

Nortel Contivity Extranet Switch Interoperability Guide

Copyright © 2004, F/X Communications. All Rights Reserved. The use and copying of this product is subject to a license agreement. Any other use is strictly prohibited. No part of this publication may be reproduced, transcribed, or translated into any language, in any form by any means without the prior written consent of F/X Communications. Information in this document is subject to change without notice and does not constitute any commitment on the part of F/X Communications.

F/X Communications, Brolaeggerstraede 12, DK-4300 Holbaek, Denmark.

Contents

1. Nortel Extranet Switch.....	3
1.1. Important notice.....	3
1.2. Brief step-by-step instructions.....	3
1.3. Configuring the Nortel Extranet Switch.....	3
1.4. Configuring the InJoy side.....	5
1.5. Connecting to the Nortel Extranet Switch.....	5

1. Nortel Extranet Switch

1.1. Important notice

The connections in the following tests were conducted over a LAN, using 192.162.x.x IP addresses for the IPSec endpoints. 192.168.x.x addresses were used to illustrate internal networks (behind the IPSec endpoints). When modifying these samples for Internet use, replace the 192.162.x.x addresses with the external IP address of the IPSec endpoints.

1.2. Brief step-by-step instructions

To create a VPN using the InJoy IPSec and Nortel Extranet Switch (v2.6 and newer), the following steps must be completed:

- 1 Install an InJoy product with IPSec ("**Local Host**").
- 2 Install the Pluto IKE server on the InJoy PC.
- 3 Configure the Nortel Extranet Switch ("**Remote Gateway**").
 - 3.1 Define the Nortel Extranet Switch setup
 - 3.2 Define user parameters.
- 4 Configure the InJoy IPSec side.
- 5 Restart the InJoy IPSec product and the IKE server.
- 6 Trigger InJoy to establish the SA. (note: any traffic between IPSec endpoints will force this).

1.3. Configuring the Nortel Extranet Switch

The below example illustrates the Nortel configuration with user based authentication and inner (Red Node) IP address assignment.

Define general IPSec parameters as shown below:

IPsec

Configure

Split Tunneling: Disabled
 Split Tunnel Networks: (None)
 Client Selection:
 - Allowed Clients: Both Contivity and non-Contivity Clients
 - Allow undefined networks for non-Contivity clients: Enabled
 Database Authentication (LDAP):
 - User Name and Password: Enabled
 - RSA Digital Signature: Enabled
 Default Server Certificate: (None)
 RADIUS Authentication:
 - User Name and Password: Disabled
 - AXENT Technologies Defender: Disabled
 - Security Dynamics SecurID: Disabled
 Encryption:
 - ESP - 56-bit DES with MD5 Integrity: Enabled
 - ESP - 40-bit DES with MD5 Integrity: Enabled
 - AH - Authentication Only (HMAC-SHA1): Enabled
 - AH - Authentication Only (HMAC-MD5): Enabled
 Perfect Forward Secrecy: Disabled
 Forced Logout: 00:00:00
 Client Auto Connect: Disabled
 Banner: (None)
 Display Banner: Disabled
 Client Screen Saver Password Required: Disabled
 Client Screen Saver Activation Time: 5 Minutes
 Allow Password Storage on Client: Disabled
 Compression: Enabled
 Relay Timeout: 08:00:00
 Relay Data Count: (None)
 Domain Name: (None)
 Primary DNS: (None)
 Secondary DNS: (None)
 Primary WINS: (None)
 Secondary WINS: (None)
 Client Policy: (None)

Define user name, password and Inner IP address as shown below:

General

	First	Last
Name	remotel	remotel
Group	/Base/CGIC	
	Static IP Address	Static Subnet Mask
Remote User	192.168.71.53	255.255.255.224

Note: The static IP subnet mask is used for IPsec connections only

User Accounts

	User ID	Password	Confirm Password	Expires (Days)
IPsec	remotel	*****	*****	Never
PPTP				
L2TP				

1.4. *Configuring the InJoy side*

On the Local Host, add the following section to the ipsec.cnf file (to describe the SA to the Nortel Extranet Switch):

```
nortel
    Description = "Nortel Extranet Switch",
    Mode = Tunnel,
    Local-IP = "192.162.5.2",           # local host IP address
    Inner-IP = "192.168.71.53",       # Inner (Red Node) IP address
    Remote-IP = "207.35.127.131",     # remote gateway IP address
    Remote-Net = "172.18.1.0",
    Remote-Mask = "255.255.255.0",
    Auth-Type = Client-IdKeyId,
    User-Id = Prompt,                 # ask for username
    AH = No,
    ESP = DES,
    Reinit = Yes,
    Preshared-Secret = "secret_phrase",
```

Restart the InJoy IPsec product and the Pluto IKE server for changes to take effect.

User-Id = Prompt allows entering of the user name and password for user based authentication.

1.5. *Connecting to the Nortel Extranet Switch*

If user based authentication support is configured, you will be prompted to enter user name and password by the InJoy product. Any traffic to the Remote Subnet behind the Gateway will force IKE negotiations.

On the Local Host, the ipsec.log will contain the following lines:

```
Jul 6 02:28:04 : adding to pluto: nortel
Jul 6 02:28:04 : setting pass for pluto: nortel
Jul 6 02:28:04 : force pluto to initiate: nortel
Jul 6 02:28:10 : ipsec: install sa [nortel]
Jul 6 02:28:10 : SA name = [nortel]
Jul 6 02:28:10 : IdKeyId = [remotel]
Jul 6 02:28:10 : Local gateway (host) ip address = [192.162.5.2]
Jul 6 02:28:10 : Inner IP = [192.168.71.53]
Jul 6 02:28:10 : Local net = [192.168.71.53]
Jul 6 02:28:10 : Local net mask = [255.255.255.255]
Jul 6 02:28:10 : Remote gateway (host) ip address = [207.35.127.131]
Jul 6 02:28:10 : Remote net = [172.18.1.0]
Jul 6 02:28:10 : Remote net mask = [255.255.255.0]
Jul 6 02:28:10 : ISAKMP SA lifetime = [3600] seconds
Jul 6 02:28:10 : IPSEC SA lifetime = [28800] seconds
Jul 6 02:28:10 : ESP encr/auth/keylen=[ESP_ALG_CBC_DES/AH_ALG_MD5/24]
Jul 6 02:28:10 : AH method/keylen = [unknown/0]
Jul 6 02:28:10 : Road Warrior = [yes]
```