Tungsten™

Next-Generation Cyber Security Ethernet Switches

Features & Benefits

- Multi-layer security enforcement at the edge of network
- Detection and identification of every element and endpoint in the network
- Real-time alerts and the ability to block any attempt to connect an unauthorized device to the network
- 10/100/1000 copper Ethernet ports and fiber (SFP) slots for a wide range of installation requirements
- High PoE power (240W) including standard (60W) support
- Port mapping and support for NAT and DHCP servers

THE CASE FOR CYBER SECURITY ETHERNET SWITCHES

PROBLEM

Today, more and more physical security systems are connected to IP communication networks. This connection leaves the physical security systems vulnerable to cyber-attacks, threatens national security and impacts public safety.

Rapidly increasing attacks on physical security systems and SCADA networks deployed in critical infrastructure facilities make the need for a comprehensive solution essential - a solution that will cover a broad range of physical and logical threats.

There are many new hazards resulting from institutional use of a growing number of physical security elements. Surveillance cameras, access control systems, sensors and controllers are all connected using TCP/IP and networking technology and rely on unsecure communication networks that are laid across the site and in the field. The use of these unsecure networks exposes the site to combined cyber and physical attacks:

- Video streams from surveillance cameras can be replaced or manipulated
- Access control systems can be hacked to open gates and doors
- Perimeter security sensors and controllers can be disabled or blinded
- Industrial controllers and power distribution systems can be taken over and damaged

SOLUTION

Senstar's Tungsten – Cyber Security Ethernet Switch – was specifically designed to cyber-secure physical security networks, SCADA based systems and safe-city applications.

Tungsten provides ironclad security with full control and customizable networking capabilities. Cutting-edge hardware, coupled with network intelligence and policy enforcement software engines, offer an effective tool for securing sites and installations.

Tungsten can be used as the foundation for field and physical security communication networks and enhance infrastructure safety with the following key features:

- Rugged hardware, designed to withstand extreme environmental conditions
- Fiber-optic and RJ45 ports with high-power PoE capabilities, for simple installation
- Increased switch functionality, for fewer devices in the field and less points of possible failure, such as media converters, power supply and injectors, serial device servers, I/O controllers, etc.
- Continuous monitoring and analysis of data traffic of all elements and points in the network
- Cyber protection, not only for servers and network points, but also for all elements in the field

UNCOMPROMISED SECURITY

A multi-layer security enforcement tool located at the edge of the network, Tungsten allows for:

- Detection and identification of every element and endpoint in the network
- Real-time alerts and the ability to block any attempt to connect an unauthorized device to the network
- Inspection of the incoming and outgoing traffic, at port level, to make sure that only known, safe, and identified traffic, from authorized entities, is allowed
- Detection of Layer2 and Layer3 cyber-attacks: CAM overflow, ARP spoofing or poisoning, IP address spoofing, streaming and video hijacking, Spanning-Tree Protocol manipulation and denial of services
- Reporting and taking automatic action to restore the continuous operation of the network
- Protection of hardware and making switch policy enforcement tamperproof

FLEXIBILITY

A combination of 10/100/1000 copper Ethernet ports and fiber (SFP) slots covers a wide range of installation requirements. Tungsten supports:

- Classic star topologies as well as redundant ring topologies
- Dry contact input and output, for monitoring discreet sensors or environmental conditions and activating external devices such as audio alarms or warning lights
- Both DIN-rail and wall-mount installation options
- Dedicated external serial port (RS232, RS422, or RS485)* for connecting legacy devices

DURABILITY

A heavy-duty aluminum die-cast casing is used for optimal heat dissipation. Tungsten complies with industrial temperature ratings and a wide range of DC input voltage.

POWER OVER ETHERNET

Tungsten supports high PoE power (240W) including ultra-high standard (60W) support. It is fully compliant with IEEE 802.3af, IEEE 802.3 at 2-event and LLDP standards and supports forced-mode powering for compatibility with legacy devices. It saves on cost and size, thus avoiding cumbersome and bulky installations or costly external injectors. Configurable port priority and power budget capabilities ensure that end devices are powered based on correct and safe priority schemes.

IP ROUTING

Tungsten remotely connects to the local network by mapping internal IP addresses to TCP or UDP ports (port mapping) and by supporting NAT and DHCP to route the inbound traffic.

AUXILIARY SERIAL PORT

Tungsten supports RS232/422/485 serial communications and X.25 over TCP (XOT). An external plug supporting synchronous communications is optional.

MONITORING AND CONTROL

Tungsten provides real-time alerts on any exception from policy, configuration, traffic behavior or protocol and accurately locates a device's physical whereabouts and port information. In cases of protocol anomalies, Tungsten will also log the traffic for effective retrospective analysis.

HIGH AVAILABILITY

Tungsten allows for easy deployment, minimum down time and reduced cost with a built-in uOTDR (Micro Optical Time Domain Reflectometer) that constantly monitors fiber optic conditions. Industry-standard Ethernet Ring Protection Switching (ERPS) G.8032 / Y.1344 protocols* enable close to zero restoration times for both copper and fiber failures with minimal packet loss.

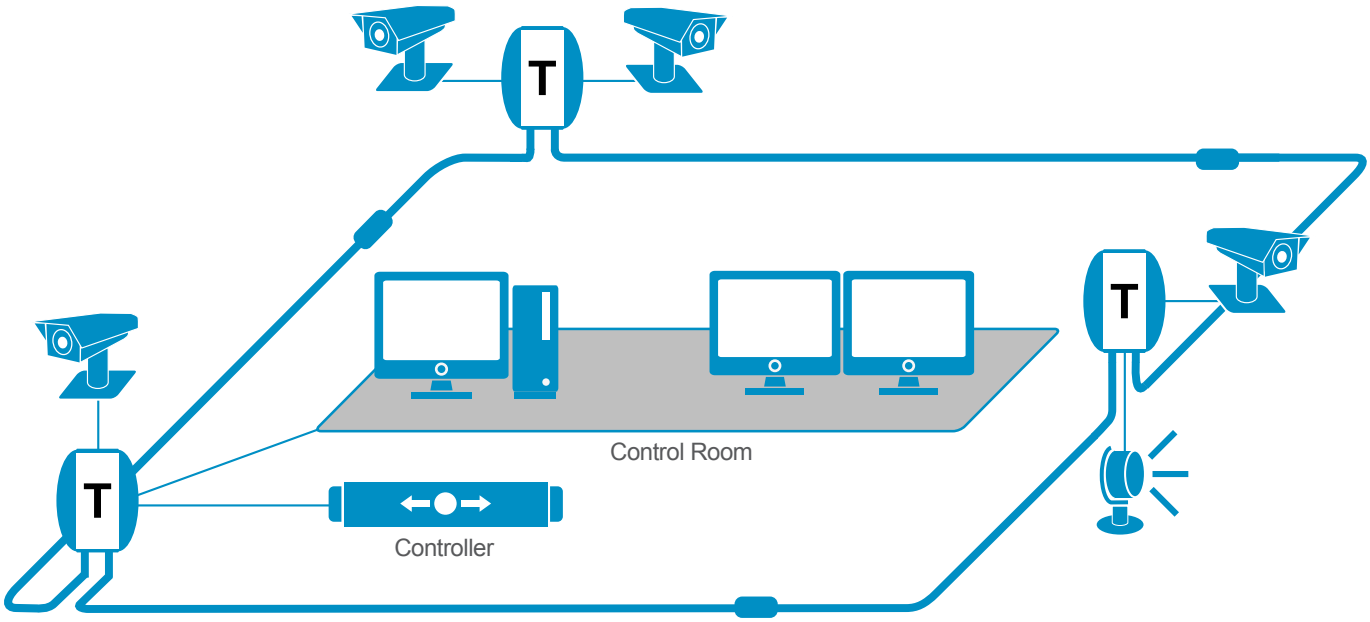
DHCP SERVER

Tungsten assigns IP addresses to local devices by configuring the embedded DHCP server and setting address lease rules.

X.25 OVER TCP

Many legacy devices (i.e. SCADA controllers) use the X.25 protocol running over an RS232 serial port. These devices can be directly connected to Tungsten's auxiliary serial port with data transported over the network using the standard XOT protocol.

TOTAL NETWORK COVERAGE



OUR CYBER SECURITY VISION

CONVERGENCE

Perhaps the first official acknowledgment of the unavoidable link between physical and cyber security came in the form of US President Barack Obama's Executive Order on Improving Critical Infrastructure Cyber Security and his Presidential Policy Directive on Critical Infrastructure Security and Resilience in 2013. Those directives state that the protection of critical infrastructure is dependent on strengthening cyber security measures and increasing collaboration with IT and physical security stakeholders. They empower US federal agencies to implement holistic security measures to protect critical infrastructure, buildings, assets, information and people.

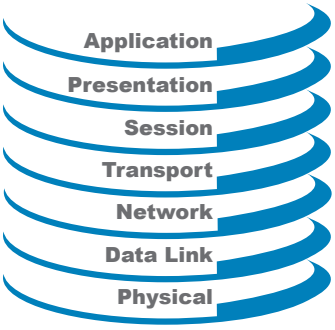
DEFENSE IN DEPTH

The Defense in Depth concept helps assure business continuity by defending a system against any kind of attack, using several different methods. Originally, the term Defense in Depth referred to a military strategy that aimed to delay, rather than prevent, the advance of an attacker by yielding space in order to buy time. In terms of network security, Defense in Depth tactics not only prevent attacks, but also buy an organization time with a forensic approach that detects and responds to threats, thereby reducing and mitigating the consequences of a breach.

MULTI-LAYER PROTECTION

Multi-Layer Protection describes the practice of combining multiple mitigating security controls to protect resources and data. A key Defense in Depth component, Multi-Layer Protection derives from a military strategy that involves multiple layers of defense that resist quick penetration by an attacker. The basic theory is that as an incursion progresses, resources are consumed and progress is slowed until it is halted and turned back. Within the Senstar context, Multi-Layer Protection is not only used as a delaying tactic but also as a first-layer threat detector and neutralizer.

ACTIVE AT EVERY LAYER



Monitoring application usage (Deep Packet Inspection)

Mapping TCP and UDP ports (protocols)

Mapping IP addresses and sessions

Monitoring link status, mapping MAC addresses, data flows and utilization

Monitoring the fibers, copper cables and PoE consumption

Power Supply

DC Feed	24V (+18Vdc to +36Vdc), 48 (+36Vdc to +72Vdc), 54Vdc, redundant power inputs
Power Consumption	Up to 255W depending on attached PoE devices
PoE	2 x 60W per port (Ultra PoE). 4 x 30W per port (IEEE 802.3af/IEEE 802.3at)

Environmental Info

Operating Temp	-40˚C to +75˚C (no fans)
Storage Temp	-40˚C to +85˚C
Relative Humidity	5 to 95% non-condensing
Dimensions	190mm x 140mm x 110mm
Enclosure	Aluminum die cast for improved heat dissipation; IP-40 protection
Environment	RoHS compliant

Interfaces

Copper Ethernet	8 x 10/100/1000Mbps auto-negotiate ports
Fiber Ethernet	4 x SFP ports including 100/1000Mbps support with Digital Diagnostic Monitoring
Console Port	RS232 port using Cisco CLI pin-out for local access
Discrete I/O	Discrete digital input and dry contact relay output
Configuration Freeze	Hidden reset button activates read-only mode and blocks any possibility of remote configuration change
External UART*	Dedicated RS232/422/485 interface for remotely accessing legacy equipment

Switch

Engine	Jumbo frame support; IPv4/IPv6 multicast; 4 Mb packet memories; 8192 MAC addresses
QoS	8 priorities + 8 CoS queues per port; Strict or Weighted Round Robin scheduling
VLAN	IEEE802.1Q VLAN with 8K MACs and 4K VLANs
STP	RSTP (Rapid Spanning-Tree) and MSTP (Multiple) support
Snooping	IGMPv2 and IGMPv3. MLDv1 and MLDv2
- Access Control*	IEEE 802.1X
- Security*	Radius and TACACS+

Management

GUI	HTTP/HTTPs server
SNMP	SNMPv1/v2/v3 agent
CLI	Telnet/SSHv2
Alerts	SNMP traps and Syslog messages
RMON	RMON Group 1, 2, 3, 9
Access List	Restricted access to management info
Back and Restore	Configuration download or upload
IP Configuration	Static or using DHCP

Compliance

IEEE 802.3	IEEE 802.3vb, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3af, IEEE 802.3at, IEEE 802.3ultra-at, EEE 802.3i, IEEE 802.3z
Regulation	CE, FCC, VCCI, UL
Isolation	2.1 KVDC, ESD: 15KV, Surge: 4KV, EFT: 4KV
Safety	EN60950-1:2001
EMC	EN61000-6-3:2007, EN55022, EN61000-6-2:2007, EN55024
Utility Substations	IEEE 1613, IEC 16850-3

*Planned features

Product Variations

Tungsten-F-POE-24-CS	Cyber security appliance embedded in a Gigabit Ethernet hardened switch, 4 SFP, 8 Copper, 240W PoE, 18-36Vdc input, 2-years warranty and software license
Tungsten-F-POE-48-CS	Cyber security appliance embedded in a Gigabit Ethernet hardened switch, 4 SFP, 8 Copper, 240W PoE, 36-72Vdc input. 2-years warranty and software license
Tungsten-F-POE-54-CS	Cyber security appliance embedded in a Gigabit Ethernet hardened switch, 4 SFP, 8 Copper, 240W PoE, 54Vdc input (if PoE needed), 18-72 Vdc input (if PoE not needed), 2-years warranty and software license
Tungsten-F-POE-24	Gigabit Ethernet hardened switch with optional cyber security appliance add-on, 4 SFP, 8 Copper, 240W PoE, 18-36Vdc input
Tungsten-F-POE-48	Gigabit Ethernet hardened switch with optional cyber security appliance add-on, 4 SFP, 8 Copper, 240W PoE, 36-72Vdc input
Tungsten-F-POE-54	Gigabit Ethernet hardened switch with optional cyber security appliance add-on, 4 SFP, 8 Copper, 240W PoE, 54Vdc input (if PoE needed), 18-72 Vdc input (if PoE not needed)
Tungsten-SFP	Optional SFP enabling Tungsten Fiber protection capability (1Gbps), 2-years warranty
Tungsten-Cyberupgrade	Software license for the addition of a cyber security appliance to a Tungsten switch

Version: 1.34 / 112014