

Setting up VPN Tracker with Nortel VPN Routers



NORTEL VPN Router															
<ul style="list-style-type: none"> + System - Services <ul style="list-style-type: none"> - Available - AOT - Demand - IPsec - PPTP - FWUA - L2TP - L2F - RADIUS - Firewall / NAT - Syslog - SSL TLS + Routing + QoS + Profiles + Servers + Admin + Status + Help 	<p>192.168.180.2 » IPsec Settings View or modify the authentication settings used for</p> <p>Authentication</p> <table border="1"> <tr> <td>User Name and Password/Pre-Shared Key</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>RSA Digital Signature</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> <p>RADIUS Authentication</p> <table border="1"> <tr> <td>PassGo Technologies Defender</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>RSA SecurID</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>User Name and Password</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> <p>Encryption</p> <table border="1"> <tr> <td>ESP - 256-bit AES with SHA1 Integrity</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>ESP - 128-bit AES with SHA1 Integrity</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	User Name and Password/Pre-Shared Key	<input checked="" type="checkbox"/>	RSA Digital Signature	<input checked="" type="checkbox"/>	PassGo Technologies Defender	<input checked="" type="checkbox"/>	RSA SecurID	<input checked="" type="checkbox"/>	User Name and Password	<input checked="" type="checkbox"/>	ESP - 256-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>	ESP - 128-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>
User Name and Password/Pre-Shared Key	<input checked="" type="checkbox"/>														
RSA Digital Signature	<input checked="" type="checkbox"/>														
PassGo Technologies Defender	<input checked="" type="checkbox"/>														
RSA SecurID	<input checked="" type="checkbox"/>														
User Name and Password	<input checked="" type="checkbox"/>														
ESP - 256-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>														
ESP - 128-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>														

Configuring the Nortel VPN Router (Contivity)	3
<i>Configuring the global IPSec settings</i>	3
<i>Authentication</i>	3
<i>RADIUS Authentication</i>	3
<i>Encryption</i>	3
<i>IKE Encryption and Diffie-Hellman Group</i>	4
<i>NAT Traversal</i>	4
<i>Save your changes</i>	4
<i>Configuring your user groups</i>	5
<i>Create a user group for your Mac users</i>	5
<i>IPSec Settings for your Macuser Group</i>	6
<i>Adding users</i>	8
Configuring VPN Tracker	9
<i>Creating a new connection</i>	9
<i>Basic settings</i>	9
<i>Network settings</i>	9
<i>Authentication</i>	9
<i>Identifier</i>	10
<i>DNS</i>	10
<i>Advanced Settings</i>	12
<i>Phase 1</i>	12
<i>Phase 2</i>	12
Start your connection	13

1. Configuring the Nortel VPN Router (Contivity)

1.1. Configuring the global IPSec settings

NORTEL	
+ System	
- Services	
- Available	
- AOT	
- Demand	
- IPSec	
- PPTP	
- FWUA	
- L2TP	
- L2F	
- RADIUS	
- Firewall / NAT	
- Syslog	
- SSL TLS	
+ Routing	
+ QoS	
+ Profiles	
+ Servers	
+ Admin	
+ Status	
+ Help	

You'll need to change the following settings under **Services > IPSec**:

1.1.1. Authentication

Authentication

User Name and Password/Pre-Shared Key	<input checked="" type="checkbox"/>
RSA Digital Signature	<input checked="" type="checkbox"/>

1.1.2. RADIUS Authentication

RADIUS Authentication

PassGo Technologies Defender	<input checked="" type="checkbox"/>
RSA SecurID	<input checked="" type="checkbox"/>
User Name and Password	<input checked="" type="checkbox"/>

1.1.3. Encryption

You can use AES 128-bit encryption if you have VPN Tracker 6 Personal and AES 256-bit if you have VPN Tracker 6 Professional or Player. Deactivate all other encryption options.

Encryption

ESP - 256-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>
ESP - 128-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>

1.1.4. IKE Encryption and Diffie-Hellman Group

Enable all AES groups

IKE Encryption and Diffie-Hellman Group

56-bit DES with Group 1 (768-bit prime)	<input type="checkbox"/>
Triple DES with Group 2 (1024-bit prime)	<input type="checkbox"/>
Triple DES with Group 7 (ECC 163-bit field)	<input type="checkbox"/>
128-bit AES with Group 5 (1536-bit prime)	<input checked="" type="checkbox"/>
128-bit AES with Group 8 (ECC 283-bit field)	<input checked="" type="checkbox"/>
128-bit AES with Group 2 (1024-bit prime)	<input checked="" type="checkbox"/>
256-bit AES with Group 5 (1536-bit prime)	<input checked="" type="checkbox"/>
256-bit AES with Group 8 (ECC 283-bit field)	<input checked="" type="checkbox"/>

1.1.5. NAT Traversal

NAT Traversal*

Enabled	<input checked="" type="checkbox"/> User Tunnel <input type="checkbox"/> Branch Office Tunnel
Disable Client IKE Source Port Switching	<input type="checkbox"/>
UDP Port	<input type="text" value="10001"/>

*Changing NAT traversal settings will cause active tunnels to disconnect.

1.1.6. Save your changes



1.2. Configuring your user groups

1.2.1. Create a user group for your Mac users

Go to **Profiles > Groups** to configure your new group.

Group	Actions
/Base	<input type="button" value="Edit"/>
/Base/detewe	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Group Name	<input type="text" value="Macuser"/>
Parent Group	<input type="text" value="/Base"/> ▾

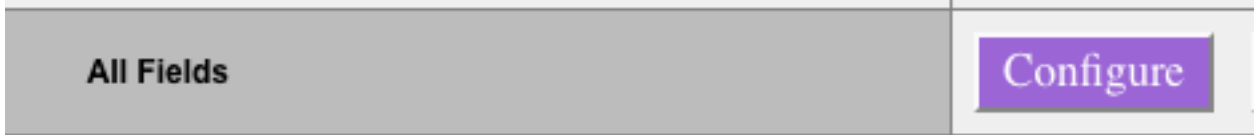
Rename your group (e.g. "Macuser") and click Ok.

/Base/Macuser	<input type="button" value="Edit"/>
---------------	-------------------------------------

You can also configure additional user access options for your group, however those settings aren't described in this guide.

1.2.2. IPSec Settings for your Macuser Group

Go right to the bottom and click the “Configure” button for “All Fields”



You probably won't need to change any other settings, as the Macuser group will inherit the settings from the "/Base" group.

However: If your "/Base" group isn't configured correctly, your Mac user group should be configured like this:

Field	Value	Actions	Inherited From
Split Tunneling	Disabled	Use Inherited	
Split Tunnel Networks	(None selected) New Network	Use Inherited	
Inverse Split Tunnel Networks	(None selected) New Network	Use Inherited	
IPSec Idle Timeout Reset on Outbound Traffic	Enabled	Use Inherited	
Client Selection	Allowed Clients: Both VPN Router and non-VPN Router Clients <input checked="" type="checkbox"/> Allow undefined networks for non-VPN Router clients	Use Inherited	
Authentication	<p>Database Authentication (LDAP)</p> <p><input checked="" type="checkbox"/> User Name and Password</p> <p><input checked="" type="checkbox"/> RSA Digital Signature</p> <p>Default Server Certificate</p> <p>No Cert</p> <p>Group Level Radius Settings</p> <p><input type="checkbox"/> Group Level Radius Server Not Configured Configure Group Level RADIUS Servers</p> <p>* Radius and LDAP Proxy Authentication</p> <p><small>Note: Required for all groups using RADIUS or LDAP Proxy authentication.</small></p> <p>GroupID Authentication Two Factor Authentication</p> <p>Group ID <input type="text"/> <input type="checkbox"/> Enable</p> <p>Group Password <input type="text"/></p> <p>Group Confirm Password <input type="text"/></p> <p>Authentication Type (select one)</p> <p><input type="checkbox"/> User Name and Password (Radius)</p> <p><input type="checkbox"/> User Name and Password (LdapProxy)</p> <p><input type="checkbox"/> PassGo (Radius)</p> <p><input type="checkbox"/> RSA SecurID (Radius) (GroupID only)</p>	Use Inherited	

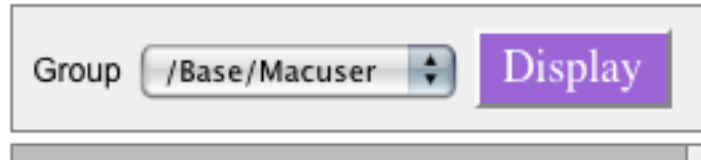
Field	Value	Actions	Inherited From
Split Tunneling	Disabled	Use Inherited	
Split Tunnel Networks	(None selected) New Network	Use Inherited	
Inverse Split Tunnel Networks	(None selected) New Network	Use Inherited	
IPSec Idle Timeout Reset on Outbound Traffic	Enabled	Use Inherited	
Client Selection	Allowed Clients: Both VPN Router and non-VPN Router Clients <input checked="" type="checkbox"/> Allow undefined networks for non-VPN Router clients	Use Inherited	
Authentication	Database Authentication (LDAP) <input checked="" type="checkbox"/> User Name and Password <input checked="" type="checkbox"/> RSA Digital Signature Default Server Certificate No Cert Group Level Radius Settings <input type="checkbox"/> Group Level Radius Server Not Configured Configure Group Level RADIUS Servers * Radius and LDAP Proxy Authentication <small>Note: Required for all groups using RADIUS or LDAP Proxy authentication.</small> GroupID Authentication <input type="text"/> Two Factor Authentication <input type="checkbox"/> Enable Group ID <input type="text"/> Group Password <input type="text"/> Group Confirm Password <input type="text"/> <u>Authentication Type (select one)</u> <input type="checkbox"/> User Name and Password (Radius) <input type="checkbox"/> User Name and Password (LdapProxy) <input type="checkbox"/> PassGo (Radius) <input type="checkbox"/> RSA SecurID (Radius) (Groupid only)	Use Inherited	

You won't need to enter any additional settings, as you can configure your DNS server etc. directly within VPN Tracker.

1.2.3. Adding users

Go to **Profiles > Users** to add additional users

As your **Group** select **"/Base/Macuser"** and then click *Display*. Now you can add additional users.



Enter the user's first and last name. Under "IPsec" you'll also need to set a password for every user.

You'll also need to enter a static IP address for VPN Tracker users.

General

	First	Last
Name	<input type="text" value="mac"/>	<input type="text" value="test"/>
Group	<input type="text" value="/Base/Macuser"/>	
	Static IP Address	Static Subnet Mask
Remote User	<input type="text" value="192.168.180.99"/>	<input type="text" value="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)	Status
IPsec	<input type="text" value="mactest"/>	<input type="password" value="*****"/>	<input type="password" value="*****"/>		
PPTP	<input type="text"/>	<input type="text"/>	<input type="text"/>		
L2TP	<input type="text"/>	<input type="text"/>	<input type="text"/>		
L2F	<input type="text"/>	<input type="text"/>	<input type="text"/>		
Firewall User Authentication	<input type="text"/>	<input type="text"/>	<input type="text"/>		
Must Change Password at Next Logon	<input type="checkbox"/> (Nortel IPSEC Client Only)				

(Automatic configuration is currently not supported.)

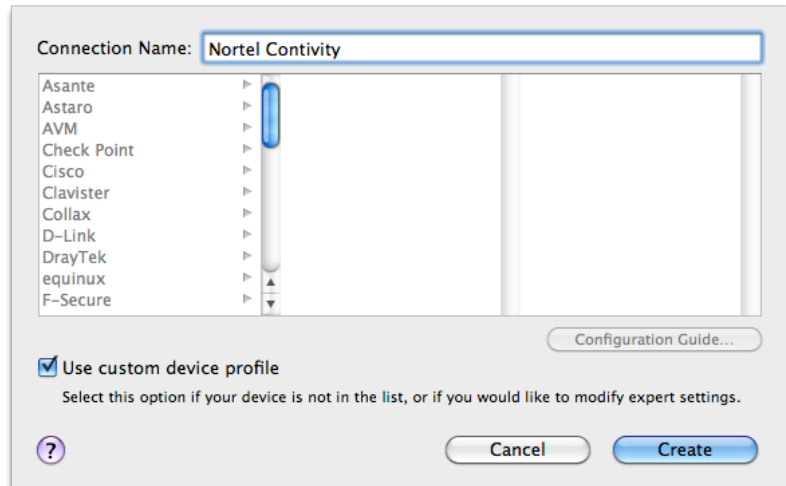
Congratulations! You've finished your Nortel router's configuration.

2. Configuring VPN Tracker

2.1. Creating a new connection

Select **File > New Connection**

Enter any name for your connection and check the “custom device profile” box at the bottom of the bottom of the window.



2.2. Basic settings

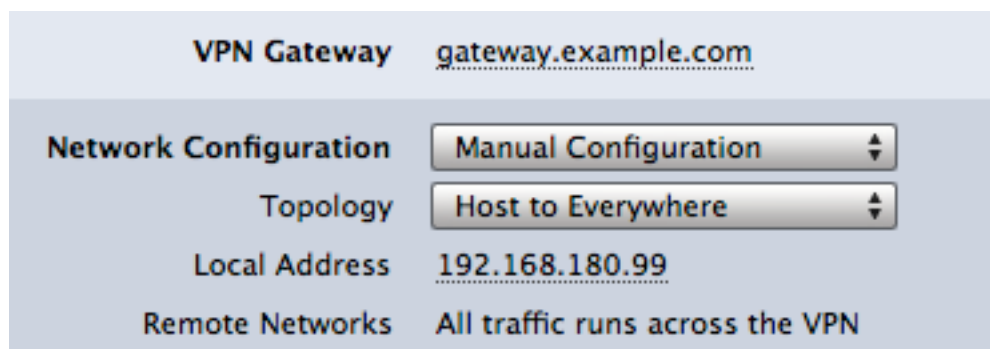
2.2.1. Network settings

Select **Manual Configuration** for your Network Configuration.

Depending on your preference, choose between Host to Everywhere or Host to Network.

If you select **Host to Network** to enter your remote networks in VPN Tracker.

In this example, we'll use **Host to everywhere**.



Enter your Contivity's external IP address in the VPN Gateway field.

As the Local Address, enter the user's IP address you configured on your VPN router earlier.

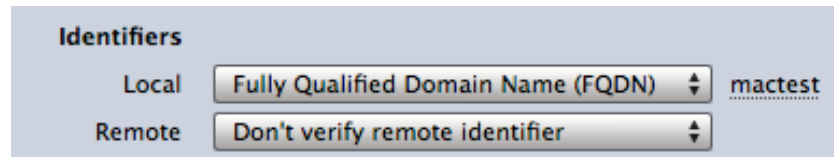
2.2.2. Authentication

Select **Pre-Shared Key** for authentication.

2.2.3. Identifier

The **Local Identifier type** is **Fully Qualified Domain Name (FQDN)**. Enter the user's ID.

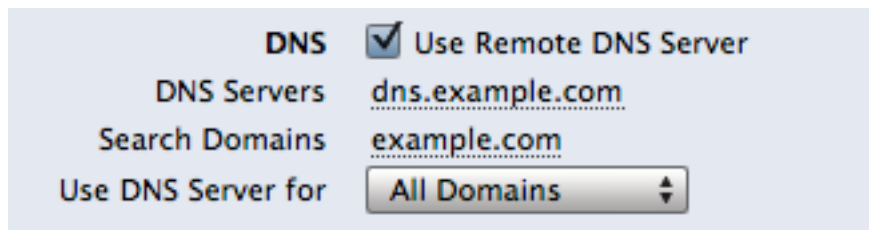
Set **Remote Identifier** to "Don't verify remote identifier".



Identifiers	
Local	Fully Qualified Domain Name (FQDN) mactest
Remote	Don't verify remote identifier

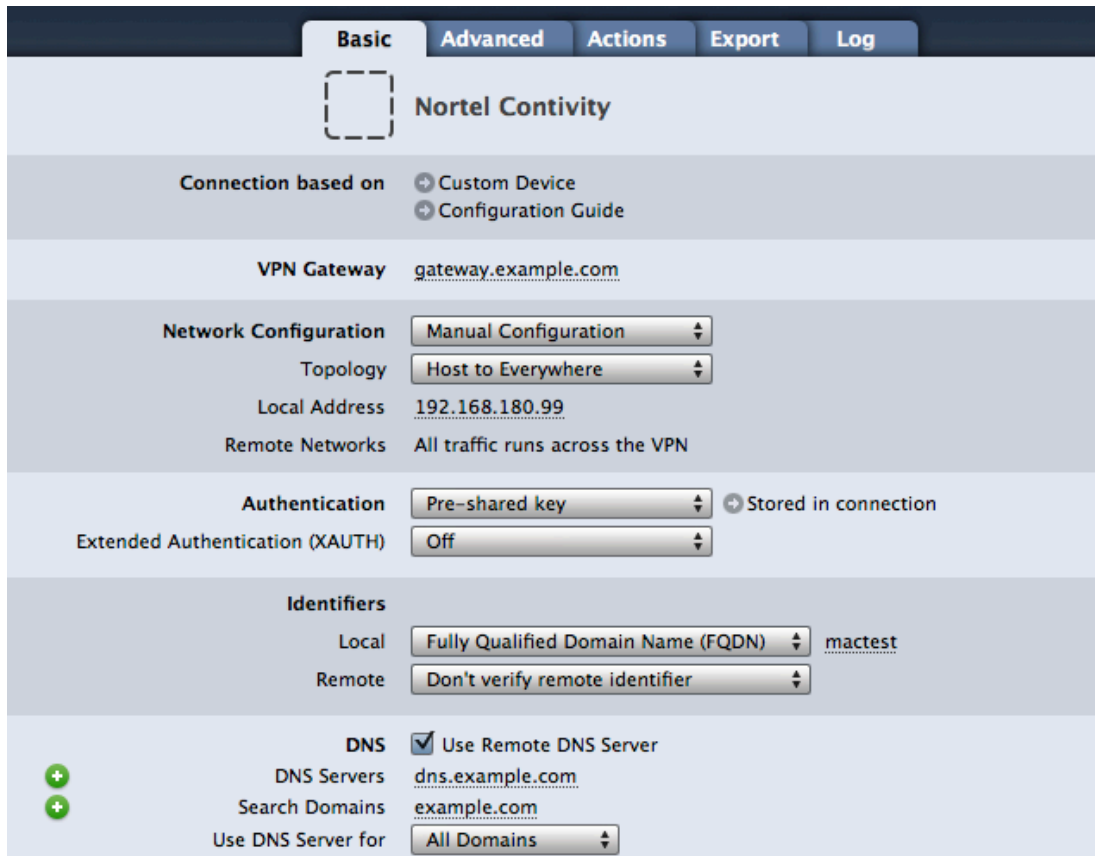
2.2.4. DNS

Enable "Use **Remote DNS-Server**" if required and enter your DNS server address and search domains.



DNS	<input checked="" type="checkbox"/> Use Remote DNS Server
DNS Servers	dns.example.com
Search Domains	example.com
Use DNS Server for	All Domains

Once you've entered your settings, it should look something like this.
Now head on over to the Advanced tab.



2.3. Advanced Settings

2.3.1. Phase 1

Select **Aggressive Mode** as your **Exchange Mode**.

Deactivate all the Encryption algorithms, except **AES-128** & **AES-256**.

Select the **SHA1** Hash algorithm and **Diffie-Hellman Group 5 (1536 bit)**.

The screenshot shows the Phase 1 configuration interface with the following settings:

- Exchange mode: Aggressive Mode
- Lifetime: 28800 seconds
- Encryption algorithm: AES-256 (checked), AES-192 (unchecked), AES-128 (checked), 3DES (unchecked)
- Hash algorithm: SHA1 (checked), MD5 (unchecked), SHA-512 (unchecked)
- Diffie-Hellman: Group 5 (1536 bit)

2.3.2. Phase 2

Deactivate all the Encryption algorithms, except **AES-128** & **AES-256**.

Select the **HMAC SHA1** Authentication algorithm and **Diffie-Hellman Group 5 (1536 bit)**.

The screenshot shows the Phase 2 configuration interface with the following settings:

- Lifetime: 28800 seconds
- Encryption algorithm: 3DES (unchecked), AES-128 (checked), AES-192 (unchecked), AES-256 (checked)
- Authentication algorithm: HMAC MD5 (unchecked), HMAC SHA1 (checked), No authentication (unchecked)
- Perfect Forward Security (PFS): DH Group 5 (1536 bit)

Select **DH Group 5 (1536 bit)** for **Perfect Forward Security (PFS)**.

3. Start your connection

Now you're ready to test your VPN Tunnel!
Click the slider and try to act your network resources.

For more information & tips, refer to VPN Tracker - The Complete Manual, available under Help > Complete Manual.

