Tofino IEC104 Firewall Setting

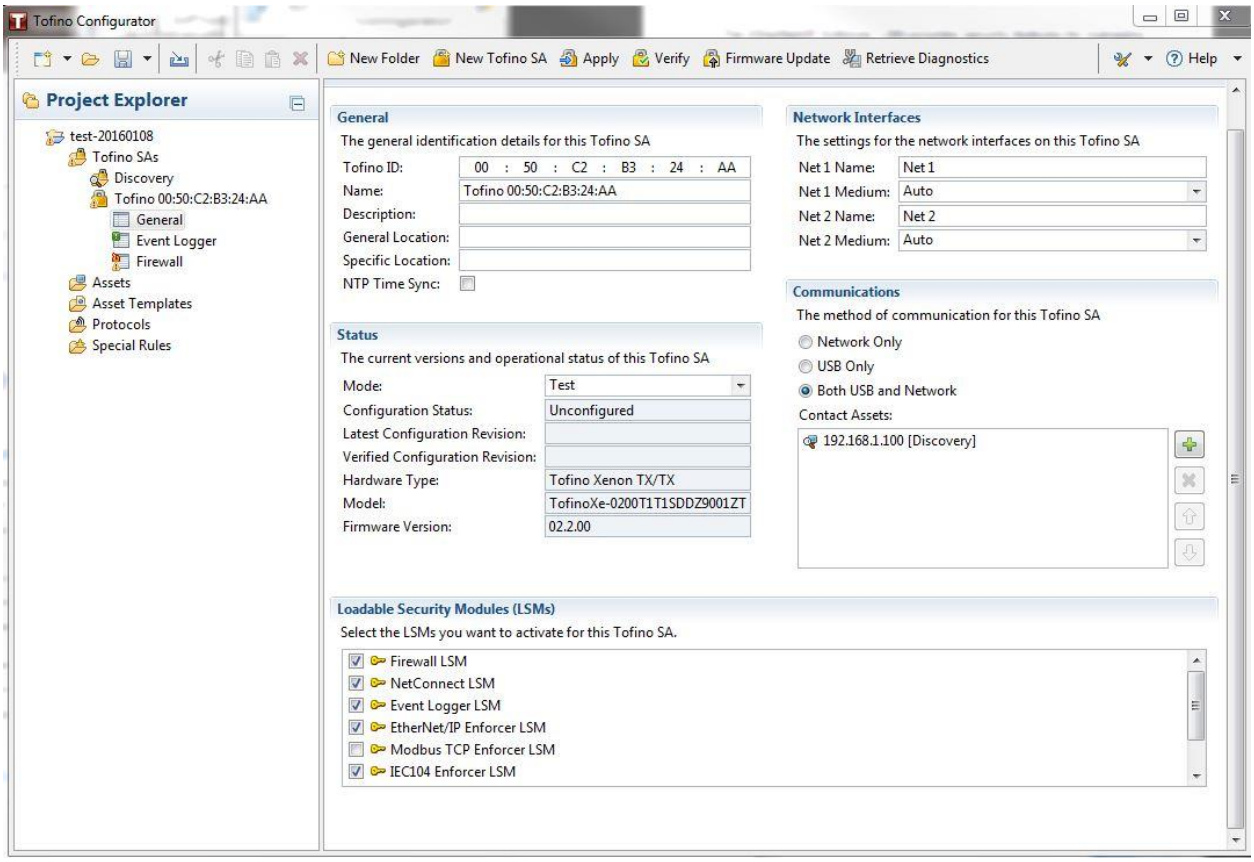
Tofino IEC104 Functionality

The Tofino Security Appliance (TSA) implements an IEC104 loadable security module (LSM) which enables deep packet inspection (DPI) firewall capabilities for IEC104 traffic. The installation engineer specifies master station (client) /substation (server) device pairs between which IEC104 traffic will be allowed to flow. Tofino Configurator provides user with the capability of specifying various ie104 application layer parameter options and formatting. Only correctly formatted IEC104 packets will be allowed.

Adding IEC Enforcer Firewall Rules

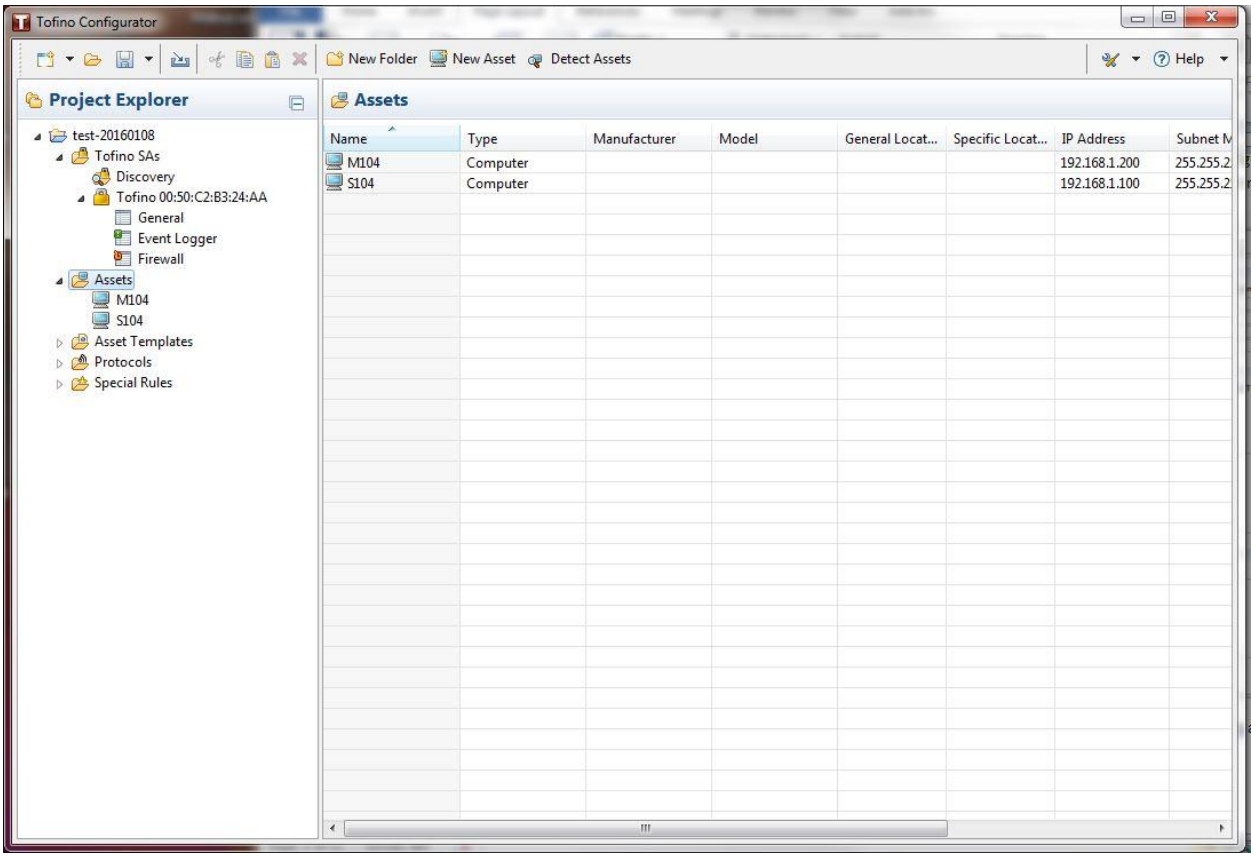
We illustrate the IEC104 enforcer firewall rule setting via the following Tofino setting.

The master station has IP address of 192.168.1.200, and the substation, 192.168.1.100, with Tofino firewall device sitting in the middle connecting both stations. The Tofino Configurator (TC) has discovered the Tofino device as shown in the following picture of TC's General Setting screen.

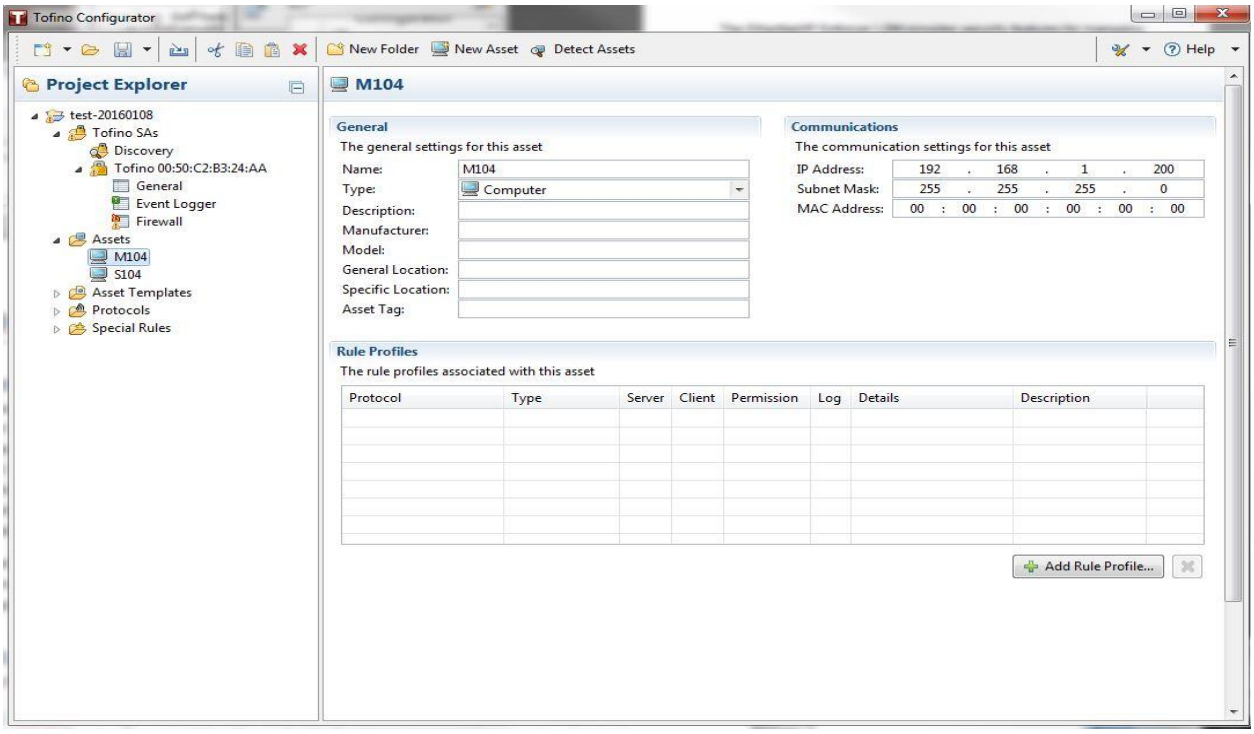


First, we create two assets M104 for the master station and S104 for substation as follows.

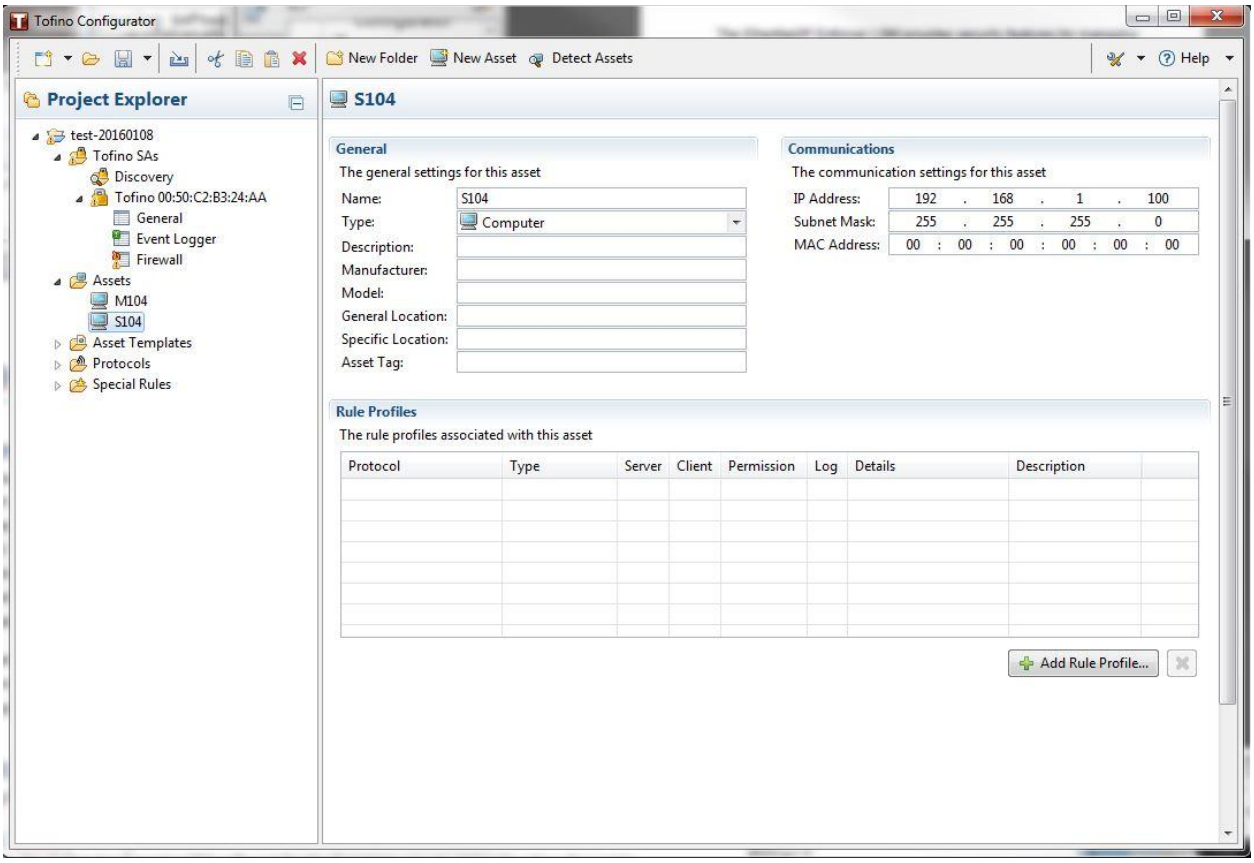
Click Assets icon on the left panel, the following screen will appear.



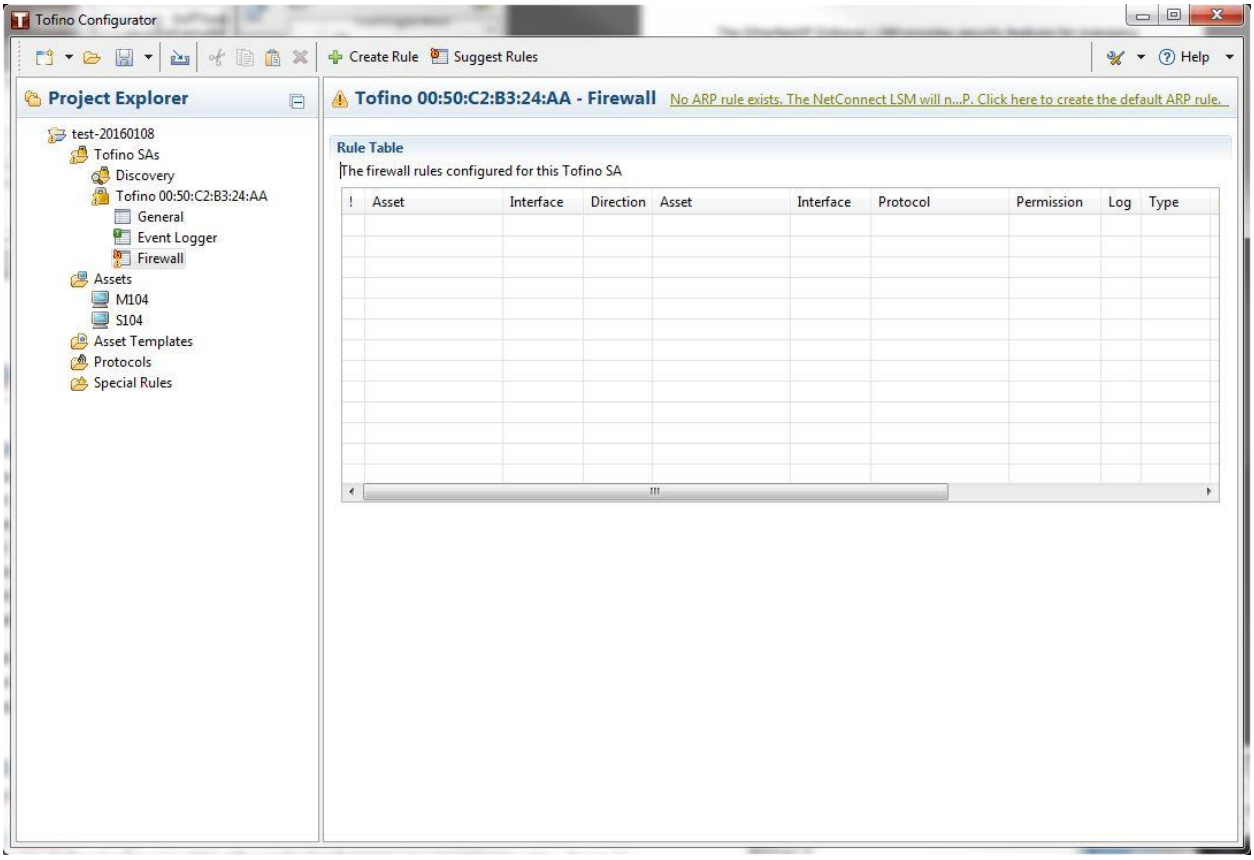
Click New Asset button to add Asset M104 as shown below.



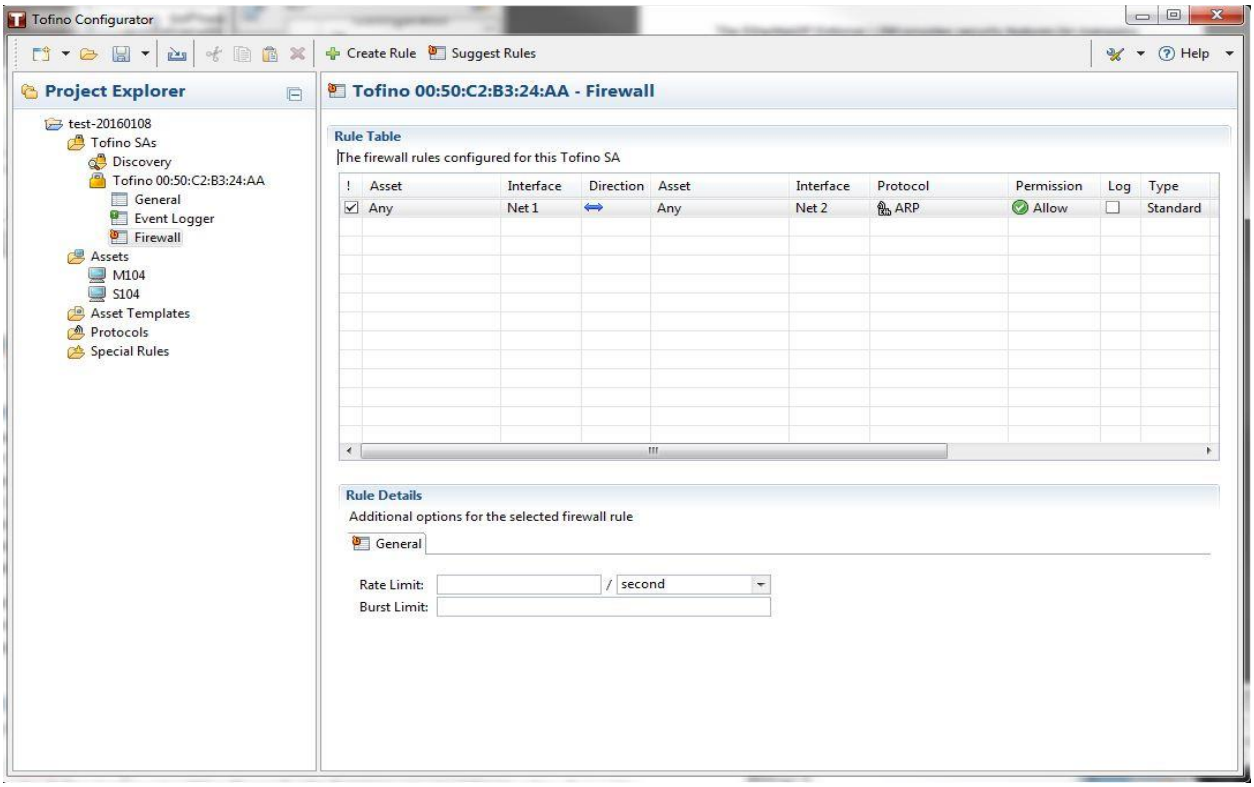
Repeat the same step to create S104 as below.



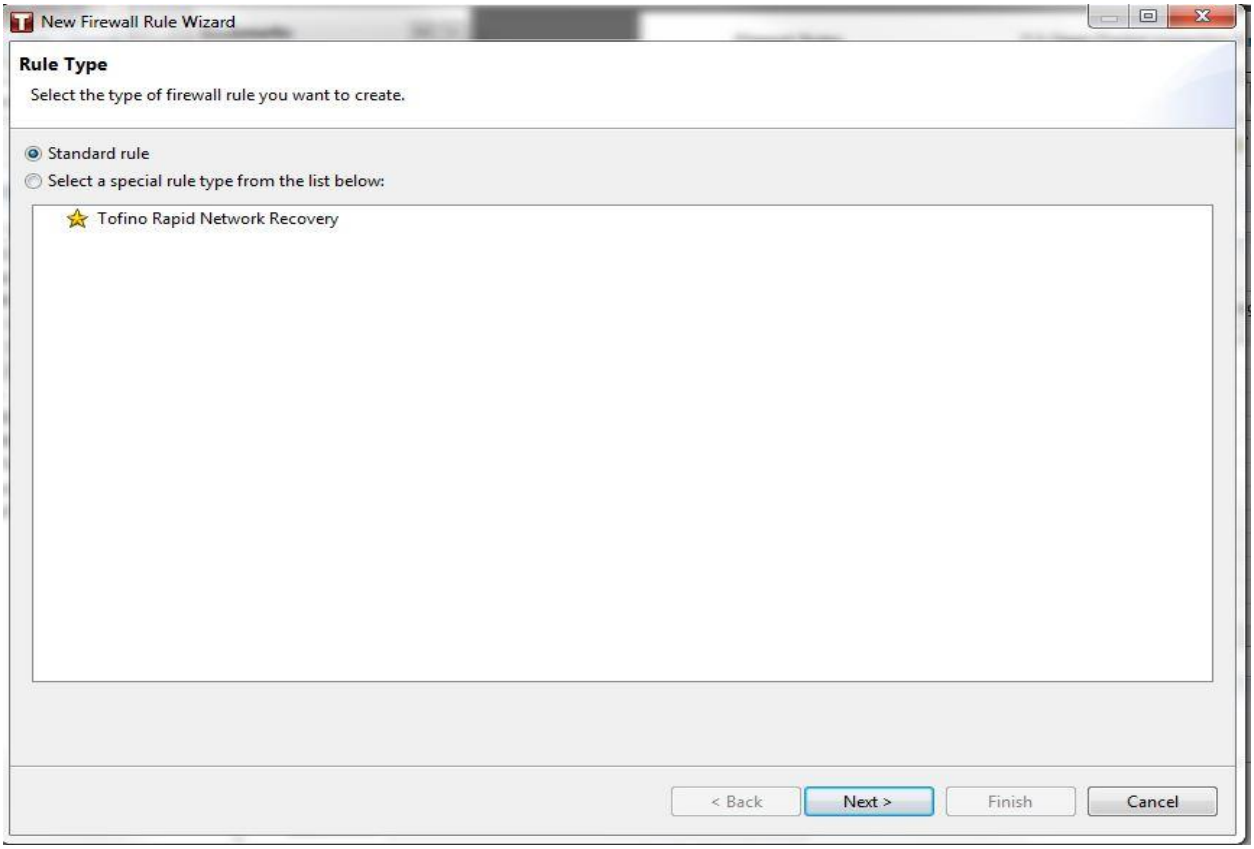
Secondly, we will create firewall rule by clicking the Firewall icon to open the Firewall screen:



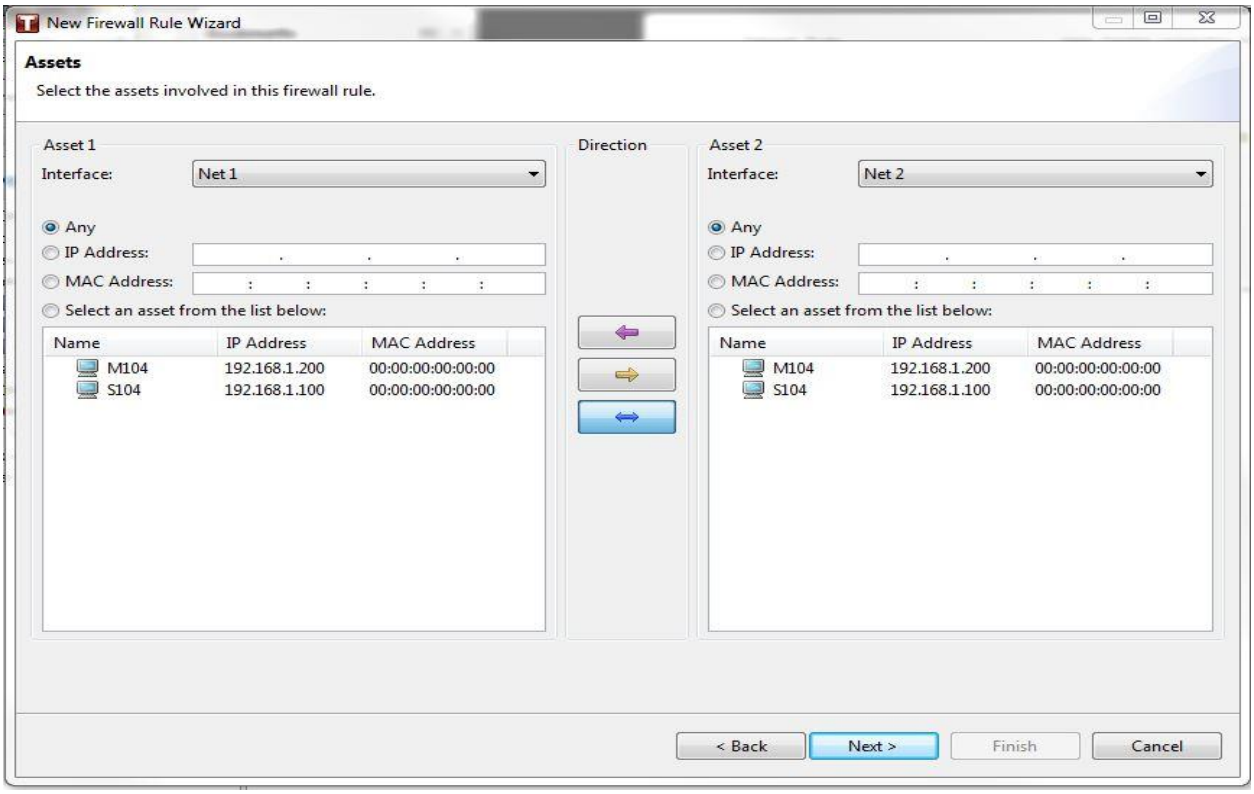
Click the **highlighted No ARP rule exists …** line at the right top of the screen to add the ARP rule:



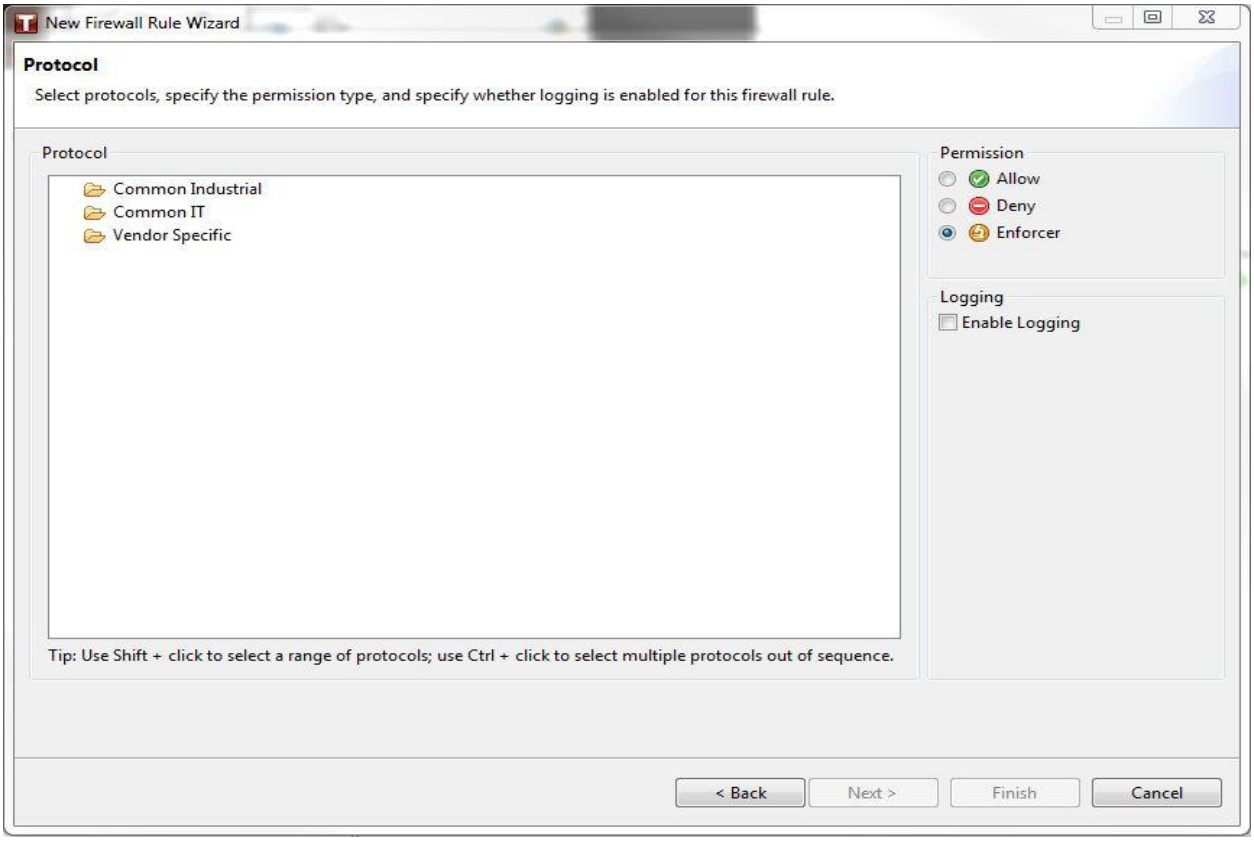
Click Create Rule button at the top of the screen to open the Rule Type wizard:



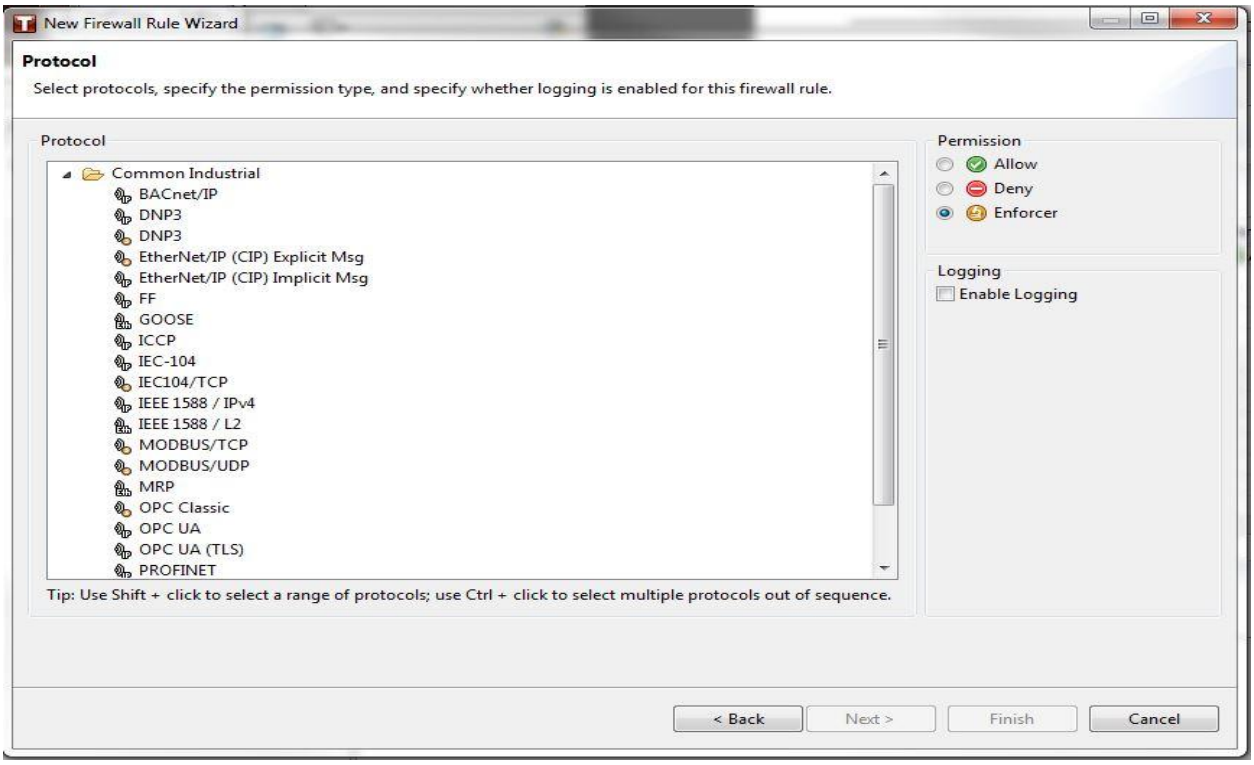
Click Next button, and the Rule Wizard will appear:



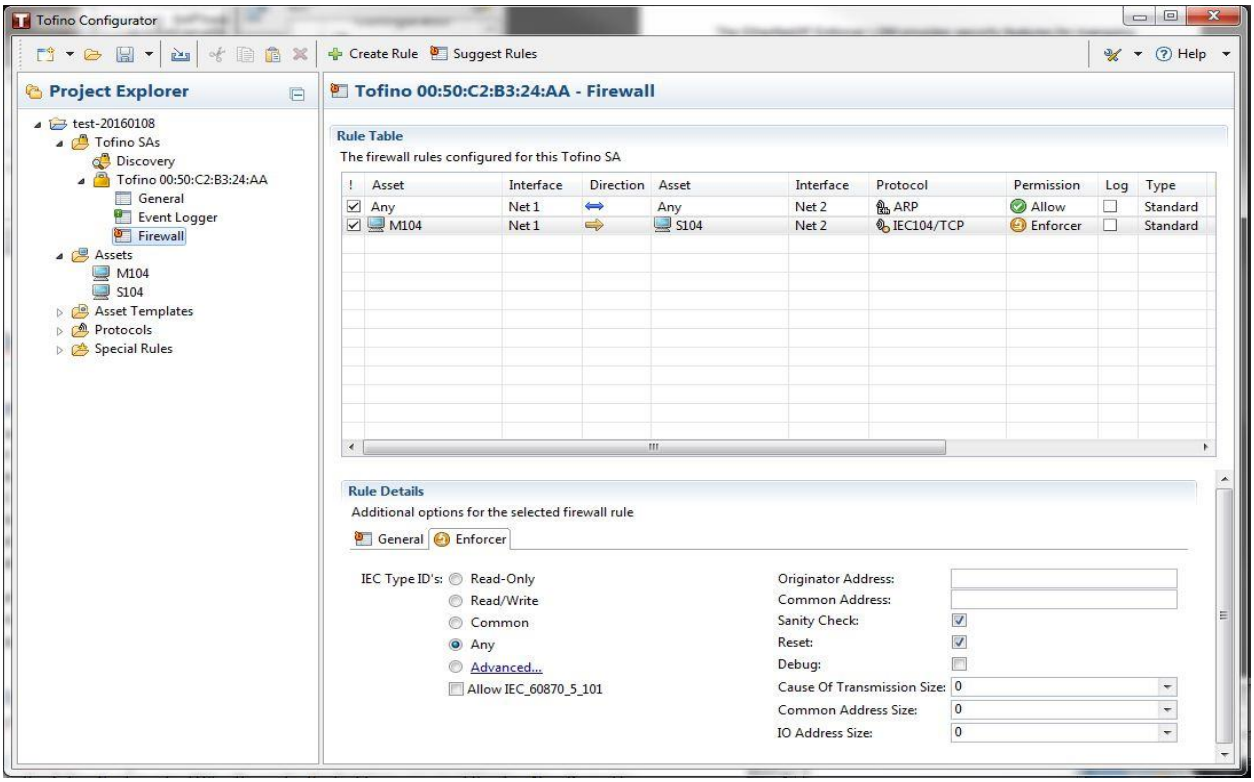
Click M104 on the left panel, right arrow in the middle, and S104 on the right panel, then click Next button, the Protocol screen will appear.



Select Enforcer at the top right and then Common Industrial folder to open the Selection screen:



Select IEC104/TCP icon in the list, the Finish button at the bottom right of the screen un-grayed. Click Finish button and the IEC104 rule is created as below:



IEC104 Enforcer Parameter Setting

Table 1 below depicts parameter options setting of the above IEC104 enforcer screen.

Parameters	Description
Type ID's	This option defines allowed type ids of incoming IEC104 packets. Only packets with type ids selected in TC will be allowed. TC offers different options to group type ids for the ease of selection. Please refer to Table 2 for a detailed explanation.
Originator Address	This parameter identifies the devices from where packets originated. Only packets with specified originator addresses will be allowed. If this field is empty, then any originator address will be allowed. Valid values are comma-separated integer list from 0-255.
Common Address	This parameter identifies the devices to where a packet is destined to. Only packets with specified common address will be allowed. If this field is empty, then any common address will be allowed. Valid values are comma-separated integer list from 0-255 when *common Address Size* is 1 byte , or from 0-65635 when *common Address Size* is 2.
Sanity Check	This Boolean flag, when checked, will enable the enforcer to perform sanity check on packets. These sanity checks ensure the packets adhere to the protocol specification.
Reset	This Boolean flag when checked will tell the enforcer to send TCP reset messages to both parties of the connection when DPI on an IEC104 packet failed.
Debug	This Boolean flag when checked will turn on the debugging of the enforcer.
Cause Of Transmission Size (COT)	The three size parameters define the variation of respective fields of packets. The enforcer will be performing DPI based on these settings. The Default value of COT size is 2. When 1 is selected, the *originator address* field will be grayed out, meaning there will not be an *originator address* in the packets. Valid values are 1 or 2 where the latter is the most commonly used.
Common Address Size	Valid values are 1 or 2 where the latter is the most commonly used.
IO Address Size	Valid values are 1, 2, or 3 where the last one is the most commonly used.

Table 1 IEC104 Parameter Setting

IEC Type IDs Option	Description
Read Only	1, 3, 5, 7, 9, 11, 13, 15, 20, 21, 30-40, 100-102, 107
Read/Write	1, 3, 5, 7, 9, 11, 13, 15, 20, 21, 30-40, 45-51, 58-64, 70, 100-102, 107
Common	1, 3, 5, 7, 9, 11, 13, 15, 20, 21, 30-40, 45-51, 58-64, 70, 100-103, 105, 107, 110-113, 120-127
Any	none
Advanced	When selected, the user can use any type ids from the pull down list, plus select one of the above three options.
Allowed	2, 4, 6, 8, 10, 12, 14, 16-19, 104, 106

IEC_60870_5_101	The type ids in this list are those defined in IEC101 Specification which may or may not be used by newer devices. This option can be checked along with one of the above 5 options. The effect is to merge the two options. Example 1: If *Read Only* and *Allowed IEC_60870_5_101* are selected, then the final list of type ids will be: 1, 3, 5, 7, 9, 11, 13, 15, 20, 21, 30-40, 100-102, 107, 2, 4, 6, 8, 10, 12, 14, 16-19, 104, 106. Example 2: Select *Common* with *Allowed IEC_60870_5_101* checked will have all type ids defined.

Table 2 Type ID's options