▷ SONICWALL TECH NOTE:

Configuring VPN's between SonicOS Standard and SonicOS Enhanced

Introduction

This technote will detail all the steps necessary to create a working IKE IPSec VPN tunnel between a SonicWALL security appliance running SonicOS Standard and a SonicWALL security appliance running SonicOS Enhanced. SonicWALL engineering has tested and validated the settings described in this technote. Please note that all settings and screenshots contained within this technote are taken from a SonicWALL TZ 170 running SonicOS Standard 2.2.0.1 acting as the remote site, and a SonicWALL PRO 2040 running SonicOS Enhanced 2.5.0.6 acting as the central site.

Recommended Versions

- SonicOS Standard 2.2.0.1 or newer strongly recommended
- SonicOS Enhanced 2.5.0.6 or newer strongly recommended

Customers with current service/software support contracts can obtain updated versions of SonicWALL software images from the MySonicWALL customer portal at https://www.mysonicwall.com. Updated software images are also freely available to customers who have registered the SonicWALL security appliance on MySonicWALL for the first 90 days for TZ 170-series and PRO-series, and the first 30 days for TZ 150-series.

Caveats

- Please take special care to correctly set the VPN proposal settings on the SonicWALL security appliances. If the settings do not match on the SonicWALLs, the security appliances will not be able to negotiate a tunnel from either side.
- If the remote SonicWALL appliance is obtaining its WAN IP address dynamically (DHCP, PPPoE, L2TP, PPTP), the central site will not be able to initiate a tunnel to the remote SonicWALL, as it does not know the remote SonicWALL's WAN IP address. For this reason, we recommend setting keepalives on the remote SonicWALL, and will be documenting this in this technote. Only set keepalives on the site that is dynamically addressed.
- For the examples in this technote, we'll be using the 'Unique Firewall Identifier' (UFI, or 'SonicWALL Identifier') as the IKE Identity method, and Aggressive Mode to negotiate the VPN tunnels. This method can be used regardless of the remote side's WAN IP addressing method.
- If running newer 3.x-series software images, you may wish to consider using the new DDNS feature on the remote SonicWALL security appliance, as this will allow the remote site to be reached by a fully-qualified domain name (FQDN) by the central site, even if its WAN IP address changes frequently. Details on how to configure this feature, including VPN setup examples, can be found here: http://www.sonicwall.com/support/SonicOS_FW_documentation.html
- Some Microsoft networking environments rely heavily on broadcasts to advertise and locate network resources (servers, print devices, etc). By default, SonicWALL devices are configured to not pass these Microsoft NetBIOS broadcasts across VPN tunnels. In this technote, we will detail how to configure SonicOS to pass these broadcasts across the VPN tunnel bidirectionally in the 'Optional Steps' section of this technote. Please note this may increase traffic in some environments.

Sample Diagram

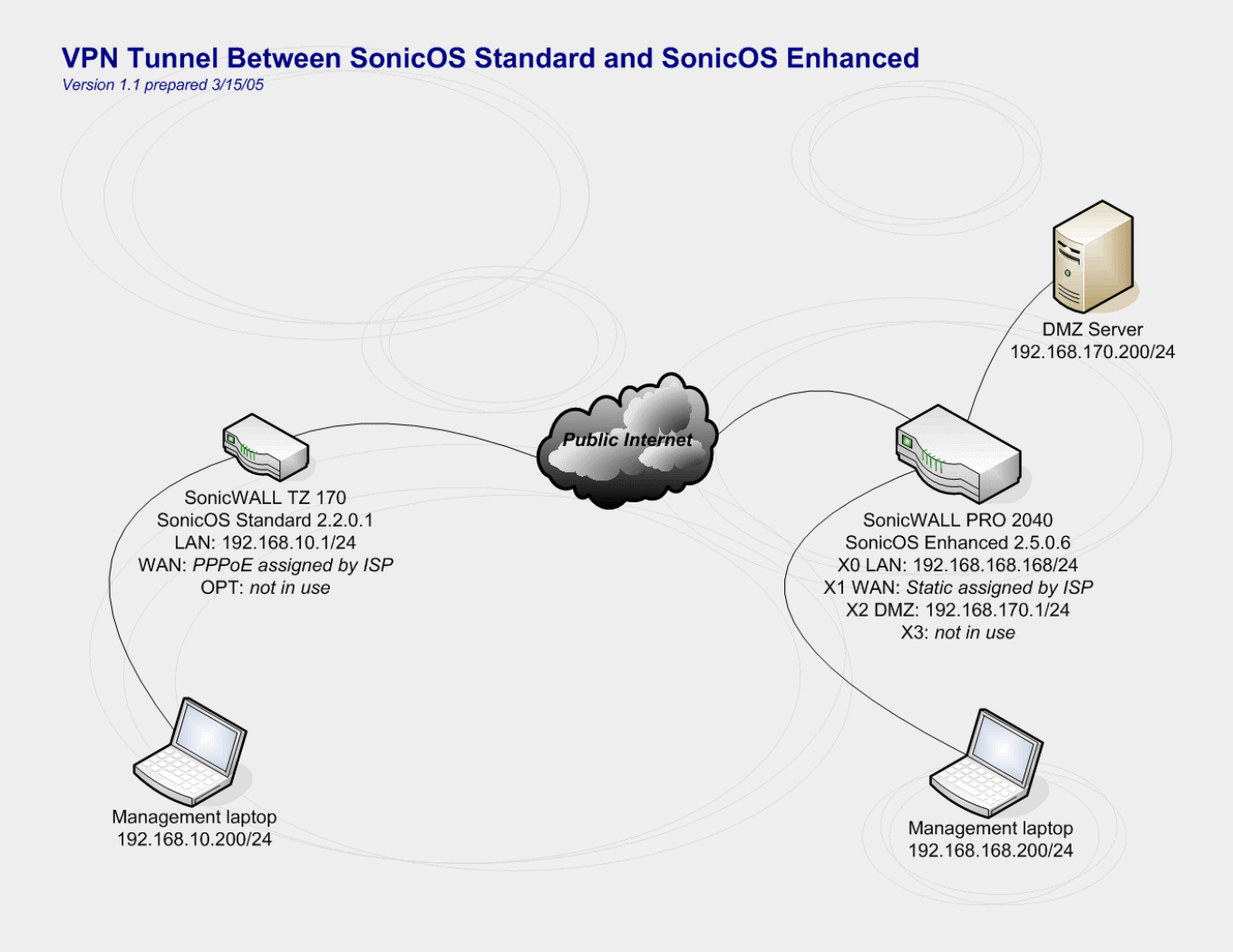

Figure 1 – Example network

Tasklist

- Configure remote site VPN settings
- Configure central site VPN settings
- Configure both sites to pass Microsoft NetBIOS broadcast traffic
- Test VPN tunnel setup from remote site
- Test keepalive function on remote site

Before You Begin

- As noted in the 'Recommended Versions' section, SonicWALL strongly recommends running SonicOS Standard 2.2.0.1 or newer and SonicOS Enhanced 2.5.0.6 or newer, as many VPN-related issues were resolved as of these releases.
- For testing purposes, you may wish to place a management station or laptop behind both sites. This will greatly aid successful testing/troubleshooting of the VPN configuration between the remote and central sites.
- **IMPORTANT NOTE:** Log into both SonicWALL security appliances and copy down the 'Unique SonicWALL Identifier' (UFI) for each device. This can be found on the 'VPN > Settings' page – **you will need to know these values before configuring the VPN settings on each security appliance.**

Setup Steps

REMOTE SITE

1. From the management station/laptop behind the remote site SonicWALL security appliance, log into the SonicWALL's Management GUI and go to the 'VPN > Settings' page. Click on the 'Add…' button under the 'VPN Policies' section. When the pop-up appears, go to the 'General' tab. On this tab, choose 'IKE using Preshared Secret' from the drop-down next to 'IPSec Keying Mode:', enter the central site's UFI into the field next to 'Name:', enter the central site's WAN IP address or FQDN in the field next to 'IPSec Primary Gateway Name or Address:', and enter a complex shared secret in the field next to 'Shared Secret:' (write this down, as you will need to enter this same shared secret on the central site). For an example, see Figure 2 below.

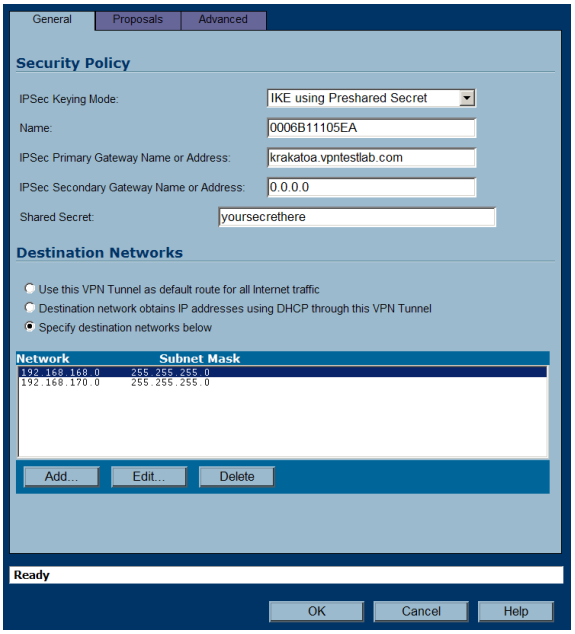

Figure 2 – Remote site VPN 'General' tab

2. Then, click on the 'Add…' button on the 'General' tab to enter the remote site's networks (the networks behind the other SonicWALL). For each network to be reached via the VPN tunnel, create an entry. In our example, there are two networks behind the remote site – see Figure 3 below.

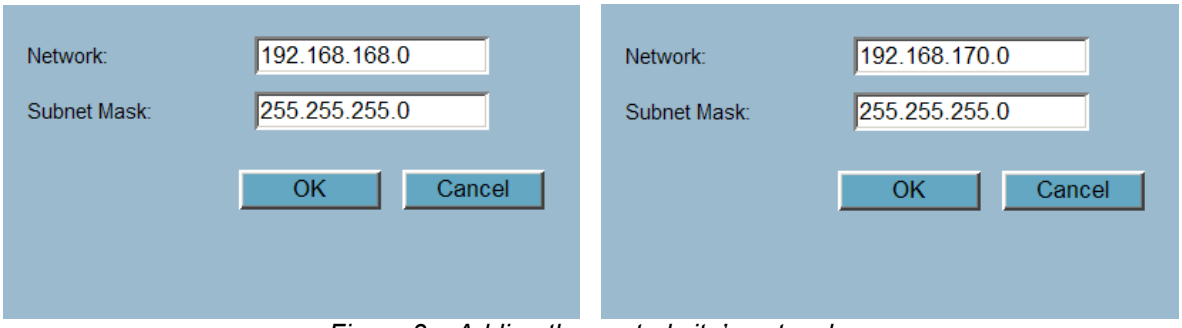

Figure 3 – Adding the central site's networks

3. Switch to the 'Proposals' tab. On this tab, select 'Aggressive Mode' from the drop-down next to 'Exchange:". Leave all other settings as-is. For an example, see Figure 4 below.

4. Switch to the 'Advanced' tab. On this tab, check the boxes next to 'Enable Keep Alive' and 'Try to bring up all possible Tunnels'. For an example, see Figure 4 below. When done, click on the 'OK' button to save and activate the changes.

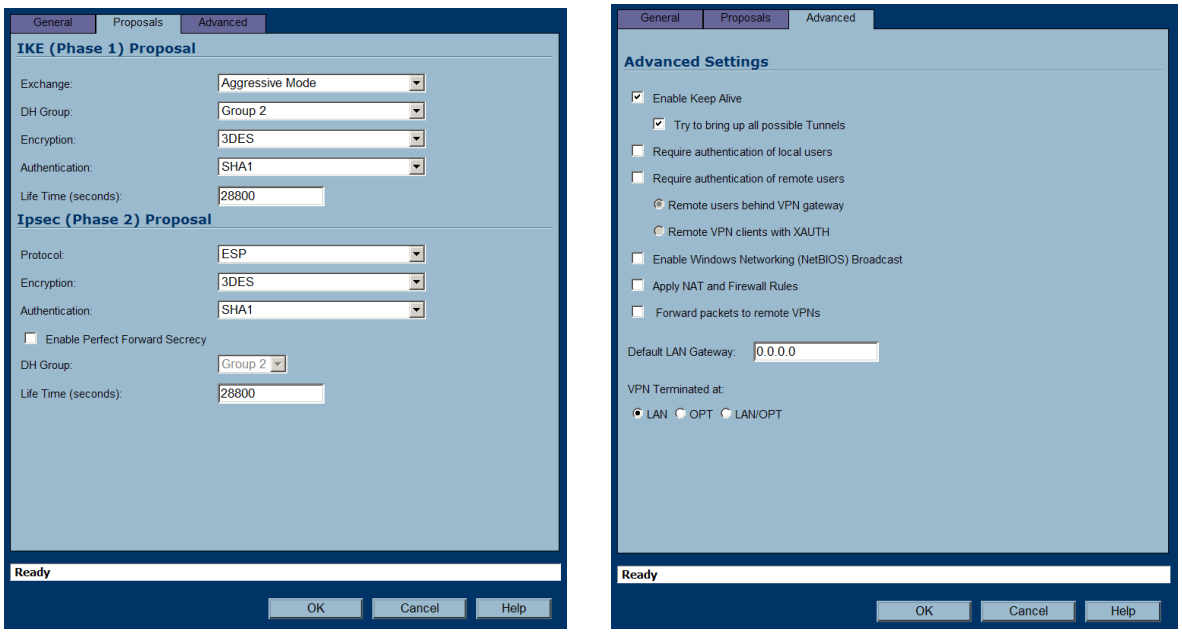

Figure 4 – Remote site VPN 'Properties' and 'Advanced' tabs

CENTRAL SITE

1. From the management station/laptop behind the central site SonicWALL security appliance, log into the SonicWALL's Management GUI and go to the 'Network > Address Objects' page. Click on the 'Add…' button at the bottom of this page under the 'Address Objects' section (not the 'Address Groups' section). On the pop-up that appears, enter a description of the remote site's LAN subnet, choose 'VPN' from the drop-down next to 'Zone Assignment', and enter in the remote site's LAN subnet and subnet mask. When done, click on the 'OK" button to save and activate the change. For an example, see Figure 5 below.

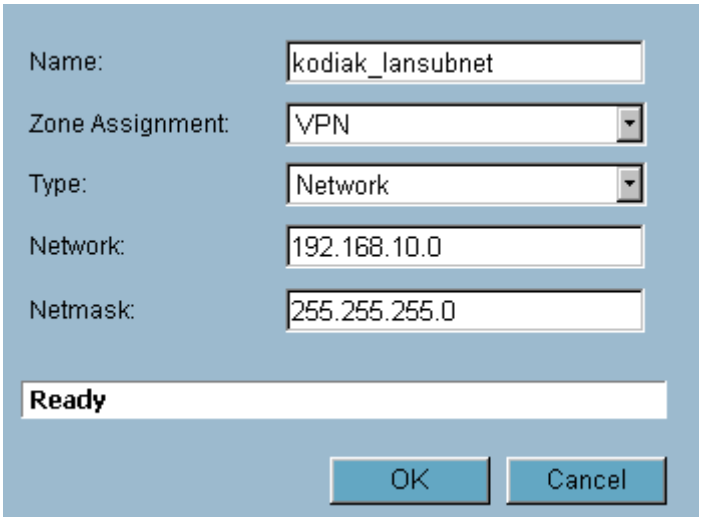

Figure 5 – Adding the remote site's address object

2. Go to the 'VPN > Settings' page, and click on the 'Add…' button under the 'VPN Policies' section. When the pop-up appears, go to the 'General' tab. On this tab, choose 'IKE using Preshared Secret' from the drop-down next to 'IPSec Keying Mode:', enter the remote site's UFI into the field next to 'Name:', enter '0.0.0.0' in the field next to 'IPSec Primary Gateway Name or Address:', enter a complex shared secret in the field next to 'Shared Secret:' (the same shared secret as entered on the remote site setup), choose 'SonicWALL Identifier' from the drop-down next to 'Local IKE ID' and enter the central site's UFI in the field next to it, and choose 'SonicWALL Identifier' from the drop-down next to 'Peer IKE ID' and enter the remote site's UFI in the field next to it. For an example, see Figure 6 below.

3. Switch to the 'Network' tab. In the 'Local Networks' section, select the radio button next to 'Choose local network from list:' and choose 'Firewalled Subnets' from the drop-down next to this. In the 'Destination Networks' section, select the radio button next to 'Choose destination network from list:' and choose the address object you previously created from the drop-down next to this. For an example, see Figure 6 below.

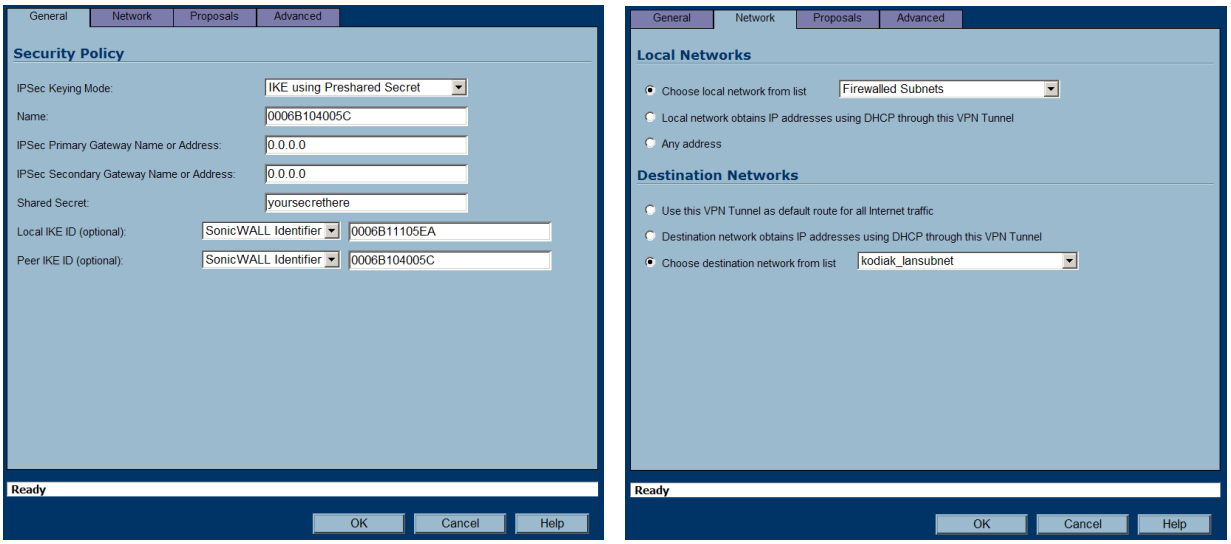

Figure 6 – Central site 'General' and 'Network' VPN tabs

4. Switch to the 'Proposals' tab. Select 'Aggressive Mode' and leave all other settings as-is (verify that these settings are the same on both sides). For an example, see Figure 7 below.

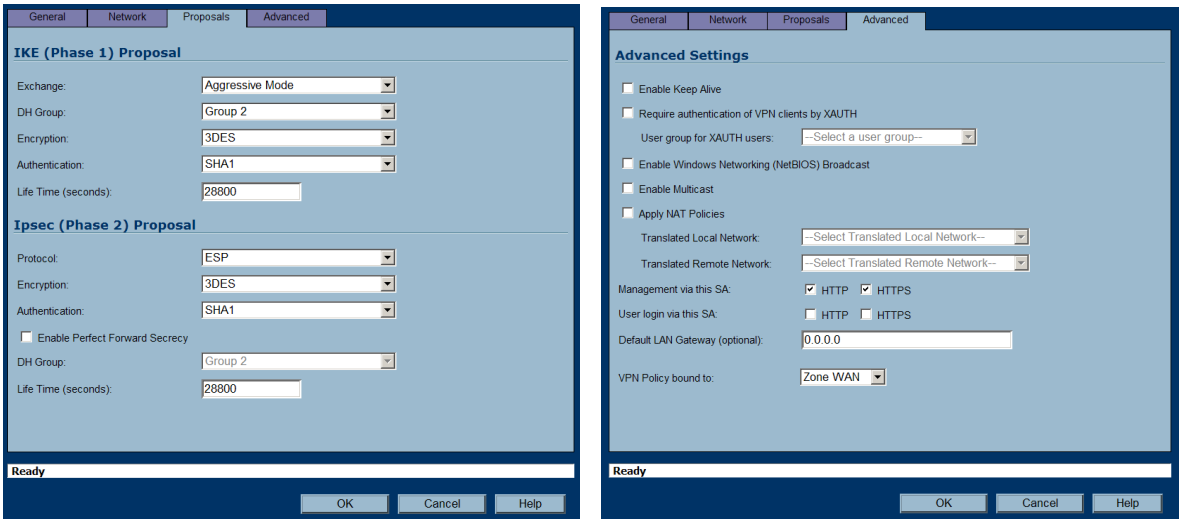

Figure 7 – Central site 'Proposals' and 'Advanced' tabs.

5. Switch to the 'Advanced' tab. Check the boxes next to 'HTTP' and 'HTTPS' in the area next to 'Management via this SA', if you intend to allow Management GUI access to the central site SonicWALL via the VPN tunnel. For an example, see Figure 7 on the previous page. When done, click on the 'OK' button to save and activate the change.

[Optional Steps]

1. On the remote side SonicWALL, go to the 'VPN > Advanced' page and uncheck the box next to 'Disable all VPN Windows Networking (NetBIOS) Broadcasts. This is a global setting, and unless unchecked, no VPN SA will be able to pass NetBIOS broadcasts. When done, click on the 'Apply' button in the upper-right-hand corner to save and activate the change. For an example, see Figure 8 below.

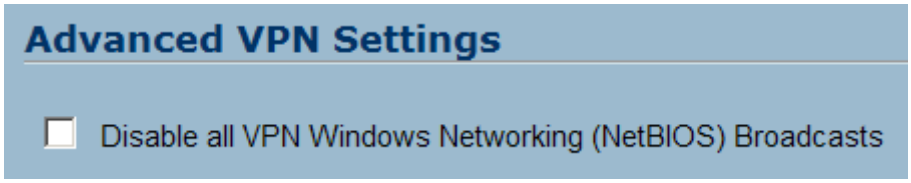

Figure 8 – Enable Microsoft Networking broadcast support

2. Then, go to the 'VPN > Settings' page and click on the 'Configure' icon next to the VPN policy you previously created to connect to the central site. On the pop-up that appears, go to the 'Advanced tab and check the box next to 'Enable Windows Networking (NetBIOS) Broadcast'. This is a per VPN SA setting and applies to this VPN tunnel only. When done, click on the 'OK' button to save and activate the change. For an example, see Figure 9 below.

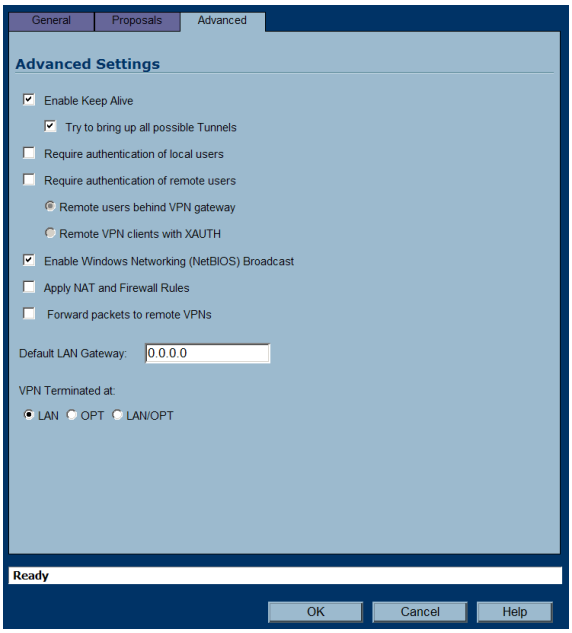

Figure 9 – Remote site 'Advanced' VPN tab

3. On the central site SonicWALL, go to the 'VPN >Settings' page and click on the 'Configure' icon next to the VPN policy you previously created to connect to the remote site. On the pop-up that appears, go to the 'Advanced tab and check the box next to 'Enable Windows Networking (NetBIOS) Broadcast'. When done, click on the 'OK' button to save and activate the change. For an example, see Figure 10 below.

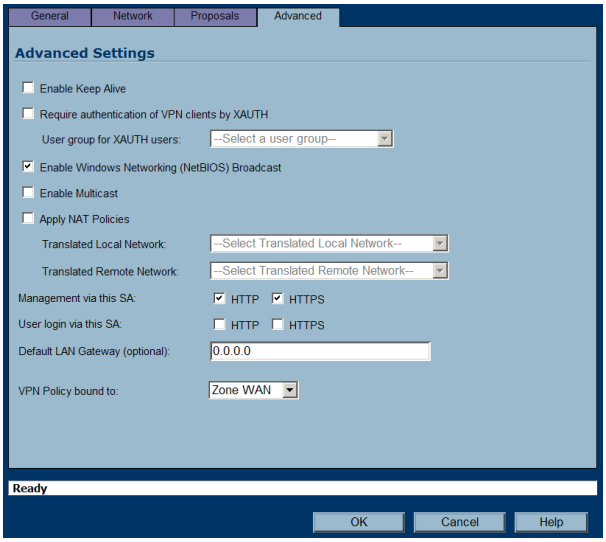

Figure 10 – Central site VPN 'Advanced' tab

4. Then, go to the 'Network > IP Helper' page. Check the box next to 'Enable IP Helper', make sure the box next to 'Enable DHCP Support' is unchecked (unless you are using this feature), and check the box next to 'Enable NetBIOS Support'. You will notice that there will be an autocreated IP Helper Policy listed as a result of the previous step's configuration. When done, click on the 'Apply' button in the upper-right-hand corner to save and activate the change. For an example, see Figure 11below.

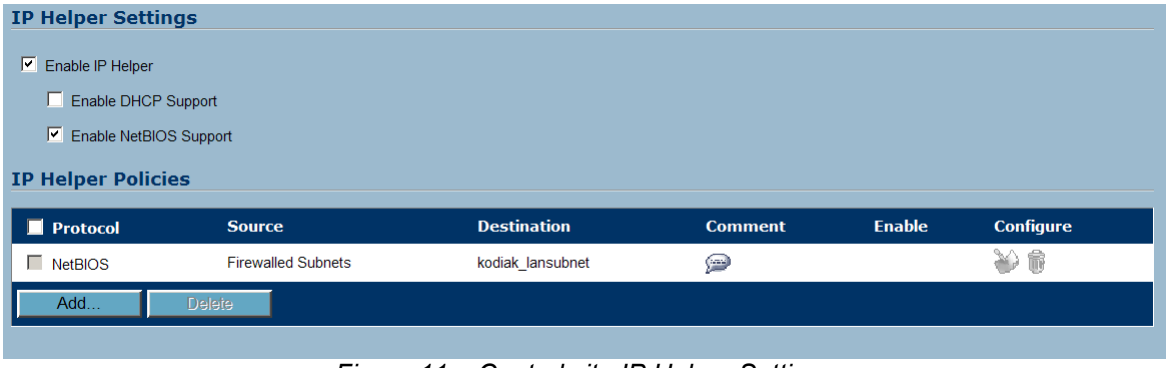

Figure 11 – Central site IP Helper Settings

Testing/Troubleshooting

- From a system behind the remote site SonicWALL, attempt to connect to a network resource behind the central site, or ping the central site SonicWALL's LAN interface IP address. Once you've done this, log into the remote site SonicWALL's management GUI and check the 'VPN > Settings' page. You should see the active VPN tunnel listed (see Figure 12 and Figure 13 below). On the remote site, you should see that the tunnel has negotiated with the Primary IPSec gateway. If the tunnel does not negotiate successfully, check the SonicWALL's log on the 'Log > View' page to see if there are any error messages for VPN negotiation. If the tunnel is not negotiating and there are error messages displayed, go over the settings on both side to make sure that they match and attempt to bring the tunnel up again.

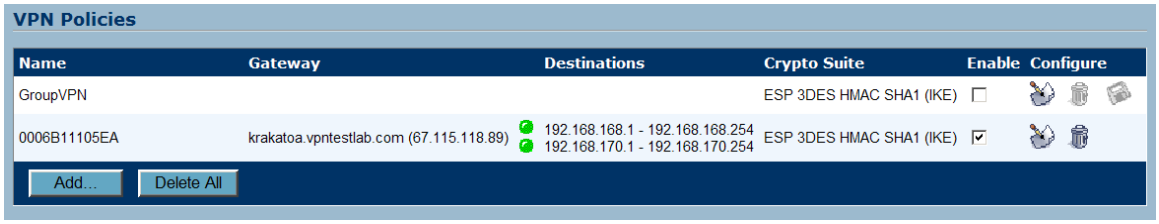

Figure 12 – VPN Policies on remote site

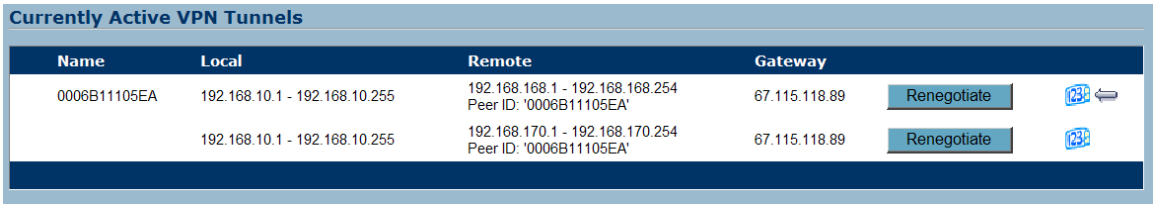

Figure 13 – Active VPN tunnels between remote and central site

- Once you've verified that the VPN settings are correct on both sides, and that initiating traffic from the remote site can force the VPN tunnel to the central site to negotiate, now test the keepalive function that we configured on the remote site. Perform a warm or cold boot of both SonicWALL security appliances, wait a few minutes to allow for reboot and VPN negotiation, then log into the remote site SonicWALL's management GUI and check the 'VPN > Settings' page. You should see the active VPN tunnel listed (see Figure 12 and Figure 13 above). On the remote site, you should see that the tunnel has negotiated with the Primary IPSec gateway. If the tunnel does not negotiate successfully, check the SonicWALL's log on the 'Log > View' page to see if there are any error messages for VPN negotiation. If the tunnel is not negotiating and there are error messages displayed, go over the settings on both side to make sure that they match and attempt to bring the tunnel up again.

Created: 11/01/2003
Updated: 03/24/2005
Version 1.2