

Establishing a VPN tunnel between Linksys BEFSX41 and SSH Sentinel

1. Introduction

This document provides a reference application on how to configure a Linksys BEFSX41 as a VPN server and how to use SSH Sentinel as software VPN client to establish a VPN tunnel. The two system topologies used in this document are summarized as followed.

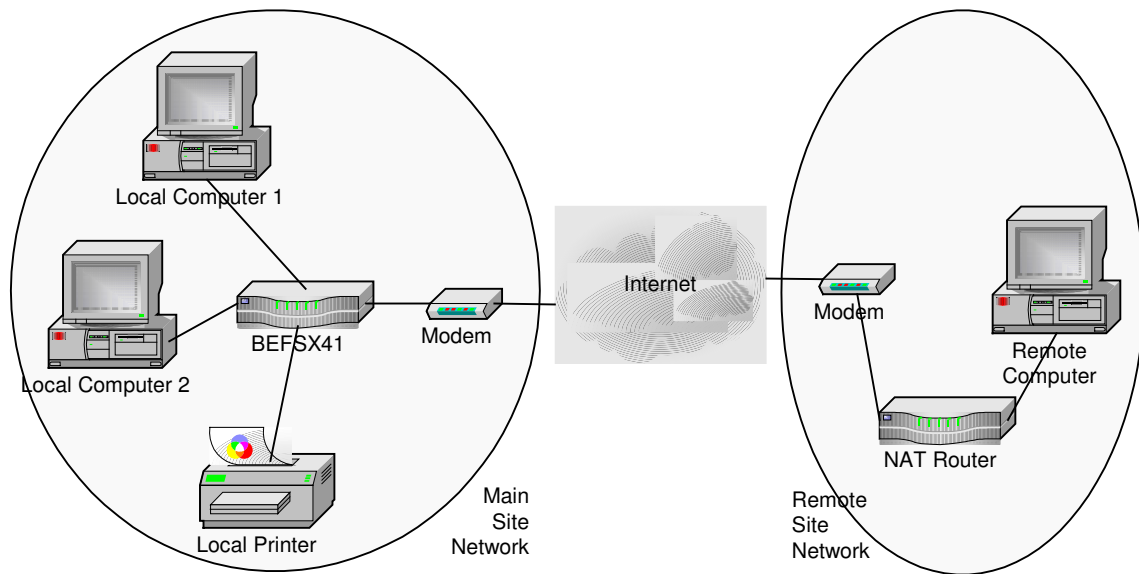


Figure 1 Remote Site Using a NAT Router

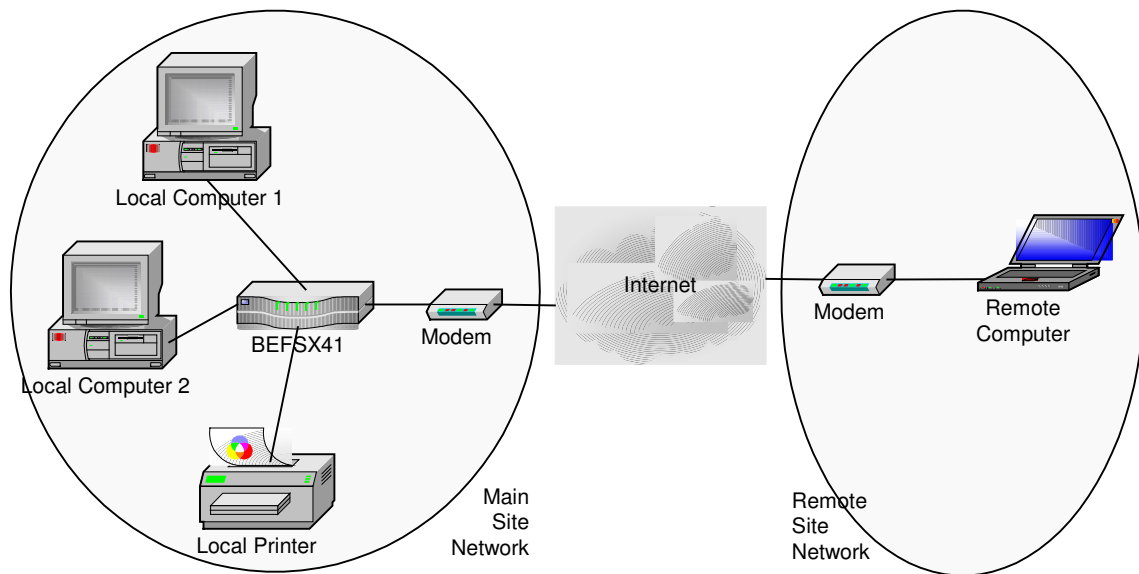


Figure 2 Remote Site Directly to a Modem

Note that in the above figures, a Linksys BEFVP41 can easily replace the Linksys BEFSX41 without any changes to the SSH Sentinel client. Additionally, for the purpose of the experiment, the remote NAT router was another BEFSX41 just because of availability. Any NAT router supporting IPsec pass through (i.e. Linksys BEFSR41) is adequate for this configuration.

The following sections describe the how to configure the Linksys BEFSX41 as a VPN server, the Linksys BEFSX41 as a remote NAT router passing through VPN traffic and the SSH Sentinel as a remote software VPN client. This document assumes that proper software and hardware installation were completed prior getting into configuration of the VPN tunnel.

Finally, and probably most importantly, this experiment is based on the following version of the BEFSX41 and SSH Sentinel.

- Linksys BEFSX41 firmware 1.45.7
- SSH Sentinel version 1.3.2 (build 2)

2. Setting up the Linksys BEFSX41 as a VPN server

There are two steps in configuring the BEFSX41 as a VPN server. The first step involves creating the VPN end-point as a server and the second step is about fine-tuning the metrics of the VPN end-point.

2.1 Creating the VPN End-Point as a Server

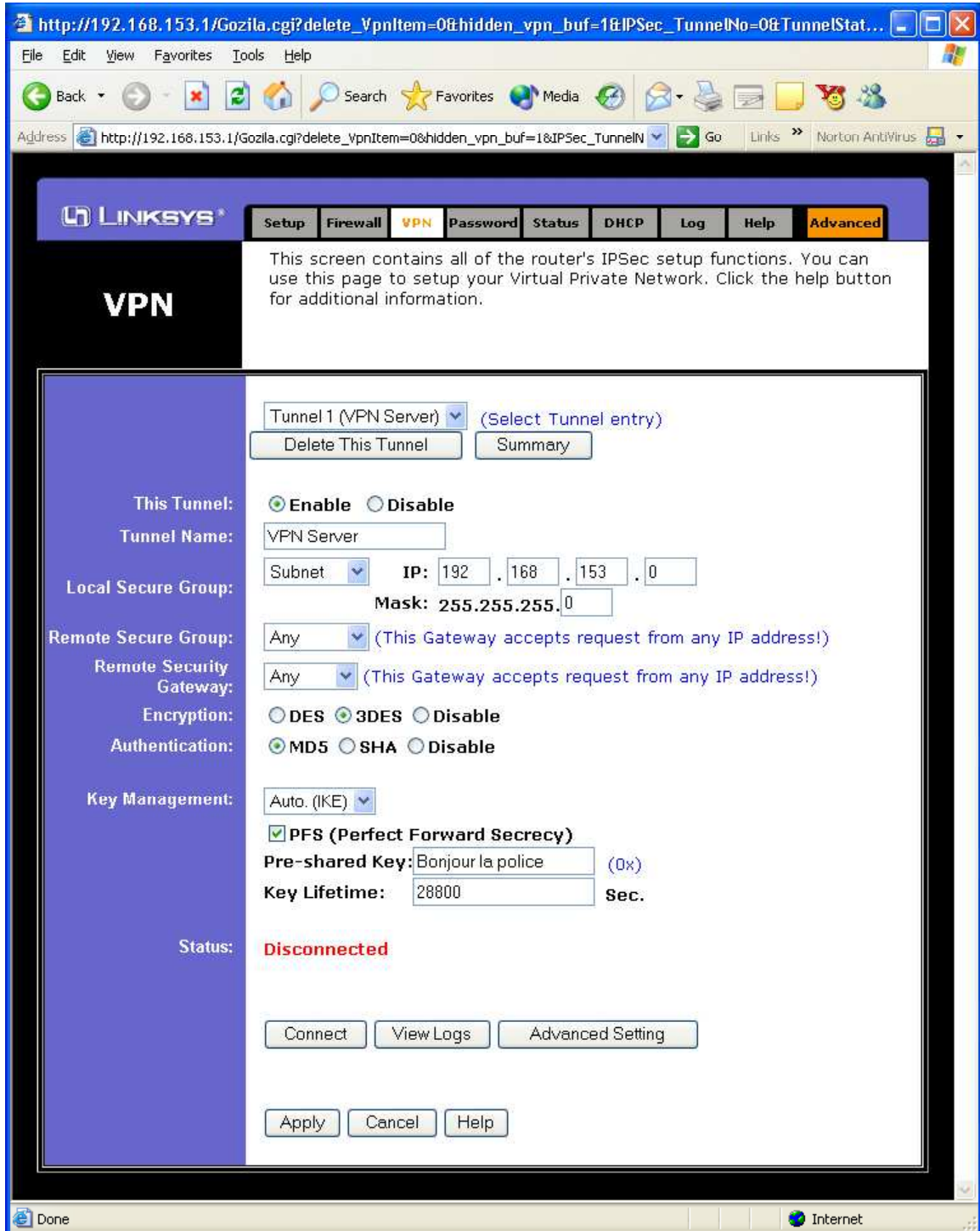


Figure 3 Creating a VPN End-Point Server

- a. Open the BEFSX41 configuration web page and click on “VPN” tab.
- b. Click on the “Enable” radio button of the “This Tunnel” field.
- c. Give your VPN tunnel a name in the “Tunnel Name” field.
- d. As a “Local Secure Group”, select “Subnet” and specify the BEFSX41 LAN subnet. Here, 192.168.153.0 was used in this example but anything goes. This should actually match to your subnet settings in the “Setup” tab.
- e. Select “Any” for the “Remote Secure Group”. This allows the client local IP (LAN) address to be anything.
- f. Select “Any” for the “Remote Security Gateway”. This allows the client Internet wide IP (WAN) address to be anything.
- g. The best “Encryption” algorithm supported by the BEFSX41 is triple-DES (3DES). Click in the “3DES” radio button.
- h. In the “Authentication” field, click in the “MD5” radio button.
- i. In the “Key Management” section, select “Auto. (IKE)”, put a checkmark in the “PFS (Perfect Forward Secrecy)” box, type in your favorite secret string in the “Pre-shared Key” field and set the “Key Lifetime” to 28800 seconds.
- j. Click on the “Apply” button. When be prompted, click on the “Continue” button.

This completes the creation of the VPN end-point on the Linksys BEFSX41. You are now ready to fine-tune your end-point.

2.2 Fine Tuning the VPN End-Point

IPSec Advance Setting - Microsoft Internet Explorer

Advanced Settings for Selected IPsec Tunnel

Tunnel 1

Phase 1:

Operation mode : Main mode
 Aggressive mode Username:

Proposal 1:

Encryption : 3DES
Authentication : MD5
Group : 1024-bit
Key Lifetime : 28800 seconds

(Note: Following three additional proposals are also proposed in Main mode:
DES/MD5/768, 3DES/SHA/1024 and 3DES/MD5/1024.)

Phase 2:

Proposal :

Encryption : 3DES
Authentication : MD5
PFS : ON
Group : 1024-bit
Key Lifetime : 28800 seconds

Other Options:

NetBIOS broadcast
 Anti-replay
 Keep-Alive
 If IKE failed more than 5 times, block this unauthorized IP for 60 seconds

Apply Cancel

Figure 4 Fine Tuning the VPN End-Point

- a. Once brought back to the “VPN” tab of the router configuration web page, click on the “Advanced Setting” button.
- b. Select the “Main mode” of the “Operation mode” field.
- c. Select the “Encryption” algorithm of “Proposal 1” to “3DES”.
- d. Select the “Authentication” algorithm of “Proposal 1” to “MD5”.
- e. Select the “Group” size of the “Proposal 1” to “1024-bit”.
- f. Configure the “Key Lifetime” of the “Proposal 1” to 28800 seconds.
- g. Select the “Group” size of the phase 2 “Proposal” to “1024-bit”.
- h. Configure the “Key Lifetime” of the phase 2 “Proposal” to 28800 seconds.
- i. Put a checkmark in the “NetBIOS broadcast” box. This allows you to use Windows Network Neighbourhood to share files and printers. Pretty handy if most of your PC are running a Windows-based OS.
- j. Put a checkmark in the “Anti-replay” box.
- k. Put a checkmark in the “Keep-Alive” box.
- l. Ensure no checkmark is in the last box.
- m. Click on the “Apply” button. When be prompted, click on the “Continue” button. You may then close this extra window.

Congratulation, you have successfully configured your BEFSX41 as a VPN server. That was the easy part ;).

3. Setting up the Linksys BEFSX41 as a NAT router

If you have chosen the topology of Figure 2, you may skip this section. Otherwise, read on. This section describes how to configure your remote NAT router as IPSec pass through.

Note that configuring a NAT router as IPSec pass through differ from one model to the other. This section illustrates, as an example, how to do this using a Linksys BEFSX41.

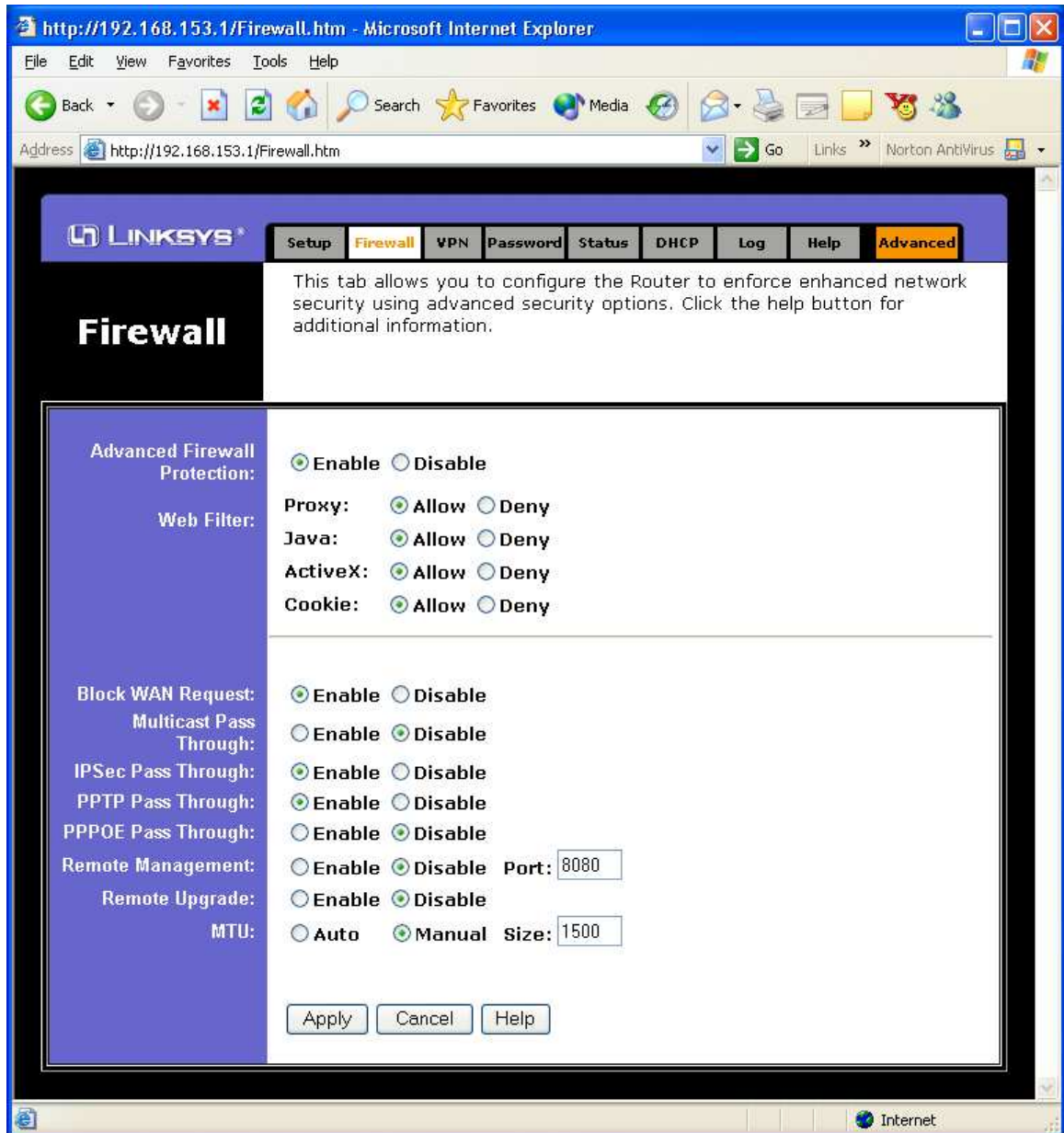


Figure 5 Configuring a BEFSX41 with IPSec Pass through

- a. Open the BEFSX41 configuration web page and click on the “Firewall” tab.
- b. This page contains multiple fields. Really, the only one that matters is the “IPSec Pass Through” radio button that you must check to “Enable”. As for the other options, those are beyond the scope of this document and Figure 5 only shows an example.
- c. Click on the “Apply” button. When be prompted, click on the “Continue” button.

This router may now allow VPN traffic passing through.

4. Setting up the SSH Sentinel software VPN client

The SSH Sentinel software is configured in two steps. The first one involves the creation of a key management and the second one is the actual VPN security policy. The instructions below are assuming that SSH Sentinel has already been installed and that the policy manager is already running.

4.1 Launching the SSH Sentinel Policy Editor

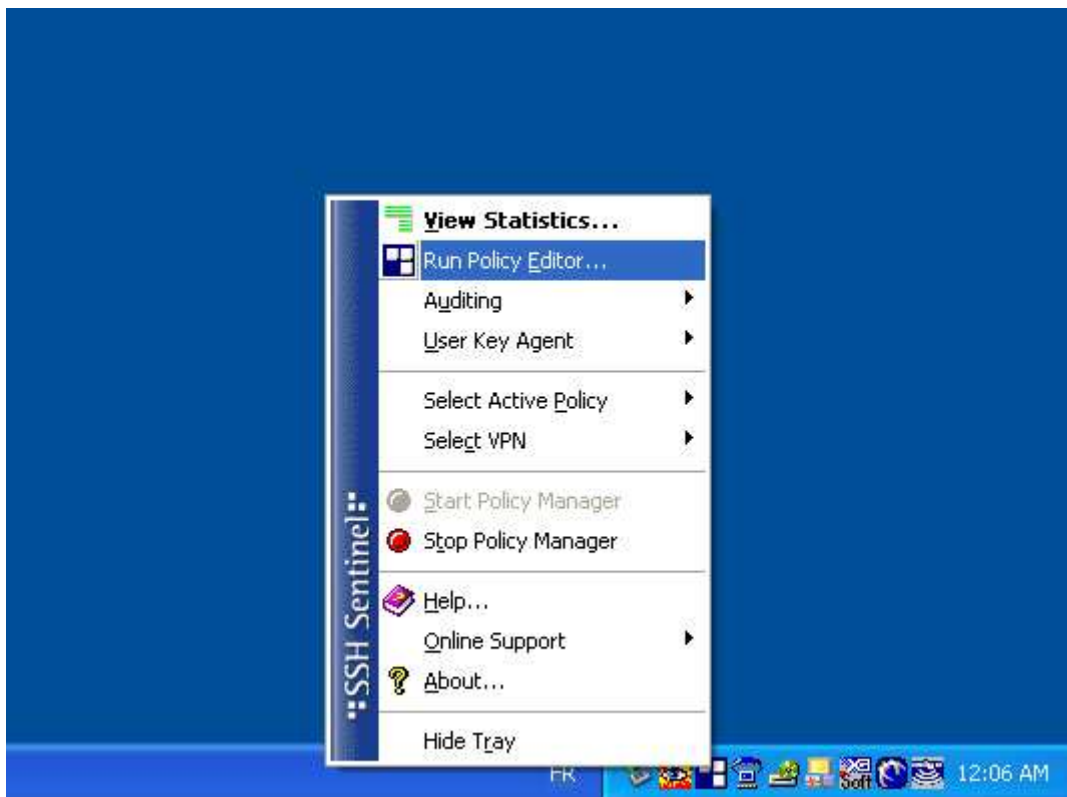


Figure 6 Launching the SSH Sentinel Policy Editor

- a. To start the SSH Sentinel policy editor, right click on the SSH Sentinel icon in the task bar.

4.2 Setting up the SSH Sentinel Key Management

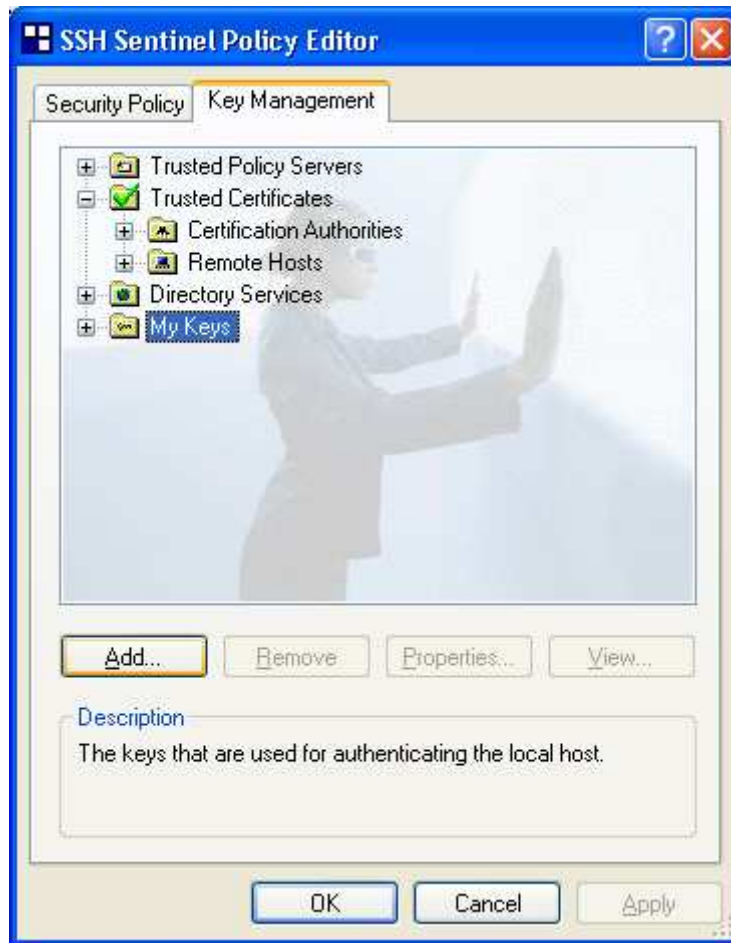


Figure 7 Adding a New Key

- a. From the SSH Sentinel policy editor, click on “Key Management” tab.
- b. Then select the “My Keys” item from the tree.
- c. Click the “Add...” button.

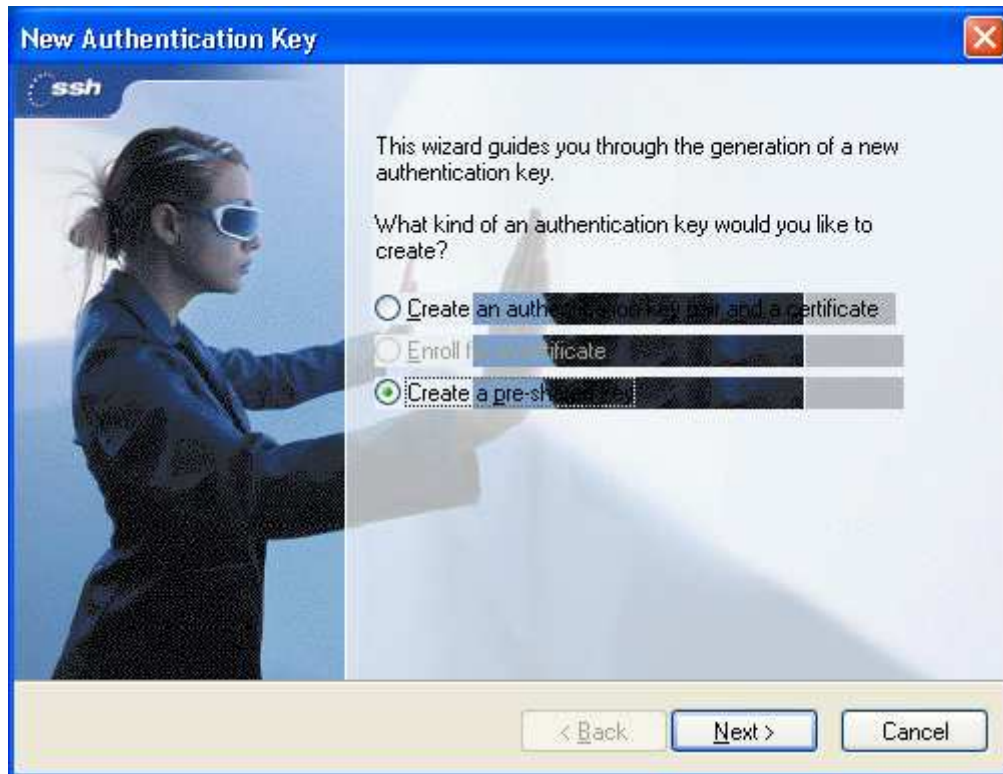


Figure 8 Creating a Pre-Shared Key

- d. From the “New Authentication Key” dialog, select the “Create a pre-shared key” radio button.
- e. Click the “Next >” button.

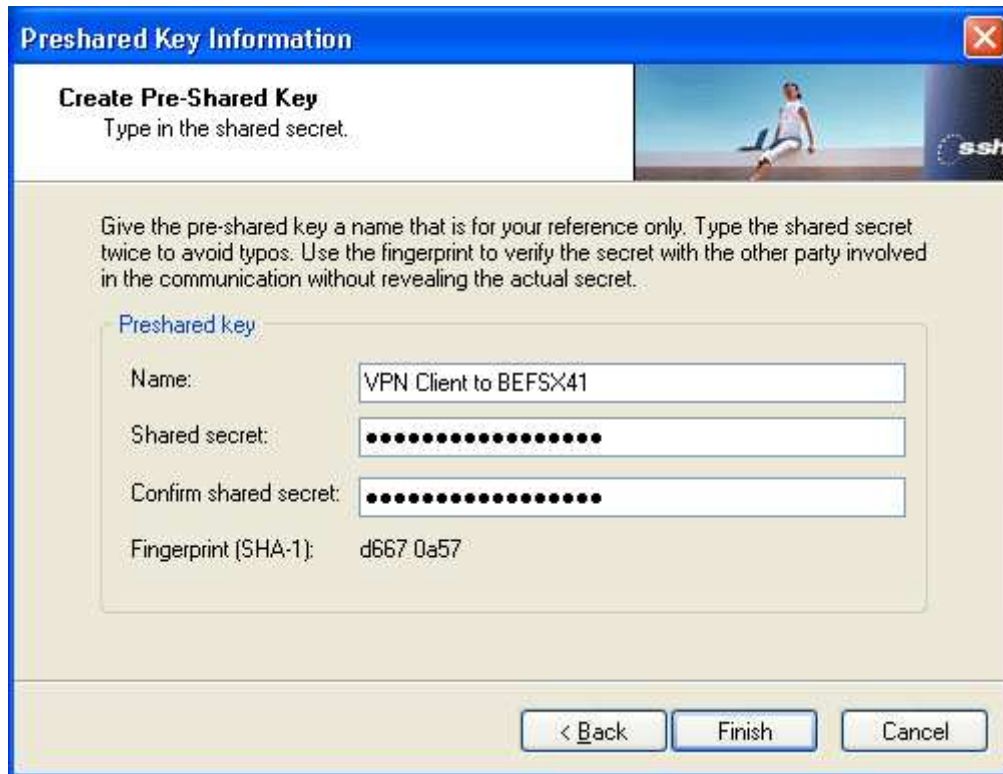


Figure 9 Entering Pre-shared Key Information

- f. From the “Pre-shared Key Information” dialog, enter the name of your choice in the “Name” field.
- g. Type in the exact same “Shared secret” as you did on the BEFSX41. The example in section 2.1, step i was using “Bonjour la police”.
- h. Retype the very same password in “Confirm shared secret” field.
- i. Click on the “Finish” button.

4.3 Setting up the SSH Sentinel Security Policy

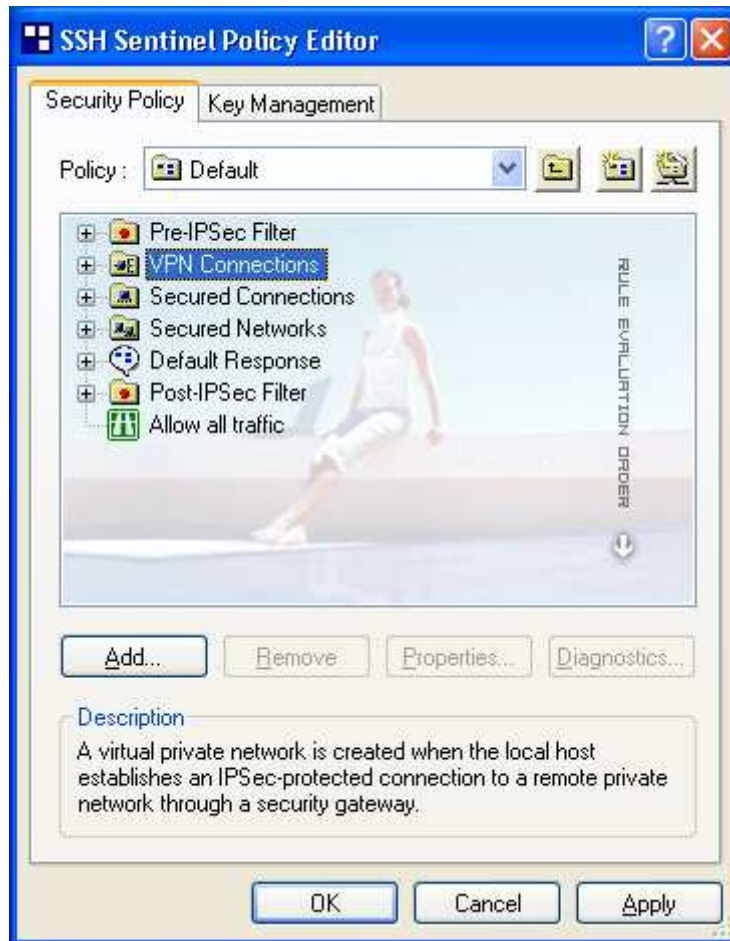


Figure 10 Adding a new VPN connection

- From the SSH Sentinel policy editor, click on “Security Policy” tab.
- Then select the “VPN Connections” item from the tree.
- Click the “Add...” button.



Figure 11 Add VPN Connection

- d. In the “Gateway name” field, type in the domain name that matches with the BEFSX41 WAN IP address. This is an FQDN (Fully Qualified Domain Name) value that can either be mapped to a fixed IP address or to a dynamic IP address such as the one managed by www.DynDNS.org (which by the way the BEFSX41 support a built-in DDNS client). If you do not wish to use a FQDN value, you could always click on the “IP” micro button to switch to a dotted notation IP address. Then you can type in your static IP address.
- e. In the “Remote network” field, click on the “...” micro button to create yourself a specific remote network information. Then the “Network Editor” dialog will popup.

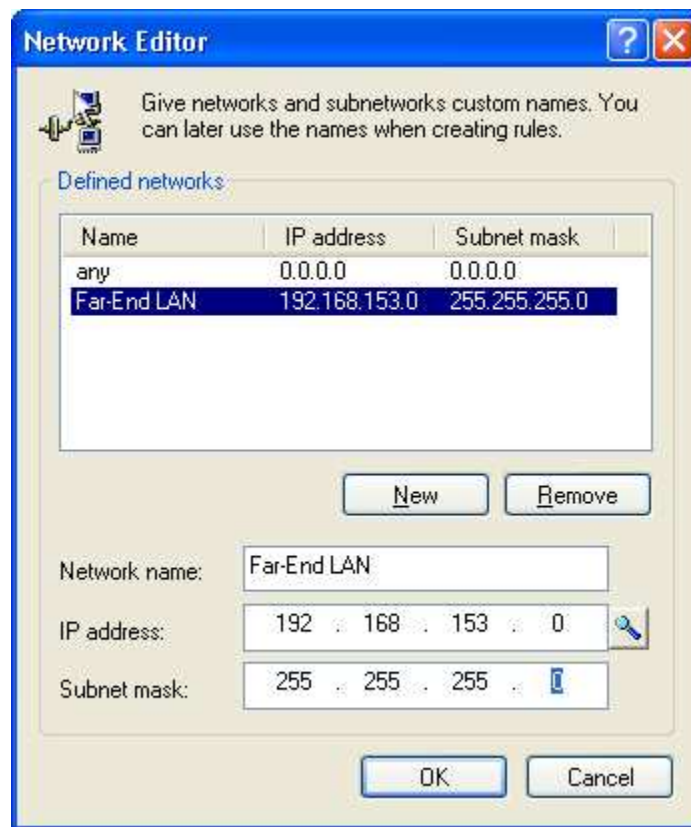


Figure 12 Network Editor

- f. Click on the “New” button.
- g. In the “Network name” field type a name (i.e. Far-End LAN).
- h. In the “IP address” field type in the far-end LAN subnet address (i.e. 192.168.153.0).
- i. In the “Subnet mask” field type in the far-end LAN subnet mask (i.e. 255.255.255.0).
- j. Click on the OK button to save the changes and return to the “Rule Properties” dialog.

- k. Back to the “Rule Properties” dialog, in the “Authentication key” field, select the pre-shared key that you have created in section 4.2. In the example, we used the name “VPN Client to BEFSX41”.
- l. Leave the “Use legacy proposal” box unchecked.
- m. Then click on the “Properties...” button.

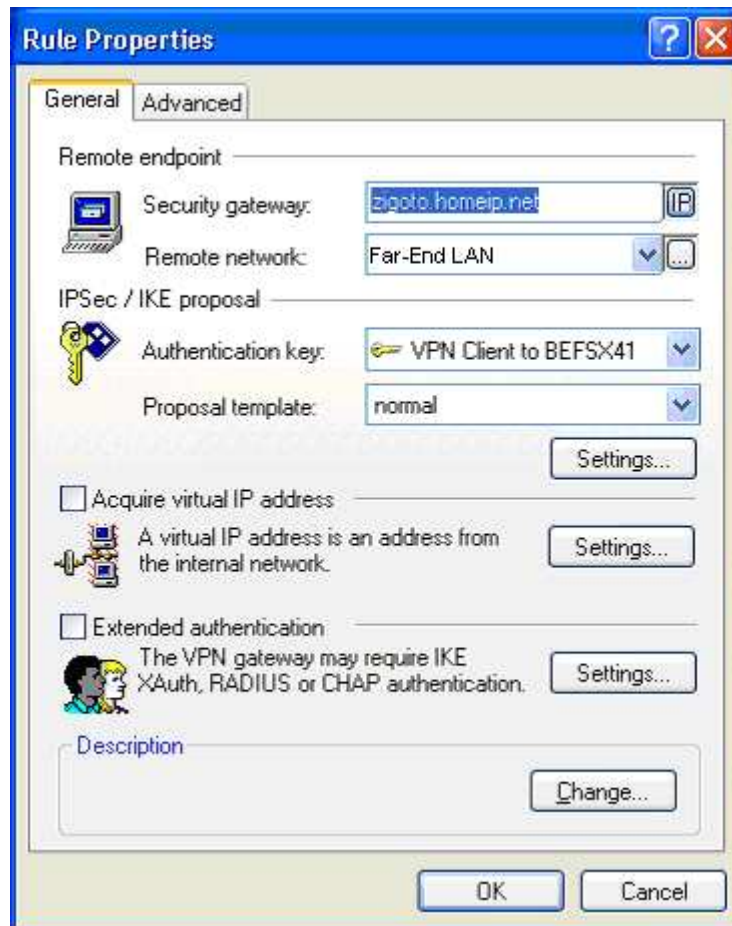


Figure 13 Modifying Rule Properties

- n. From the “Rule Properties” dialog, click on the “Settings...” button of the “IPSec / IKE proposal” area.

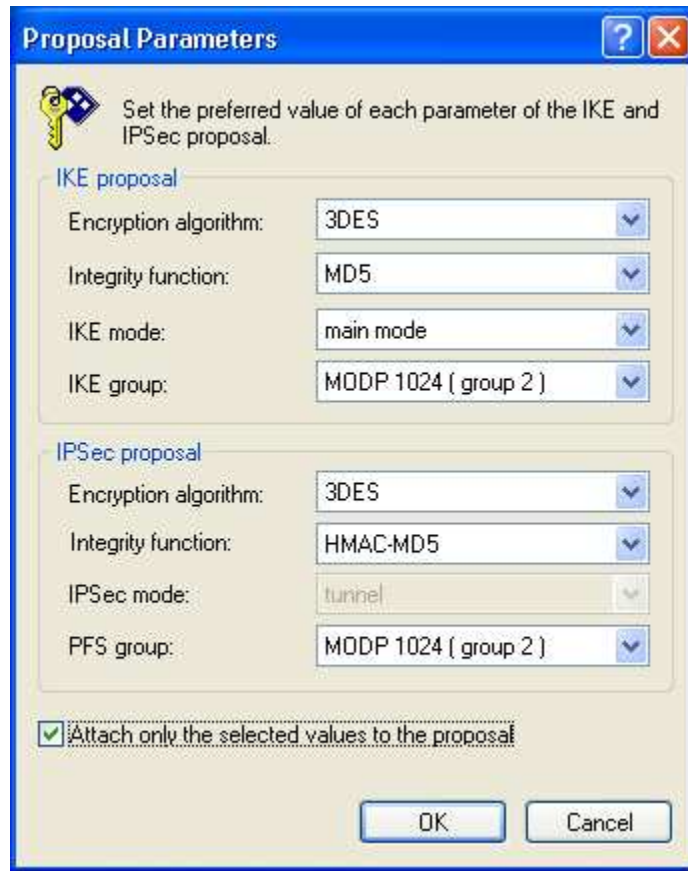


Figure 14 Proposal Parameters

- o. In the “IKE proposal” area, select “3DES” for the “Encryption algorithm”, “MD5” for the “Integrity function”, “main mode” for the “IKE mode” and “MODP 1024 (group 2)” for the “IKE group”.
- p. In the “IPSec proposal” area, select “3DES” for the “Encryption Algorithm”, “HMAC-MD5” for the “Integrity function” and “MODP 1024 (group 2)” for the “PFS group”.
- q. Put a checkmark in the “Attach only the selected values to the proposal” box. This will save some time to the BEFSX41 to determine which parameters to use as only the one you have specified in this dialog will be signalled to the BEFSX41.
- r. Click on the “OK” button.

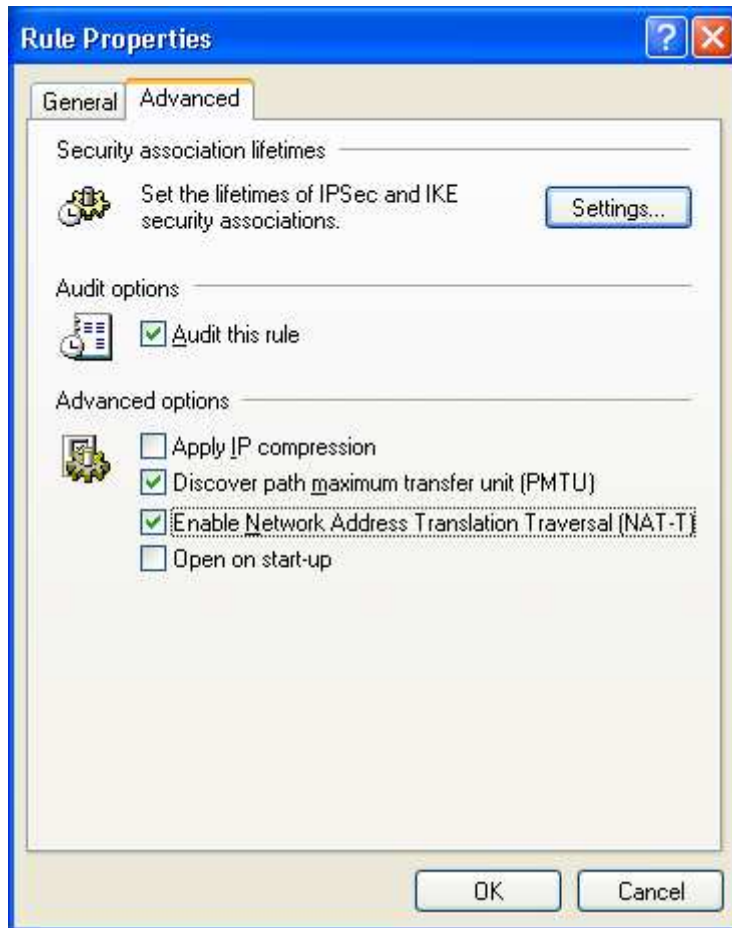


Figure 15 Advanced Rule Properties

- s. Back to the “Rule Properties” dialog, click on the “Advanced” tab.
- t. Put a check mark in the “Audit this rule” box.
- u. Put a check mark in the “Discover path maximum transfer unit (PMTU)” box.
- v. If you have chosen the topology in Figure 1, put a checkmark in the “Enable Network Address Translation Traversal (NAT-T)” box. Otherwise, leave it unchecked.
- w. Leave all remaining boxes unchecked and click on the “Settings...” button.

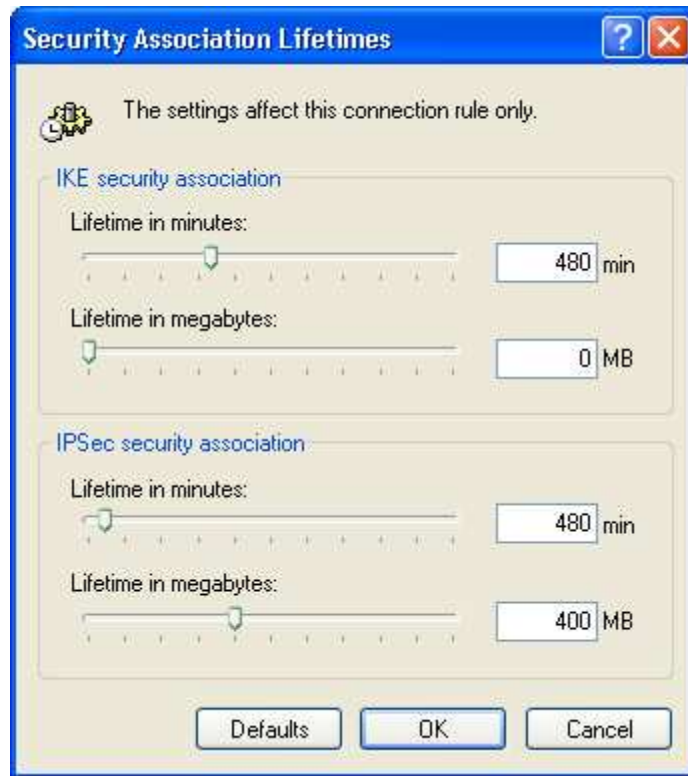


Figure 16 Security Association Lifetimes

- x. In both “Lifetime in minutes” fields, type in 480 minutes. This is equivalent to 28800 seconds that you have configured in the BEFSX41.
- y. Leave the remaining fields to their default values and click the “OK” button.
- z. Back on the “Rule Properties” dialog from Figure 14, click the “OK” button.
- aa. Back on the “Add VPN Connection” dialog from Figure 11, click the “OK” button.
- bb. Back on the “SSH Sentinel Policy Editor” dialog from Figure 10, click the “OK” button.

We have finally completed the SSH Sentinel configuration.

Additionally, please note that in this experiment, I was unsuccessful in getting the diagnostics working ☹. You may try it if you want but don’t get too sad if it fails. The diagnostics do not prevent the VPN tunnel to get establish. You will feel much better reading through the next section to establish your VPN tunnel ☺.

4.4 Establishing the VPN tunnel

Now that our hard work is completed, here is how we initiate the VPN connection from the SSH Sentinel client.

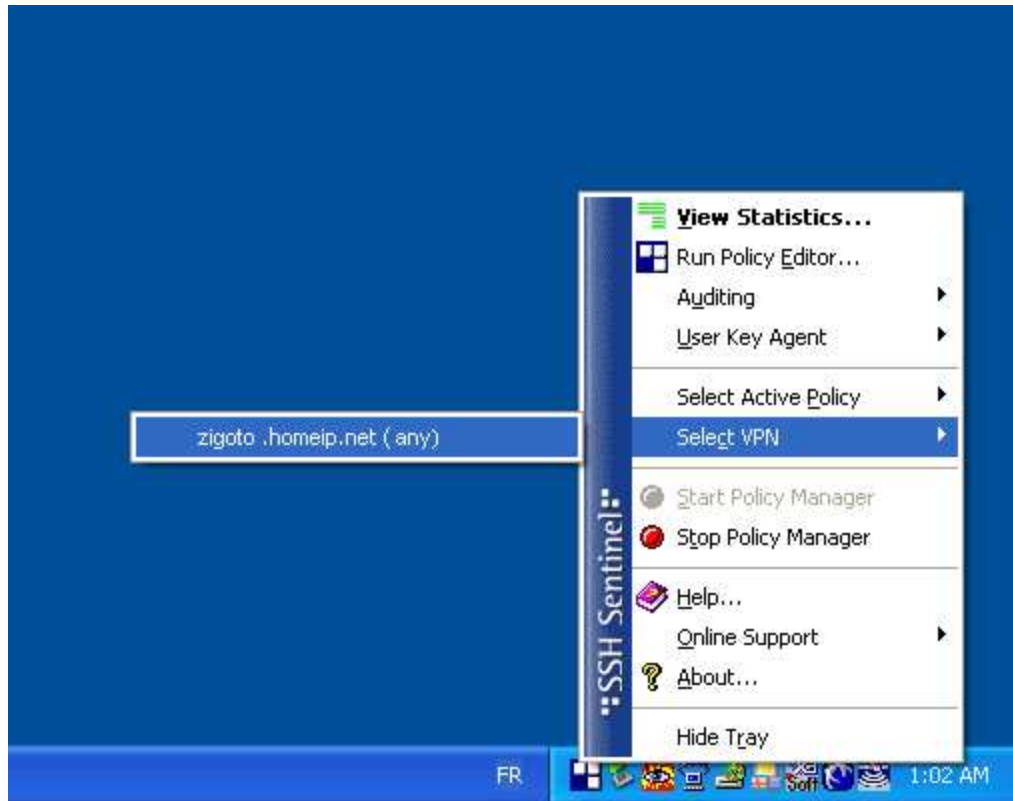


Figure 17 Launching the VPN Tunnel

- a. Right click on the SSH Sentinel icon in the task bar.
- b. Click on the “Select VPN” item.
- c. Click on the VPN connection you have just created.



Figure 18 VPN Connection Status

- d. Watch the connection status dialog. If you have done your homework correctly, you should be getting the dialog from Figure 18. Be quick, this dialog will disappear after few seconds.



Figure 19 VPN Connection Status Success

Youpi! We finally got our VPN tunnel established. The fun part is now to send data through this VPN tunnel. Good luck.

5. Conclusion

This experiment demonstrated the capabilities of the Linksys BEFSX41 to act as a VPN server for very small organization. If more than two simultaneous VPN tunnels are required, the Linksys BEFVP41 can accommodate additional simultaneous tunnels without major reconfiguration.

We have also demonstrated the ability to get two very similar topologies working. The only difference between these really resides on the NAT function performed by a remote NAT router when present. The configuration differences between the two topologies are summarized by section 3 on the NAT router side and by section 4.3 step v (Figure 15) on the SSH Sentinel side.

Finally, because of the ability of the BEFSX41 of broadcasting NetBIOS packets (see section 2.2, step i, in Figure 4), we can also prove that we can get Windows Network Neighbourhood to work correctly across the VPN tunnel. This enables files and printers sharing.

6. Reference

Most of the information used in this document was found on the DSLR/BBR forum. Most specifically in the following thread:

<http://www.broadbandreports.com/forum/remark,8789125~mode=flat>

As pointed out in the above thread, a free copy of SSH Sentinel can be found at the following link, which also provides documents on how to install the software.

<http://www.olin.wustl.edu/computing/reference/wireless/ipsec.cfm>

Additional information was also taken from the following link.

<http://forum.homenethelp.com/tm.asp?m=5590&p=1&tmode=1&smode=1&cookieC heck=588677370>