Written by Marc Grote – www.it-training-grote.de

Configuring Forefront TMG client VPN access with NAP

Abstract

This article will show you how to configure Forefront TMG for VPN client access with NAP (Network Access Protection).

Let's begin

In this article I will show you only the required steps to configure Forefront TMG VPN client access for NAP. The article will not cover how to configure Forefront TMG as a VPN Server for VPN client access and for this article I assume that Forefront TMG is correctly configured as a VPN Server so we will cover only the required changes to enable Forefront TMG VPN for NAP. If you want to know more about how to configure Forefront TMG as a VPN Server for VPN client access, read the following article.

Configuring Forefront TMG for VPN access with NAP is a three part process:
1) Configure Forefront TMG for VPN with NAP
2) Configure the NPS Server for NAP
3) Configure the VPN client for NAP

Configure Forefront TMG for VPN with NAP

As mentioned above I assume that Forefront TMG client VPN is already configured and we only have to change the TMG configuration for NAP. Navigate to the VPN properties and to the *Authentication* tab and enable the *EAP* checkbox.

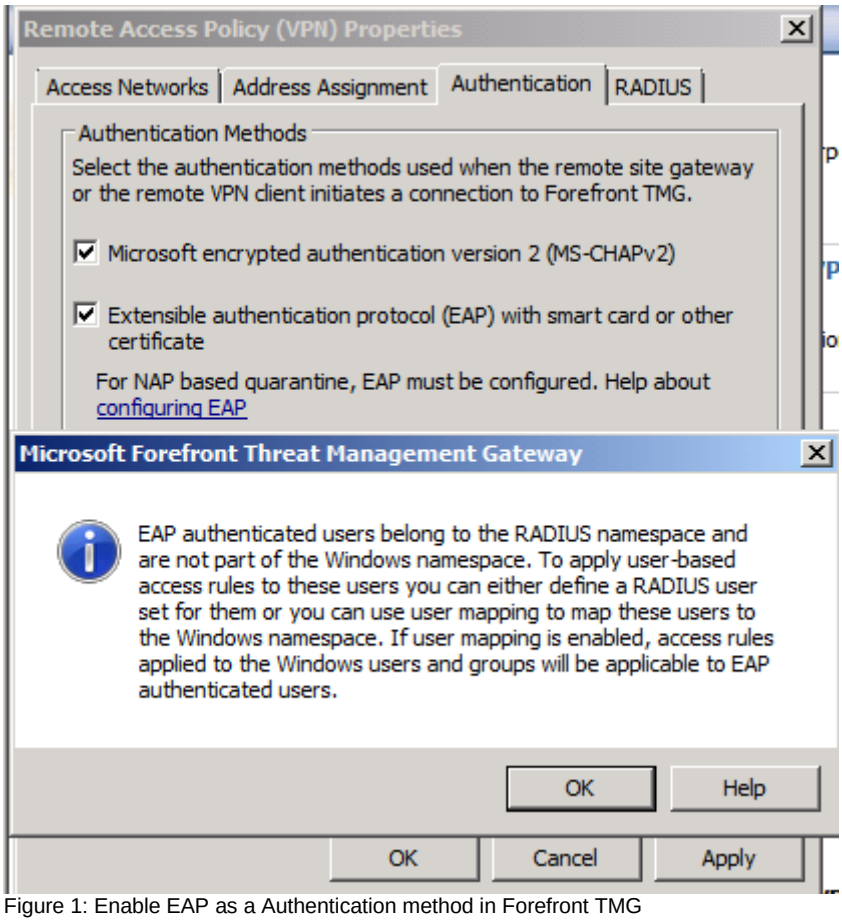

Figure 1: Enable EAP as a Authentication method in Forefront TMG

Specify the NPS Server with the RADIUS Server component. We only use RADIUS for authentication.

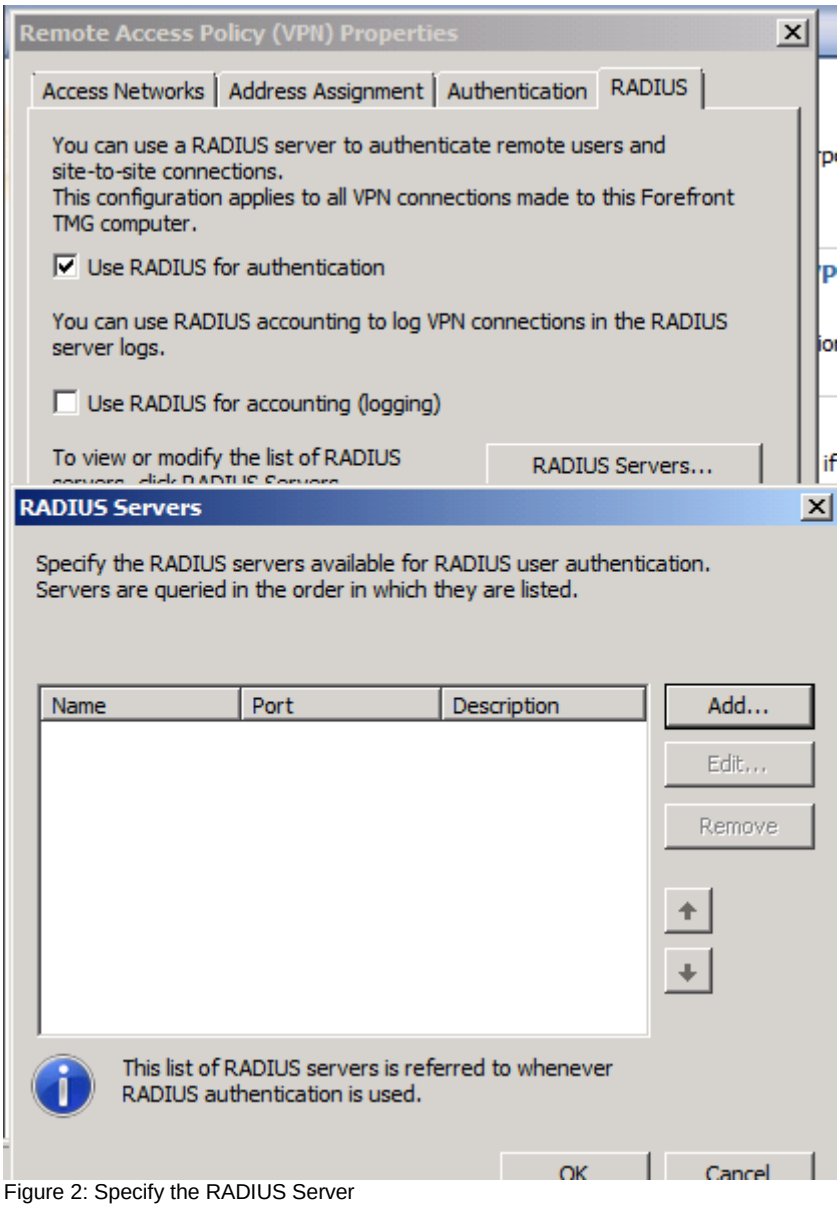

Figure 2: Specify the RADIUS Server

Enter the name of the RADIUS Server, the Authentication port (1812 is default and should not be changed), and the Shared Secret (PSK = PreSharedKey), which is used to authenticate the RADIUS client (Forefront TMG) and the RADIUS Server.

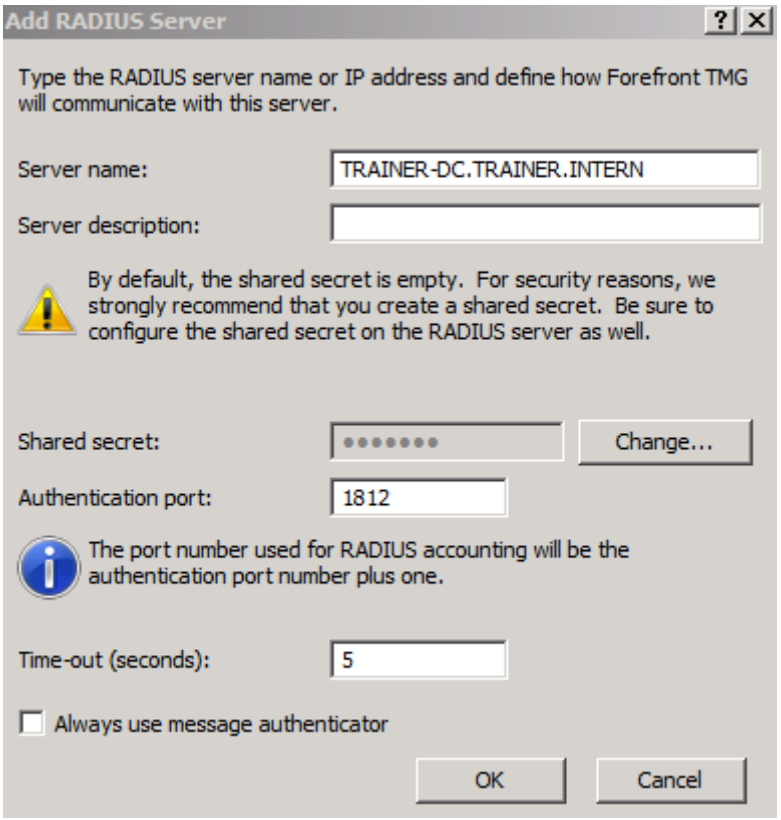

Figure 3: Verify Authentication port and enter the Shared secret

After Forefront TMG is configured as a RADIUS client and RADIUS support is activated, enable VPN client Quarantine on the Quarantine tab. If the NPS Server is not located on the Forefront TMG Server activate the Radio button *Quarantine according to RADIUS server policies*, else use the other radio button.

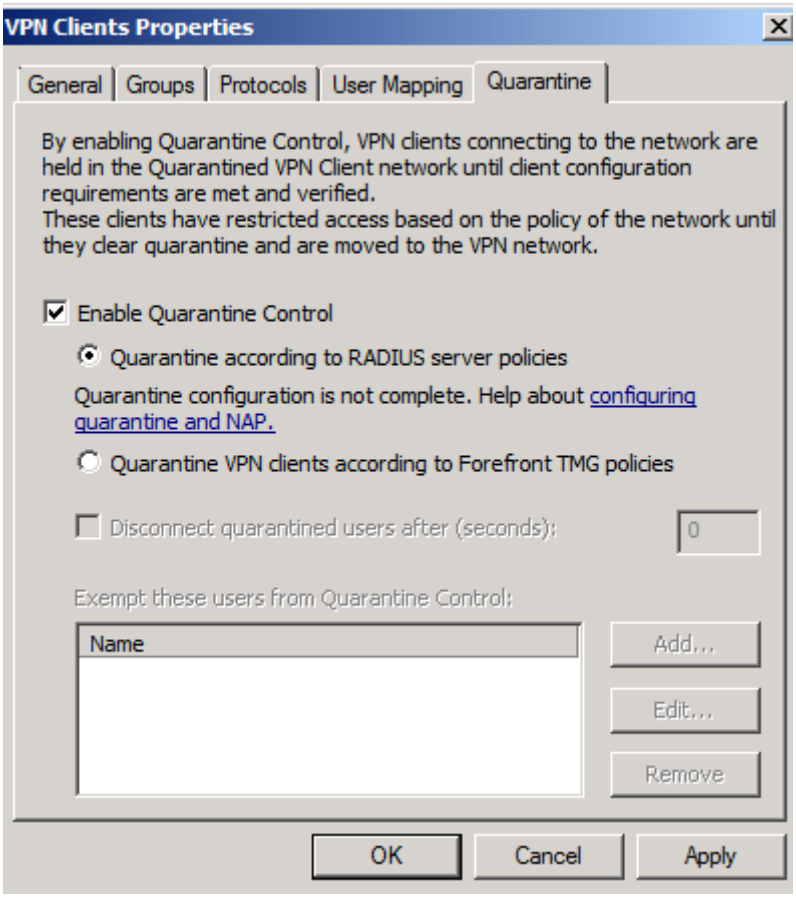

Figure 4: Enable VPN Quarantine Control

If you want to exempt specify users from Quarantine control you can add these users here.

Configure the NPS Server for NAP

The most time consuming part to enable Forefront TMG client access for NAP is the configuration of the NPS Server. If the NPS role is not installed on the Server in the internal network, you have to install the role with the Server Manager of Windows Server 2008/R2.

After the NPS role is installed and correctly configured (don’t forget to register the NPS Server in Active Directory), configure Forefront TMG as a RADIUS client. Start the NPS Server MMC navigate to the RADIUS clients and Servers node and add the Forefront TMG Server as a RADIUS client as shown in the following screenshot.

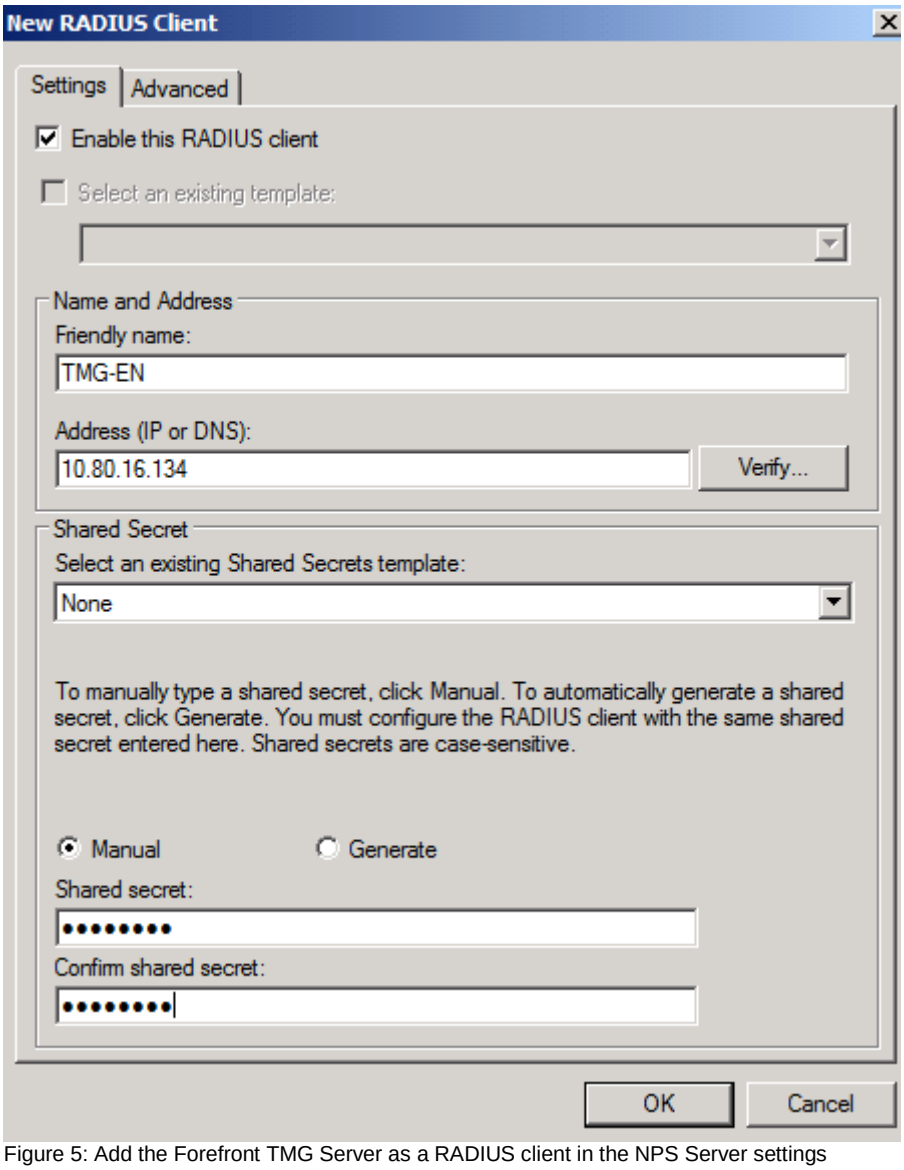

Figure 5: Add the Forefront TMG Server as a RADIUS client in the NPS Server settings

Don’t forget to activate the checkbox that the RADIUS client (the Forefront TMG Server) is NAP-capable.

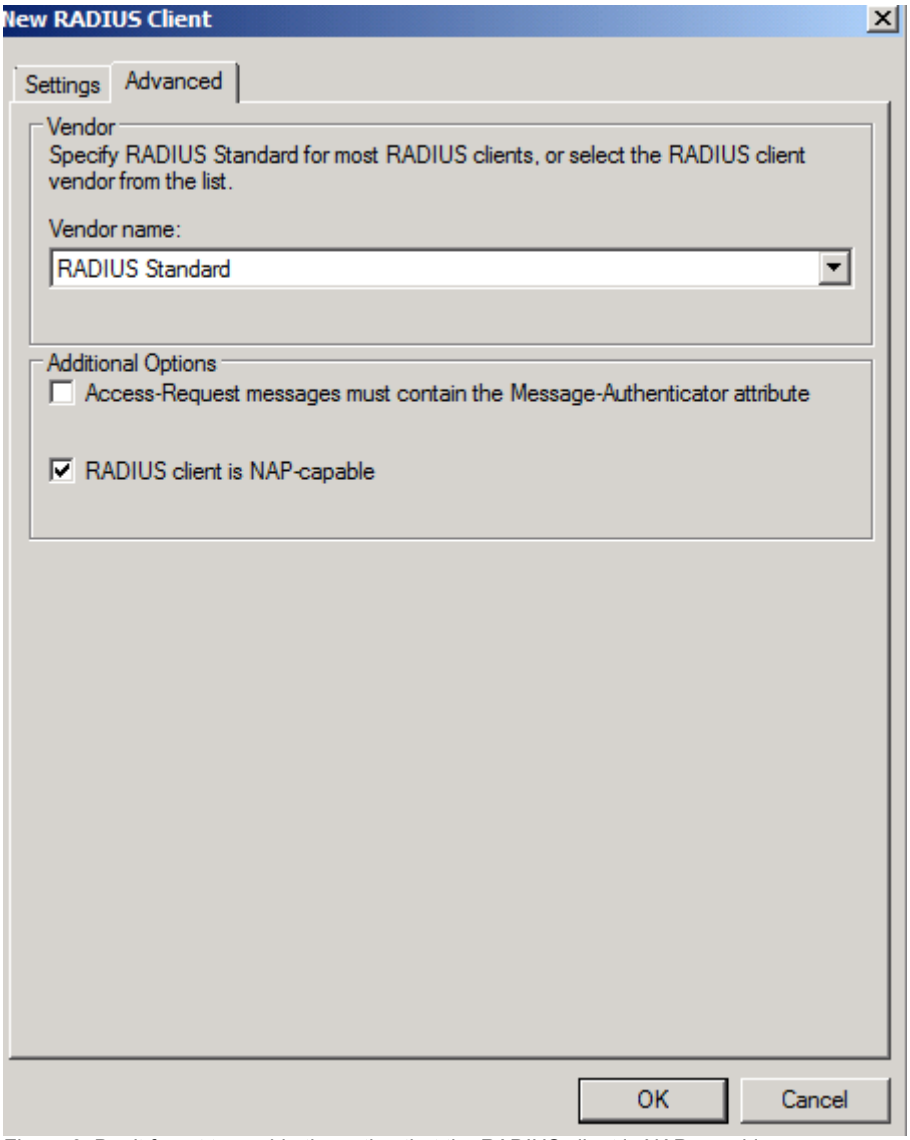

Figure 6: Don't forget to enable the option that the RADIUS client is NAP-capable

Configure the Windows Security Health Validator to verify at the client that only the Windows Firewall must be activated to gain unrestricted access to the corporate network.

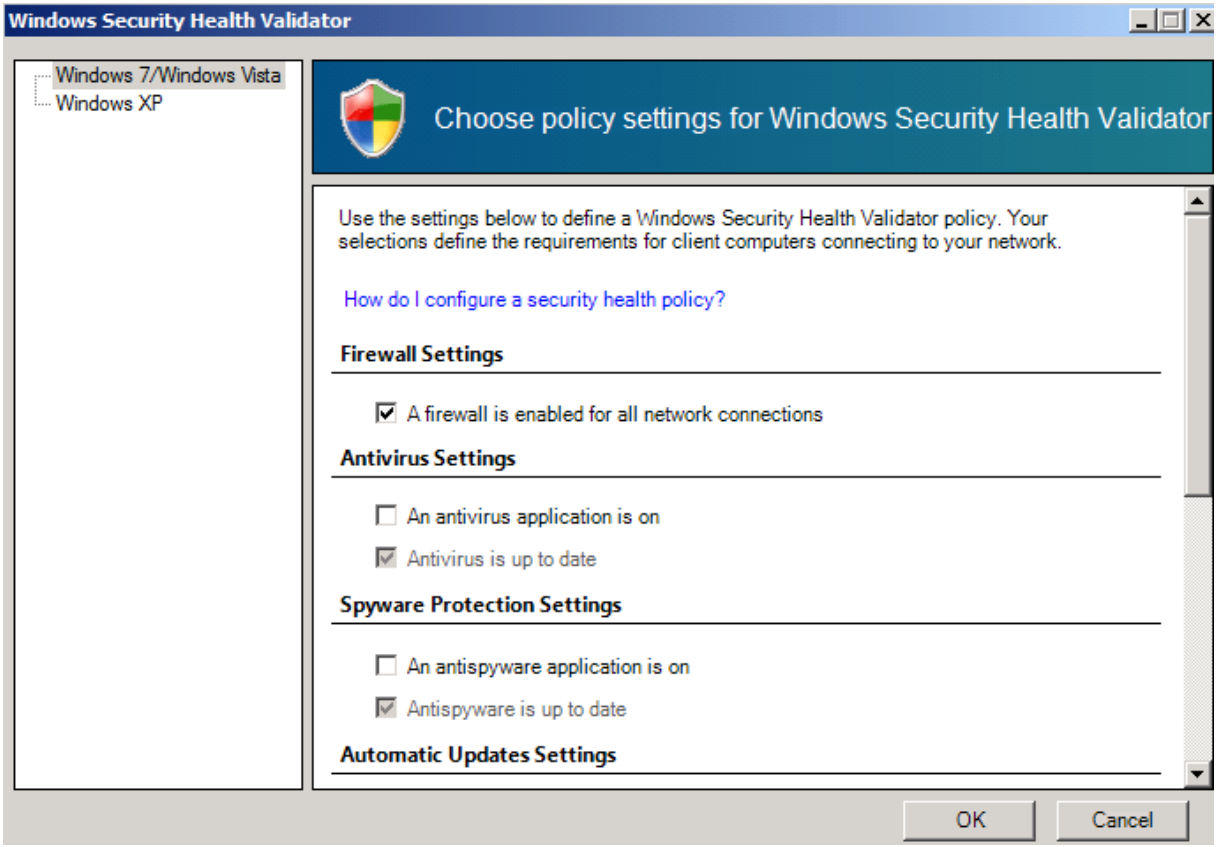

Figure 7: Specify SHV requirements

After we configured the Windows Security Health Validator we have to configure two Health Policies. One Health Policy which makes the VPN client Compliant when the client passes all SHV checks and one Health Policy which makes the VPN client Noncompliant when more than one SHV checks failed. These Health Policies can be used by Network Policies to gain or restrict access for VPN clients.

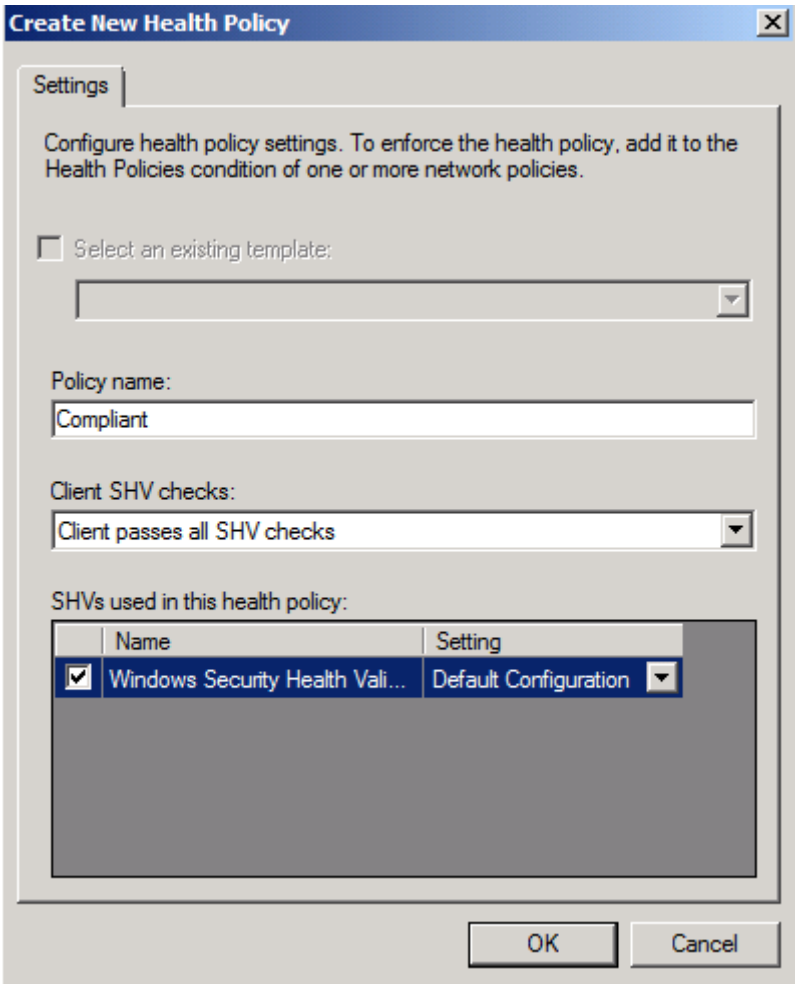

Figure 8: Compliant Health Policy

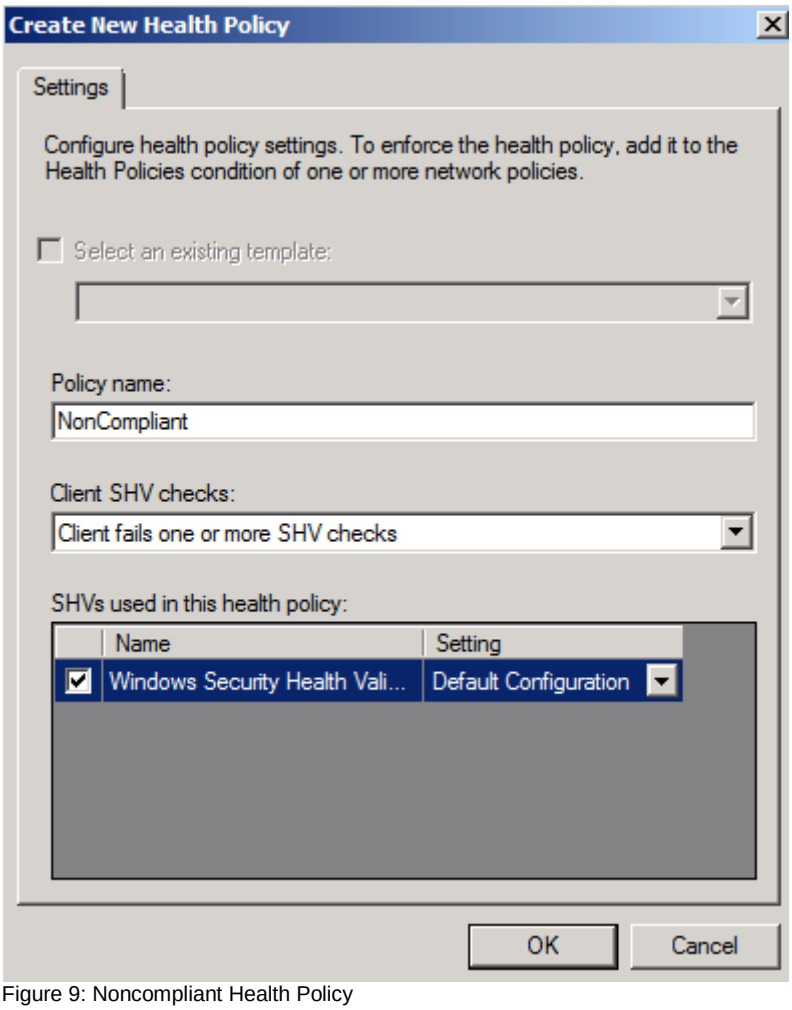

Figure 9: Noncompliant Health Policy

Next we must create new Network Policies for Compliant and Noncompliant VPN clients. In this article I will only show the required steps for creating a Network Policy for compliant VPN clients.

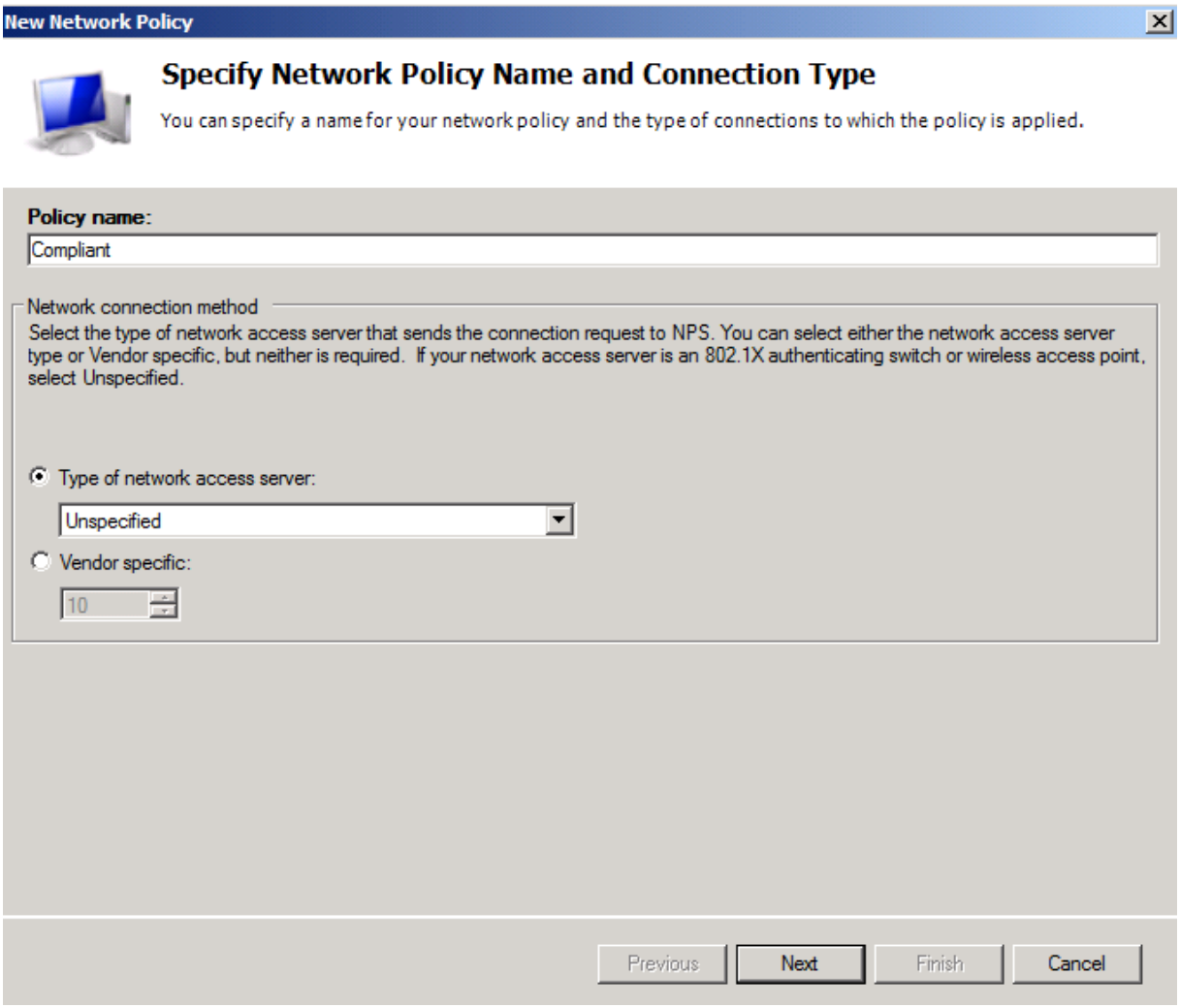

Figure 10: New Network Policy

As a condition select Health Policies and select the previously created Compliant Health Policy.

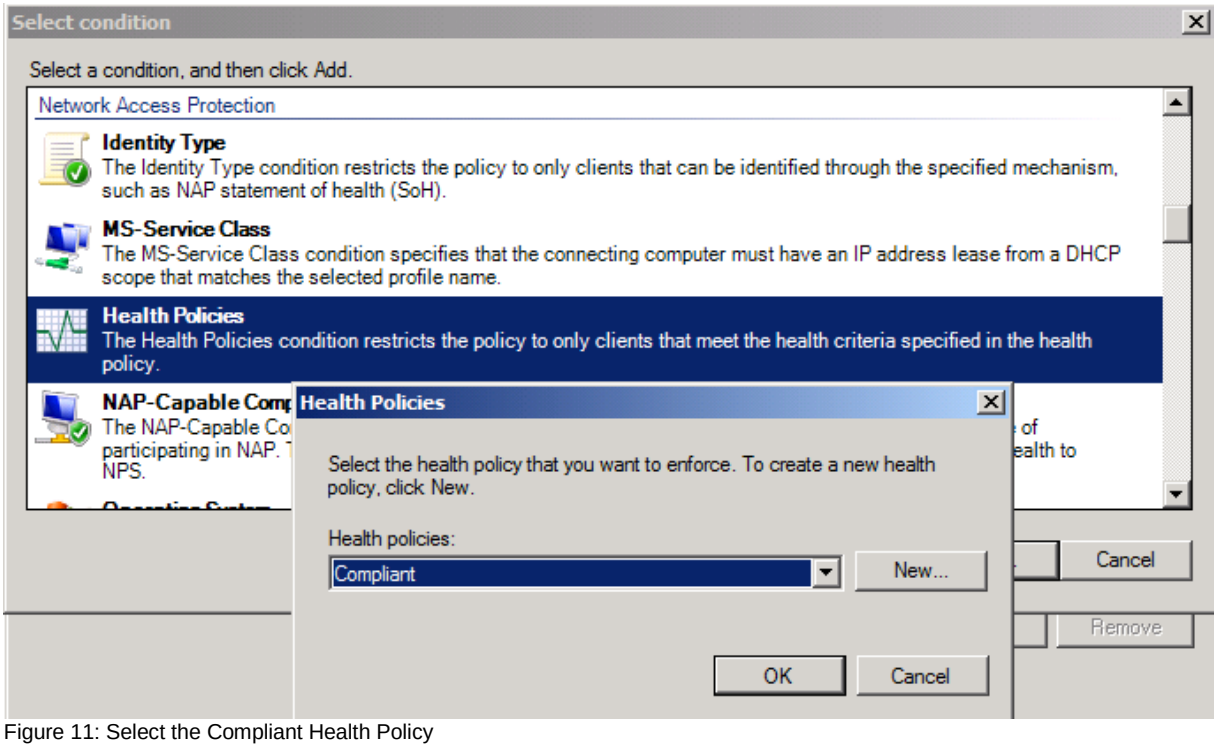

Figure 11: Select the Compliant Health Policy

Because the VPN client will be NAP compliant when the Windows Firewall is activated we grant full access to the corporate network.

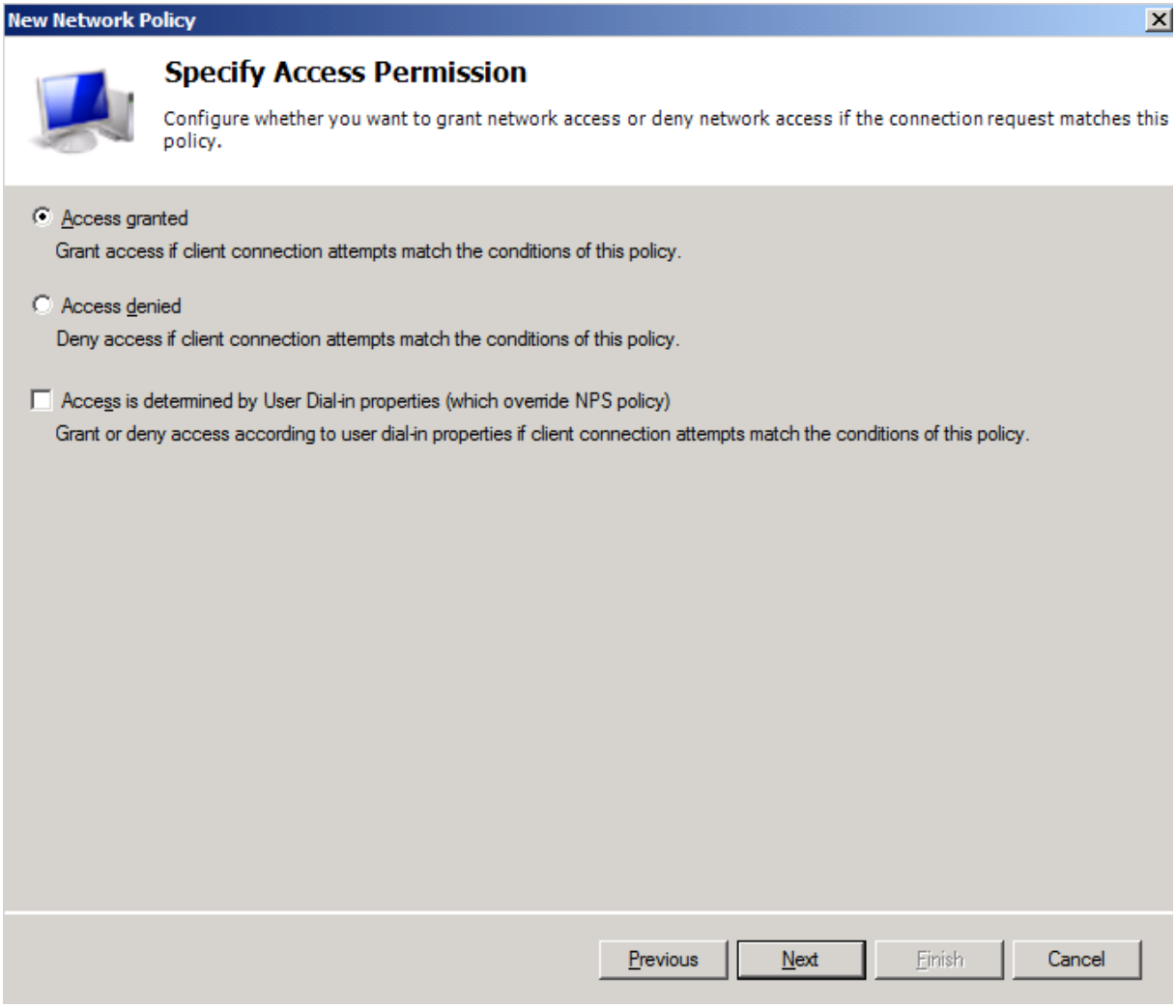

Figure 12: Grant access for compliant clients

As the Authentication method select all enabled and required authentication methods for your environment.

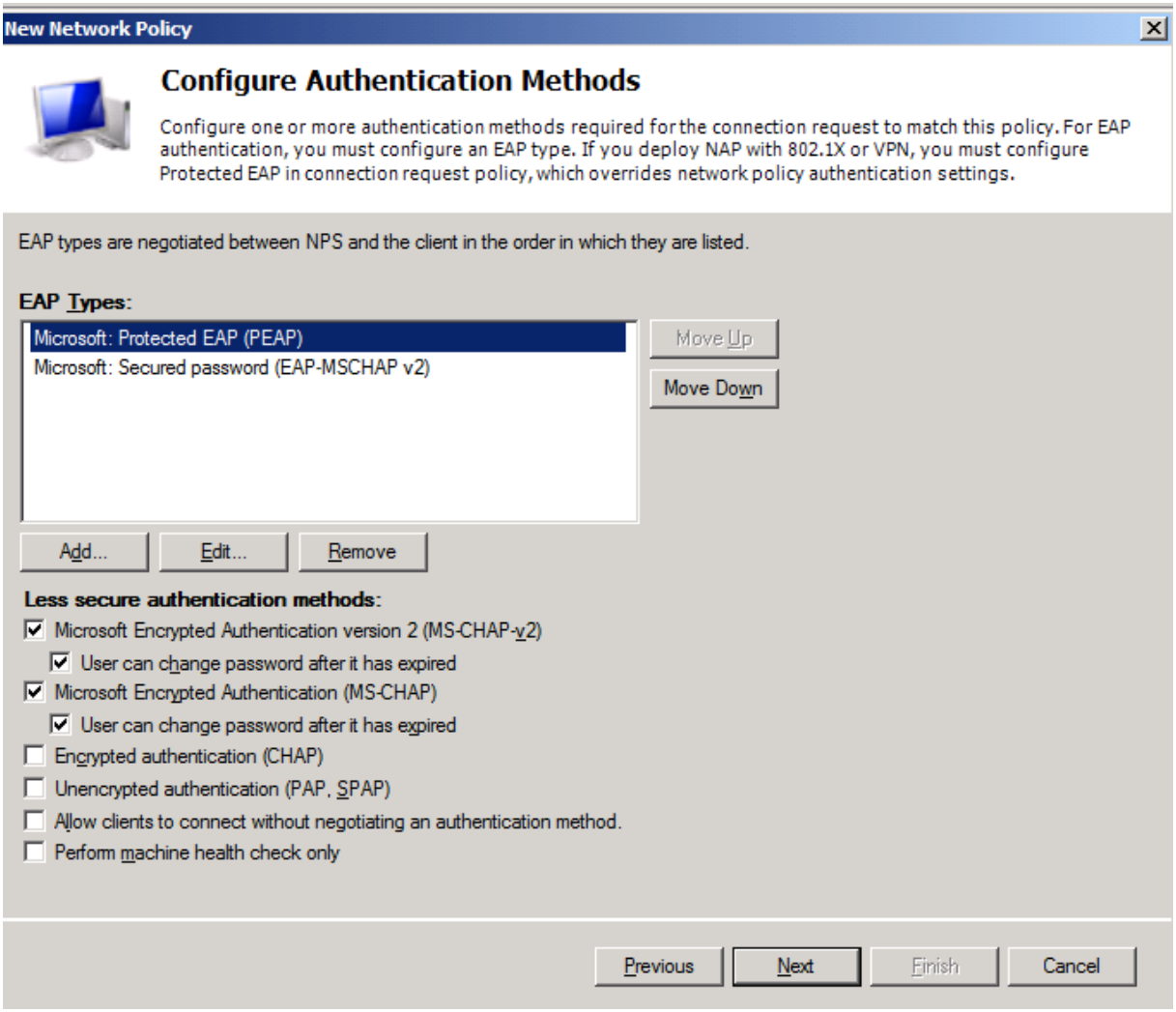

Figure 13: Select EAP types

Do the same for a Noncompliant Network Policy.

As the next step we must create a Connection Request Policy (CRP) to allow VPN access. As the type of Network Access server select *Remote Access Server (VPN-Dial up)*.

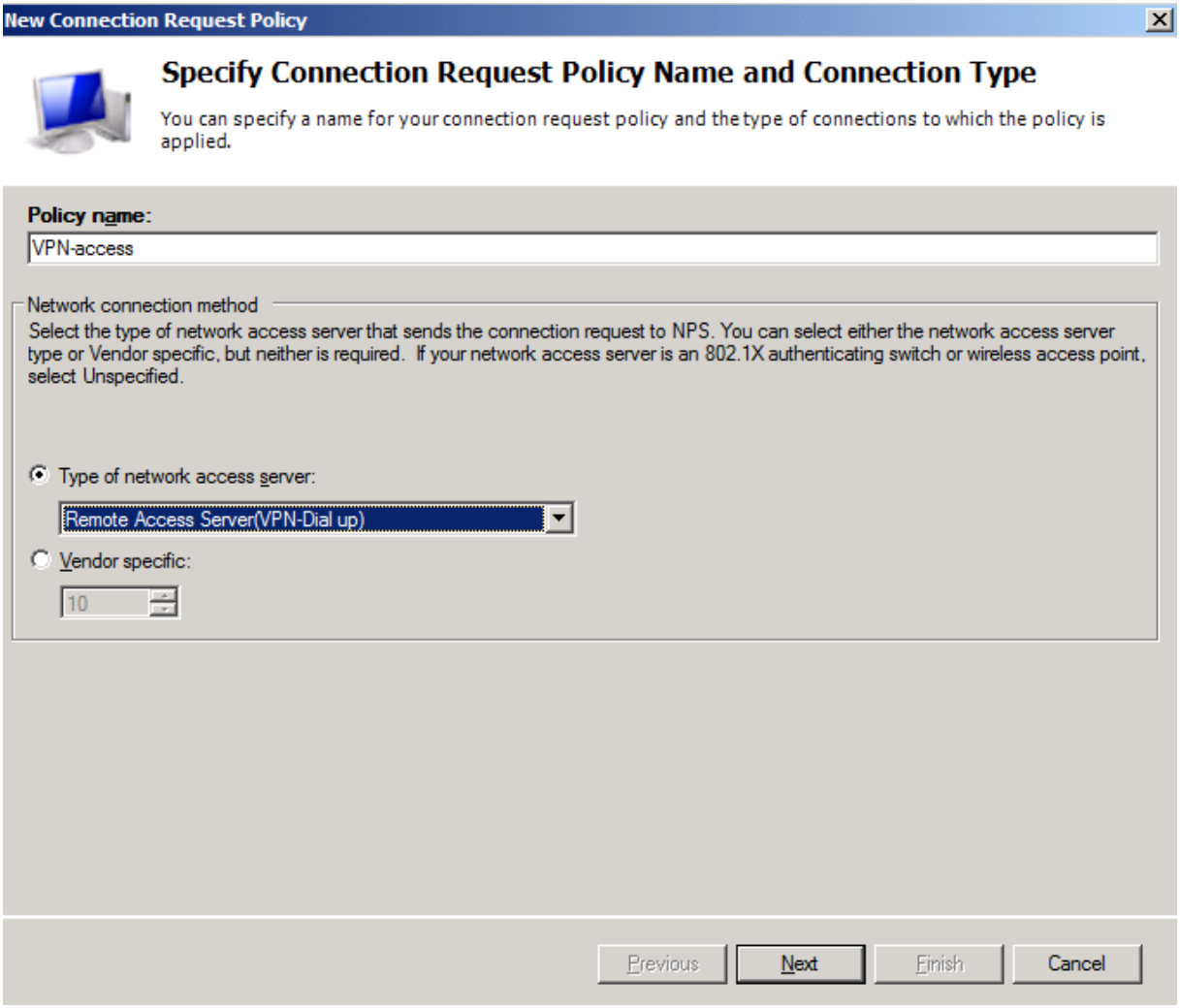

Figure 14: Specify type of Network Access Server

As a condition select the Access Client IPv4 address of the internal Network Interface of the Forefront TMG Server.

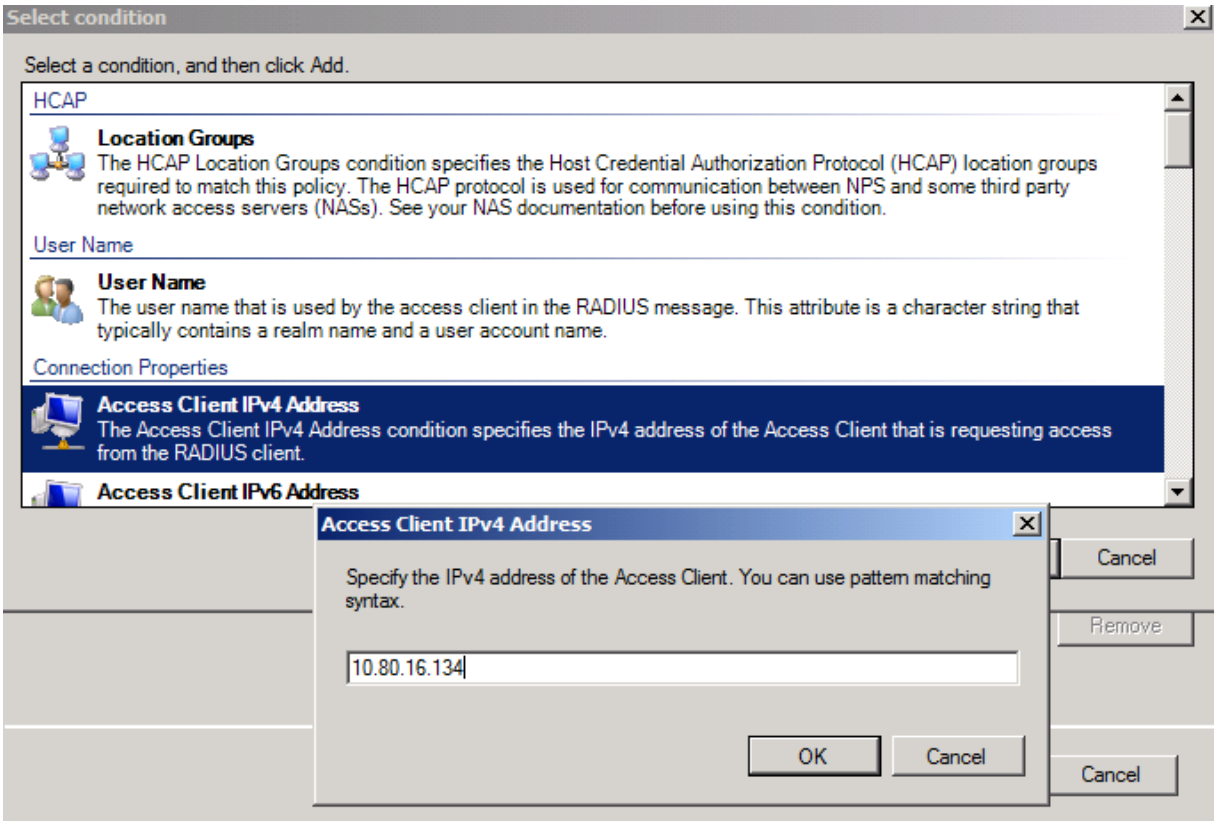

Figure 15: Add the IP address of the TMG Server to the CRP

Authenticate requests go to this Server.

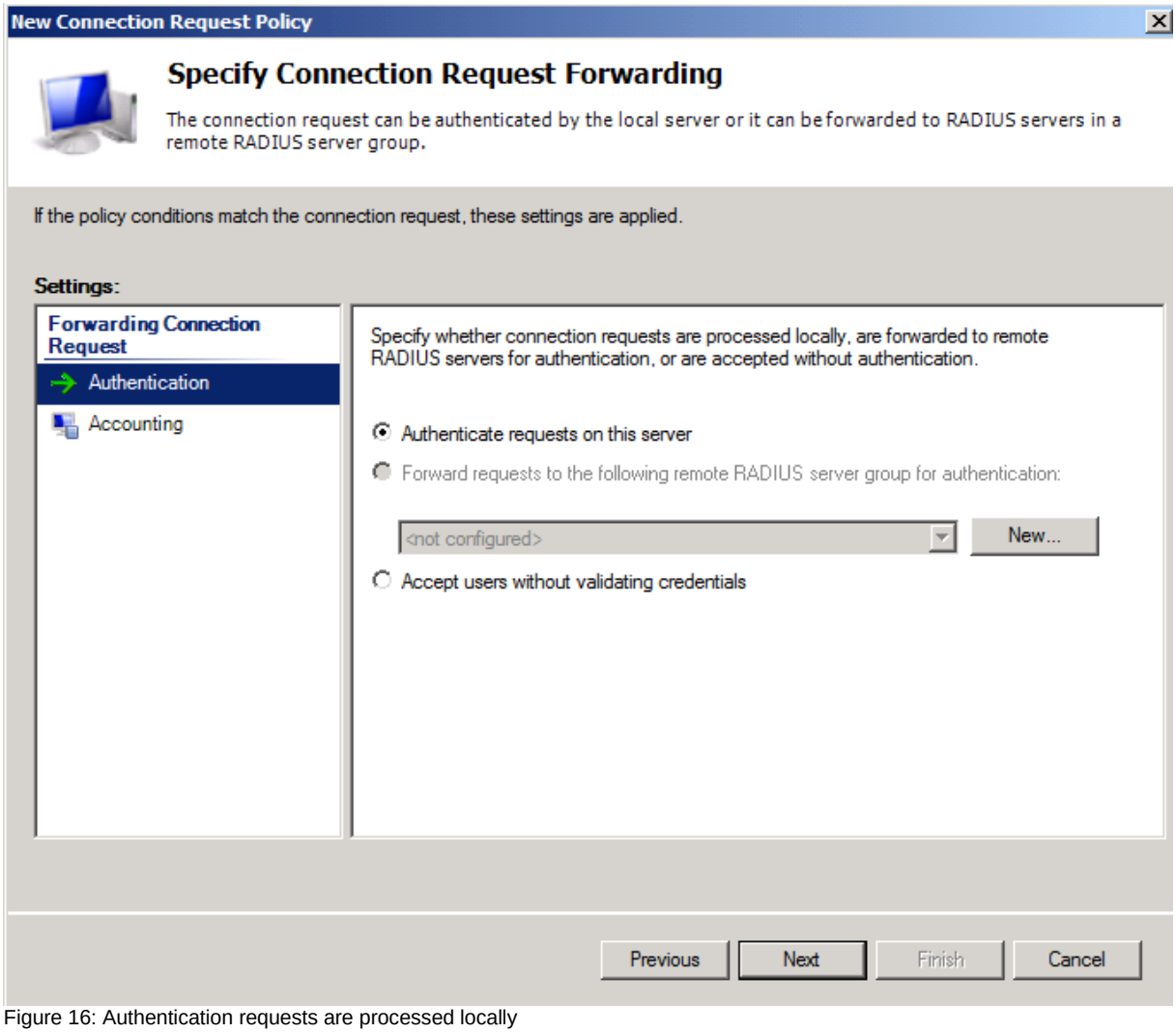

Figure 16: Authentication requests are processed locally

As the supported EAP types select a minimum of one configured authentication method on your Forefront TMG Server and at the VPN client.

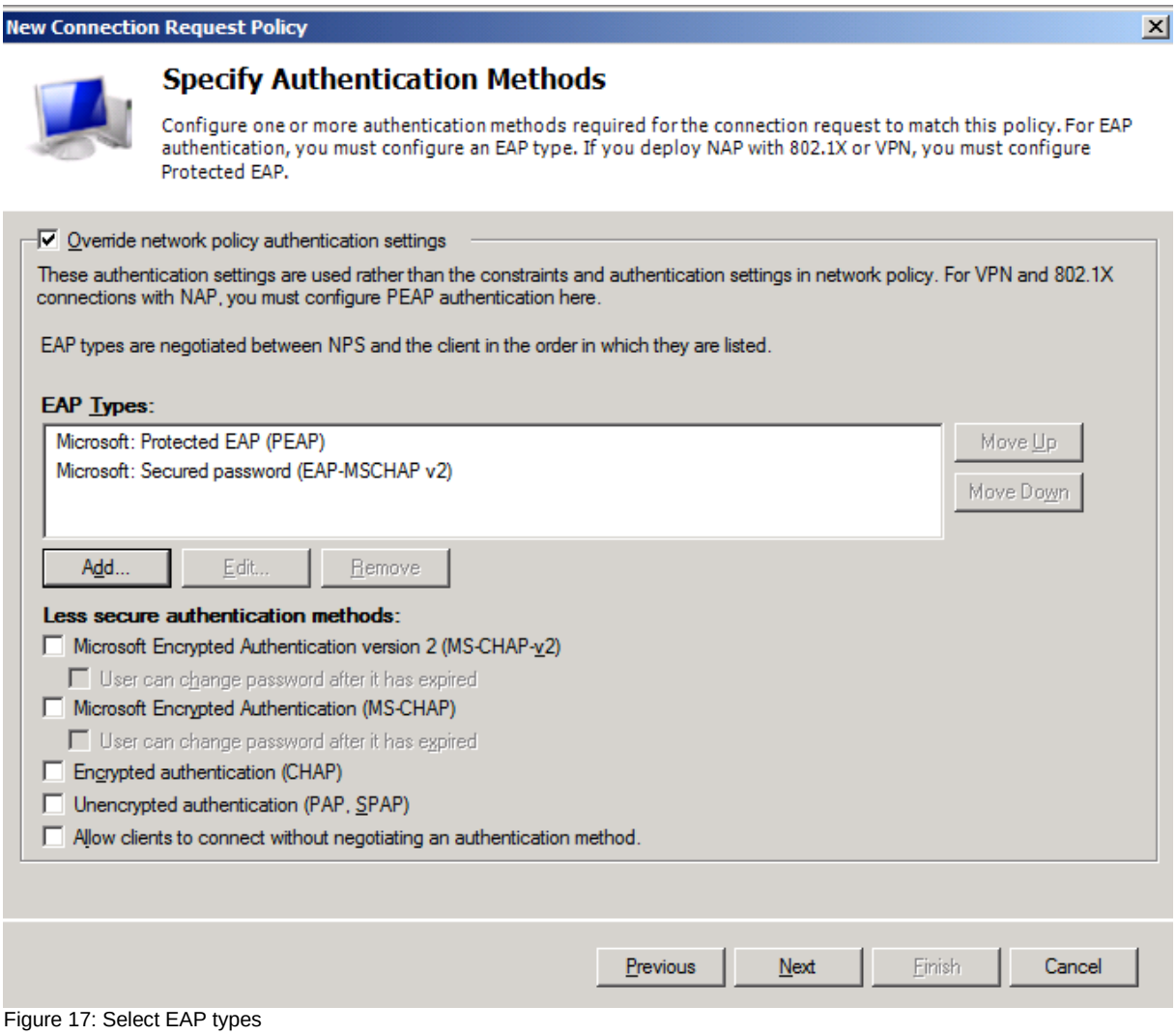

Figure 17: Select EAP types

In the Protected EAP Properties select the certificate which the Server uses to establish a secure connection with the client. The VPN client must trust the issuing Certificate Authority. You must also enable the checkbox *Enforce Network Access Protection*.

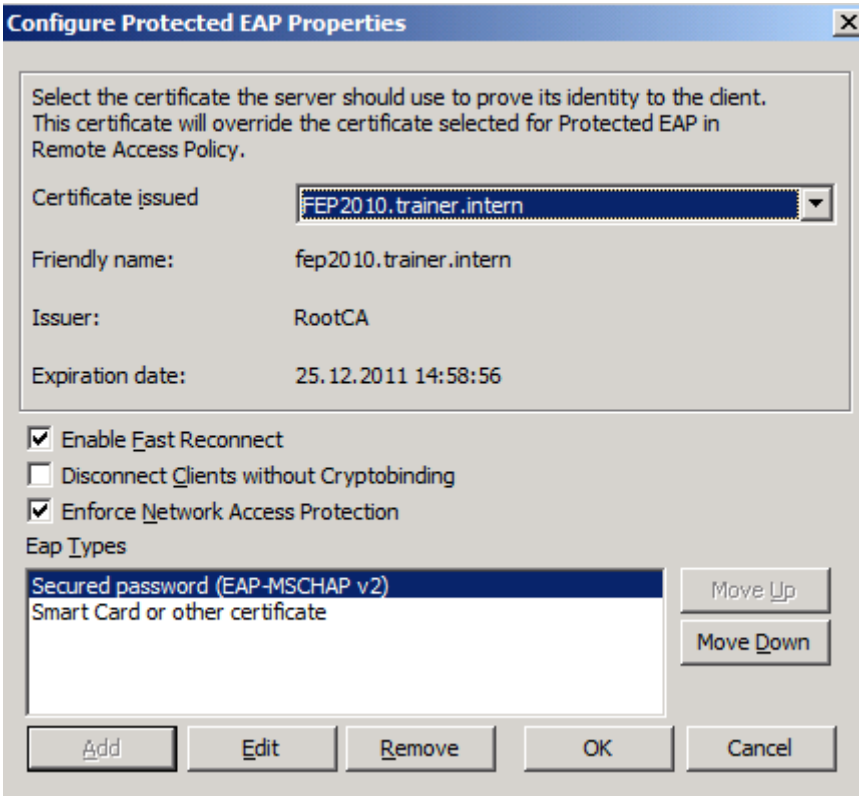

Figure 18: Enforce NAP and select the certificate

Configure the VPN client for NAP

Start *NAPCLCFG.MSC* on the Windows 7 client. This opens the NAP client configuration console. In Windows 7 the NAP VPN client is called the EAP Quarantine Enforcement client. Enable *the EAP Quarantine Enforcement Client* as shown in the following screenshot.

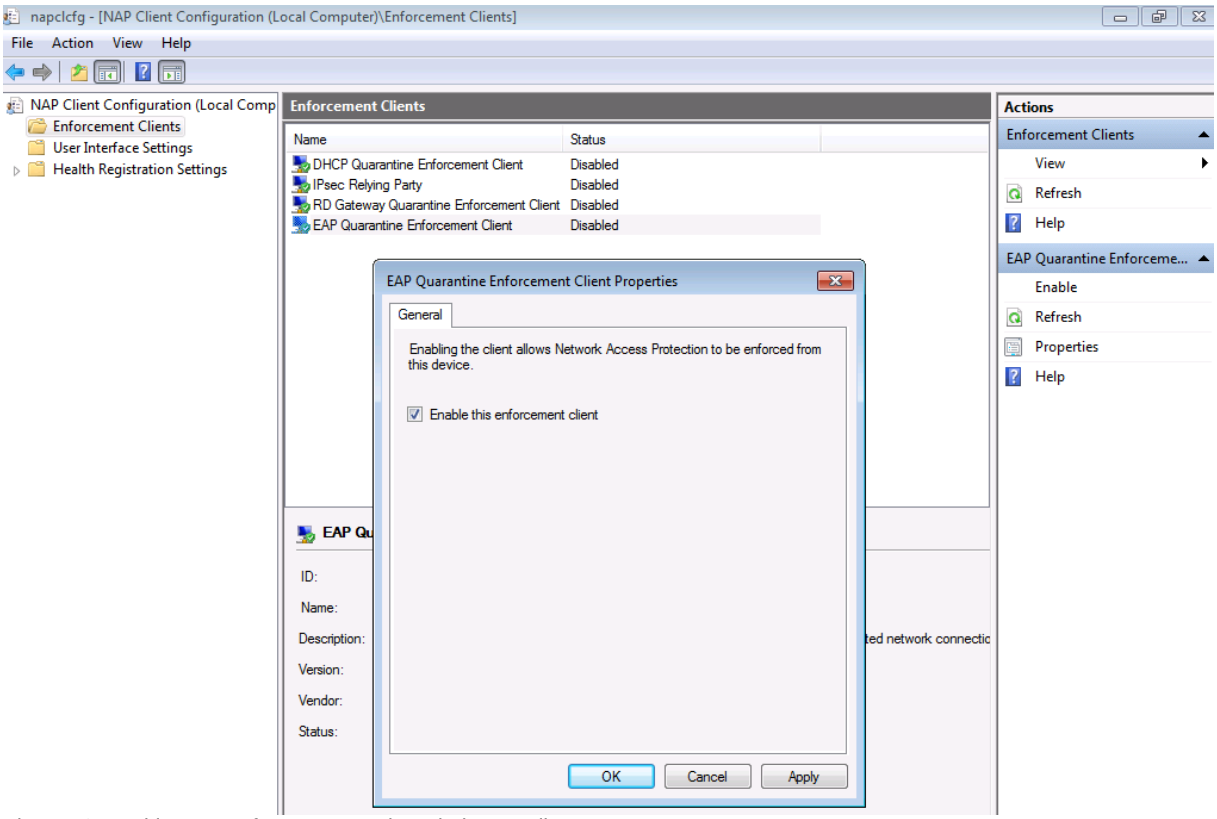

Figure 19: Enable NAP enforcement on the Windows 7 client

Please note: In Windows Vista the client is called the Remote Access Quarantine Enforcement Client.

Set the startup type of the *Network Access Protection Agent* service to Automatic and start the service.

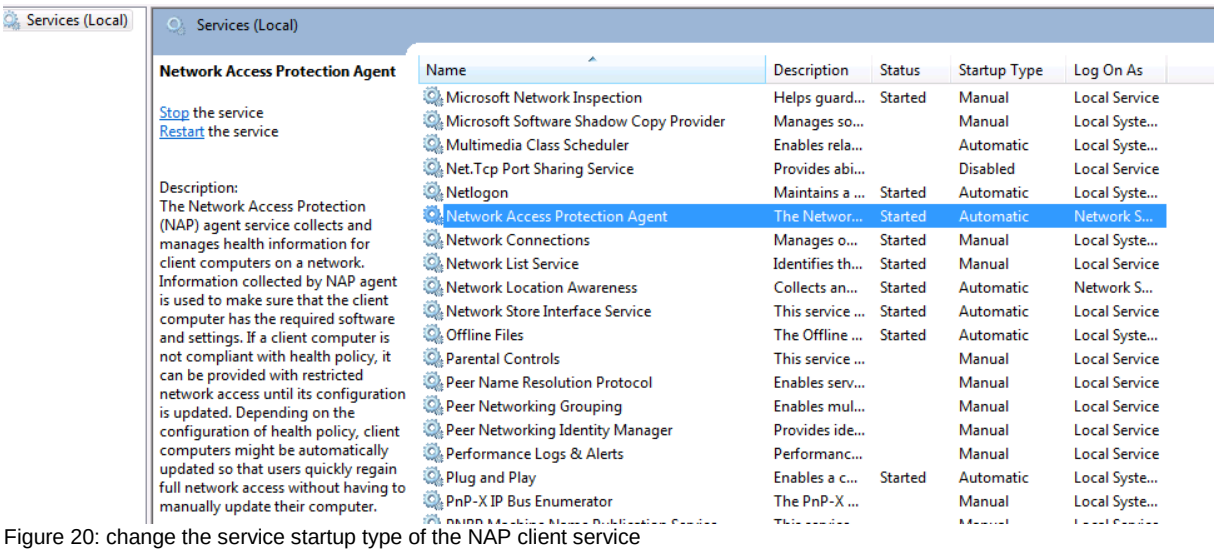

Figure 20: change the service startup type of the NAP client service

Configure the VPN client connection for NAP enforcement

Navigate to the *Security* tab and select the *EAP* radio button and click *Properties*.

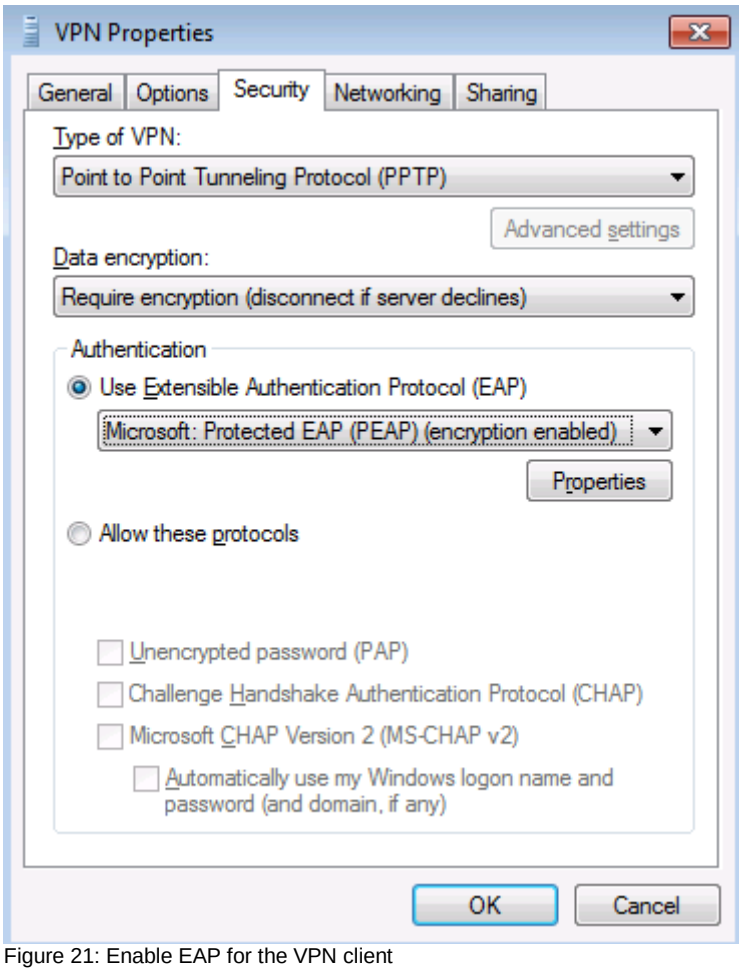

Figure 21: Enable EAP for the VPN client

Activate the Checkbox *Enforce Network Access Protection* and the required Authentication Method which depends on the settings in your environment and your Forefront TMG Server settings. Select the Trusted Root Certification Authority which issued the certificate for the NPS Server.

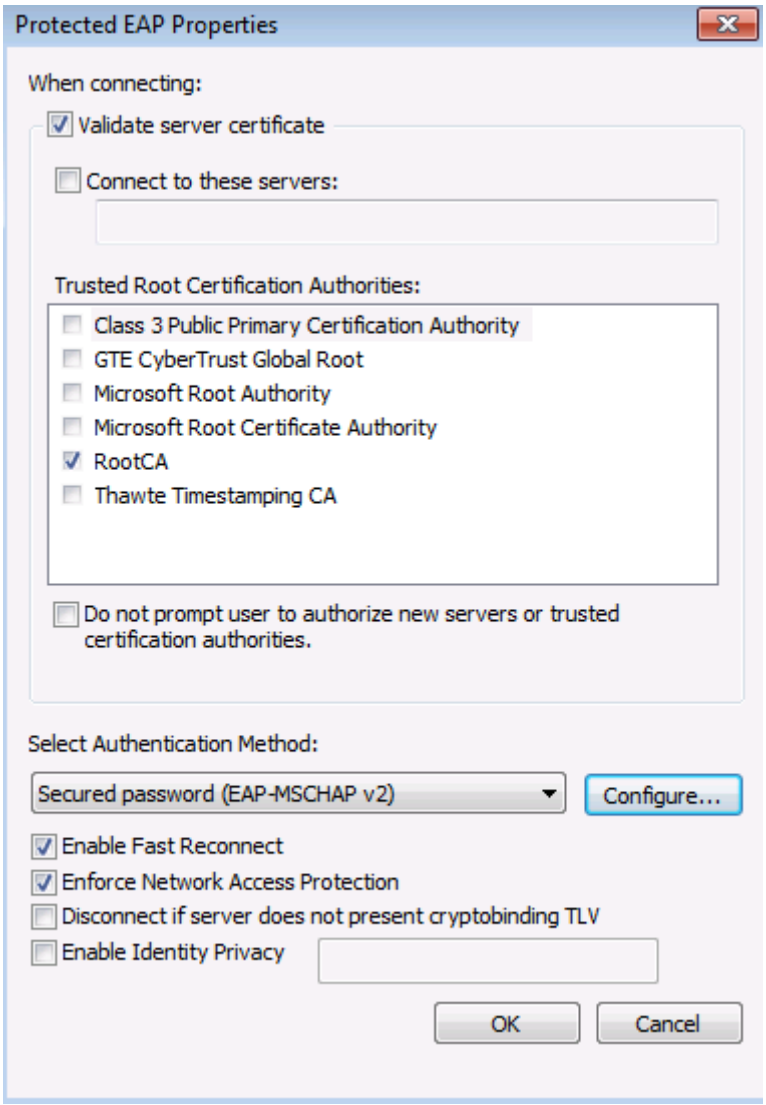

Figure 22: Enforce NAP on the client and select the issuing Root CA

Test the connection. Enable the Windows Firewall on the VPN client and the VPN connection should be successful. After the connection was successful, disconnect the VPN connection and disable the Windows Firewall and try to establish the VPN connection again. Depending on your NPS Server configuration the connection fails or you gain access to the restricted network for unhealthy VPN clients.

Conclusion

In this article I tried to show you in some high level steps how to configure Forefront TMG and the NPS Server for VPN client access with NAP. I hope that this article will give you enough information to create your own NAP environment with Forefront TMG.

Related links

Configuring VPN remote access connections to use NAP based quarantine
http://technet.microsoft.com/en-us/library/cc984479.aspx
Configuring VPN Client Access on Forefront TMG with NAP Integration
http://blogs.technet.com/b/yuridiogenes/archive/2008/09/29/configuring-vpn-client-access-on-forefront-tmg-with-nap-integration.aspx

Installing the remote access quarantine tool
http://technet.microsoft.com/en-us/library/cc995091.aspx
Enabling NAP on VPN clients
http://technet.microsoft.com/en-us/library/cc984450.aspx
Configuring NAP on the Network Policy Server (NPS)
http://technet.microsoft.com/en-us/library/dd182017.aspx