VPN Tracker for Mac OS X

How-to:

Interoperability with

Novell BorderManager 3.8

Rev. 1.0

1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and Novell BorderManager 3.8 installed on a Novell NetWare server.

The Novell BorderManager server is configured as a router connecting a company LAN to the Internet.

This paper is only a supplement to, not a replacement for, the instructions that have been included with Novell NetWare / BorderManager. Please be sure to read those instructions and understand them before starting.

2. Prerequisites

First you have to make sure, that you've installed a recent Novell NetWare server, for this document version 6.5 has been used.

Furthermore you should verify, that you use Novell BorderManager 3.8, since previous versions haven't been confirmed to interoperate with VPN Tracker.

For the configuration of the Novell BorderManager VPN services, iManager has been used. So please also make sure, that iManager 2.0 or higher and the VPN snap-ins for iManager are installed.

On the Mac side you need one VPN Tracker Personal license for each Mac connecting to the Novell BorderManager server. VPN Tracker is compatible with Mac OS X 10.2 or higher.

3. Connecting a VPN Tracker host to a Novell BorderManager server

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.[1]

The Novell BorderManager server is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The Stations in the LAN behind the Novell BorderManager server use 192.168.1.1 as their default gateway and should have a working Internet connection.

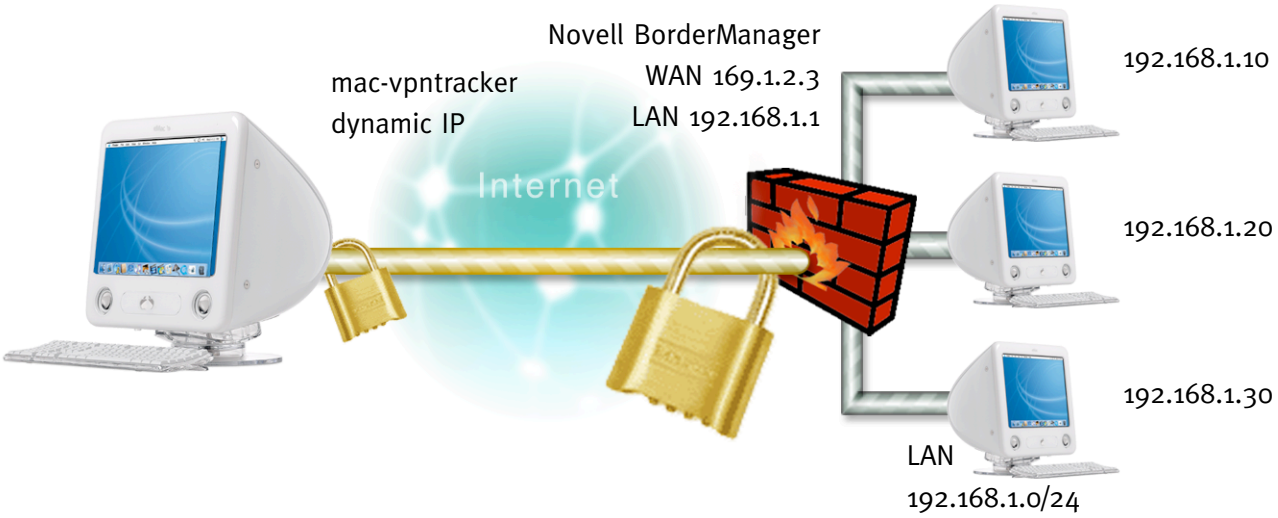

Figure 1: VPN Tracker – Novell BorderManager connection diagram

[1] Please note that the connection via a router, which uses Network Address Translation (NAT), only works if the NAT router supports „IPsec pass-through“. Please contact your router's manufacturer for details.

3.1 Novell BorderManager Certificate Creation

Please follow the next steps to create the trusted root object, trusted root certificate, server certificates and user certificates. We'll need these objects later for the VPN Client to Site and VPN Server Configuration.

Step 1 Please select "Create Trusted Root Containers" under Novell Certificate Server from the left panel and enter the name and context of the container.

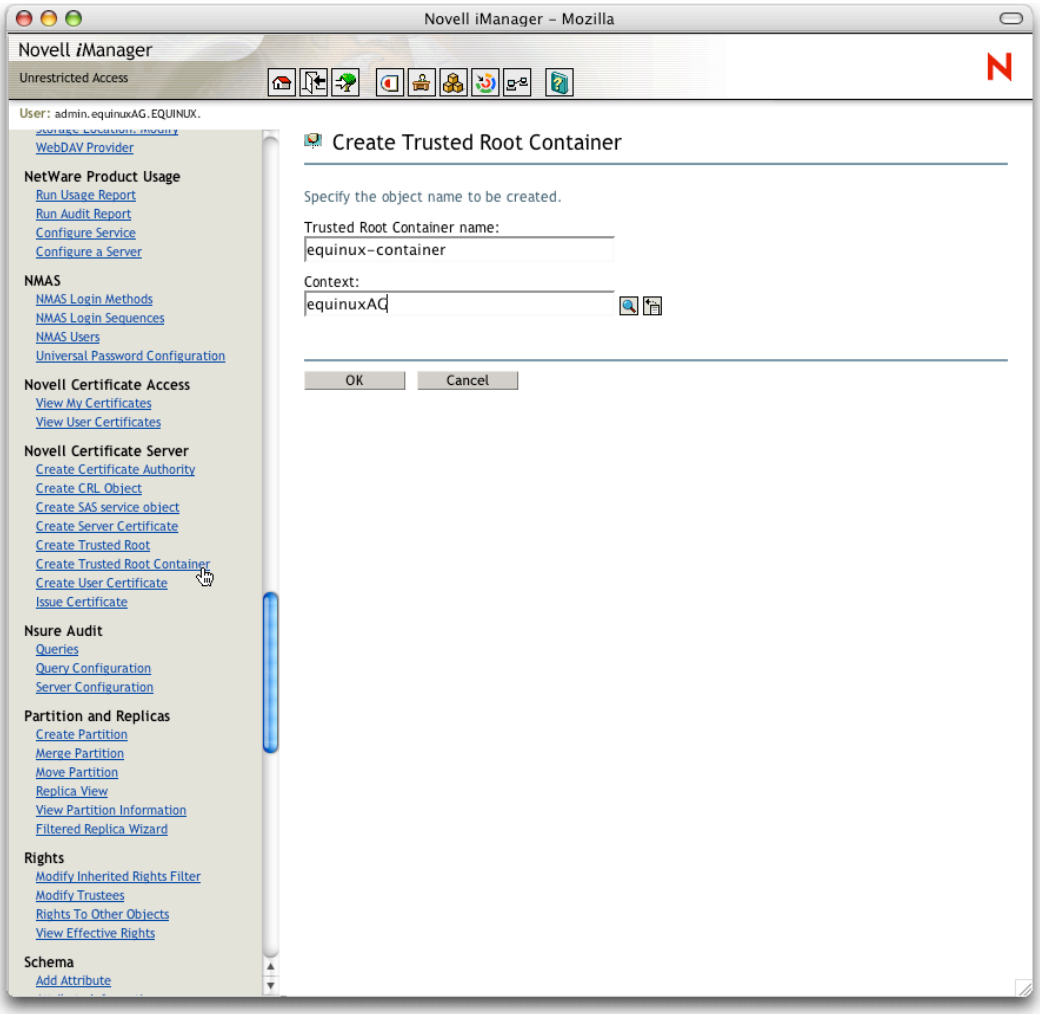

Figure 2: Novell BorderManager - Create Trusted Root Container

Step 2

Click on “Create Trusted Root” under Novell Certificate Server and enter an arbitrary certificate name, select the container you created in step 1 and browse the RootCert.der file (normally located in the pub directory).

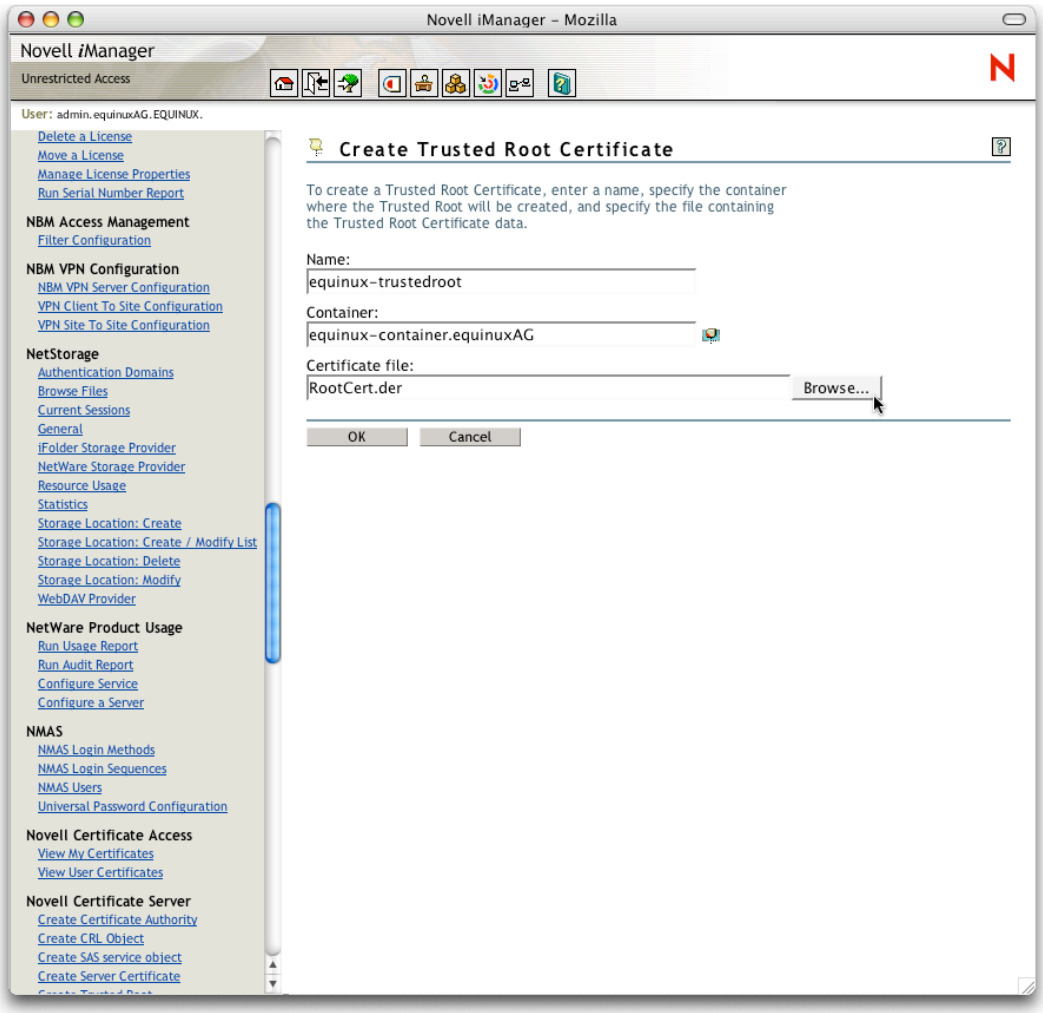

Figure 3: Novell BorderManager - Create Trusted Root Certificate

Step 3

Select “Create Server Certificate” under Novell Certificate Server and enter the server name and an arbitrary certificate nickname. Make sure that the Creation method is set to “Custom” and click on Next.

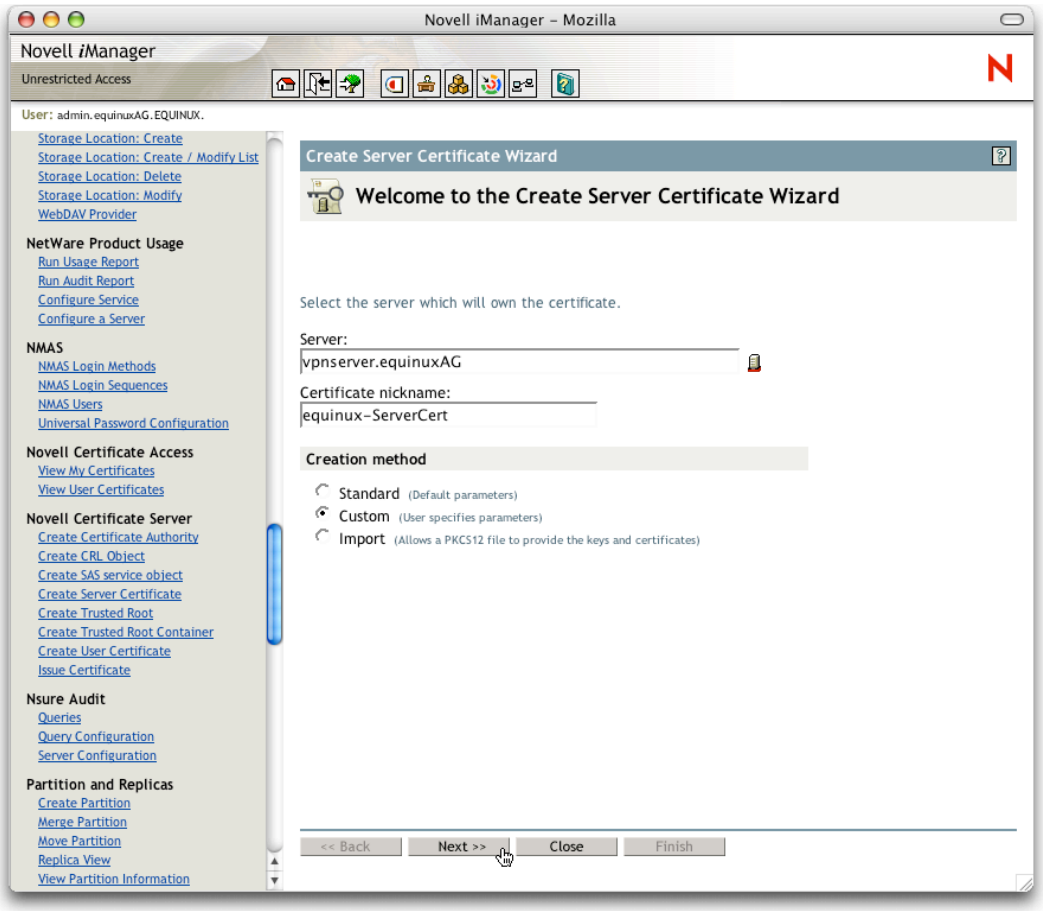

Figure 4: Novell BorderManager - Create Server Certificate Wizard

Check the Organizational Certificate Authority checkbox and click on Next.

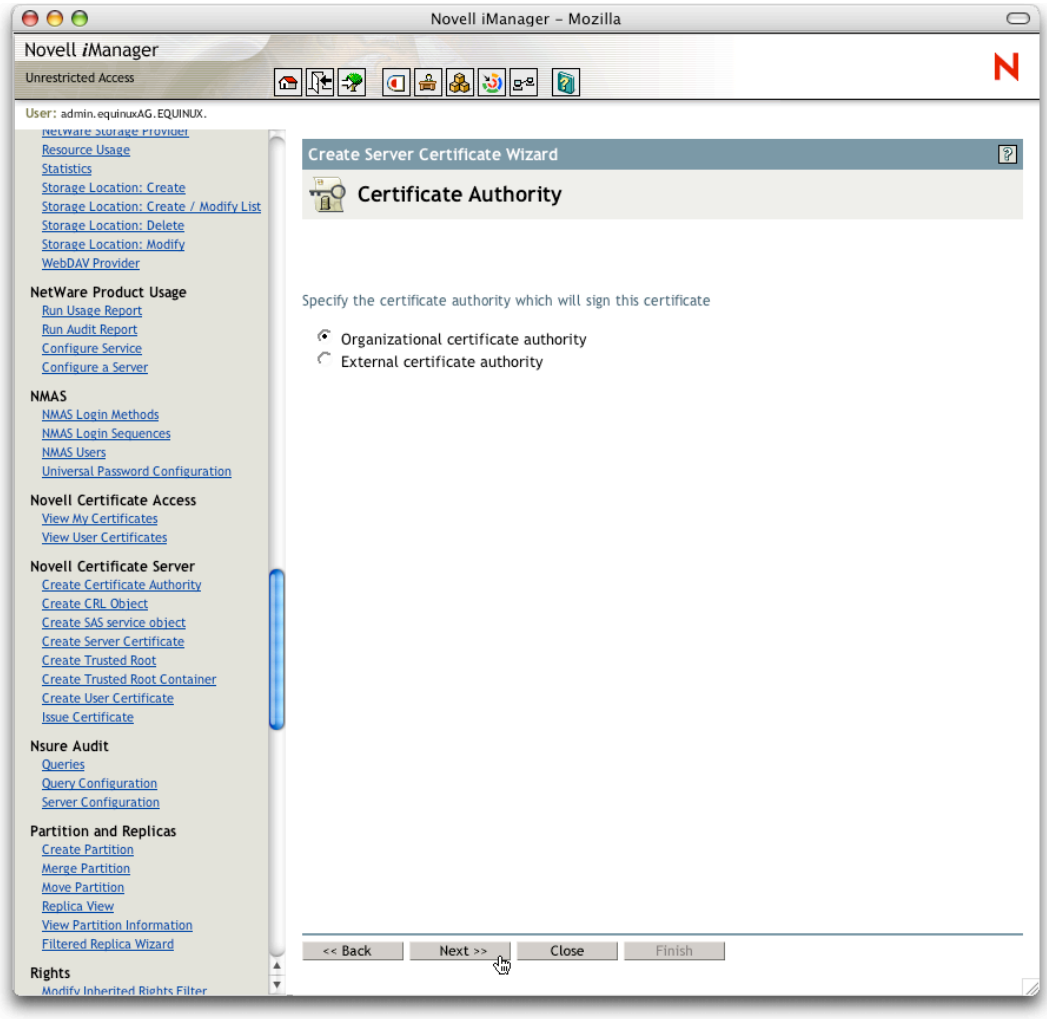

Figure 5: Novell BorderManager - Certificate Authority

Select “Custom” as Key Type and make sure that all Key Usage checkboxes are checked.

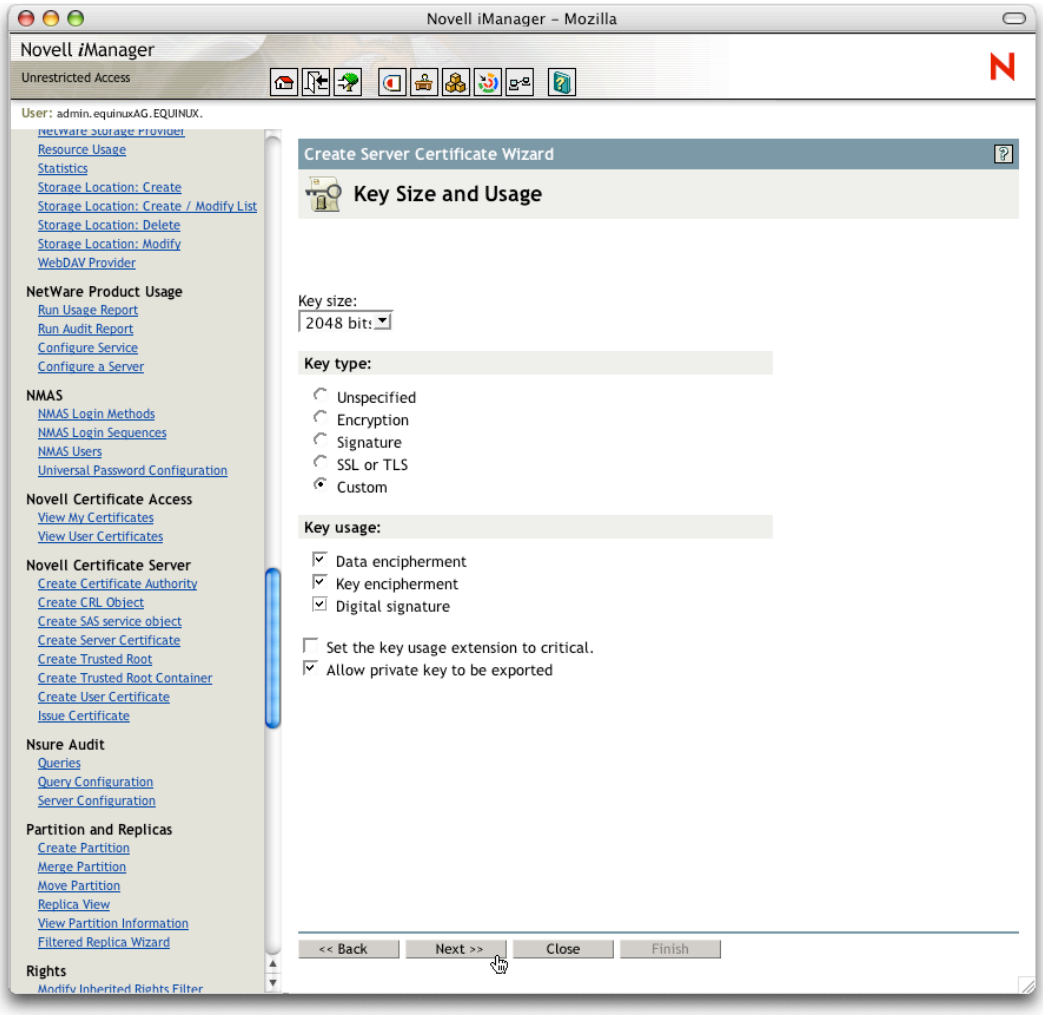

Figure 6: Novell BorderManager - Key Size and Usage

Just click on Next in the following 2 screens.

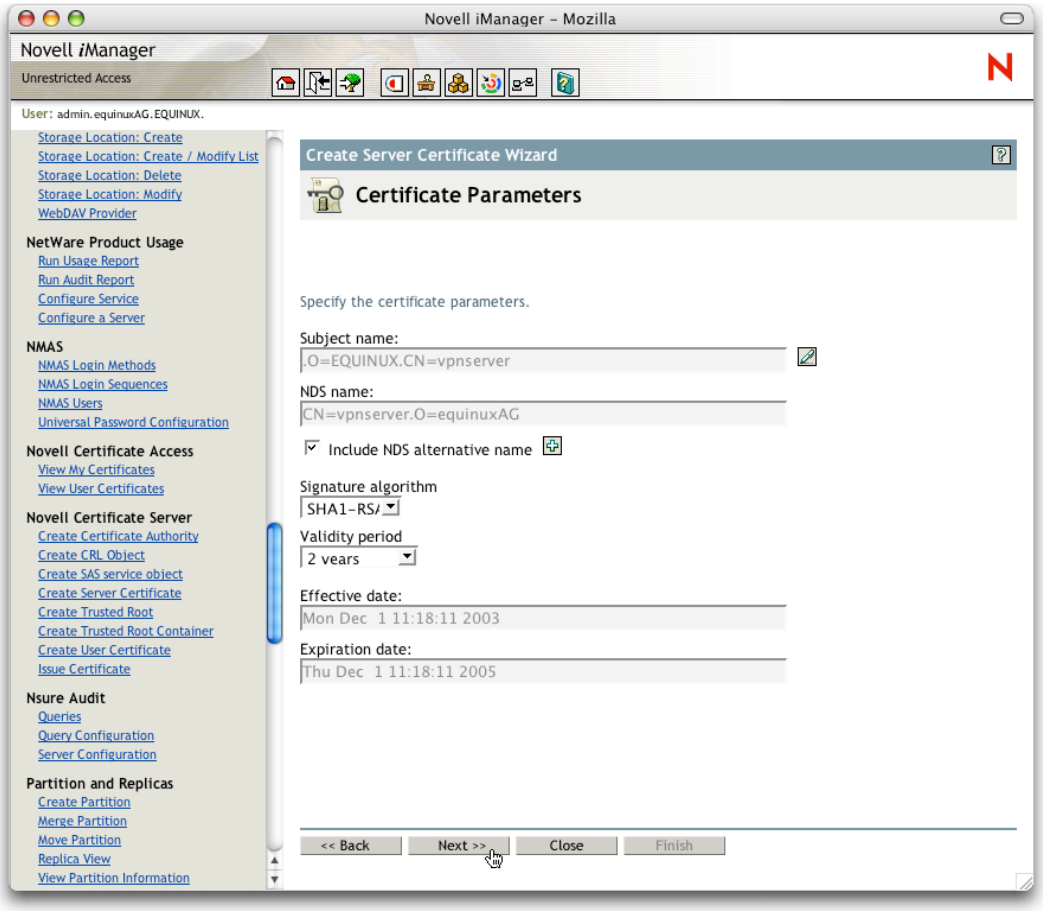

Figure 7: Novell BorderManager - Certificate Parameters

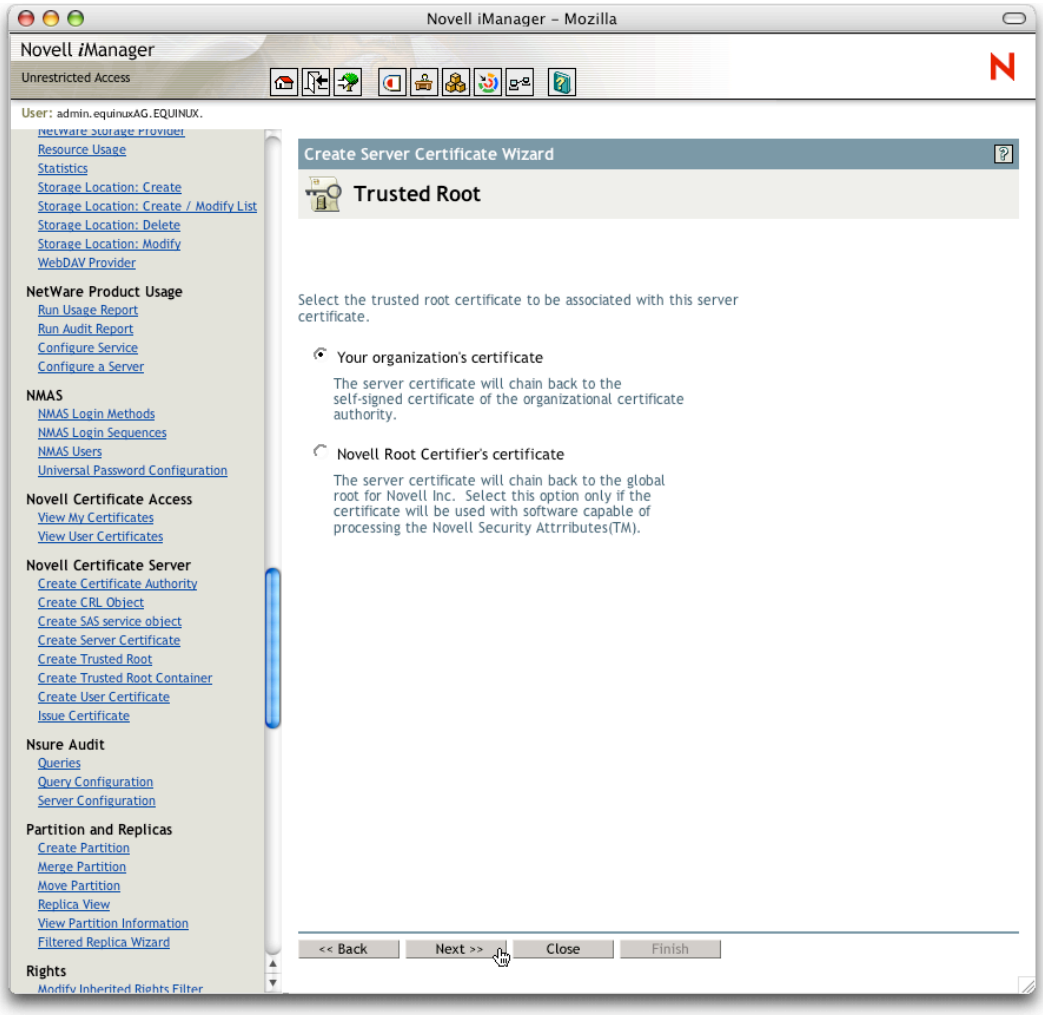

Figure 8: Novell BorderManager - Trusted Root

After **step 3** your configuration should look like this:

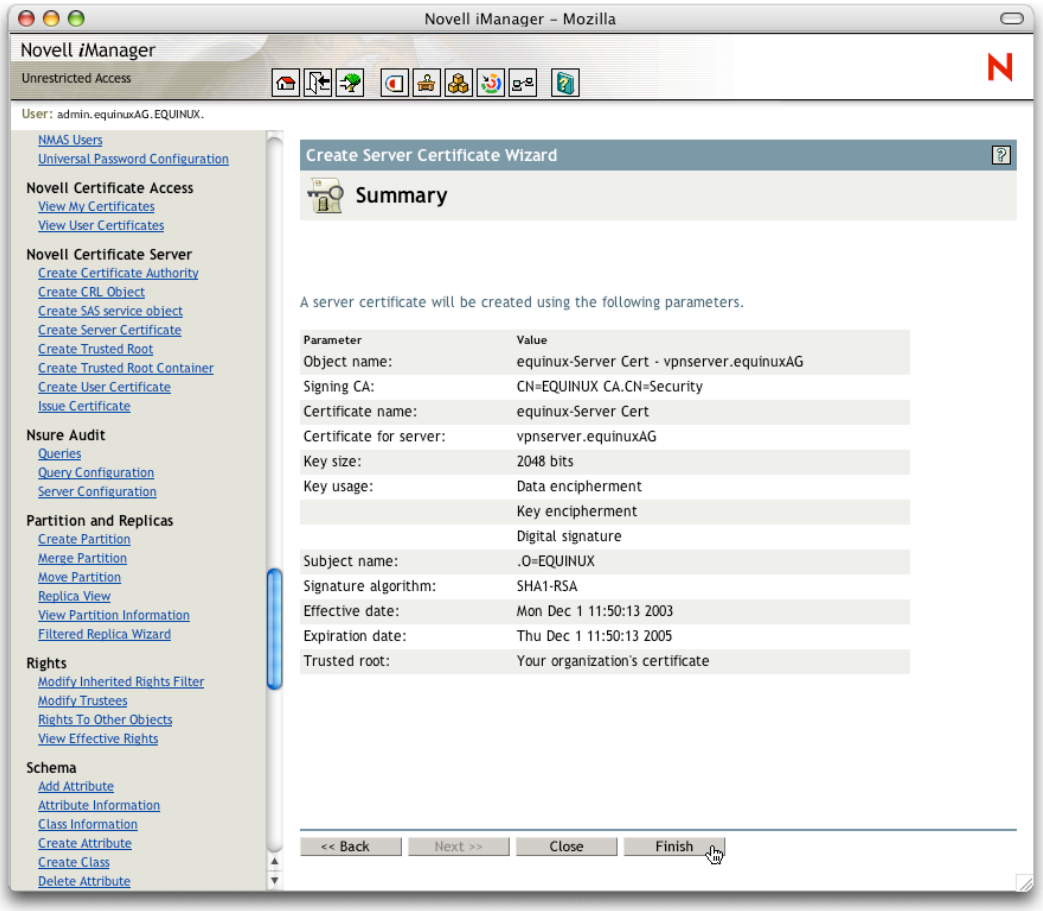

Figure 9: Novell BorderManager – Summary

Step 4 Please create a new Certificate Signing Request (CSR) in the VPN Tracker Certificates menu, Tab “Request”.

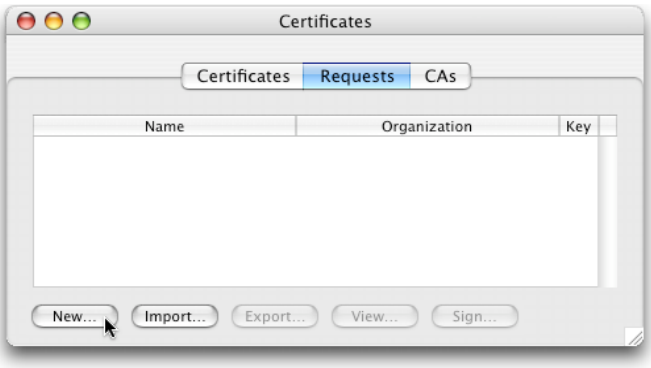

Figure 10: VPN Tracker – Certificates

Enter your details, then save and export the request in the .pem format.

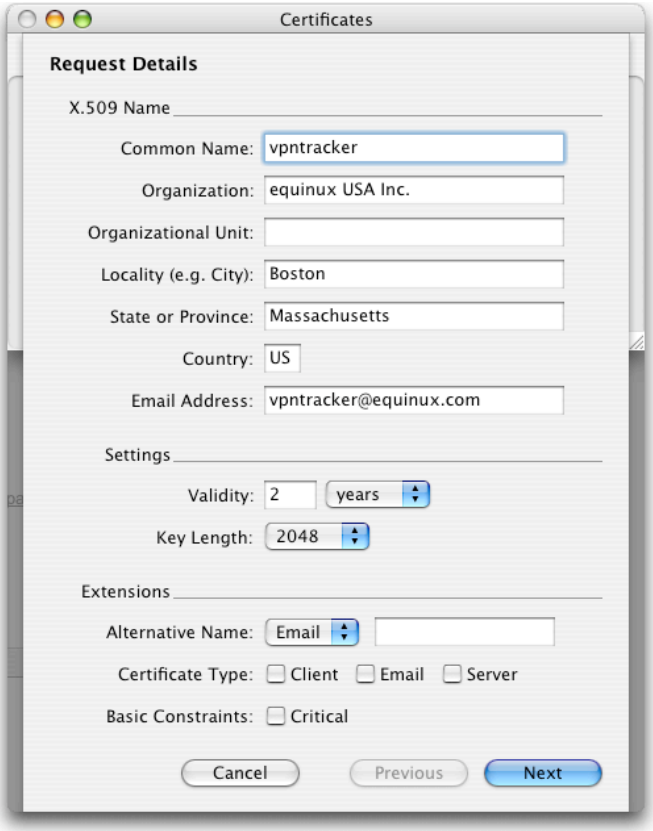

Figure 11: VPN Tracker - Certificate Request Details

Step 5 Import and sign the request you have created in VPN Tracker.

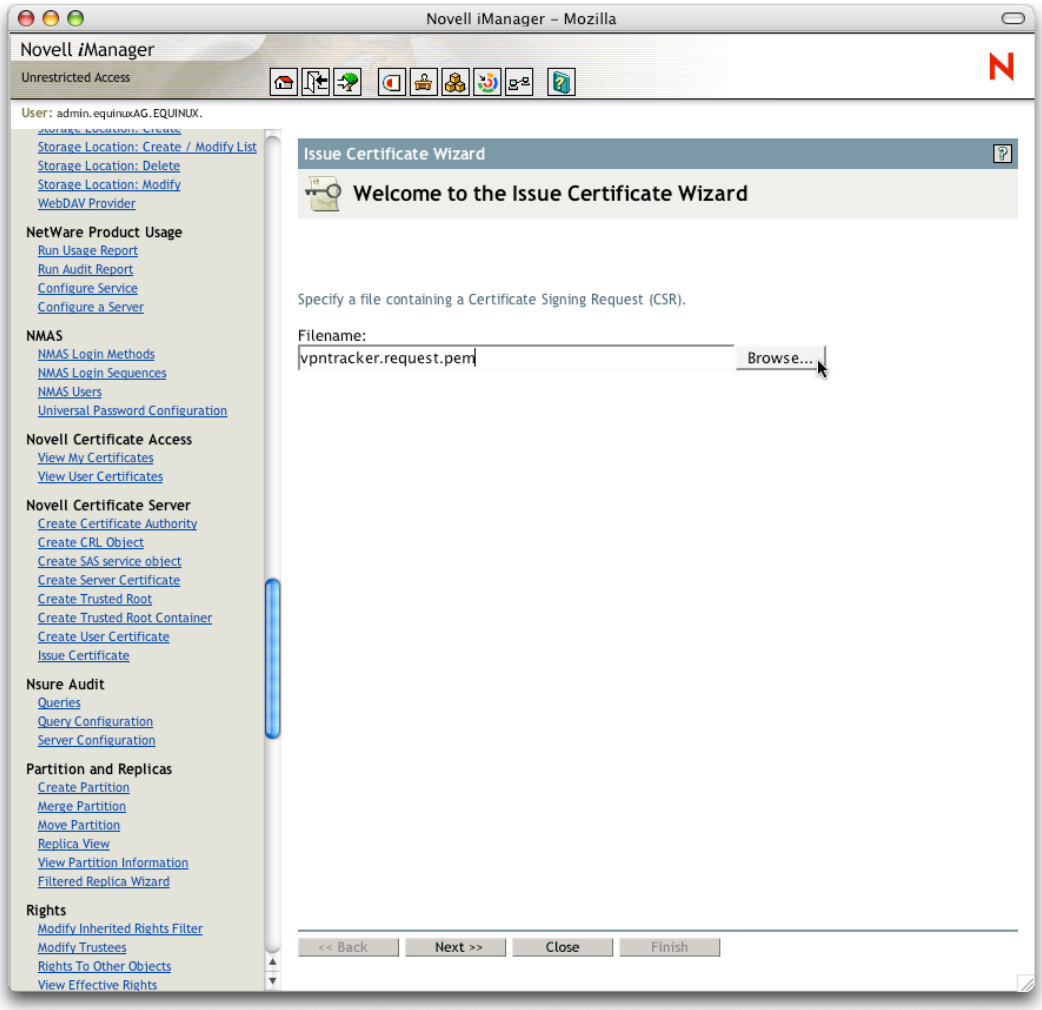

Figure 12: Novell BorderManager - Issue Certificate Wizard

Please refer to **step 3** for the settings of the next two screens.

Save the certificate in binary DER format.

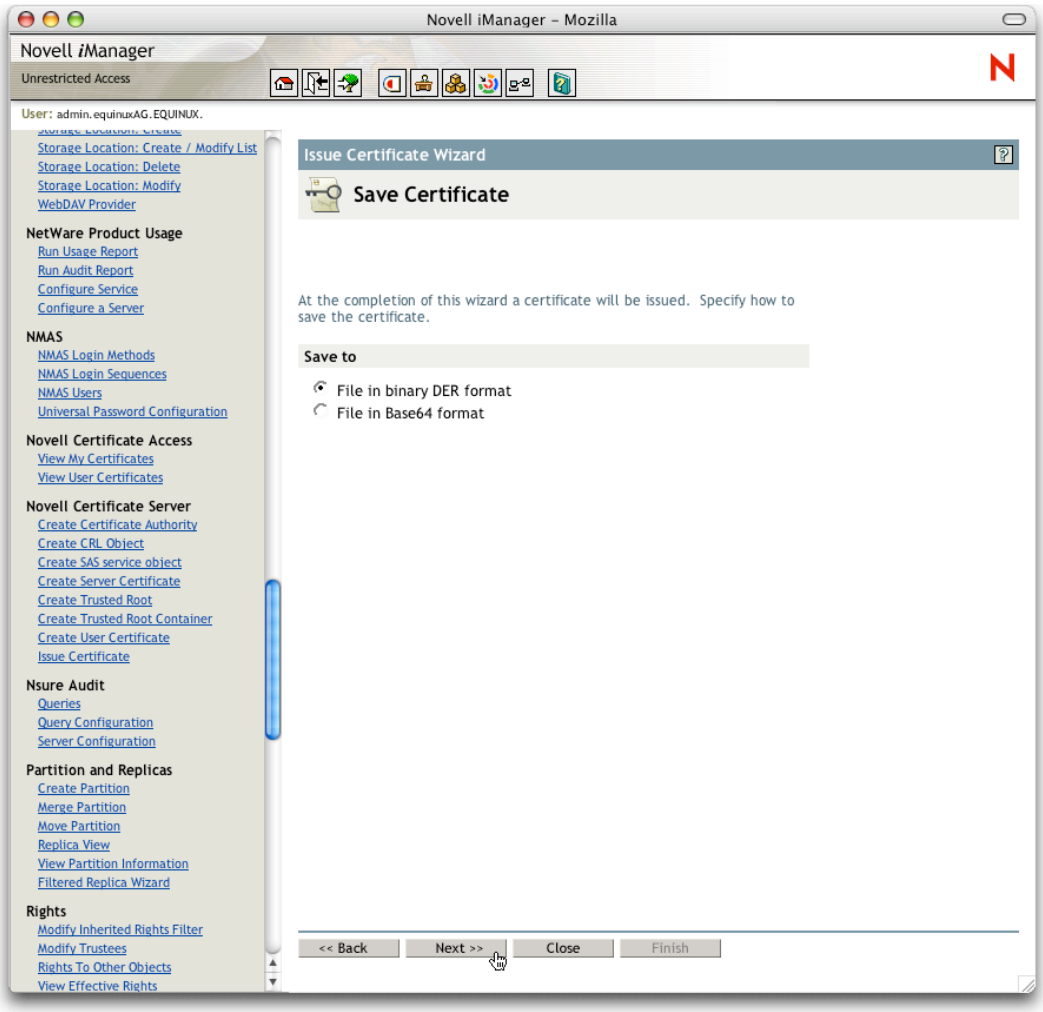

Figure 13: Novell BorderManager - Save Certificate

Finally save the certificate to your disk and import it into VPN Tracker.

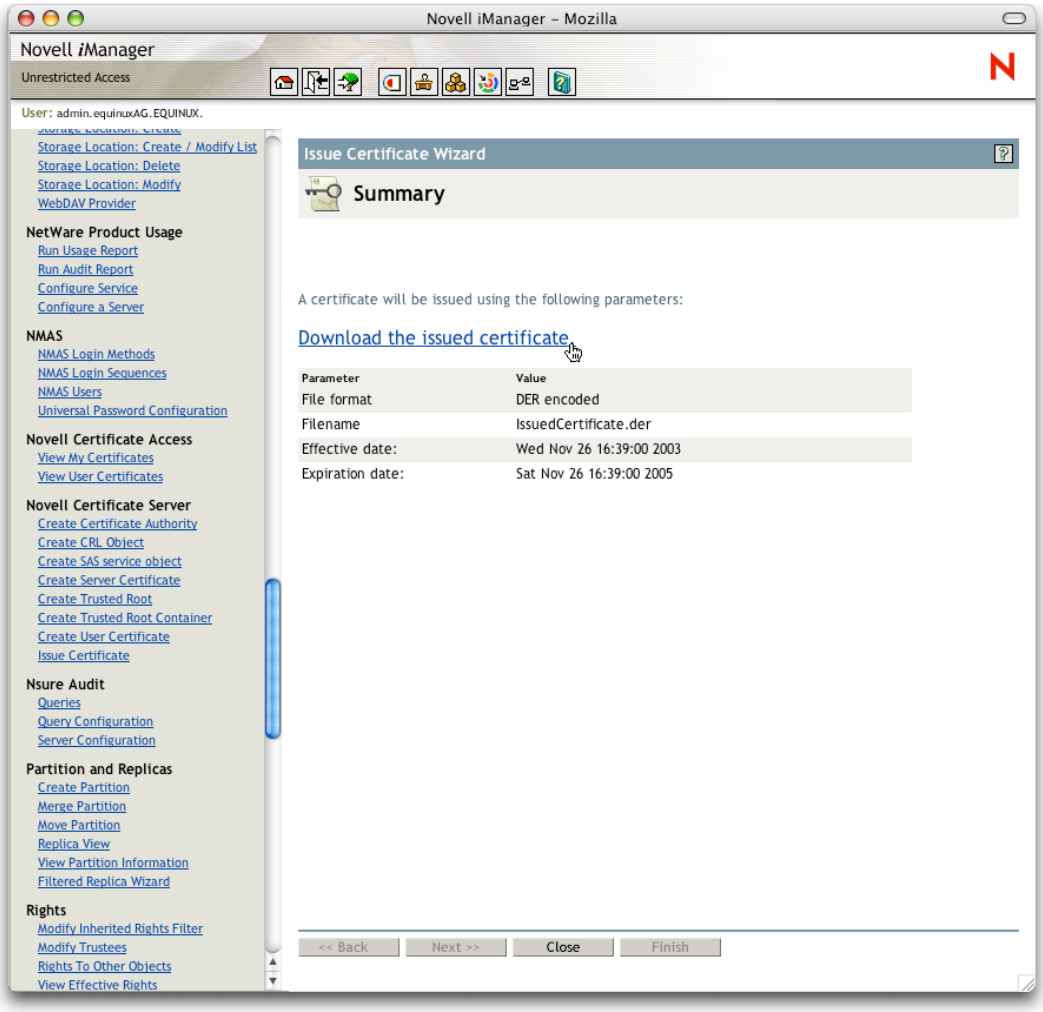

Figure 14: Novell BorderManager - Download Certificate

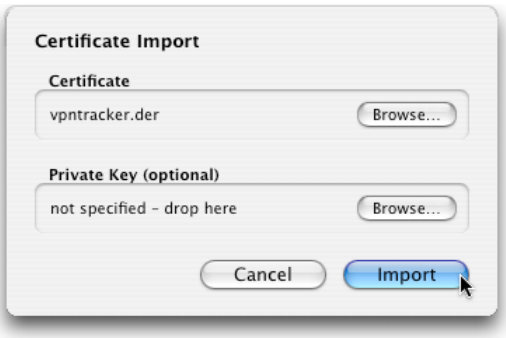

Figure 15: VPN Tracker - Import Signed Certificate

3.2 Novell BorderManager VPN Client to Site Configuration

Now you should have all the objects required to configure VPN services. Next we'll need to setup the VPN Client To Site Configuration, which we'll later need for the VPN Server Configuration.

Step 1 Please click on "Default_C2S_Service_yourContext" under "NBM Client To Site Configuration".

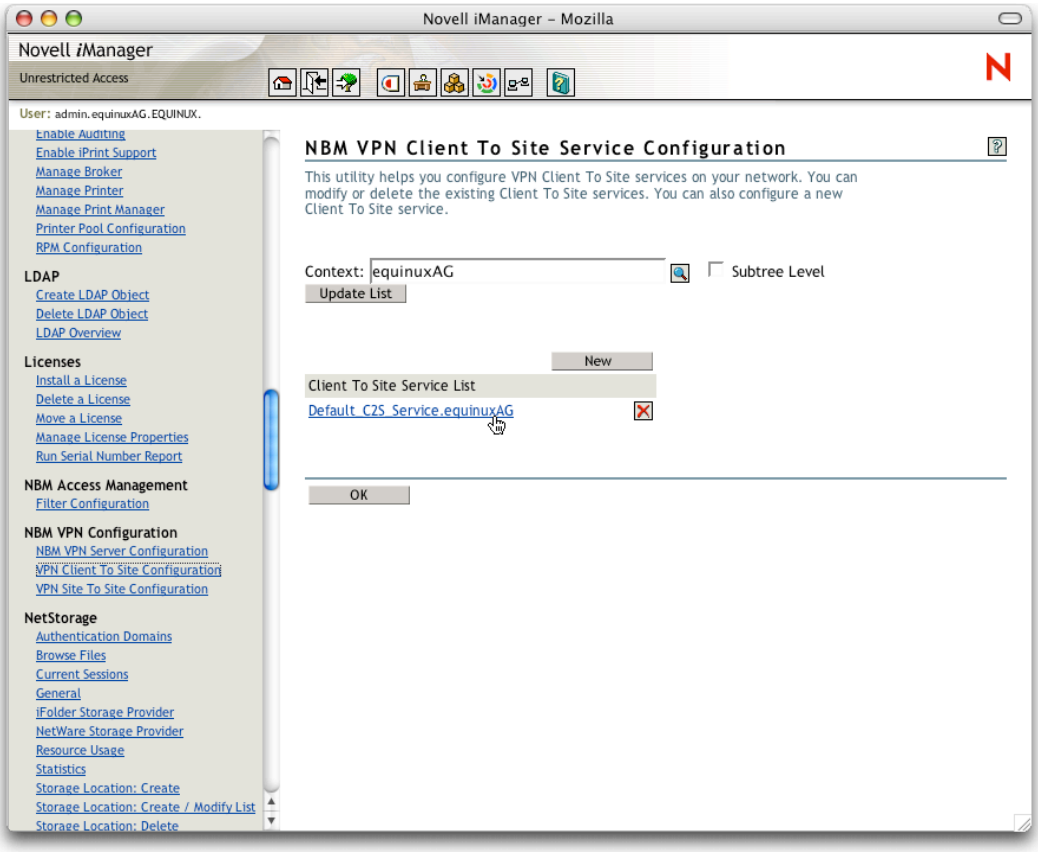

Figure 16: Novell BorderManager - Client To Site Service List

Step 2 Select the Trusted Root Container we've created before and click on apply.

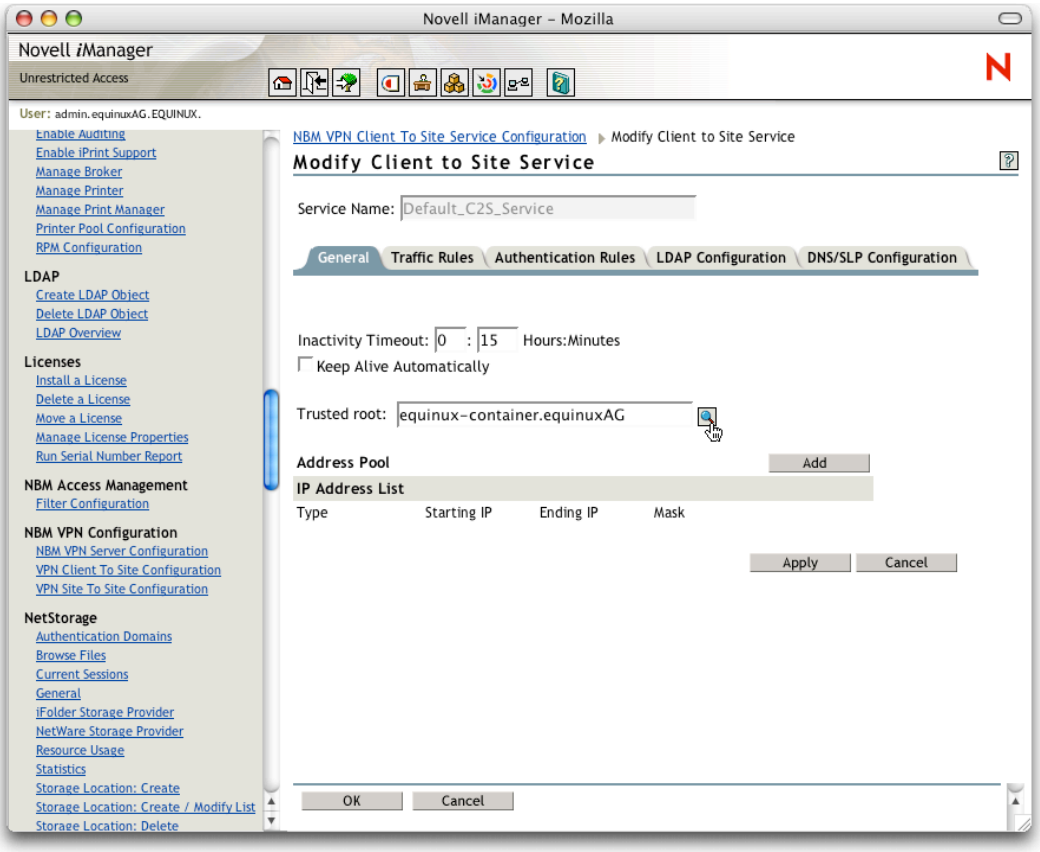

Figure 17: Novell BorderManager - Client to Site General

Step 3 Now click on Traffic Rules and change the “Default rule action” to “Encrypt”.

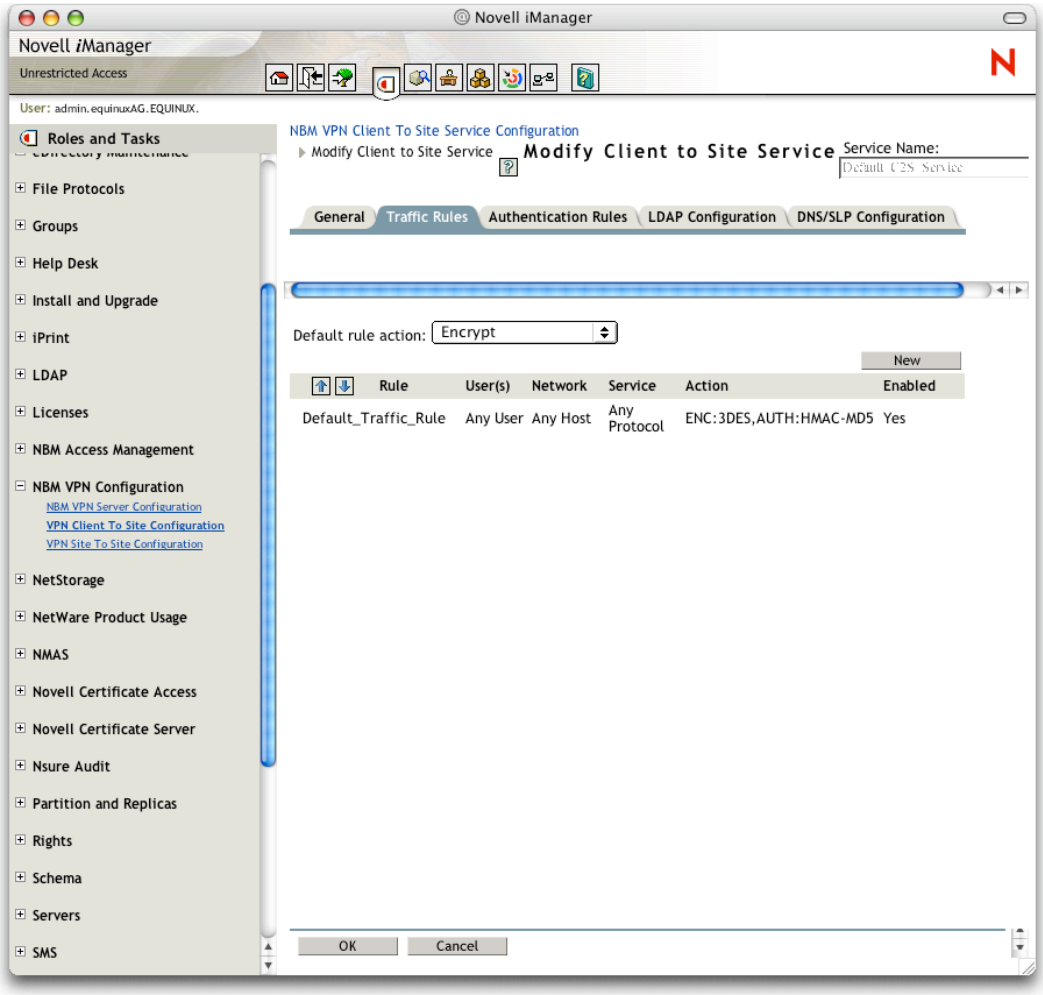

Figure 18: Novell BorderManager - Client to Site Traffic Rule

Step 4

Finally click on Authentication Rules and add a new Rule. Enter an arbitrary name for the rule, check “Allow Certificate Authentication” and “Trust Server CA” under Authentication Condition and add your Trusted Root to the “Issuer List”.

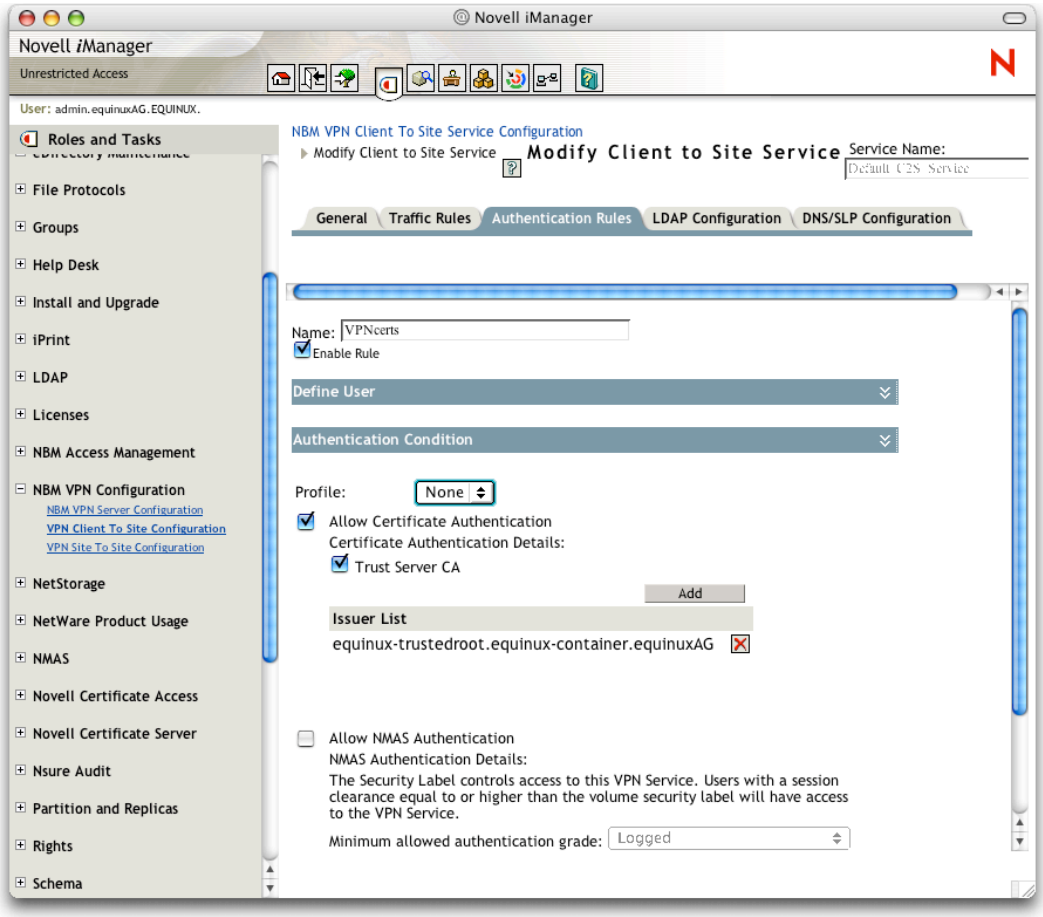

Figure 19: Novell BorderManager - Client to Site Authentication Rules

Then just click on Apply and Ok to save your settings. We’ve now configured the authentication method (certificates) and the authentication algorithms. In the next step we’ll add these settings to the VPN Server Configuration.

3.3 Novell BorderManager VPN Server Configuration

Step 1

Please click on "NBM VPN Server Configuration" and add a new server. Select the correct Server and click on Next.

In the Server Properties screen enter the public IP and Netmask of your Novell BorderManager Server as "Server Address" and an arbitrary Tunnel Address. Please make sure, that the "Tunnel Address" is not in the real LAN subnet.

Also select the "Server Certificate" and the "Trusted Root" we've created in section 3.1.

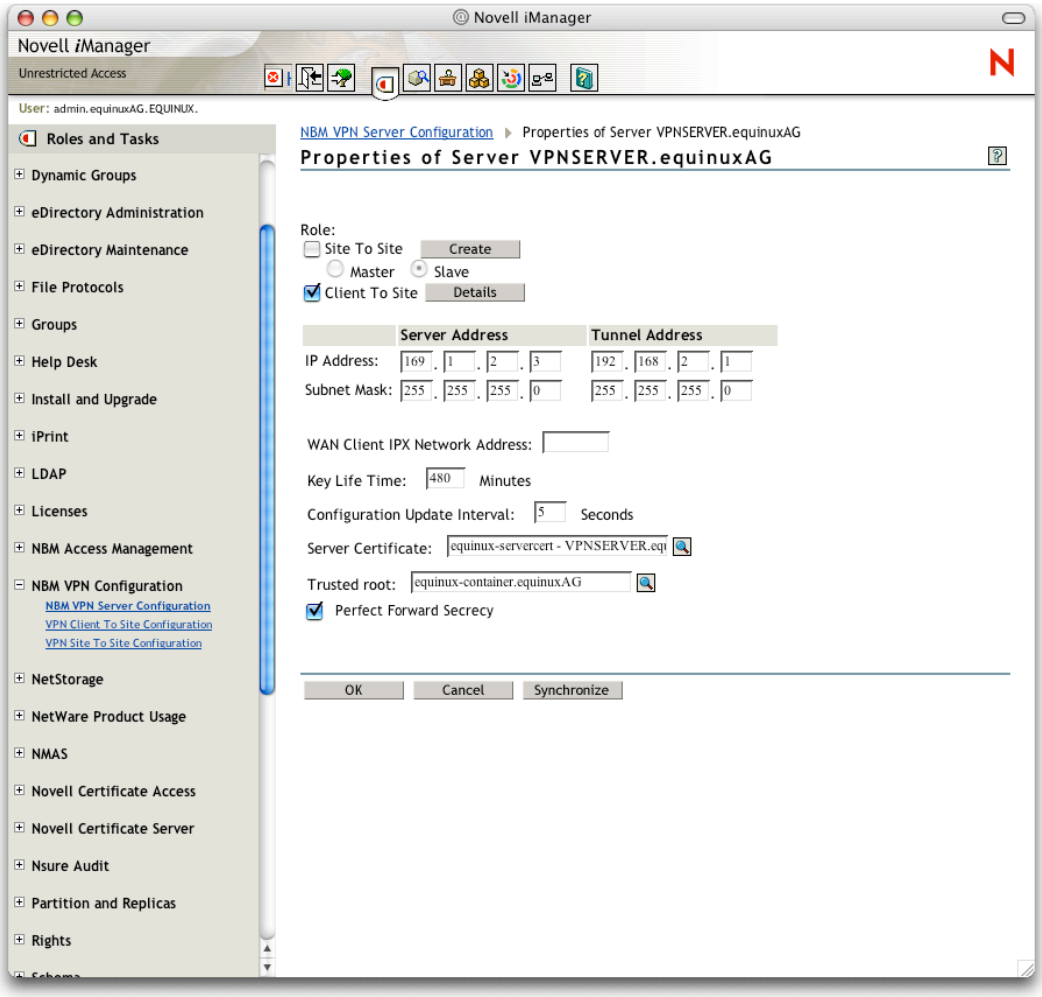

Figure 20: Novell BorderManager - VPN Server Configuration

Step 2

Please make sure, that “Client To Site” is checked and click on details to select the “Default_C2S_Service.yourContext” VPN Service.

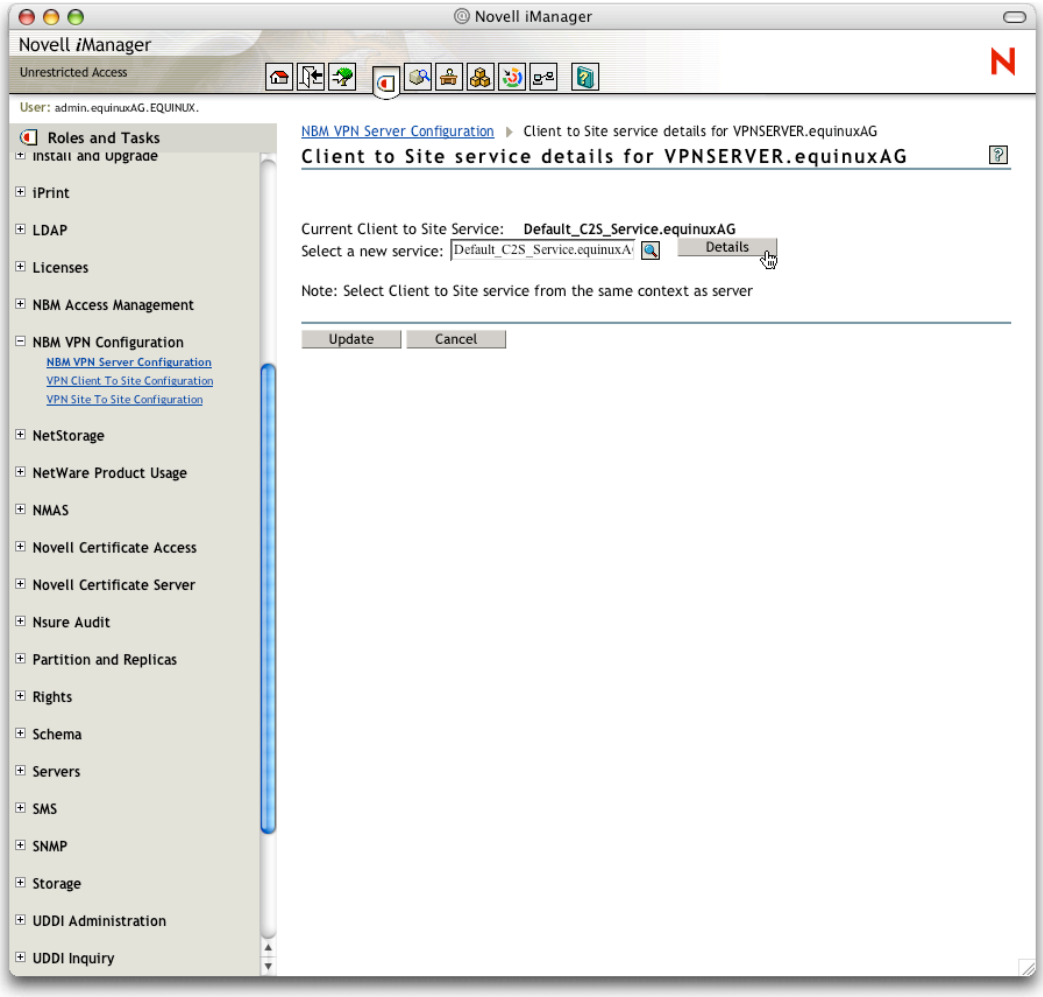

Figure 21: Novell BorderManager - Select Client To Site Service

Finally update and save your VPN Server Configuration. Now all the configuration steps on the Novell BorderManager side are done and we can go over to the VPN Tracker configuration.

3.4 VPN Tracker Configuration

Step 1 Add a new connection with the following options: Choose „Novell BorderManager“ as the Connection Type, „Host to Network“ as Topology, then type in the remote endpoint (169.1.2.3) and the remote network (192.168.1.0/24).

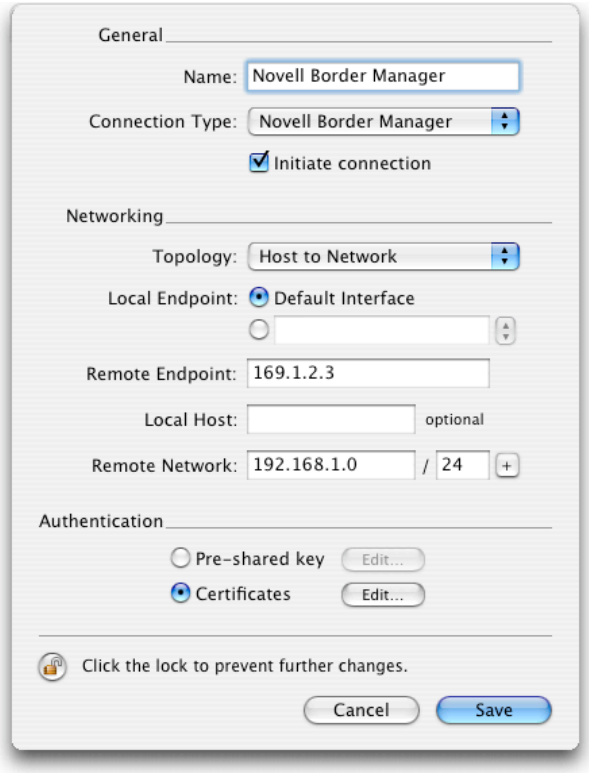

Figure 22: VPN Tracker - Main Window

Step 2

Select „Certificates“ as “Authentication” method and click on “Edit...”.

Choose the certificate you’ve created with VPN Tracker and Novell BorderManager as “Own Certificate and verify the remote certificate “with CAs”.

Change the “Local/Remote” Identifier to Own/Remote certificate.

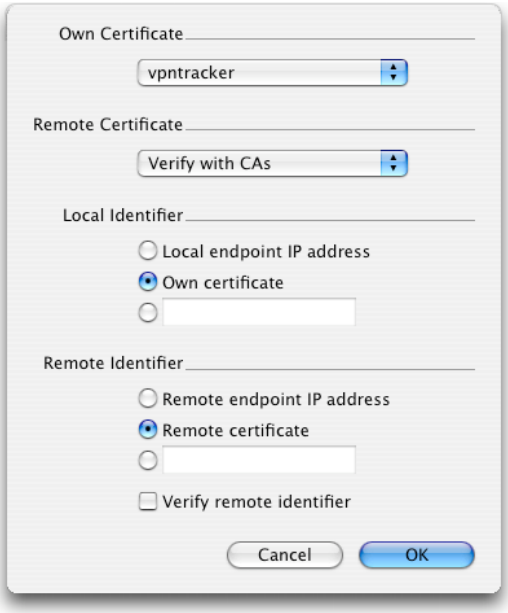

Figure 23: VPN Tracker - Certificate Dialog

Step 3

Save the connection and Click „Start IPsec“ in the VPN Tracker main window.

You’re done. After 10-20 seconds the red status indicator for the connection should change to green, which means you’re securely connected to the Novell BorderManager Server. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Now to test your connection simply ping a host in the Novell BorderManager Server network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.1
```

Debugging

If the status indicator does not change to green please have a look at the log file on both sides. You can define the amount of information available in the log file in the VPN Tracker preferences.