

Draytek IPSec VPN with Windows Vista

Update 18-09-2007: [Jacco de Leeuw](#) correctly pointed out that DES should be disabled in the IPSec general settings.

This tutorial will show the steps needed to connect a Windows Vista client computer to a Draytek using an IPSec VPN tunnel. Please check for the latest version of this tutorial on www.fiereworks.nl, since new security issues could require different steps. If you find any errors, please contact me at www.fiereworks.nl/contact.html.

Note: These steps are created using a Draytek Vigor 2700 Series. Therefore some settings will not be available on other models, or placed elsewhere within the router's menu.

Draytek settings

IPSec general settings

1. Login to the router by entering the IP address into your favorite web browser (e.g. Internet Explorer).
2. Navigate to IPSec General Setup and enter your Pre-Shared Key. Create one using this excellent [secure password generator](#). Be sure to remember the password!
3. Deselect the Medium (AH) and High (ESP) DES IPSec security methods.

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

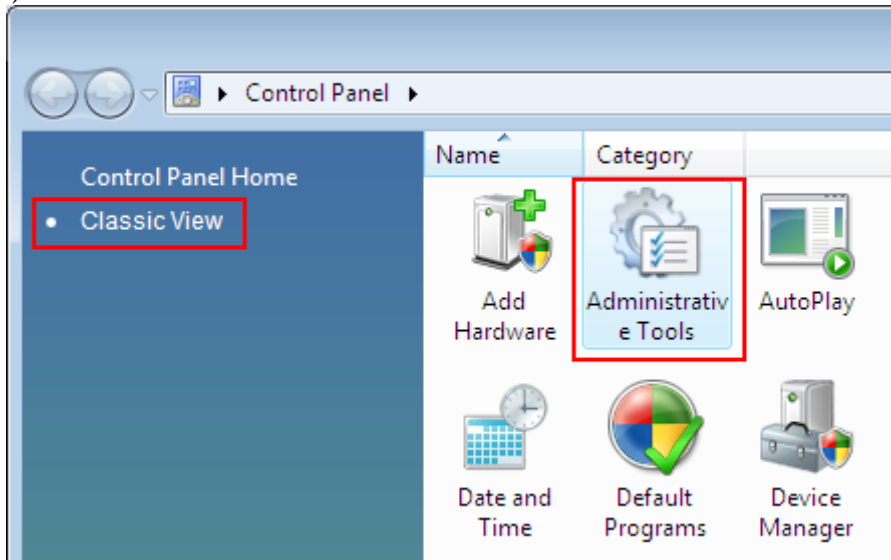
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method	
Pre-Shared Key	<input type="text" value="*****"/>
Re-type Pre-Shared Key	<input type="text" value="*****"/>
IPSec Security Method	
<input type="checkbox"/> Medium (AH)	Data will be authentic, but will not be encrypted.
High (ESP) <input type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	Data will be encrypted and authentic.

Windows Vista IPSec settings

Note: when performing the steps below to Windows Vista User Account Control (UAC) will ask for your permission to perform a task. You should click continue.

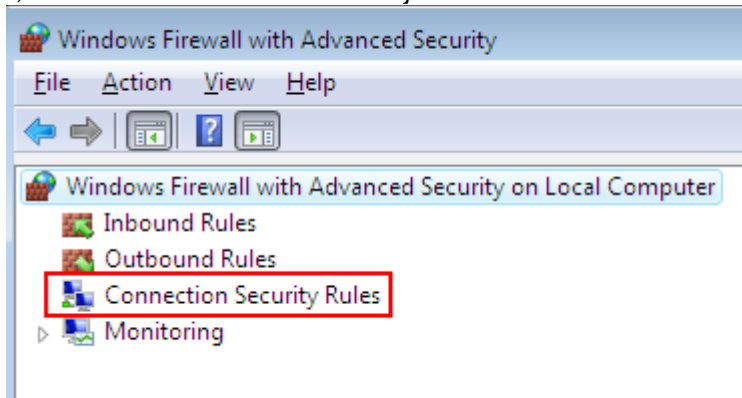
1) Browse to Control Panel -> Choose Classic View -> Administrative Tools



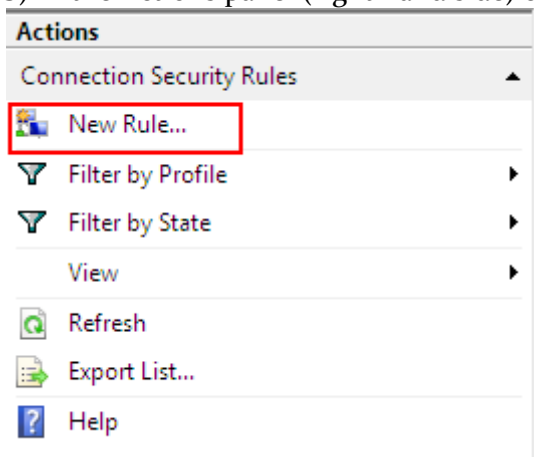
2) In the Administrative Tools menu select Windows Firewall with Advanced Security (UAC asks permission)

3)

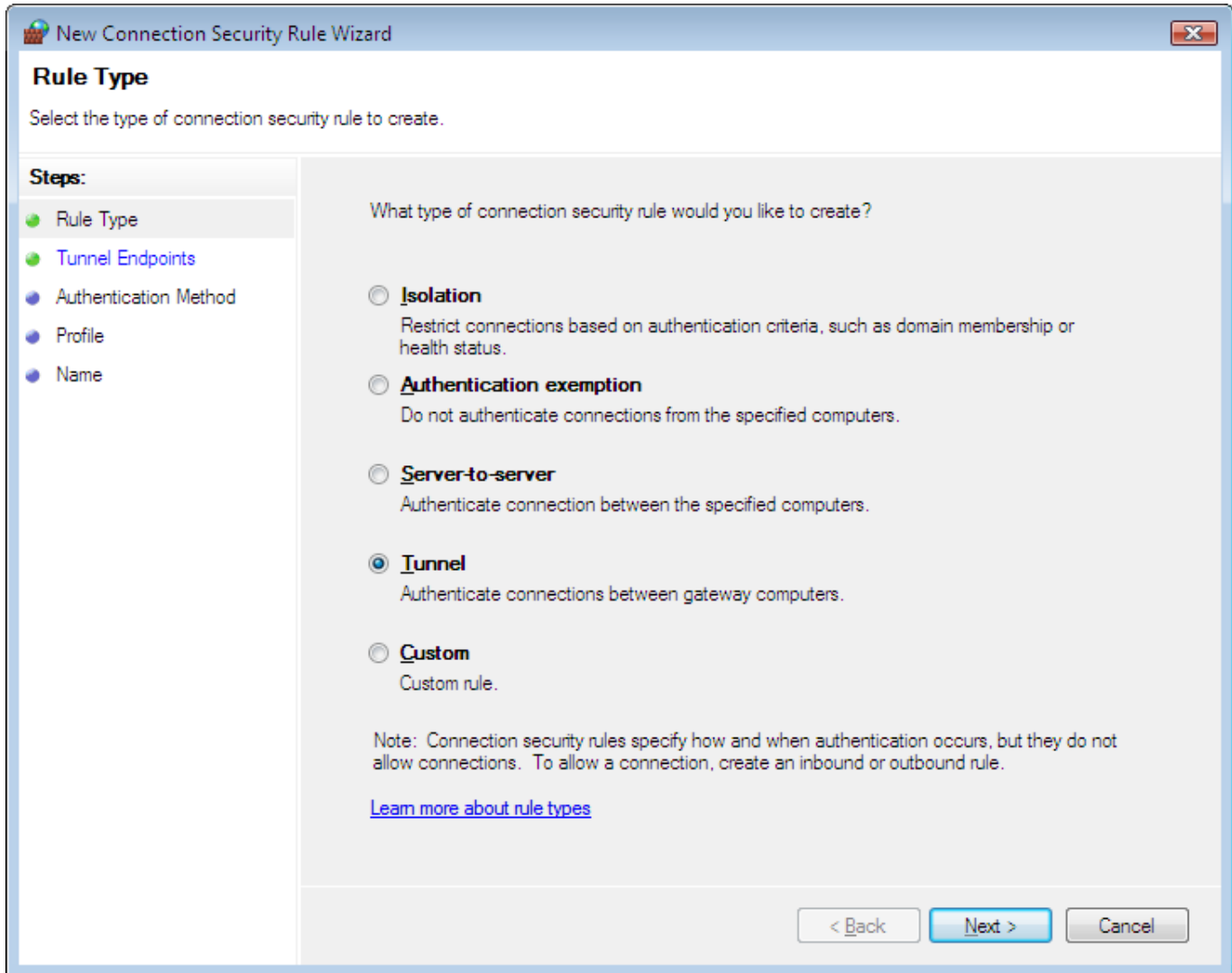
a) Select the connection security rules in the Windows Firewall with Advanced Security view.



b) In the Actions panel (right hand side) choose New Rule.



4) The New Connection Security Rule Wizard is launched. Select Tunnel and click next.



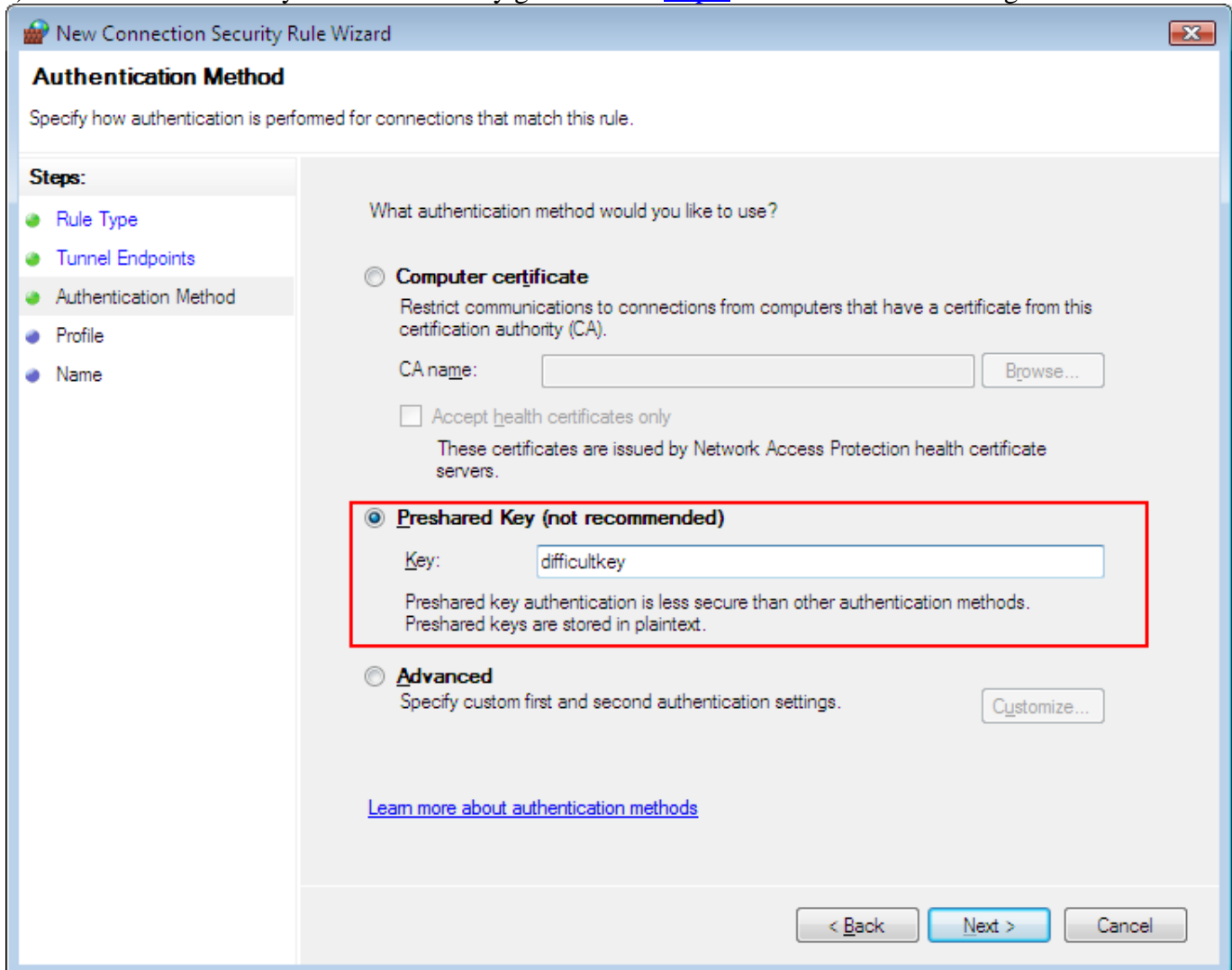
5) Endpoint one concerns the local network settings, and endpoint two concerns the settings of the Draytek router. Use the buttons Add to add a range of IP addresses or a single address. Remote tunnel computer (closest to computers in Endpoint 2) is the WAN IP address of the Draytek router.

Endpoint 2 below is setup as 192.168.2.0/24. This means that access to all the IP addresses in the 192.168.2.x is needed. If you need access to only one computer just insert only that IP address.

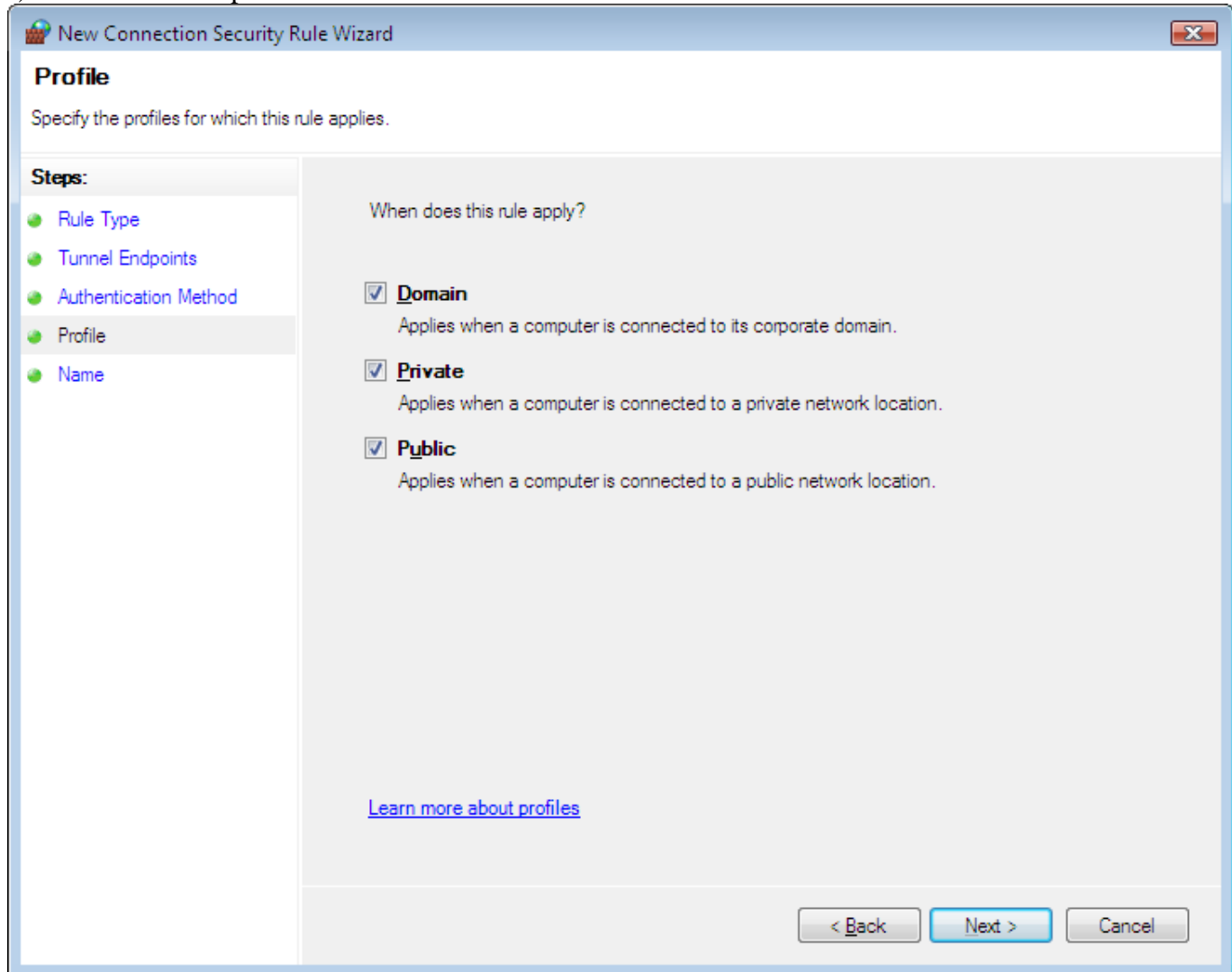
Click Next when settings are complete.

The screenshot shows a Windows-style dialog box titled "New Connection Security Rule Wizard" with a close button in the top right corner. The main heading is "Tunnel Endpoints" and the instruction reads: "Specify the endpoints for the IPsec tunnel defined by this rule." On the left, a "Steps:" sidebar lists "Rule Type", "Tunnel Endpoints", "Authentication Method", "Profile", and "Name", with "Tunnel Endpoints" selected. The main area contains explanatory text: "Connections from Endpoint 1 to Endpoint 2 will pass through the specified tunnel endpoints. Tunnel endpoints are generally gateway servers." It then asks "Which computers are in Endpoint 1?" with a text box containing "192.168.1.1" and buttons for "Add...", "Edit...", and "Remove". Below this, it asks "What is the local tunnel computer (closest to computers in Endpoint 1)?" with fields for "IPv4 address:" (containing "192.168.1.1") and "IPv6 address:". It then asks "What is the remote tunnel computer (closest to computers in Endpoint 2)?" with fields for "IPv4 address:" (containing "202.211.200.241") and "IPv6 address:". Finally, it asks "Which computers are in Endpoint 2?" with a text box containing "192.168.2.0/24" and buttons for "Add...", "Edit...", and "Remove". A link "Learn more about tunnel endpoints" is present. At the bottom are buttons for "< Back", "Next >", and "Cancel".

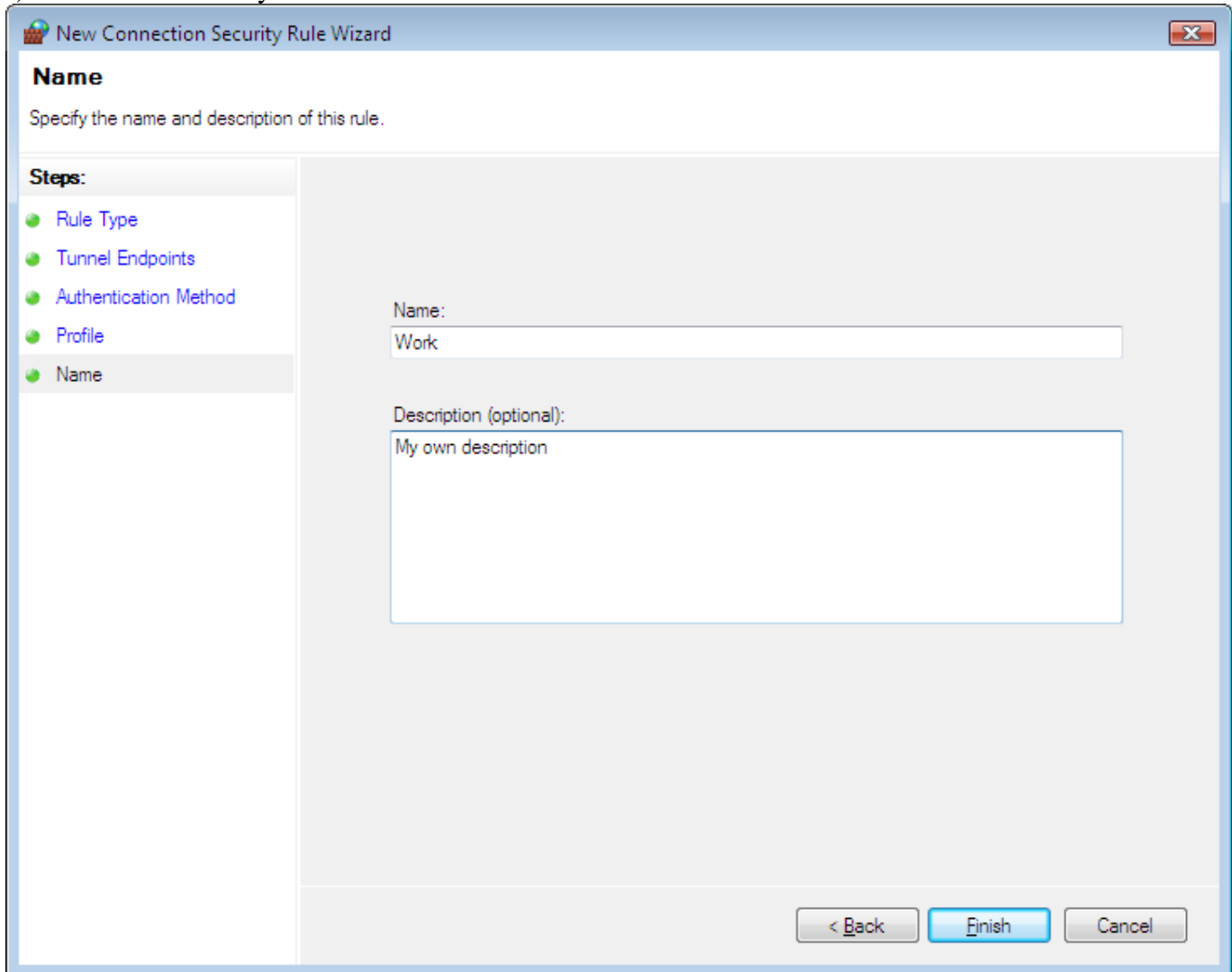
6) Choose Preshared Key and insert the key generated in [step a](#) of General IPsec settings.



7) Select when this profile should be active. In our case we select all the fields.



8) Choose a name for your rule and click finish.



9) You should see your rule in the Connection Security Rules

Name	Enabled	Endpoint 1	Endpoint 2	Authentication mode	Authentication method	Group
Work	Yes	192.168.1.1	192.168.2.0...	Require inbound and outbound	Custom	