PANDUIT™ infrastructure for a connected world

smartzone™

Technical Reference 77-SZ

Published: **7/25/18**

Windows Server 2008 Firewall Exception Configuration

Applies to:	Windows Server 2008
Objective:	Windows Server 2008 (WS2008) comes with more security features that must be configured for SmartZone to send and receive messages from other devices in its network.
Pre-Requisites:	An inbound exception rule must be set at the specified server port to receive external messages sent by other devices in the SmartZone network. Likewise, an outbound exception rule must be set to allow messages to exit the specified server port. Failure to configure the inbound and outbound rules for ports listed below will lead to lack of communication. SNMP messages won't be able to pass through server ports 161 and 162.

Description

A step-by-step process on the SmartZone communication ports.

Performing the Procedure

Below are all the server ports that need to be configured for SmartZone to function properly on WS2008. Follow the steps in section 2 (Setting up the Server Ports for Incoming SNMP Messages) and section 3 (Setting up the Server Ports for Outgoing SNMP Messages) for configuring all the applications in Table 1, Table 2, and Table 3.

1. Essential Server Ports for SmartZone Communication

Go to **Windows Firewall** and select **Inbound Rules** to open following ports used by SmartZone:

Application	Protocol	Port Numbers
Naming Port	TCP	10990
RMI	TCP	1099, 10980
PIM Client	TCP	8080
SNMP	UDP	161, 162
ADA	TCP	636
JMS	TCP	8093

Table 1 – Inbound rules

Go to **Windows Firewall** and select **Outbound Rules** to open following ports used by SmartZone:

Application	Protocol	Port Numbers
Naming Port	TCP	10990
RMI	TCP	1099, 10980
SNMP	UDP	161, 162
PIM Client	TCP	8080
ADA	TCP	636

Table 2 – Outbound rules

Go to **Windows Firewall** to open the relevant ports depending on the database configured to communicate with SmartZone:

Application	Protocol	Port Numbers
MySQL	TCP	3306
MS SQL	TCP	1433
DB2.9.5	TCP	5000
DB2.9.7	TCP	6000

Table 3 - Inbound and Outbound rules

2. Setting up the Server Ports for Incoming SNMP Messages

To allow SNMP Messages to pass freely in and out of the server, open port 161 and port 162 as indicated in Table 1 for inbound rules and Table 2 for outbound rules.

1. Click **Start** and select **Administrative Tool**. Then, select **Windows Firewall with Advanced Security**.

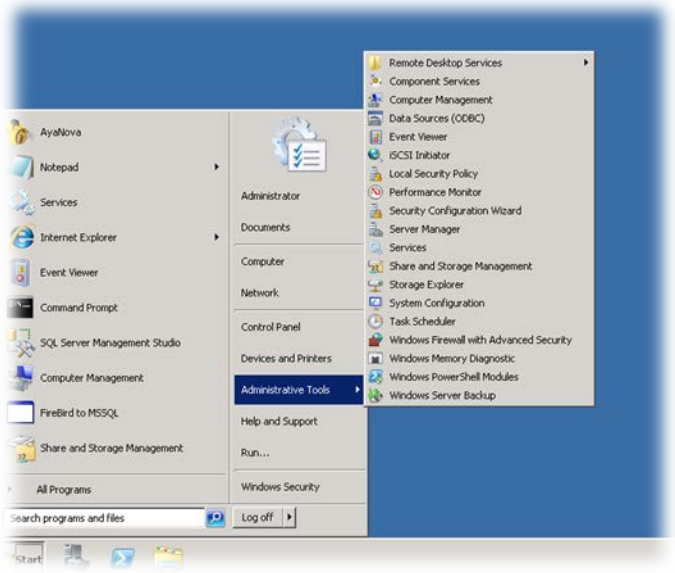

Figure 1 – Administrative Tools

The Firewall with Advanced Security Windows opens and offers on the left options for Inbound Rules and Outbound Rules, among others.

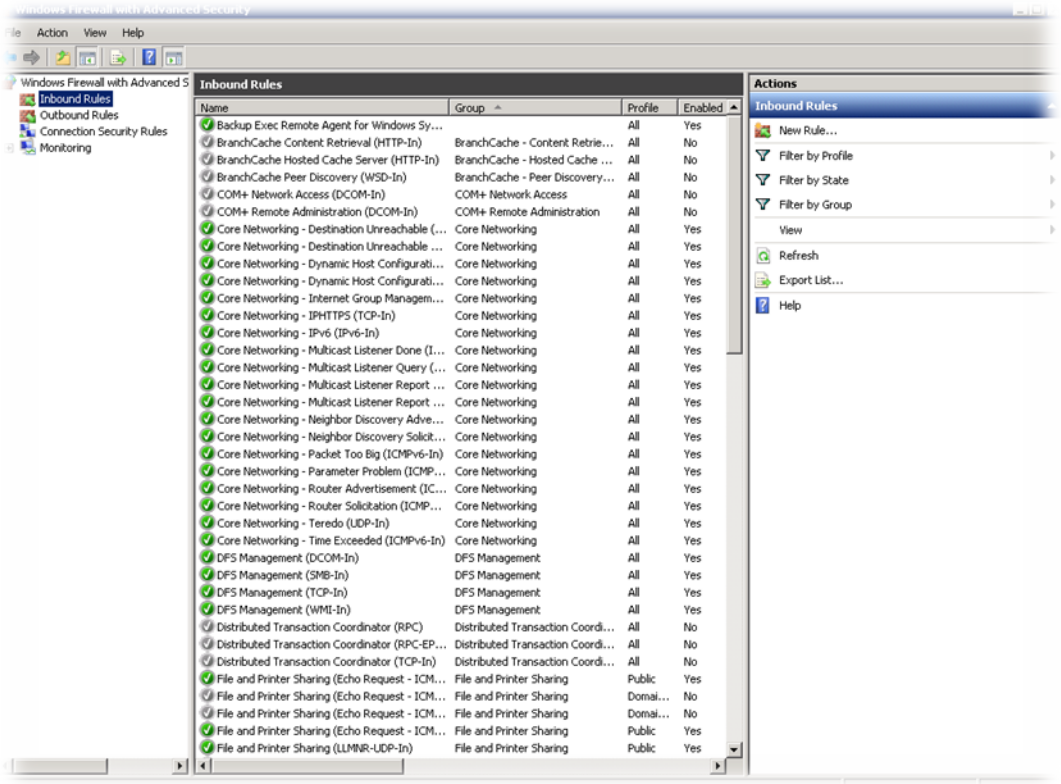

Figure 2 – Windows Firewall with Advanced Security - Inbound Rules

2. Make sure that none of the exceptions (with the gray or green check marks in Figure 2 Windows Firewall with Advanced Security - Inbound Rules) are selected. If an existing rule is selected, the option to create a new rule won't be available when you select **Action**.
3. On the left in Figure 2, select **Inbound Rules**.
4. Click the **Action** menu to create a new Inbound Rules.
5. Fill the name field with a name such as SZ2.
6. Fill the protocol type field with UDP as provided in the Table 1 Inbound rules.

7. Set the Remote port field to All Ports as shown in Figure 3 Windows Firewall with Advanced Security - Inbound Rules.
8. Set the Local port fields to Specific Ports and 161, 162 as shown in Figure 3 Windows Firewall with Advanced Security - Inbound Rules.

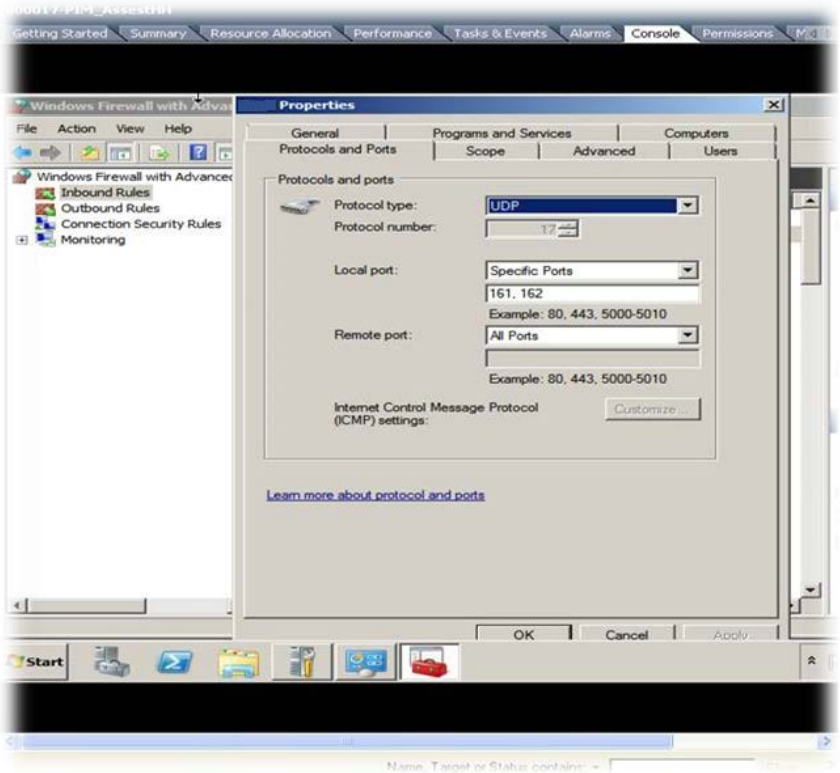

Figure 3 Windows Firewall with Advanced Security - Inbound Rules

9. Click **Save.**

You have completed setting up the server ports for incoming SNMP messages. Next, set up the server ports for outgoing SNMP messages.

3. Setting up the Server Ports for Outgoing SNMP Messages

1. Perform Step 1 from above— Setting up the Server Ports for Incoming SNMP Messages.
2. Make sure that none of the exceptions in Figure 2 are selected.
3. On the left in Figure 2, select **Outbound Rules**.
4. Click the **Action** menu to create a new Outbound Rules.
5. Fill the name field with a name such as SZ2.
6. Fill the protocol type field with **UDP** as provided in the Table 2 Outbound rules.
7. Set the Local port fields to All Ports as shown in Figure 4 Windows Firewall with Advanced Security - Outbound Rules.
8. Set the Remote port field to Specific Ports and 161, 162 as shown in Figure 4 Windows Firewall with Advanced Security - Outbound Rules and Figure 3 Windows Firewall with Advanced Security - Inbound Rules.

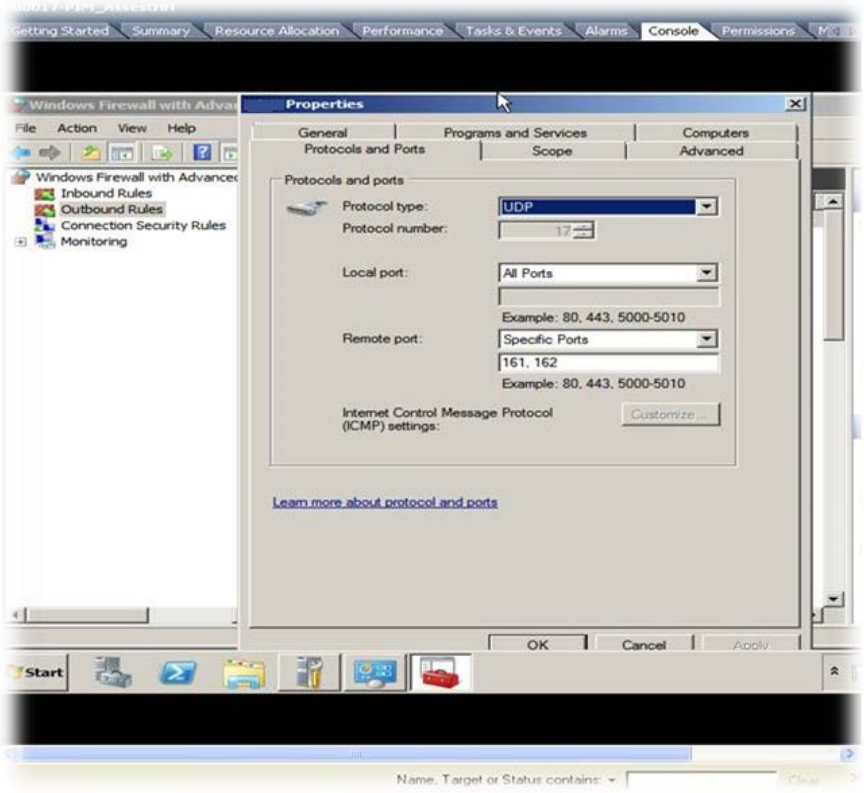

Figure 4 Windows Firewall with Advanced Security - Outbound Rules

9. Press **Save**.
   Similar steps used for setting up SNMP server ports should be followed for configuring all the remaining ports listed in Table 1 and Table 2.

End State

You have successfully set up firewall exceptions for server ports within SmartZone.