



IPSec w/ IKE to a Nortel Contivity VPN Switch

Written by:	Jeff Linam	This application note describes the process of configuring the Netopia router to establish an IPSec tunnel using IKE to a Nortel Contivity VPN Switch.
Date:	{08-02-01}	
Revised:	None	

Introduction

This document describes the configuration of an IPSec tunnel using IKE between a Netopia r-series router and a Nortel Contivity Extranet switch. Although implementation is essentially identical across the Netopia product line, the example configuration is based on an r9100 router and a Nortel Contivity Extranet 1500 switch. The Netopia must have at a minimum firmware version 4.94. This example uses DES encryption with MD5 authentication, and operates in 'Main Mode' with shared secrets, although other options are also possible. In order to provide a detailed step-by-step configuration, a number of assumptions must be made about the configuration options used, particularly regarding the non-IPSec portions of the configuration. These options can be changed as desired or needed, but may lead to incompatible configurations.

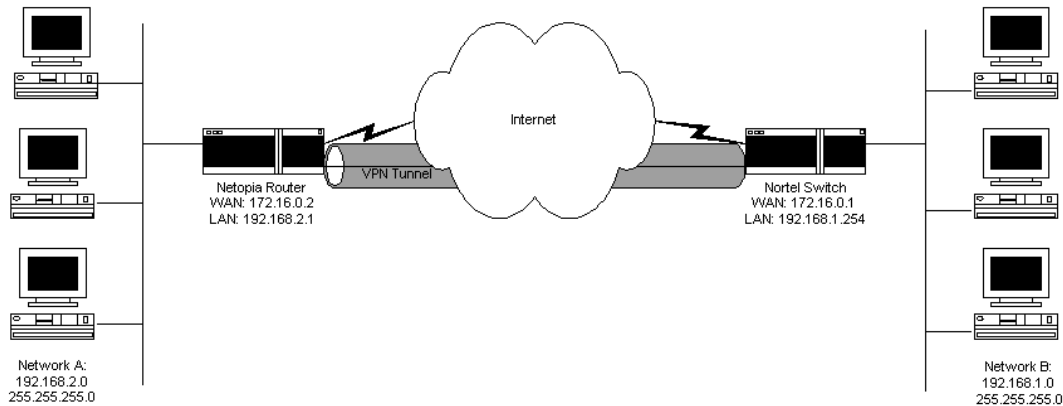
Assumptions

This application note is for reference purposes only; it will need to be modified to suit individual needs, and thus a general working knowledge of the equipment used is assumed. It is further assumed that both the Netopia router and the Nortel switch are already configured for internet access, and that there are no access lists, firewalls, proxy servers, or NAT in place upstream from devices in question preventing access between the devices for UDP port 500 (IKE), protocol 50 (ESP) and protocol 51 (AH). Use of the 3DES encryption in the Netopia option requires the optional VPN Accelerator card. It also assumes that you will be configuring the Netopia via its telnet or console interface, and that you will be configuring the Nortel via its web interface.

Notice:

This example configuration is provided by Netopia as a courtesy to our customers. While this configuration has been tested and proven to work, there are many configuration options in the Nortel product line, and it may be necessary to adjust these parameters to accommodate the configuration already in place on your Nortel switch. Netopia technical support cannot assist with the configuration of non-Netopia products.

Example Network



	Netopia Router	Nortel Contivity Switch
WAN IP Address:	172.16.0.2	172.16.0.1
WAN IP Mask:	255.255.0.0	255.255.0.0
LAN IP Address:	192.168.2.1	255.255.255.0
LAN IP Mask:	192.168.1.254	255.255.255.0

Note that this makes the Network Address of the Netopia's Ethernet interface 192.168.2.0 and the Network Address of the LAN interface of the Nortel switch 192.168.1.0. These addresses will be used throughout the creation of the tunnel.

Netopia Configuration:

- 1) Telnet or Console into the Netopia.
 - 2) Go to Quick Menus, Add Connection Profile.
 - 3) Supply a descriptive Profile Name and set the Data Link Encapsulation to IPSec.
 - 4) Select Data Link Options
 - 5) Set Key Management to IKE
 - 6) Select IKE Phase 1 Profile, <<ADD PH1 PROFILE>>
 - 7) Supply a descriptive name for the IKE profile
 - 8) Leave Mode at Main Mode.
-
- 9) Leave Authentication Method at Shared Secret
 - 10) Set the Shared Secret to an agreed upon password – this can be any alphanumeric string.
 - 11) Select either DES or 3DES for the Encryption Algorithm. Note: you must have the optional VPN accelerator card to select 3DES.
 - 12) Select either MD5 or SHA1 for the Hash Algorithm
 - 13) Diffie-Hellman Group MUST be set to Group 1 (768 bits) to interoperate with the Nortel switch.
 - 14) Leave the Advanced IKE Phase 1 Options alone.
 - 15) Select ADD IKE PHASE 1 PROFILE
 - 16) Make Sure that IKE Phase 1 Profile lists the IKE profile you just created.
 - 17) Leave Encapsulation set to ESP

- 18) Set ESP Encryption Transform to either DES or 3DES. Note that 3DES requires the optional VPN Accelerator card. Null is not recommended, as it offers no data security.
- 19) Set ESP Authentication Transform to either HMAC-MD5-96 or HMAC-SHA1-96
- 20) Make sure Compression Type (if you have the option for it) is set to None.
- 21) Leave the Advanced IKE Options alone.
- 22) Hit enter on COMMIT
- 23) Arrow down to IP Profile Parameters and hit ENTER
- 24) Set Remote Tunnel Endpoint to the WAN Interface address of the Nortel switch. This is the same value used in step #11 above (172.16.0.1 in the example).
- 25) Leave Remote Member Format at Subnet
- 26) Set Remote Member Address to the LAN interface network address of the Nortel switch (192.168.1.0 in the example).
- 27) Set Remote Member Mask to subnet mask used on the LAN interface of the Nortel switch (255.255.255.0 in the example)
- 28) Leave Local Member Format as Subnet
- 29) Set Local Member Address to the network address associated with the Ethernet IP of the Netopia (192.168.2.0 in the example).
- 30) Set the local Member Mask to the Ethernet IP Subnet Mask of the Netopia (255.255.255.0 in the example).
- 31) Leave Address Translation Enabled set to No
- 32) Leave Filter Set set to <<None>>, and leave the Advanced IP Profile Options alone.
- 33) Arrow down to COMMIT and hit ENTER. Repeat this for the Add Connection Profile screen.
- 34) This completes the Netopia portion of the configuration.

Nortel Contivity configuration:

- 1) Use your web browser to connect to the Nortel's Management IP address.
- 2) Click on Manage Switch and enter your administrative name and password.
- 3) Click on Services, IPSec.
- 4) In the Authentication section, make sure that User Name and Password/Pre-Shared Key is checked.
- 5) Under the Encryption section, make sure that the options you have configured in the Netopia profile are selected. Note that DES and 3DES with MD5 are enabled by default but SHA1 is not.
- 6) Click OK when finished.
- 7) Click on Profiles, Networks.
- 8) Enter a new network name in the supplied field that describes the LAN network of the Nortel switch, e.g. 'Local', and click on Create.
- 9) Under the New Subnet section, enter the Network Address and Mask on the Nortel's LAN interface (192.168.1.0 and 255.255.255.0 in the example). Click on Add.
- 10) Click on Close.
- 11) Click on Profiles, Branch Office.
- 12) Click on Add Group.
- 13) Leave Parent Group as /Base, and supply a descriptive group name, e.g., Netopia.
- 14) Click OK.
- 15) Click on the Edit button next to the new group.
- 16) Click on the Configure button in the IPSec section.
- 17) Click on the Configure button in the Encryption section.
- 18) Check to enable all the encryption options you have selected to use in the Netopia's profile, e.g. ESP – Triple DES with MD5 integrity, etc.
- 19) Leave all other options at the defaults and click on OK.
- 20) Click on Close at the Edit Group page.
- 21) Click on Define Branch Office Connection.
- 22) Supply a descriptive Connection Name, e.g. Netopia.
- 23) Under the Group Name, select the group created in step #12 above, e.g. /Base/Netopia.
- 24) Do not check Control Tunnel. Click on OK.

- 25) Leave Routing Type as Static, and leave Enable Branch Office Connection checked.
- 26) For Local Endpoint, select the IP address that corresponds to the WAN interface of the Nortel switch (172.16.0.1 in the example).
- 27) In the Remote Endpoint field, enter the WAN address of the Netopia (172.16.0.2 in the example).
- 28) Under Accessible Networks, select the Network defined under step #7 above, e.g. 'Local'.
- 29) Click on the Add button to the right of the Accessible Networks section.
- 30) Under New Subnet Details, enter the Netopia's Ethernet Network Address and Subnet Mask in the IP Address and Mask fields (192.168.2.0 and 255.255.255.0 in the example). Click OK.
- 31) Under NAT, select (No NAT Translation selected).
- 32) Under Filters, select permit all
- 33) Tunnel Type is IPSec
- 34) IPSec Authentication is Text Pre-Shared Key.
- 35) Enter and confirm the password phrase you used in step #13 of the Netopia configuration above.
- 36) Leave all the other fields alone, and click on OK.
- 37) Click on Admin, Shutdown, Restart, OK.
- 38) This completes the Nortel configuration.

At this point, you should test the tunnel. Remember that it may take as long as two minutes for the tunnel to complete it's initial negotiation; if you are testing with a ping, send at least 200 packets.