Tofino Ethernet IP Enforcer Guide

This guide is designed to help configure the Ethernet IP enforcer rules with TC Version 3.1 and newer. To use this guide the Tofino will need the Netconnect LSM and the EtherNet IP LSM.

Table of Contents

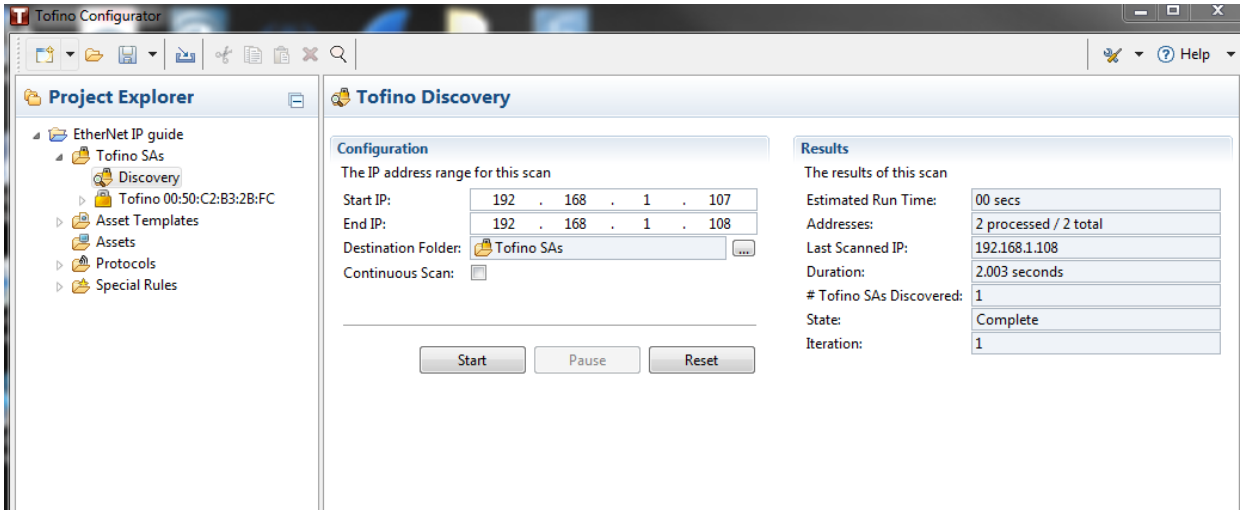
Featured Brands

Phone: **1.800.BELDEN1**

www.belden.com

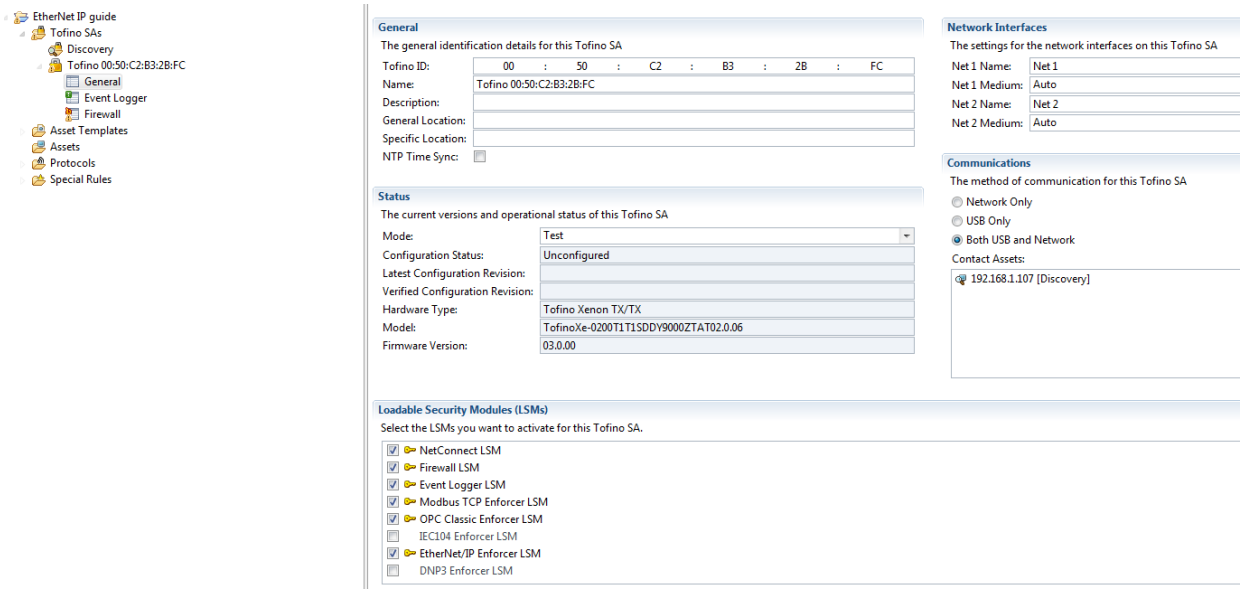
Discovering the Tofino

To get started the Tofino device will need to be discovered. The device needs to be power up and have a device attached to the secure port and the computer with the Tofino Configurator on the unsecure port. The IP address of the device attached to the secure port will be used in the discovery process and needs to be within the IP range configured in the TC as shown below (PLC with IP 192.168.1.107). Click start to discover the Tofino SA once the IP range is entered. The Tofino will appear in the tree after it is discovered.



Verifying MODE and LSMs

Expand the Tofino in the tree and go to the general tab to verify the appropriate LSMs are checked and it is Test mode.

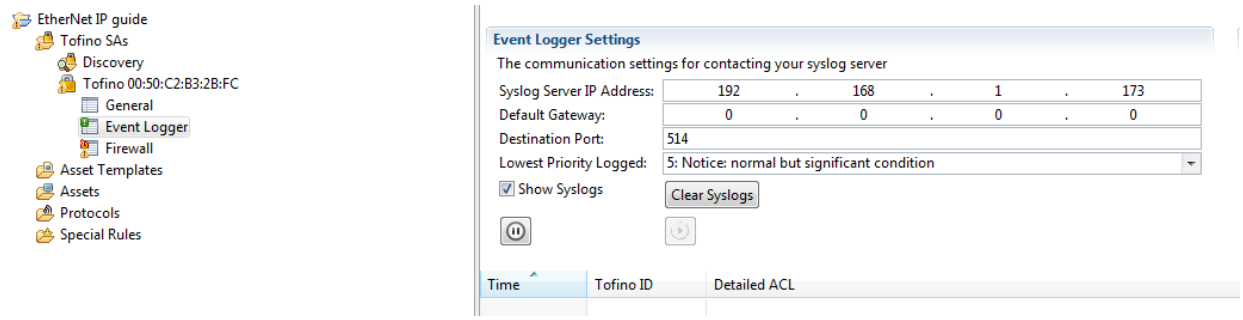


Phone: **1.800.BELDEN1**

www.belden.com

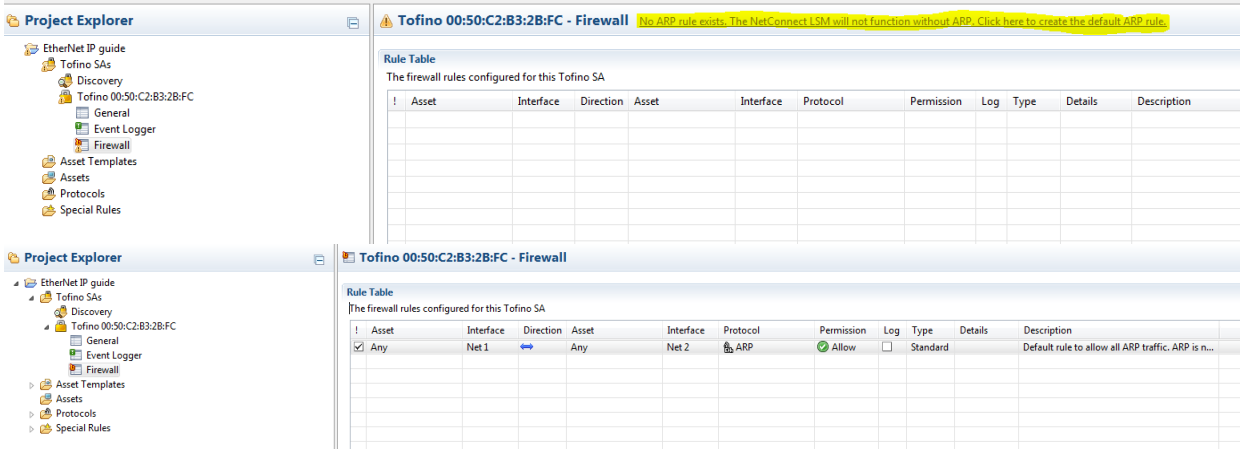
Event Logger Configuration

Go to the Event Logger, set the syslog server IP address to the IP of the TC computer, and click the show syslogs checkbox.

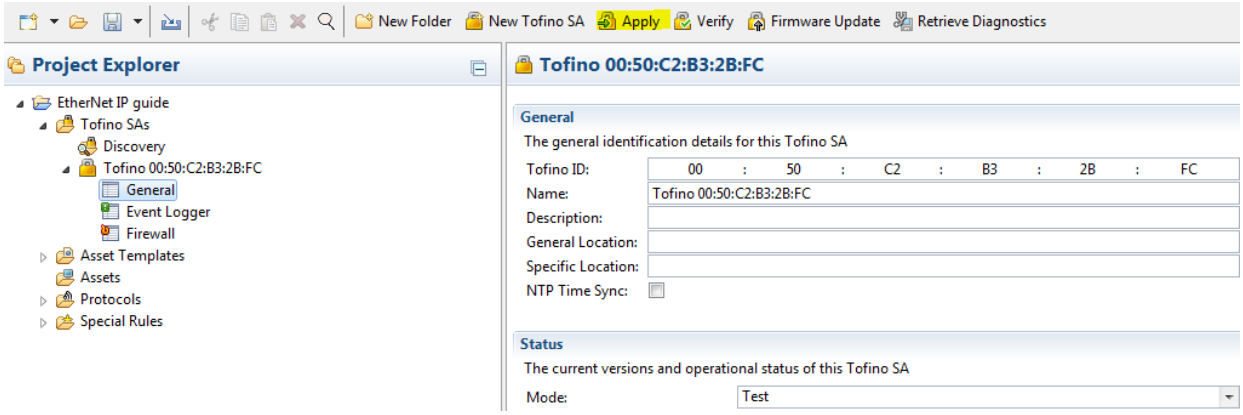


Configuring Rules

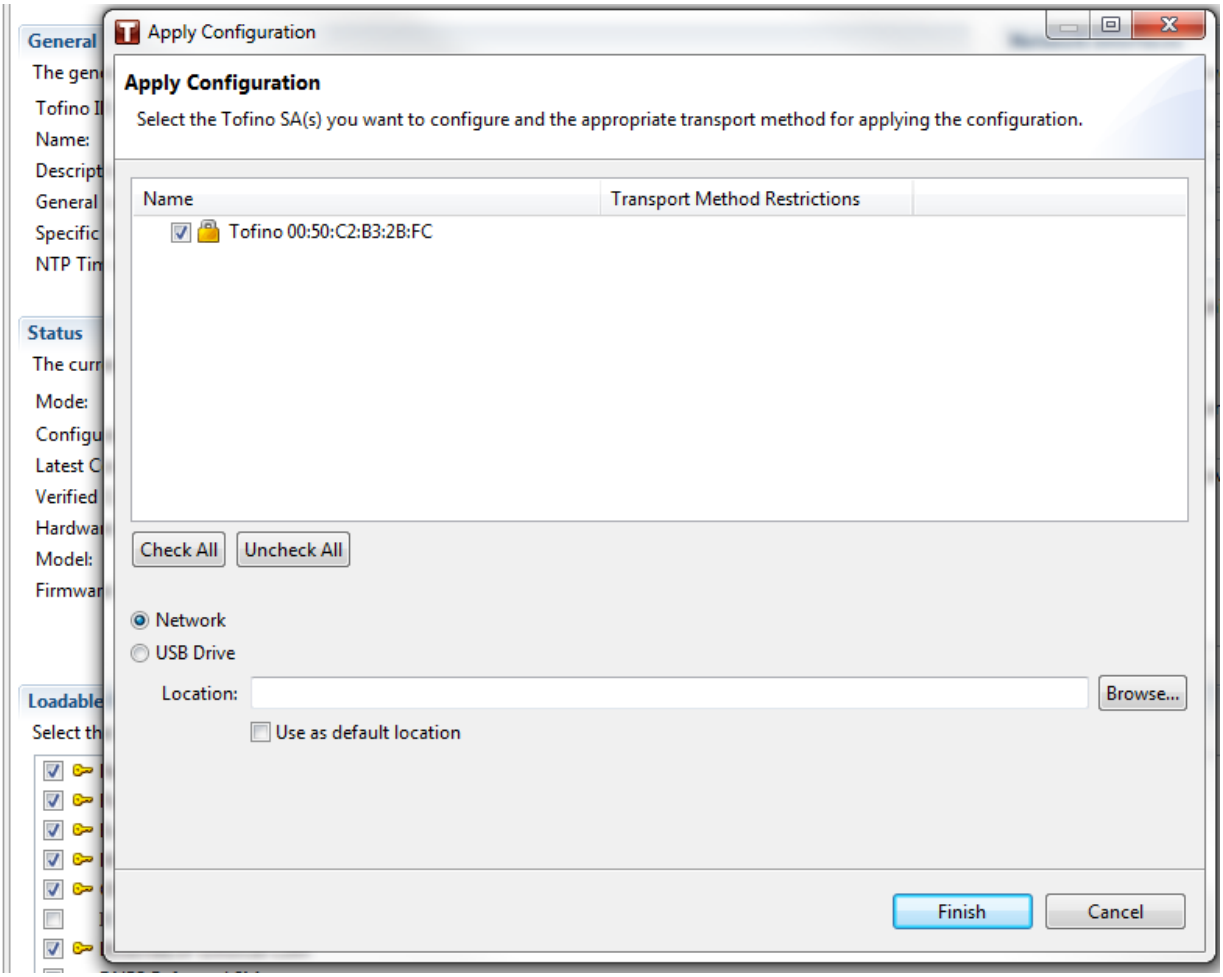
1. Click on the firewall tab in the tree. Along the top of the Firewall page it will suggest an ARP rule. By clicking on this the rule will be created.



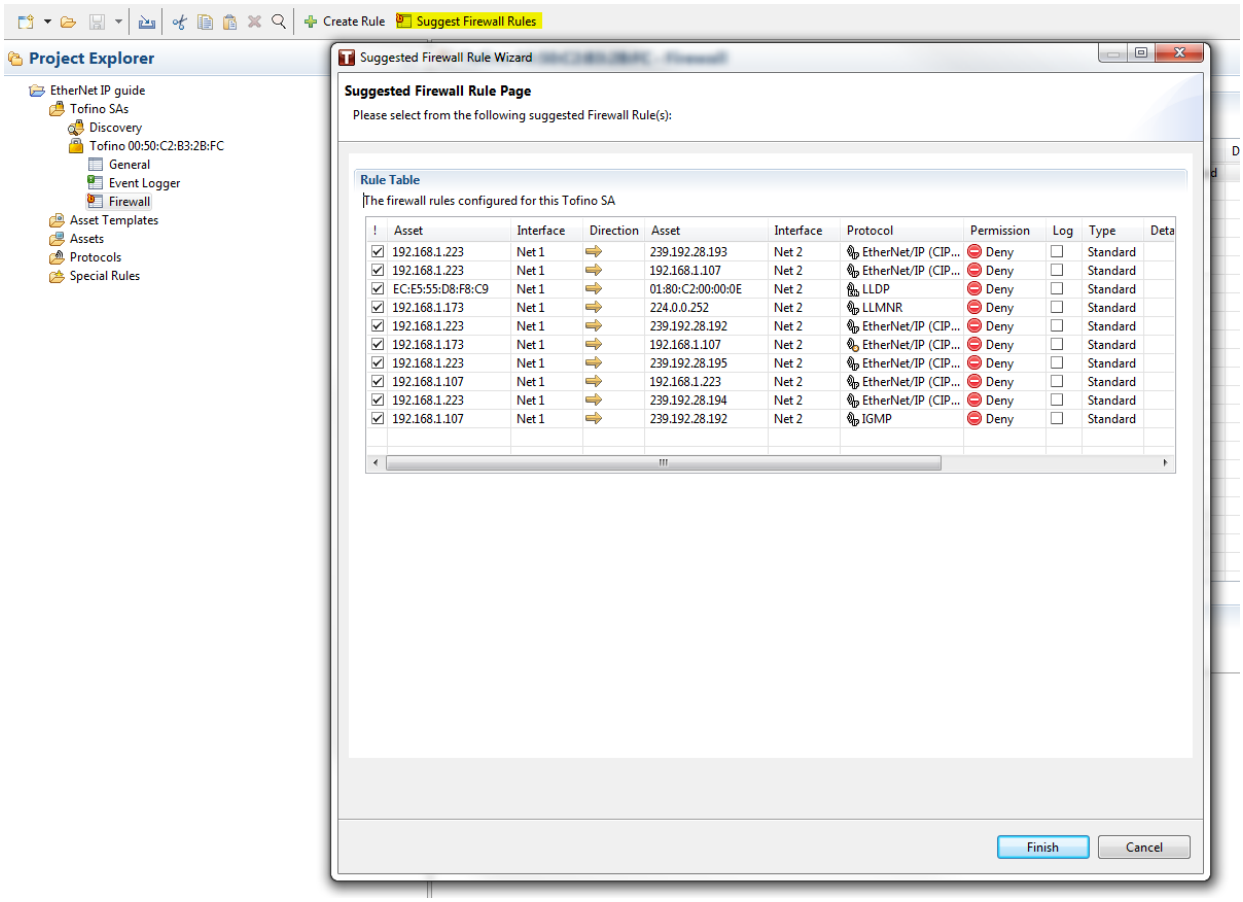
2. After the ARP rule is create go to the General tab and click Apply in the tool bar at the top of the page.



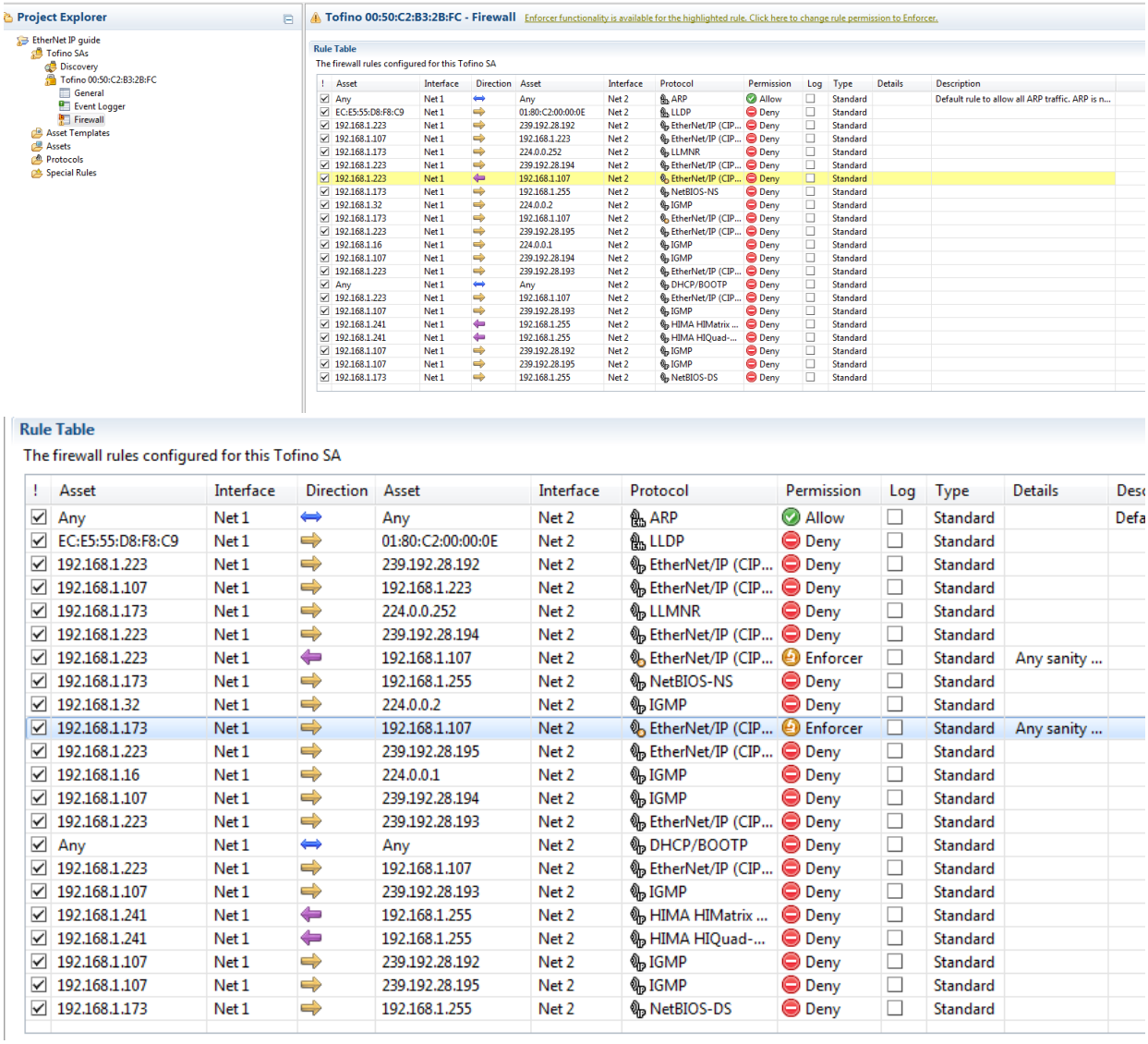
3. Press OK to save the Project and save to the desired location. Then make sure the correct Tofino is checked if you have multiple Tofinos in your project. Also make sure that Network is selected and click finish.



4. Wait a couple of minutes to allow the traffic to go through the Tofino. Then go back in the firewall tab and click on suggested rules in the tool bar. Select all of the rules that apply and click finish. The rules will auto fill into the rule table. The rules that fill into the rule table will have to be change to allow if the traffic is require in the network when the process is finished. Note if you change to allow before you are done suggesting rules you will see the same rules as deny everytime you click on suggest rules..



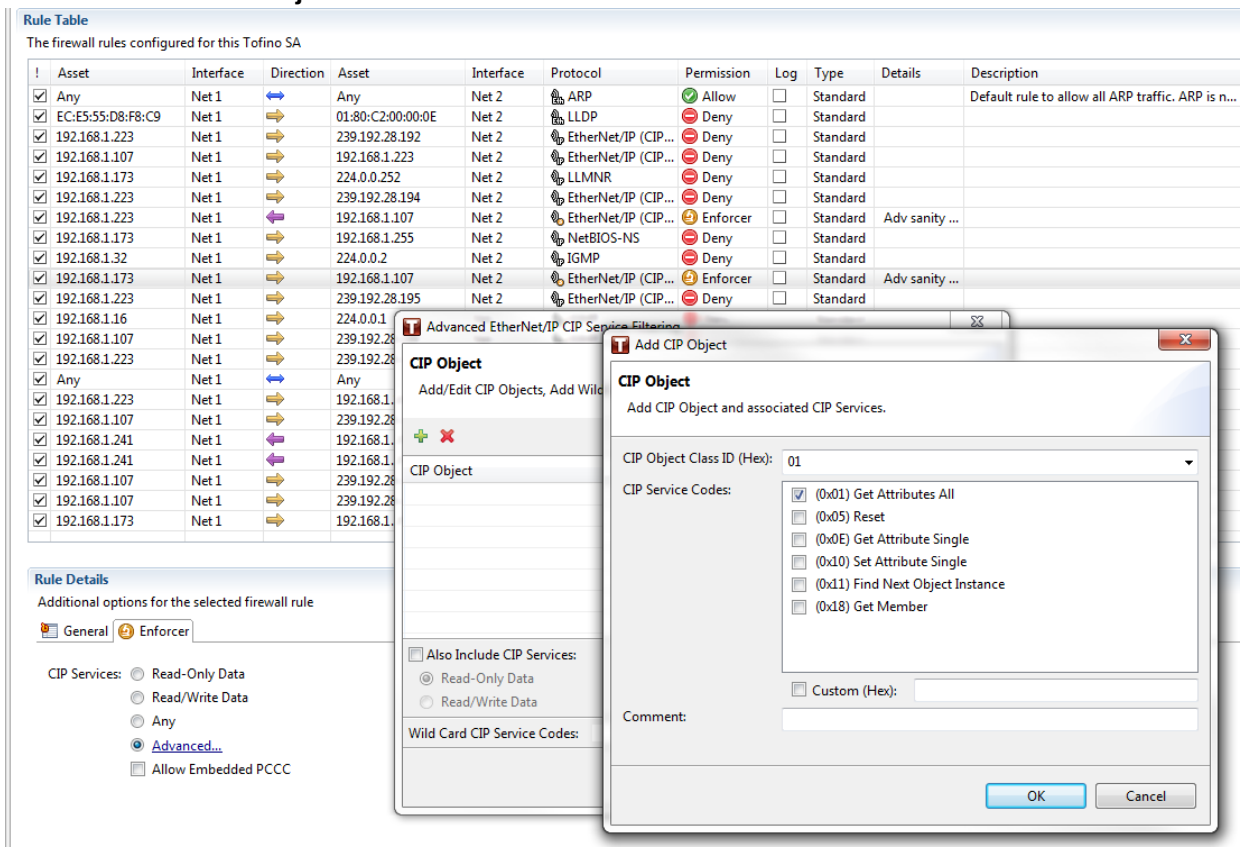
5. If there is a rule that can be an enforcer it will be high lighted in yellow and there will be a message at the top of the rule table you can click on to automatically change to enforcer.



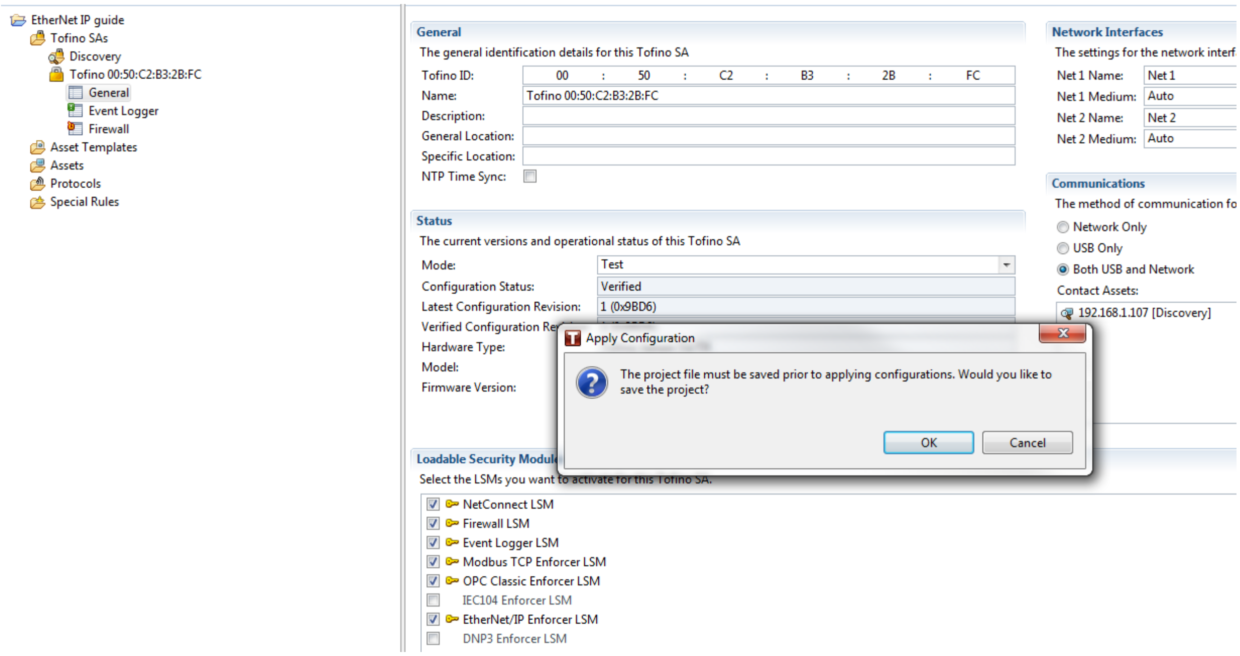
Rule Table
The firewall rules configured for this Tofino SA

!	Asset	Interface	Direction	Asset	Interface	Protocol	Permission	Log	Type	Details	Desc
☑	Any	Net 1	⟺	Any	Net 2	ARP	Allow	☐	Standard		Defa
☑	EC:E5:55:D8:F8:C9	Net 1	⇨	01:80:C2:00:00:0E	Net 2	LLDP	Deny	☐	Standard		
☑	192.168.1.223	Net 1	⇨	239.192.28.192	Net 2	EtherNet/IP (CIP...	Deny	☐	Standard		
☑	192.168.1.107	Net 1	⇨	192.168.1.223	Net 2	EtherNet/IP (CIP...	Deny	☐	Standard		
☑	192.168.1.173	Net 1	⇨	224.0.0.252	Net 2	LLMNR	Deny	☐	Standard		
☑	192.168.1.223	Net 1	⇨	239.192.28.194	Net 2	EtherNet/IP (CIP...	Deny	☐	Standard		
☑	192.168.1.223	Net 1	⇦	192.168.1.107	Net 2	EtherNet/IP (CIP...	Enforcer	☐	Standard	Any sanity ...	
☑	192.168.1.173	Net 1	⇨	192.168.1.255	Net 2	NetBIOS-NS	Deny	☐	Standard		
☑	192.168.1.32	Net 1	⇨	224.0.0.2	Net 2	IGMP	Deny	☐	Standard		
☑	192.168.1.173	Net 1	⇨	192.168.1.107	Net 2	EtherNet/IP (CIP...	Enforcer	☐	Standard	Any sanity ...	
☑	192.168.1.223	Net 1	⇨	239.192.28.195	Net 2	EtherNet/IP (CIP...	Deny	☐	Standard		
☑	192.168.1.16	Net 1	⇨	224.0.0.1	Net 2	IGMP	Deny	☐	Standard		
☑	192.168.1.107	Net 1	⇨	239.192.28.194	Net 2	IGMP	Deny	☐	Standard		
☑	192.168.1.223	Net 1	⇨	239.192.28.193	Net 2	EtherNet/IP (CIP...	Deny	☐	Standard		
☑	Any	Net 1	⟺	Any	Net 2	DHCP/BOOTP	Deny	☐	Standard		
☑	192.168.1.223	Net 1	⇨	192.168.1.107	Net 2	EtherNet/IP (CIP...	Deny	☐	Standard		
☑	192.168.1.107	Net 1	⇨	239.192.28.193	Net 2	IGMP	Deny	☐	Standard		
☑	192.168.1.241	Net 1	⇦	192.168.1.255	Net 2	HIMA HIMatrix ...	Deny	☐	Standard		
☑	192.168.1.241	Net 1	⇦	192.168.1.255	Net 2	HIMA HIQuad-...	Deny	☐	Standard		
☑	192.168.1.107	Net 1	⇨	239.192.28.192	Net 2	IGMP	Deny	☐	Standard		
☑	192.168.1.107	Net 1	⇨	239.192.28.195	Net 2	IGMP	Deny	☐	Standard		
☑	192.168.1.173	Net 1	⇨	192.168.1.255	Net 2	NetBIOS-DS	Deny	☐	Standard		

6. Next you will have to add an object and service code so the TC can suggest DPI enfocer rules. This is done by clicking on the enforcer rule to highlight it. Then click the enforcer tab under the rule table. Click on the advaced tab and then the green plus sign to add a CIP Object and a service code for the object.



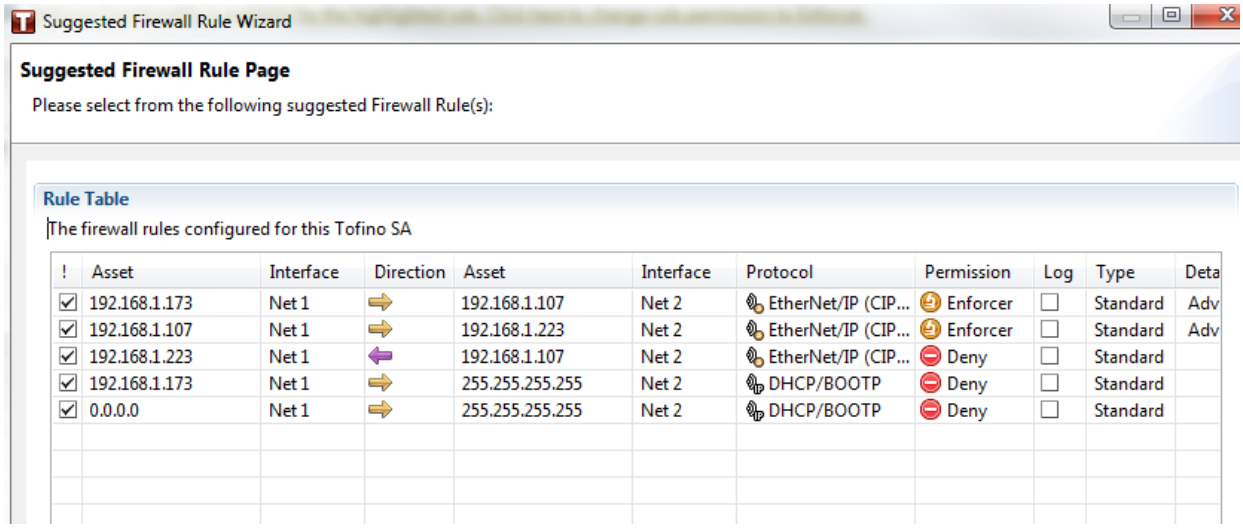
7. In the general tab apply the rule set that is now in the rule table by clicking the Apply button in the tool bar at the top of the page.



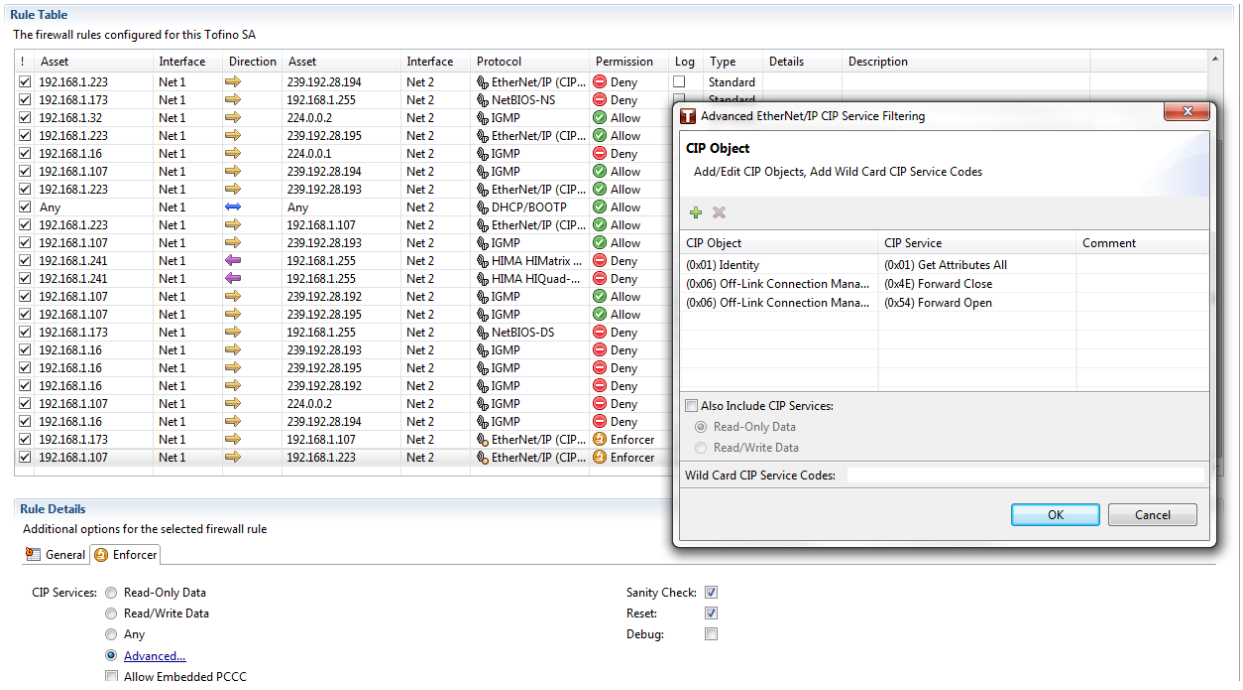
8. Give the tofino a minute log some of the traffic from the new rules and verify that you can see the enforcer logs in the syslog server.

```
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|200001|Tofino Firewall: ACL Violation|6|msg=ACL violated due to incorrect network address(es), protocol, ports, rate limit and/or state TofinoMode=TEST smac=ec:e5:55:d8:f8:c9 dmac=01:80:c2:00:00:00 proto=LLC TofinoSNAPdsnap=42 TofinoSNAPsnap=42 TofinoSNAPctrl=3 TofinoPhysIn=eth0
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310036|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x0a:Multiple Service Packet is not permitted TofinoMode=TEST smac=00:00:bc:33:50:0d src=192.168.1.107 spt=44818 dmac=34:e6:d7:38:bc:cc dst=192.168.1.173 dpt=52580 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=64 TofinoPhysIn=eth1
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310037|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x4c:Unknown Vendor Specific Service - CIP Class 0x0072:Unknown Vendor Specific Class is not permitted TofinoMode=TEST smac=34:e6:d7:38:bc:cc src=192.168.1.173 spt=52580 dmac=00:00:bc:33:50:0d dst=192.168.1.107 dpt=44818 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=128 TofinoPhysIn=eth0
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310036|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x0a:Multiple Service Packet is not permitted TofinoMode=TEST smac=00:00:bc:33:50:0d src=192.168.1.107 spt=44818 dmac=34:e6:d7:38:bc:cc dst=192.168.1.173 dpt=52580 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=64 TofinoPhysIn=eth1
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310037|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x4c:Unknown Vendor Specific Service - CIP Class 0x0072:Unknown Vendor Specific Class is not permitted TofinoMode=TEST smac=34:e6:d7:38:bc:cc src=192.168.1.173 spt=52580 dmac=00:00:bc:33:50:0d dst=192.168.1.107 dpt=44818 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=128 TofinoPhysIn=eth0
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310036|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x0a:Multiple Service Packet is not permitted TofinoMode=TEST smac=00:00:bc:33:50:0d src=192.168.1.107 spt=44818 dmac=34:e6:d7:38:bc:cc dst=192.168.1.173 dpt=52580 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=64 TofinoPhysIn=eth1
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310037|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x4c:Unknown Vendor Specific Service - CIP Class 0x0072:Unknown Vendor Specific Class is not permitted TofinoMode=TEST smac=34:e6:d7:38:bc:cc src=192.168.1.173 spt=52580 dmac=00:00:bc:33:50:0d dst=192.168.1.107 dpt=44818 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=128 TofinoPhysIn=eth0
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310036|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x0a:Multiple Service Packet is not permitted TofinoMode=TEST smac=00:00:bc:33:50:0d src=192.168.1.107 spt=44818 dmac=34:e6:d7:38:bc:cc dst=192.168.1.173 dpt=52580 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=64 TofinoPhysIn=eth1
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310037|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x4c:Unknown Vendor Specific Service - CIP Class 0x0072:Unknown Vendor Specific Class is not permitted TofinoMode=TEST smac=34:e6:d7:38:bc:cc src=192.168.1.173 spt=52580 dmac=00:00:bc:33:50:0d dst=192.168.1.107 dpt=44818 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=128 TofinoPhysIn=eth0
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310036|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x0a:Multiple Service Packet is not permitted TofinoMode=TEST smac=00:00:bc:33:50:0d src=192.168.1.107 spt=44818 dmac=34:e6:d7:38:bc:cc dst=192.168.1.173 dpt=52580 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=64 TofinoPhysIn=eth1
Dec  1 23:28:33 00:50:C2:B3:2B:FC CEF:1|Tofino Security Standard|Tofino Xenon|03.0.00|310037|Tofino EtherNet/IP Enforcer: Filter Check|6|msg=EtherNet/IP Command 0x0070 - CIP Service 0x4c:Unknown Vendor Specific Service - CIP Class 0x0072:Unknown Vendor Specific Class is not permitted TofinoMode=TEST smac=34:e6:d7:38:bc:cc src=192.168.1.173 spt=52580 dmac=00:00:bc:33:50:0d dst=192.168.1.107 dpt=44818 proto=IPv4/TCP TofinoEthType=800 TofinoTTL=128 TofinoPhysIn=eth0
```

9. Because the TC will not create duplicate rules the enforcer rule will need to be deleted before clicking on suggest rules again. After the rule is deleted click on suggest rules.



10. After all of the suggested rules are in place change all of the traffic that needs to pass through the Tofino that is being denied to allow. Also go back into the advanced enforcer to add in the 01 object with the 01 service code.



11. Go to the general tab and apply the new rule set. After this is done go to the syslog and verify that the needed traffic is not being blocked. If the logs are not clear you will need add the rules in manually. If the log is clear you can put the Mode to Operational and apply.