**Firewall Rules for Migration of ArcGIS WebGISDR**

**Introduction**

This document provides instructions for setting up firewall rules to prevent communication between prod and testing environments. These rules are applied locally on Windows Server firewalls to isolate each environment and prevent "cross talk" or unauthorized access between test servers (which may use production data) and the Production servers when attempting to do a restore of prod data or maybe just having a second availability environment.

**Scope**

These instructions apply to administrators responsible for network configuration and security on gis servers. The document provides detailed steps for configuring firewall rules on Windows Server to block IP-based communication between servers in the Production environment and testing environment. The firewall rules should be applied on both environments to fully isolate traffic (if they have the same DNS name)

**Purpose**

The purpose of this guidance is to implement secure network isolation between the Production and Vortex environments, preventing cross-environment "cross talk" or data access that could compromise data integrity or security. These firewall rules will block all IP-based connections between specified servers, allowing each environment to operate independently. This separation supports compliance with security requirements and reduces the risk of accidental or unauthorized data access.

**Step-by-Step Firewall Rule Configuration**

1. **Open the Windows Firewall Configuration:**
   * Display the Windows Run dialog box by pressing the **Win + R** keys (the Windows key and the “R” key at the same time).
   * Type Control Panel and press **Enter** to open the Control Panel.
2. **Navigate to Windows Defender Firewall:**
   * Go to **Control Panel > System and Security > Windows Defender Firewall**.
   * Select **Advanced Settings** to open the **Windows Firewall with Advanced Security** dialog box.
3. **Create a New Inbound Rule:**
   * Click on **Inbound Rules** in the left pane.
   * In the Actions panel on the right-hand side, click on **New Rule…** to set up a new rule.
4. **Configure the Rule in the New Inbound Rule Wizard:**
   * **Rule Type:** Select **Custom** and click **Next**.
   * **Program:** Select **All programs** and click **Next**.
   * **Protocol and Ports:** Accept the default settings and click **Next**.
   * **Scope:** Select **These IP addresses** under “Which remote IP addresses does this rule apply to?” Then click **Add…**.
5. **Specify IP Addresses to Block:**
   * In the **IP Address** dialog box, choose **This IP address or subnet** and enter the IP address. Click **OK** to add it.

Graphical user interface, application

Description automatically generated

* + **Production Environment:** Add the following IP addresses to block access to testing env:
    - Localhost.domain(test) - 10.236.2.248
    - Localhost.domain(test) - 10.236.2.251
    - Localhost.domain(test) - 10.236.2.252
    - Localhost.domain (test) - 10.236.2.253
    - Localhost.domain (test) - 10.236.2.254
  + **Testing Environment:** Add the following IP addresses to block access to Production:
    - Localhost.domain(prod) - 10.236.1.222
    - Localhost.domain(prod) - 10.236.1.221
    - Localhost.domain(prod) - 10.236.1.196
    - Localhost.domain(prod) - 10.236.1.199
    - Localhost.domain(prod) - 10.236.2.247
    - Localhost.domain(prod) - 10.236.58.23
    - Localhost.domain(prod) - 10.236.2.234

Graphical user interface, text, application

Description automatically generated

1. **Set the Action for the Rule:**
   * Choose **Block the connection** to prevent access for the specified IP addresses and click **Next**.
2. **Select the Profile for the Rule:**
   * Choose the applicable profile(s) (Domain, Private, Public). By default, all three are selected. Click **Next**.
3. **Name and Finish the Rule Setup:**
   * **Production Servers:** Name: "Deny Access to Testing Servers" | Description: "This rule is used to deny IP communications from Production servers to test servers."
   * **Test Servers:** Name: "Deny Access to Production Servers" | Description: "This rule is used to deny IP communications from test servers to Production servers."
   * Click **Finish** to save the rule.

**Test and Verify Firewall Rules**

1. **Testing from Each Environment:**
   * **Ping Test:** Run ping <ipaddress> -t to try and reach IPs in the other environment. A successful firewall rule will prevent any connection.
   * **Application Access Test:** Attempt access to shared services or applications (like the admin URL) between environments. Confirm the block if connectivity is denied.

This setup effectively isolates the two environments, ensuring that neither can communicate with the other across your network.