FiberPatrol® FP1150 Cybersecurity Features

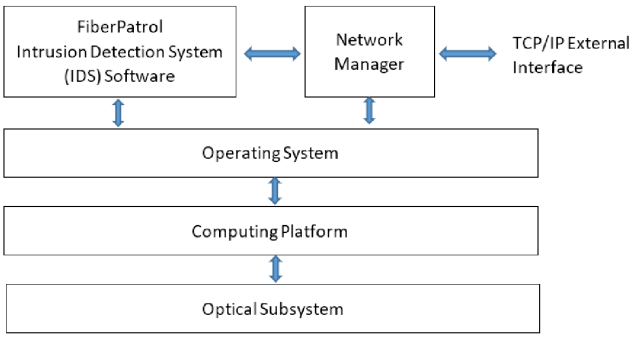
This application note provides information on cybersecurity features for the FiberPatrol® FP1150 system when used in conjunction with the Senstar's Network Manager software.

Senstar's FiberPatrol FP1150 is a fiber-optic distributed acoustic sensor that supports fence-mounted, wall-top, and buried installations for perimeter intrusion detection as well as third-party interference detection (TPI) for pipelines and buried conduits.

FIBERPATROL FP1150 ARCHITECTURE

The general architecture of the FP1150, as illustrated in Figure 1, consists of the following elements:

- **Optical subsystem** – Generates ultra-stable pulses of laser light for transmission into the field fibers and processes the reflected light that is received
- **Computing platform** – Intel®-based CPU
- **Operating system** – Windows® 10 Pro, 64-bit
- **Intrusion Detection System (IDS) Software** – Senstar-developed software that implements the signal processing algorithms, the detection algorithms, and a graphical user interface (GUI) for system setup and configuration. The IDS software uses third-party libraries from National Instruments and the Windows® .NET framework. The IDS software communicates alarm and status information to the Network Manager software over TCP/IP using one TCP/IP port.
- **Network Manager** – Senstar-developed software that interfaces between the IDS software and external systems (security management system (SMS), video management system (VMS), PSIM, etc.). Network Manager receives alarm and status information from the IDS software via TCP/IP and then forwards it to external systems over TCP/IP. Note that Network Manager can run on a separate server if so desired – in this bulletin it will be assumed that Network Manager is running on the FIberPatrol FP1150 sensor unit.



FiberPatrol FP1150 Architecture

FIBERPATROL FP1150 CYBERSECURITY PRECAUTIONS

The following general cybersecurity mitigations are implemented on the FP1150 Sensor Unit:

- All unnecessary Windows® applications are removed.
- All unnecessary Windows® background services are disabled.
- Firewall software is enabled.
- Anti-malware software is enabled.
- A full anti-malware scan is performed before shipment.
- Windows® security updates are applied.

NETWORK MANAGER CYBERSECURITY FEATURES

The Network Manager software provides an interface to external systems (SMS/VMS/PSIM). In consideration of this function, it includes numerous features that minimize the "attack surface" to potential cyber attacks:

- Network Manager runs as a Windows® service (instead of running under a standard user account, it runs under a Windows® service account which has a reduced set of system privileges). This limits the access that a piece of malware will have to the rest of the system in the unlikely event that malware manages to penetrate the system.
- Network Manager uses only one TCP/IP port to provide alarm reporting for the FiberPatrol systems. Additional ports may be required if other Senstar sensors, such as microwave sensors or wireless sensors, are being monitored by the onboard Network Manager.
- As of version 2.39 (released August 2020), Network Manager implements Transport Layer Security (TLS) 1.2 on its external connections. This provides encryption of the data exchanged between Network Manager and the remote system and forces both systems to provide authentication certificates before any data is exchanged.
- Network Manager implements an Allow List whereby Network Manager will only accept a TCP/IP connection from a system for which the IP addresse has been configured in the Network Manager Allow List. This provides a simple authentication process for exchanging data with external systems that do not implement TLS 1.2

Version: R1 09/20