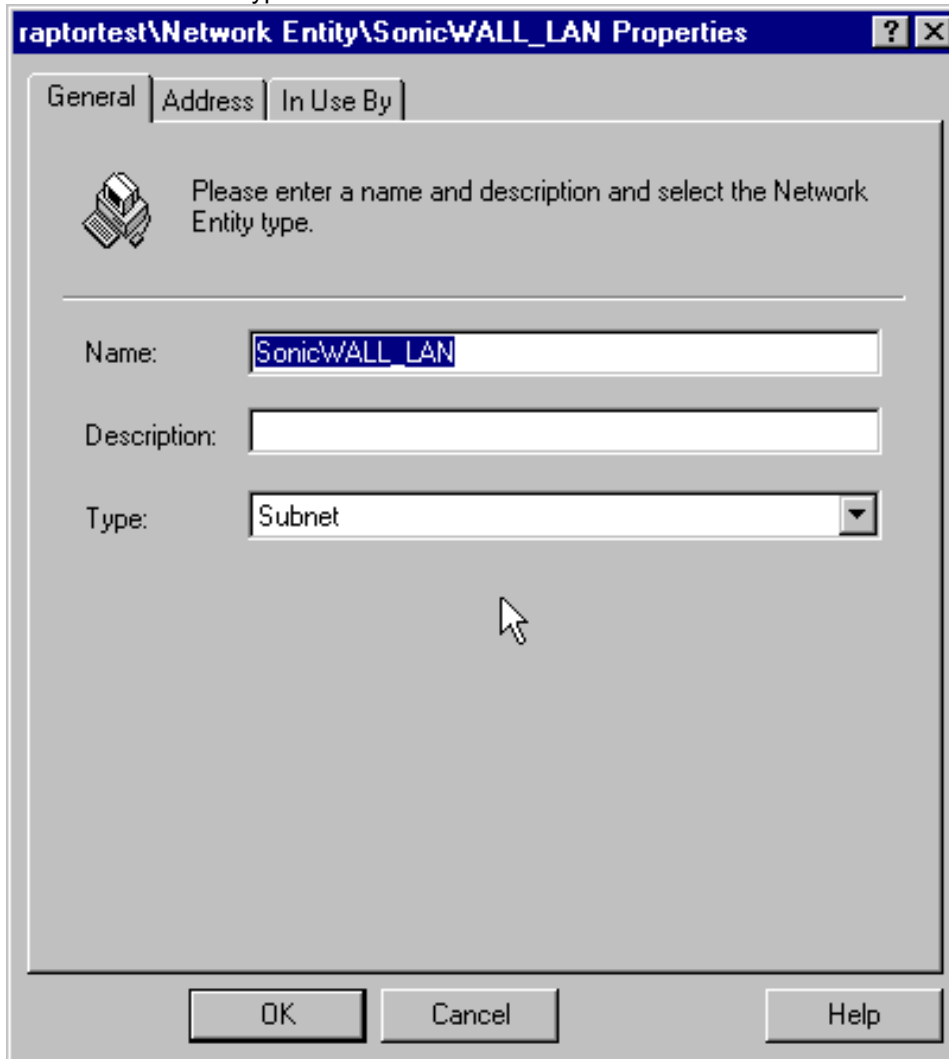
## SonicWALL VPN with Raptor PowerVPN 6.5

**Create SonicWALL Subnet**

Right click on Network Entities, select New, and select Subnet

Enter a Name for the subnet

Make sure Type is Subnet

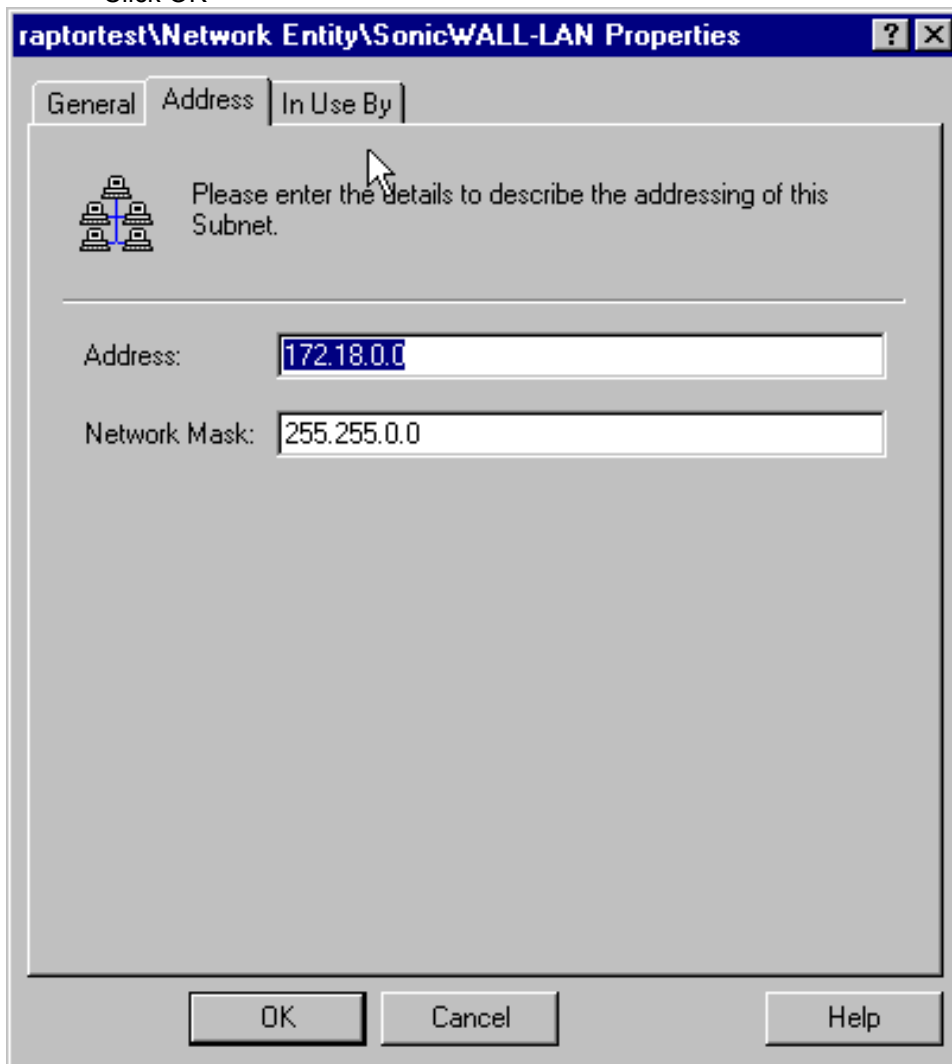


The screenshot shows a dialog box titled "raptortest\Network Entity\SonicWALL\_LAN Properties". It has three tabs: "General", "Address", and "In Use By". The "General" tab is active. Inside the dialog, there is a message: "Please enter a name and description and select the Network Entity type." Below this message are three input fields: "Name:" with the text "SonicWALL\_LAN", "Description:" which is empty, and "Type:" which is a dropdown menu currently showing "Subnet". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

## SonicWALL VPN with Raptor PowerVPN 6.5

**Click on the Address Tab**

Enter the LAN network and subnet mask which is behind the SonicWALL  
Click OK



The screenshot shows a Windows-style dialog box titled "raptortest\Network Entity\SonicWALL-LAN Properties". It has three tabs: "General", "Address", and "In Use By". The "Address" tab is selected. The dialog contains a message: "Please enter the details to describe the addressing of this Subnet." Below this message are two text input fields. The first field is labeled "Address:" and contains the text "172.18.0.0". The second field is labeled "Network Mask:" and contains the text "255.255.0.0". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

## SonicWALL VPN with Raptor PowerVPN 6.5

**Edit IKE Policy**

Open up the Virtual Private networks folder  
Select IKE Policy  
Right click global\_ike\_policy, select properties  
Select SHA1 for Data Integrity Preference 1<sup>st</sup>  
Select BLANK for Data Integrity Preference 2<sup>nd</sup>  
Select 3DES for Data Privacy Preference 1<sup>st</sup>  
Select BLANK for Data Privacy Preference 2<sup>nd</sup>  
Select Group2 for Diffie-Hellman Preference 1<sup>st</sup>  
Select BLANK for Diffie-Hellman Preference 2<sup>nd</sup>  
Enter number of seconds for Time Expiration.

**NOTE: This is for Phase One and should match the SonicWALL Phase One Settings. See page 2**

The screenshot shows a Windows-style dialog box titled "raptortest\IKE Policy\global\_ike\_policy Properties". The "General" tab is active. At the top, there is a message: "Please specify the global IKE Policy." Below this, there are three sections for preferences:

- Data Integrity Preference:** 1st dropdown is "SHA1", 2nd dropdown is empty.
- Data Privacy Preference:** 1st dropdown is "3DES", 2nd dropdown is empty.
- Diffie-Hellman Preference:** 1st dropdown is "Group2", 2nd dropdown is empty.

At the bottom, there is a "Time Expiration" field with the value "28800". The dialog has "OK", "Cancel", and "Help" buttons at the bottom.

## SonicWALL VPN with Raptor PowerVPN 6.5

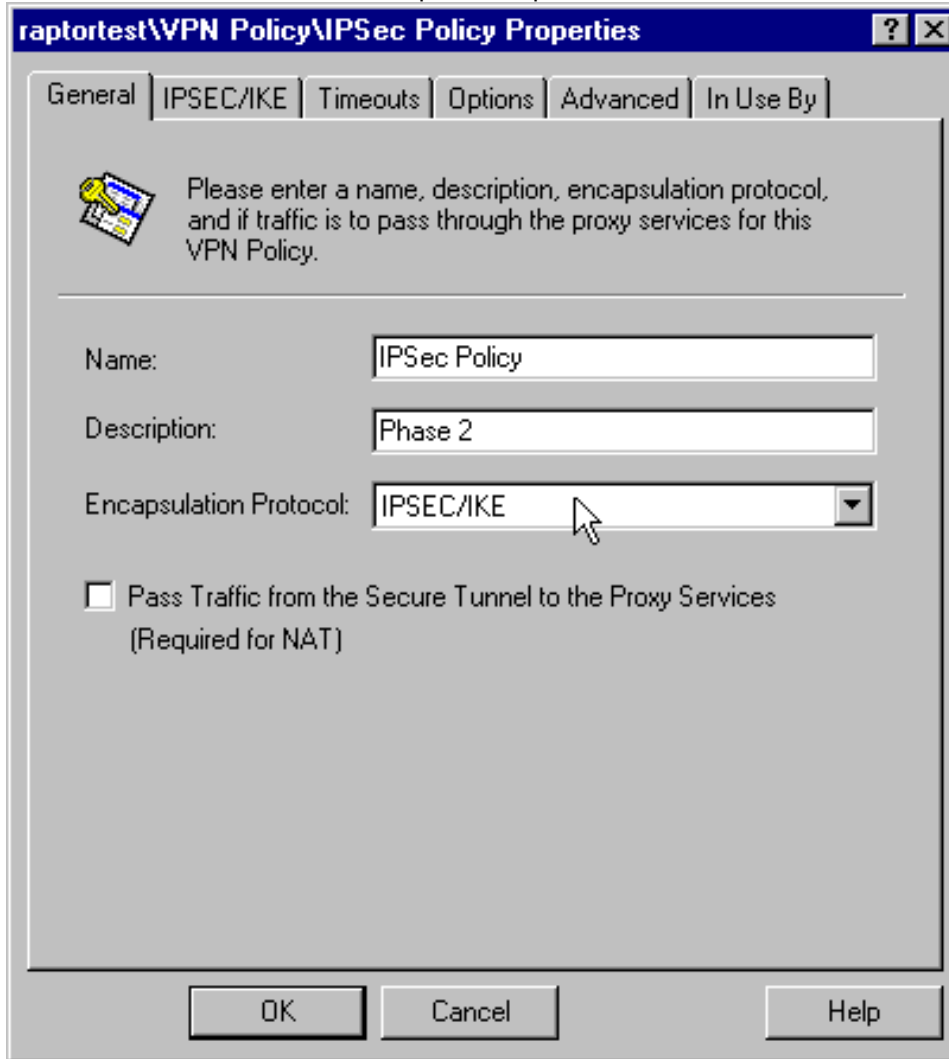
**Create VPN Policy**

Under Virtual Private Networks

Right Click on VPN Policy, select New, Select VPN Policy


Name the policy

Select IPSEC/IKE for encapsulation protocol



**raptortest\VPN Policy\IPSec Policy Properties** ? X

General | IPSEC/IKE | Timeouts | Options | Advanced | In Use By

 Please enter a name, description, encapsulation protocol, and if traffic is to pass through the proxy services for this VPN Policy.

Name:

Description:

Encapsulation Protocol:

Pass Traffic from the Secure Tunnel to the Proxy Services  
(Required for NAT)

OK Cancel Help

## SonicWALL VPN with Raptor PowerVPN 6.5

**Select the IPSEC/IKE Tab**

Select SHA1 for Data Integrity Preference 1<sup>st</sup>

Leave Blank for Data Integrity Preference 2<sup>nd</sup>

Select 3DES for Data Privacy Preference 1<sup>st</sup>

Leave Blank for Data Privacy Preference 2<sup>nd</sup>

Leave NONE for Data Compression

**NOTE: This is for Phase Two and should match the SonicWALL Phase Two Settings. See page 2**

raptortest\VPN Policy\NewVPNPolicy Properties (New)

General IPSEC/IKE Timeouts Options Advanced In Use By

Please select the integrity, encryption, and compression algorithms for this VPN Policy.

Data Integrity Preference:  
1st SHA1 2nd 3rd

Data Privacy Preference:  
1st 3DES 2nd 3rd

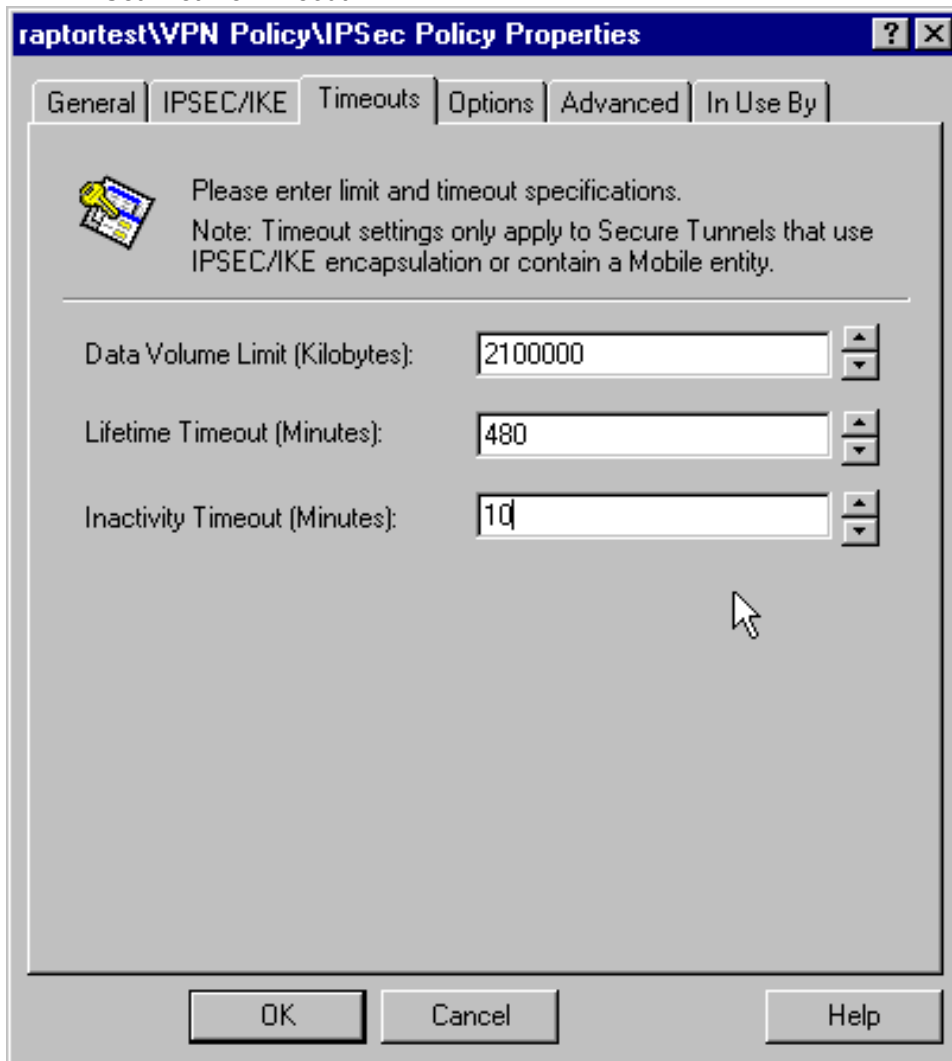
Data Compression: <NONE>

OK Cancel Help

## SonicWALL VPN with Raptor PowerVPN 6.5

## Select the Timeouts Tab

Set Lifetime Timeout



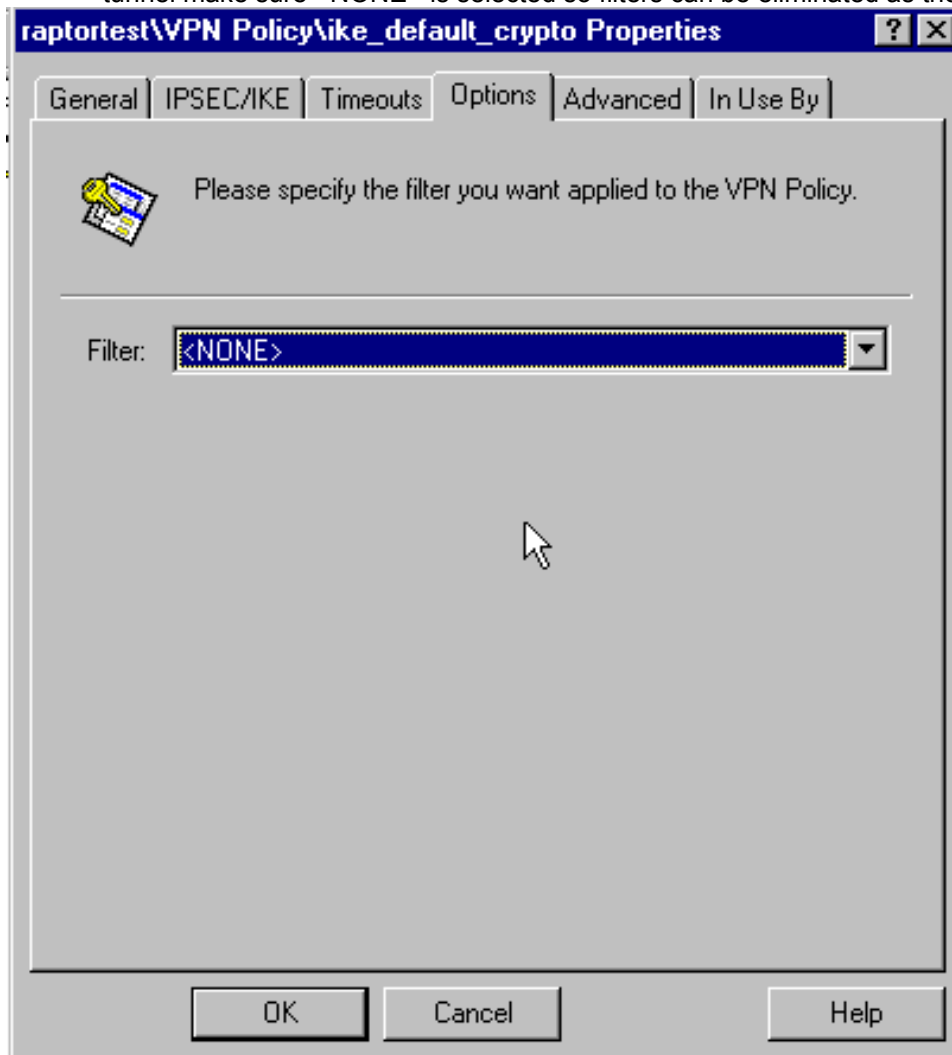
The screenshot shows a dialog box titled "raptorrest\VPN Policy\IPSec Policy Properties" with a help icon and a close button. The "Timeouts" tab is selected, and the "Set Lifetime Timeout" sub-tab is active. The dialog contains a message icon and text: "Please enter limit and timeout specifications. Note: Timeout settings only apply to Secure Tunnels that use IPSEC/IKE encapsulation or contain a Mobile entity." Below this, there are three input fields with up/down arrows: "Data Volume Limit (Kilobytes):" with the value "2100000", "Lifetime Timeout (Minutes):" with the value "480", and "Inactivity Timeout (Minutes):" with the value "10". At the bottom, there are "OK", "Cancel", and "Help" buttons.

Setting	Value
Data Volume Limit (Kilobytes)	2100000
Lifetime Timeout (Minutes)	480
Inactivity Timeout (Minutes)	10

## SonicWALL VPN with Raptor PowerVPN 6.5

**Select Options Tab**

Select <NONE> for filters(this is not necessary, but if you have problems bringing up the tunnel make sure <NONE> is selected so filters can be eliminated as the problem)



## SonicWALL VPN with Raptor PowerVPN 6.5

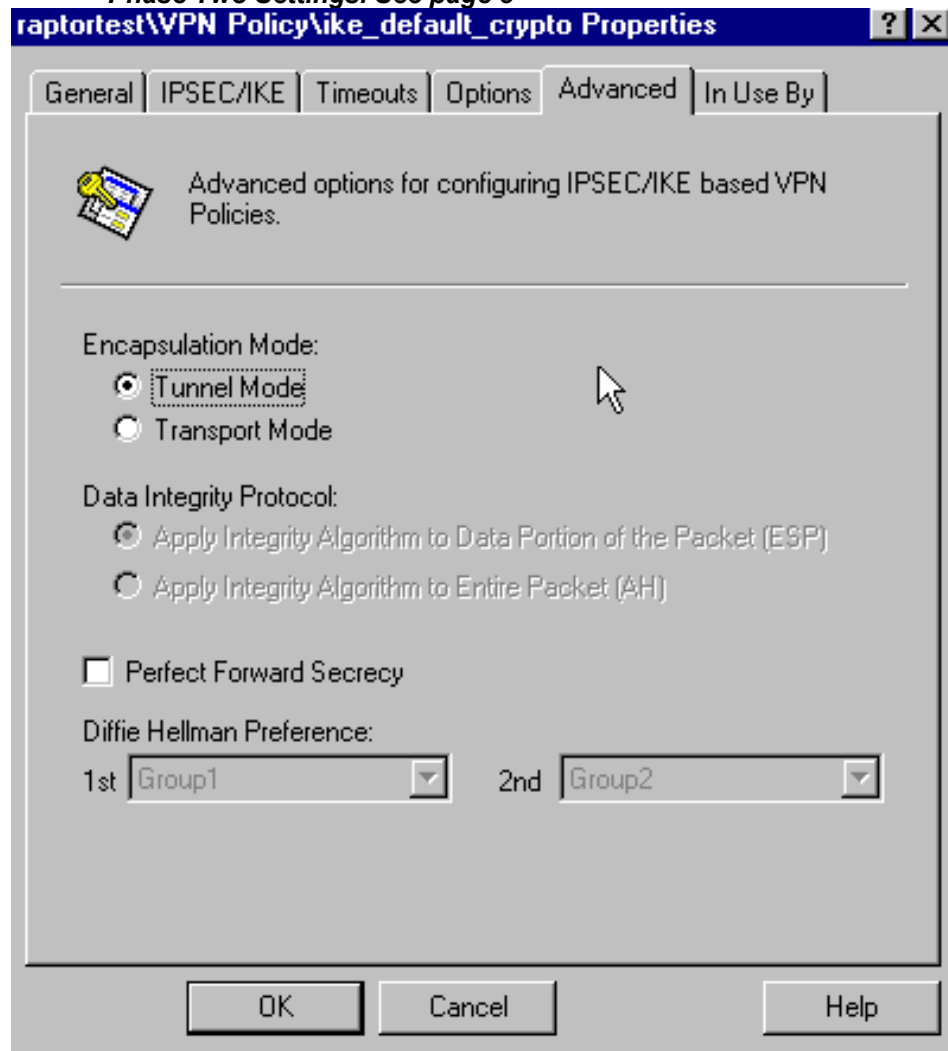
**Select the Advanced Tab**

Select Tunnel Mode

Make sure PFS is not checked.

Click OK

**NOTE: This is for Phase Two and should match the SonicWALL Phase Two Settings. See page 3**



## SonicWALL VPN with Raptor PowerVPN 6.5

**Create Secure Tunnel**

Right Click Secure Tunnels, select New, and select Secure Tunnel

Name the Secure Tunnel

Select Raptor\_LAN for Local Entity

Select SonicWALL\_LAN for Remote Entity

Select Raptor for Local Gateway

Select SonicWALL for Remote Gateway

Select IPSec Policy for VPN Policy

Click OK

Click SAVE on the Raptor console.

raptortest\Secure Tunnel\SonicWALL-Raptor Properties

Description Summary

Please complete the name and description of this Secure Tunnel and define each end of the tunnel along with the VPN Policy you wish to enforce on this tunnel.

Name: SonicWALL-Raptor

Description:

Local Entity: Raptor\_LAN

Local Gateway: Raptor

Remote Entity: SonicWALL\_LAN

Remote Gateway: SonicWALL

VPN Policy: IPSec Policy

IKE Policy: global\_ike\_policy

OK Cancel Help

## SonicWALL VPN with Raptor PowerVPN 6.5

### **Trouble Shooting Tips:**

Stop and Start the Raptor firewall if you can't get the tunnel up

Make sure that you have not defined a phase1 ID for the Raptor or SonicWALL security gateways. See page 5 and page 7.

Verify that your global\_ike\_policy settings on Raptor match the Phase one settings on SonicWALL

Verify that your VPN Policy settings on Raptor match the Phase two settings on SonicWALL