# 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

Group Policy Management	Group Policy Objects in school.local
<ul> <li>A Forest: school.local</li> <li>A Domains</li> </ul>	Contents Delegation
<ul> <li>school.local</li> <li>Default Domain Policy</li> </ul>	New GPO × G
> Domain Controllers	Name:
Faculty     Transform     Faculty     Faculty     Faculty     Faculty	Enable Windows Firewall
Group Policy Objects     Appl ocker	Source Starter GPO:
Apps Install     test     Default Domain Controllers Polic	3 OK Cancel

- 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

Computer Configuration     Policies	Windows Defender Firewall with Advanced Ser
> Software Settings	
Vindows Settings     Name Resolution Policy	Overview
<ul> <li>Scripts (Startup/Shutdown)</li> <li>Imployed Printers</li> <li>Security Settings</li> </ul>	Domain Profile      Windows Defender Firewall state is not configure
Account Policies     Local Policies     Event Log	Private Profile  Windows Defender Firewall state is not configure
Restricted Groups     System Services     Registry	Public Profile  Windows Defender Firewall state is not configure
A File System     The Wired Network (IEEE 802.3) Policies     The Windows Defender Firewall with Advances	Windows Defender Firewall Properties     Oction     Started
Windows Defender Firewall with Adva	Authenticate communications between Create connection security rules to specify how and w protected by using Internet Protocol security (IPsec).
Network List Manager Policies	Connection Security Rules

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

Specify beha	avior for when a	computer	ris conne	ected to it:	ings s corpora	te
State	irewall state:		On (recor	mmended	)	~
	Inbound conne	ections:		Block (de	fault)	~
	Outbound con	nections:		Allow (de	fault)	~
Settings S	pecify settings th lefender Firewall	nat contro behavior	l Windov	ws	Customize	Ð
Logging S tr	pecify logging se oubleshooting.	ettings for		1	Customiz	e

- 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)

Customize Settings for the Domain Profile		$\times$	
Specify settings that control Windows Defender Firewa behavior.	II with Advanced Security		
Firewall settings			
Display notifications to the user when a program is blo inbound connections.	cked from receiving		
Display a notification:	No ~		
Unicast response			
Allow unicast response to multicast or broadcast network traffic.			
Allow unicast response: Yes (default)			
Bule merging			
Allows rules created by local administrators to be merg through Group Policy. This setting can only be applied	ed with rules distributed by using Group Policy.		
Apply local firewall rules:	No ~		
Apply local connection security rules:	Yes (default)		
	OK Cancel		

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.

3.

- 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.

5

#### Rule Type

Select the type of firewall rule to cre	eate.
Steps: Rule Type	What type of rule would you like to create?
<ul> <li>Predefined Rules</li> <li>Action</li> </ul>	<ul> <li>Program Rule that controls connections for a program.</li> <li>Port Rule that controls connections for a TCP or UDP port.</li> <li>Predefined: Rule that controls connections for a Windows experience.</li> <li>Custom Custom Custom rule.</li> </ul>

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

Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Name	Rule Exists	Profile	
File and Printer Sharing (LLMNR-UDP-In)	No	All	
File and Printer Sharing (Echo Request - ICMPv6-In)	No	All	
File and Printer Sharing (Echo Request - ICMPv4-In)	No	All	
File and Printer Sharing (Spooler Service - RPC-EPMA	No	All	
File and Printer Sharing (Spooler Service - RPC)	No	All	
File and Printer Sharing (NB-Datagram-In)	No	All	
File and Printer Sharing (NB-Name-In)	No	AII	
File and Printer Sharing (SMB-In)	No	All	
File and Printer Sharing (NB-Session-In)	No	All	
<			>

iv. Allow the connection and click Finish

b. Allow WMI and DCOM

i. Right click Inbound Rules and select New Rule

× 🗋	Windows Defender Fir	ewall with	
~	Windows Defende	r Firewall v	
	🔣 Inbound Rut		
	🔀 Outbound	New Rule	
-	Connection	Filter by Profile	>

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

🔗 New Inbound Rule Wiz	ard	×
Rule Type		
Select the type of firewall rule t	o create.	
Steps: Predefined Rules Action	What type of rule would you like to create?  Program Rule that controls connections for a program. Pot Rule that controls connections for a TCP or UDP port.  Predefined: Windows Management Instrumentation (WMI) Rule that controls connections for a Windows experience. Custom Custom rule.	×
	< Back Next >	Cancel

#### iii. Leave all 3 boxes checked

-

Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Name	Rule Exists	Profile	
Windows Management Instrumentation (ASync-In)	No	All	
Windows Management Instrumentation (WMI-In)	No	All	
Windows Management Instrumentation (DCOM-In)	No	All	

iv. Allow the connection and click Finish

- c. Allow Remote Event Log Management
  - i. Right click Inbound Rules and select New Rule

~	1 V	Vindows Defender Fire	ewall with	
	~ 1	Windows Defender	Firewall v	
		🔣 Inbound Rut		
		S Outbound	New Rule	
		Connection	Filter by Profile	>

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

🔗 New Inbound Rule Wiz	zard	$\times$
Rule Type		
Select the type of firewall rule t	to create.	
Steps:		
Rule Type	What type of rule would you like to create?	
Predefined Rules		
	Rule that controls connections for a program.         Pott         Rule that controls connections for a TCP or UDP port.         Predefined:         Remote Event Log Management         Rule that controls connections for a Windows expensive.         Custom         Custom rule.	
	< Back Next > Cancel	

iii. Leave all 3 boxes checked

Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Rules:			
Name	Rule Exists	Profile	
Remote Event Log Management (RPC-EPMAP)	No	All	
Remote Event Log Management (NP-In)	No	All	
Remote Event Log Management (RPC)	No	All	
<			>

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 Remote Event Log Management (RPC-EPMAP) Properties

General	Programs and Services		5	Remote	e Computers
Protocols and Ports	Scope	Advanced	Loc	al Principals	Remote Users
Local IP address	IP address e IP addres	ses:			
				Add	
				Edit	
				Remove	
Remote IP address	s				
N 🔿 Any I	IP address				
These results of the second	e IP addres	ses:			
				Add	
		/		Edit	
				Remove	

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

IP Address		×
Specify the IP addresses to match:		
• This IP <u>a</u> ddress or subnet:		
192.168.88.10		
Examples: 192.168.0.12 192.168.1.0/24 2002:9d3b:1a31:4:2 2002:9d3b:1a31:4:2	208:74ff.fe39:6c4 208:74ff.fe39:0/1	43 112
O This IP address range:		
<u>F</u> rom:		
<u>T</u> o:		
<u>Predefined set of computers:</u>		
Default gateway		~
C	OK	Cancel

### 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'

Workstations	
Linked Gr	oup Policy Objects
	Link Order
	1
domain, ar mg Wizard. Unit lere	nd Link it here
	ng Wizard. Unit Here

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

Select GPO	$\times$
Look in this domain:	
school.local	~
Group Policy objects:	
Name	
Default Domain Controllers Policy	
Default Domain Policy	
Enable Windows Firewali	
$\mathbf{X}$	
ок	Cancel