Application Note

FIBER PROTECTION

FIBER OPTIC LINK CYBER SECURITY SOLUTION

OFFERING A UNIQUE SOLUTION TO THE NERC CIP REQUIREMENTS

GENERAL

Mission critical communication infrastructure is based on wired or wireless links between sites. Modern wired links between those sites are commonly based on fiber optics. These lines are installed in public and insecure environments and are exposed to security threats and maintenance-related hazards.

The NERC CIP requirements for protection of the electronic and physical assets of cyber threats define a set of measures to protect those links.

REQUIREMENTS

A fiber protection cyber security solution must provide a means to:

- Assure that the transmitted data cannot be modified or tapped by any active or passive attack tools
- Generate an alarm on any attempt to cut, bend, and/or tap the fiber and allow automatic actions to shut down the breached link
- Provide a backup fiber link for any failure or security breach in order to assure continuous data flow
- Assure 100% detection accuracy of threats and hacking attempts and nearly 0% false alarms

FIBER PROTECTION KIT

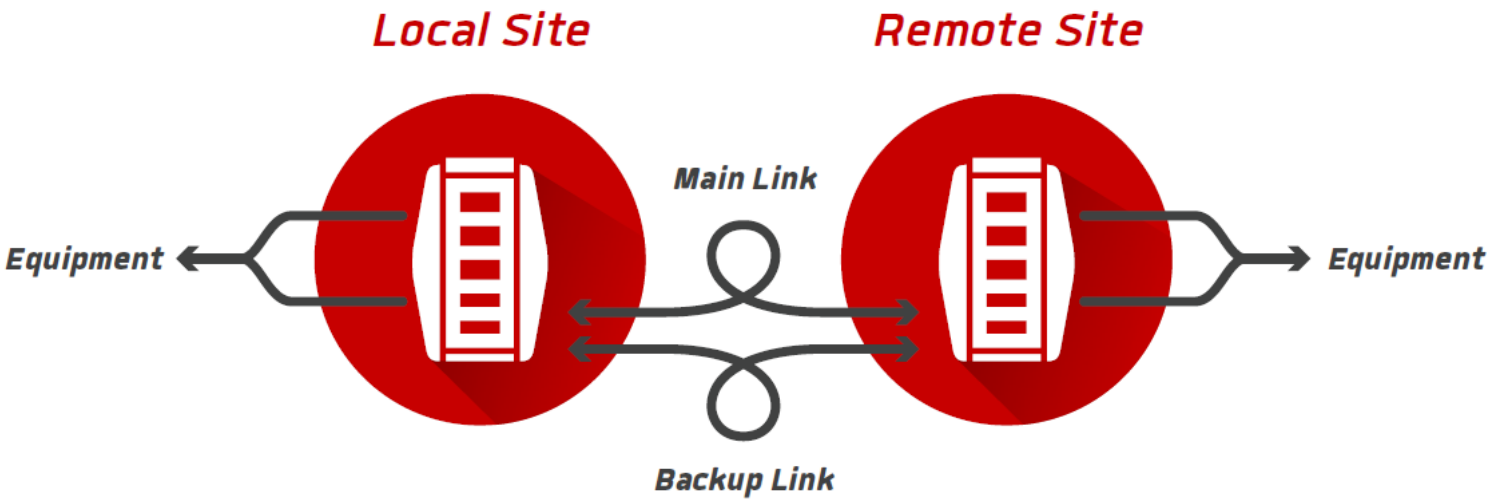
Senstar's fiber protection cyber security solution is delivered as a simple to install kit which includes:

- Rugged hardware, designed to withstand tough environmental conditions
- Two Tungsten Cyber Security Ethernet Switches
- Four OTDR SFP modules (and a fiber calibration kit for 4 fibers)
- Two DIN Rail AC/DC power supplies

THE SOLUTION

Senstar's fiber protection cyber security solution is based on two Tungsten Cyber Security Ethernet Switches, connected by two fiber optical links, offering the following:

- Unique OTDR modules that continually monitor the link health, reflections, power levels and length, and report on any change
- Algorithm to increase detection capabilities while maintaining 100% accuracy and nearly 0% false alarms
- User configurable automatic link shutdown upon security breach detection and configurable link redundancy parameters



The Senstar fiber protection cyber security solution offers:

- Link redundancy which allows user configurable parameters for automatic switchover functionality, user selectable automatic revert functionality and configurable thresholds and timing
- Pairing mechanism of the link components for simple installation and usage by minimizing the required setup configuration
- Monitoring and control functionality based on both the CLI and Web user interface of Tungsten and offering a simple view of the entire link protection status and providing a simple configuration tool
- Optional cyber security features based on the Tungsten Cyber Security engine which add additional security layers including network connections mapping, session and data flow discovery and anomaly discovery on both the equipment and links ports

Version: 1.32 / 092014