DRAGOS AND WATERFALL SECURITY

Validated Architecture Improves ICS Cybersecurity

OVERVIEW

Waterfall Security Solutions is the OT security company, keeping operations networks safe from cyber intruders. Waterfall's Unidirectional Security Gateways provide physical protection for OT networks at OT network perimeters. The gateways enable seamless IT / OT integration, providing safe, enterprise-wide visibility into OT networks, with disciplined control.

The Dragos Industrial Cybersecurity Platform provides continuous passive monitoring which identifies and visualizes assets, detects threats through intelligence-driven analytics, and provides a workbench with playbooks to respond to attacks with speed and confidence.

By ensuring these technologies work together, organizations can leverage the Dragos Platform inside networks protected by Unidirectional Security Gateways, thereby enabling more secure and continuous monitoring of critical assets.

Both the Dragos platform and Waterfall WF-500 platform have been tested and validated for compatibility. This document outlines the steps needed to install and configure the Dragos Midpoint Sensor and a Waterfall Unidirectional Gateway using the span function to provide continuous monitoring of OT networks, without compromising the integrity of those networks.

GENERAL INSTALLATION AND CONFIGURATION

The Waterfall Unidirectional Gateway hardware and software components are installed per the Waterfall WF-500 User Guide, which is available to credentialed Waterfall customers. The WF-500 is mounted in a rack, powered and cabled per the User Guide, and the latest version of Waterfall Unidirectional Gateway software is installed on the gateway's TX and RX Hosts.

A Waterfall license for Ethernet Spoofing is entered into the configuration, and the heartbeat channel between the Waterfall TX and RX Modules is verified. Finally, IP addresses are configured on the TX and RX hosts, and connectivity verified from TX host to the source SPAN/mirror port and from RX to the Dragos Sensor.

DRAGOS TEST SETUP

The recommended configuration consists of the Dragos Sensor connected to the Waterfall WF-500 Unidirectional Security Gateway RX Host. From there, the standard configuration is followed. See fig. 1 below.

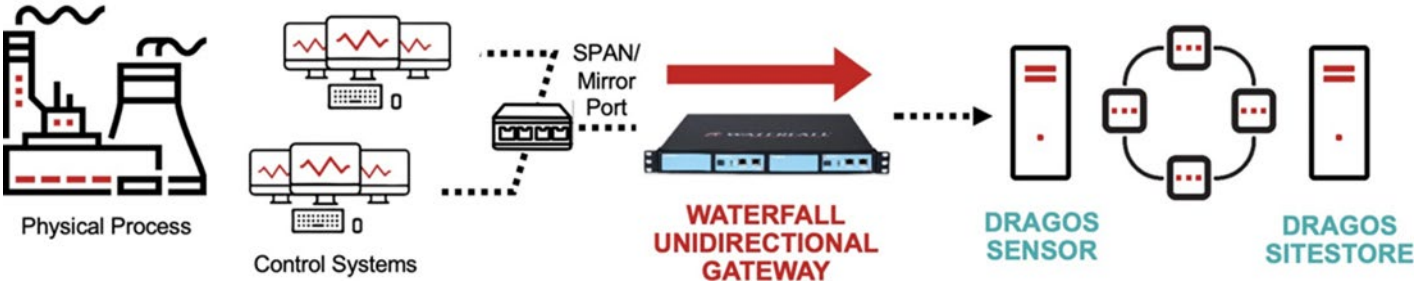

FIG. 1 – RECOMMENDED CONFIGURATION

This architecture permits sensor data to flow from the protected OT network to the Dragos Platform without introducing any potentially harmful upstream connections.

WATERFALL SECURITY RX CONFIGURATION

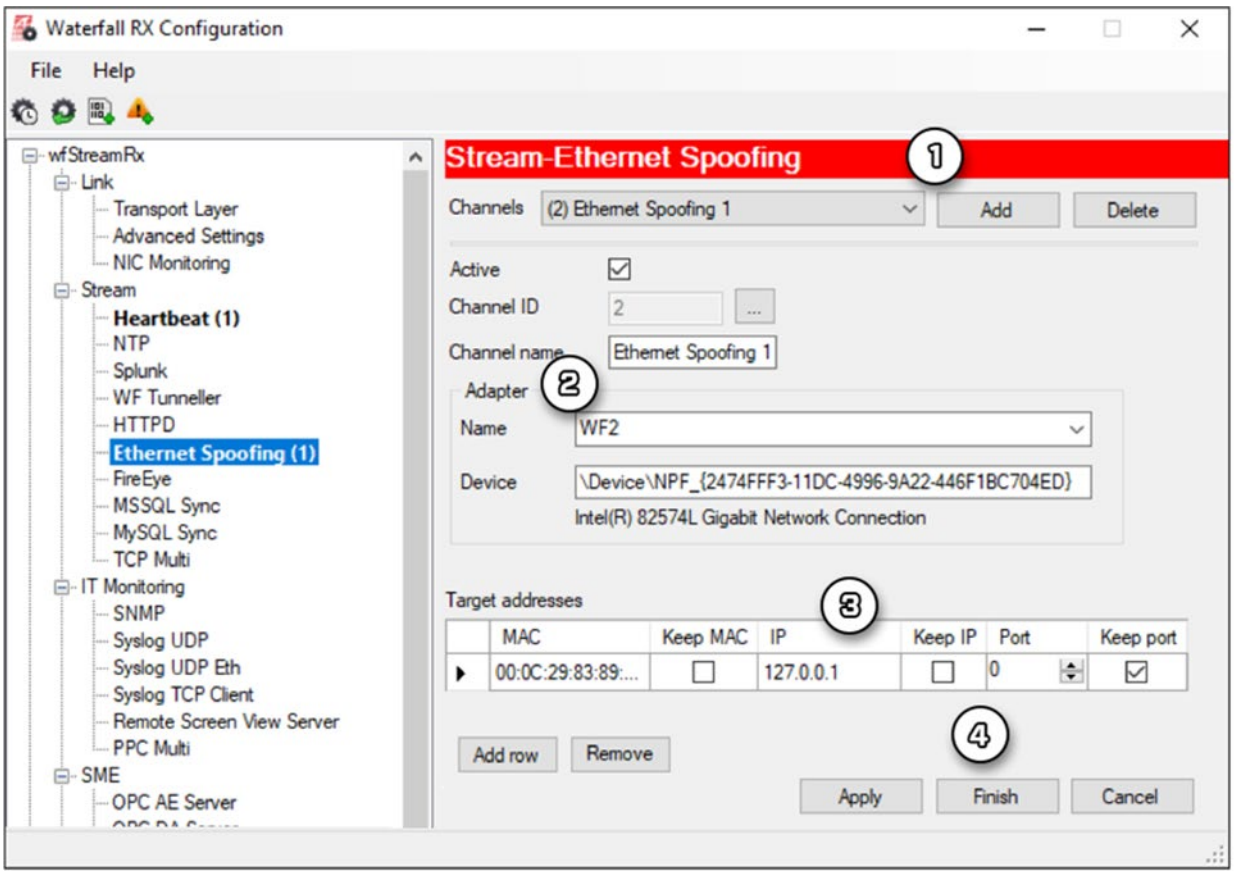

FIG. 2 – RX CONFIGURATION

TO CONFIGURE THE RX CONNECTOR SOFTWARE, CARRY OUT THE FOLLOWING STEPS:

1. Add the Ethernet Spoofing channel.
2. Choose the NIC that the SPAN port will be sent in the Adapter Name drop down. The device will automatically populate.
3. Enter the Dragos Sensor MAC address in Target Addresses and select Keep Port.
4. Press Finish to save the configuration and exit.

WATERFALL SECURITY TX CONFIGURATION

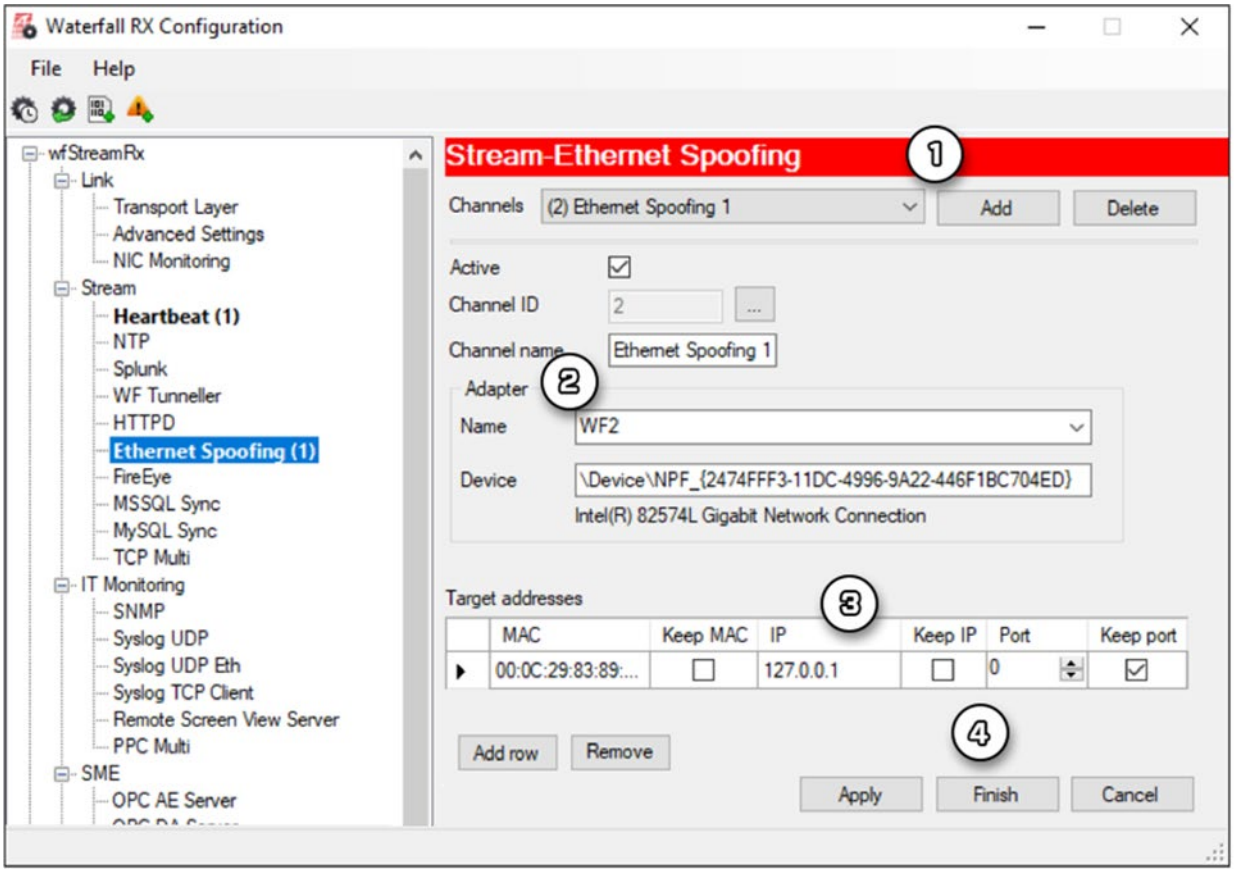

FIG. 3 – TX CONFIGURATION

TO CONFIGURE THE TX CONNECTOR SOFTWARE, CARRY OUT THE FOLLOWING STEPS:

1. Add the Ethernet Spoofing channel.
2. Choose the NIC that the SPAN port is connected to in the Adapter Name drop down. The device will automatically populate.
3. Delete the contents of Filter Expression. The goal is to replicate the SPAN port traffic in its entirety.
4. Press Finish to save the configuration and exit.

VERIFICATION

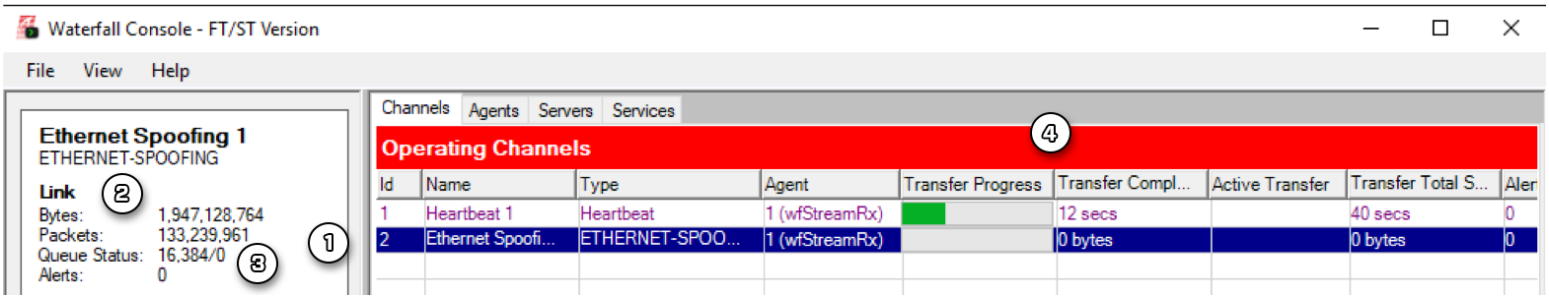

FIG. 4 – WATERFALL SECURITY CONSOLE

TO VERIFY THE PROCESS, OPEN THE WATERFALL SECURITY SOLUTIONS CONSOLE ON THE RX HOST AND:

1. Select the previously configured Ethernet Spoofing channel.
2. On the left side under Link, Bytes and Packets should be incrementing.
3. Queue Status should be 0/0 if there is a connection to the Dragos Sensor.
4. Transfer Progress, Transfer Completed, Active Transfer, and Transfer Total Size are not applicable to Ethernet Spoofing channel because Ethernet Spoofing is not a finite transfer.

For more information, please visit www.dragos.com or contact us at info@dragos.com