How to create a firewall rule for RDP and VNC on Windows

Users on campus aren’t supposed to have RDP and VNC ports open to the public. This guide will help lock it down to on-premises and VPN

Step-by-step guide

Open Firewall with Advanced Security. You can get here by opening Control Panel > System and Security > Administrative Tools > Windows Firewall with Advanced Security:
1. Left click on “Inbound Rules”
2. Click “New Rule” on the right side of the window
3. Click the “port” option
4. For the Specific local ports, enter (exactly as displayed):
   
<table>
<thead>
<tr>
<th>Port 1</th>
<th>Port 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>5900</td>
<td>3389</td>
</tr>
</tbody>
</table>

5. Click “Block the connection”
6. Click Leave Domain, Private and Public checked
7. Name it “@Restrict off-campus remote access”

Once the rule is created, find it in the list, so we can make sure the rule only applies to off-campus:
1. Right-click the rule you just created, and click Properties
2. Click on the Scope tab
   a. Under Remote IP Address, click These IP Addresses
   b. Click Add
   c. Enter the following, one at a time, under “This IP Range” and continue until all of the IP ranges are entered:
      i. 0.0.0.0 - 9.255.255.255
      ii. 11.0.0.0 - 128.61.255.255
      iii. 128.63.0.0 - 128.82.255.255
      iv. 128.84.0.0 - 129.115.255.255
      v. 129.117.0.0 - 146.5.255.255
      vi. 146.7.0.0 - 172.15.255.255
      vii. 172.32.0.0 - 192.167.255.255
      viii. 192.169.0.0 - 198.213.191.255
      ix. 192.214.0.0 - 198.214.227.255
      x. 198.214.230.0 - 206.76.136.255
      xi. 206.76.138.0 - 255.255.255.255

Related articles

- How to create a firewall rule for RDP and VNC on Windows