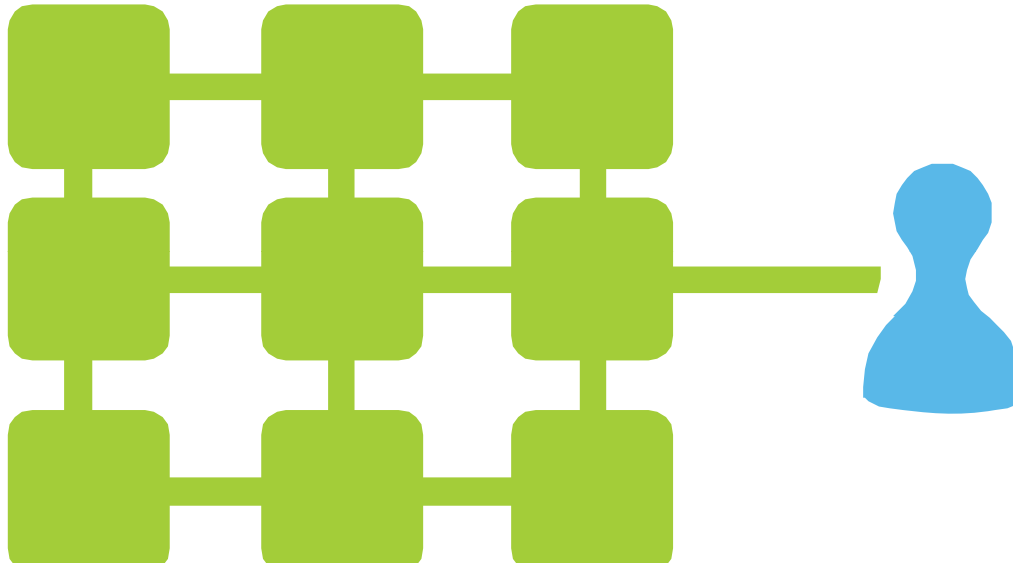
Configure a Remote Access Policy

June 6, 2012

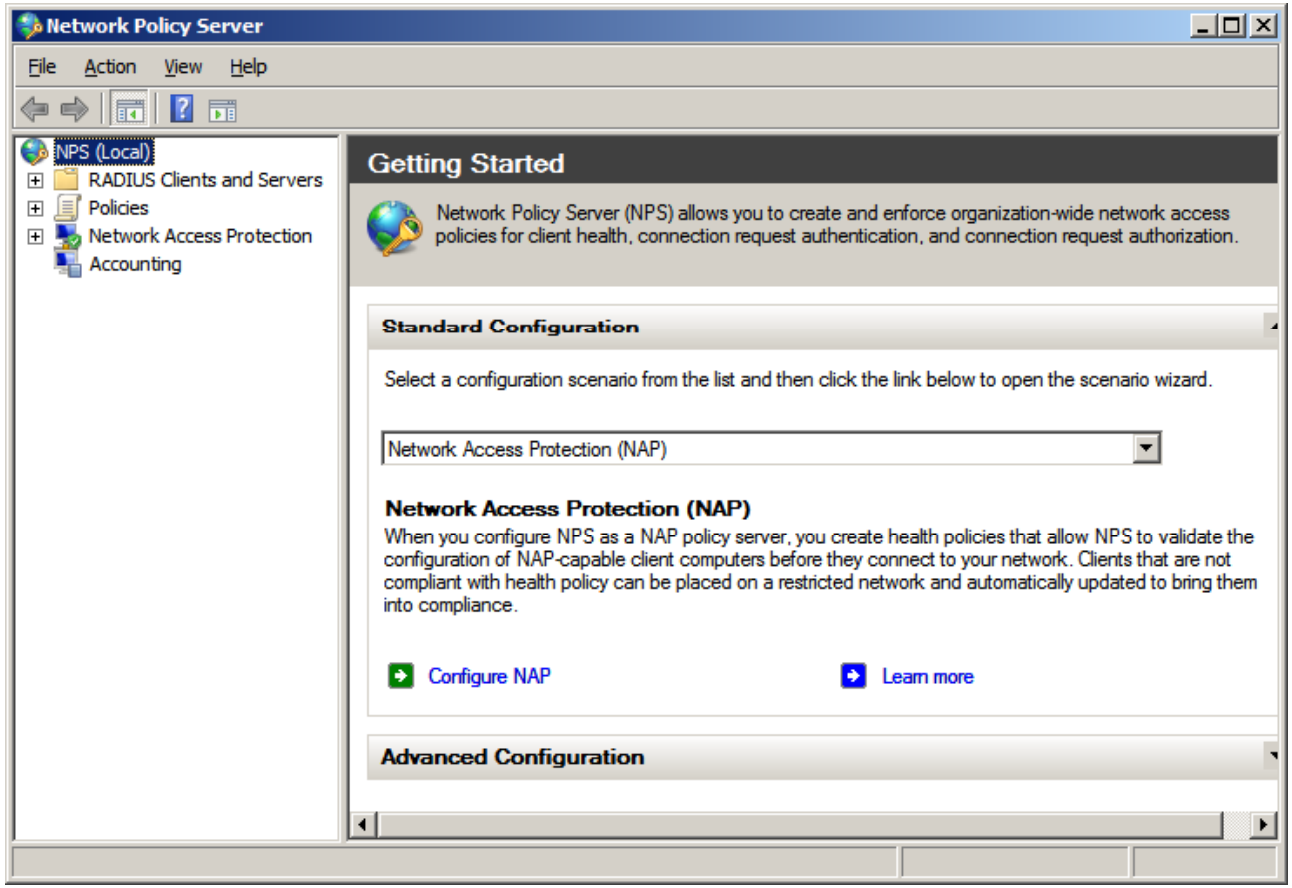
Network Policies

We need to set policies on the Network Policy Server so that the VPN connection can function.



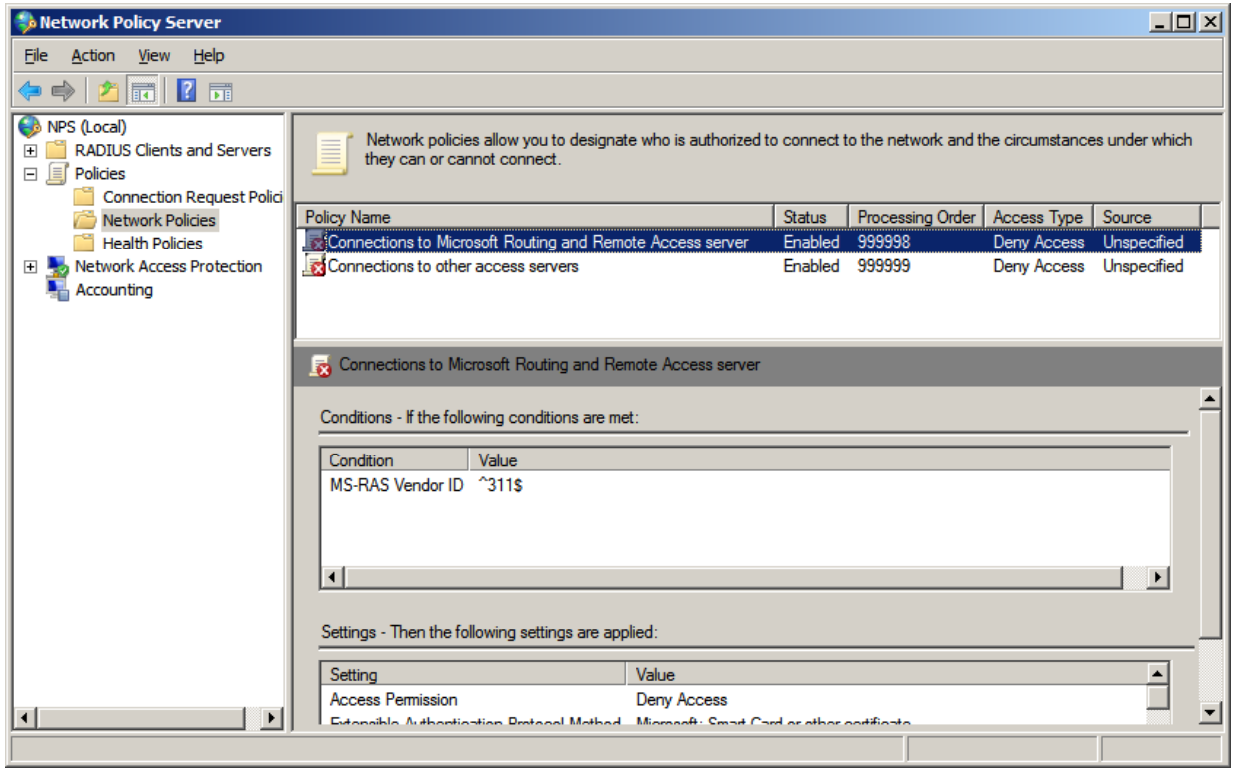
Open Network Policy Server

To access the Network Policy Server, we click on the Start menu, select Administrative Tools and Network Policy Server.



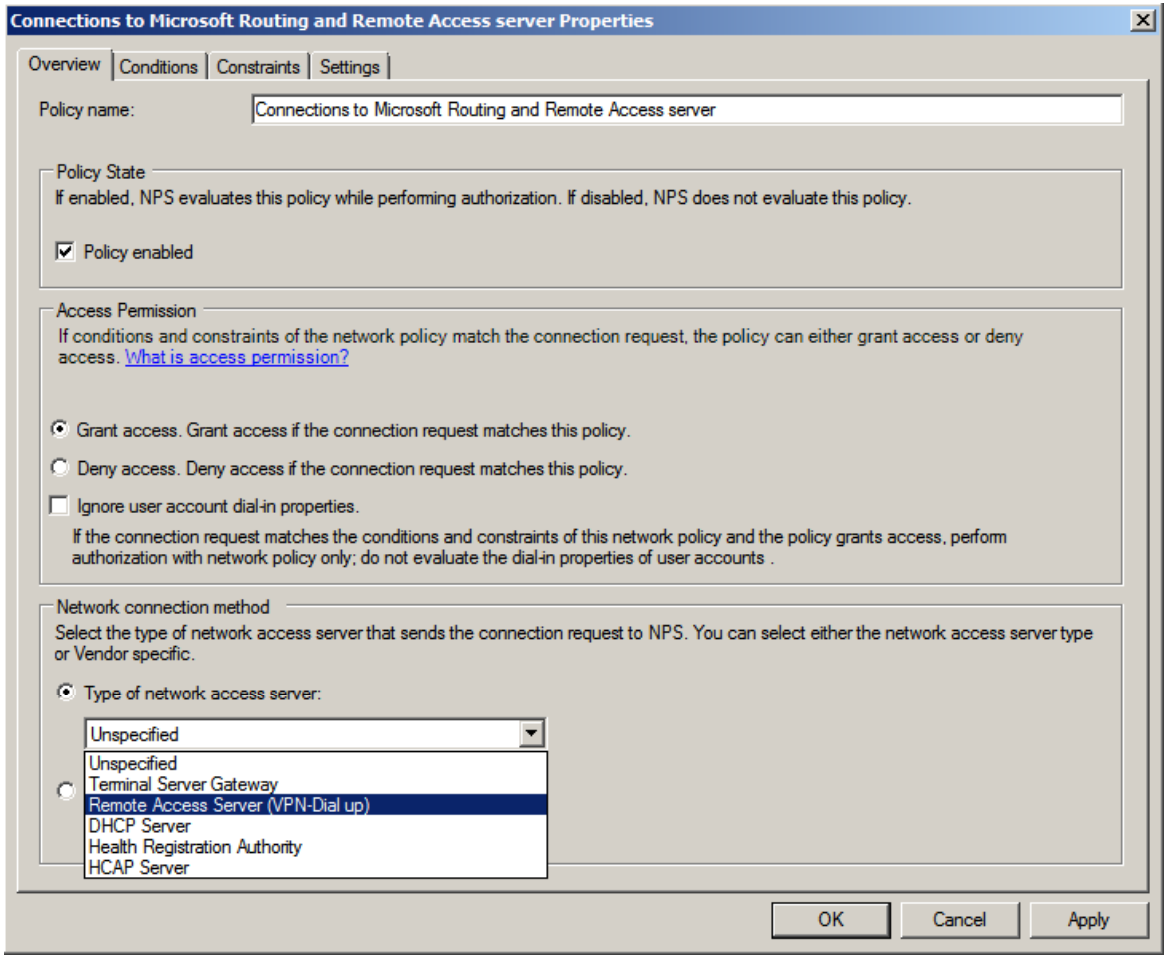
Network Policy Server Window

The Network Policy Server window will appear and in left pane, and we should open the policies folder. We will see two policies in the right pane. The first is Connections to Microsoft Routing and Remote Access server and the second is Connections to other access servers. We will open the first policy by double clicking on it.



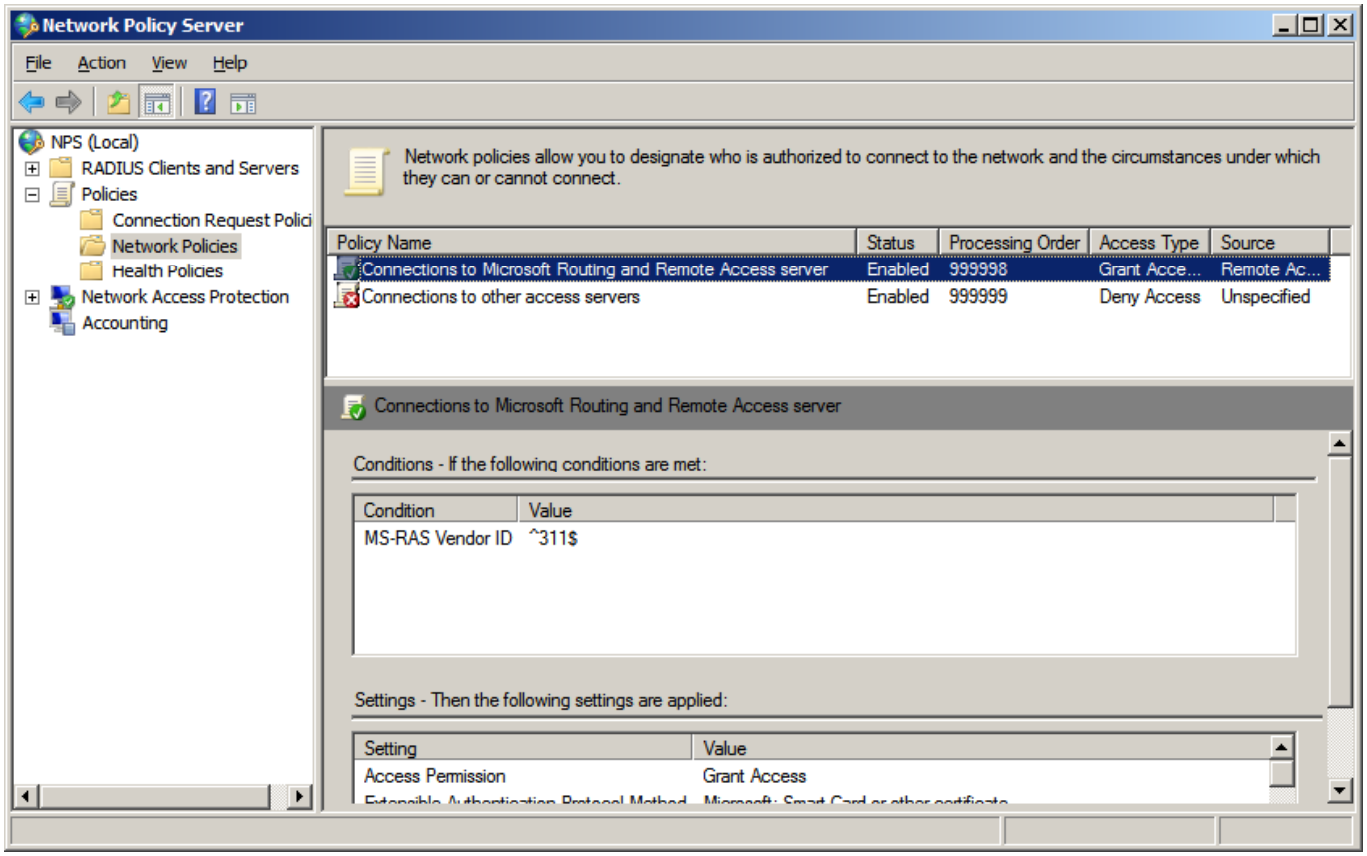
Connections to Microsoft Routing and Remote Access Server

There are two things we need to do in this dialog box. We need to change the deny access option to grant access. Then we need to pick Remote Access Server (VPN Dial up) from the list of types of network access servers. We need to push the Apply button to save our changes. We should press OK to return to the Network Policy Server window.



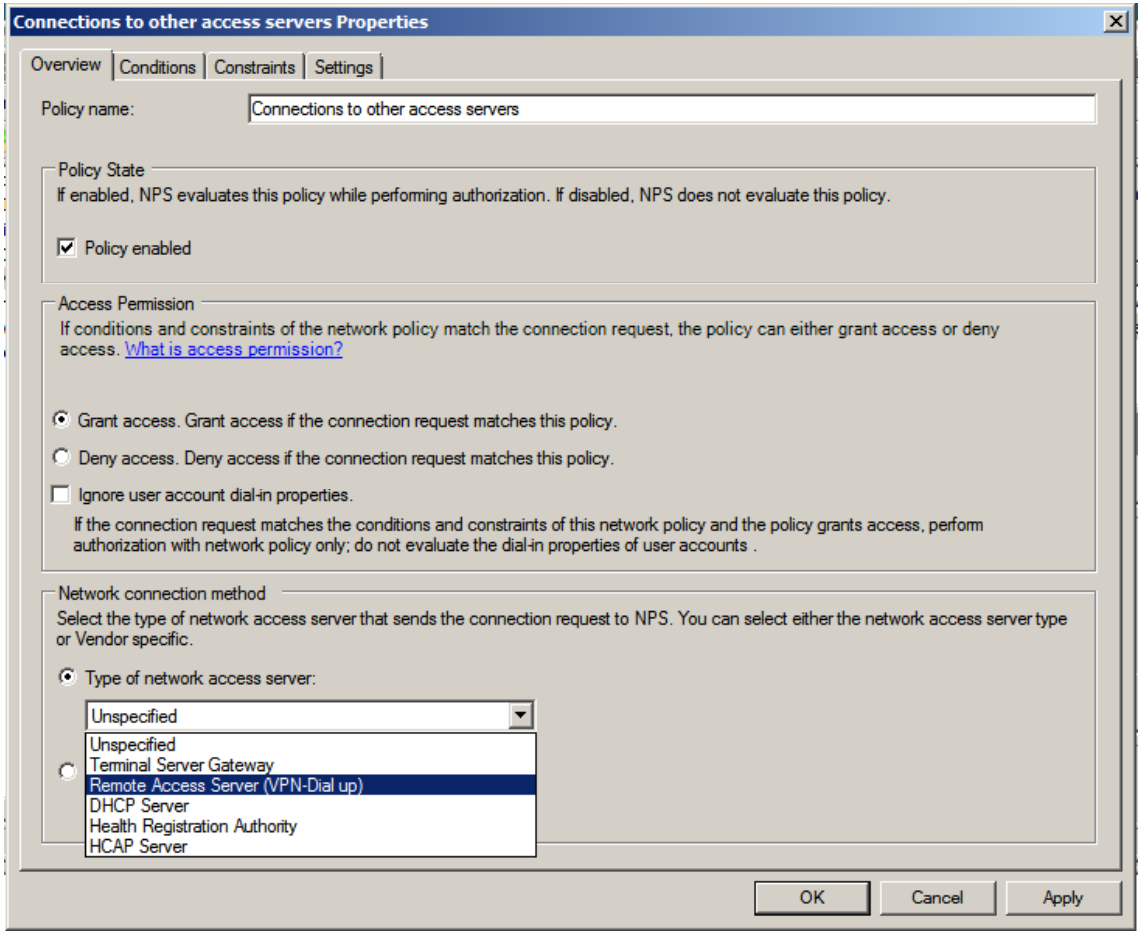
Network Policy Server Window

Back at the Network Policy Server window, we can see the Connections to Microsoft Routing and Remote Access Server no longer has a red “x” but a green check mark. To open the Connections to the other access servers dialog box, double click on this policy.



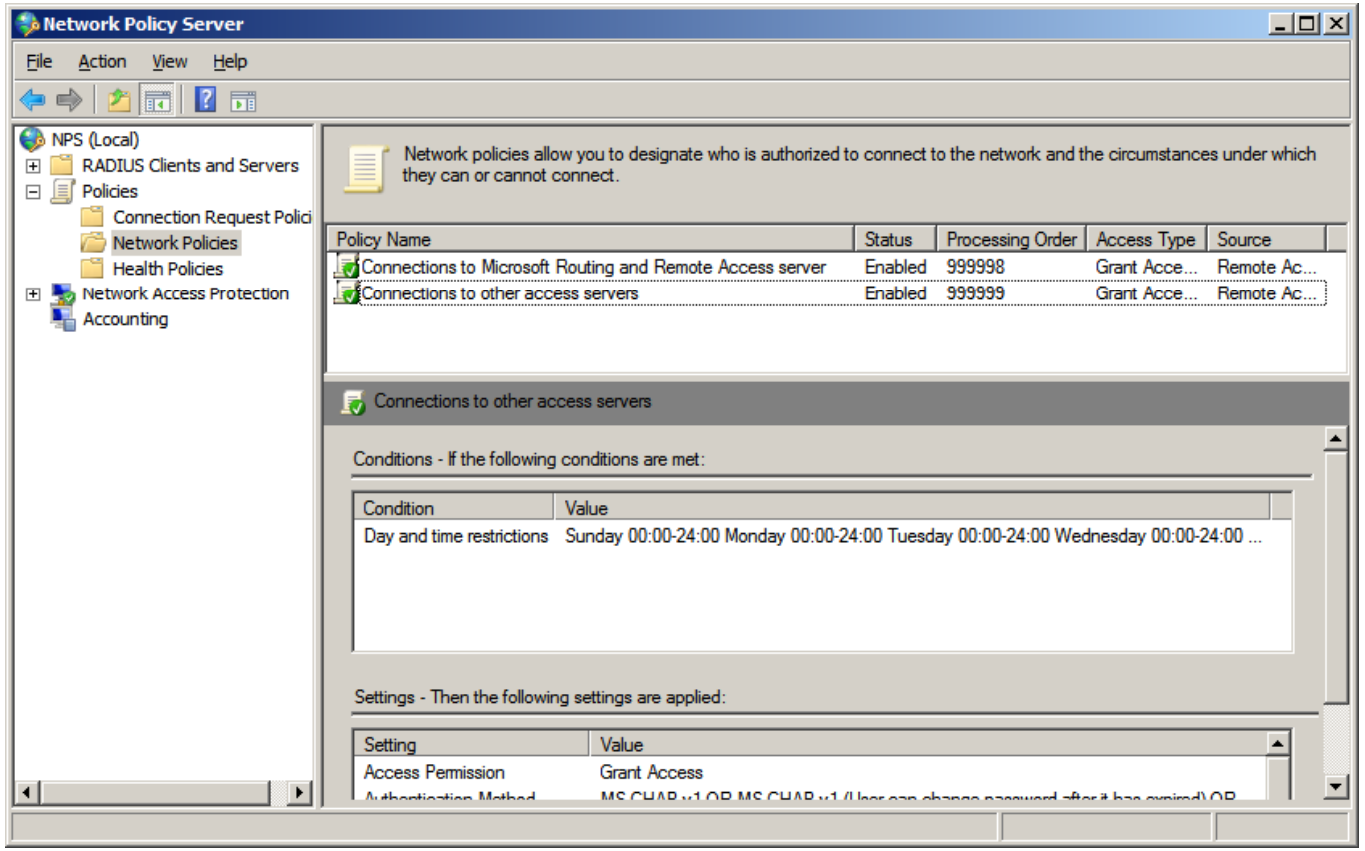
Connections to Other Access Servers

Again, there are two things we need to do in this dialog box. We need to alter the deny access option to grant access. Then we need to pick Remote Access Server (VPN Dial up) from the list of types of network access servers. We need to push the Apply button to save our changes. We should press OK to return to the Network Policy Server window.



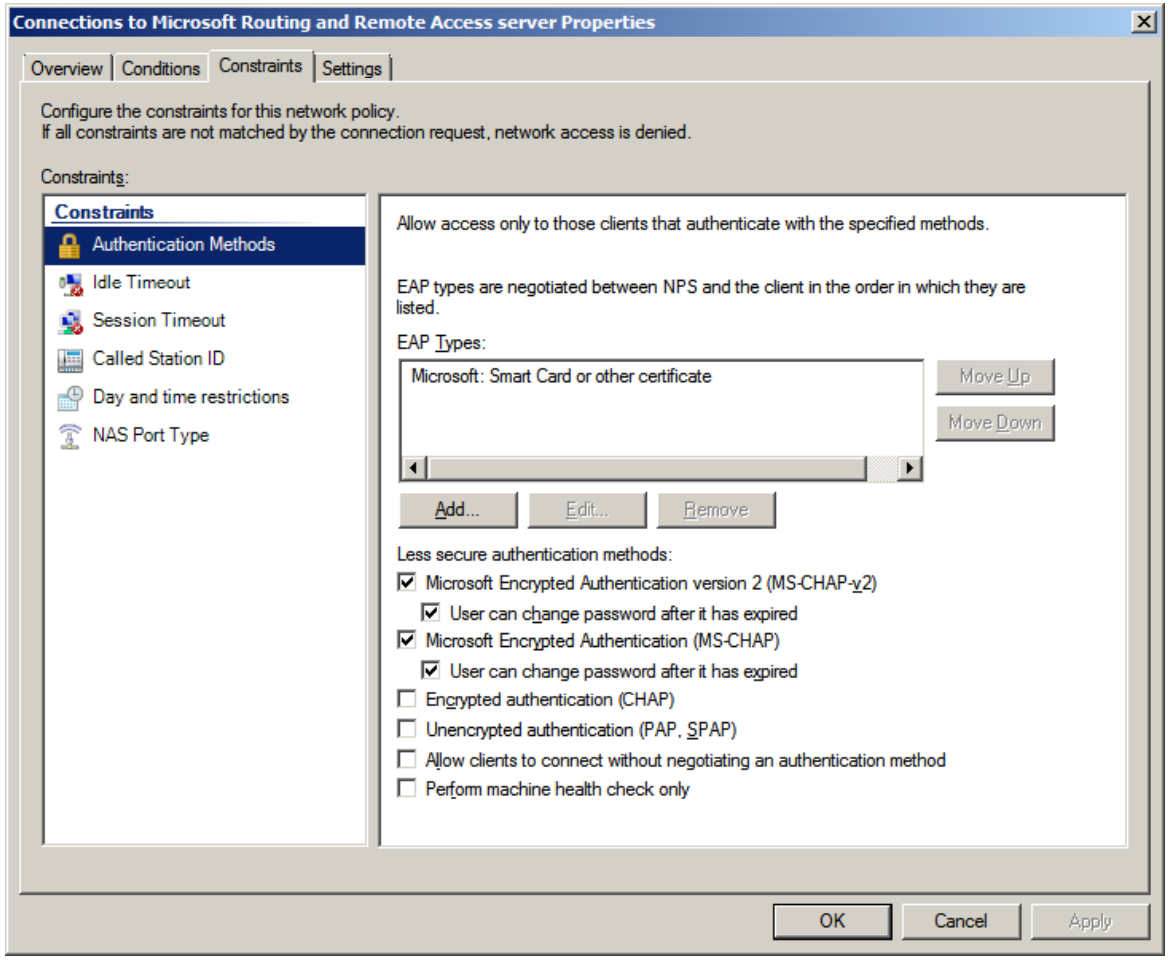
Network Policy Server Window

When we return to the Network Policy Server window, we can see the Connections to other access Server no longer has a red “x” but also has a green check mark. Next, we will want to alter some of the settings on the Connections to Microsoft Routing and Remote Access Server policy, so right click on the name and select Properties from the menu..



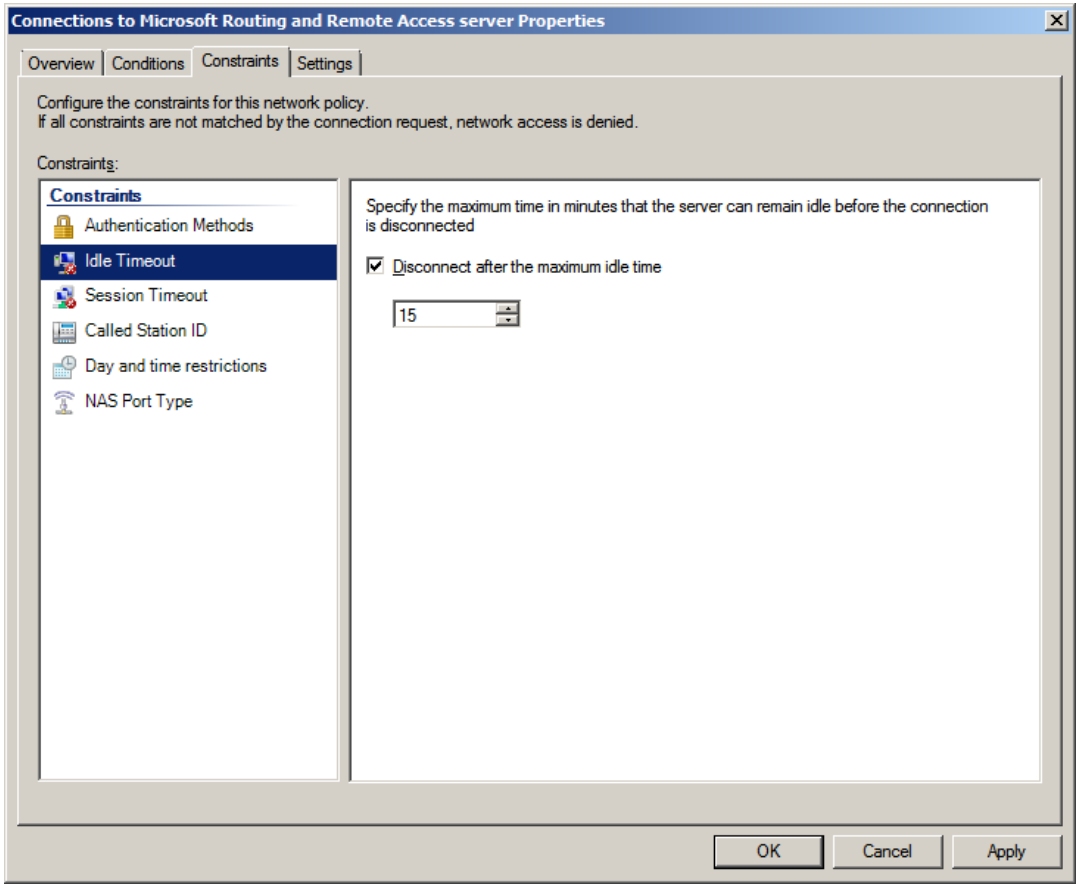
Connections to Microsoft Routing and Remote Access Server Properties

In the Connections to Microsoft Routing and Remote Access Server Properties dialogue box, we will choose the Constraints tab. There are six constraints shown in the left pane which are Authentication Methods, Idle Timeout, Session Timeout, Called Station ID, Day and Time restrictions, and NAS Port type.



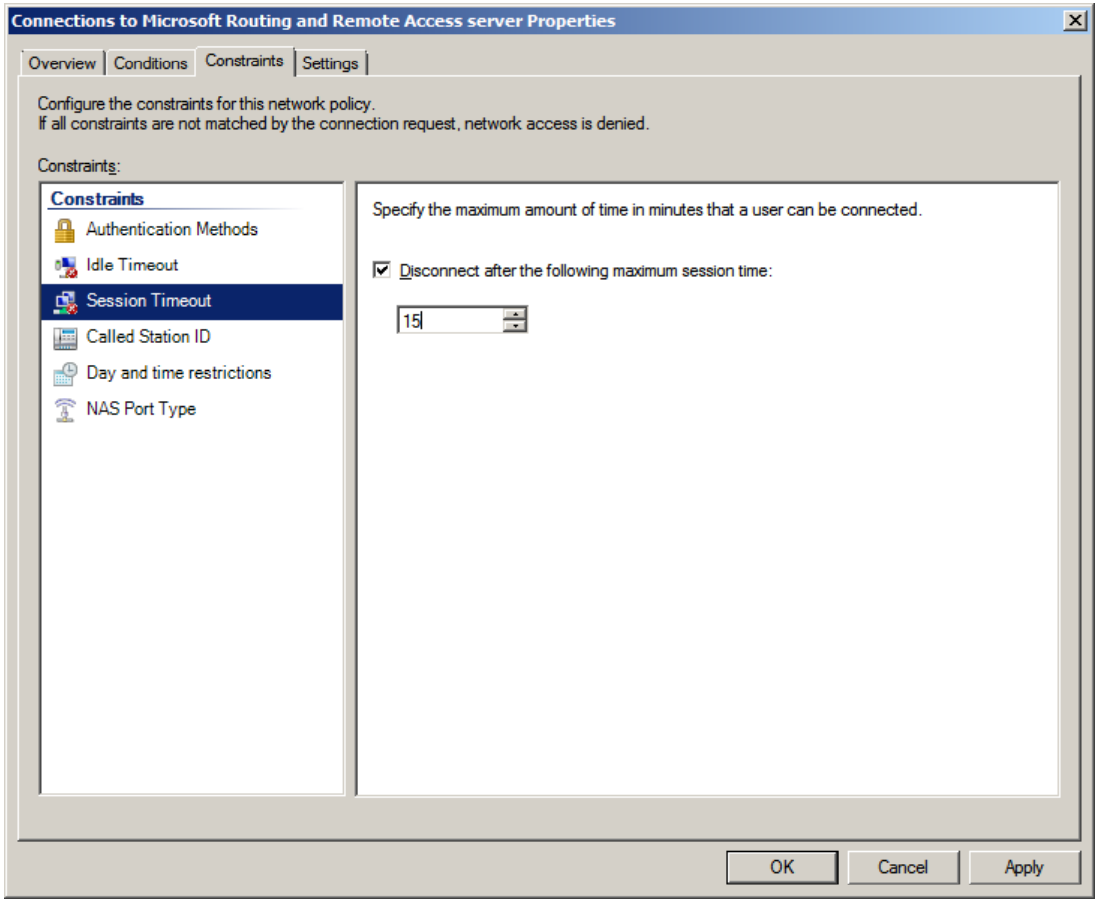
Idle Timeout

We should select idle timeout in the left pane. We will annotate the disconnect after the maximum idle time checkbox and set that period for 15 minute. What ever time we choose, it is the amount of minutes that the server can remain idle before the connection to server is terminated. After making changes, we should press the Apply button.



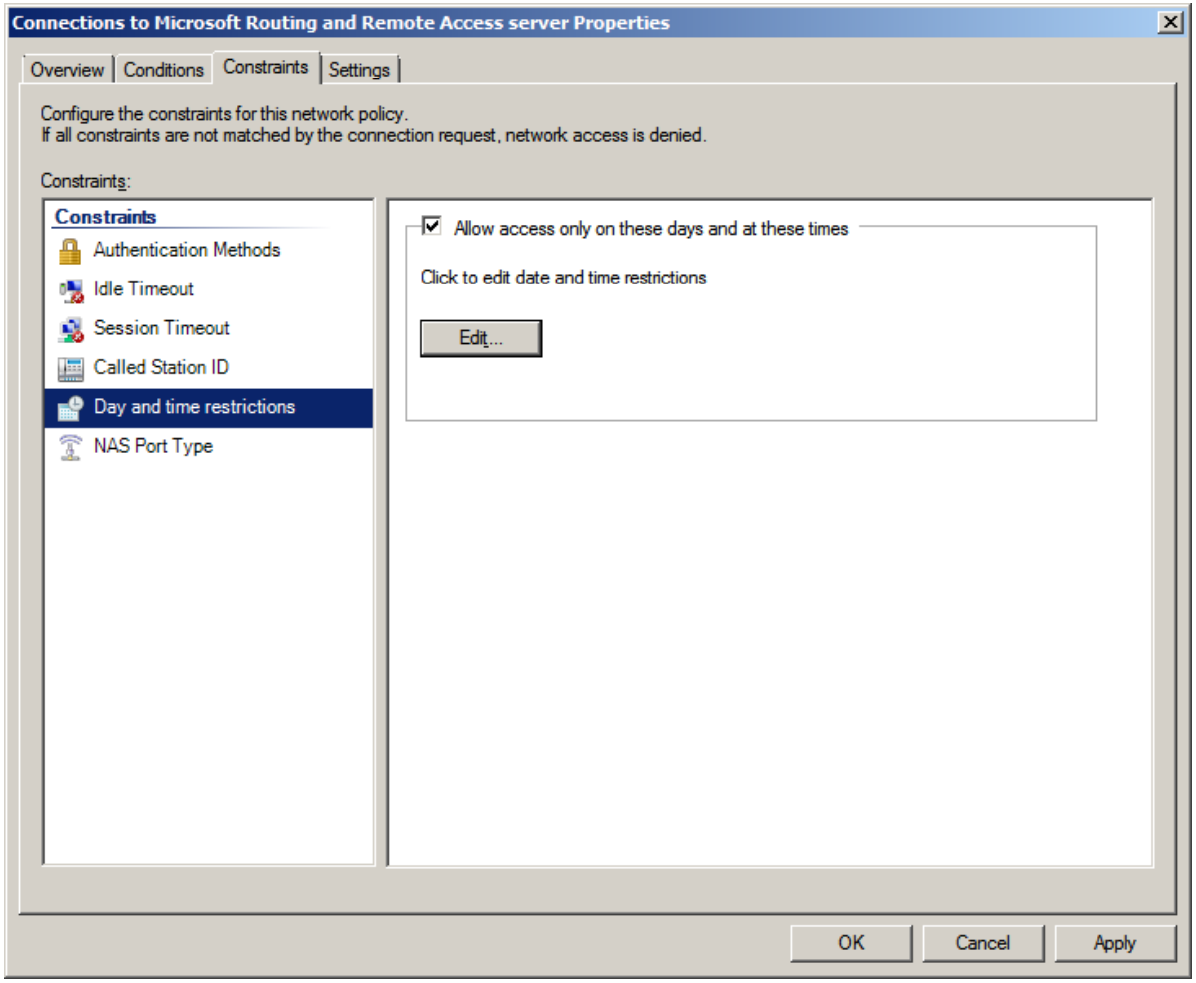
Session Timeout

We next select session timeout in the left pane. We will annotate the disconnect after the following maximum session time checkbox and set that period for 240 minute. What ever time we choose, it is the maximum amount of minutes that the user can stay connected to server before the connection is terminated. After making changes, we should press the Apply button.



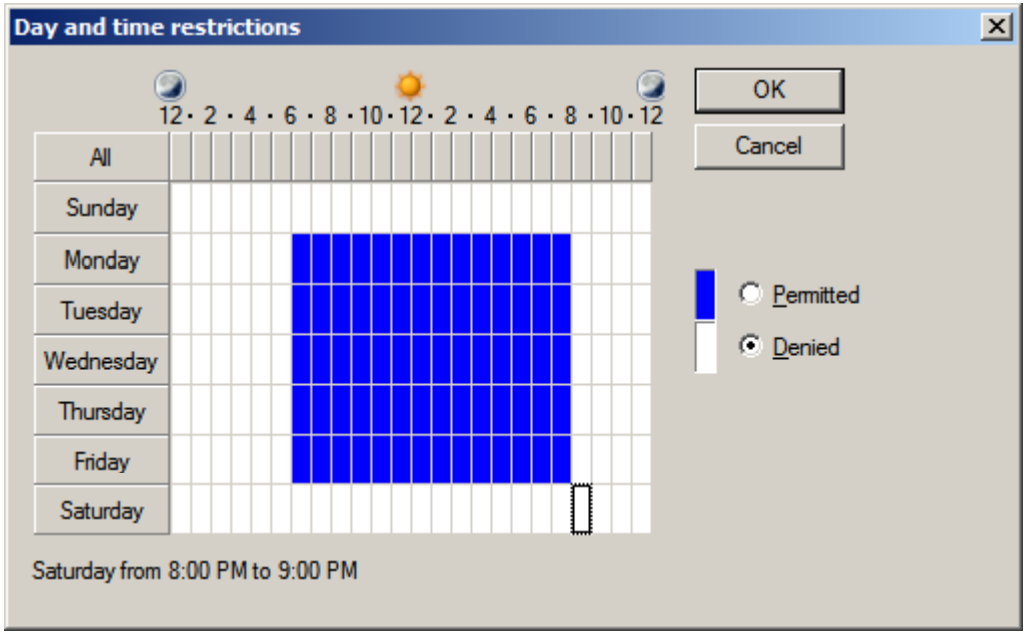
Day and Time Restrictions

On the day and time restriction constraints, we are able to enable or deny access to the remote access computer according to day of the week and hour of the day. We press the Edit button to make the specific settings. After making changes, we should press the Apply button.



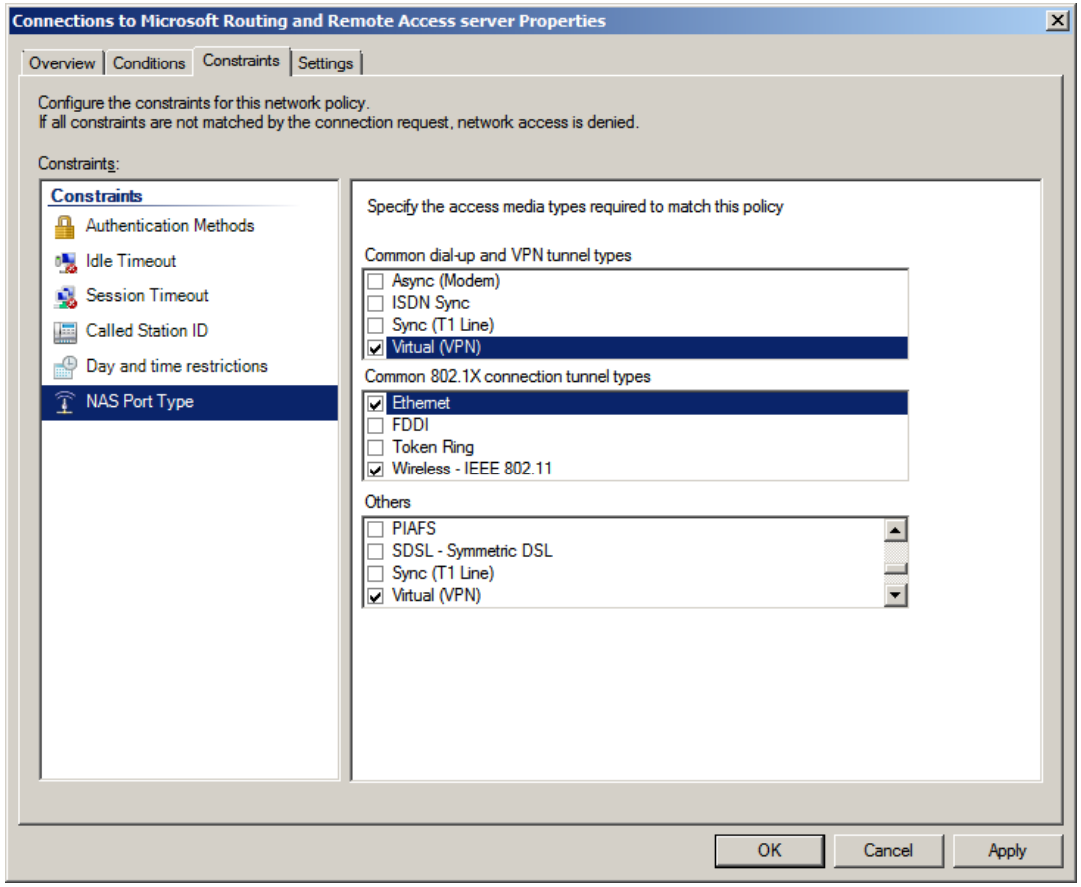
Day and Time Restrictions Window

In the Day and time restrictions window , we can allow access to server from 6 am to 8 pm, Monday through Friday. We highlight the hours that we should not be in the office and opt for the Logon denied radial button. Only the blue area represents when the connection can be made.



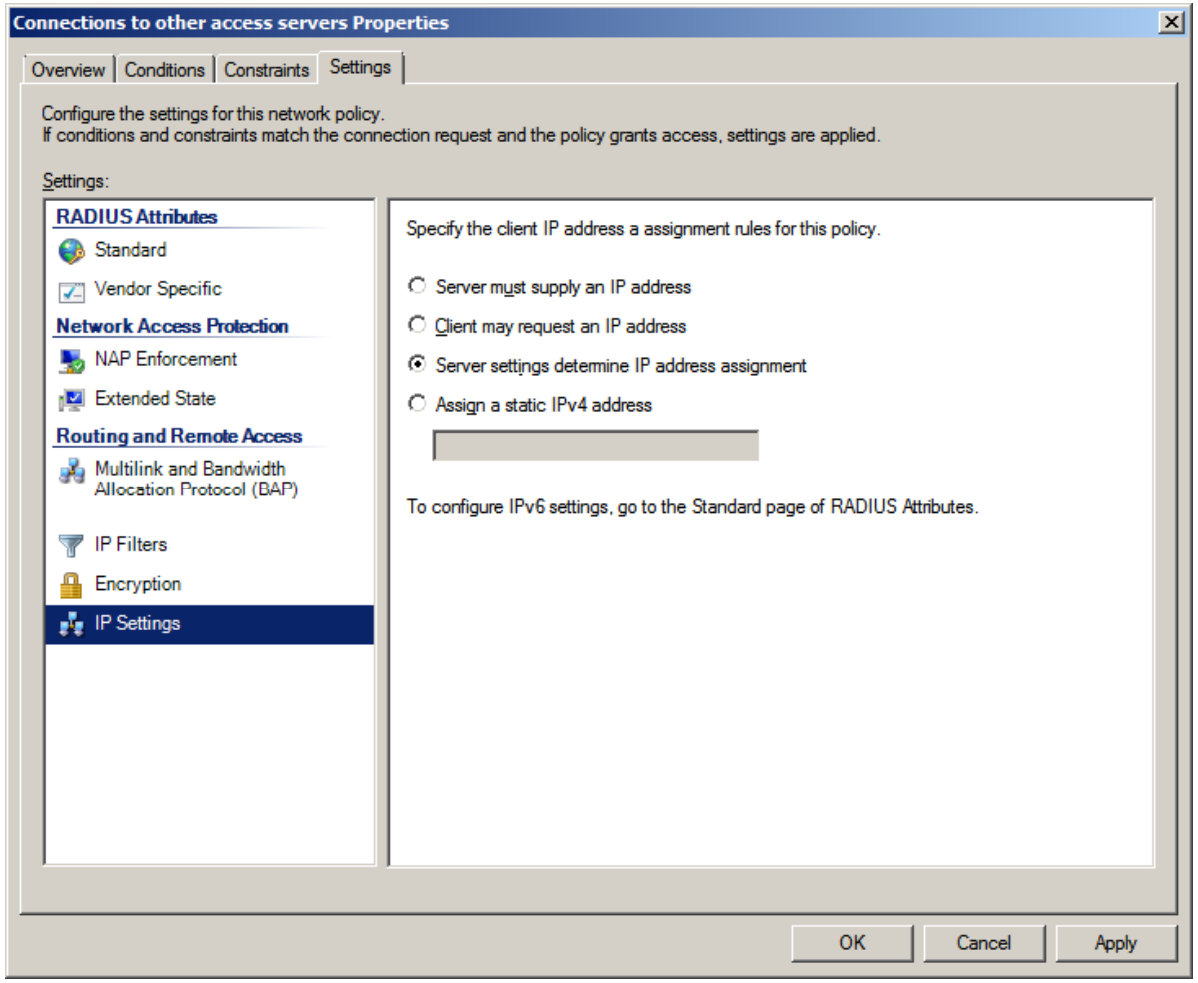
NAS Port Type

On the NAS Port Type, we make sure that VPN checkbox is annotated for common dial up and VPN tunnel types and Ethernet and Wireless checkboxes for common 802.1X connections tunnel types and the VPN checkbox for others. After making changes, we should press the Apply button.



Settings Tab

We will check the settings for the polices and particularly the IP Settings. We can even assign a static IPv4 address if we would like to. After making changes, we should press the Apply button.



Network Policy Server Window

We can see the policies on the window and the summaries below it.