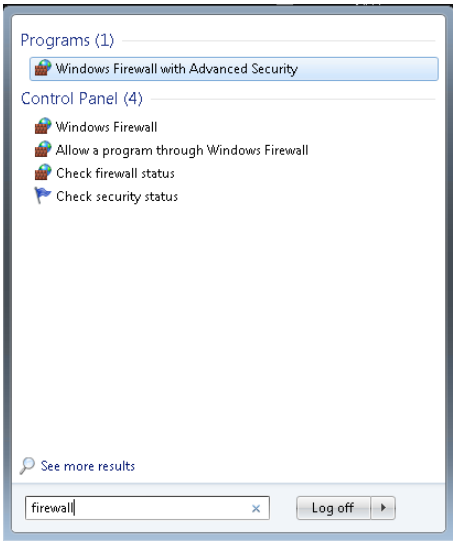
Blocking CodeMeter Run Time Server Vulnerabilities – Windows 7

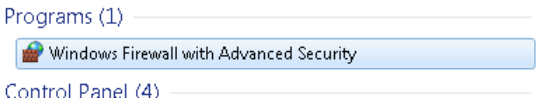
Purpose
The following instructions are to be used to mitigate the risk posed by the vulnerabilities in the Code Meter Runtime Server on systems running LAS-X, LMD and Paula.

Instructions

Login to the workstation running the product.

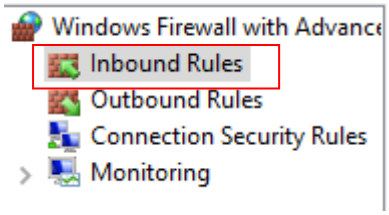
Click on the start menu and  and type firewall.



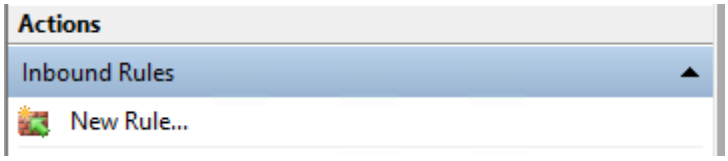
Select the 

from the menu.

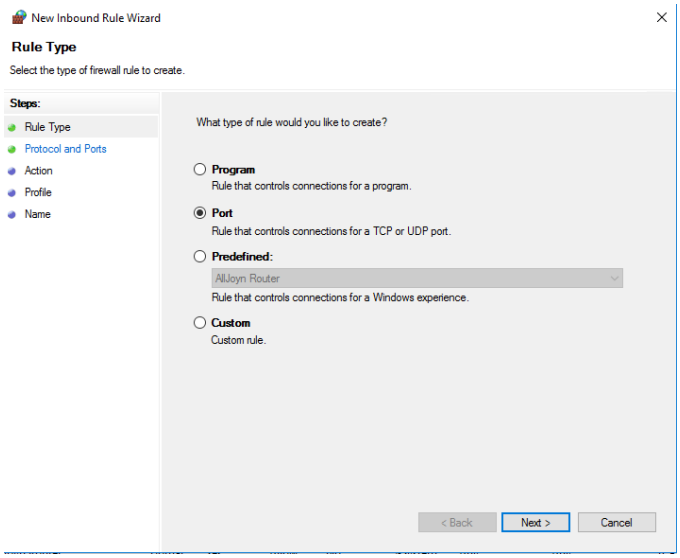
From the new windows that appears select the option „Inbound Rules“ as indicated below.



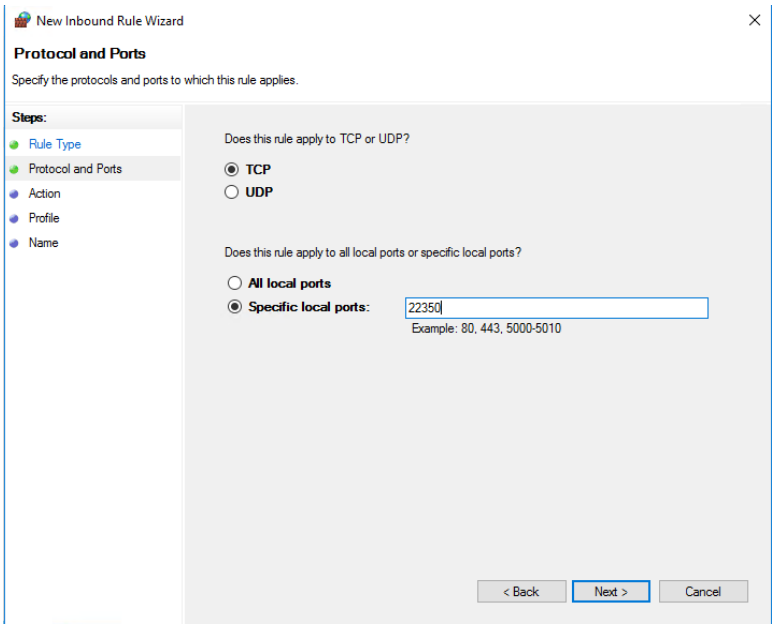
Then select the option New Rule...



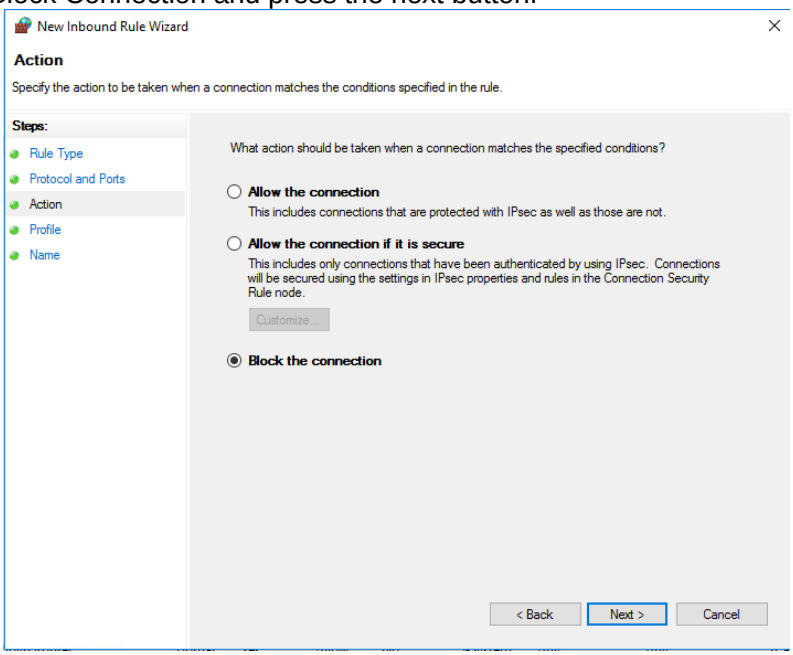
In the dialogue that appears Select the option Port and press the next button.



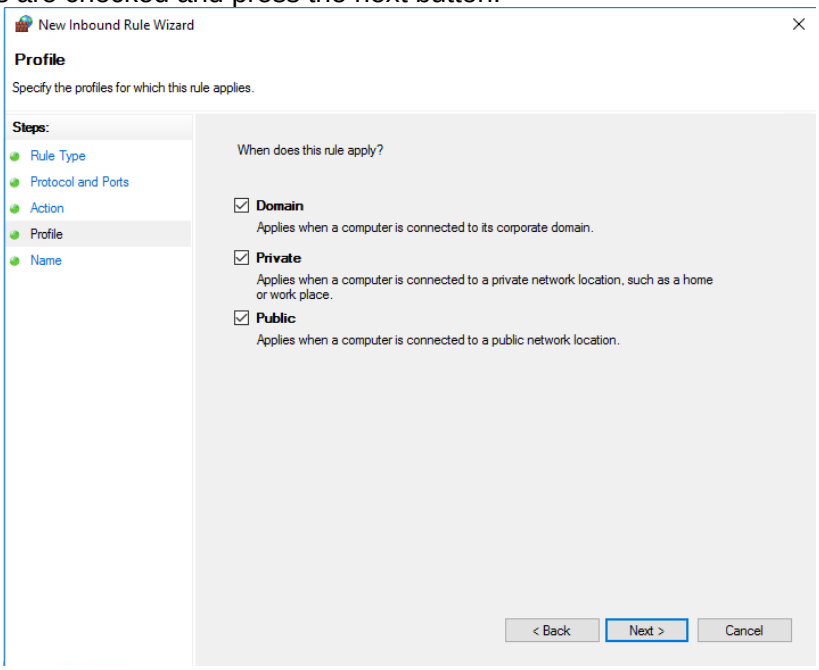
In the Specified Local Ports enter the port 22350 and press the next button.



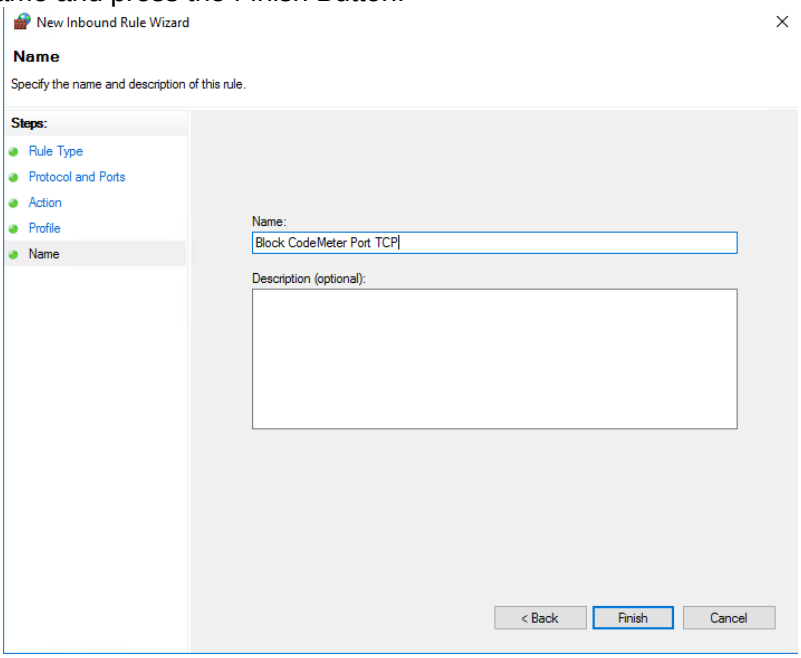
Select the action Block Connection and press the next button.



Ensure all options are checked and press the next button.

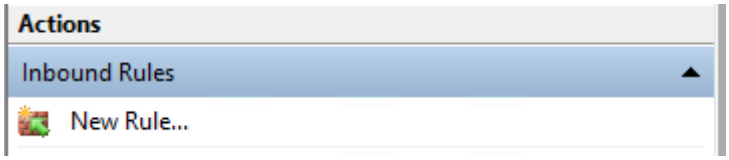


Give the Rule a name and press the Finish Button.

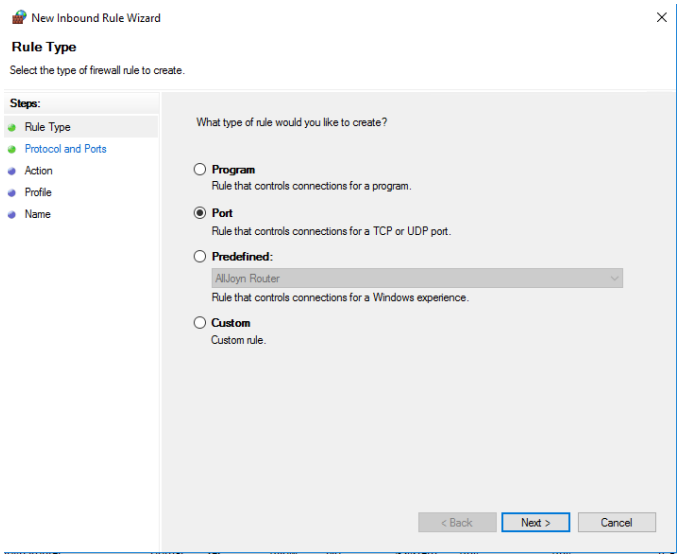


Now repeat the process for UDP

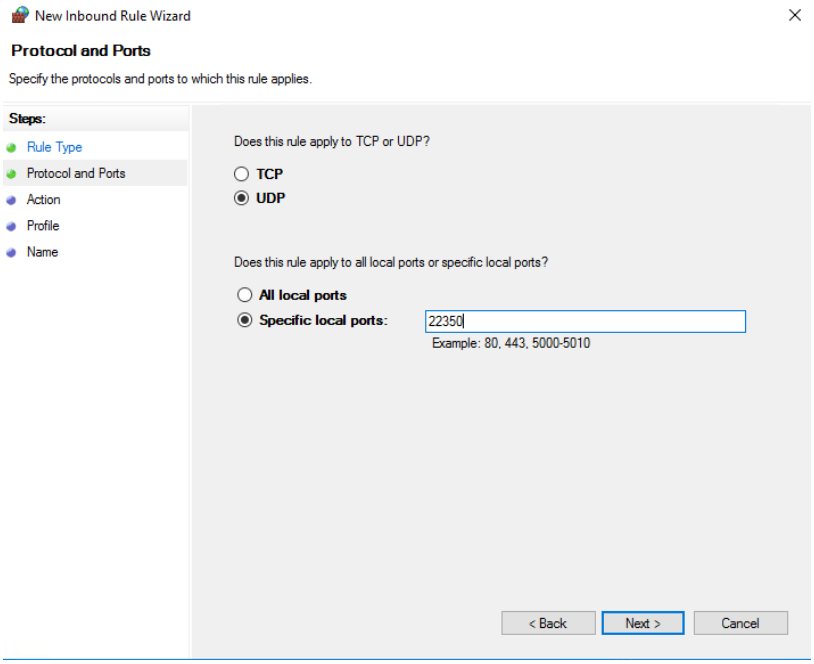
Then select the option New Rule...



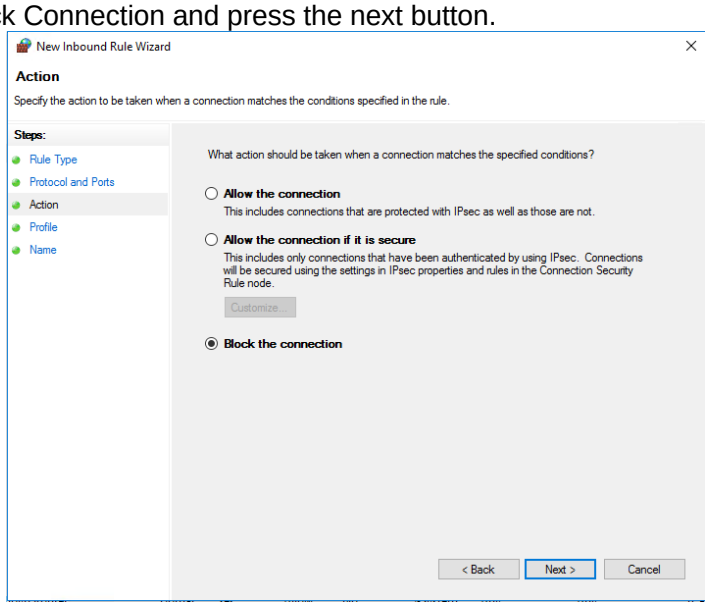
In the dialogue that appears Select the option Port and press the next button.



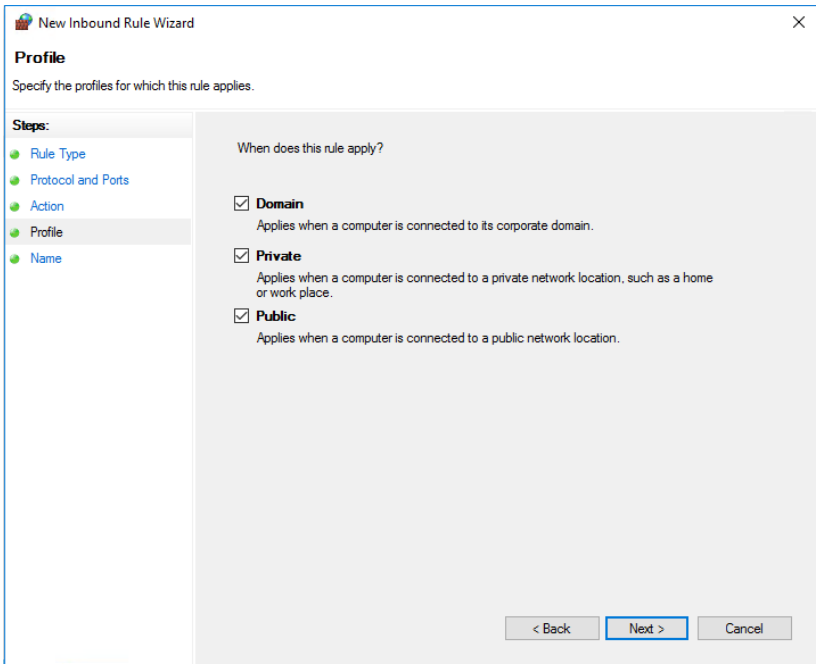
Select the option UDP and in the Specified Local Ports enter the port 22350 and press the next button.



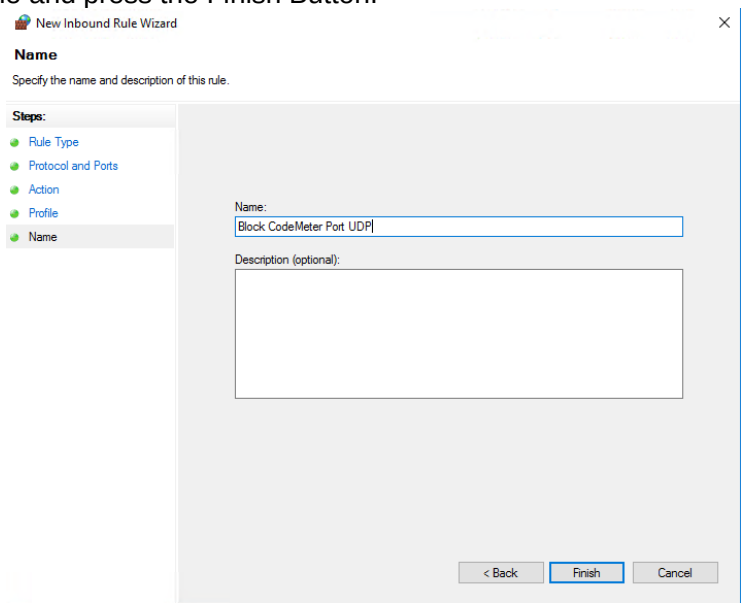
Select the action Block Connection and press the next button.



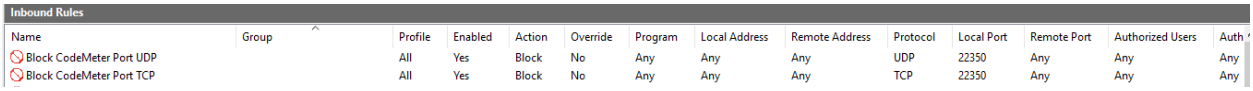
Ensure all options are checked and press the next button.



Give the Rule a name and press the Finish Button.



You should now see in the list of inbound rules the new rules



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Auth
Block CodeMeter Port UDP		All	Yes	Block	No	Any	Any	Any	UDP	22350	Any	Any	Any
Block CodeMeter Port TCP		All	Yes	Block	No	Any	Any	Any	TCP	22350	Any	Any	Any