How to Configure the Windows Server 2012 R2 Firewall

Applies to
SecureAuth IdP 8.2 on Windows Server 2012 R2

Introduction
This article explains how to manage the Windows Advanced Firewall on a SecureAuth IdP Appliance. For documentation on configuring a perimeter firewall, see the support document Network Communication Requirements for SecureAuth IdP 8.2.

Configuration Steps

Firewall Settings Management

Windows Firewall with Advanced Security is a host-based firewall included with Windows Server 2012 and enabled by default on all SecureAuth IdP appliances. Firewall settings within Windows Server 2012 are managed from within the Windows Firewall MMC (Microsoft Management Console). Do the following to review and configure firewall settings:

1. Open Windows Firewall with Advanced Security
   a. Click Start > All Programs > Administrative Tools > Windows Firewall with Advanced Security.
   b. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.
   a. Open a command window.
   b. Type `wf.msc` and press Enter.
   c. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.

2. First review the Required Rules to ensure they are securely configured, then review the Optional Rules to see which of them should be activated in your environment.

Required Rules

DNS

By default, the DNS rules on the SecureAuth IdP Appliance allow it to communicate with any DNS server for greater ease during the initial configuration. Post configuration security best practices recommend restricting communication to only trusted DNS servers on your network. Follow the instructions below to only include DNS traffic from DNS servers within your organization.
1. Select **Outbound Rules** on the left side of the management console.

2. Locate the rule titled **Core Networking - DNS (UDP-Out)** and click the **Properties** button in the **Actions** section of the management console.

3. In the **Core Networking - DNS (UDP-Out) Properties** window, select the **Scope** tab.

4. In the **Remote IP Address** section, select the **These IP Addresses**: radio button, then click the **Add...** button.

5. In the **IP Address** window, enter the IP for your trusted DNS server.

6. When you have finished adding all of the IPs for your DNS servers, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound rule allowing DNS requests over UDP</td>
<td>Outbound</td>
<td>53</td>
<td>UDP</td>
</tr>
</tbody>
</table>

7. Locate the rule titled **SecureAuth - Allow DNS (TCP-Out)** and click the **Properties** button in the **Actions** section of the management console.

8. In the **SecureAuth - Allow DNS (TCP-Out) Properties** window, select the **Scope** tab.

9. In the **Remote IP Address** section, select the **These IP Addresses**: radio button, then click the **Add...** button.

10. In the **IP Address** window, enter the IP for your trusted DNS server.

11. When you have finished adding all of the IPs for your DNS servers, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound rule to allow DNS requests over TCP</td>
<td>Outbound</td>
<td>53</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**Network Time Protocol (NTP)**

By default, the NTP rule on the SecureAuth IdP Appliance allows it to communicate with any (S)NTP server for greater ease during the initial configuration. Post configuration security best practices recommend restricting communication to only trusted (S)NTP servers on your network. Follow the instructions below to permit NTP traffic only to servers within your organization.
1. Select **Outbound Rules** on the left side of the management console.

2. Locate the rule titled **SecureAuth - Allow NTP** and click the **Properties** button in the **Actions** section of the management console.

3. In the **SecureAuth - Allow NTP Properties** window, select the **Scope** tab.

4. In the **Remote IP Address** section, select the **These IP Addresses**: radio button, then click the **Add...** button.

5. In the **IP Address** window, enter the IP for your trusted (S)NTP server, then click the **Add** button.

6. When you have finished adding all of the IPs for your NTP servers, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>The preferred (S)NTP server</td>
<td>Outbound</td>
<td>123</td>
<td>UDP</td>
</tr>
</tbody>
</table>

**Remote Desktop**

By default, a SecureAuth IdP Appliance allows any IP address to initiate a Remote Desktop session for greater ease during the initial configuration. Post configuration security best practices recommend restricting communication to only trusted IPs or a range of trusted IPs to maximize security on the appliance. Follow the instructions below to restrict Remote Desktop traffic.
1. Select **Inbound Rules** on the left side of the management console.

2. Locate the rule titled **Remote Desktop - User Mode (UDP-In)** and click the **Properties** button in the **Actions** section of the management console.

3. In the **Remote Desktop - User Mode (UDP-In) Properties** window, select the **Scope** tab.

4. In the **Remote IP Address** section, select the **These IP Addresses**: radio button, then click the **Add...** button.

5. In the **IP Address** window, enter an IP or network range.

6. When you have finished adding all of the IPs or network ranges, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow RDP traffic for Desktop</td>
<td>Inbound</td>
<td>3389</td>
<td>UDP</td>
</tr>
</tbody>
</table>

7. Locate the rule titled **Remote Desktop - User Mode (TCP-In)** and click the **Properties** button in the **Actions** section of the management console.

8. In the **Remote Desktop - User Mode (TCP-In) Properties** window, select the **Scope** tab.

9. In the **Remote IP Address** section, select the **These IP Addresses**: radio button, then click the **Add...** button.

10. In the **IP Address** window, enter an IP or network range.

11. When you have finished adding all of the IPs or network ranges, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow RDP traffic for Desktop</td>
<td>Inbound</td>
<td>3389</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**Optional Rules**

**Active Directory / LDAP**

If the SecureAuth IdP Appliance will be communicating with a Microsoft **Active Directory (AD)** domain controller or an **LDAP** server, the following rules must be enabled and configured:
1. Select **Outbound Rules** on the left side of the management console.

![Image of Windows Firewall with Advanced Security](image)

2. Locate the rule titled **SecureAuth - Allow Active Directory-LDAP (TCP-Out)** and click the **Properties** button in the **Actions** section of the management console.

3. In the **SecureAuth - Allow Active Directory-LDAP (TCP-Out) Properties** window, select the **General** tab.

4. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

5. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

6. Click the **Add...** button, and in the **IP Address** window, enter an IP for an AD/LDAP server.

7. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound traffic to AD/LDAP</td>
<td>Outbound</td>
<td>88,389,636,3268,3269</td>
<td>TCP</td>
</tr>
</tbody>
</table>

8. Locate the rule titled **SecureAuth - Allow Active Directory-LDAP (UDP-Out)** and click the **Properties** button in the **Actions** section of the management console.

9. In the **SecureAuth - Allow Active Directory-LDAP (UDP-Out) Properties** window, select the **General** tab.

10. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

11. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

12. Click the **Add...** button, and in the **IP Address** window, enter an IP for an AD/LDAP server.

13. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound traffic to AD/LDAP</td>
<td>Outbound</td>
<td>88,389</td>
<td>UDP</td>
</tr>
</tbody>
</table>

**Active Directory Password Reset**

If the SecureAuth IdP Appliance will be using Microsoft **Active Directory** as a Data Store and you would like to leverage the Password Reset IdM functionality, the following rules must be enabled and configured:
1. Select **Outbound Rules** on the left side of the management console.

2. Locate the rule titled **SecureAuth - Allow Active Directory Password Reset (TCP-Out)** and click the **Properties** button in the **Actions** section of the management console.

3. In the **SecureAuth - Allow Active Directory Password Reset (TCP-Out) Properties** window, select the **General** tab.

4. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

5. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

6. Click the **Add...** button, and in the **IP Address** window, enter an IP for an Active Directory Domain Controller.

7. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound traffic to AD for Password Reset</td>
<td>Outbound</td>
<td>139,445,464</td>
<td>TCP</td>
</tr>
</tbody>
</table>

8. Locate the rule titled **SecureAuth - Allow Active Directory Password Reset (UDP-Out)** and click the **Properties** button in the **Actions** section of the management console.

9. In the **SecureAuth - Allow Active Directory Password Reset (UDP-Out) Properties** window, select the **General** tab.

10. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

11. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

12. Click the **Add...** button, and in the **IP Address** window, enter an IP for an Active Directory Domain Controller.

13. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound traffic to AD for Password Reset</td>
<td>Outbound</td>
<td>445,464</td>
<td>UDP</td>
</tr>
</tbody>
</table>

**Joining a Domain**

If the SecureAuth IdP Appliance will be joined to a Microsoft **Active Directory** domain, the following rules must be enabled and configured:
1. Select **Outbound Rules** on the left side of the management console.

2. Locate the rule titled **SecureAuth - Allow Domain Membership (TCP-Out)** and click the **Properties** button in the **Actions** section of the management console.

3. In the **SecureAuth - Allow Domain Membership (TCP-Out) Properties** window, select the **General** tab.

4. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

5. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

6. Click the **Add...** button, and in the **IP Address** window, enter an IP for an Active Directory Domain Controller.

7. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound traffic for AD Domain</td>
<td>Outbound</td>
<td>389,636,3268,3269,88,445,139,1025-5000,49152-65535</td>
<td>TCP</td>
</tr>
</tbody>
</table>

8. Locate the rule titled **SecureAuth - Allow Domain Membership (UDP-Out)** and click the **Properties** button in the **Actions** section of the management console.

9. In the **SecureAuth - Allow Domain Membership (UDP-Out) Properties** window, select the **General** tab.

10. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

11. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

12. Click the **Add...** button, and in the **IP Address** window, enter an IP for an Active Directory Domain Controller.

13. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound traffic for AD Domain</td>
<td>Outbound</td>
<td>389,88,445,137,138,1025-5000,49152-65535</td>
<td>UDP</td>
</tr>
</tbody>
</table>

**SQL**

If the SecureAuth IdP Appliance will use a SQL server as a Data Store and/or for reporting, the following rule must be enabled and configured:
1. Select **Outbound Rules** on the left side of the management console.

![Windows Firewall with Advanced Security](image)

2. Locate the rule titled **SecureAuth - Allow SQL** and click the **Properties** button in the **Actions** section of the management console.

3. In the **SecureAuth - Allow SQL Properties** window, select the **General** tab.

4. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

5. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

6. Click the **Add...** button, and in the **IP Address** window, enter an IP address for a SQL server.

7. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound SQL traffic</td>
<td>Outbound</td>
<td>1433</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**SMTP**

If the SecureAuth IdP Appliance will send One Time Passwords (OTP) via Email, the following rule must be enabled and configured:
1. Select **Outbound Rules** on the left side of the management console.

2. Locate the rule titled **SecureAuth - Allow SMTP** and click the **Properties** button in the **Actions** section of the management console.

3. In the **SecureAuth - Allow SMTP Properties** window, select the **General** tab.

4. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

5. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

6. Click the **Add...** button, and in the **IP Address** window, enter an IP address for a SMTP server.

7. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound SMTP traffic</td>
<td>Outbound</td>
<td>25</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**Syslog**

If the SecureAuth IdP Appliance will be using Syslog for reporting, the following rule must be enabled and configured:
1. Select **Outbound Rules** on the left side of the management console.

![Windows Firewall with Advanced Security](Image)

2. Locate the rule titled **SecureAuth - Allow Syslog** and click the **Properties** button in the **Actions** section of the management console.

3. In the **SecureAuth - Allow Syslog Properties** window, select the **General** tab.

4. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

5. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

6. Click the **Add..** button, and in the **IP Address** window, enter an IP address for a Syslog server.

7. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound Syslog traffic</td>
<td>Outbound</td>
<td>514</td>
<td>UDP</td>
</tr>
</tbody>
</table>

**RADIUS**

If the SecureAuth IdP Appliance will be hosting the RADIUS service, the following rule must be enabled and configured:
1. Select **Inbound Rules** on the left side of the management console.

2. Locate the rule titled **SecureAuth - Allow RADIUS** and click the **Properties** button in the **Actions** section of the management console.

3. In the **SecureAuth - Allow RADIUS Properties** window, select the **General** tab.

4. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

5. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

6. Click the **Add...** button, and in the **IP Address** window, enter an IP address for a RADIUS server.

7. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound RADIUS traffic</td>
<td>Outbound</td>
<td>1812,1813</td>
<td>UDP</td>
</tr>
</tbody>
</table>

**SecureAuth Filesync Service**

If the SecureAuth IdP Appliance will be participating in a FileSync cluster, the following rules must be enabled and configured:

1. Select **Outbound Rules** on the left side of the management console.

2. Locate the rule titled **SecureAuth - Allow SecureAuth Filesync Service (TCP-Out)** and click the **Properties** button in the **Actions** section of the management console.

3. In the **SecureAuth - Allow SecureAuth Filesync Service (TCP-Out) Properties** window, select the **General** tab.

4. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.
5. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

6. Click the **Add...** button, and in the **IP Address** window, enter the IP address of another cluster member.

7. Repeat step 6 until all cluster member IPs (except for the one being configured) have been entered.

8. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound Filesync Service traffic</td>
<td>Outbound</td>
<td>139,445</td>
<td>TCP</td>
</tr>
</tbody>
</table>

9. Locate the rule titled **SecureAuth - Allow SecureAuth Filesync Service (UDP-Out)** and click the **Properties** button in the **Actions** section of the management console.

10. In the **SecureAuth - Allow SecureAuth Filesync Service (UDP-Out) Properties** window, select the **General** tab.

11. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

12. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

13. Click the **Add...** button, and in the **IP Address** window, enter the IP address of another cluster member.

14. Repeat step 12 until all cluster member IPs (except for the one being configured) have been entered.

15. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound Filesync Service traffic</td>
<td>Outbound</td>
<td>137,138</td>
<td>UDP</td>
</tr>
</tbody>
</table>

16. Select **Inbound Rules** on the left side of the management console.

17. Locate the rule titled **SecureAuth - Allow SecureAuth Filesync Service (TCP-In)** and click the **Properties** button in the **Actions** section of the management console.

18. In the **SecureAuth - Allow SecureAuth Filesync Service (TCP-In) Properties** window, select the **General** tab.

19. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

20. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

21. Click the **Add...** button, and in the **IP Address** window, enter the IP address of another cluster member.

22. Repeat step 21 until all cluster member IPs (except for the one being configured) have been entered.

23. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow inbound Filesync Service traffic</td>
<td>Inbound</td>
<td>139,445</td>
<td>TCP</td>
</tr>
</tbody>
</table>
24. Locate the rule titled **SecureAuth - Allow SecureAuth Filesync Service (UDP-In)** and click the **Properties** button in the **Actions** section of the management console.

25. In the **SecureAuth - Allow SecureAuth Filesync Service (UDP-In) Properties** window, select the **General** tab.

26. In the **General** section, tick the **Enabled** checkbox and click the **Apply** button.

27. Select the **Scope** tab, and in the **Remote IP Address** section, select the **These IP Addresses**: radio button.

28. Click the **Add...** button, and in the **IP Address** window, enter the IP address of another cluster member.

29. Repeat step 21 until all cluster member IPs (except for the one being configured) have been entered.

30. When you have finished adding all of the IPs, click the **OK** button to accept the changes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Direction</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow inbound Filesync Service traffic</td>
<td>Inbound</td>
<td>137,138</td>
<td>UDP</td>
</tr>
</tbody>
</table>