Tech Tip
Contivity Secure IP Services Gateway

Branch Office Tunnels with Contivity 221 and 251

Contents

Overview

This document shows how to configure an asymmetric branch office tunnel (ABOT) or branch office tunnel (BOT) from a Contivity Secure IP Services Gateway 221 or 251 (Contivity 2x1) at a remote branch office to another Contivity gateway at a central office.

Generally, the Contivity 2x1 is used at small remote branch offices and SOHO (small office/home office). In these situations, it is very common for the branch office to be assigned an IP address from the ISP via DHCP, rather than being assigned a static IP address. This is one case where the concept of an ABOT comes into play. Typically, when you configure a BOT, you must know the IP address of the remote gateways (the public IP address of both gateways) so they can communicate with each other and bring up a tunnel. However, when one of the gateways gets its public IP address via DCHP, then that address may change from time to time. This does not allow you to configure this address as the remote gateway address in its peer's tunnel configuration. Hence we configure the tunnel as an ABOT, where the gateway with an IP address assigned via DHCP on its public interface acts as an "initiator", and the gateway with the static IP address on its public interface acts as a "responder". Only the "initiator" can initiate the tunnel establishment. The "responder" can only respond to tunnel requests.

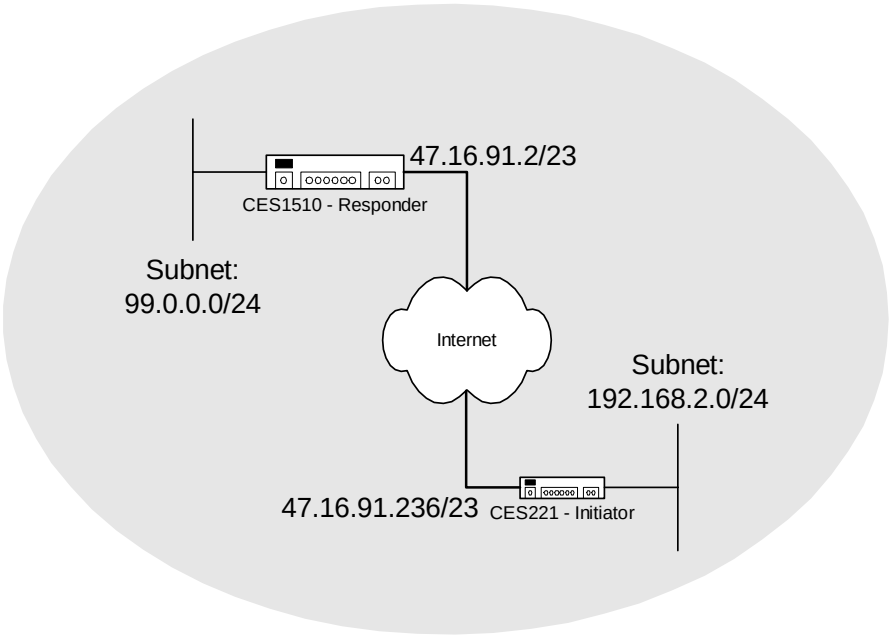
Note: With a BOT, the group that the branch office connection is a member of should have compression disabled. This is because the Contivity 2x1 does not support compression.

When configuring the ABOT, the central office Contivity needs to know the Initiator ID of the remote gateway. For more information on configuration see the following example. Also, as we proceed through the example, if you would like further details on any of the settings that are given here, or if you would like to configure any additional options, please click on the Help link in the upper right-hand corner of the screen while managing Contivity via GUI. It is very informative and offers an explanation for each setting in clear and easy-to-understand terms.

Note: This document provides a sample configuration of a branch office tunnel between a Contivity 2x1 and a Contivity from the 1xxx, 2xxx, 4xxx and 5xxx families, and should be used only as such. The configurations here will not apply to all implementations, nor are they intended to. For further information on alternative options and configurations, and on the details of the options used here, please consult the proper product documentation.

Sample Configuration

1. Setup



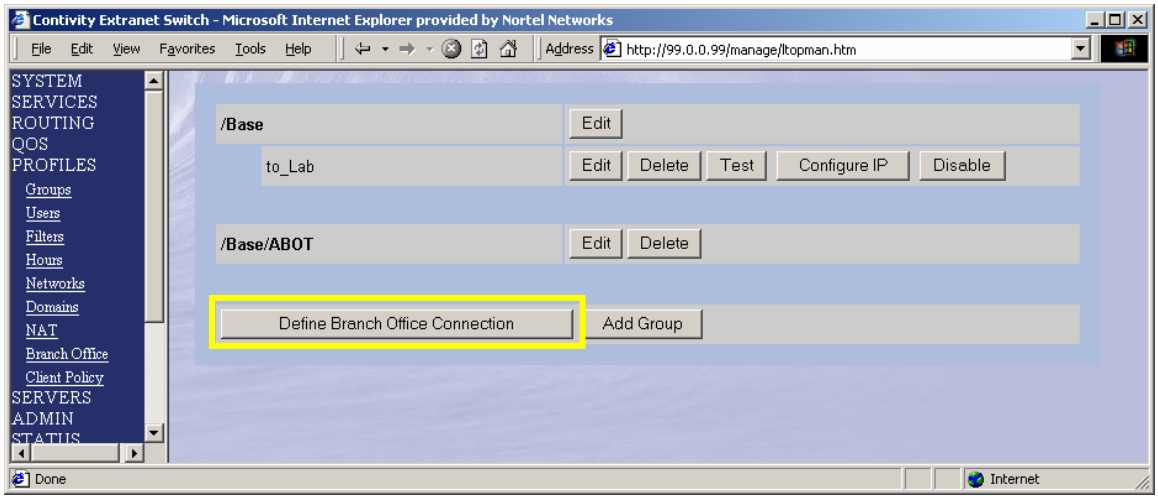
For the purposes of this document, the central office Contivity is any member of the Contivity family other than the Contivity 100, 221, or 251. The remote office Contivity could be either the Contivity 221 or 251.

2. Configuring Central Office Contivity

Let's start by configuring the Contivity at the home office. This is the Contivity with the static IP address on its public interface.

1. You can see in the following figure that we have already gone to **PROFILES → Branch Office** and created a Branch Office Group with a parent group of **/Base**. This is optional, as the ABOT may be configured in any group you desire. We have called this group ABOT.
2. Click on **Define Branch Office Connection** to create your ABOT.

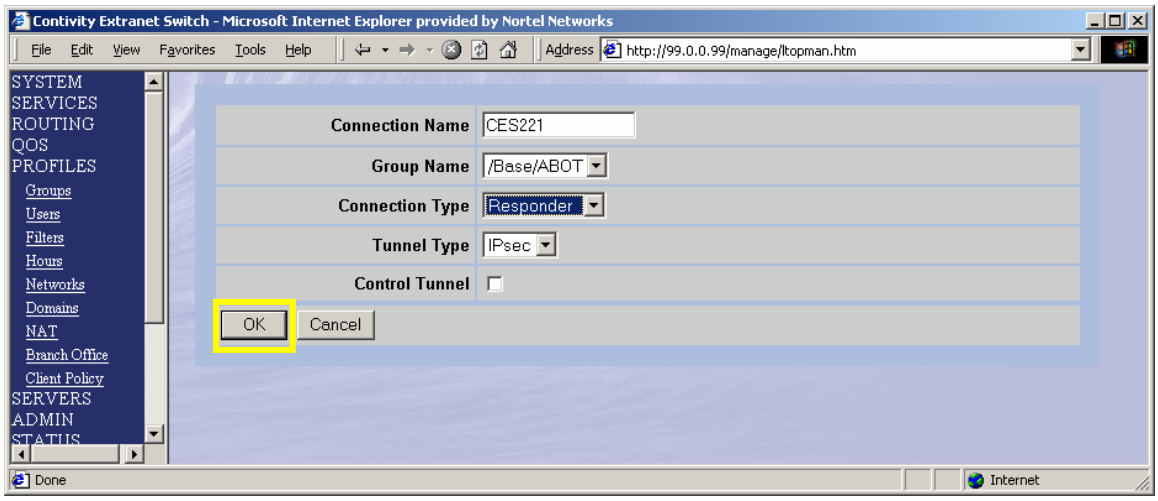
Note: If this was going to be a BOT, we would have had to click **Edit** next to the group name. This would bring us to the group page. We would then click on **Configure** under the **IPSec** settings and disable **Compression**. But since the central office Contivity will be configured as a Responder, it will not try to negotiate compression, so this is not necessary with an ABOT.



The **Branch Office Connection** screen comes up.

3. Enter the **Name** of the connection.
4. Select the **Group** it will be a member of.
5. Select Connection Type: **Responder**.
6. Select the Tunnel Type: **IPSec**.
7. Leave the **Control Tunnel** option de-selected.
8. Click **OK**.

Note: If this was going to be a BOT, we would have had to select **Peer-to-Peer** in the **Connection Type** pull-down menu.

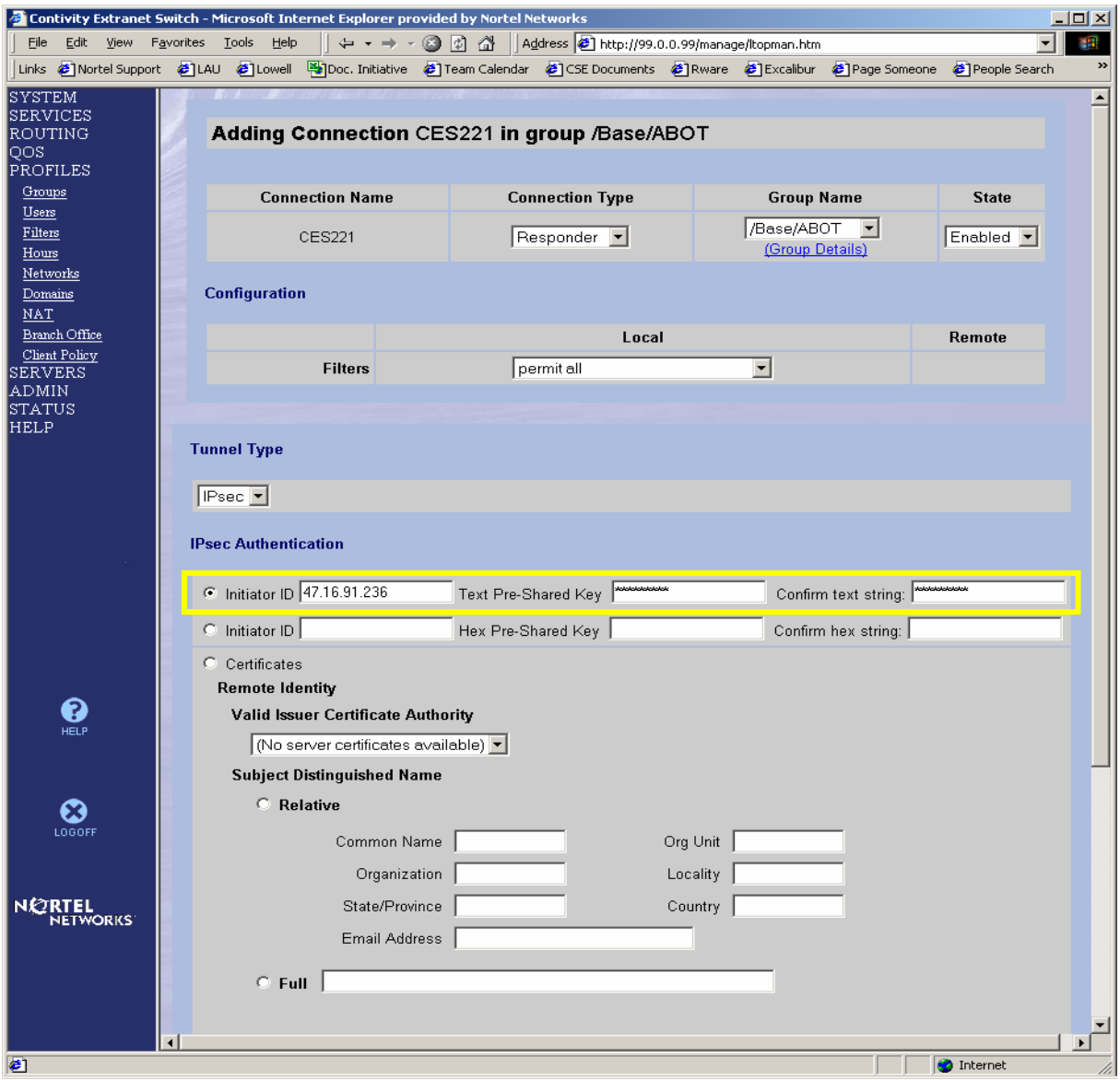


Branch Office Tunnels with Contivity 221 and 251

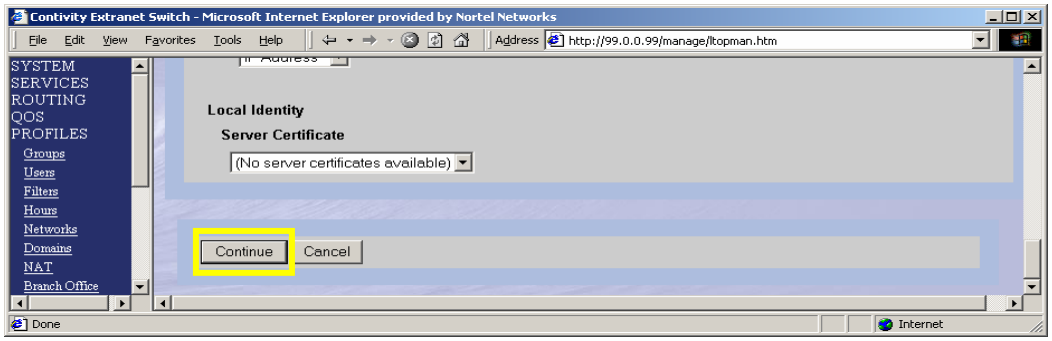
The following screen is where you will configure the rest of the tunnel configuration parameters. The top half of this screen is filled out properly by default. The only information we need to enter here is the **IPSec Authentication** information. For this demonstration, we have chosen to use a **Text Pre-Shared Key**.

9. For the **Initiator ID**, we have entered the IP address of the remote gateway that we will be establishing a tunnel to. The **Initiator ID** does not have to be the IP address of the remote gateway. This could be almost any name you choose. We will cover this in greater detail when we configure the CES 221.
10. Enter your **Text Pre-Shared Key**. We used **test12345**, which will need to be the same on both ends. The CES 221 requires that this value be at least 8 characters long.

Note: If this was going to be a BOT, there would be no field to enter the **Initiator ID**.



11. Scroll to the bottom of the screen and click **Continue**:



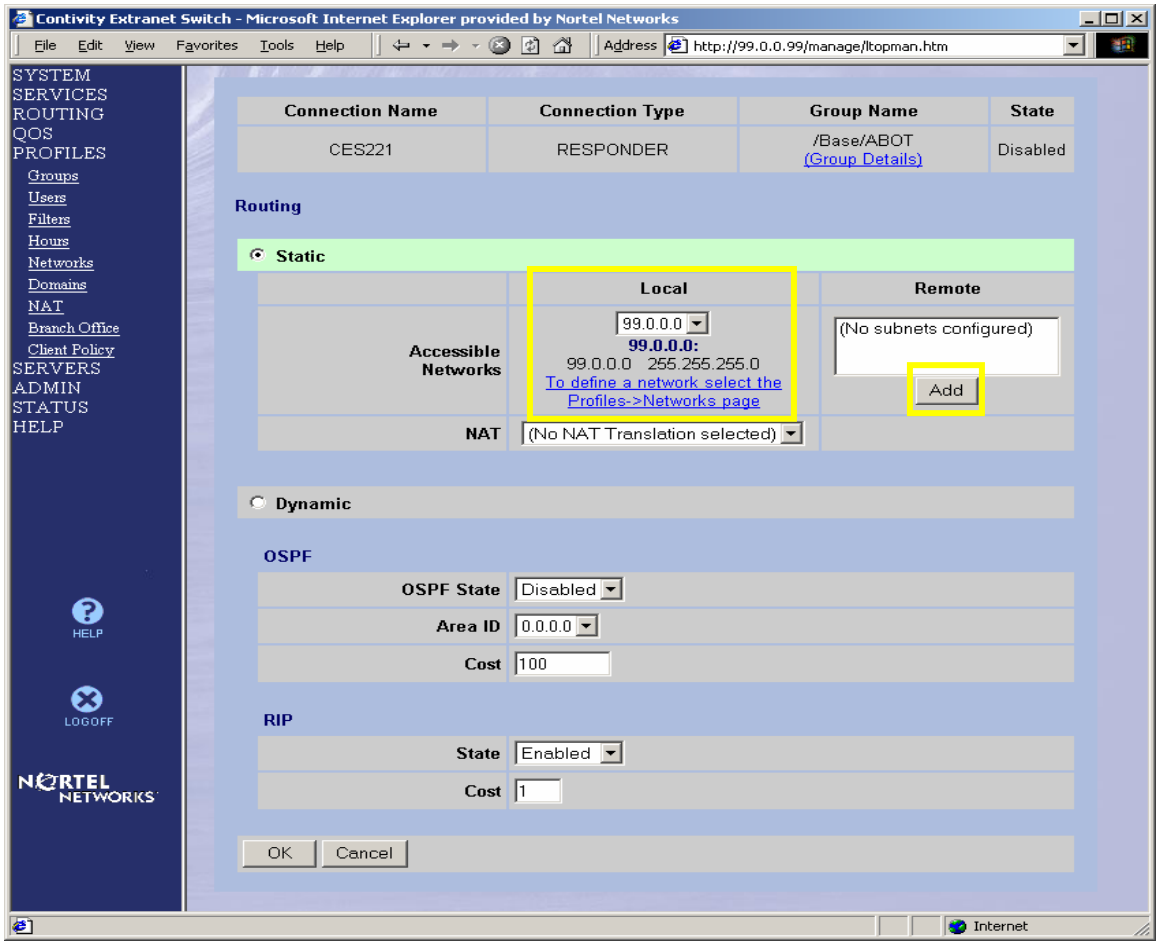
Branch Office Tunnels with Contivity 221 and 251

You now see the screen where you will configure the local networks that are available to the remote gateway (CES 221) and the remote networks that are available across the tunnel and on the private side of the CES 221.

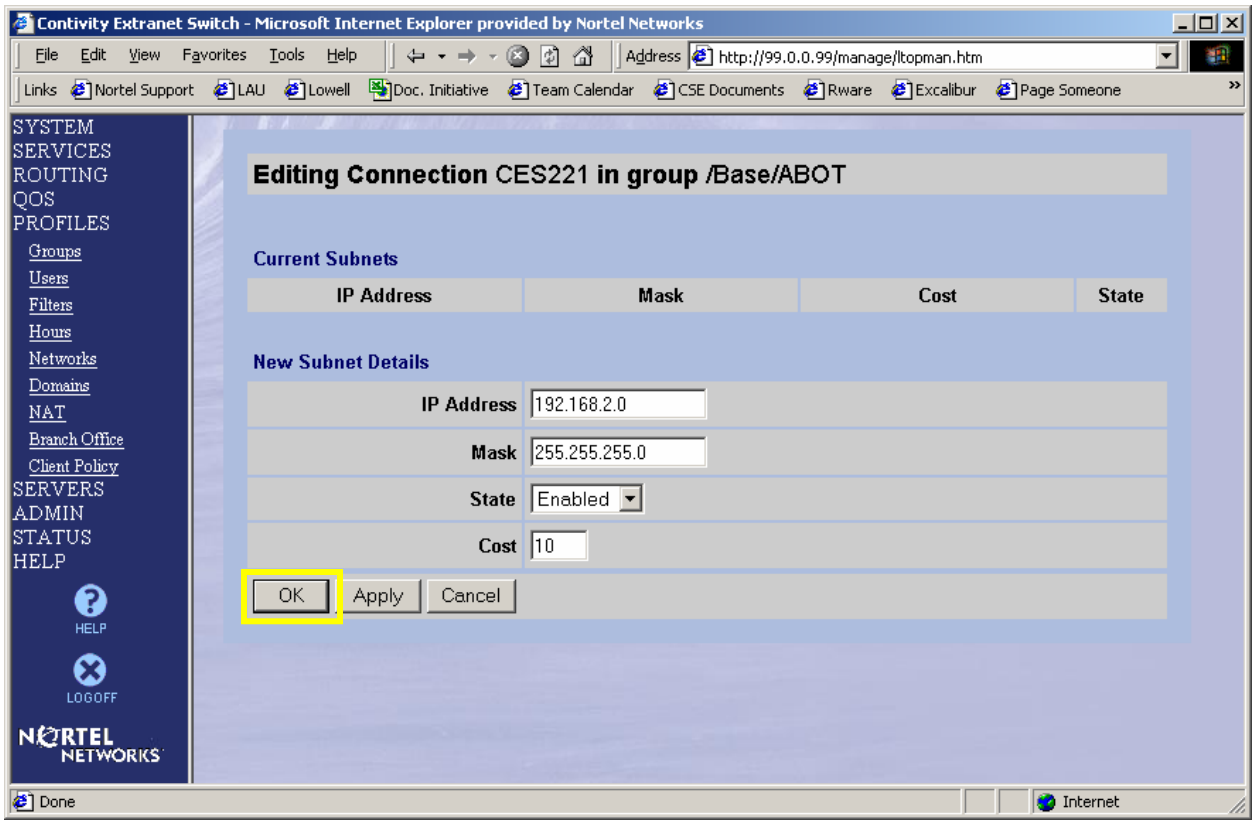
You will need to use the **Static Routing** configuration as, at the current time, the CES 221 does not support **Dynamic Routing** across the tunnel.

12. First you set the local networks that are available to the remote subnet behind the CES 221. To do this, you must first have created a network in **PROFILES → Networks**.
13. Select this network in the **Local** drop-down menu.
14. Enter the remote subnet(s) available across this tunnel. Do this by clicking **Add** under the **Remote** section of **Accessible Networks**.

Note: If you had not created your local network prior to coming to this screen, and had used the link to go there and create the network, then the tunnel will be disabled after you are done creating it. You will need to enable it before it will work.

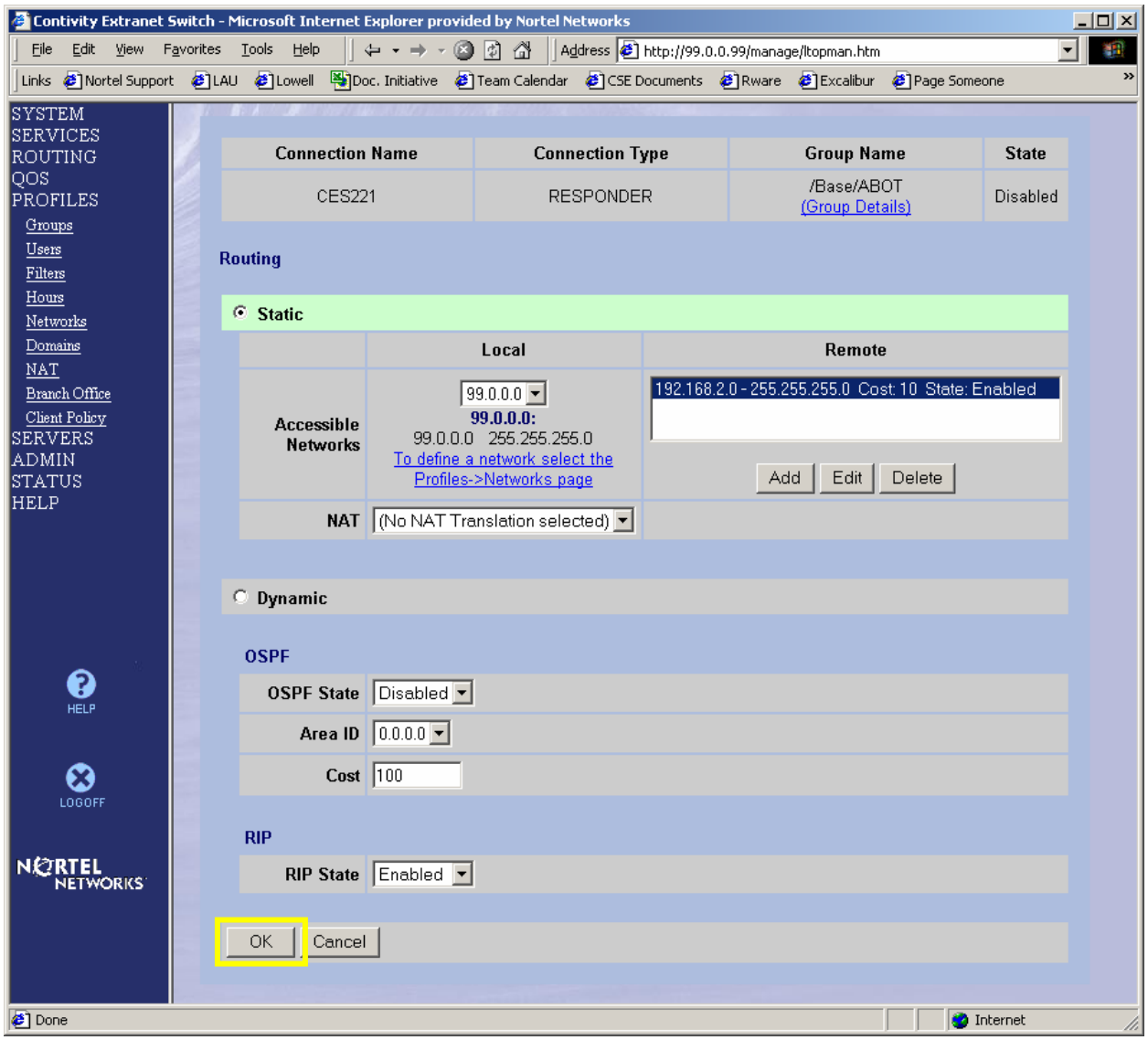


15. Enter the **IP Address** for the subnet and subnet **Mask** of the remote subnet that will be available upon tunnel establishment.
16. Click **OK**.



You will now see the **Remote Networks** accessible across the tunnel listed.

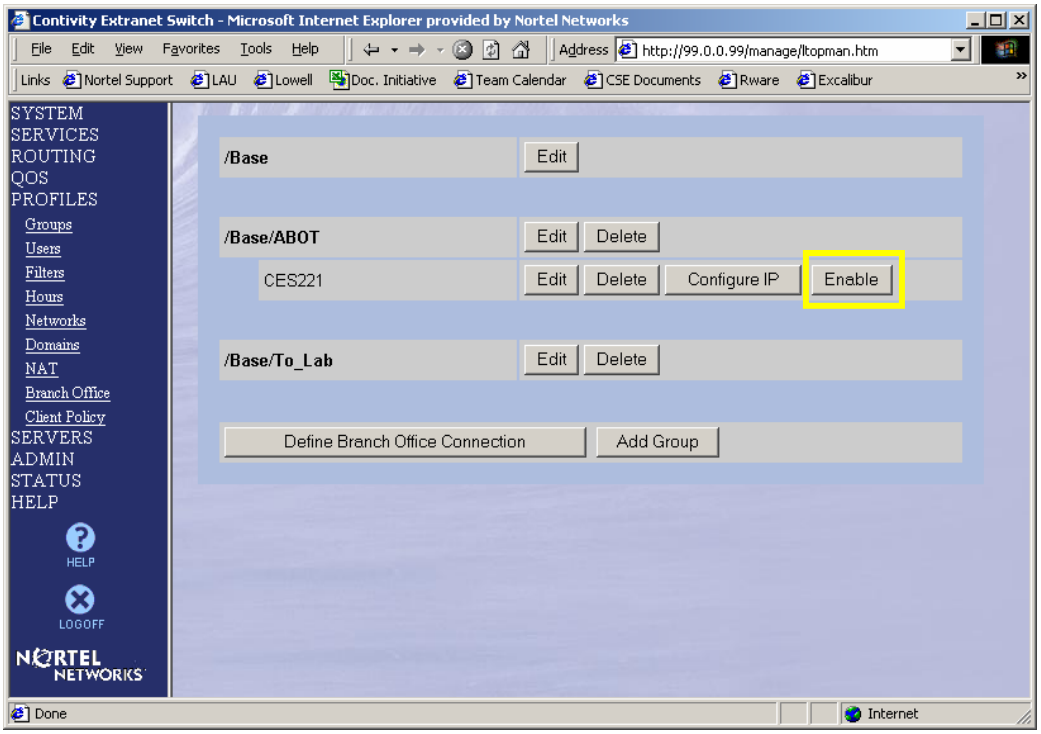
17. Click **OK**.



Branch Office Tunnels with Contivity 221 and 251

As stated previously, we created our network from the link to **PROFILES → Networks** from within the BOT configuration screen. This is why our tunnel is disabled.

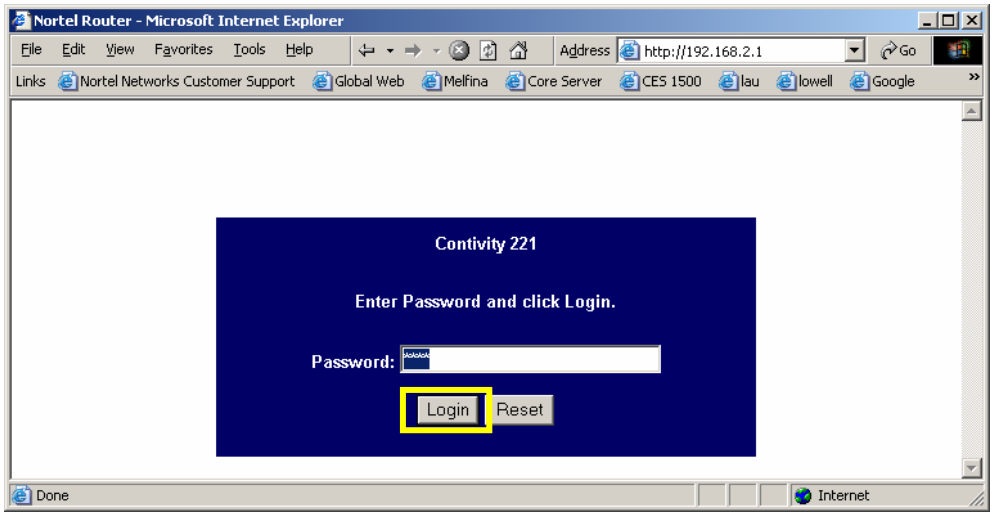
18. Click **Enable** to enable the new tunnel.



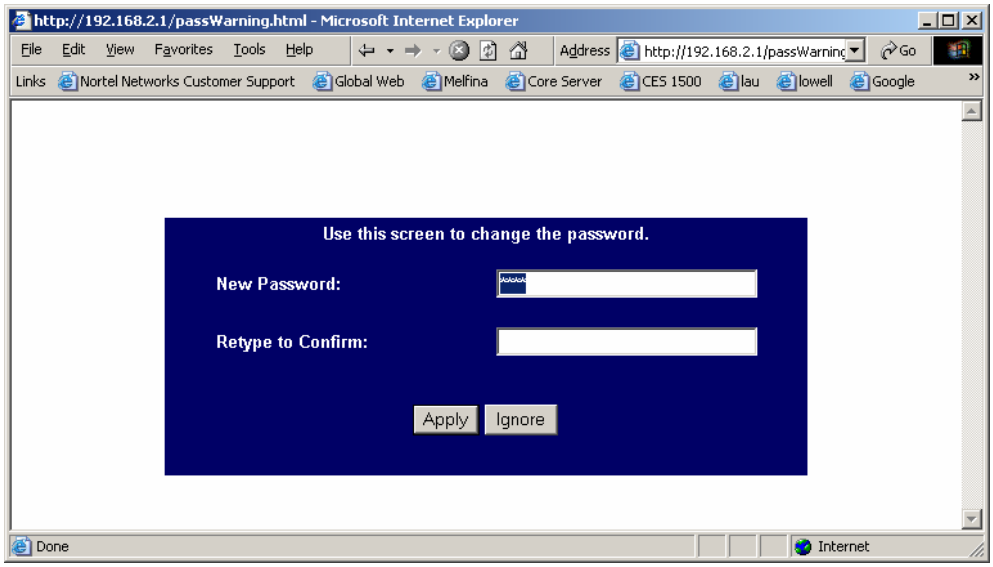
3. Configuring Remote Office Contivity

Now that we are finished configuring the ABOT at the central office, we must configure the tunnel on the CES 221 side.

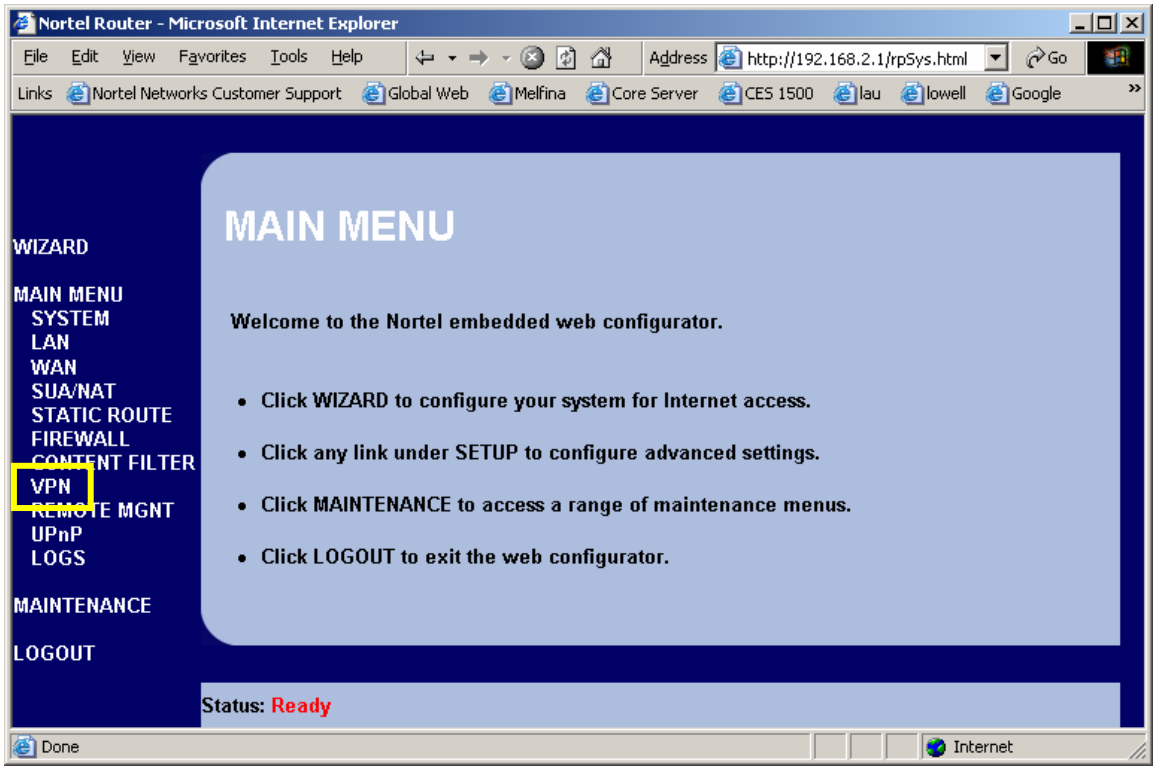
1. To log into the CES221 for the first time, you must have access to the private interface of the CES 221 and enter the IP address **192.168.2.1** in a web browser. This is the default address of the private interface and is used for management.
2. Once you do this, you will be prompted to enter the Password. By default, this password is **1234**.
3. Click **Login**.



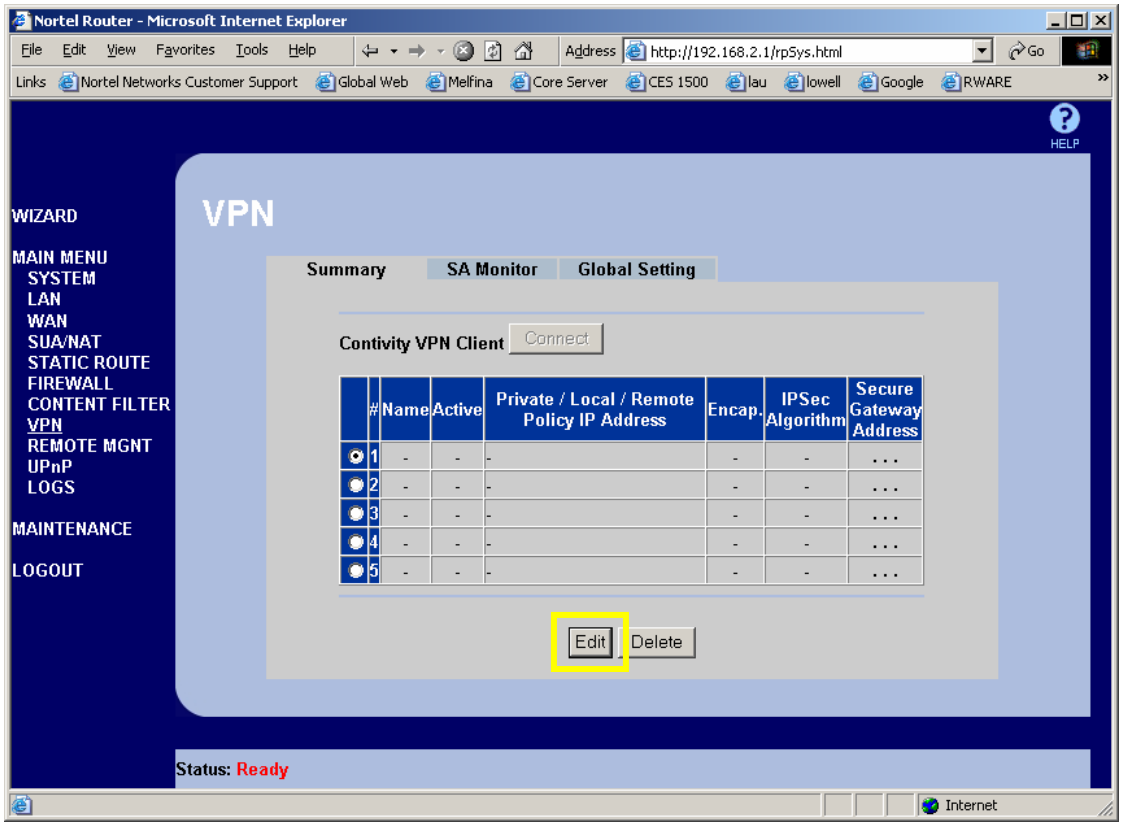
4. You will then be prompted to change the default password. You can either change the password or **Ignore** this option and leave the default password in place.



5. Once logged in, you see the main menu. To configure our branch office tunnel, you must click the **VPN** link on the left-hand side of the screen.



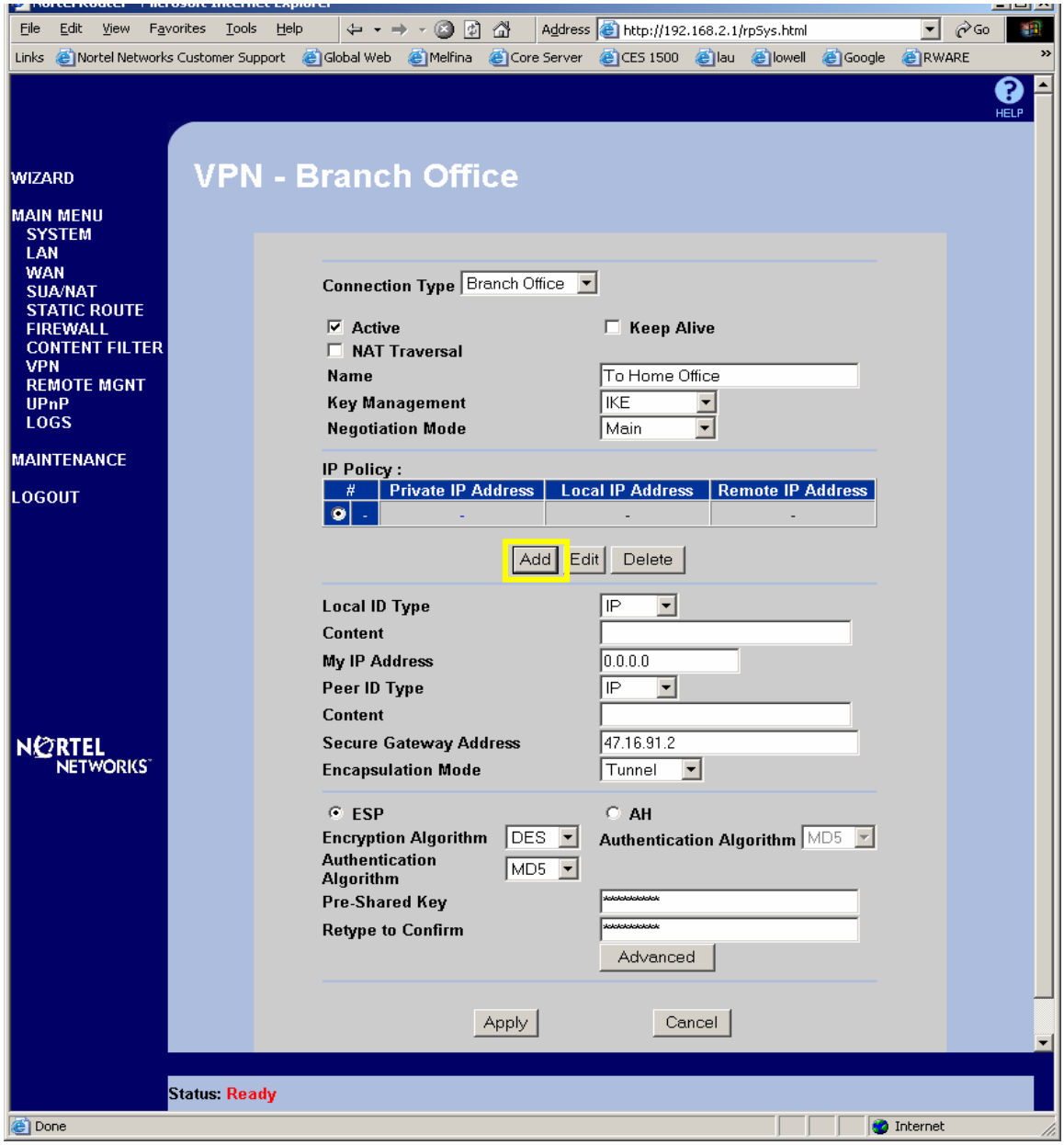
6. Make sure the first available tunnel is selected, and click **Edit**.



Branch Office Tunnels with Contivity 221 and 251

The Basic configuration settings for the Branch Office are shown.

1. Leave the Connection Type at **Branch Office**.
2. Select the **Active** option.
3. If you want to keep the tunnel up even when there is no traffic, select the **Keep Alive** option. This must be enabled on both ends for it to work. We want our tunnel to be an "On Demand" tunnel, so we have left it unchecked.
4. If there is a NAT device between the two IPsec devices, enable **NAT Traversal**.
5. Give your ABOT/BOT a user-friendly Name, such as **`To Home Office`**.
6. Leave the **Key Management** and **Negotiation Mode** at their defaults.



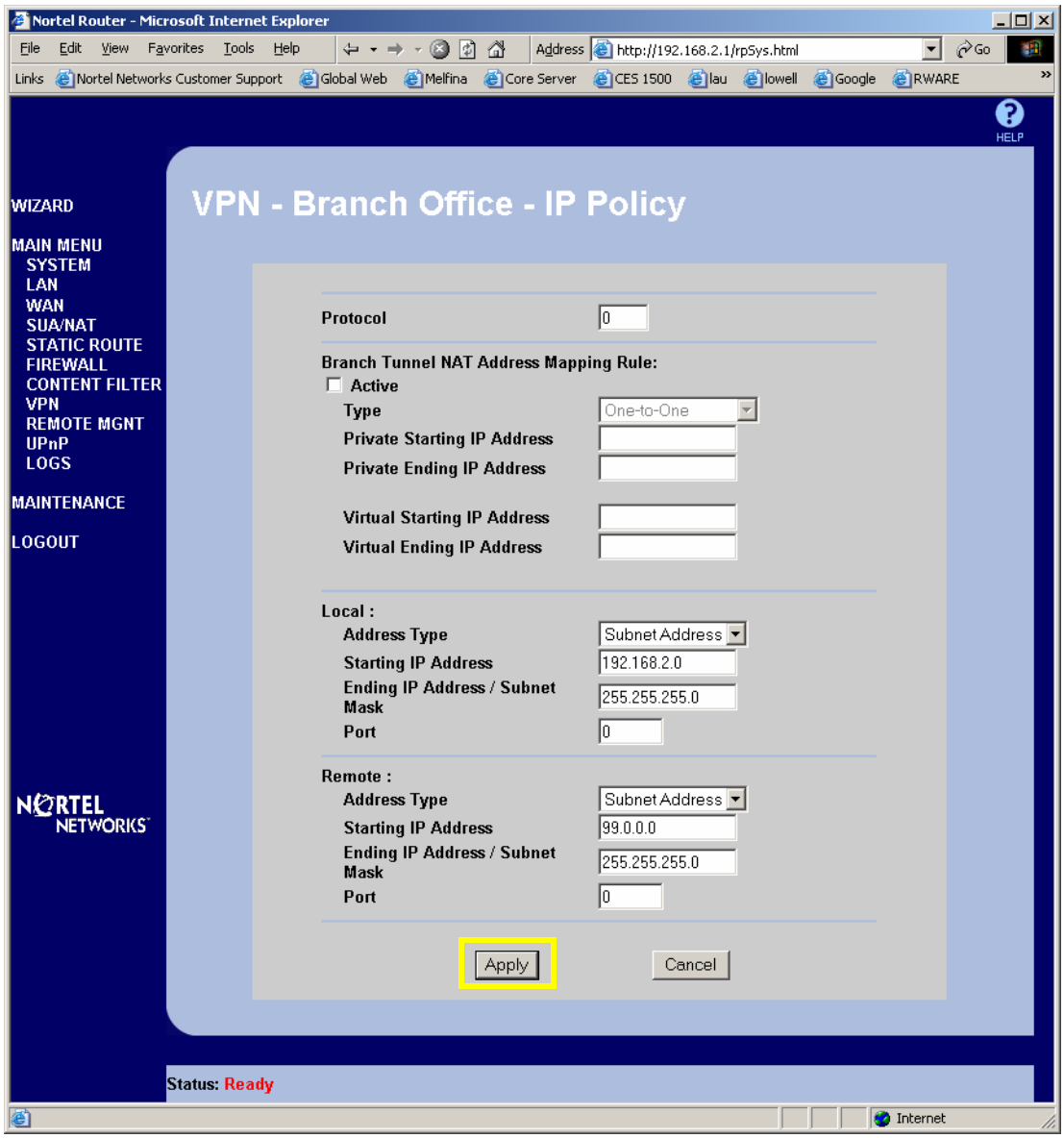
7. The Local ID Type is used to define what type of local ID we will be using. We used the default of **IP**. This setting determines what we can enter in the next setting of Local Content.
8. Local Content is the name we will use to identify ourselves to the remote gateway. Remember when we were configuring the **Initiator ID** in the **IPSec Authentication** settings of the central office Contivity and we entered the public IP address of the CES 221? This is why. Whatever we enter in this box, we must also enter in the Contivity Initiator **ID** box. We do not have to use our WAN IP address here. We could use any unique address, as long as it matches on the other end of the tunnel. If you leave this field blank, then it will use its WAN IP address, which is what we have done here.
9. My IP Address is where you would enter the local IP address assigned by the ISP. In our case, the ISP uses DHCP to assign us an IP address, so this address can change from time to time. Thus, we enter **`0.0.0.0`**, which will tell the gateway to use the current WAN interface IP address.
10. The Peer ID Type and Peer Content are the same as Local settings, only for the remote gateway (central office Contivity). Here we have used a Peer ID Type of **IP**, and left the Content field blank, which will have the CES 221 automatically use the IP address that you enter in the Secure Gateway Address field.
11. The Secure Gateway Address is the public IP address of the central office Contivity. If the remote gateway got a dynamic IP address from its ISP, then you would leave this IP address at 0.0.0.0. In our case, the remote gateway has a static IP address, so we placed it here.
12. Leave the Encapsulation Method at its default value of **Tunnel**.
13. Leave the default value of **ESP** selected.
14. We chose to leave the Encryption Algorithm at **DES**, and changed the default Authentication Algorithm from SHA-1 to **MD5**. This is because the central office Contivity defaults to **DES** and **MD5**. We could have alternatively left SHA-1 enabled and changed the setting in the central office Contivity to SHA-1. Whichever settings you choose for these two settings are fine, as long as they are properly enabled at both ends of the tunnel.
15. We set the Pre-Shared Key to the same value that we set the central office Contivity gateway's Text Pre-Shared Key, which was **`test12345`**. Enter it again in the Retype to Confirm field.
16. Leave the remaining settings at their default values.
17. Click **Add**.

The following **IP Policy** screen appears.

18. The **Protocol** setting is for the IP Policy. Enter **1** for ICMP, **6** for TCP, **17** for UDP, and so on. The default setting is 0 (zero) and signifies any protocol.

Branch Tunnel NAT Address Mapping Rule: Please note that if you choose to use a **Branch Tunnel NAT Address Mapping Rule**, you will not configure the **Local** settings.

19. Select the **Active** option to enable the NAT rule. It is disabled by default.



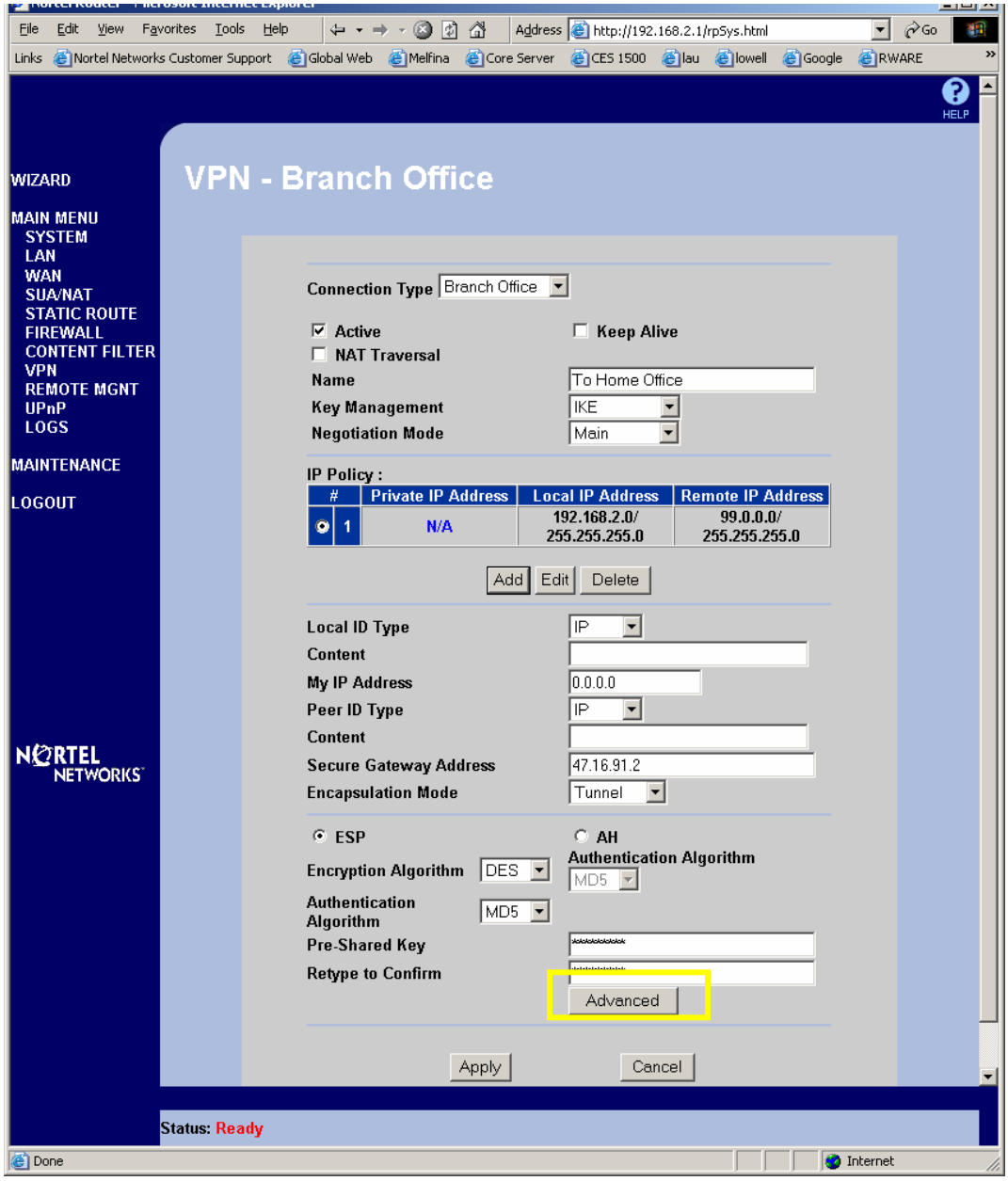
20. **Type** represents the type of NAT being used. The three options are **One-to-One**, **Many-to-One**, or **Many One-to-One**. This field and the four fields below it are not used in our example and are beyond the scope of this document. However, if you choose to activate NAT here, then we recommend that you click on the Help link in the top right-hand corner of your screen. All of these fields are explained in detail and in easy-to-understand terms.

Local: The **Local** settings are for the local addresses that will be made available to the home office. This must be configured as the **Remote Address** in the remote VPN device at the opposite end of the tunnel.

21. **Address Type** is used to define whether the tunnel will be making a **Single Address** available, a **Range Address**, or an entire **Subnet Address**.
22. If it is
    - a single address: enter the address in the **Starting IP Address** box
    - a range of addresses: enter the starting address of the range there, and the ending address of the range in the **Ending IP Address End/Subnet Mask**
    - an entire subnet address: enter the subnet IP address and the subnet's mask. In our example, we will be making the entire subnet of **`192.168.2.0/255.255.255.0`** available to the central office (remote gateway).
23. Use the same method in setting the values for the **Remote Addresses Start** and **End/Mask**. Those are the addresses that will be available to the local subnet on the private side of the CES 2x1.
24. Once the appropriate parameters have been set, click **Apply**.

The main configuration page of the tunnel appears. You will now see your newly created **IP Policy**.

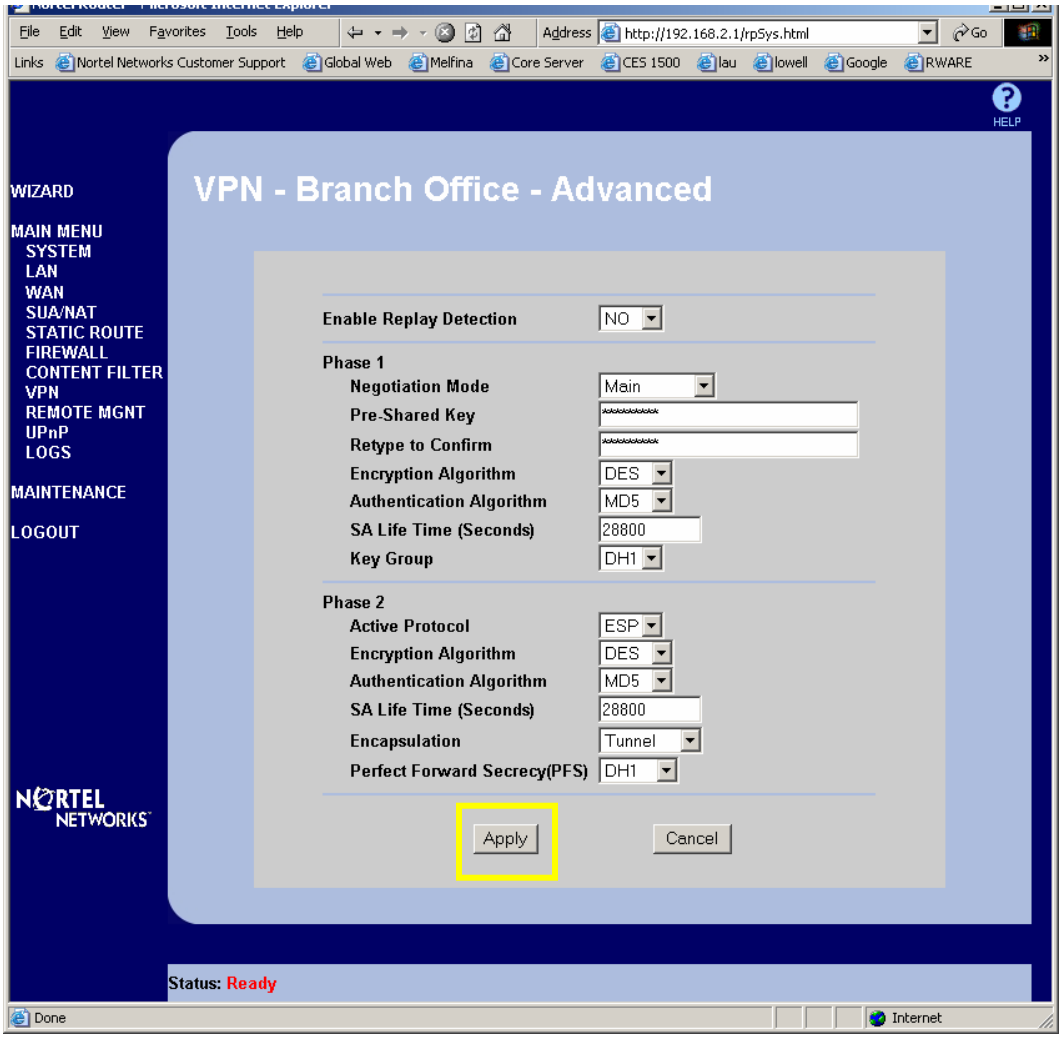
25. Click the **Advanced** button.



Branch Office Tunnels with Contivity 221 and 251

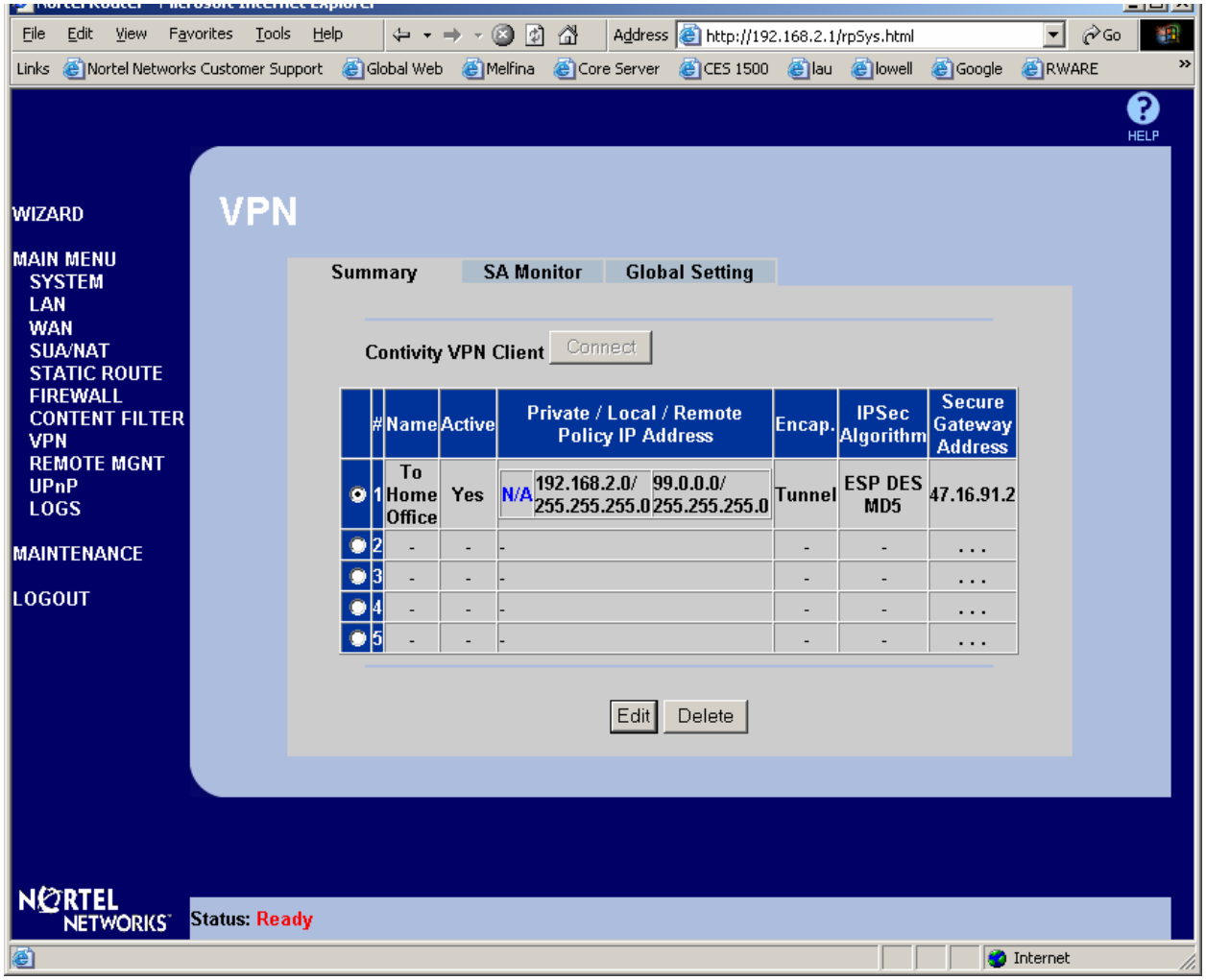
The only settings we have changed in the Advanced settings are the Perfect Forward Secrecy (PFS) and the Phase 2 Authentication Algorithm.

26. By default, the central office Contivity has PFS enabled, so we have enabled it here to **DH1** (Diffie-Hellman Group 1). Alternatively, we could leave this disabled and disable it on the central office Contivity as well.
27. The same situation goes for the Phase 2 Authentication Algorithm. We could have left it at SHA-1 here and enabled it at the central office as well. Instead, we chose to change it to **MD5** here.
28. Click **Apply**.
29. Click **Apply** again on the main tunnel configuration page.



Branch Office Tunnels with Contivity 221 and 251

Here is what the **Summary** tab will look like after the tunnel has been configured.



4. Testing the setup

Once the tunnels are configured on both gateways, you may need to start a ping from the remote branch office to the central office subnet to get traffic to initiate the tunnel. Below are the logs from the central office Contivity and the CES 2x1, respectively, of the ABOT coming up.

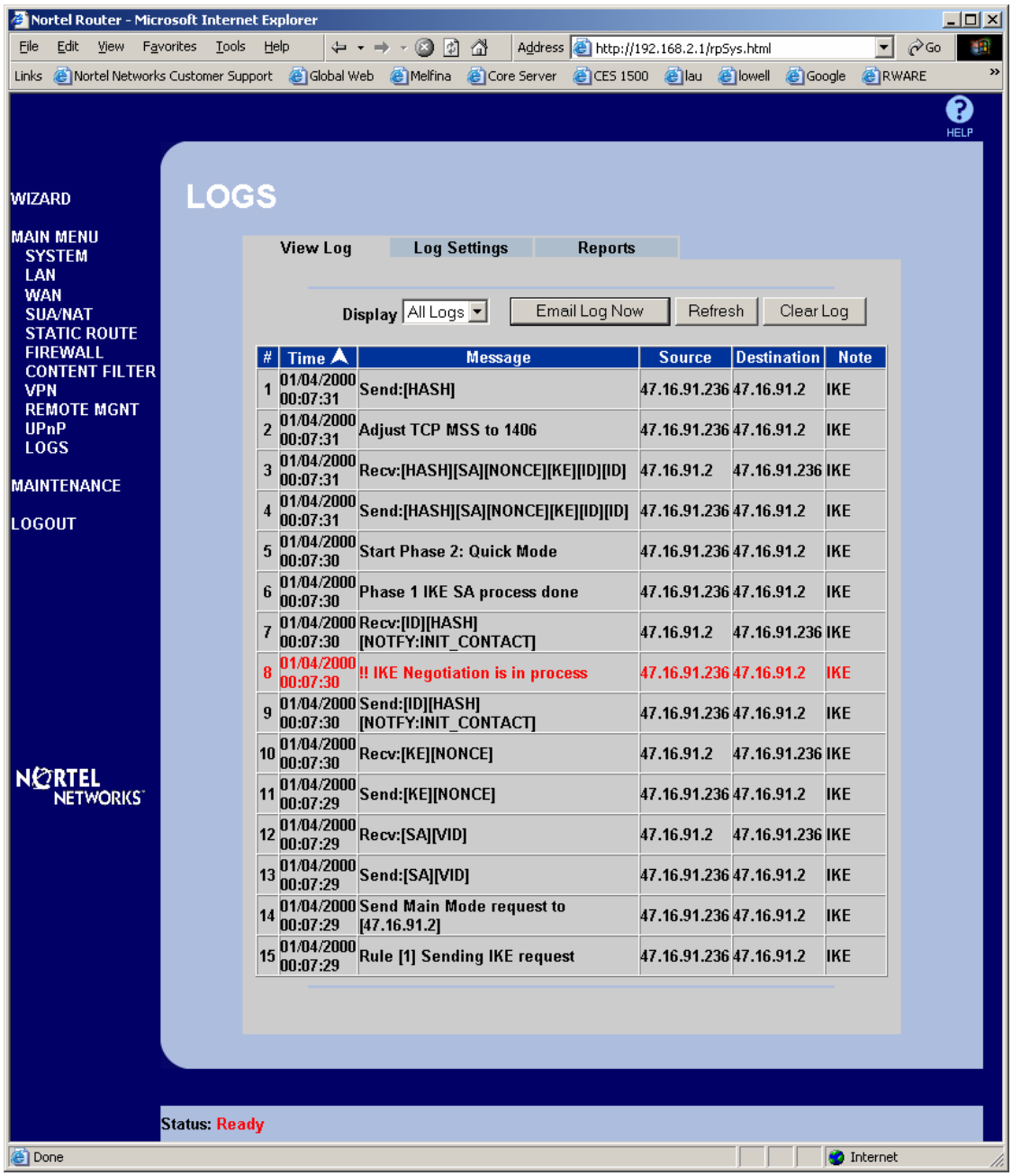
4.1. Central Office Contivity

10/13/2003 11:08:06 0 Security [11] Session: IPSEC[47.16.91.236] attempting login
10/13/2003 11:08:06 0 Security [01] Session: IPSEC[47.16.91.236] has no active sessions
10/13/2003 11:08:06 0 Security [01] Session: IPSEC[47.16.91.236] CES221 has no active accounts
10/13/2003 11:08:06 0 ISAKMP [02] Oakley Main Mode proposal accepted from 47.16.91.236
10/13/2003 11:08:07 0 Security [01] Session: IPSEC[47.16.91.236]:65 SHARED-SECRET authenticate attempt...
10/13/2003 11:08:07 0 Security [01] Session: IPSEC[47.16.91.236]:65 attempting authentication using LOCAL
10/13/2003 11:08:07 0 Security [11] Session: IPSEC[47.16.91.236]:65 authenticated using LOCAL
10/13/2003 11:08:07 0 Security [11] Session: IPSEC[47.16.91.236]:65 bound to group /Base/ABOT/CES221
10/13/2003 11:08:07 0 Security [01] Session: IPSEC[47.16.91.236]:65 using group filter permit all
10/13/2003 11:08:07 0 Security [11] Session: IPSEC[47.16.91.236]:65 authorized
10/13/2003 11:08:07 0 Branch Office [01] Setting up branch office gateway [47.16.91.236] uid:[47.16.91.236]
10/13/2003 11:08:07 0 Branch Office [01] InstallBOSession: IPSEC[47.16.91.236] routing [STATIC]
10/13/2003 11:08:07 0 McRelay [00] Received circuit up for circuit num = 66. local 192.168.2.0
10/13/2003 11:08:07 0 McRelay [00] MC circuit enabled. circuit num = 66, ifp 1614c60
10/13/2003 11:08:07 0 MarshalerRtmClient [00] MarshalerRtmClient::Inject(): mwriting 1 nexthops.
10/13/2003 11:08:07 0 RTM [10] netWrite RTM_RouteDef: N 192.168.2.0 M 255.255.255.0 NumNH 1 NH 47.16.91.236 CM 0x5cec8c0
10/13/2003 11:08:07 0 RTM [00] writeNewEntry: adding new: 192.168.2.0 to 192.168.2.255
10/13/2003 11:08:07 0 RTM [00] NextHop:newEntry NextHop: 47.16.91.236 NHI 47.16.91.2 C 66 CM 0x5cec8c0 PR (5493f24) 47.16.91.2
10/13/2003 11:08:07 0 Branch Office [01] 5cecf18 BranchOfficeCtxtCls::InstallRoute: Route installed for rem[192.168.2.0-255.255.255.0]@47.16.91.236
10/13/2003 11:08:07 0 RTM [00] Best::nextRoute fini for 0x40
10/13/2003 11:08:07 0 ISAKMP [02] ISAKMP SA established with 47.16.91.236
10/13/2003 11:08:07 0 BaseCmsClient [00] RipCmsClient::New() : handling new circuit event for circuit 66 [0x7188230].
10/13/2003 11:08:07 0 BaseCmsClient [00] RipCmsClient::New(): FAILED; unknown circuit type.
10/13/2003 11:08:07 0 RTM [00] Best::nextRoute fini for 0x1
10/13/2003 11:08:07 0 DHCP Relay Table [00] Circuit config node for interface 192.168.2.0 inserted
10/13/2003 11:08:08 0 Security [11] Session: network IPSEC[192.168.2.0-255.255.255.0] attempting login
10/13/2003 11:08:08 0 Security [11] Session: network IPSEC[192.168.2.0-255.255.255.0] logged in from gateway [47.16.91.236]
10/13/2003 11:08:08 0 Security [12] Session: IPSEC[47.16.91.236]:65 physical addresses: remote 47.16.91.236 local 47.16.91.2

Branch Office Tunnels with Contivity 221 and 251

10/13/2003 11:08:08 0 Security [12] Session: IPSEC[-]:68 physical addresses: remote 47.16.91.236 local 47.16.91.2
10/13/2003 11:08:08 0 Outbound ESP from 47.16.91.2 to 47.16.91.236 SPI 0x30f2f1d0 [03] ESP encap session SPI 0xd0f1f230 bound to cpu 0
10/13/2003 11:08:08 0 Inbound ESP from 47.16.91.236 to 47.16.91.2 SPI 0x00229b6f [03] ESP decap session SPI 0x6f9b2200 bound to cpu 0
10/13/2003 11:08:08 0 Security [01] Session: IPSEC[-]:68 Using gateway input filters 57914f8 57fb5b8 699d898
10/13/2003 11:08:08 0 Security [01] Session: IPSEC[-]:68 returning gateway output filter 6697550
10/13/2003 11:08:08 0 Branch Office [00] 5cecf18 BranchOfficeCtxtCls::RegisterTunnel: rem[192.168.2.0-255.255.255.0]@[47.16.91.236] loc[99.0.0.0-255.255.255.0] overwriting tunnel context [0] with [57fbef0]
10/13/2003 11:08:08 0 ISAKMP [03] Established IPsec SAs with 47.16.91.236:
10/13/2003 11:08:08 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-MD5 outbound SPI 0x30f2f1d0
10/13/2003 11:08:08 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-MD5 inbound SPI 0x229b6f

4.2. Remote Office Contivity (CES 221)



Tech Tip
Contivity Secure IP Services Gateway

Branch Office Tunnels with Contivity 221 and 251

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Networks Technical Support on the web at: http://www.nortel.com/support

If after following this guide you are still having problems, please ensure you have carried out the steps exactly as in this document. If problems still persist, please contact Nortel Networks Technical Support (contact information is available online at: http://www.nortel.com/cgi-bin/comments/comments.cgi?key=techsupport_cu).

We welcome you comments and suggestions on the quality and usefulness of this document. If you would like to leave a feedback please send your comments to: CRCONT@nortel.com

Author: Sean Merrow