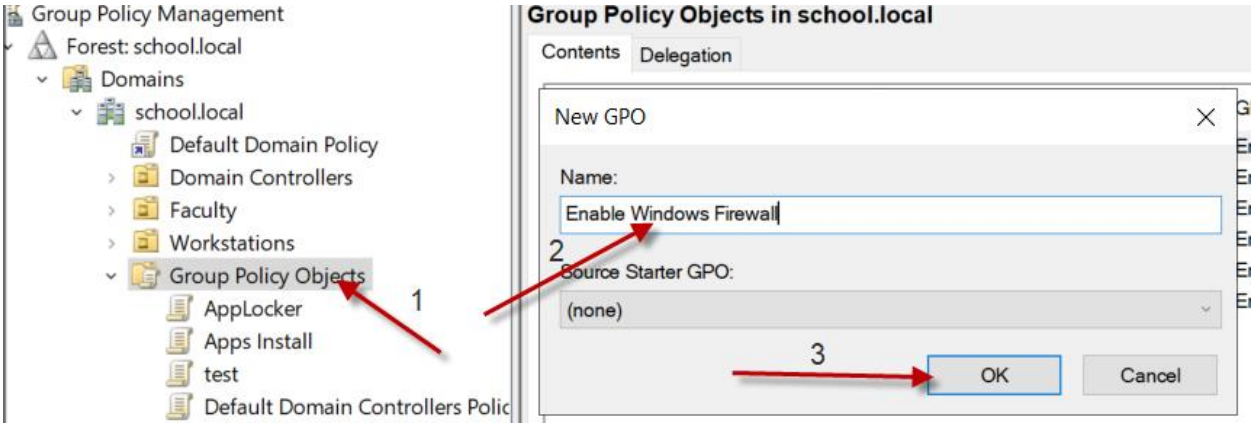
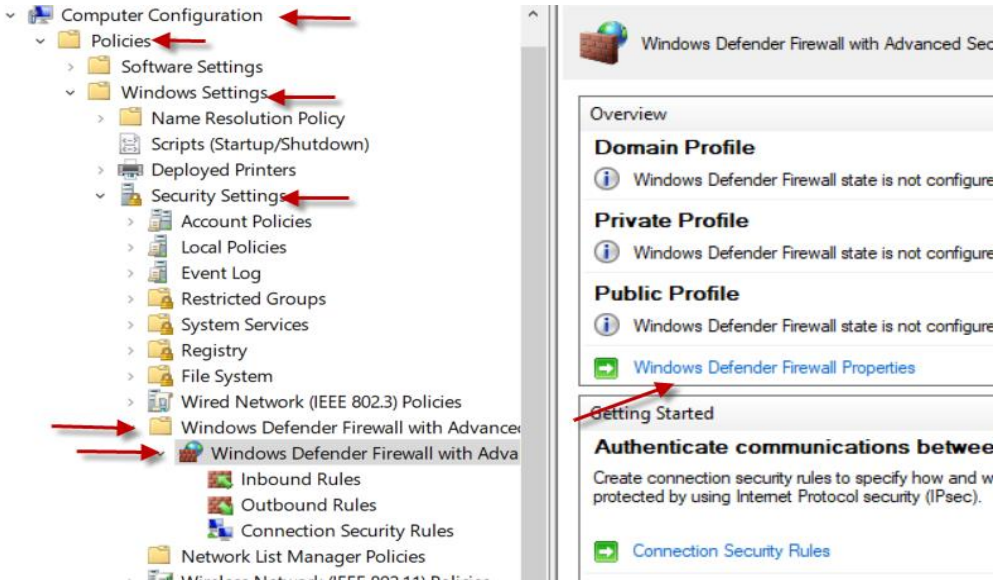
Enable Windows Firewall via GPO

VERY IMPORTANT! DO NOT APPLY THIS POLICY UNTIL COMPLETLEY CONFIGURED!!

1. Open Group Policy Management
    a. Expand Domain and Right Click on Group Policy Objects
    b. Select New
    c. Name: Enable Windows Firewall

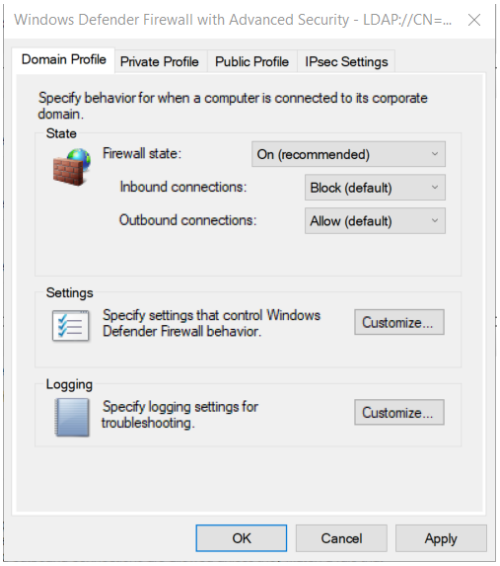


2. Right Click the newly created GPO and select Edit
    a. Expand Computer Configuration>Policies>Windows Settings>Security Settings
    b. Open Windows Defender Firewall with Advanced Security
    c. Click Windows Defender Firewall Properties

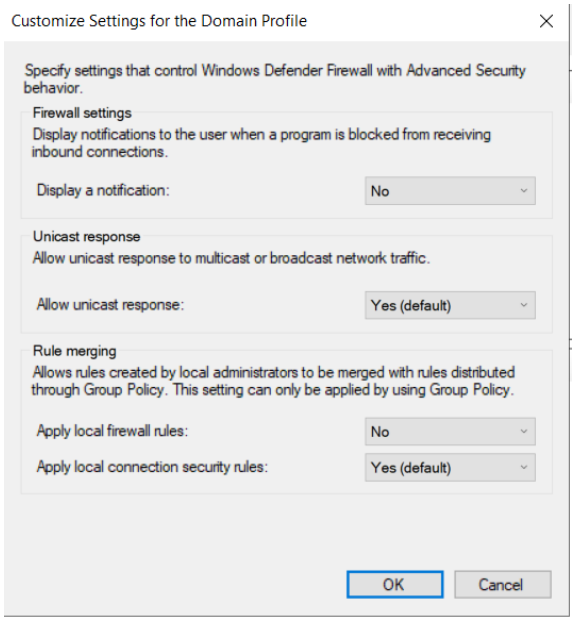


3.

a. For EACH Profile Firewall state: On (recommended)
b. For EACH Profile Inbound connections: Block (default)
c. For EACH Profile Outbound connections: Allow (default)



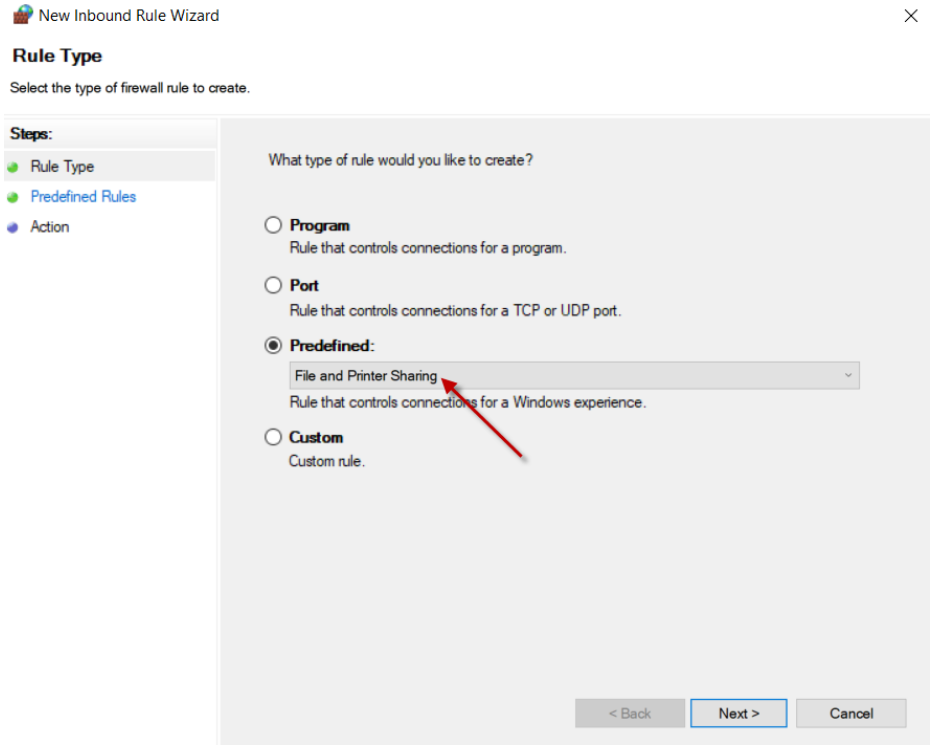
d. For EACH Profile Settings Customize
    i. Display a notification: No
    ii. Allow Unicast response: Yes (default)
    iii. Apply local firewall rules: No *note: this setting forces the machine to only allow rules set by the GPO*
    iv. Apply local connection security rules: Yes (default)



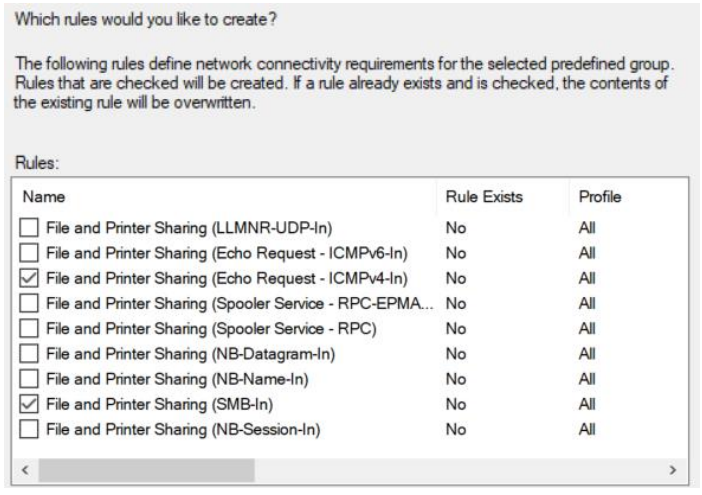
e. For EACH profile leave logging set to Not configured. This will allow us to manually enable and customize the logging settings on the machine(s) we are troubleshooting.

4. Configure Inbound Rules
    a. Allow Ping and SMB
        i. Right click Inbound Rules and select New Rule

        ii. Select Predefined and choose 'File and Printer Sharing' from the dropdown.



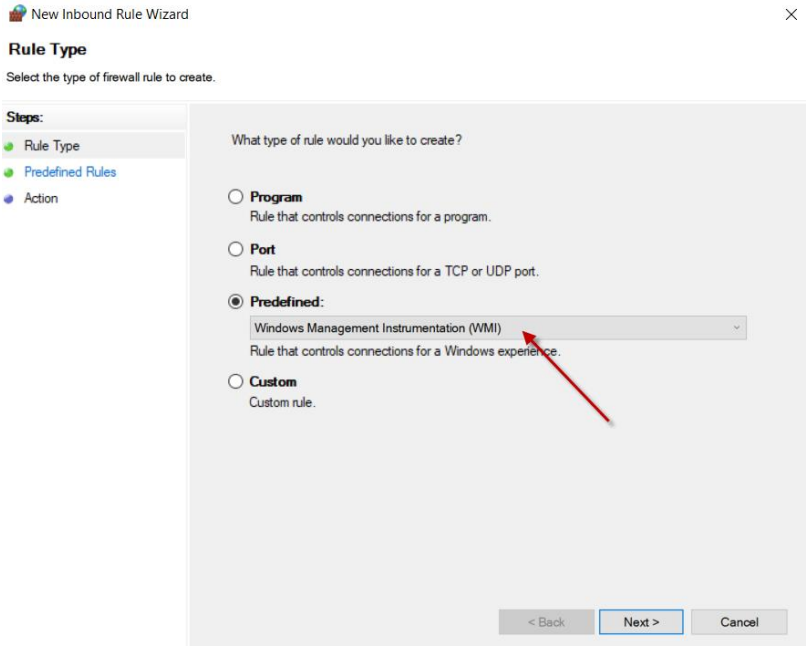
        iii. Only Check Echo Request – ICMPv4-In AND SMB-In



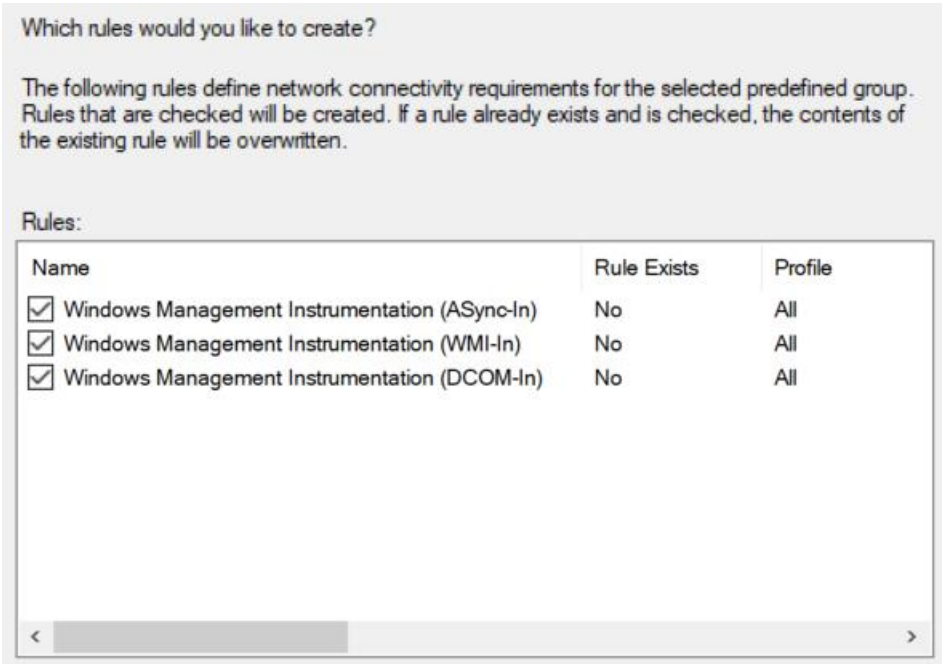
        iv. Allow the connection and click Finish

b. Allow WMI and DCOM
   i. Right click Inbound Rules and select New Rule

   ii. Select Predefined and choose 'Windows Management Instrumentation WMI'



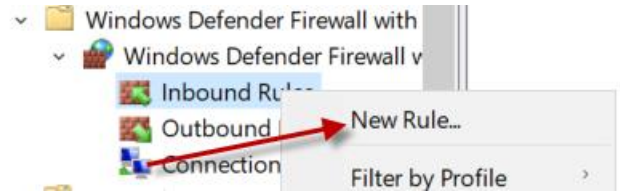
   iii. Leave all 3 boxes checked



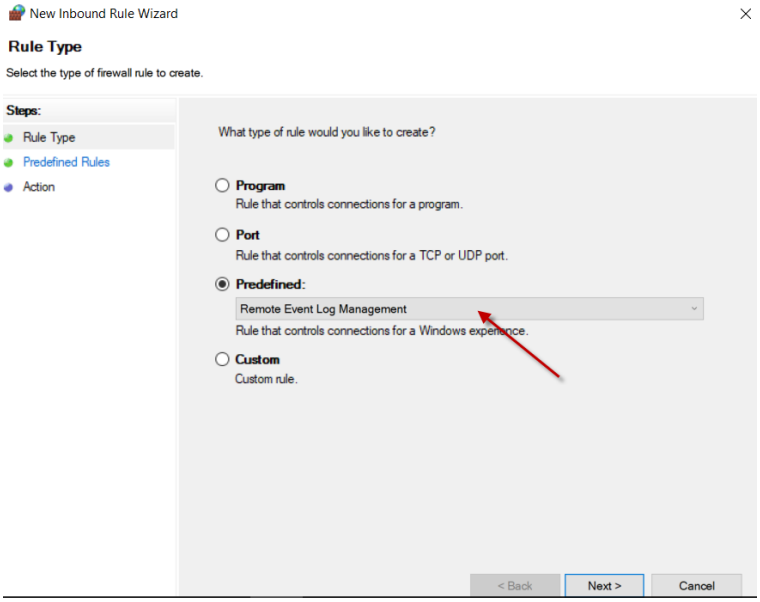
   iv. Allow the connection and click Finish

c. Allow Remote Event Log Management

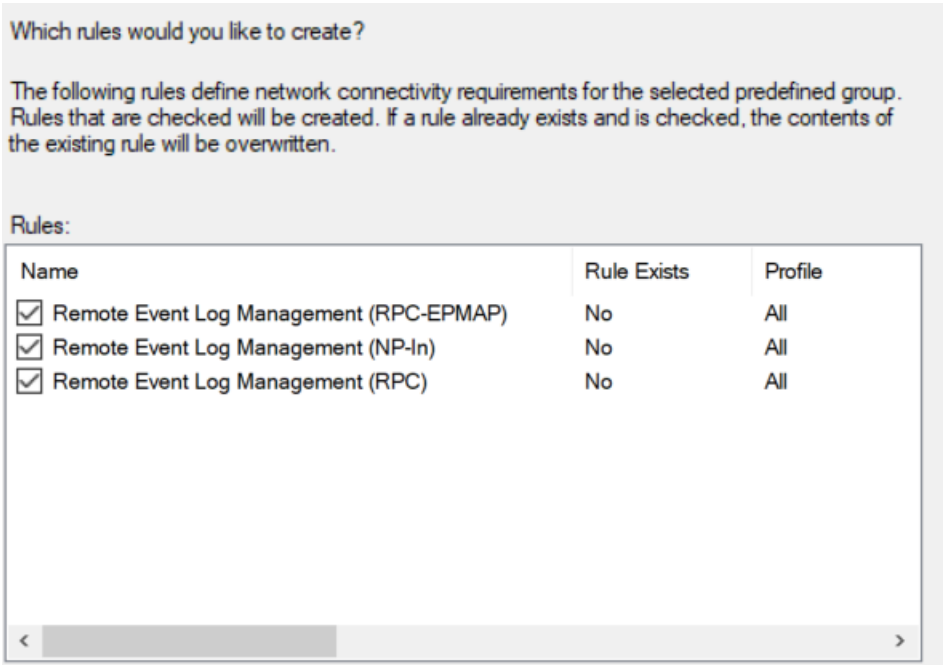
i. Right click Inbound Rules and select New Rule



ii. Select Predefined and choose 'Remote Event Log Management'

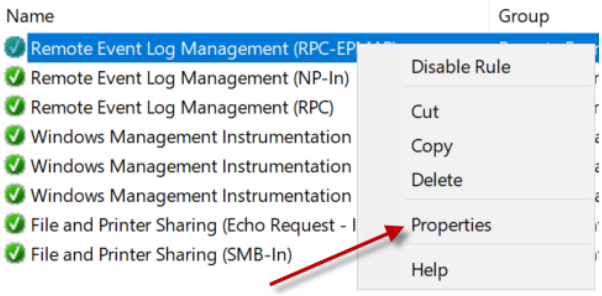


iii. Leave all 3 boxes checked

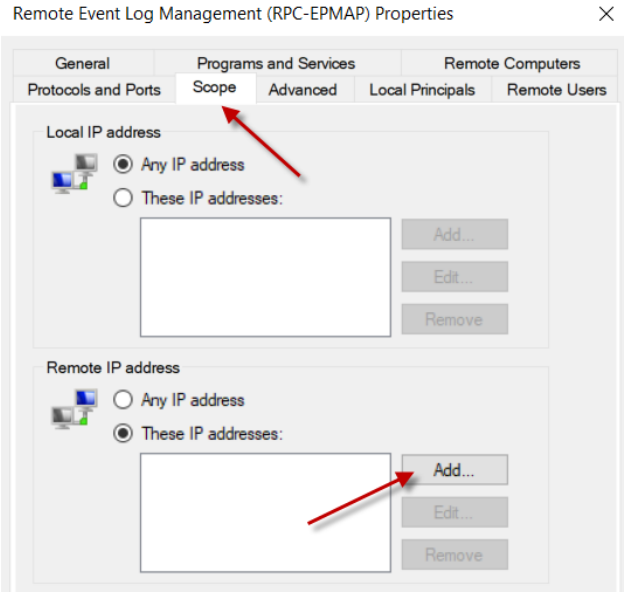


iv. Allow the connection and click Finish

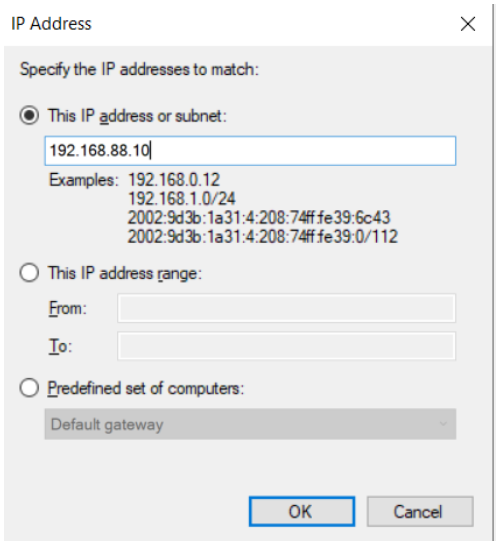
5. Limit Inbound Rules to only allow from specific Remote IP addresses.
    a. For EACH of the Inbound Rules you want to limit, Right Click and Select Properties



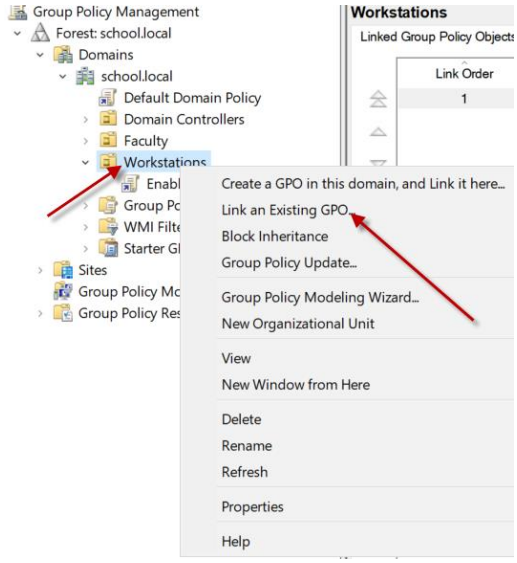
    b. Go to the Scope tab and on *Remote IP address* select These IP addresses, click Add



    c. Enter the IP address you want to allow the connection from and click OK (I recommend adding ALL of your domain controllers, and any computer's IP address you might manage your workstations from) Click OK and close the Group Policy Editor



6. Apply GPO to Workstations OU
    a. From Group Policy Management, expand your Domain and find the Workstations OU you want to apply the Firewall GPO to. Do not apply this to your servers!
    b. Right Click and select 'Link an Existing GPO'



    c. Select your Enable Windows Firewall GPO and click OK.