1. Open Windows Firewall, go to the Start menu, select Run, type WF.msc, and then select OK.

2. Right-click the top-level Windows Defender Firewall with Advanced Security node in the left pane and then selecting Properties.

3. Select the Domain Profile tab.

4. Under Firewall State, Inbound Connections, select Block from the dropdown box.

5. Click OK.

**To create an inbound ICMP rule:**

1. Open Windows Firewall, go to the Start menu, select Run, type WF.msc, and then select OK.
2. In the navigation pane, click Inbound Rules.
3. Click Action, and then click New rule.
4. On the Rule Type page of the New Inbound Rule Wizard, click Custom, and then click Next.
5. On the Program page, click All programs, and then click Next.
6. On the Protocol and Ports page, select ICMPv4 or ICMPv6 from the Protocol type list. If you use both IPv4 and IPv6 on your network, you must create a separate ICMP rule for each.
7. Click Customize.
8. In the Customize ICMP Settings dialog box, do one of the following:
	* To allow all ICMP network traffic, click All ICMP types, and then click OK.
	* To select one of the predefined ICMP types, click Specific ICMP types, and then select each type in the list that you want to allow. Click OK.
	* To select an ICMP type that does not appear in the list, click Specific ICMP types, select the Type number from the list, select the Code number from the list, click Add, and then select the newly created entry from the list. Click OK
9. Click Next.
10. On the Scope page, you can specify that the rule applies only to network traffic to or from the IP addresses entered on this page. Configure as appropriate for your design, and then click Next.
11. On the Action page, select Allow the connection, and then click Next.
12. On the Profile page, select the network location types to which this rule applies, and then click Next.
13. On the Name page, type a name and description for your rule, and then click Finish.

**To configure Advanced Security Logging:**

1. Open Windows Firewall, go to the Start menu, select Run, type WF.msc, and then select OK.
2. In the details pane, in the Overview section, click Windows Defender Firewall Properties.
3. For each network location type (Domain, Private, Public), perform the following steps.
4. Click the tab that corresponds to the network location type.
5. Under Logging, click Customize.
6. The default path for the log is %windir%\system32\logfiles\firewall\pfirewall.log. If you want to change this, clear the Not configured check box and type the path to the new location, or click Browse to select a file location. ( The location you specify must have permissions assigned that permit the Windows Defender Firewall service to write to the log file.)
7. The default maximum file size for the log is 4,096 kilobytes (KB). If you want to change this, clear the Not configured check box, and type in the new size in KB, or use the up and down arrows to select a size. The file will not grow beyond this size; when the limit is reached, old log entries are deleted to make room for the newly created ones.
8. No logging occurs until you set one of following two options:
	* + To create a log entry when Windows Defender Firewall drops an incoming network packet, change Log dropped packets to Yes.
		+ To create a log entry when Windows Defender Firewall allows an inbound connection, change Log successful connections to Yes.
		+ Click OK twice.