Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Nortel Instant Internet 100-S VPN Configuration

This paper will discuss the configuration and use of the Nortel Instant Internet 100-S as a VPN client in one organization's network environment.

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

Nortel Instant Internet 100-S VPN Configuration
Lloyd V Ardoin
version 1.2e
June 28, 2001

This paper will discuss the configuration and use of the Nortel Instant Internet 100-S as a VPN client in our network environment. The Instant Internet 100-S has evolved from the BayStack Instant Internet product. Nortel acquired this product line when it purchased Baynetworks in 1998. A general description of the product can be found in a n article in the Network World publication dated 11-01-1999 (URL below).

> "The 100 model connects branch office LANs to the corporate networks via Internet VPNs. The device also provides LAN-to-Internet connectivity for business that need Net access now and may later want to implement a VPN via a software upgrade."[1]

Nortel is taking this product not only through a software evolution upgrade but also making hardware enhancements as well. On December 30,2000 Nortel released a "End of life" notification for the Baystack Instant Internet. In part it states:

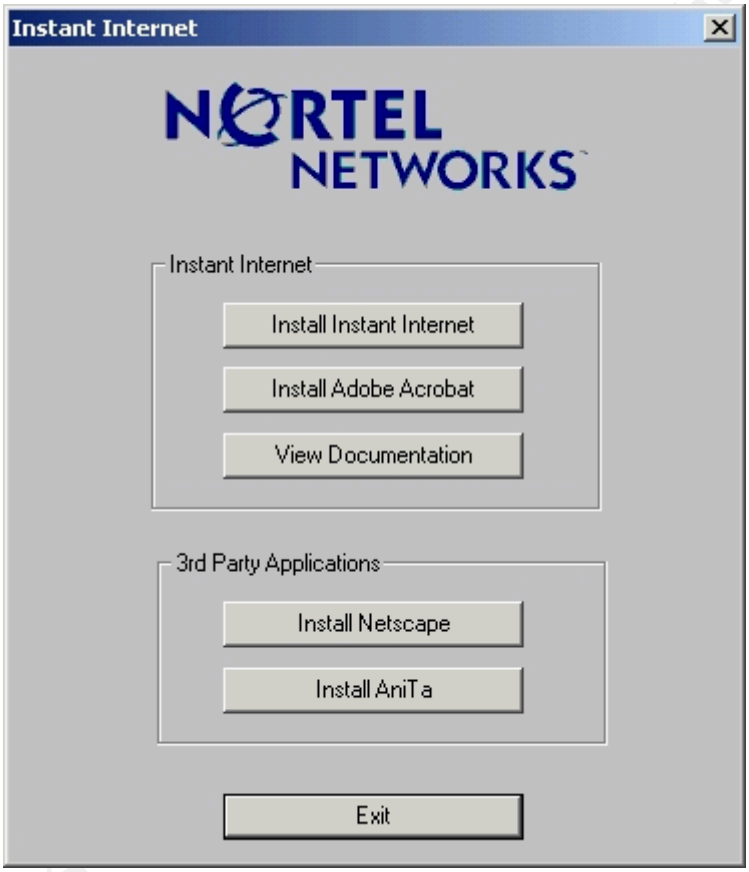
> "Approximately one year ago, the Instant Internet product team started working on the next generation of hardware, the 100-S and the 400-S series. The new product will begin shipping mid-December. The changes between the older series are as follows:
> The new hardware includes:
>
> > 7-port layer 2 autosensing 10/10 Ethernet Switch
> > faster processor on both units
> > Additional Ethernet port
> > (the 100-S now has 2 Ethernet ports on the base chassis and the 400-S automatically ships with 3 Ethernet ports)"[2]

The Instant Internet family is currently being evolved over to the Nortel Contivity line of products and will eventually include the Contivity 100, 400 and 600 appliances. The software upgrade program is being done in a two phase process. Phase 1 scheduled for July 1 of 2001, Nortel will release v7.21. Phase 2 Nortel will release v8.0 scheduled for November 2001. With the upgrade program on going the Instant Internet includes many rich features such as Ripv1 and Ripv2, DHCP client and server, NAT, SNMP, NTP, Telnet, PPP, Multi link and PPoE. It also incorporates security through stateful inspection in Network Address Translation (NAT) and five-proxy firewall. It also supports PPP, CHAP and IPSEC. Interface support includes Analog, ISDN, X.21, V.35, Frame Relay and Dual Ethernet. We purchased the the dual ethernet configuration because it allows the flexibility of not being tied to a specific 'flavor' of service at the remote sites (i.e. DSL, Cable Modem, ISDN, etc.). At the corporate end of the tunnel we have a Contivity 1510 which is also part of the Nortel family. It is part of the Contivity VPN Switch product family including the 1500, 2600 and 4500. The Contivity 1510 will support up to 100 simultaneous tunnels. Since we are in the process of moving from current network technology of ISDN and Frame Relay to either DSL or Cable Modems and some of these

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

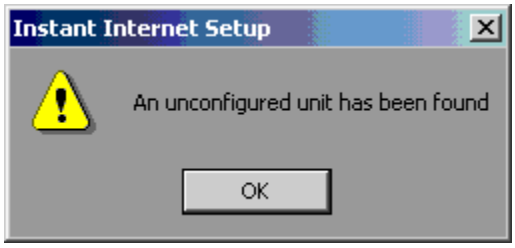
remote sites are located in rural areas. The dual ethernet configuration will allow us to adopt what ever technology becomes available in those areas first. Now that we have got that behind us it's time to concentrate on actually getting the thing out of the box it was shipped in and see if we can make it work.

First things first we must install the Instant Internet Configuration utility on the PC that we are going to use to configure the Instant Internet 100-S. This utility can be found on a CD that is included with the device. Just slip it into your CDROM drive and you are off and running. There is an auto start file that will bring up a menu like the one in the screen shot below.

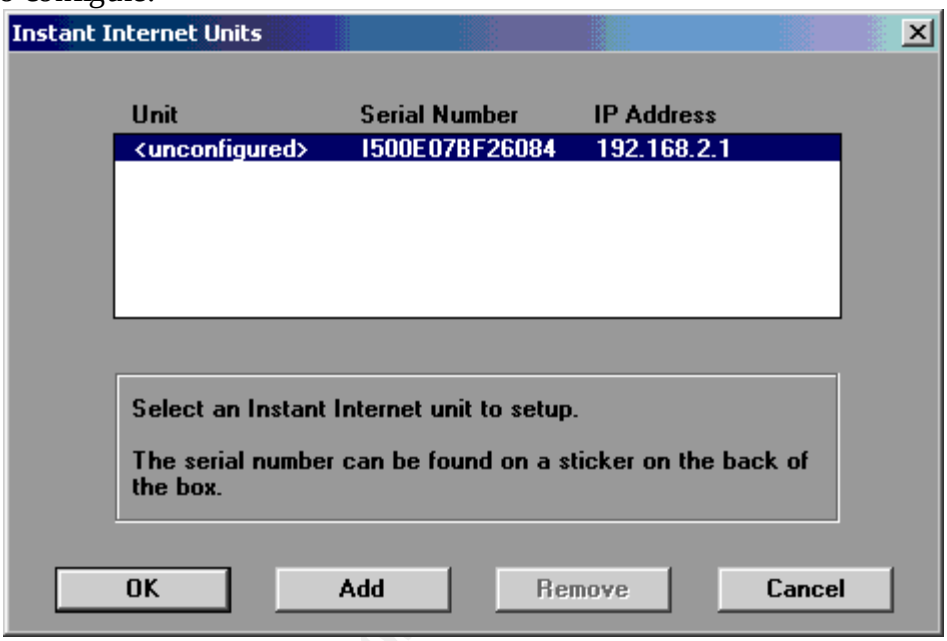


By clicking on the first button you will start the instal process. Once this has completed you will have a new menu option on your PC called Instant Internet. There will be six options available on this menu; Admin, Autolog, Monitor, Setup, Tools and Uninstal. We will be using the Setup option to connect to the unconfigured device. I have a separate hub that I use in my office which allows me to connect my PC to all types of devices that I need to configure, test, etc. This isolates this equipment from my production LAN, which of course is a good thing. The Instant Internet 100-S has been described as a 'plug-n-play' device and getting it up and talking to my PC is pretty much that. Plugging in the power cable, a Cat 5 cable from the hub to the ethernet port and turning it on. Once this is done all I need to do is select the Setup option from the menu and the software will look for any 'unconfigured' devices. If it finds one the utility will prompt you with the screen like the one below.

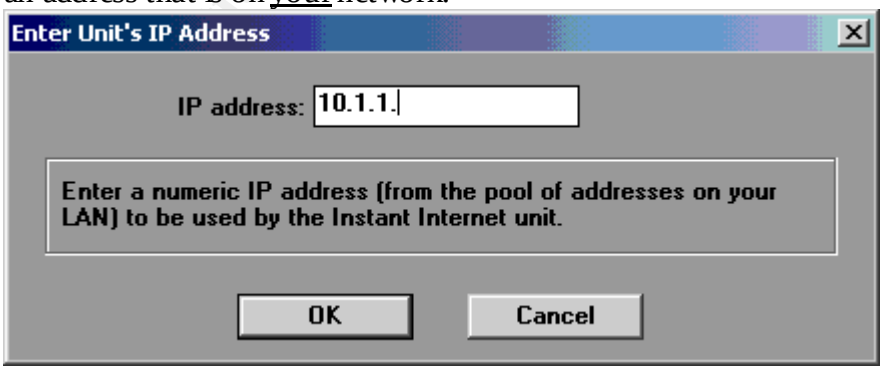
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



By clicking the 'OK' button it will present you with the next screen so you can select the device to configure.

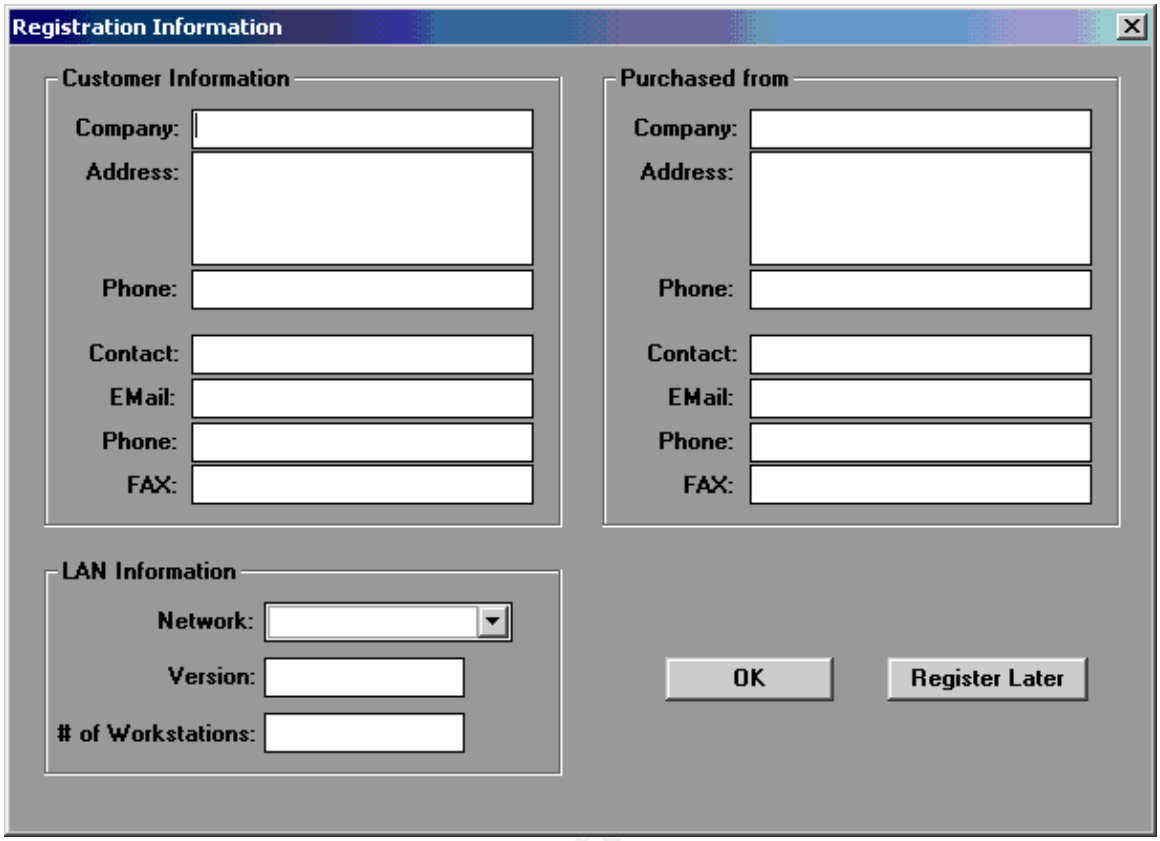


This screen shows you the serial number, the unit name as 'unconfigured' and uses a default IP address of one of the 'reserved' network addresses described in RFC 1918. By clicking on the 'OK' button the utility will present you with a screen to change the IP address to an address that is on your network.

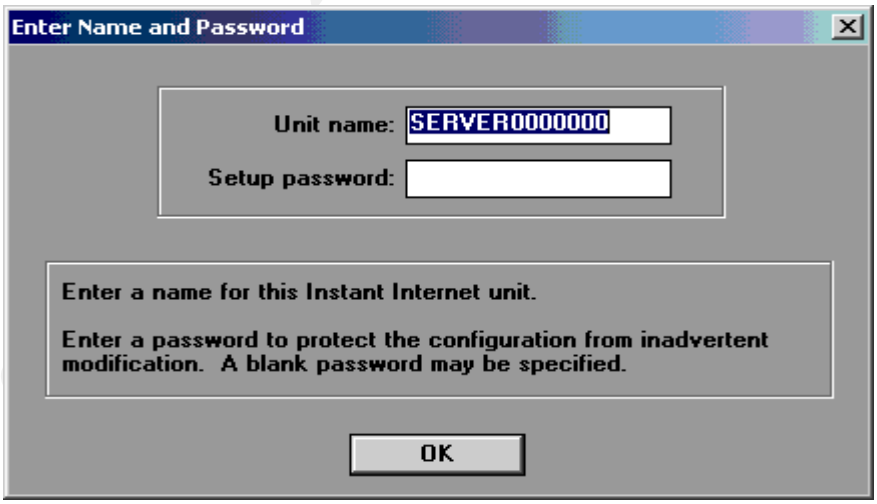


I have changed my computer's address to the network address of the remote site that I am configuring this device for. Since my computer address for this example is 10.1.1.2 it is presenting me with a '10.1.1._' option so that once I enter this address it will put the device on my local network. Once I enter a '1' and click 'OK' it ask if I want to start the DHCP server. I select 'No' since we do not use this service in our configuration. The next screen shown below is the Registration Screen.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

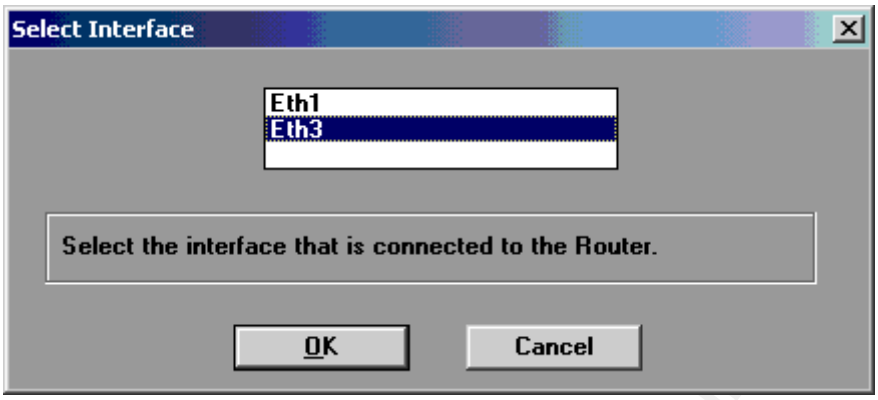


If you don't fill it out now it will show up every time you get back in it so you might as well get it over with. Once I complete this information I click on the 'OK' button and it takes me to the next screen where I will need to enter a name for this device. This is just like a description on any device you might setup on your network.

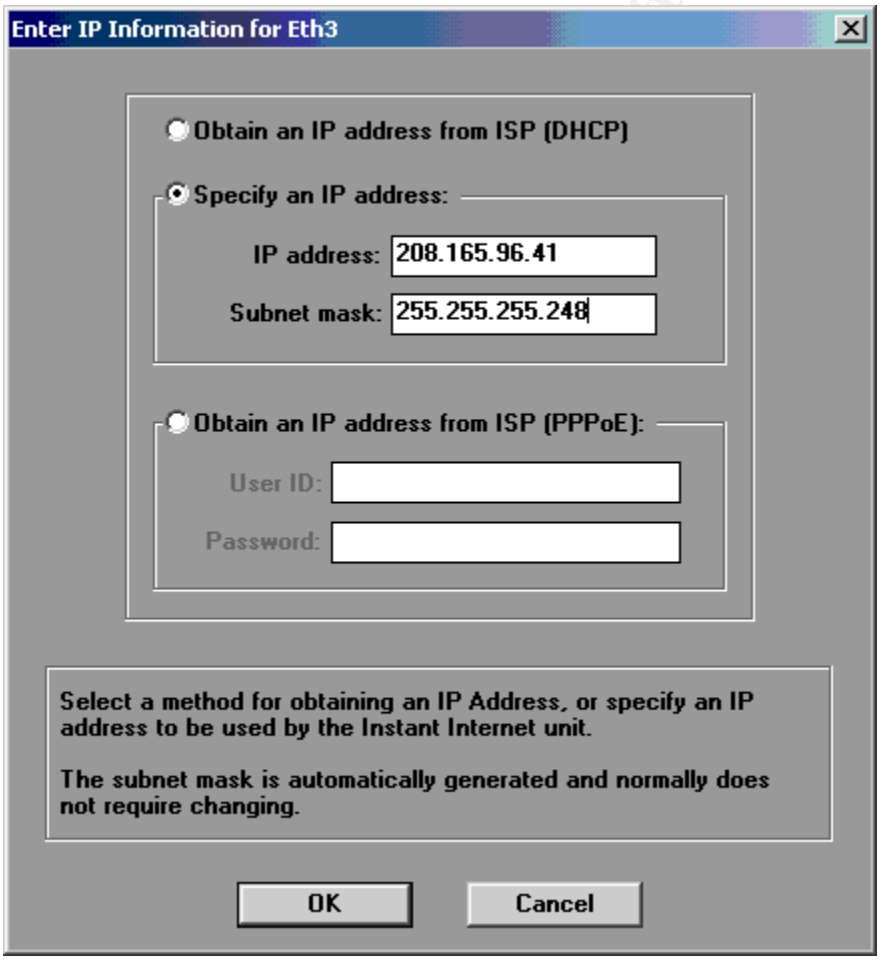


To complete this step I type in 'Test_system' for a name and 'test' for the password that I will use for my example. The password will be needed next time I try and use this utility to access the device or telnet into it. I have to re-confirm the password and then I get the next screen to select the port connected to the router, which is defined as the 'public' port of the Instant Internet 100-S.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



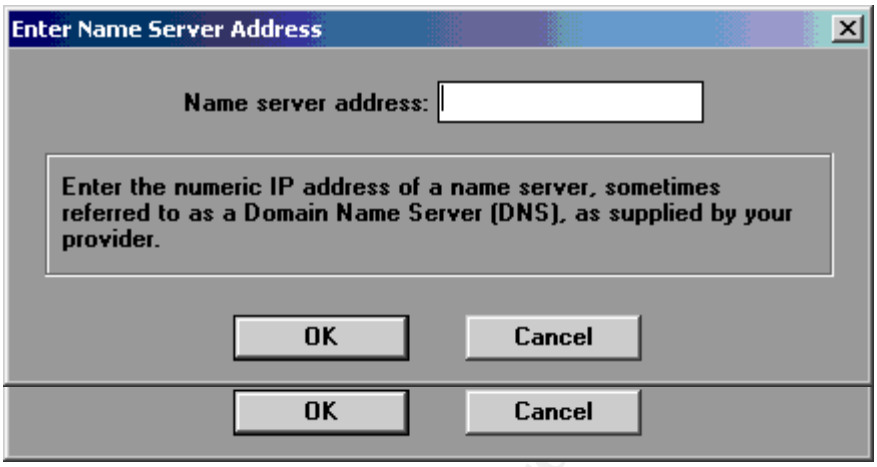
We are using 'Eth1' as our LAN port so we select the 'Eth3' as our public port and click the OK button.



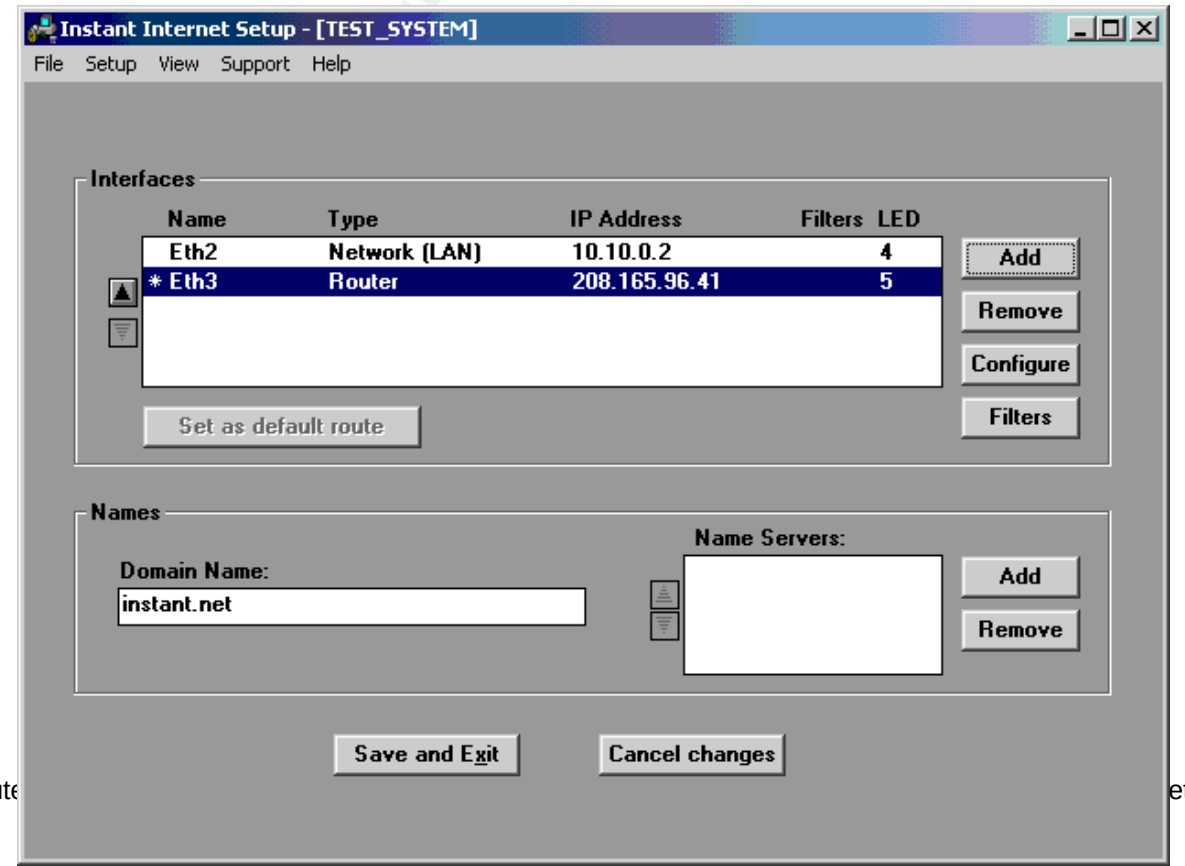
The next screen presents us with options on how our public port gets it's IP address. We can choose to have it assigned dynamically or we can enter a static IP address.
Since this is going to be sitting behind a DSL modem, Cable modem or router and we are going to be doing tunneling to it we will use a static IP address. I enter the public address and subnet mask that I was given from my ISP and click the OK button.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This next screen shown above is asking for the router address which represents the next hop back to the ISP. Based on the example addressing I am using it would be the last valid IP address in the range of 208.165.96.41 – 46 (your ISP could configure this differently). So I enter 208.165.96.46 and click the OK button to continue.



The next screen shown above is asking for a DNS server address for this device. If you are going to provide Internet access though this device for your users you can set up the DNS Proxy service on here. It expects something in here even though we do not provide this service for this particular case so I go ahead and enter the DNS server addresses for the ISP. It will prompt you to enter another and you can or just click 'No'. Once this is completed the configuration utility will give you an opportunity to 'Save and Exit' or 'Customize Setup'. We choose the latter option to continue our configuration for tunneling.

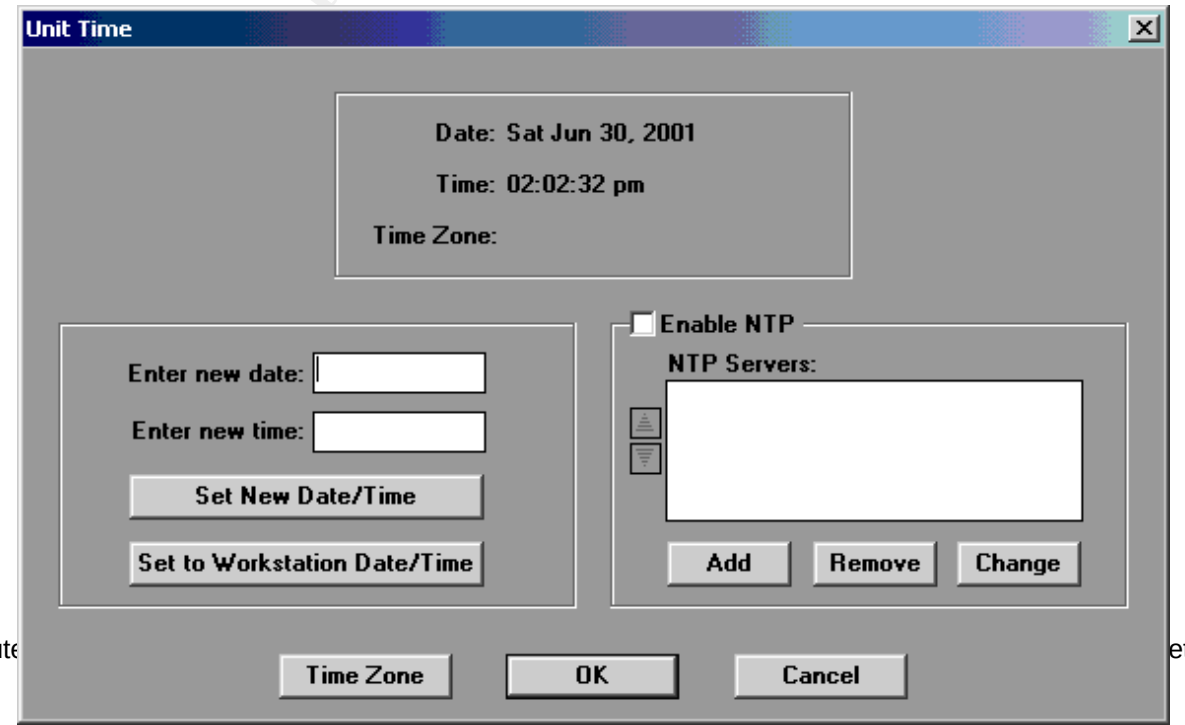


© SANS Institute etains full rights.

This finally brings us to the main screen of the configuration utility. This screen as several areas of interest. Along the top you see that the title bar includes the name of the device that we are currently configuring. The menu system is located just below that area. In the middle of the screen is a list of the ports that are currently configured on the device. Since this is a dual ethernet model we have the two default ports in the list. The are up and down arrow keys located on the left side of this area which allow you to change the order of the ports list. There is a button below the ports list that allows you to set the default route. The asterisk next to eth3 reflects that this is the default route. The buttons to the right of the ports list allow you to add, remove, configure, and set filters on the ports. In the bottom portion of the window on the left side is where you can list the domain name of the device. On the right side is where we could add or remove DNS servers if you want to configure the Instant Internet 100-S to provide DNS service. Since we use this device strictly to provide a tunnel back to our private network it is not necessary to configure this service.

I will take you through a quick tour of the menu options keeping in mind that most of the work to be done will be under the 'Support' menu option. The 'File' menu option includes Configure, Backup/Restore to/from a disk, Restart the unit and Exit. The 'Setup' option includes Register, Change Password, Change Unit Name, Time, and Test Connection. The Time option provides a configuration screen like the one below.

Since the unit does not have an internal clock it must get it's time from an external source. You can manually set it, you can have it use a workstation's time or you can enable it to use a NTP server. The 'Test Connection' menu option allow you to test the connection to the internet and will provide a results screen and suggestions depending on the results. Under the 'View' menu you will find several logs that can be viewed as well as the ability to view 'Users' that are connected in a live environment. I will skip over the 'Support' option and save it for last since this is where most of the configuration is done. The 'Help' option includes the usual 'Index, Using Help and About...'. Now let's take a detailed look at the 'Support' menu option. We will look at these in more detail in just a minute. The options list is Advanced TCP/IP Settings, Port Mappings, Hosts, Services,

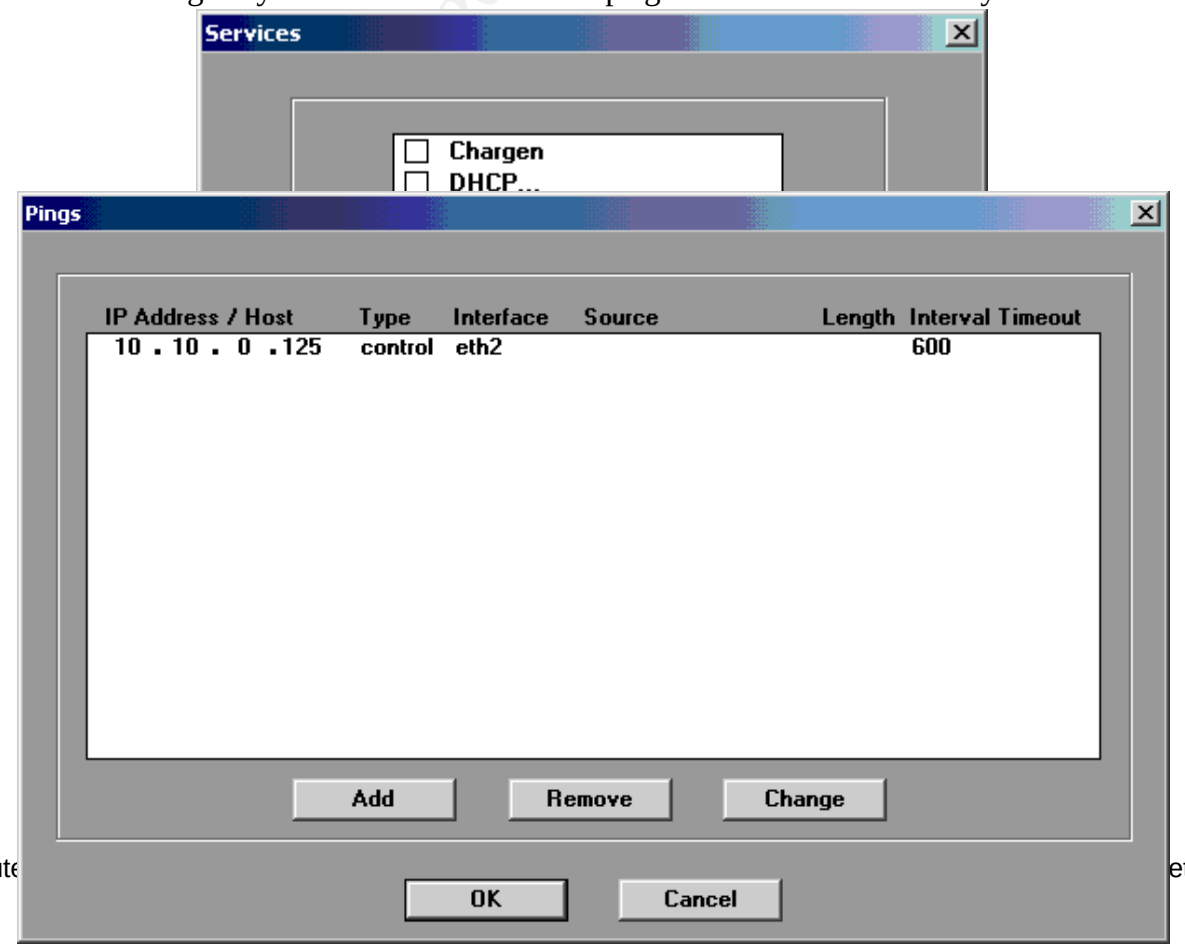


© SANS Institute
etains full rights.

Server Publishing, Static Routes, Rip's..., Pings, Other Settings..., IPX Frame Type (yes it does support IPX!). The Advanced TCP/IP option allows you to view the command line version of the configuration file. You can add entries here but this is kind of like the Windows Registry. If you fumble finger something here it can get quite ugly! The 'Port Mapping' menu option will give you a list similar to what you would see in the services file on a Linux box. As with the Advanced TCP/IP option the information is editable and printable to a file and comes with the same Beware! message. The 'Hosts' option is like the hosts file on a PC and is also editable and printable.

The next option is the 'Services' option and when you click on it you get a screen like the one above. This shows the defaults services that are enabled by default. For our specific configuration example we are going to turn off the DSN Proxy, Ident and SNMP. As you can also see, the Instant Internet supports several services, including a WEB Configuration. This allows you to do configuration via your favorite browser. The next option 'Server Publication' allows you to publish server services out to the Internet if you chose to do so. The 'Static Routes' option allows you to manually configure your routing table if you are not using one of the routing protocols that are supported such as Rip V1 or V2 broadcast and multicast and OSPF (OSPF is considered an 'add on' and requires a key to turn on). The next option 'Rip's...' gives you configuration for the RIP protocol.

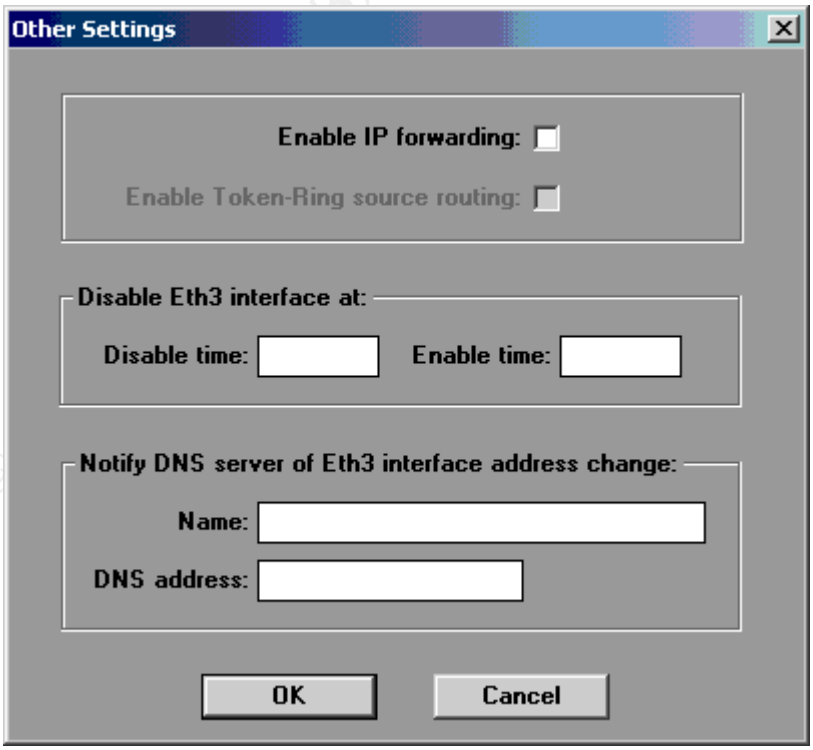
The 'Pings...' option allows you to view, add, remove or change for a particular IP address. This option is use to manage a connection with another device. There are three options for a ping, monitor, control and background. The monitor or control ping can be used to manage any connection. The monitor ping does not count as activity or traffic



© SANS Institute etains full rights.

versus the control ping that does. If you were doing dial on demand routing depending on your needs you would select one of these. We use the control ping in our specific configuration as a 'keep alive' for the tunnel between the Instant Internet box and the Contivity Switch back at the corporate office. As you can see I have added a control ping from this device back to an IP address that is located at the corporate office. It is set for 600 seconds. The monitor ping is used for an IPSEC tunnel. This option checks for the validity of the tunnel. After a number of failed pings the tunnel is destroyed.

The last option 'Other Settings...' looks like the screen below.

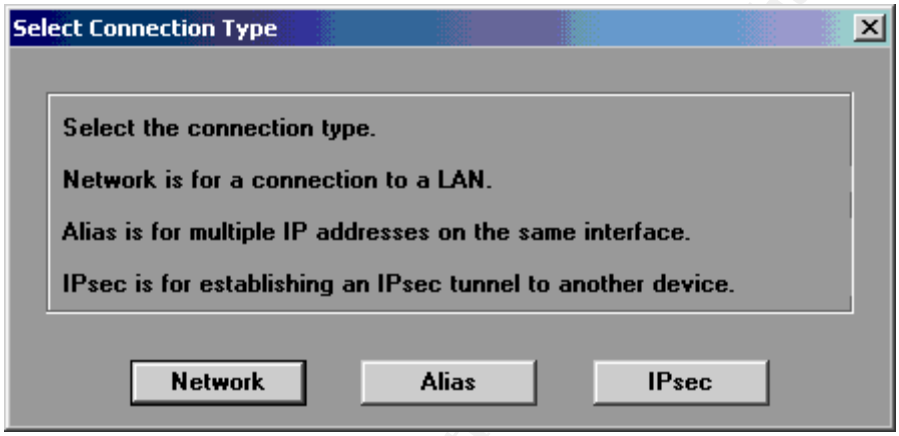


Here you can see there are several options available to you. Enable IP forwarding allows

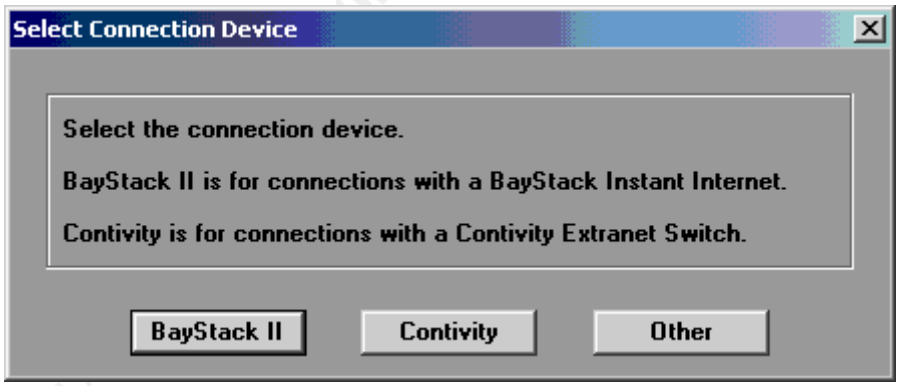
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the Instant Internet to actually route IP traffic with no filtering turned on. This has security issues and needs to be used with caution. On a multiple interface box you can actually use the "Disable Eth3 interface at:' to turn the WAN interface on and off at predetermined times. The last option basically does what it says. If there is a DNS server available that will allow this device to update, this option will allow you to do that.

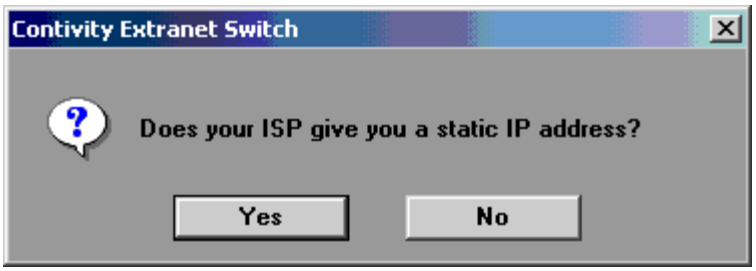
The next step is to build the IPSEC interface that will be the control the tunnel from this box back to the Contivity Switch at the corporate office. To start the process you click on the 'Add' button next to the port list and the configuration utility will prompt you with a screen like the one below.



We select the 'Ipsec' button since we are going to build an IPSEC tunnel.

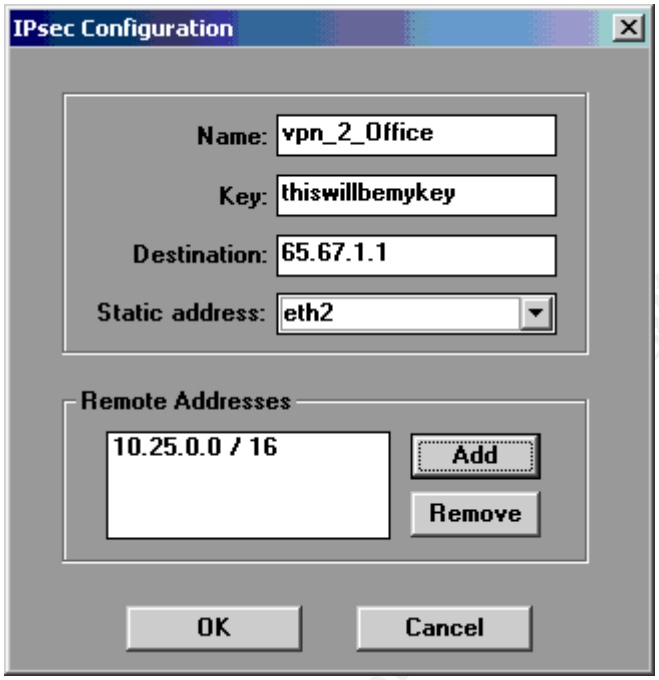


On the next prompt we select the 'Contivity' option since that is the device we will be connecting to at the other end.



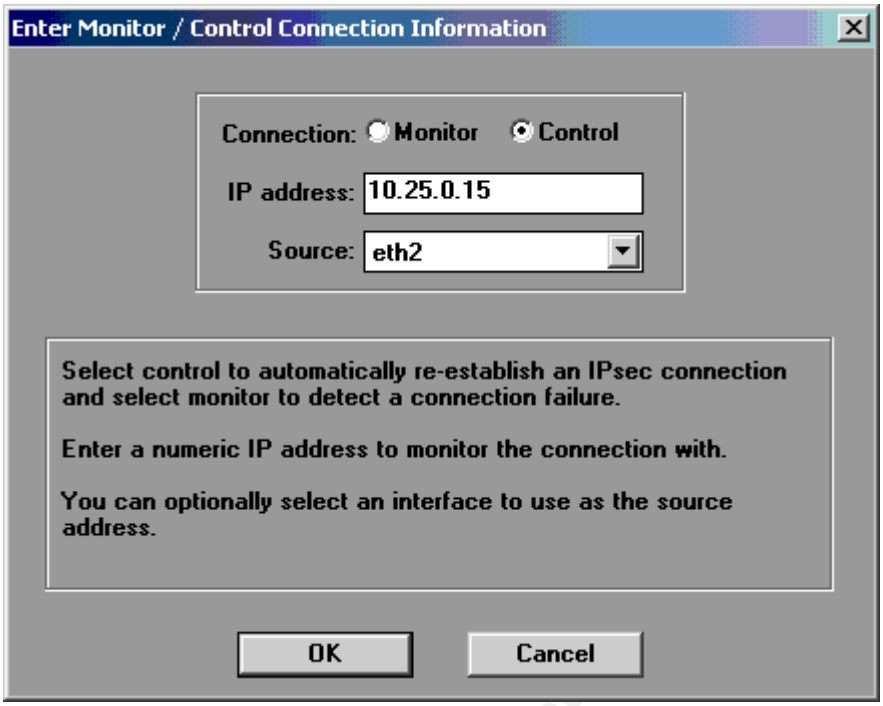
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

It then asks if you ISP provides a static address. We click 'Yes' to confirm that we do have a static IP from our ISP.



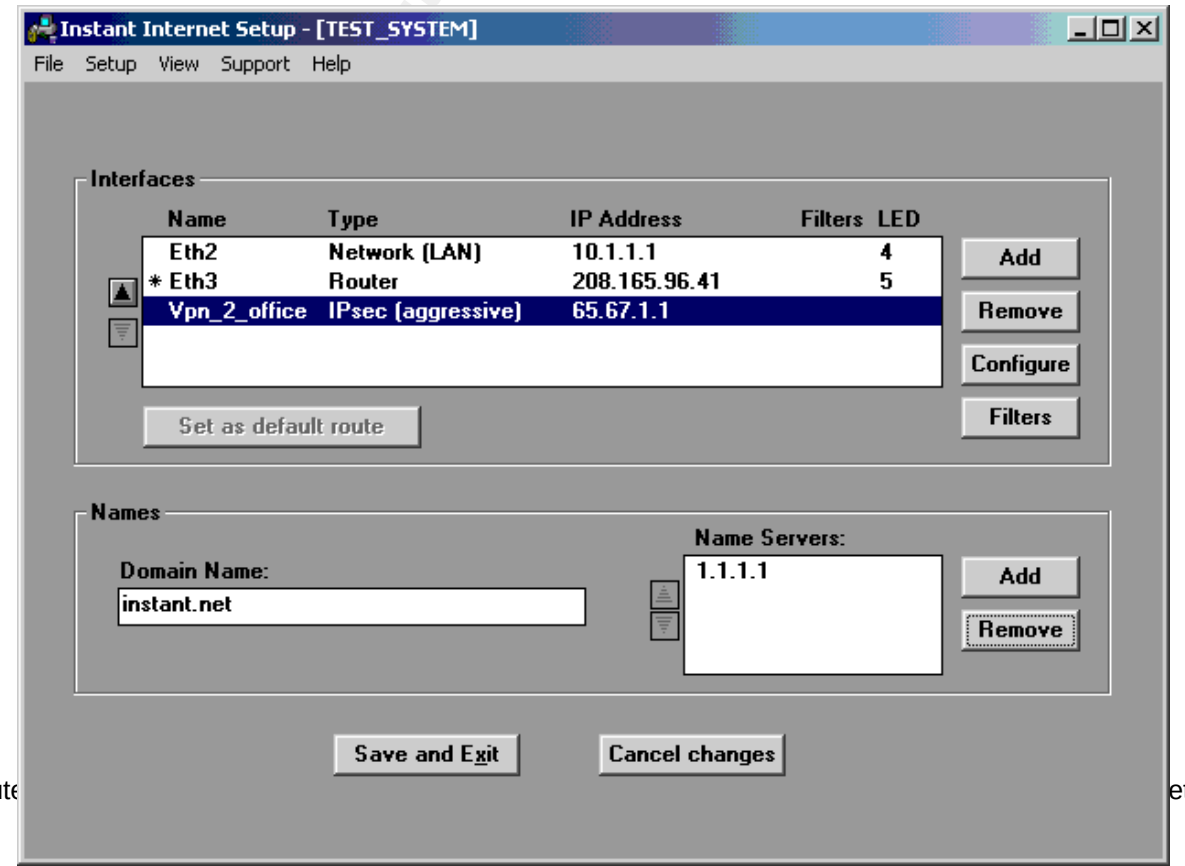
The screen above is the next prompt you get from the configuration utility. I have completed the information that it needs based on my example. The name field is just a description for the IPSEC port that we are creating. The key is the pre-shared key that will be used at both ends of the tunnel for encryption and decryption. The destination is the public endpoint of our tunnel. Using a class A address in this example as the public address of the Contivity Switch. The 'remote addresses' box basically says that we have a private class A address network sitting behind the Contivity at the other end of our VPN tunnel. There can be multiple private subnets available at both ends. The important thing to remember here when doing the configuration is that this information has to match exactly at both ends or the VPN connection will not come up. <u>This includes the bit masking on the subnets</u>.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



The last bit of information to include in your IPSEC configuration is adding a 'ping'. I have added a 'control' ping as a 'keep-alive' and the address of a device located at the corporate end of the tunnel. Once you have completed this information you are back at the main window as below.

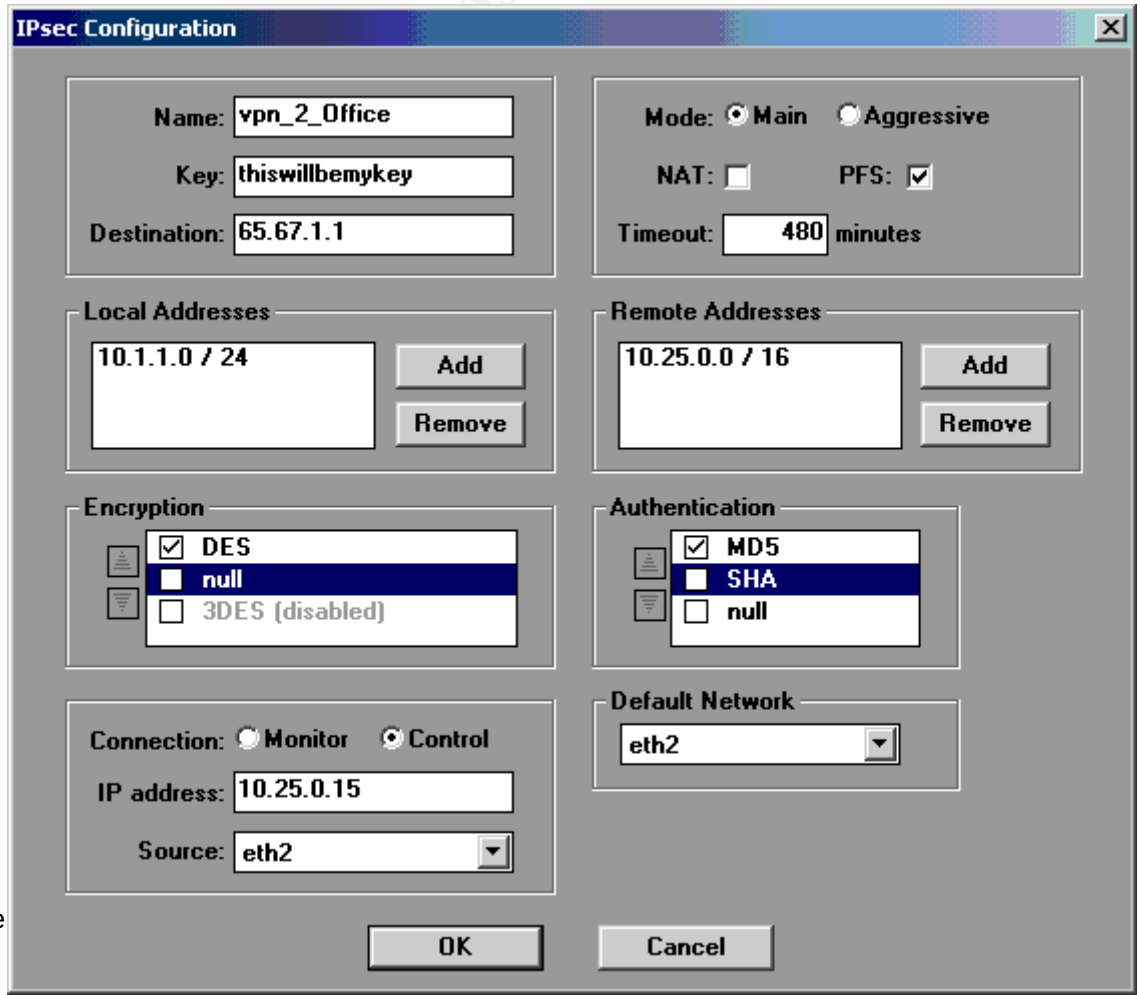
As you can see from the screen shot above, we now have a new interface in our lists. We click on configure to complete the configuration of the IPSEC interface.



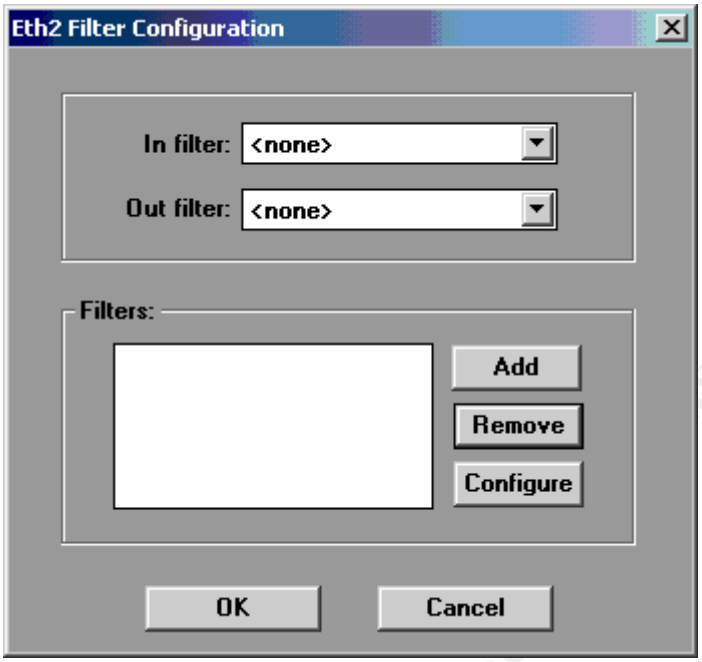
© SANS Institute etains full rights.

Here is the summary screen of our IPSEC interface above. I t is important to restate that the information here must match our setup on the Contivity Switch or the tunnel will refuse to come up, so let's review. The name again is just a description. The key is the 'pre-shared' key that will be used by both devices. The Destination is the public address at the other end of the VPN tunnel. I am using the 'Main' mode and PFS (perfect forward secrecy) and my rekey time reflects the default of the device of 8 hours. You can change this to fit your environment making sure that they are the same on both ends. Next is the private addressing on both ends of the tunnel which again must match up with what is reflected in the configuration at the other end including the bit masking. I have selected DES for the encryption and unchecked the 'null' box which is turned on by default. As you can see 3DES is grayed out because it is not available by default. Under Authentication I have selected MD5 and unchecked 'SHA' and 'null' We have a Control ping in place for a 'keep-alive'.

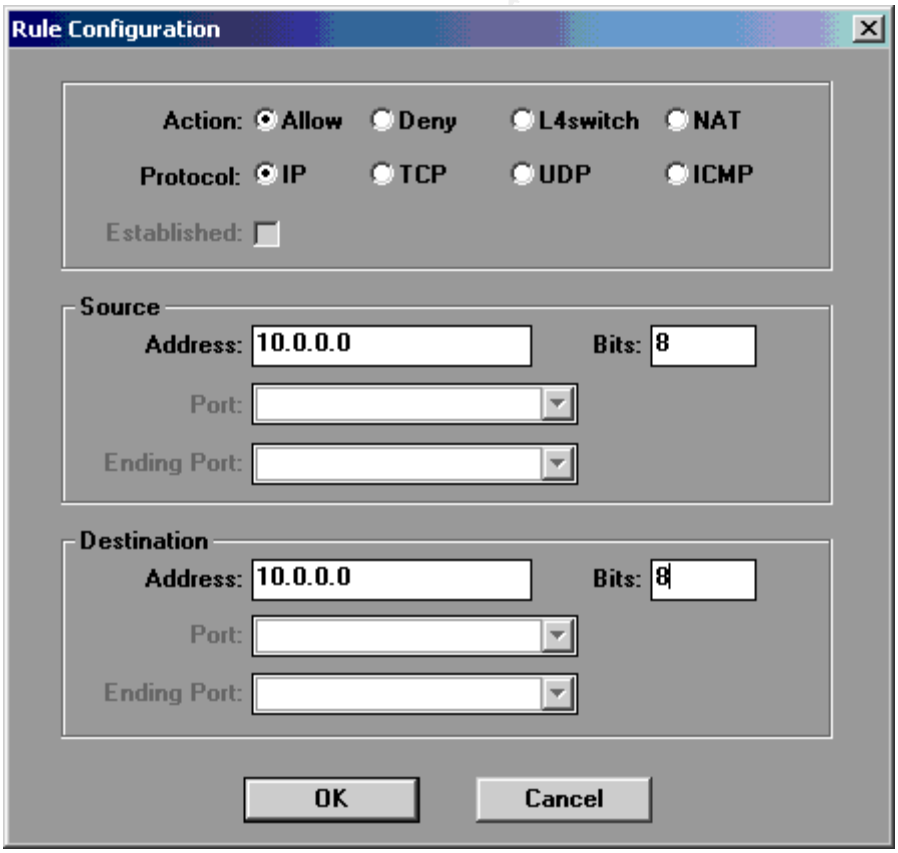
The last part of configuring the Instant Internet 100-S will be to add a filter for the tunnel. I select the internal LAN interface and click on filters.



© SANS Institute 2003, Author retains full rights.

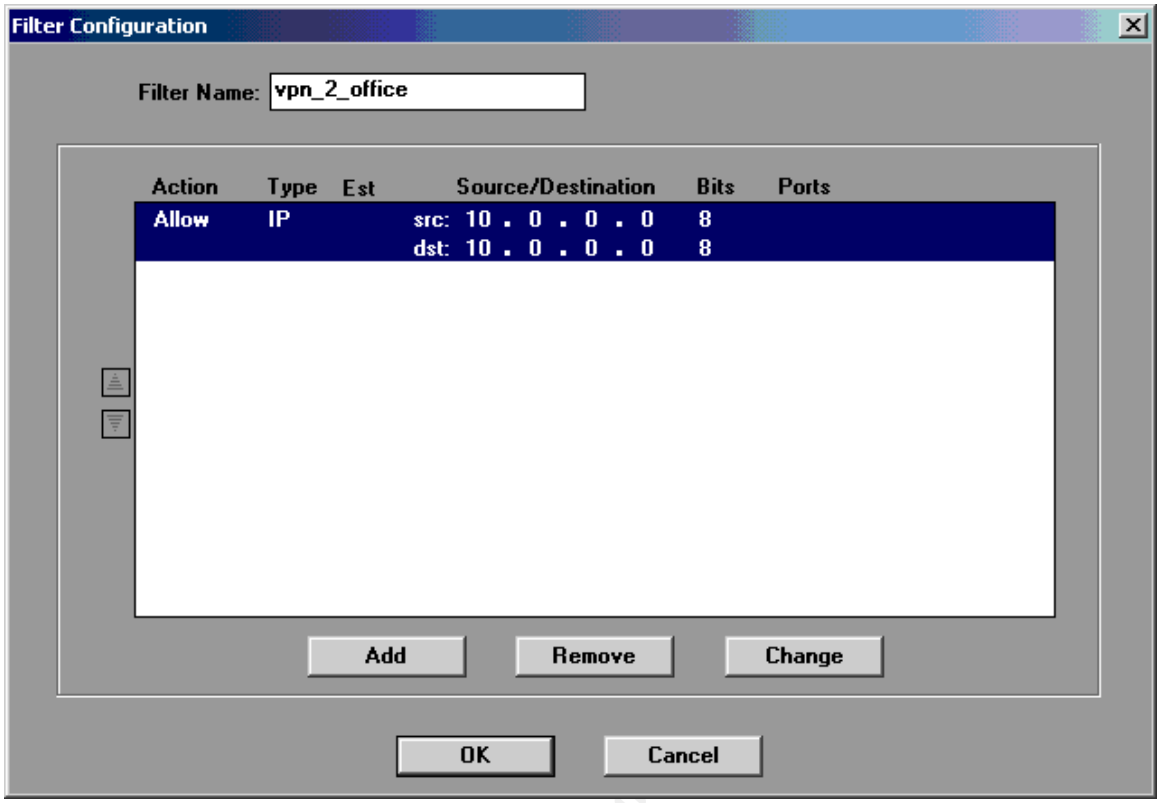


From here I click on the 'Add' button to get the next screen.

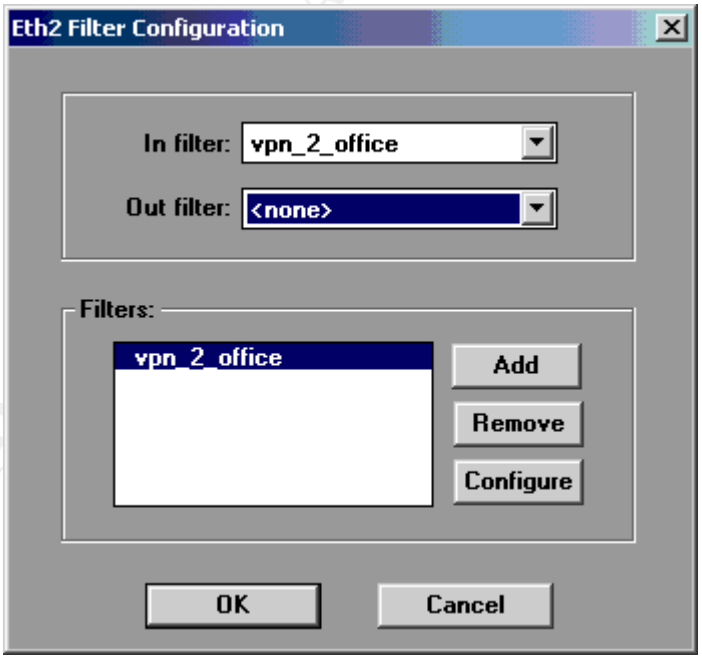


I call my filter 'vpn_2_office' which is just a description. I then fill out the information as above. This basically says that any traffic on class 'A' network is allowed and everything else is denied. Once you click OK you will see the screen like the one below.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

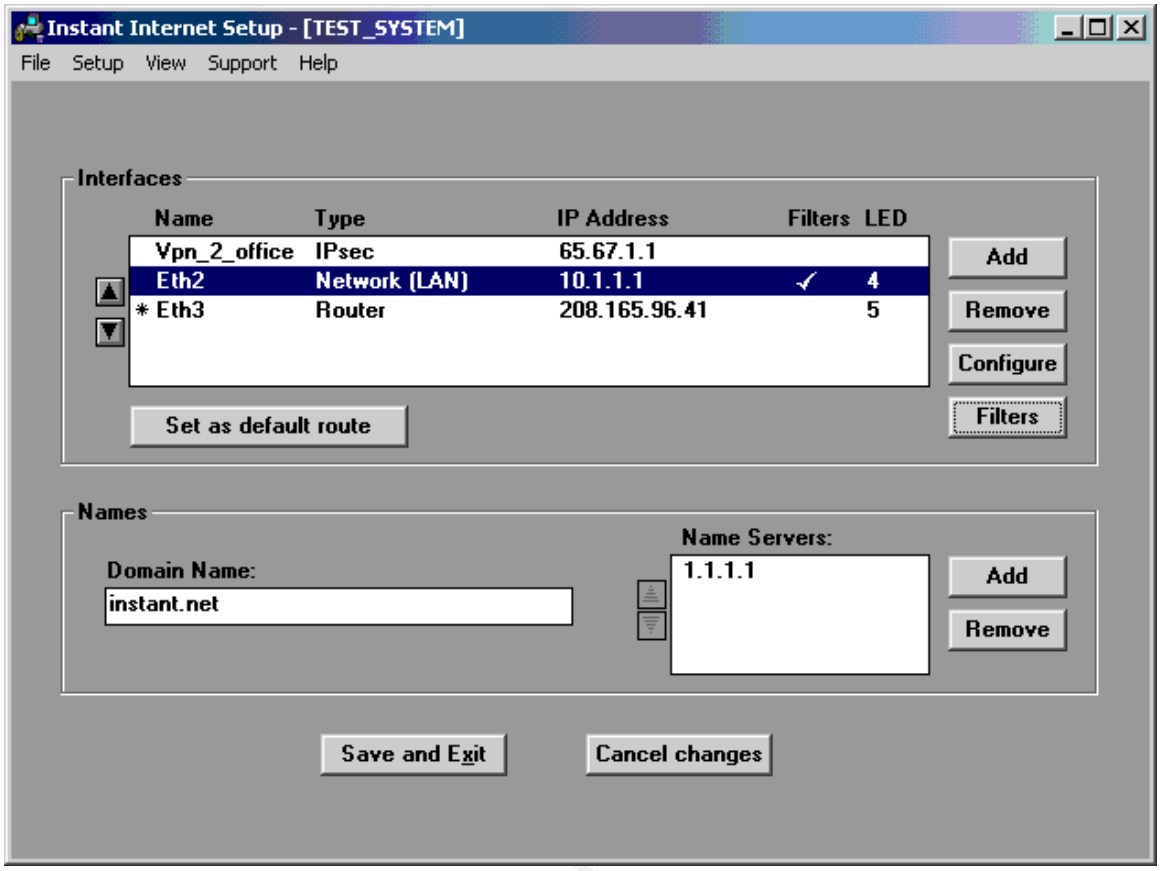


Once you click OK you will have a screen like the one below.



Here I have selected the filter as an 'in' filter which will be located on the LAN interface of my Instant Internet 100-S and click OK to complete (the interface is shown in the title bar and was selected when we started).

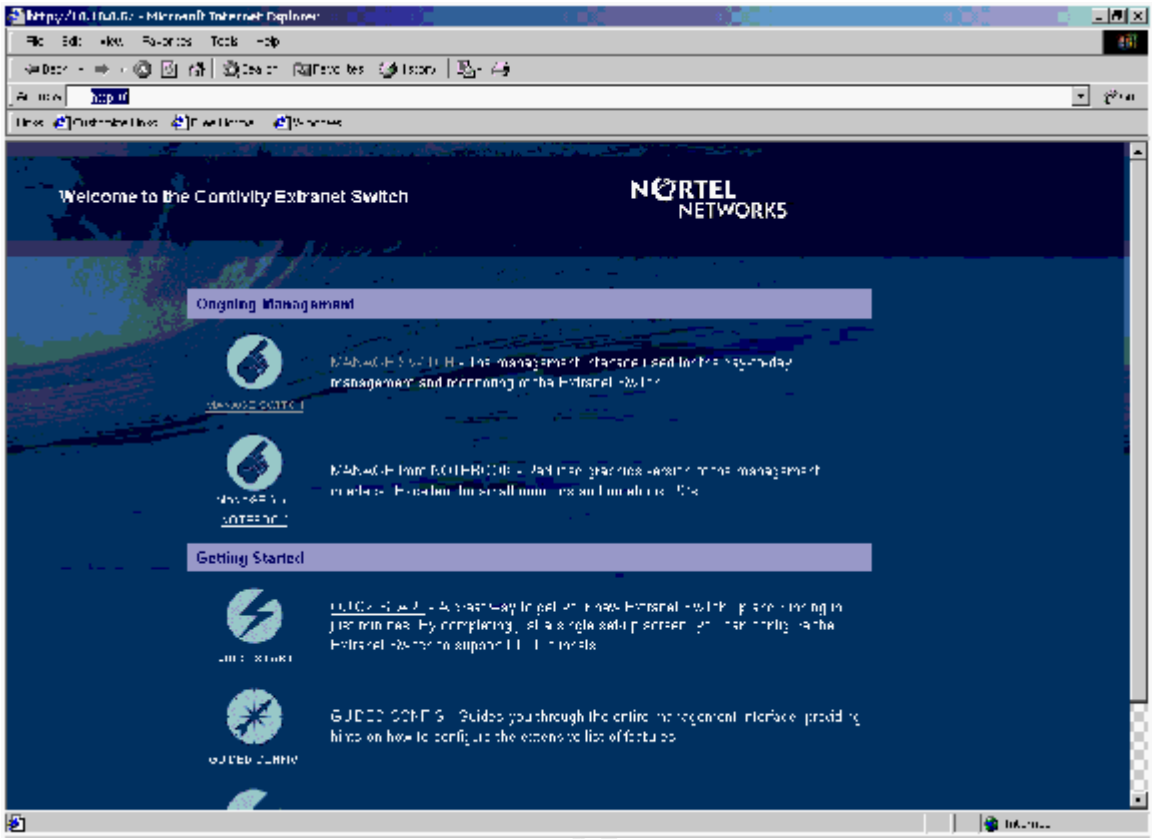
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



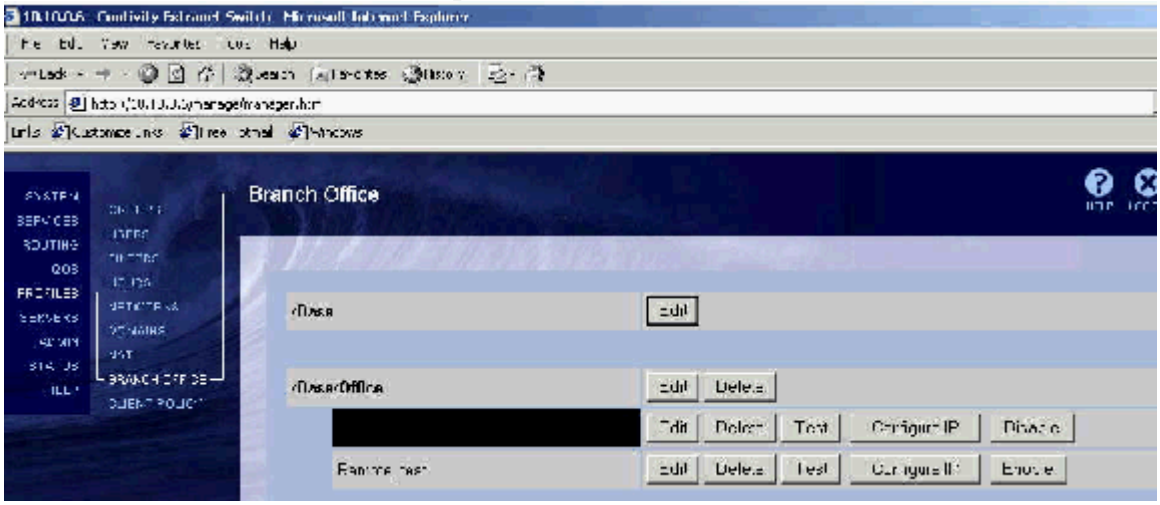
Now that we have completed the filter you can see there is a check mark in the 'Filters' column of the Eth2 interface. The last step in the configuration is to select 'Save and Exit' so that the changes can be applied to the device. It is also important to note that on the back of the Instant Internet 100-S there is a set of eight dip switches. If you have problems with the configuration and want to start from scratch or you forget the password to get back into the box you can use these to return the device back to it's factory defaults. To do this you would power the device off. Set all the dip switches to the down position, place number four and number eight in the up position and turn the device on. If you watch the LED's on the front during the boot up process they will all turn an orange color with the exception of the four and eight positions. Once this happens it is your visual cue that the box has reset itself. You can then power down, place all the dip switches back in the up position, power on and your ready to go!

Now we are going to configure the Contivity Switch with a Branch Office connection to mirror the information on this box. The Contivity also has a web interface that the configuration is done from once it is up and going.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



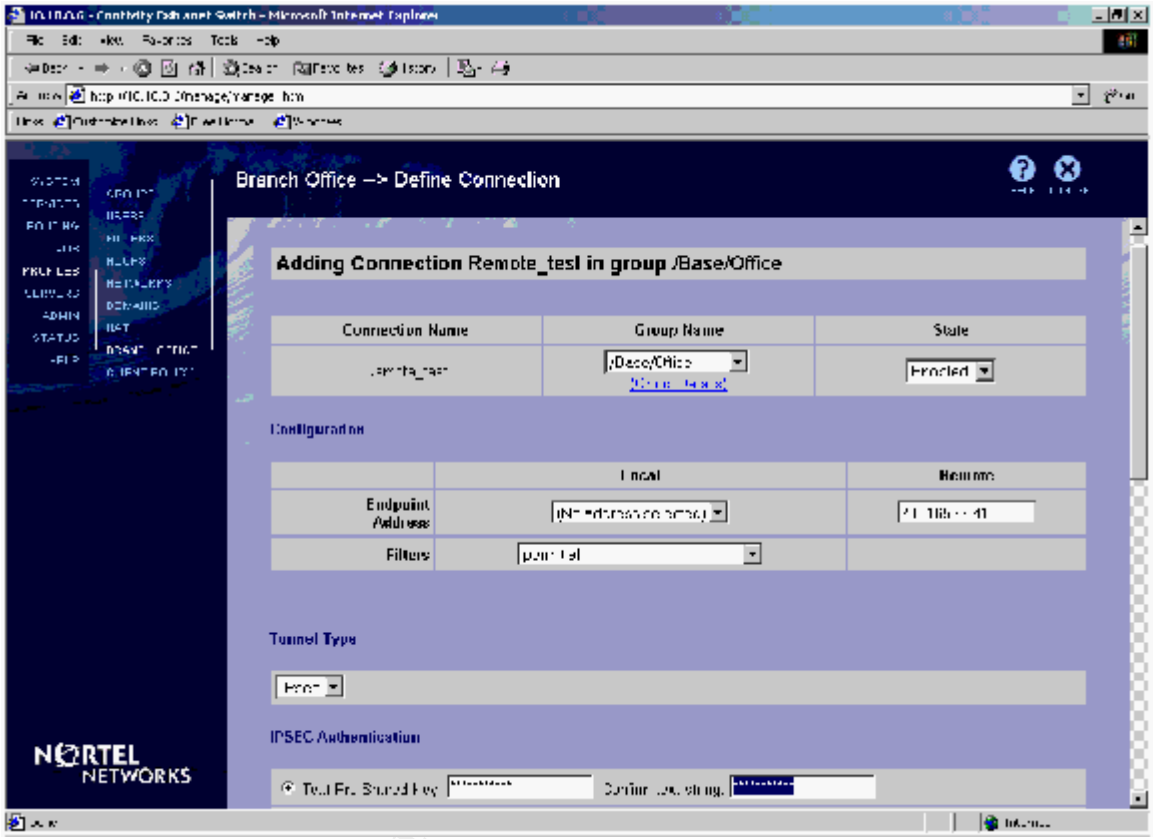
Once you connect to the Contivity you click on the 'Manage Switch' link that is listed as the first link on the page. You do your normal user name and password authentication and it will then load the main configuration screen shown below.



Here we are looking at the Profiles->Branch Office page. From here we can 'Define a Branch Office Connection', Edit, Delete, Test, Configure IP and Enable/Disable a connection.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

You can create groups to manage users and Branch Office connections from. This allows a lot of flexibility in configuring users or Branch Office connections. Examples of things you can control by groups are; when they can connect, where they can go (accessible networks), how they can connect (i.e. PPTP, LTP, IPSEC). Once you create a Branch Office connection there are just a few settings that must be done in my environment to get us up and running.



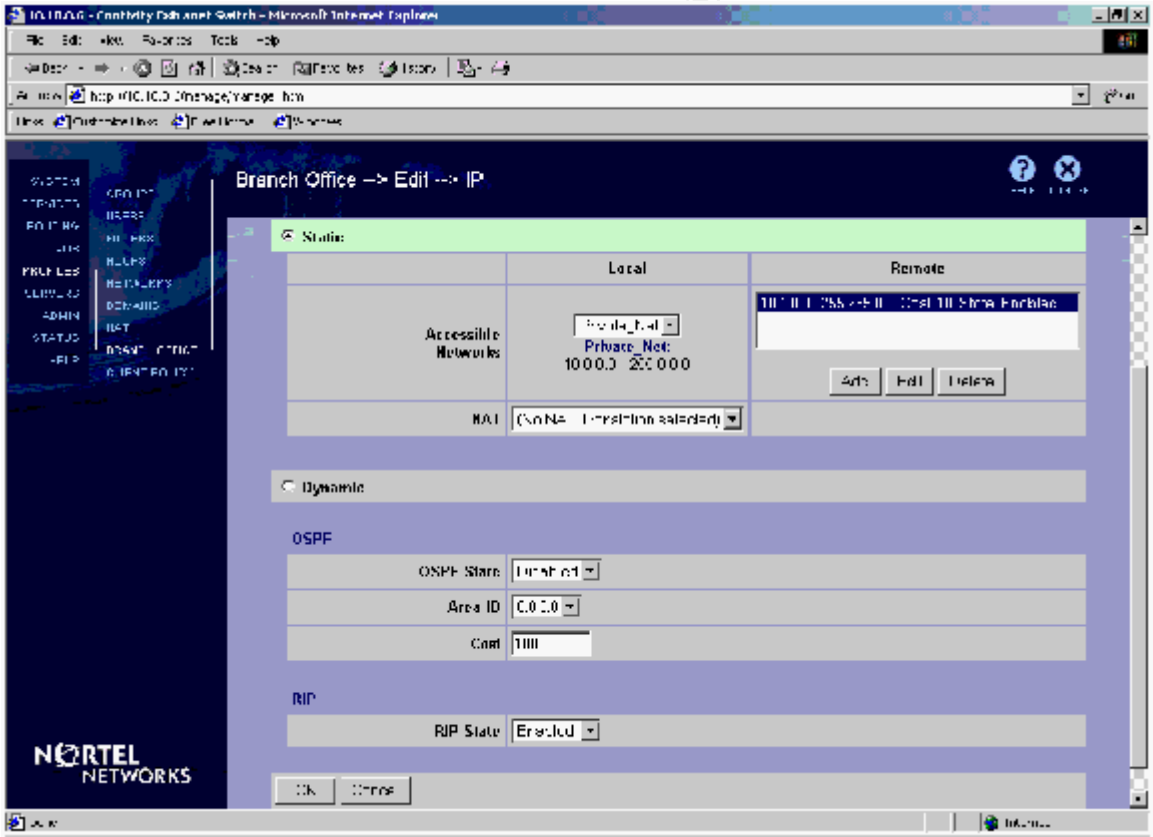
The screen shot above is the first set of options to configure once you create the Branch Office connection. Here we find the 'Group Name' the connection belongs to, the 'State' of the connection (enabled/disabled), the 'Local Endpoint' and 'Remote Endpoint' (the public addresses of the vpn tunnel), Filters, Tunnel Type (IPSEC, PPTP and L2TP), and IPSEC Authentication, which we have chosen the pre-shared key.

At the bottom of the screen you click on the 'Continue' button to arrive at the second configuration screen which looks like the one below.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As you can see your options are 'Static' or Dynamic for routing. Under dynamic you can turn on Rip but if you wanted to use OSPF you would have to purchase a 'Key' from your vendor. We have chosen the 'Static' option and have selected the local network that I have defined under 'Networks' as 'Private'. I have also added a 'Remote' network of the Instant Internet 100-S which was the 10.1.1.0/24 subnet range. Again I must emphasis that if you have multiple networks listed here for both devices they must be exact including the bit masking or your connection will refuse to come up, I speak to this from experience! Once you have completed this screen and click the 'OK' button your are done. If you have the device up and running at the other end you can actually use the 'Test' option to see if you have done everything right. It will attempt to make a connection and display a 'results' window based on a 'success' or 'failure' and allow you to view the logs if there was a problem to help and trouble shoot.

The Contivity Switch obviously has a lot more to it that I have mentioned here. There is some setup to do to get it up and running but it is not that intense as far as the basics. It can provide a tremendous amount of services including DHCP, LDAP, RADIUS, NAT,



supports PKI, and has a nice firewall product (version 3.5 or higher) that can be turned on with a 'Key' that can be purchased from your vendor. Again with the dual ethernet models I have one sitting behind a DSL connection in one location and one sitting behind a Frame T1 in another location with a tunnel up between them and it is very fast!

Based on my personal experience with these devices I would highly recommend looking at them as a option if you are needing to deploy VPN technology in your business

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

environment. Since we are mostly pushing just pizza delivery orders over our connections we have not incorporated the higher encryption or taken advantage of the PKI technology, but if our needs change it is nice to know that these services are available.

References:

1. Network World "Nortel to snap up Baynetworks" Author, Jim Duffy
URL: http://www.nwfusion.com/news/0515nortel.html

2. Nortel Networks 'End of Life Notification'
URL: http://nortelnetworks.com/products/announcements/baystackii/

Nortelnetworks.com Documentation Library
URL: http://www.nortelnetworks.com/products/01/cpe/ii100/index.html

Instant Internet 100-S Product Description
URL: http://www.cmssoft.co.uk/instant/instant.htm

Baynetworks Instant Internet 100 User's Guide PDF
URL: http://www.charter.ca/Nortel_solutions/PDF/BayStack/300866F.PDF

Nortelnetworks.com Product Direction:
URL:
http://www.nortelnetworks.com/products/01/contivity/collateral/contivity_ii_trans.pdf

Contivity Switch 1500 Product Overview
URL: http://www.activator-uk.net/home/index.htm?http://www.activator-uk.net/products/nortel/contivity/1500/index.htm

Request for Comments 1918 on Private Addressing
URL: ftp://ftp.isi.edu/in-notes/rfc1918.txt

Acrobat Reader Download Link:
URL: http://www.adobe.com/products/acrobat/readstep2.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**