Optimal firewall configuration

Covers Citrix SaaS products involving our servers as of November 2013

Citrix SaaS products are configured to work outbound through ports 8200, 80 or 443. In a restricted environment, port 8200 can be set up for outbound connections. Our products do not listen for, nor do they require, any inbound connections. Connections outbound via port 8200 are optimal, although connections through ports 80 and 443 can also be used.

Integrated Voice over IP connections are configured to work outbound through UDP port 8200. Integrated webcam video support is configured through UDP port 1853.

For most firewall or proxy systems, we recommend specifying a whitelist of DNS addresses for Citrix services so outbound connections can be made. The list of Citrix domains currently includes but is not limited to the following:

```
*assist.com
*.citrixonline.com
*.citrixonlinecdn.com
*.cloudfront.net
*.expertcity.com
*.fastsupport.com
*.go2assist.me
*.gofastchat.com
*.gotoassist.com
*.gotoassist.me
*.gotomeet.me
*.gotomeeting.com
*.gotomypc.com
*.gototraining.com
*.gotowebinar.com
*.helpmefast.com
*.hu.tt
*.joingetmeeting.com
*.joingototraining.com
*.joinwebinar.com
*.openvoice.com
*.osdimg.com
*.podio.com
*.securevdr.com
*.sf-api.com
*.sf-api.eu
*.sharefile.com
*.sharefile.eu
*.sharefileftp.com
*.sharefile-webdav.com
```

Important Note: The next steps below are discouraged unless absolutely necessary because our IP ranges and those of our provider networks need to be periodically audited and modified, creating additional maintenance to your network. These changes are necessary to continue to provide the maximum performance for the Citrix SaaS family of applications. Maintenance and failover events may cause you to connect to servers within any of the ranges.
If your firewall includes a content or application data scanning filter, this may cause blocking or latency, which would be indicated in the log files for the filter. To address this problem, verify the below IP ranges will not be scanned or filtered by content or application data scanning filters by specifying exception IP ranges that will not be filtered.

If your security policy requires you to specify explicit IP ranges, then configure your firewall to limit port 8200 or 80 or 443 destination, UDP ports 8200 and 1853 and IP addresses to only the Citrix ranges and those of our provider networks given below.

### Citrix server / Datacenter IP addresses for use in firewall configurations

<table>
<thead>
<tr>
<th>Citrix Assigned Range by Block</th>
<th>Numeric IP Address Range</th>
<th>Netmask Notation</th>
<th>CIDR Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block 1</td>
<td>216.115.208.0 - 216.115.223.255</td>
<td>216.115.208.0/20</td>
<td>216.115.208.0/20</td>
</tr>
<tr>
<td>Block 2</td>
<td>216.219.112.0 - 216.219.127.255</td>
<td>216.219.112.0/20</td>
<td>216.219.112.0/20</td>
</tr>
<tr>
<td>Block 3</td>
<td>66.151.158.0 - 66.151.158.255</td>
<td>66.151.158.0/24</td>
<td>66.151.158.0/24</td>
</tr>
<tr>
<td>Block 5</td>
<td>66.151.115.128 - 66.151.115.191</td>
<td>66.151.115.128/26</td>
<td>66.151.115.128/26</td>
</tr>
<tr>
<td>Block 6</td>
<td>64.74.80.0 - 64.74.80.255</td>
<td>64.74.80.0/24</td>
<td>64.74.80.0/24</td>
</tr>
<tr>
<td>Block 8</td>
<td>67.217.64.0 - 67.217.95.255</td>
<td>67.217.64.0/19</td>
<td>67.217.64.0/19</td>
</tr>
<tr>
<td>Block 9</td>
<td>78.108.112.0 - 78.108.127.255</td>
<td>78.108.112.0/20</td>
<td>78.108.112.0/20</td>
</tr>
<tr>
<td>Block 10</td>
<td>68.64.0.0 - 68.64.31.255</td>
<td>68.64.0.0/24</td>
<td>68.64.0.0/24</td>
</tr>
<tr>
<td>Block 11</td>
<td>206.183.100.0 - 206.183.103.255</td>
<td>206.183.100.0/22</td>
<td>206.183.100.0/22</td>
</tr>
<tr>
<td>Block 12</td>
<td>173.199.0.0 - 173.199.63.255</td>
<td>173.199.0.0/18</td>
<td>173.199.0.0/18</td>
</tr>
<tr>
<td>Block 13</td>
<td>103.15.16.0 - 103.15.19.255</td>
<td>103.15.16.0/22</td>
<td>103.15.16.0/22</td>
</tr>
<tr>
<td>Block 15</td>
<td>140.207.108.0 - 140.207.109.255</td>
<td>140.207.108.0/23</td>
<td>140.207.108.0/23</td>
</tr>
</tbody>
</table>

Citrix scales its services into third-party cloud and carrier networks for improved performance. To ensure continuous uptime, Citrix also maintains datacenters in San Jose, Las Vegas, Chicago, New York, Atlanta, Washington D.C., Hong Kong, Sydney, Amsterdam, Frankfurt, Bangalore and Shanghai.

Information about the IP ranges of our provider networks is available in these third-party references.

**IP ranges for the content delivery network (CDN)**

**IP ranges for other services (audio, video and screen sharing)**