Windows Firewall Configuration with Group Policy for SyAM System Client Installation

SyAM System Client can be deployed to systems on your network using SyAM Management Utilities. If Windows Firewall is enabled on target systems, it may be necessary to configure the firewall to allow discovery and deployment. In an Active Directory environment, Group Policy can be used to perform the firewall configuration. In this document we’ll show how to do this on Windows Server 2008 R2. We present two options: create rules to allow firewall exceptions, or disable the firewall.

Option 1: Allow Firewall Exceptions
From the Start menu, go to Administrative Tools – Group Policy Management. In the menu under Domains, find the domain to be configured. Under the domain name, right-click Group Policy Objects. From the menu, select New.

Enter a name for the new Group Policy. Click OK.
Right-click the new policy and choose Edit from the menu.

In the Group Policy Management Editor, navigate to Computer Configuration - Policies - Windows Settings - Security Settings - Windows Firewall with Advanced Security, then expand Windows Firewall with Advanced Security - LDAP://cn=... and under this, select Inbound Rules.
Right-click Inbound Rules and choose New Rule.

First we’ll set up the rules for specific ports. In the New Inbound Rule Wizard, click the Port radio button. Click Next.
Set the rule to apply to TCP and specific port 3894. Click Next.
Set the Action to Allow the connection. Click Next.
You may restrict the scope of the rule. In our example we'll uncheck the Private and Public networks to make the rule apply only when the computer is connected to the domain. When finished, click Next.
Enter a name for the inbound rule. We'll call it SyAM-Agent-3894. Click Finish.
Create another rule for the same port, but specifying the UDP protocol. The same name can be used for the TCP and UDP rules.

Create rules for other ports in the same way. A total of six rules for specific ports will be created:

- NAME: SyAM-Agent-3894, PORT: 3894, PROTOCOL: TCP
- NAME: SyAM-Agent-3894, PORT: 3894, PROTOCOL: UDP
- NAME: SyAM-Health-Updates-3895, PORT: 3895, PROTOCOL: TCP
- NAME: SyAM-Health-Updates-3895, PORT: 3895, PROTOCOL: UDP
- NAME: SyAM-Remote-Console-5800, PORT: 5800, PROTOCOL: TCP
- NAME: SyAM-Remote-Console-5900, PORT: 5900, PROTOCOL: TCP

You can review the rules in Group Policy Management Editor to verify that everything is correct.
Now we can create the predefined rules. Right-click Inbound Rules and choose New Rule. In the New Inbound Rule Wizard, click the Predefined radio button. From the drop down menu, choose Core Networking. Click Next.

The wizard displays the rules defined by the Core Networking rule group. Leave all rules selected. Click Next.
Set the Action to Allow the connection. Click Finish.
Create the other predefined rules in the same way, for a total of six groups:

- Core Networking
- File and Printer Sharing
- Netlogon Service
- Network Discovery
- Remote Administration
- Remote Desktop

As we did with the rules for individual ports, the predefined rules can be restricted in scope, but this must be done for each individual rule in a group. Right-click a rule and choose Properties.
Click the Advanced tab. We'll deselect Private and Public profiles, leaving only Domain enabled. Click OK.
Repeat for each rule to be modified. You can then review the rules in the Group Policy Management Editor.
Close the Group Policy Management Editor. In the Group Policy Management console, we can link the new policy to an Organizational Unit. Right-click the OU and choose Link an Existing GPO.

Select the Group Policy Object. Click OK.
Apply the Group Policy to other organizational units in the same way. Allow enough time for the policy update to propagate to client systems. By default this will be between 60 and 120 minutes. Once the target machines have the updated firewall settings, you can proceed with network discovery and deployment of SyAM System Client.

**Option 2: Disable Windows Firewall**

From the Start menu, go to Administrative Tools – Group Policy Management. In the menu under Domains, find the domain to be configured. Under the domain name, right-click Group Policy Objects. From the menu, select New.
Enter a name for the new Group Policy. Click OK.

Right-click the new policy and choose Edit from the menu.
Find the setting Windows Firewall: Protect all network connections. Right-click the setting and choose Edit.
Click the Disabled radio button. Click OK.
This will disable Windows Firewall for the domain profile. Repeat for Standard Profile if desired.

Close the Group Policy Management Editor. In the Group Policy Management console, we can link the new policy to an Organizational Unit. Right-click the OU and choose Link an Existing GPO.
Select the Group Policy Object. Click OK.
Apply the Group Policy to other organizational units in the same way. Allow enough time for the policy update to propagate to client systems. By default this will be between 60 and 120 minutes. Once the target machines have the updated firewall settings, you can proceed with network discovery and deployment of SyAM System Client.