

# Protecting OPC Servers with Tofino™ OPC Enforcer

Application Note #105

AN-105  
Version 1.0

## Overview

OPC, originally called OLE for Process Control, is used extensively in control systems to provide interoperability between devices and software from different vendors. While the latest version of OPC (OPC UA) has included security requirements in its design, the OPC 'Classic' protocols (OPC DA, OPC HDA, and OPC A&E) are based on the Microsoft DCOM protocols which were designed before network security issues were widely understood. As a result, these protocols present significant challenges for control engineers who wish to ensure the security and reliability of the control system.

This application note provides a summary of the security issues related to OPC, and shows how the Tofino OPC Enforcer can be used to protect OPC servers and clients.

## OPC Classic Security Issues

Most TCP and UDP communication protocols use a single standardized port number – for example, Modbus/TCP always uses port 502. Client devices can create a single connection to a server device on this port number, and then send and receive data to and from the server. Protecting these client and server devices with a firewall is relatively straightforward – simply configure the firewall to allow communications on the desired port numbers, and block all other network traffic.

The OPC Classic protocols are not so simple. OPC connections are created using a two-step process:

1. The client queries the server on port 135 to obtain a TCP port number for the desired data object.
2. The client connects to the server on the port number obtained in step 1 (above) to access the desired data.

The port number for the data object request (step 1) is standardized and well-known. However, the

port numbers for the actual data connections (step 2) are allocated dynamically by the OPC server in a pseudo-random sequence, so there is no way to know in advance which port numbers the server will return to the client. In addition, the range of port numbers that the server may assign is very large – over 16,000 port numbers for Windows Server 2008, and over 48,000 ports for earlier Windows versions.

Because of this, a conventional firewall protecting the OPC server would have to allow TCP connections between the OPC client(s) and server on any TCP port within this very large range. The security provided by the firewall in this case is minimal at best. As a result, the vast majority of OPC servers operate today without any firewall protection at all, and are therefore vulnerable to malware and other security threats.

## The Tofino OPC Classic Enforcer

The Tofino OPC Enforcer tracks the port numbers for OPC data connections dynamically, as they are allocated by the OPC server. It opens only the minimum required ports in the Tofino Firewall to allow the data connections to pass through it, while keeping all unused ports closed. It can also perform a 'sanity check' on the OPC data request and response messages, and block any messages that do not conform to the relevant DCE/RPC standards.

As a result, the OPC Enforcer enables effective firewall protection for systems that use OPC Classic protocols. OPC data connections will pass unimpeded through the Tofino Security Appliance (SA), while abnormal or undesired traffic will be blocked and reported by the Tofino Firewall LSM. The Tofino Security Appliance provides this protection independently of the Windows PCs; no changes are required to the OPC clients or servers.

## Example Use Case

The following subsections show how to use the Tofino OPC Enforcer to protect communications between an OPC client and server device.

In this example we will use Matrikon OPC Explorer as an OPC client to communicate with Matrikon OPC Server for simulation. A Tofino Security Appliance is installed between the OPC server and the rest of the control network. A Tofino Central Management Platform (CMP) is used to configure and manage the Tofino Security Appliance. A network diagram of the example system is shown in Figure 1.

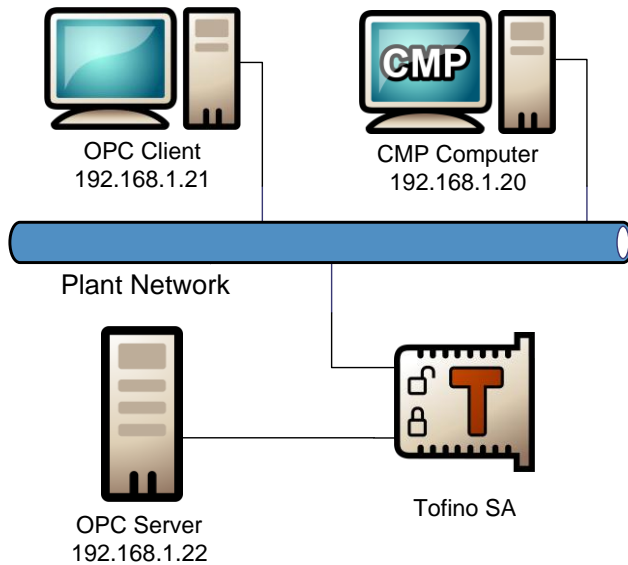


Figure 1: OPC Server Protected by Tofino

## Configuration in the Tofino CMP

The Tofino CMP enables the user to create a model of the control network by dragging icons from the Nodes view (or by using the Tofino Discovery and Asset Discovery features) and dropping them into the Network Editor. It's possible to model the entire network if desired, but only devices that will appear in the firewall rules are required to be included in the network model. As a result, the finished model of the OPC example network (Figure 2) is very simple.

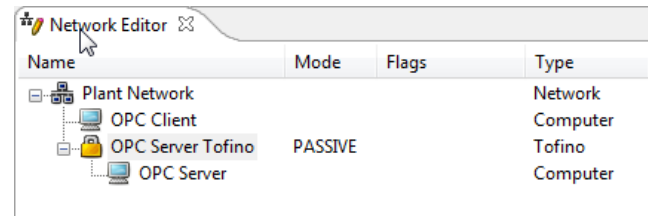


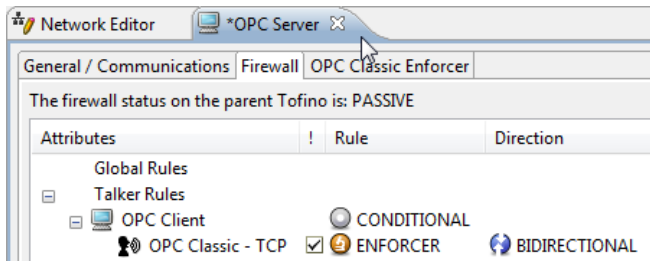
Figure 2: Network Model in the Tofino CMP

Once the model is complete, the Tofino Firewall and OPC Enforcer Modules must be activated on the Tofino Security Appliance. This is done on the 'Modules' tab of the Tofino icon in the Network Editor.

## Create and Configure a Firewall Rule

Next, a firewall rule is created to allow OPC communications between the client and server. A 'Talker' firewall rule is created as follows:

1. Double-click on the OPC Server icon to display the server's settings, then click on its Firewall tab.
2. Locate the OPC Client icon in the 'Network' view (top left corner of the Tofino CMP), then drag this icon and drop it on the 'Talker Rules' row in the OPC Server's firewall tab.
3. Drag the 'OPC Classic - TCP' protocol from the 'Protocols' view (bottom right corner of the Tofino CMP) and drop it on the OPC Client icon in the Server's firewall tab.
4. Double-click on the 'OPC Classic - TCP' firewall rule, change its permission to 'Enforcer', and click OK. This permission setting enables the OPC Enforcer to inspect the traffic between the computers and track OPC data connections that are created.



**Figure 3: OPC Server Firewall Tab**

The completed firewall rule is shown in Figure 3. Clicking the OK button at the bottom of the view will save the new rule in the Tofino CMP and download it to the Tofino Security Appliance.

### Testing the Rule

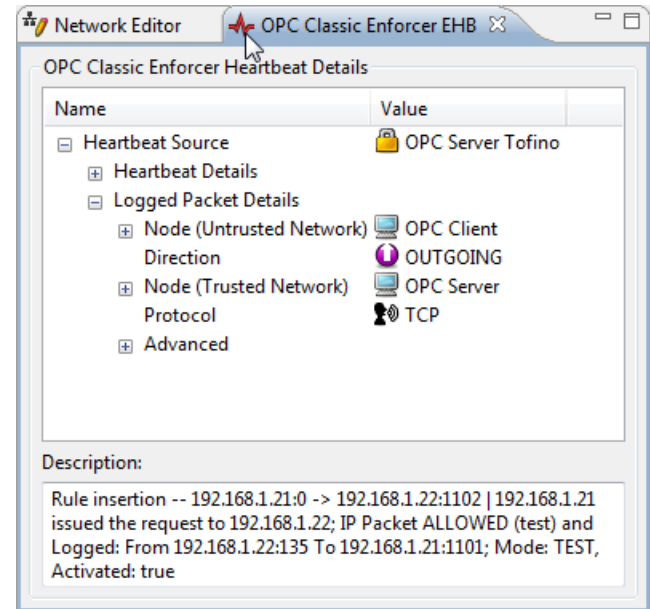
Tofino's unique 'Test' mode allows all network traffic to pass through the security appliance, but generates alarm messages for any traffic that would have been blocked if the device was operational. This permits testing firewall and OPC Enforcer rules with no risk of accidentally blocking traffic that must be allowed through for correct plant operation.

The Tofino's operating mode is set using the pull-down control at the bottom of its 'General/Communications' tab. The OPC client must be stopped and re-started after changing the Tofino's mode, so that the OPC Enforcer will see the data connection requests, parse out the allocated port numbers, and configure the Tofino Firewall to let the data connection pass through.

When a firewall rule is created by the OPC Enforcer to allow a data connection through the Tofino Security Appliance, an alarm message called an 'Exception Heartbeat' will be sent to the Tofino CMP to notify the user. These messages are displayed in the Event view at the bottom of the screen. Double-clicking on one of these heartbeat messages will open up a detail view as shown in Figure 4.

By monitoring the exception events and editing the firewall and OPC Enforcer configuration, the user may ensure that all required system traffic can pass through the Tofino SA without

generating alarms. After testing is complete, the Tofino SA may be deployed in Operational mode to enforce the rules that have been configured.



**Figure 4: Tofino OPC Enforcer Exception Heartbeat**

### OPC Enforcer Options

Three options are available to control how the OPC Enforcer manages each OPC connection.

'Sanity Check' causes the OPC Enforcer to check the data connection requests and responses for compliance with the DCE/RPC protocol specification, and block any that are non-compliant. This option may need to be turned off for some OPC clients and/or servers.

'Fragment Check' causes the OPC Enforcer to block fragmented DCE/RPC data connection requests. Similar to Sanity Check, this option may need to be turned off for some OPC clients.

The 'Connection T/O' sets a maximum time limit between the data connection request and the beginning of the actual data connection. This limit ensures that the 'hole' created in the Tofino Firewall by the OPC Enforcer will eventually close up if for some reason the OPC client never creates the data connection. The default time limit is 5 seconds, but some OPC clients may

need this to be increased. Testing with Matrikon's OPC Explorer indicates that a timeout setting of 10 seconds is optimal for this client, as shown in Figure 5.

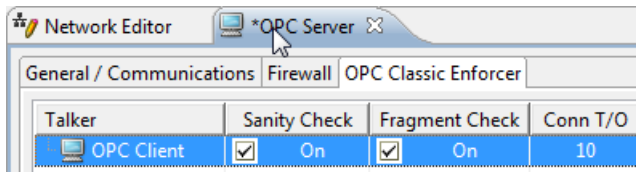


Figure 5: OPC Enforcer Options

## Connecting by Computer Name vs IP Address

If the OPC client references the OPC server by IP address, then only the 'OPC Classic – TCP' firewall rule is required. If OPC clients are configured to reference the name of the OPC server rather than its IP address, additional firewall rules may need to be configured in the Tofino Security Appliance to allow the name resolution traffic through the firewall.

In our example system, talker rules must be configured on the OPC Server firewall tab to allow NetBIOS Name Service and NetBIOS Datagram Service traffic between the OPC Client and OPC Server; as shown in Figure 6.

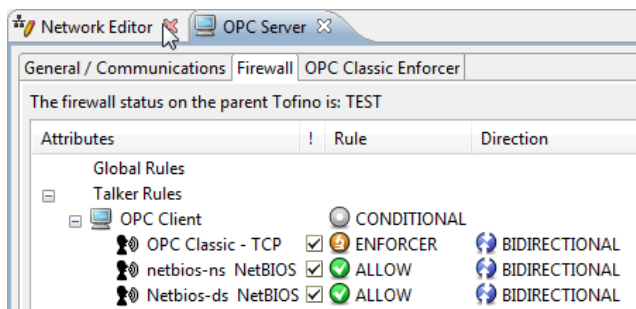


Figure 6 Talker Rules for NetBIOS Protocols

In a peer-to-peer networking configuration, OPC clients and servers must also be able to send and receive broadcast NetBIOS traffic to locate each other. In a Domain-based network, these machines must be able to send and receive NetBIOS traffic to and from the domain controller. Additional broadcast, talker and/or global rules may be required depending on the design of the network and the specific communication protocols that are used.

Broadcast rules for the peer-to-peer case are shown in Figure 7. The broadcast rules are configured on the Tofino's firewall tab, rather than on the OPC Server, in the Tofino CMP Network Editor.

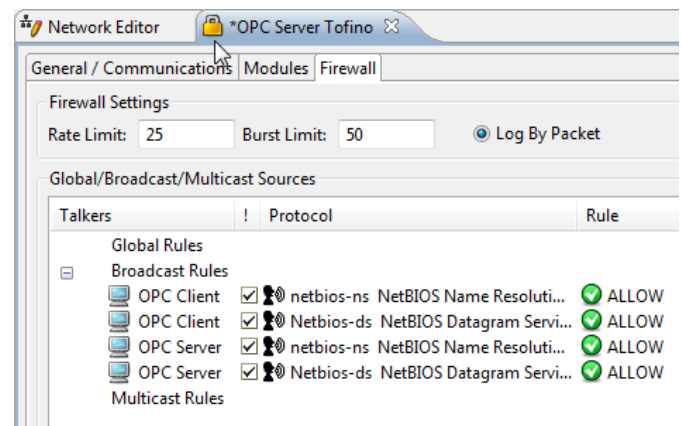


Figure 7: Broadcast Rules for Peer-to-Peer NetBIOS

## Summary

The Tofino OPC Classic Enforcer provides effective firewall protection for OPC clients and servers that use the ubiquitous OPC Classic communications services. The OPC Enforcer is simple to configure, and Tofino's Test mode provides the opportunity to test the configuration before deployment.



### BYRES SECURITY INC.

TELEPHONE: 1 250 390 1333  
TOLL FREE: 1 877 297 3799 (N. America)  
EMAIL: sales@tofinosecurity.com

# TOFINO®