Configuring Windows Firewall on Windows 7 CheckPoint server to allow SQL traffic for database connections and to allow HTTP traffic for Thin Client connections.

Description

This document provides step by step instructions for configuring The Windows Firewall on Windows 7 CheckPoint servers to allow inbound and outbound SQL server and browser traffic (required for database connectivity) and to allow inbound and outbound HTTP traffic on port 80 (required for thin client connectivity).

Step 1 – Allowing Inbound SQL server traffic

Click on "Start" → "Control Panel" → "Windows Firewall". This will open the main Windows Firewall configuration window.

Click on "Advanced Settings", this will open the "Windows Firewall with Advanced Security" window (see image 1).

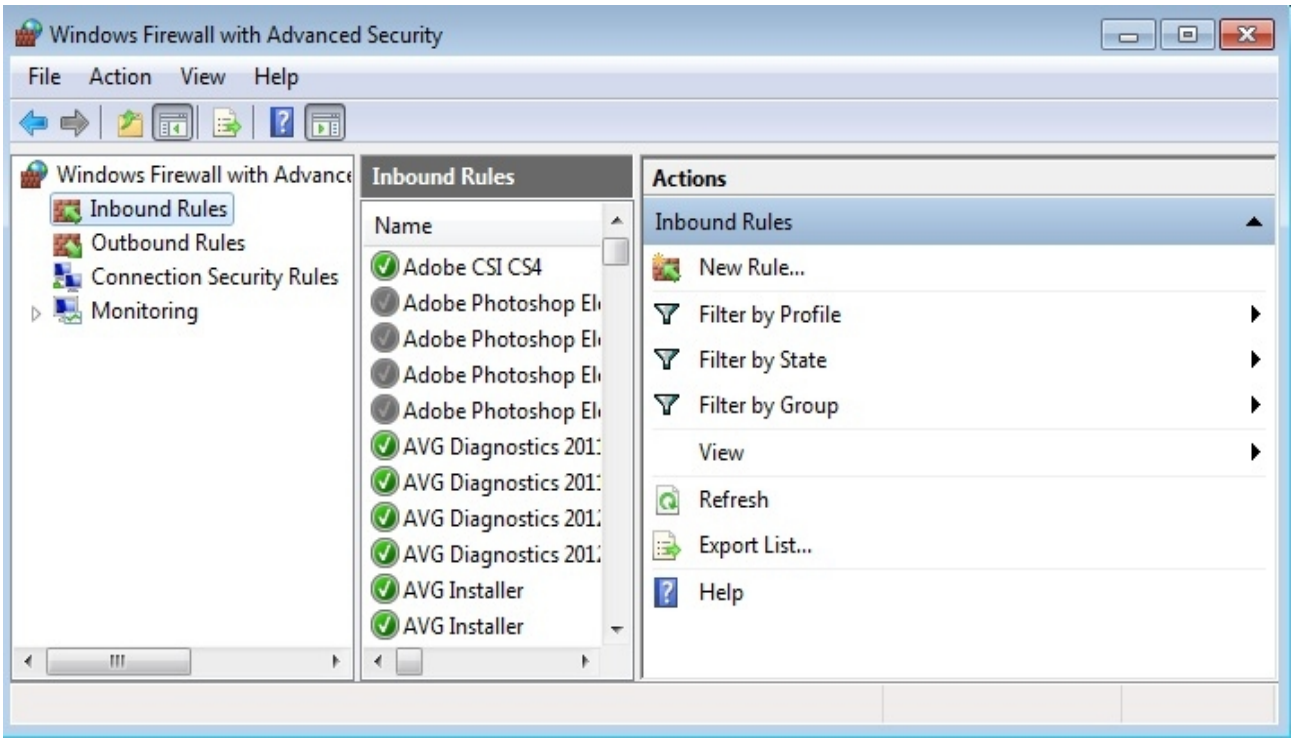

Image 1 - "Windows Firewall with Advanced Security" window

Click on “Inbound Rules” → “New Rule”. This will open the “New Inbound Rule Wizard” window (see image 2).

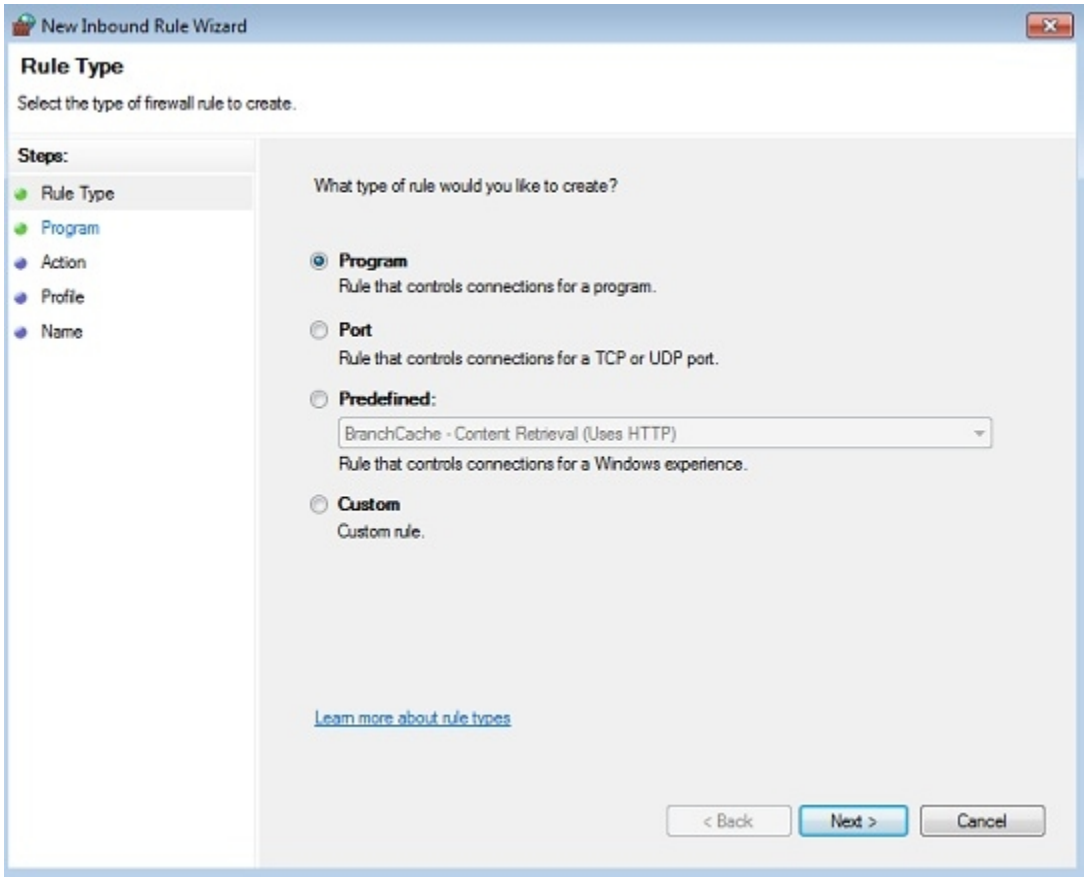

Image 2 - “New Inbound Rule Wizard” window

Select “Program” → “Next” → “This program path” → “Browse”. This will open a new window that will allow you to browse your file system directory. Browse to C:\Program Files (x86)\Microsoft SQL Server\MSSQL10.TEMPSYS\MSSQL\Binn on 64-bit systems, or to C:\Program Files\Microsoft SQL Server\MSSQL10.TEMPSYS\MSSQL\Binn on 32-bit systems and locate the sqlservr.exe file. Double-click on this file to select it (see image 3).

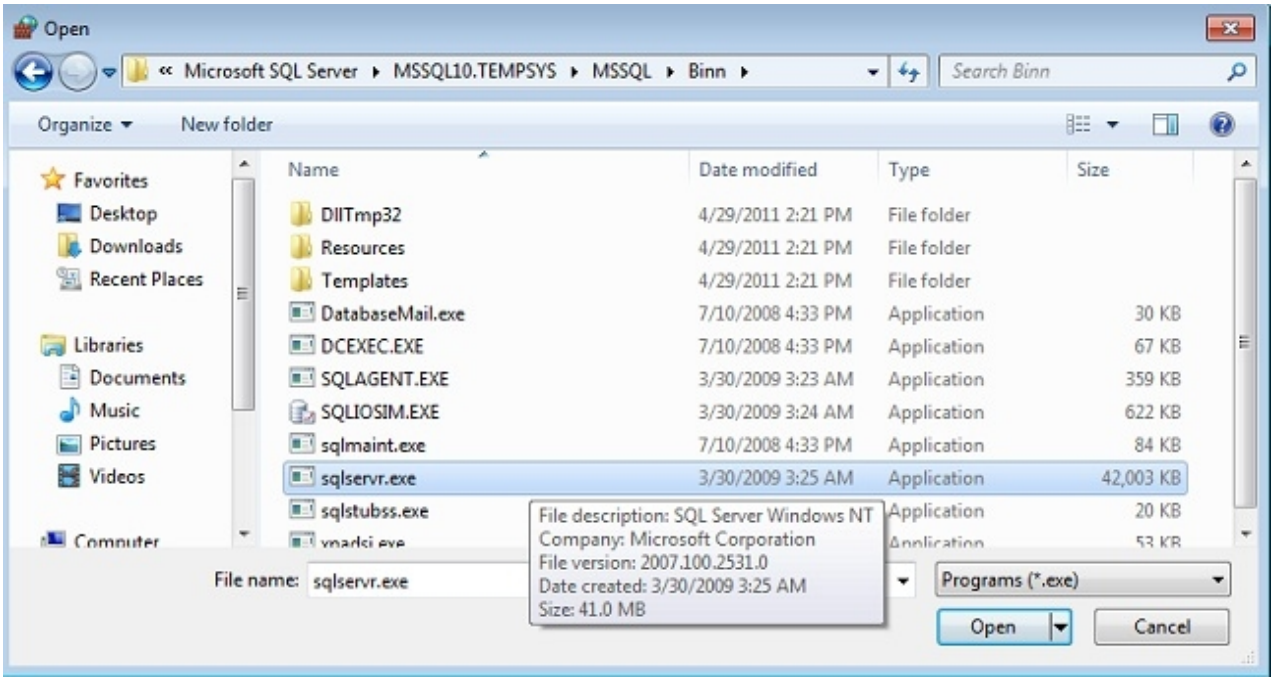

Image 3 – select path to sqlservr.exe file

This will take you back to the "New Inbound Rule Wizard" window. Click on "Next". Select "Allow The Connection" and click on "Next". Make sure that "Domain", "Private", and "Public" are selected, and click on "Next". Type "Tempsys SQL Server" in the "Name" field, and click on "Finish".

Step 2 – Allowing Outbound SQL server traffic

Click on "Start" → "Control Panel" → "Windows Firewall". This will open the main Windows Firewall configuration window.

Click on "Advanced Settings", this will open the "Windows Firewall with Advanced Security" window (see image 1).

Click on "Outbound Rules" → "New Rule". This will open the "New Outbound Rule Wizard" window.

Select "Program" → "Next" → "This program path" → "Browse". This will open a new window that will allow you to browse your file system directory. Browse to C:\Program Files (x86)\Microsoft SQL Server\MSSQL10.TEMPSYS\MSSQL\Binn on 64-bit systems, or to C:\Program Files\Microsoft SQL Server\MSSQL10.TEMPSYS\MSSQL\Binn on 32-bit systems and locate the sqlservr.exe file. Double-click on this file to select it (see image 3).

This will take you back to the "New Outbound Rule Wizard" window. Click on "Next". Select "Allow The Connection" and click on "Next". Make sure that "Domain", "Private", and "Public" are selected, and click on "Next". Type "Tempsys SQL Server" in the "Name" field, and click on "Finish".

Step 3 – Allowing Inbound SQL browser traffic

Click on “Start” → “Control Panel” → “Windows Firewall”. This will open the main Windows Firewall configuration window.

Click on “Advanced Settings”, this will open the “Windows Firewall with Advanced Security” window (see image 1).

Click on “Inbound Rules” → “New Rule”. This will open the “New Inbound Rule Wizard” window (see image 2).

Select “Program” → “Next” → “This program path” → “Browse”. This will open a new window that will allow you to browse your file system directory. Browse to C:\Program Files (x86)\Microsoft SQL Server\90\Shared on 64-bit systems, or to C:\Program Files\Microsoft SQL Server\90\Shared on 32-bit systems and locate the sqlbrowser.exe file. Double-click on this file to select it.

This will take you back to the “New Inbound Rule Wizard” window. Click on “Next”. Select “Allow The Connection” and click on “Next”. Make sure that “Domain”, “Private”, and “Public” are selected, and click on “Next”. Type “Tempsys SQL Browser” in the “Name” field, and click on “Finish”.

Step 4 – Allowing Outbound SQL browser traffic

Click on “Start” → “Control Panel” → “Windows Firewall”. This will open the main Windows Firewall configuration window.

Click on “Advanced Settings”, this will open the “Windows Firewall with Advanced Security” window (see image 1).

Click on “Outbound Rules” → “New Rule”. This will open the “New Outbound Rule Wizard” window.

Select “Program” → “Next” → “This program path” → “Browse”. This will open a new window that will allow you to browse your file system directory. Browse to C:\Program Files (x86)\Microsoft SQL Server\90\Shared on 64-bit systems, or to C:\Program Files\Microsoft SQL Server\90\Shared on 32-bit systems and locate the sqlbrowser.exe file. Double-click on this file to select it.

This will take you back to the “New Outbound Rule Wizard” window. Click on “Next”. Select “Allow The Connection” and click on “Next”. Make sure that “Domain”, “Private”, and “Public” are checked, and click on “Next”. Type “Tempsys SQL Browser” in the “Name” field, and click on “Finish”.

Step 5 – Allowing Inbound HTTP traffic for Thin Client Application

Click on “Start” → “Control Panel” → “Windows Firewall”. This will open the main Windows Firewall configuration window.

Click on “Advanced Settings”, this will open the “Windows Firewall with Advanced Security” window (see image 1).

Click on “Inbound Rules” → “New Rule”. This will open the “New Inbound Rule Wizard” window (see image 2).

Select “Port” → “Next” → Select “TCP” and “Specific Local Ports” and enter the number “80” for the port number, then click on “Next” (see image 4).

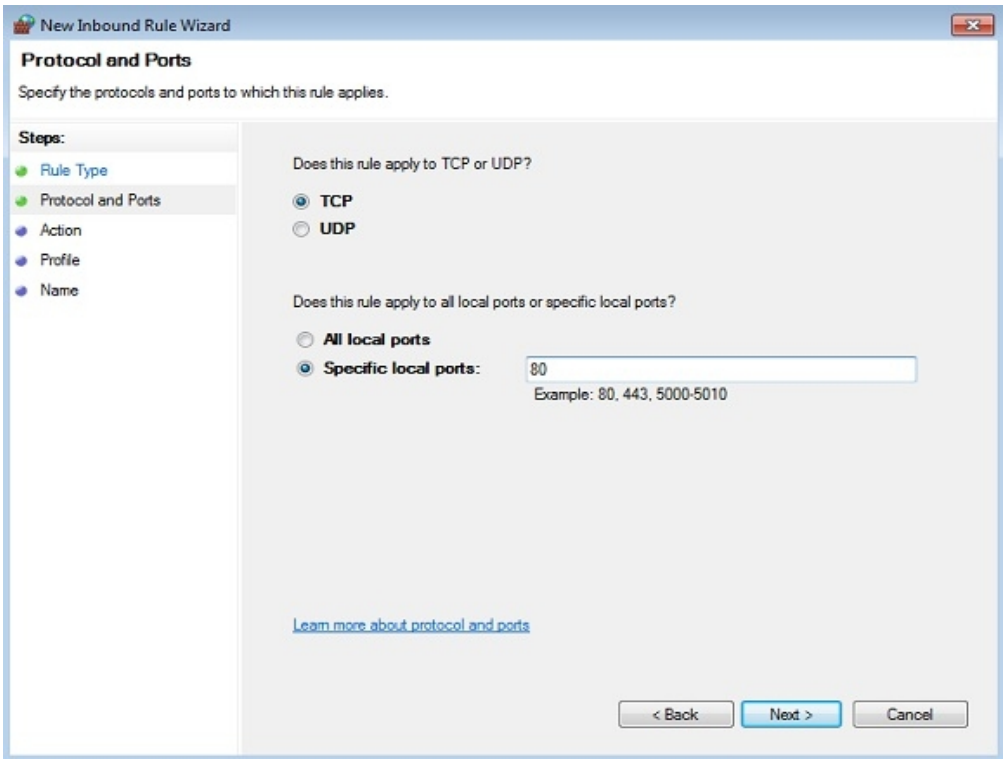

Image 4 - “New Inbound Rule Wizard” TCP port 80

Select “Allow The Connection” and click on “Next”. Make sure that “Domain”, “Private”, and “Public” are selected, and click on “Next”. Type “Tempsys HTTP Thin Client” in the “Name” field, and click on “Finish”.

Step 6 – Allowing Outbound HTTP traffic for Thin Client Application

Click on “Start” → “Control Panel” → “Windows Firewall”. This will open the main Windows Firewall configuration window.

Click on “Advanced Settings”, this will open the “Windows Firewall with Advanced Security” window (see image 1).

Click on “Outbound Rules” → “New Rule”. This will open the “New Outbound Rule Wizard” window.

Select “Port” → “Next” → Select “TCP” and “Specific Local Ports” and enter the number “80” for the port number, then click on “Next” (see image 4).

Select “Allow The Connection” and click on “Next”. Make sure that “Domain”, “Private”, and “Public” are selected, and click on “Next”. Type “Tempsys HTTP Thin Client” in the “Name” field,

and click on “Finish”.

Step 7 – Contacting TempSys for further assistance

- If the Basic Resolution Steps have not successfully corrected the NSC condition, please contact CheckPoint Customer Support for further assistance:
- Customer Support Portal: http://checkpoint.kayako.com – Submit a ticket
- E-Mail: Send an e-mail message to support@tempsys.net and include the following information:
- Your name and contact information (phone and e-mail address)
- Name of your organization
- Description of the problem
- Best time to reach you
- Phone: Call our Support Center Dispatching Center at (510) 526-7624