

# Tech Note

VPN

VPN Interoperability Between TZ 170 and CheckPoint NGX R60

## Introduction

This technote will detail the steps necessary to create a working IKE IPSec VPN tunnel between a SonicWALL TZ 170 SP SonicOS 3.1.0.11 Enhanced and a CheckPoint NGX R60 (418) build.

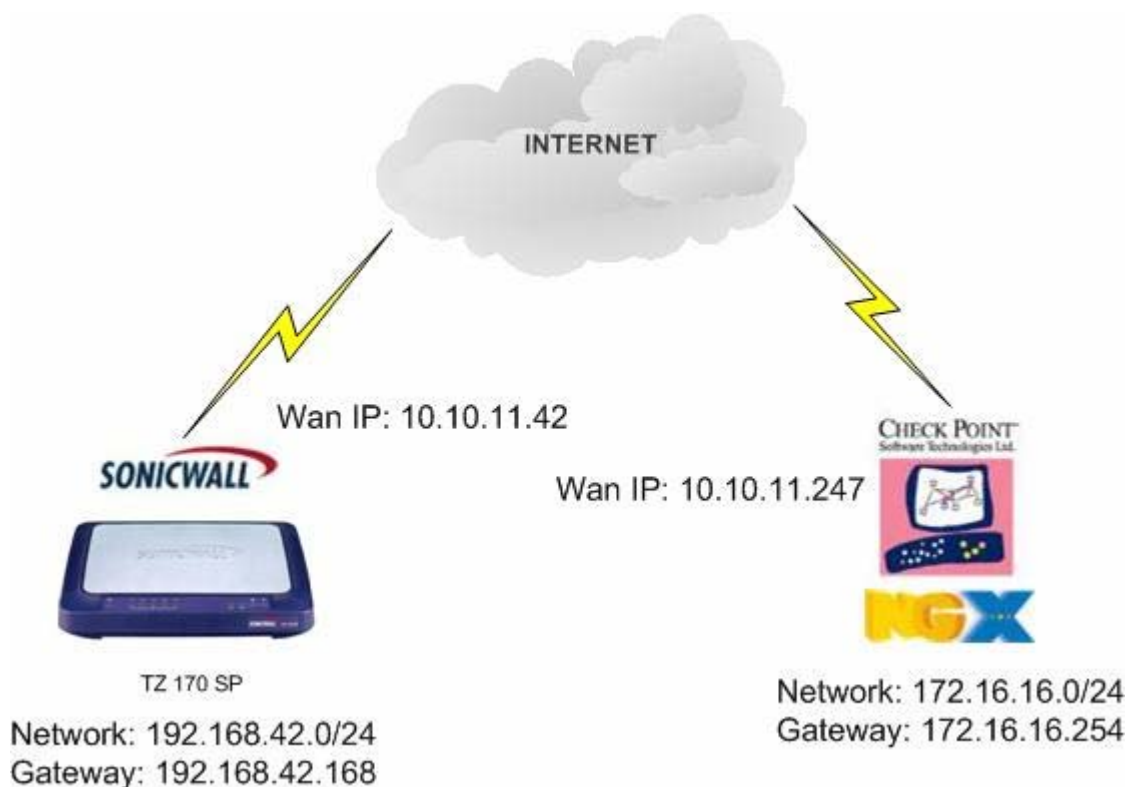
## Recommended Versions

- Any SonicWALL device running SonicOS Enhanced 3.1.X.X
- CheckPoint NGX R60

## Notes

This technote is based on the use of the SonicWALL SonicOS Enhanced, but the scenario below is supposed to work as well if running the SonicWALL SonicOS Standard.

## Sample Diagram



# Tech Note

## TaskList

### On the SonicWALL:

Create a new network object for the CheckPoint LAN.  
Create a new VPN Policy for the CheckPoint NGX R60.  
Configure the VPN Policy (specify the destination network, IKE phase 1 and 2 etc.)

### On the CheckPoint:

Create a new network object for the SonicWALL LAN  
Create a new Interoperable device object  
Edit the CheckPoint gateway object  
Create and edit a new VPN Meshed Community

### Testing:

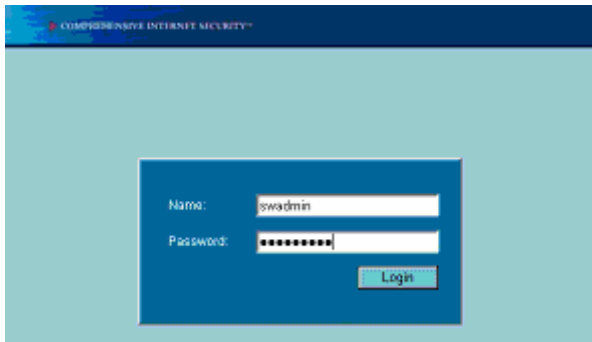
Verify that the traffic is going through the tunnel  
Verify that applications function properly through the tunnel  
Verify that the tunnel can be re-established if one of the side gets disconnected

### BEFORE YOU BEGIN

Verify that the SonicWALL security appliance is configured for internet access. If not, do this before completing any further steps. The CheckPoint is also assumed to be properly configured in order to have an available internet access.

### SonicWALL Setup

Login to the SonicWALL's Management GUI using a compatible web-browser.



# Tech Note

Create an Address Object for the CheckPoint NGX R60 Lan network.

From the SonicWALL Management GUI select **Network > Address Object** and then click **Add**.

Name -> CheckPoint-NGX-Lan

Zone Assignment -> VPN

Type -> Network

Network -> 172.16.16.0

Netmask -> 255.255.255.0

The dialog box shows the following configuration:

- Name: CheckPoint-NGX-Lan
- Zone Assignment: VPN
- Type: Network
- Network: 172.16.16.0
- Netmask: 255.255.255.0
- Status: Ready
- Buttons: OK, Cancel

From the navigation bar of the SonicWALL Management GUI select **VPN > Settings** and then click **Add a new VPN Policy**.

The screenshot shows the SonicWALL Management GUI with the following sections:

- VPN > Settings** (Header)
- VPN Global Settings**
  - Enable VPN
  - Unique Firewall Identifier: snwl-tz170sp
- VPN Policies** (Items 1 to 2 of 2)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Config
1	WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	[Edit] [Delete]
2	WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	[Edit] [Delete]

Buttons: Add..., Delete, Add a new entry
- Site To Site Policies:** 0 Policies Defined, 0 Policies Enabled, 10 Maximum Policies Allowed
- GroupVPN Policies:** 2 Policies Defined, 1 Policies Enabled, 6 Maximum Policies Allowed
- Currently Active VPN Tunnels** (Items 0 to 0 of 0)

# Tech Note

The VPN Policy will then appear.

On the **General** tab page; **Security Policy** select the following;

IPSec Keying Mode -> IKE using Preshared Secret

Name -> cpmodule (as per CheckPoint gateway)

IPSec Primary Gateway Name or Address -> 10.10.11.247 (CheckPoint WAN IP)

IPSec Secondary Gateway Name or Address -> none

Shared Secret -> 1234abcd

Local IKE ID (optional) -> none

Peer IKE ID (optional) -> none

The screenshot shows the 'Security Policy' configuration window with the 'General' tab selected. The configuration is as follows:

Field	Value
IPSec Keying Mode:	IKE using Preshared Secret
Name:	cpmodule
IPSec Primary Gateway Name or Address:	10.10.11.247
IPSec Secondary Gateway Name or Address:	0.0.0.0
Shared Secret:	1234abcd
Local IKE ID (optional):	IP Address
Peer IKE ID (optional):	IP Address

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

# Tech Note

Select the **Network** tab.

Local Networks;

Choose local network from the list -> LAN Primary Subnet (pre-defined object for the SNWL LAN network)

Destination Networks;

Choose destination network from the list -> CheckPoint-NGX-Lan (object previously created for the CheckPoint NGX R60 LAN network)

The screenshot shows a configuration window with four tabs: General, Network, Proposals, and Advanced. The Network tab is selected. The window is divided into two sections: Local Networks and Destination Networks. In the Local Networks section, the 'Choose local network from list' radio button is selected, and the dropdown menu shows 'LAN Primary Subnet'. The other two radio buttons, 'Local network obtains IP addresses using DHCP through this VPN Tunnel' and 'Any address', are unselected. In the Destination Networks section, the 'Choose destination network from list' radio button is selected, and the dropdown menu shows 'CheckPoint-NGX-Lan'. The other two radio buttons, 'Use this VPN Tunnel as default route for all Internet traffic' and 'Destination network obtains IP addresses using DHCP through this VPN Tunnel', are unselected. At the bottom of the window, there is a status bar that says 'Ready' and three buttons: OK, Cancel, and Help.

# Tech Note

Select the **Proposals** tab.

IKE (Phase1) Proposal;  
Exchange -> Main Mode  
DH Group -> Group 2  
Encryption -> DES  
Authentication -> MD5  
Life Time (seconds) -> 3600  
IKE (Phase2) Proposal;  
Protocol -> ESP  
Encryption -> DES  
Authentication -> MD5  
Enable Perfect Forward Secret -> none  
DH Group -> Group 2 (grayed out)  
Life Time (seconds) -> 3600

The screenshot displays the SonicWall configuration interface for the Proposals tab. It is divided into two sections: IKE (Phase 1) Proposal and Ipsec (Phase 2) Proposal. The IKE (Phase 1) Proposal section includes fields for Exchange (Main Mode), DH Group (Group 2), Encryption (DES), Authentication (MD5), and Life Time (seconds) (3600). The Ipsec (Phase 2) Proposal section includes fields for Protocol (ESP), Encryption (DES), Authentication (MD5), a checkbox for Enable Perfect Forward Security (unchecked), DH Group (Group 2), and Life Time (seconds) (3600). The status bar at the bottom shows 'Ready' and buttons for OK, Cancel, and Help.

On the **Advanced** tab, leave all the settings by default.

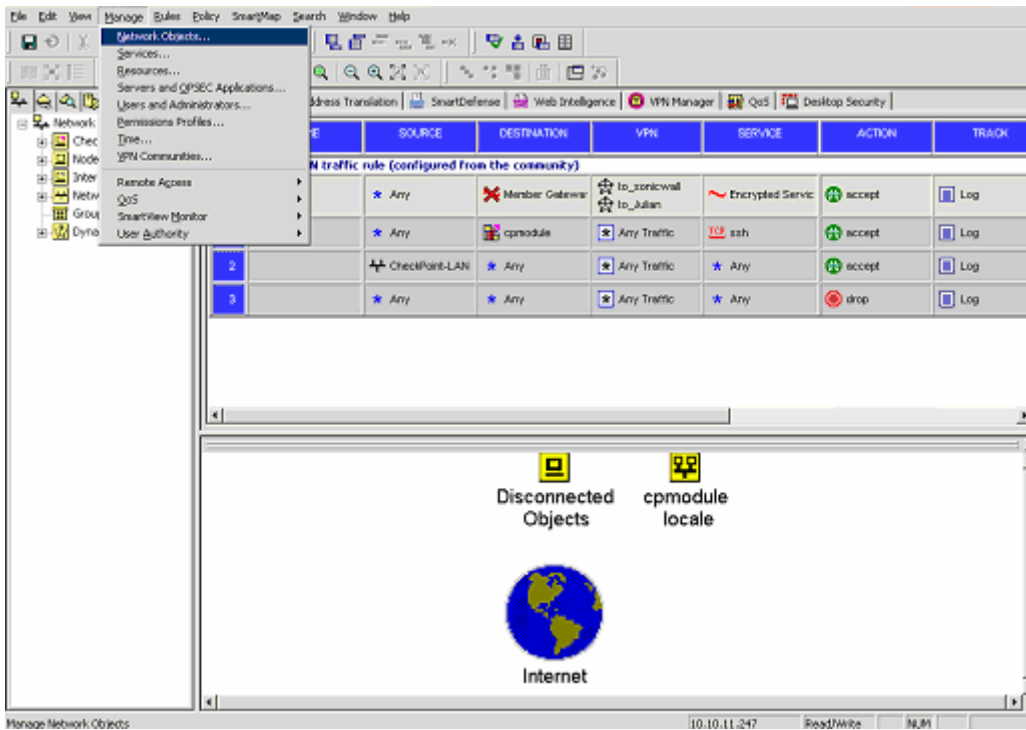
# Tech Note

## CheckPoint Setup

Login to the CheckPoint SmartDashboard.



Create a Network Object for the SonicWALL LAN network.  
From the CheckPoint SmartDashboard select **Manage > Network Objects**.



## Tech Note

General NAT

Name: SNWL-TZ170SP

Network Address: 192.168.42.0

Net Mask: 255.255.255.0

Comment:

Color: [Black]

Broadcast address:  
 Included  Not included

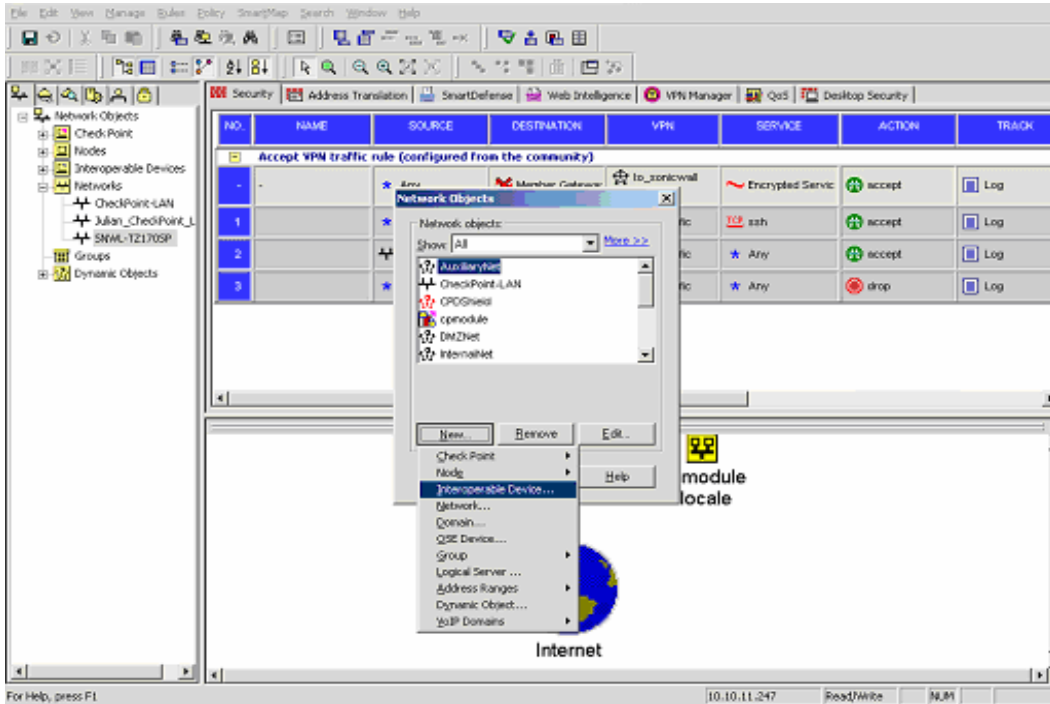
OK Cancel Help

Name -> SNWL-TZ170SP  
Network Address -> 192.168.42.0  
Net Mask -> 255.255.255.0  
Comment -> none  
Broadcast address -> Included

# Tech Note

Create an `Interoperability Device` object.

Select from the CheckPoint SmartDashboard **Manage > Networks Objects** and then click the **New** button; then select **Interoperable Device**.



# Tech Note

The **Interoperability Device** window will then appear.

General Properties;

Name -> snwl-tz170sp

IP Address -> 10.10.11.42

Comment -> none

Topology;

Make sure that under VPN Domain the option `Manual Defined` it is selected and the remote SNWL LAN network is specified. (SNWL-TZ170SP)

Interoperable Device - General Properties

Name:

IP Address:    Dynamic Address

Comment:

Color:

OK Cancel Help

Topology

Name	IP Address	Network Mask	IP Addresses behind Gateway

VPN Domain

All IP Addresses behind Gateway based on Topology information.

Manually defined

OK Cancel Help

# Tech Note

Edit the CheckPoint NGX R60 gateway object. (cpmodule)

General Properties;

Verify that under the section `CheckPoint products`, VPN is selected.

Topology;

Verify that under VPN Domain the option `Manual Defined` it is selected and the local Checkpoint LAN network is specified. (CheckPoint-LAN)

**Check Point Gateway - General Properties**

Name:

IP Address:

Comment:

Color:

Secure Internal Communication  
Communication... DN:

Version:

OS:

Type:

Check Point Products

- Firewall
- VPN
- QoS
- SecureClient Policy Server
- Primary SmartCenter Server
- SVN Foundation

Additional Products:

**Topology**

Name	IP Address	Network Mask	IP Addresses behind Gateway
eth0	172.16.16.254	255.255.255.0	This Network
eth1	10.10.11.247	255.255.255.0	External

VPN Domain

All IP Addresses behind Gateway based on Topology information.

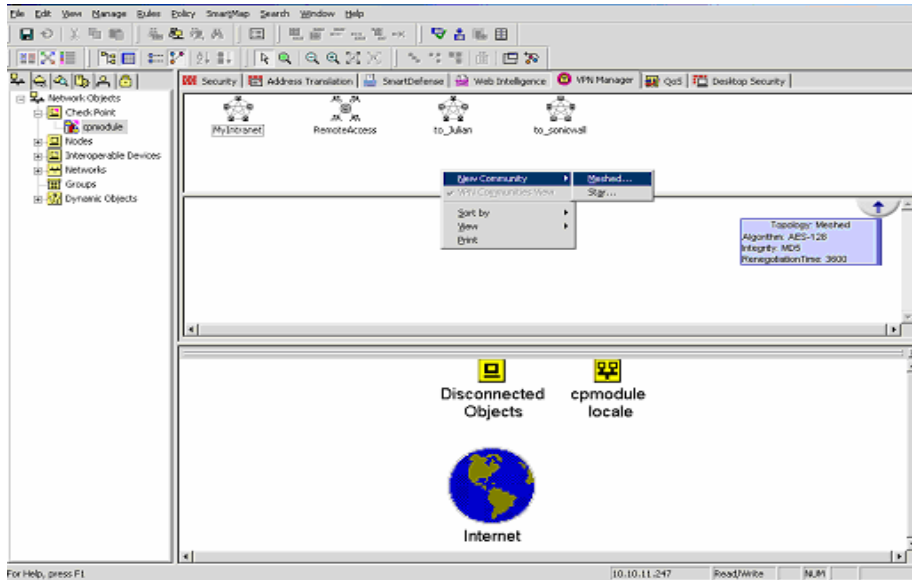
Manually defined

# Tech Note

Define the VPN.

Select from the CheckPoint SmartDashBoard the `VPN Manager` tab and then right click with the mouse in the field below.

Select **New Community > Meshed**



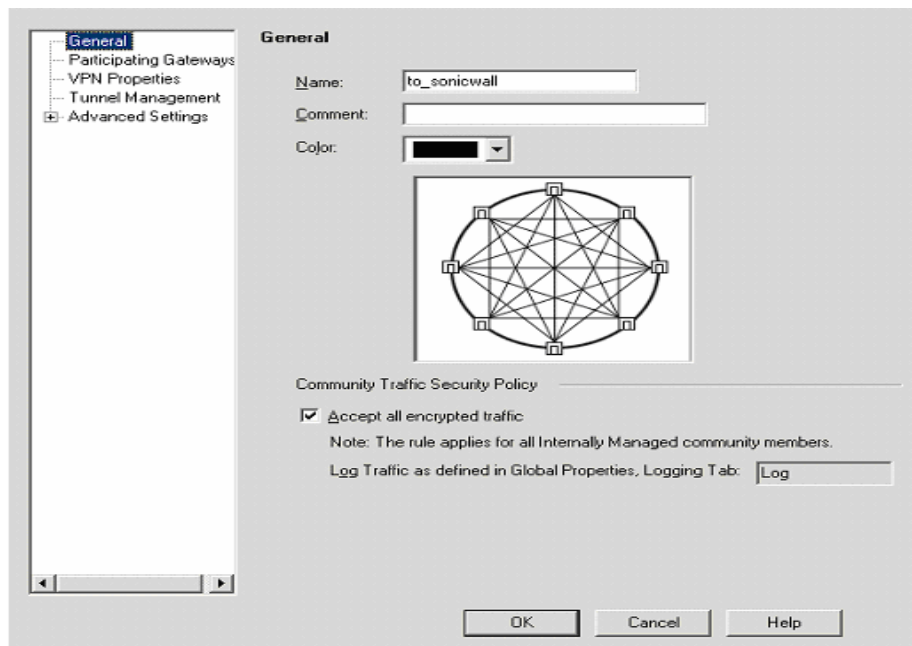
In the `Meshed Community Properties` page, proceed as follow;

Name -> to\_sonicwall

Comment -> none

Community Traffic Security Policy;

Enable -> Accept all encrypted traffic

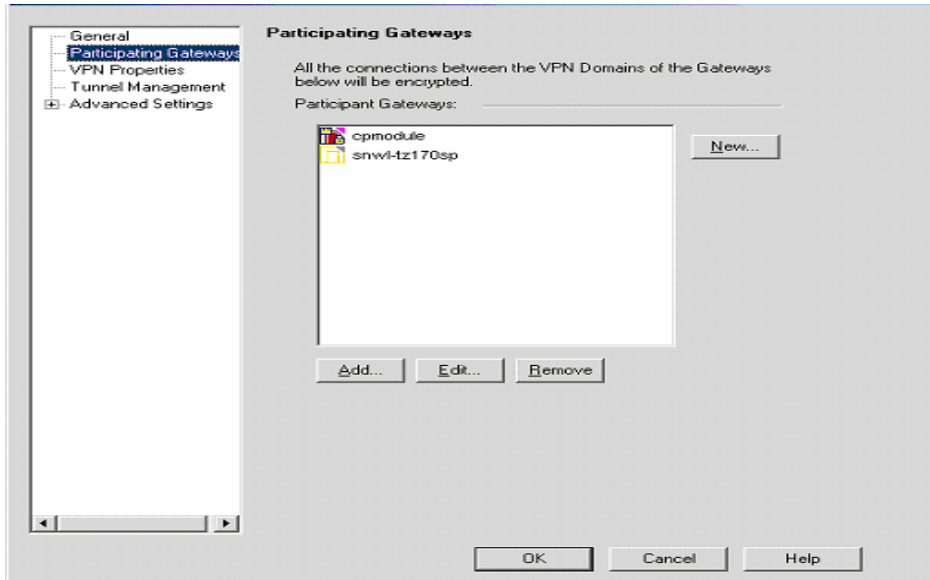


# Tech Note

On the `Participating Gateways`, click on `Add`.

In this case you will see the following gateways;

- cpmodule -> CheckPoint NGX R60 gateway
- snwl-tz170sp -> SNWL TZ 170 gateway interp. object (previously created)



Select VPN Properties

IKE (Phase1) properties;

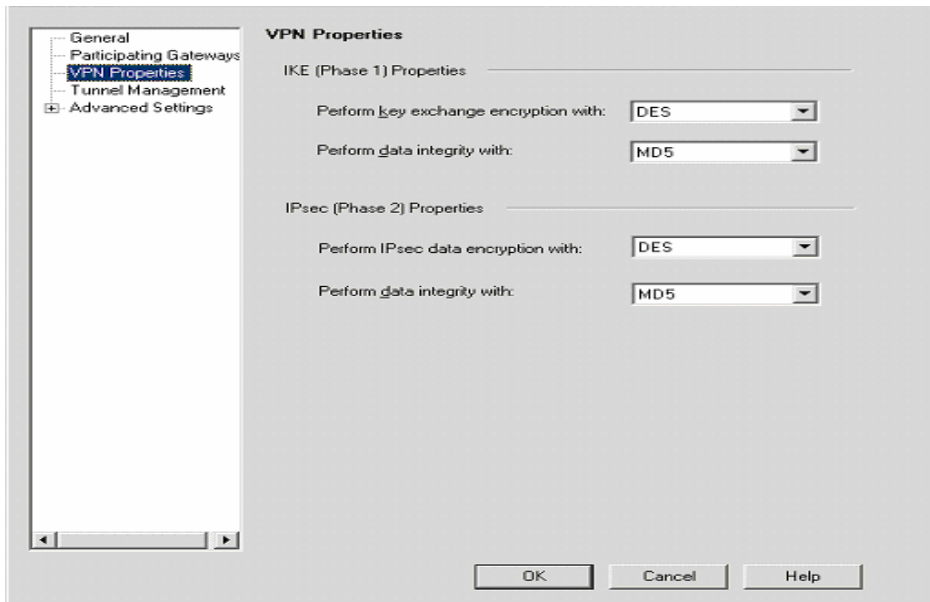
Perform key exchange encryption with -> DES

Perform data integrity with -> MD5

IPSec (Phase2) Properties

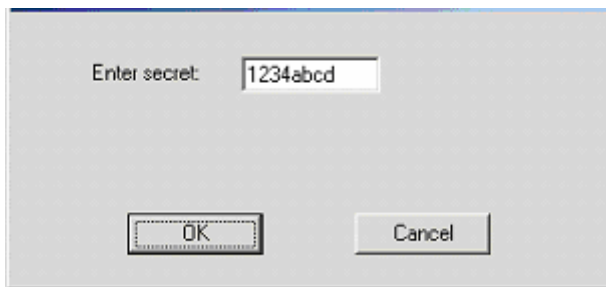
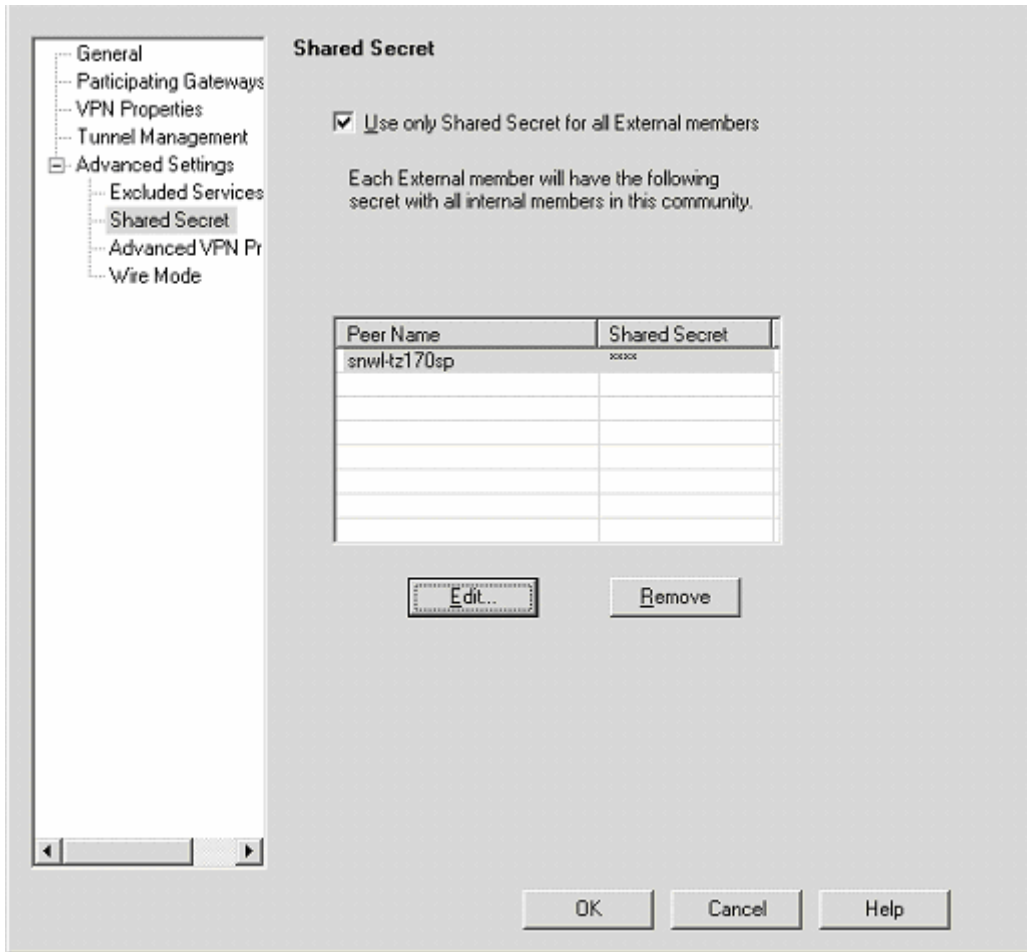
Perform key exchange encryption with -> DES

Perform data integrity with -> MD5



# Tech Note

In the `Advanced Settings` select `Shared Secret`  
Click on the `Edit` button and enter -> 1234abcd (used as well on the SNWL).



## Tech Note

Select then always from `Advanced Settings` the tab `Advanced VPN Properties`.

Advanced VPN Properties

IKE (Phase1)

Use Diffie-Hellman group -> Group 2 (1024 bit)

Renegotiate IKE security association every -> 60 minutes

Use aggressive mode -> none

IPSec (Phase2)

Use Perfect Forward Secrecy -> none

Use Diffie-Hellman group -> Group 2 (1024 bit) – grayed out

Renegotiate IKE security association every -> 3600 seconds

Support IP compression -> none

NAT

Select -> Disable NAT inside the VPN community

The screenshot shows the 'Advanced VPN Properties' configuration window. On the left is a tree view with 'Advanced VPN Properties' selected. The main area is divided into three sections: IKE (Phase 1), IPsec (Phase 2), and NAT. In the IKE section, 'Use Diffie-Hellman group' is set to 'Group 2 (1024 bit)', 'Renegotiate IKE security associations every' is set to 60 minutes, and 'Use aggressive mode' is unchecked. In the IPsec section, 'Use Perfect Forward Secrecy' is unchecked, 'Use Diffie-Hellman group' is set to 'Group 2 (1024 bit)', 'Renegotiate IPsec security associations every' is set to 3600 seconds, and 'Support IP compression' is unchecked. A 'Reset All VPN Properties' button is located below the IPsec section. In the NAT section, 'Disable NAT inside the VPN community' is checked. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

**Advanced VPN Properties**

IKE (Phase 1)

Use Diffie-Hellman group: Group 2 (1024 bit)

Renegotiate IKE security associations every 60 minutes

Use aggressive mode

IPsec (Phase 2)

Use Perfect Forward Secrecy

Use Diffie-Hellman group: Group 2 (1024 bit)

Renegotiate IPsec security associations every 3600 seconds

Support IP compression

Reset All VPN Properties

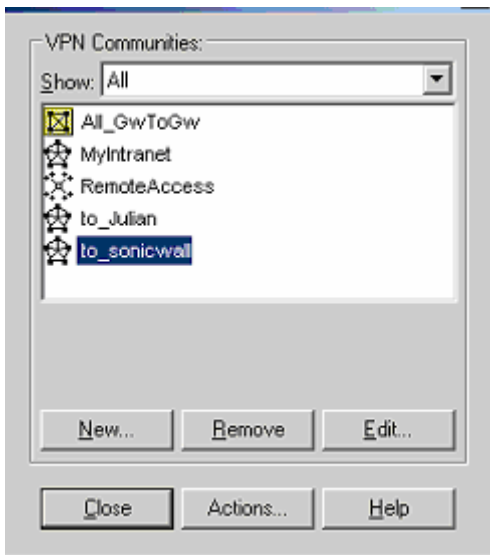
NAT

Disable NAT inside the VPN community

OK Cancel Help

## Tech Note

Finally you should be able to see in the `VPN Communities` the object related to the SNWL VPN tunnel. In this case it was named `to\_sonicwall`.



From the management consoles of both the SNWL and CheckPoint verify the active tunnel, verify that there is traffic going through the tunnel.

**Created: October 13, 2005**  
**Last Updated: December 8, 2005**  
**Matteo Marzoli**