Tofino/DNP3 Quick Start Guide

Tofino DNP3 Functionality

The Tofino Security Appliance (TSA) implements a DNP3 loadable security module (LSM) which enables deep packet inspection (DPI) firewall capabilities for DNP3 traffic. The installation engineer specifies master/slave device pairs between which DNP3 traffic will be allowed to flow. Only correctly formatted DNP3 traffic will be allowed. For example most of the DNP3 exceptions suggested in the Open DNP Group's document "DNP3 Application Note AN2013-004b: Validation of Incoming DNP3 Data" are implemented within the LSM. This includes checking of common header byte fields, packet lengths, DNP3 CRC values, etc.

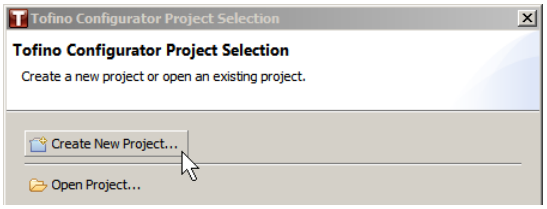
For each master/slave device pair, the engineer can also specify which DNP3 Application Layer message types or function codes will be allowed for request and response traffic. By selecting function codes, writing to, operating on, etc. objects can be disabled.

Setting Up a Tofino in a DNP3 Environment

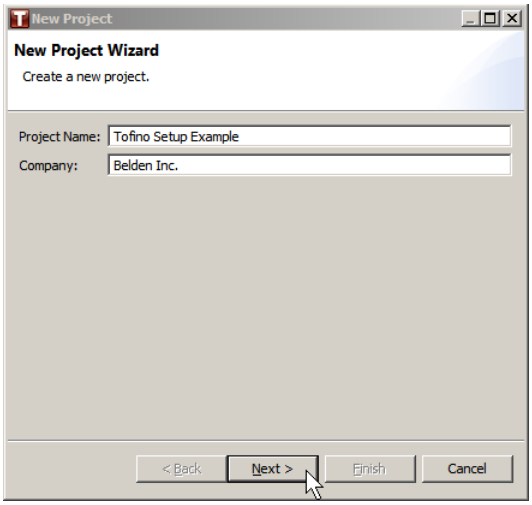
Place Tofino Xenon in the network between master and slave DNP3 devices.

Installing Tofino Configurator

When you run the Tofino Configurator (TC) software for the first time, you must Create a New Project by clicking on the "Create New Project…" button:

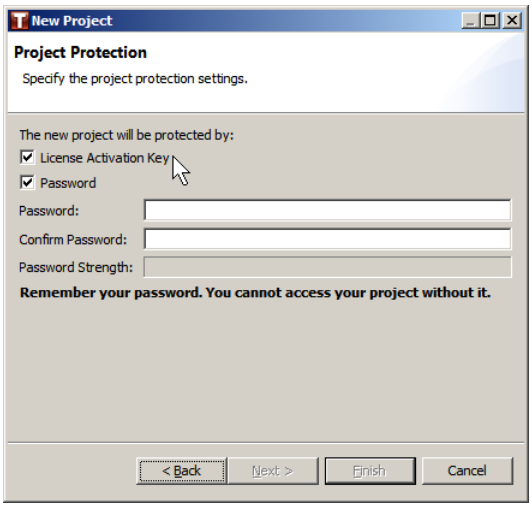


Choose a Project Name and fill in the name of your Company or leave it blank as you choose and click Next:

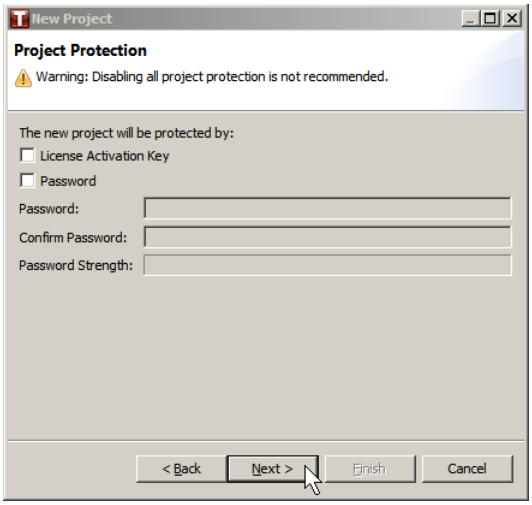


For demonstration purposes, access to the project will not be protected. Do NOT do this as part of a production installation.

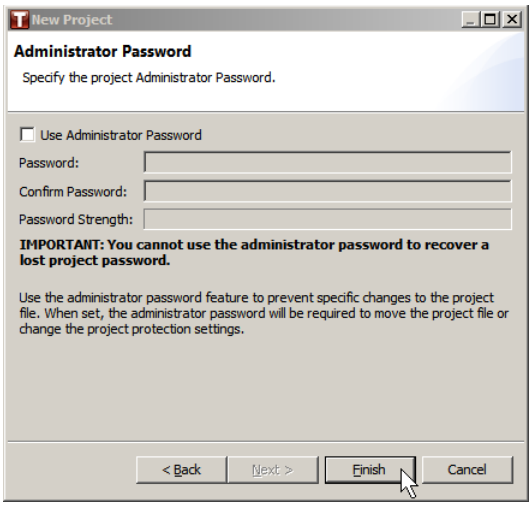
In the Project Protection dialog box, uncheck the License Activation Key and Password boxes:



When the boxes are unchecked, the Next button will be active. Click on the Next button:

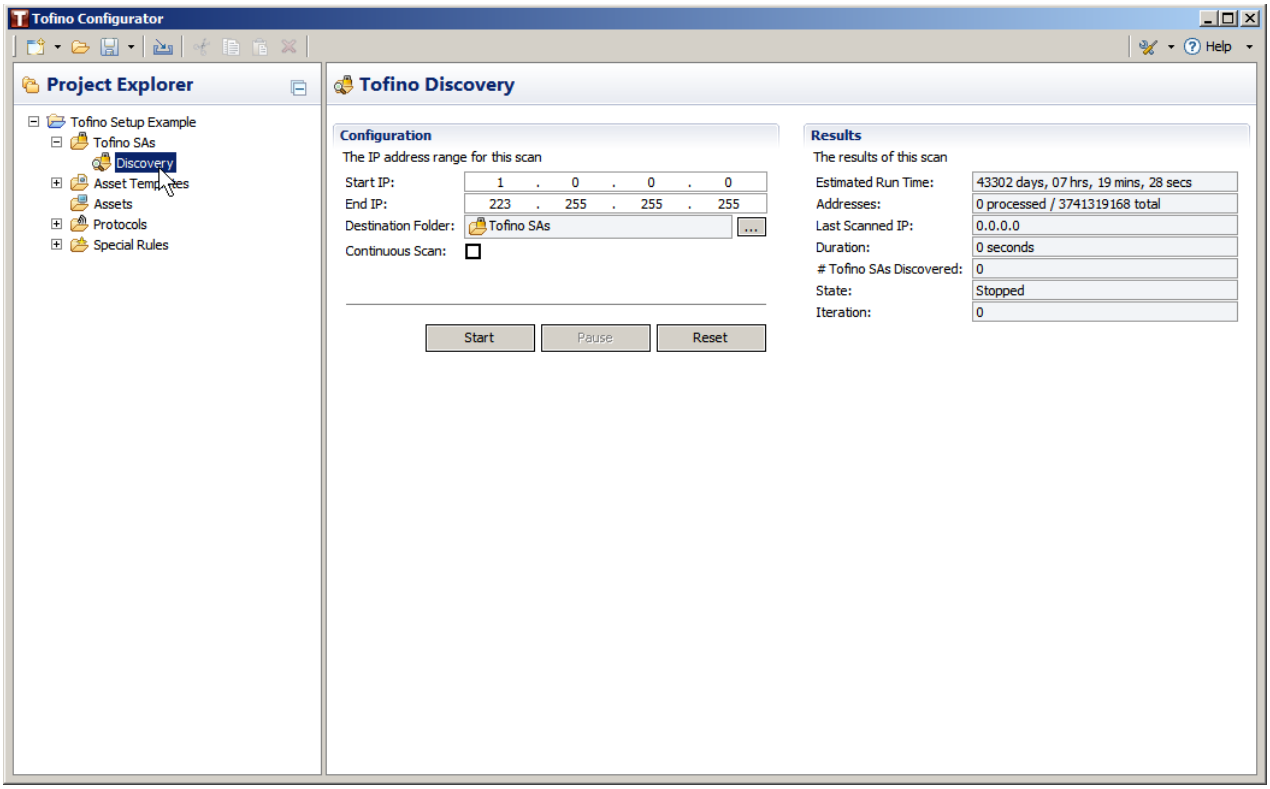


Then click on the Finish button in the next dialog box:



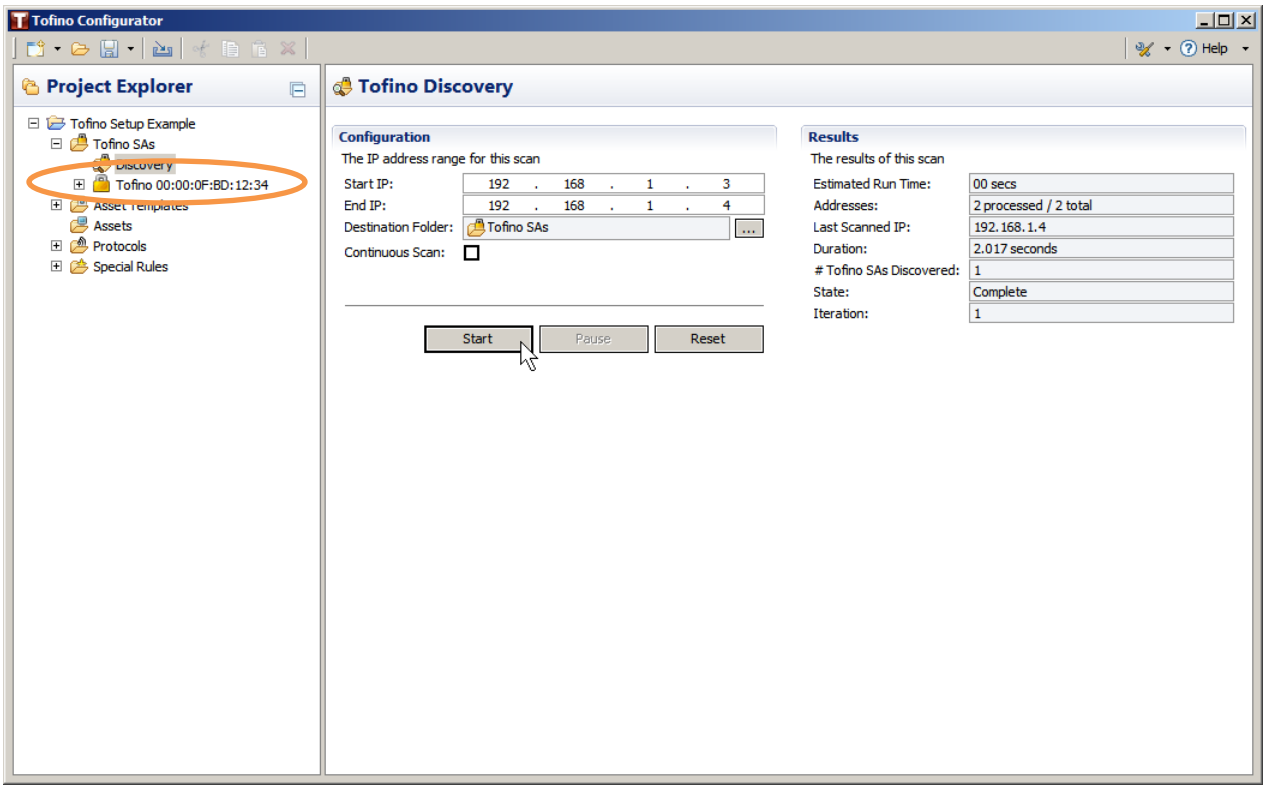
Tofino Discovery

You will now see the main Tofino Configurator page with the **Project Explorer** panel running along the left side. Click the "+" sign to the left of Tofino SAs in the Project Explorer panel and then click on Discovery:



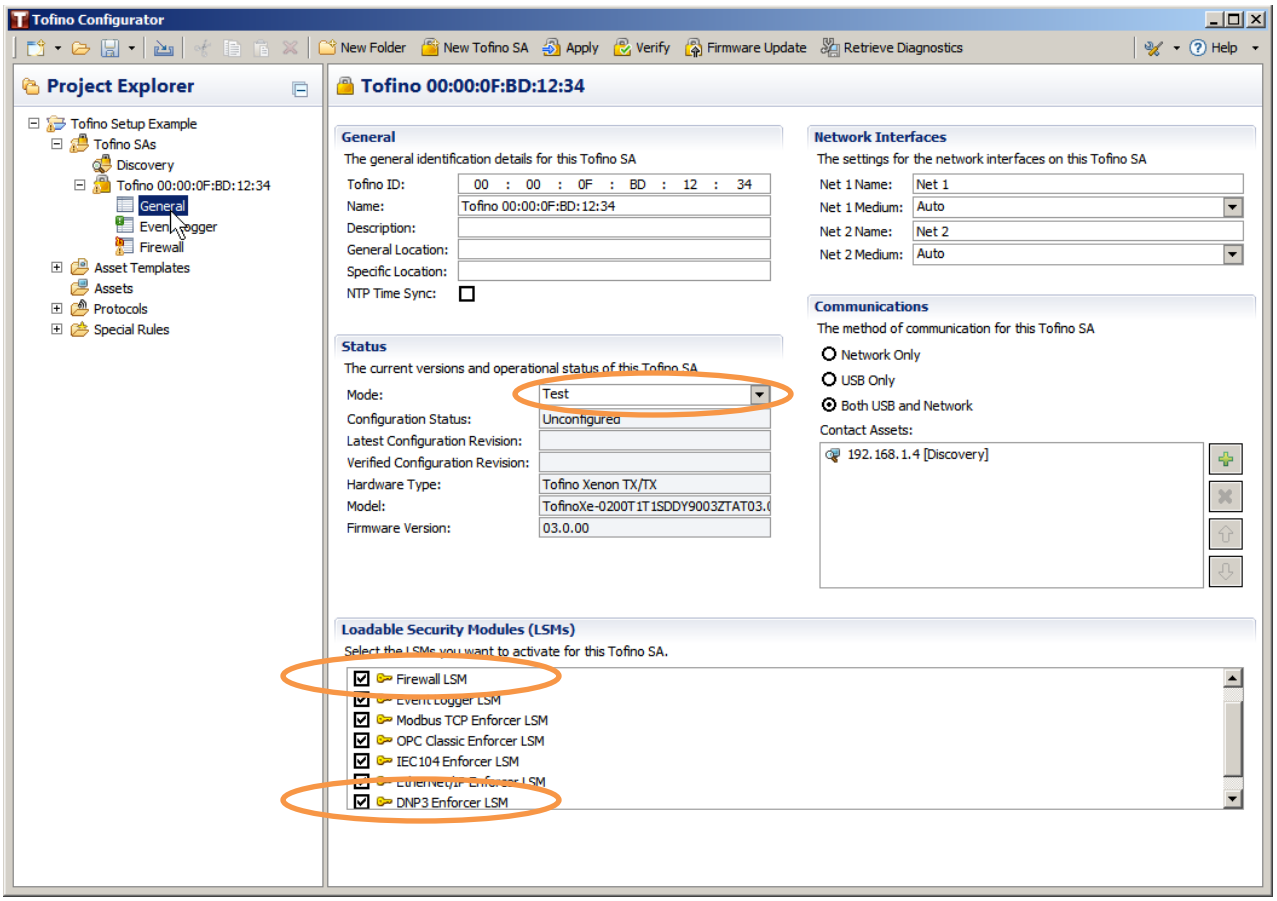
In the Tofino Discovery panel under Configuration, enter a Start IP and End IP which bracket the addresses on the network you are protecting. This is usually the network which contains your slave/server devices. For instance, if you have two meter devices with IP addresses 192.168.1.3 and 10.168.1.4, you can use those addresses as the Start IP and End IP to define the scan range. The

discovery will scan through all addresses in single address steps one per second, so **it is important to limit the size of the range specified**. When you have entered the addresses, click Start to start the scan:



Looking at the screenshot above, a Tofino with MAC address 00:00:0F:BD:12:34 was discovered and now appears in the Project Explorer panel. If no Tofino is discovered, the Project Explorer panel will look similar to it did in the previous screenshot with no Tofino MAC address listed. [1] Click on the "+" sign to the left of the Tofino device to expand the information and control selections available for the Tofino device and then click on General to open the General information panel for the Tofino:

[1] If your scan fails to discover the connected Tofino device, check your connections, IP addresses, and contact a Belden representative if necessary.

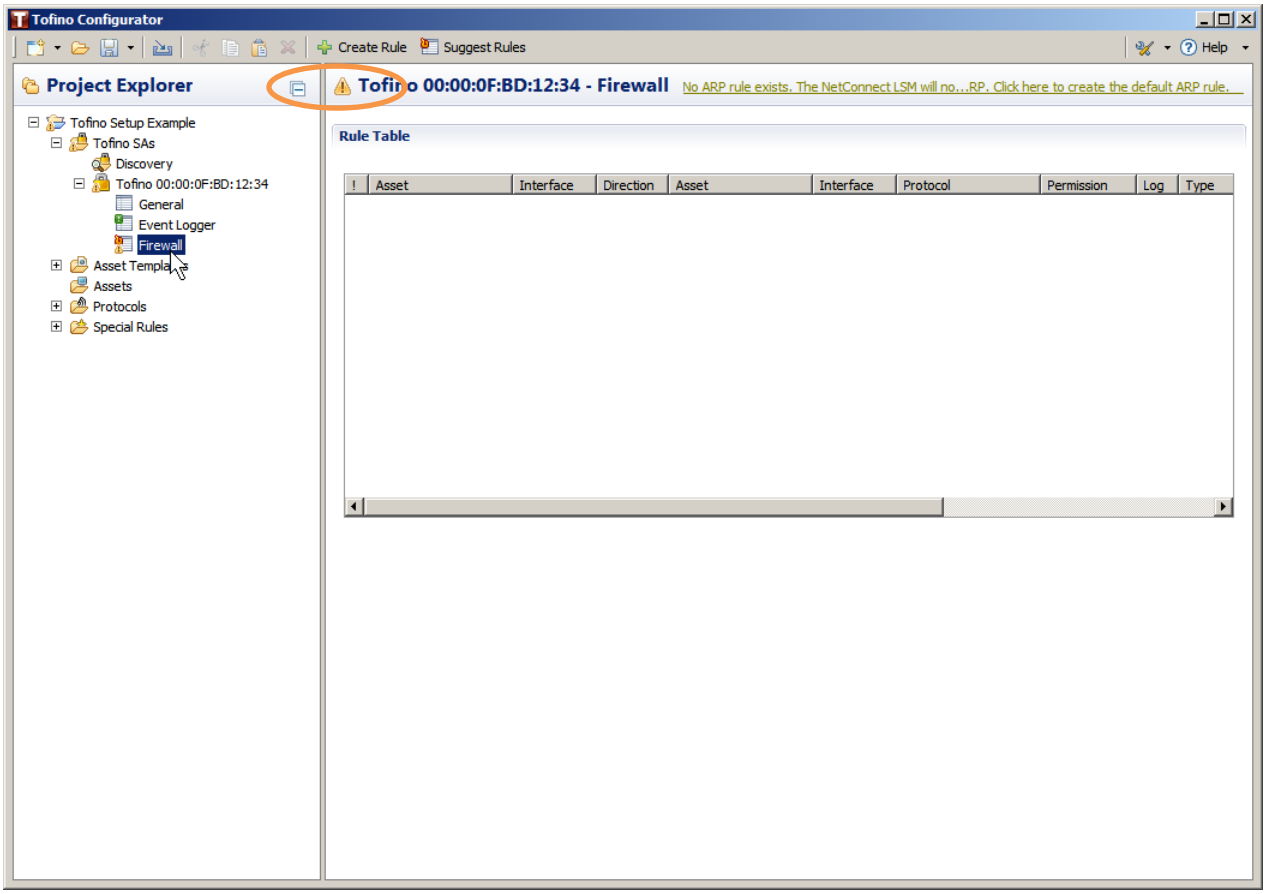


Two things are of interest in the above General information screenshot. First, the Status panel shows the Tofino Mode as Test. Second, the Loadable Security Modules (LSMs) panel shows the Firewall LSM and the DNP3 Enforcer LSM as selected. You can to scroll the list if necessary to see all listed LSMs. Additional LSMs might be selected as in the screenshot above but are not necessary.

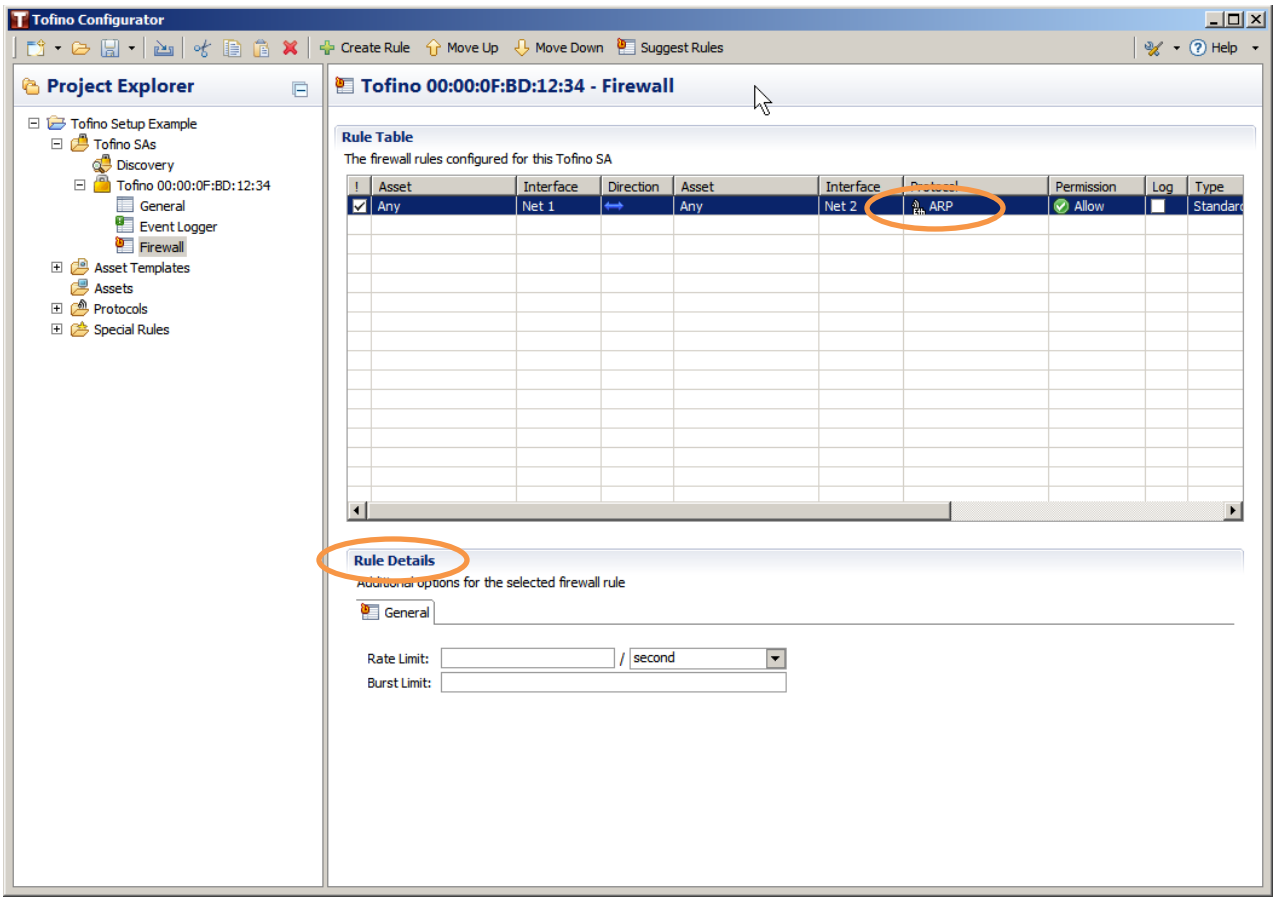
Tofino Firewall Settings

The firewall rules determine what traffic is allowed to pass through the Tofino once it is placed in Operational mode. In Test mode, the Tofino will allow all traffic to pass, but will still flag traffic which would have been flagged and blocked by an Enforcer in Operational mode, given the current list of firewall rules.

To show the Firewall Rule panel, click on the Firewall selection under the Tofino in the Project Explorer panel:



In the Firewall panel screenshot above, notice the yellow triangle alert symbol. This is associated with the message, "No ARP rule exists… Click here to create the default ARP rule." The ARP rule allows ARP discovery to pass through the Tofino device. Click the "No ARP rule…" message and the ARP rule appears in the Rule Table panel:

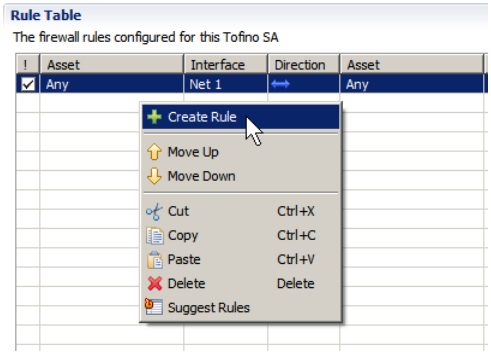


Looking at the screenshot above, we see the Rule Table panel has a new rule with the protocol ARP. You can scroll the table to the right to see additional columns in the Rule Table.

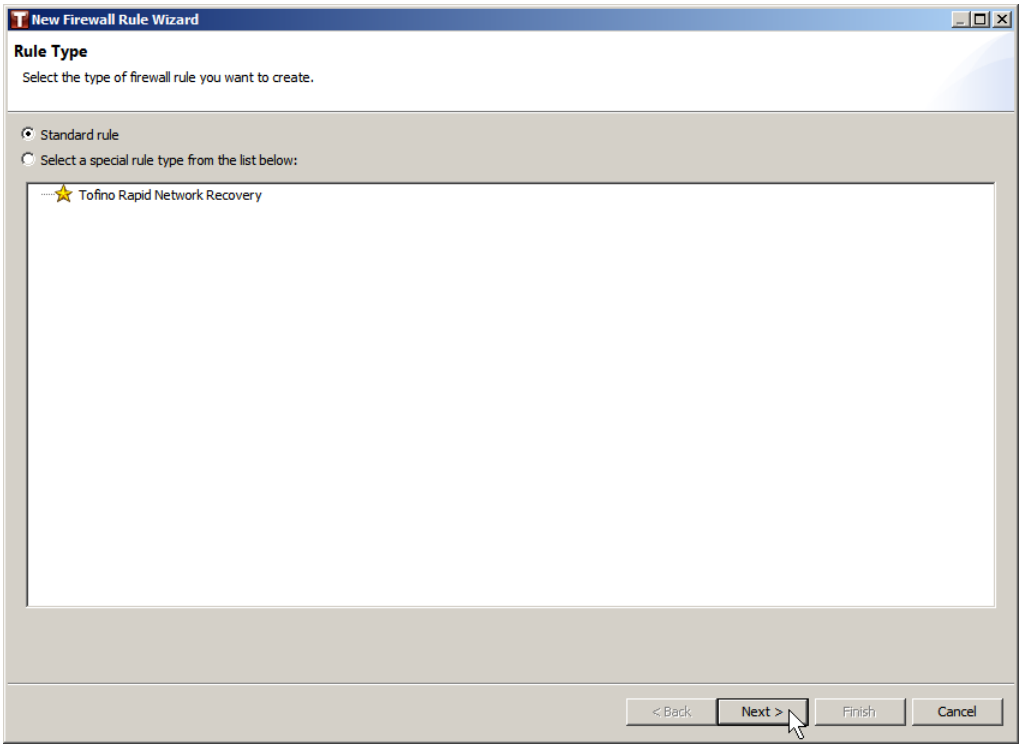
With the inclusion of a firewall rule, the Rule Details panel appears below the Rule Table panel. The Rule Details are used to configure the currently highlighted rule in the Rule Table, and will be described in more detail with respect to configuring DNP3 Enforcer firewall rules.

Adding DNP3 Enforcer Firewall Rules

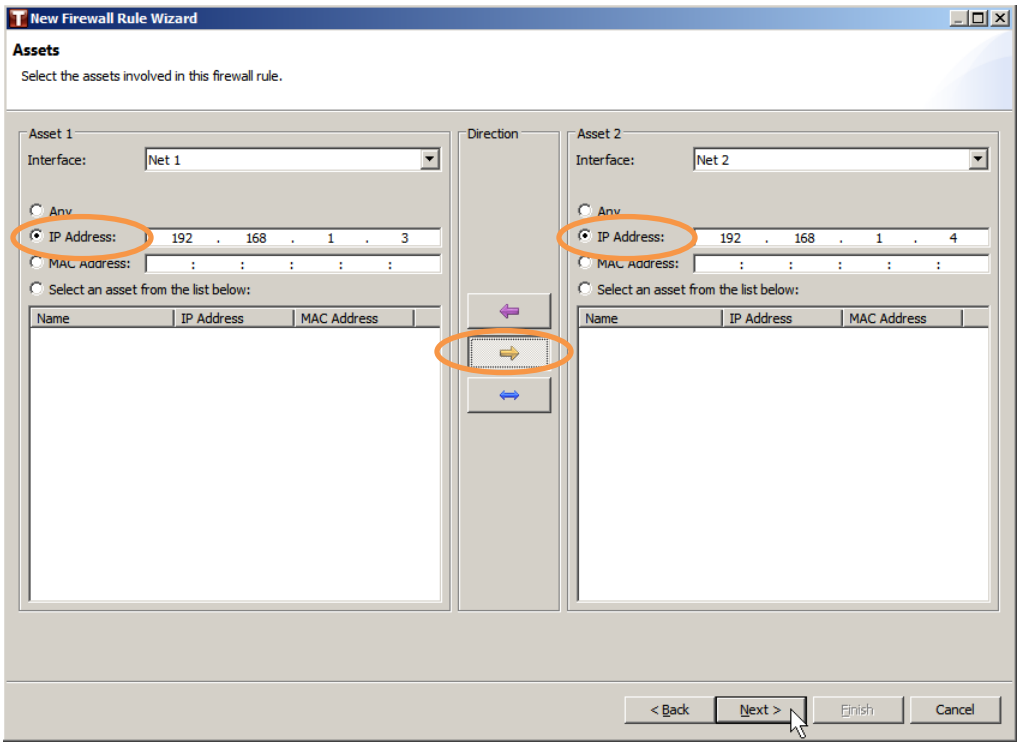
To add a DNP3 Enforcer firewall rule, right-click on the empty line below the ARP rule and select/click Create Rule:



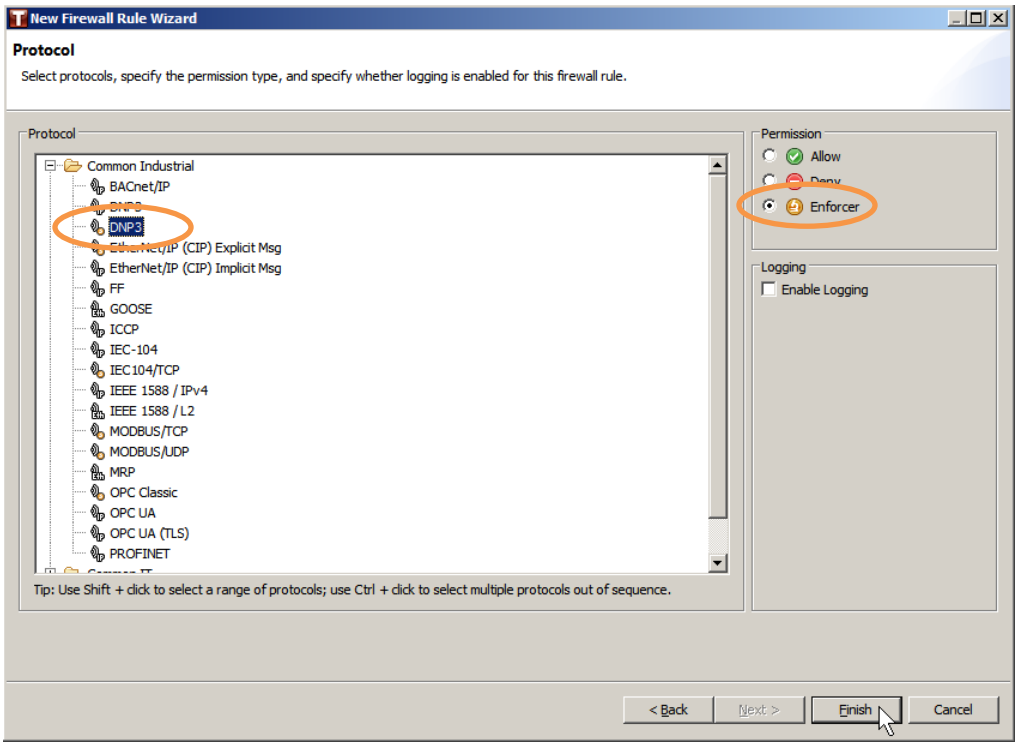
This opens the New Firewall Rule Wizard. Click Next to open the rule Assets panel:



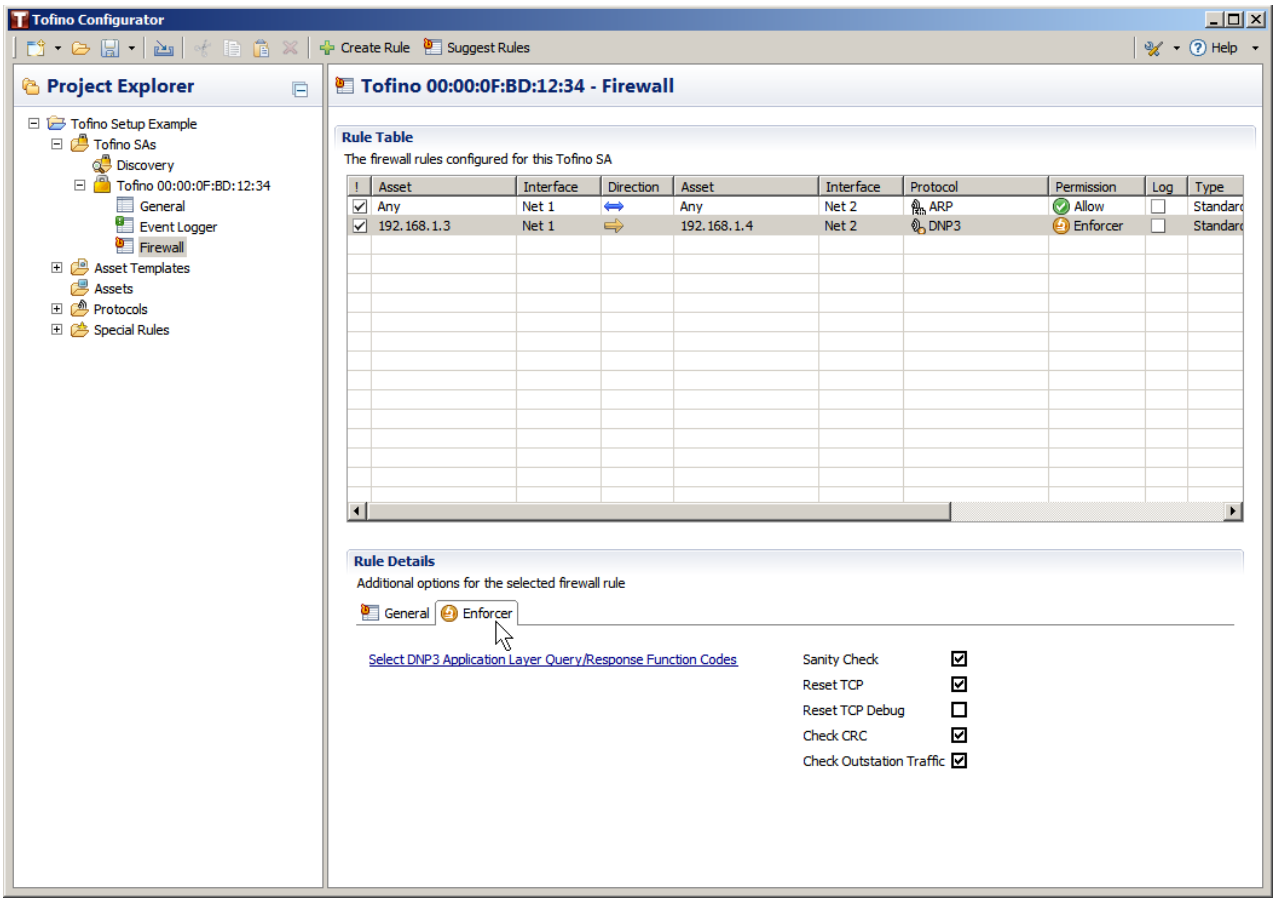
DNP3 Enforcer rules are unidirectional, mapping from the client/master to the server/slave device. As an example, the screenshot below shows an Assets panel with a mapping from a DNP3 master at IP address 192.168.1.3 to a DNP3 slave device at 192.168.1.4. This is created by selecting the IP Address bullet and entering the IP address for each of Asset 1 and Asset 2, and then selecting the right arrow for the client-to-server direction. After entering this information, click Next to open the rule Protocol panel:



The firewall rule Protocol panel allows configuration of the protocol associated with a firewall rule. In this case, configuring the rule as a DNP3 Enforcer rule requires we select DNP3 under the Common Industrial rules. Click on the "+" to the left of Common Industrial in the panel to expand the list of industrial protocols. Then select the instance of DNP3 which has the icon with the orange, circular badge on it as shown in the screenshot below. In the Permissions panel on the right, select Enforcer. Note the similar orange, circular badge to the left of the word Enforcer. Then click Finish to complete the rule configuration:



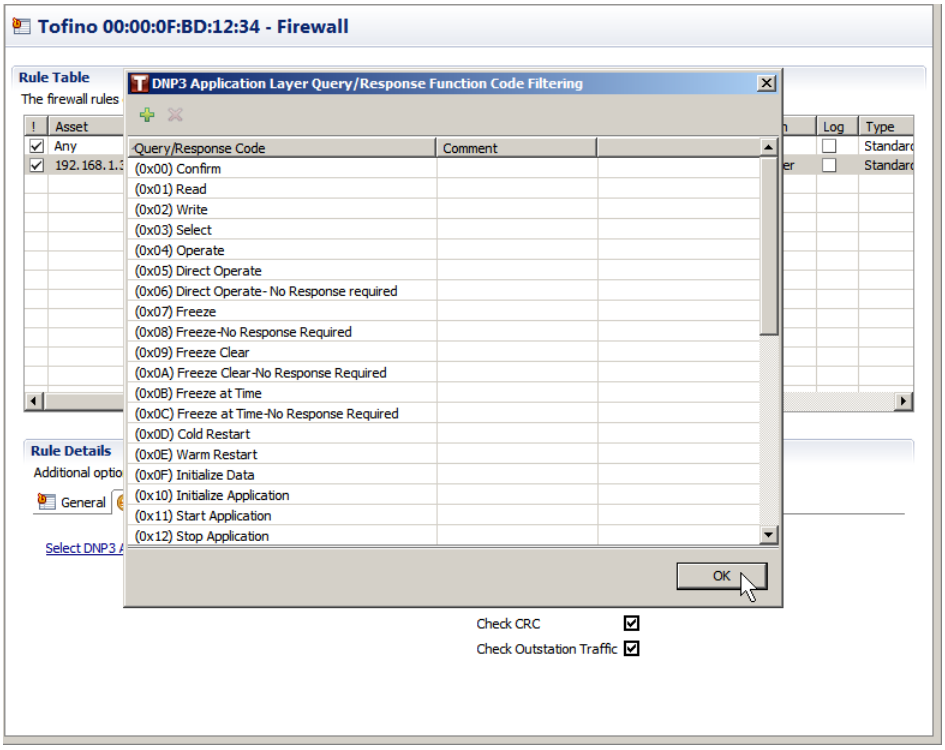
The Tofino Configurator will now show the firewall Rule Table with the newly configured DNP3 Enforcer rule highlighted. To see the detailed configuration for this Enforcer rule, click on the Enforcer tab in the Rule Details panel:



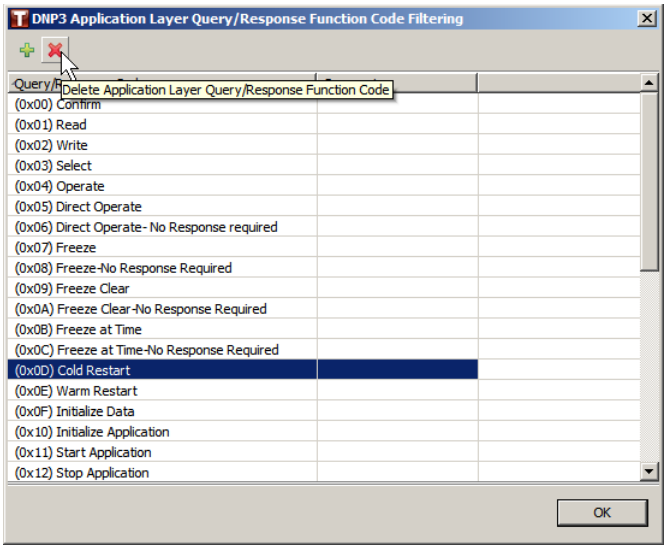
DNP3 Enforcer Check Boxes

Check Box	Meaning When Checked
Sanity Check	Enables sanity checking and validation of DNP3 packets. This can be disabled if one of the sanity checks is causing a problem for valid network traffic.
Reset TCP	Enables the generation of a TCP reset packet on both Tofino ports when a DNP3 packet is dropped by the Enforcer.
Reset TCP Debug	Enables the generation of a debug message when a TCP reset is sent by the Enforcer.
Check CRC	Enables the computation and verification of CRCs in both DNP3 Data-Link Layer Headers and Application Layer Messages. The overhead of computing and checking the CRCs is not as large as might be expected. Even for heavily loaded systems, toggling this flag may not result in a detectable change in performance.
Check Outstation Traffic	Enables the checking of packets originating at an outstation. Packets originating at a master are always checked when the Enforcer is active. Note: If this flag is not enabled, packets originating at an outstation will not trigger any of the sanity checks mentioned in these requirements.

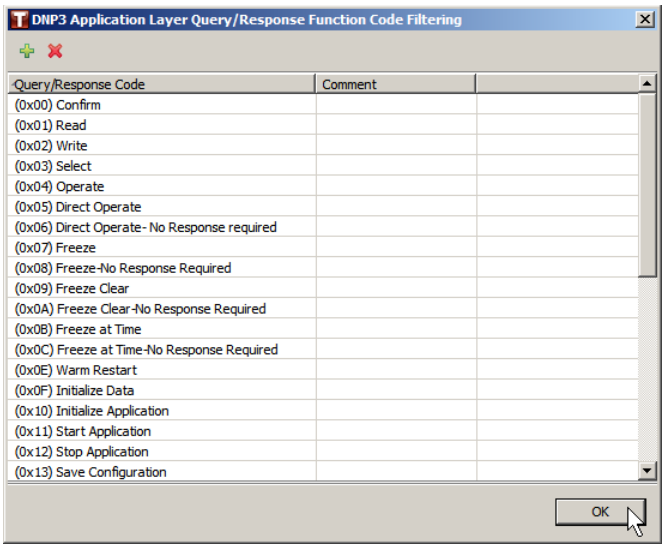
In addition to the check boxes described in the table above, additional deep-packet inspection (DPI) capabilities of the DNP3 Enforcer allow it to pass or block packets based on the Application Layer Function Code (FC). The function codes are configured in the Function Code Filtering dialog box. Open the dialog by clicking on Select DNP3 Application Layer Query/Response Function Codes in the Rule Details panel:



To disable the ability to do a Cold Restart of a DNP3 device from outside the Tofino-protected portion of the network, remove the Cold Restart function code from the list. To do this, highlight the Cold Restart function code in the list and click on the red "X" at the top of the dialog:



Note the context-sensitive help which appears while the cursor is on the red "X". After clicking, there is a confirmation dialog, and finally the list appears with Cold Restart removed:



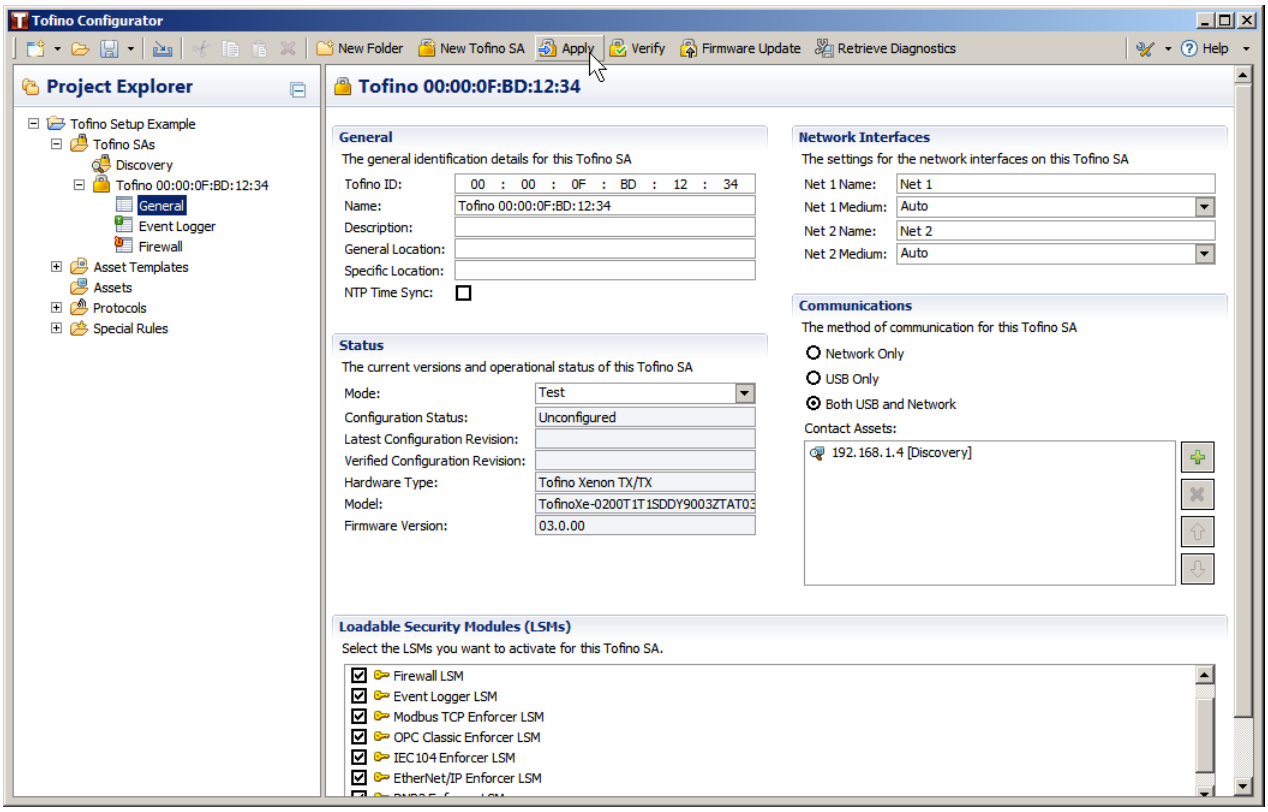
Click OK to close the Function Code Filtering dialog.

To add new function codes click on the green "+" and follow the dialog.

The Rule Details are unique for each rule. If a rule is copied using the copy-paste feature, the Rule Detail information is also copied.

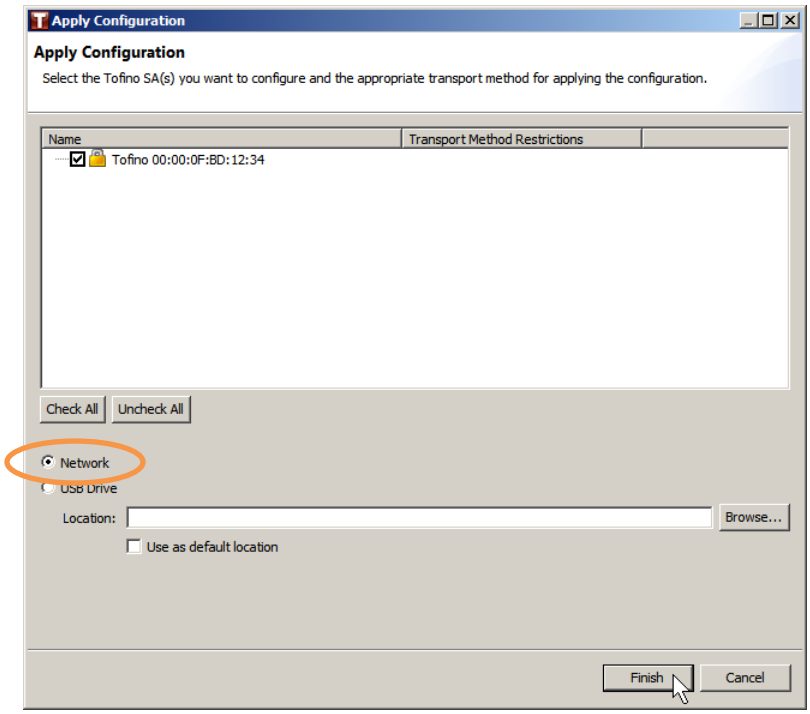
Applying Rules to the Tofino Security Appliance

The configured firewall rules exist only in the Tofino Configurator (TC). To move them to the Tofino we must apply the configuration. To do this, select General under the Tofino in the Project Explorer and click on the Apply selection at the top of the TC window:

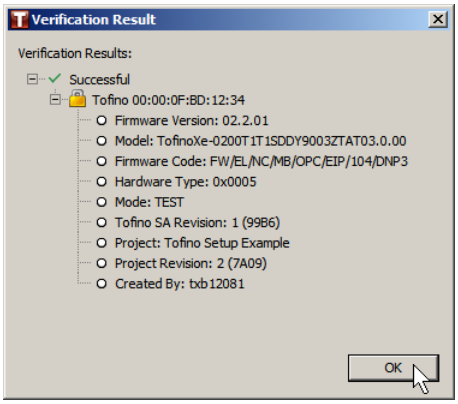


An Apply Confirmation dialog appears for a confirmation to save the configuration to disk. Click OK and specify a file name if necessary to continue.

The Apply Configurations dialog opens. This allows applying configurations to multiple Tofino devices over the network or via USB drives. The dialog includes the single Tofino in this example and the network is selected as the delivery medium. Click Finish to continue:



A progress dialog appears. Configuring the Tofino can take some time. When the configuration completes, a verification step is automatically triggered. When it completes, a Verification Result dialog appears. Clicking on the "+" to the right of the Tofino in this dialog shows information about the firmware, model, operation mode, etc.:



Click OK to exit this dialog. The Tofino Security Appliance is now configured to work as a DNP3 DPI firewall.