**Windows XP/Vista/7/8/10 Firewall Checklist**

Windows User Firewalls is user-friendly and very GUI-dependent

Group policies can be leveraged to mandate certain firewall rules.

**1. Check status**

* Ensure Windows Firewall is turned on
  + Click on Windows button
  + Type “firewall”
  + Click first result
  + If all bars are red
    - Not “recommended settings”
    - Might all be “Off”
    - Expand all bars and make sure none are listed as “Windows Firewall state: Off”
    - As necessary to not conflict with services or the Group Policy, look at panel on left
      * Click “Turn Windows Firewall on or off”
      * Select proper status of firewall
  + If some bars are red
    - Most likely
    - Not “recommended settings”
    - Expand all bars and make sure none are listed as “Windows Firewall state: Off”
    - As necessary to not conflict with services or the Group Policy, look at panel on left
      * Click “Turn Windows Firewall on or off”
      * Select proper status of firewall
  + If all bars are green
    - Windows Firewall ‘works’

**2. Update Microsoft Firewall**

* Click “Troubleshoot my network”
  + Install any updates

**3. Check Individual Rules**

* Click “Advanced settings”
  + If group policy, ensure group policy enabled
  + If not
    - Click “Inbound Rules”

**Observe current rules, compare to connection issues**

* + - * + Click on rules to edit existing rules
        + Click “Add Rule” to add new rules

Select rule type from list

Choose program(s), protocol(s), port(s), and/or address(es) affected

Choose action to take

Choose when to apply rule

Name the rule

Give appropriate description

* + - Click “Outbound Rules”

**Observe current rules, compare to connection issues**

* + - * + Click on rules to edit existing rules
        + Click “Add Rule” to add new rules
  + Click on “Monitoring”
    - Click on services you would like monitored
    - Take note of file path of log