End-to-end Infrastructure Protection for Institutions

In the last few years, the demand for classified information experienced by many government agencies has increased exponentially. At the same time agencies responsible for building and managing those classified networks are facing a sharp decrease in funding. The need for innovative technology solutions capable of protecting classified information while reducing the short-term operational costs and total cost of ownership is crucial in today's mission critical communications environment.

Government agencies currently protect classified information using several different compliant solutions. The most commonly deployed data protection systems are:

- Encryption Devices (bulk encryption and desktop encryption)
- Hardened Carrier Protection Distribution Systems (PDS)
- Alarmed Carrier Protection Distribution Systems (PDS)

Each classified data protection system has its pros and cons when comparing the level of protection, up-front costs and total cost of ownership. For example, encryption devices offer the highest level of data protection but are the most costly both in up-front costs and total cost of ownership due to the funding and staff required for COMSEC management of the encryption devices. Hardened Carrier PDS solutions were, until recently, the most commonly deployed type of PDS, in part because they have been included in construction guidelines for military installations and provide unlimited network bandwidth access that Encryption devices can’t match, but Hardened Carrier PDS solutions are the most susceptible to intrusion attacks and they require labor intensive post-deployment activities such as personal visual inspections every 24 hours for every system worldwide.

Alarmed Carrier Protective Distribution Systems offer a significant improvement over Hardened Carrier Protective Distribution Systems by offering 24/7/365 constant monitoring of the physical infrastructure, eliminating the need for 24 hour personal visual inspections. However, they have a reputation for receiving ‘false’ alarms leading many agencies to desensitize the alarm systems, potentially leaving the classified infrastructure vulnerable to intrusion attacks.

AT A GLANCE

Challenge
Secure physical fiber infrastructure from intrusions and minimize network down time caused by fiber damage.

Solution
CyberSecure IPS allows for alarmed cable alerting when cables are tampered with or physically damaged. The Optical cross-connect capability allows for quarantining of circuits and rerouting traffic.

Benefits
Comprehensive solutions provide multiple layers of protection for better security and defense.
- Tight integration allows for faster response to threats.
- Reporting capabilities allow incidents detail, response, and mitigation data to be stored and easily accessed.
- 3D MEMS Optical Circuit Switch allows traffic to be dynamically rerouted regardless of data rate, protocol or wavelength.
- Configurable software
The Technology Innovation Challenges:

1. Support the exponential growth of classified networks worldwide
2. Significantly reduce up-front costs
3. Reduce long-term maintenance and COMSEC management costs
4. Leverage the existing classified data protection infrastructures
5. Increase the effectiveness of existing classified data protection systems

CyberSecure IPS is designed and created by American Networking Solutions specifically to solve the technology innovation challenges facing today’s budget conscious government agencies. This is achieved by merging cost-effective, readily available, government approved COTS products with an innovative Information Assurance software management tool that reduces expenses, simplifies and centralizes IA management, eliminates COMSEC management, leverages the existing classified data protection infrastructures and enhances the protection of classified data networks worldwide. The CyberSecure Infrastructure Protection System (IPS) integrates hardware from Network Integrity Systems and CALIENT Technologies, with a government approved Infrastructure Management System (IMS) provided by ANS. CyberSecure Infrastructure Protection System (IPS) provides a wide-range of security solutions to enable institutions to protect both their physical infrastructure and communications networks from end-to-end. Using a combination of sophisticated software and hardware, customers can monitor for intrusions to their site and their network equipment.

The Challenge

Classified networks need to be physically protected from intrusion as well as provide quick response to physical damage that could disrupt service. Protection of the Secure Internet Protocol Router Network (SIPRNet) and Joint Worldwide Intelligence Communications System (JWICS) networks from physical intrusion requires fiber cables to be routed in concrete-encased conduit banks or to utilize encryptors for building-to-building connections and a hardened Protected Distribution System (PDS) for in-building Local Area Networks (LANs). This traditional approach is rife with complications: concrete-encased conduit and PDS are both expensive, and time consuming and disruptive to install. PDS is also very much aesthetically unappealing as it is usually installed in plain view along the ceiling (it also has the undesired effect of revealing critical and sensitive communications). Inline encryptors are expensive, require Communications security COMSEC material, and limit the bandwidth available on a circuit.

Remote shut off and redundancy switching in a traditional network relies on a Network Management System (NMS) communicating with individual network elements, using each element’s unique command set. Not only does this approach require the NMS to know the command language to communicate with the network element, it also depends on each element to respond to those commands. If an element is compromised and is unresponsive, physical intervention is required, wasting precious time.

As networks continue to grow in the face of increasing mobile and digital data traffic, the problem of how to secure the physical and network infrastructures is becoming a top priority for proactive service providers and institutions.
CyberSecure Solutions

CyberSecure IPS employs a comprehensive hardware and software solution to protect the physical network infrastructure as well as network traffic. Interceptors from Network Integrity turn existing fiber conduit into alarmed enclosures detecting any attempts to tamper with the fiber. The CALIENT S320 optical circuit switch allows the CyberSecure IMS to quarantine network elements to prevent them from sending sensitive information across compromised circuits, while allowing traffic to be remotely rerouted, ensuring users maintain network connectivity. Network analytic tools allow traffic to be recorded and analyzed, providing valuable information in response to cyber attacks. CyberSecure IPS, comprising hardware from Network Integrity Systems and CALIENT, addresses security requirements, such as those stated in NSTISSI 7003, with a comprehensive set of services and products designed to protect the physical infrastructure, as well as network applications. Addressing the needs of government and financial institutions, these end-to-end solutions secure the network, provide ongoing monitoring and protect devices from evolving threats.

How it works

The CyberSecure Infrastructure Protection System (IPS) is a five level network security solution (see Figure 2) developed by American Network Solutions (ANS). This solution integrates hardware from Network Integrity Systems and CALIENT Technologies with an Infrastructure Management System (IMS) software provided by ANS.

Level 1

Level one combines the Network Integrity Systems Interceptor and CyberSecure IPS IMS software to provide physical alarming for data network cables.

The Interceptor monitors a pair of unused fibers to protect all fibers traversing a given conduit. The alternative to this approach involves guards visually inspecting conduits (both inside and outside plant) every 24 hours, looking for damage and evidence of tampering. The Interceptor detects minute fluctuations caused when the fiber is moved or tampered with. This system effectively alarms the entire conduit system.

The IMS software provides a dashboard for users to visually monitor the health of the network and the history of events and alarms. When the IMS detects that a number of incidents have occurred that exceed the configured threshold, it generates an incident report detailing the type of event, approximate location of the event, and a map with instructions of what needs to be physically inspected. It also provides a form for the security staff to fill in with pictures of their inspection and recommended follow-up actions & mitigations.
Level 2

The level one system is able to monitor infrastructure and generate alarms and reports. With level two, the ability to remotely "pull the plug" on network elements when the IMS determines they may be vulnerable is incorporated. This is accomplished by integrating one or more CALIENT S320 Optical Circuit Switches into the physical network architecture.

When it is determined that a circuit may have been compromised, there are situations (for example, the circuit is being tapped) when it is necessary to prevent the elements on that circuit from transmitting. The traditional approach sends commands to each element telling it to cease transmission, but this requires the IMS to know the command set for each type of element. There is also a risk that the network elements themselves have been compromised, in which case, they may ignore the command and continue transmitting sensitive data across a compromised circuit. By interconnecting the network elements through the CALIENT S320, a network element that is controlled via a closed network, the IMS commands the S320 to physically break the connection between the concerned network elements and the compromised circuit.

The S320 makes use of an array of 3D MEMS micro-mirrors to angle optical signals from any of 320 input ports to any of 320 output ports, providing true any to any switching connectivity. Because it operates purely in the photonic domain (no OEO conversions) it is completely agnostic to bit rates and protocols, making it ideal for environments where an array of traffic types are present. In the Cybersecure IPS application the S320 can either switch optical traffic to alternate paths (level 3) or disable the traffic path completely (level 2).

Level 3

Level three utilizes the CALIENT S320 Optical Circuit Switch to reroute traffic that would otherwise be traversing a compromised circuit. Level three network architectures have redundant paths for high availability circuits and predetermined special users. For these cases, in the event of an alarm on a primary circuit, the level one and two services would be implemented, but the IMS would utilize the CALIENT S320 to dynamically route traffic away from the compromised circuit and on to the protection paths.

Levels 4 and 5

At levels four and five, the CyberSecure IPS surpasses simply securing the physical infrastructure to now providing cyber security at the packet level.

Level four incorporates optical tap couplers allowing for non-obtrusive optical multicasting that enables network monitoring.

Level five adds analytic elements that can be used to record traffic, extract Ethernet from SONET/SDH, and perform packet filtering. This solution level allows customers to monitor their networks, discovering specific signatures of an intrusion as well as specifying data that may have been compromised.
CyberSecure IPS applications

The primary applications for the CyberSecure solution provide a means to monitor the physical network without requiring a site visit and monitoring network traffic for security and quality of service and enabling traffic rerouting and the collection of network records.

Monitoring the physical infrastructure

- CyberSecure IMS coordinates monitoring of infrastructure, reporting, and switching.
- Physical infrastructure is alarmed by the Network Interceptor
- CALIENT S320 Optical Circuit Switch shuts down ports, as required and reroutes traffic
- Optical splitters passively copy traffic
- Optical tools record selected circuits

Figure 1 – CyberSecure IPS
In this application, the system is used by the physical security personnel to monitor fiber intrusions. When an alarm occurs, a report is generated detailing the location, and type of event. Two different responses are possible depending on predetermined user requirements:

1. The CALIENT S320 can be used to shut off the circuit in question.
2. After shutting off the circuit, the switch moves the traffic to a backup path, protecting the network traffic from intrusion while maintaining service.
3. If the circuit in question has not been configured with a backup path, and the incident does not warrant immediate termination of transmission, the S320, in conjunction with the optical splitters and network recorder, are utilized to monitor and record all traffic traversing the circuit in question. If it is later determined that there was an intrusion and a resulting data breech, security personnel have an exact copy of all traffic that was compromised, allowing a more precise response.

**Monitoring network traffic**

- Network analytic tools and optical splitters monitor for cyber security and quality assurance
- CALIENT S320 Optical Circuit Switch allows specific circuits to be routed to the proper analytic tools
- Network Interceptors provide monitoring for the physical fiber infrastructure
- CyberSecure IMS coordinates all of the above

In this application, the system monitors network traffic (for security or quality of service) and correlates traffic anomalies with physical incidents. The CALIENT S320 allows operators to select circuits to analyze, switching whole pipes of traffic through optical splitters and routing a record to the appropriate analytic tools. This allows operators to analyze traffic for attack signatures or degradation of service. When an event is found in the network traffic, operators are able to view historic reports from the Network Interceptors, gaining insight into physical events that may have resulted in the event in question.

**Benefits and Features**

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Monitoring</td>
<td>CyberSecure IMS provides physical alarming for fiber infrastructure by utilizing Network Interceptors to monitor the physical cable, alerting when the cable or incasing conduit have been touched.</td>
</tr>
<tr>
<td>Remote Equipment Shutoff</td>
<td>The CALIENT S320 provides the ability to remotely “pull the plug” on network elements when the IMS determines they may be vulnerable to a network intrusion.</td>
</tr>
<tr>
<td>Dynamic Redundancy</td>
<td>In the event of an alarm on a primary circuit, the level one and two services would be implemented, utilizing the S320 to dynamically route important traffic to protection paths, ensuring that high value users continue to have access to services.</td>
</tr>
<tr>
<td>Damage Assessment</td>
<td>Network analytic tools allow traffic to be recorded and inspected, giving network administrators the ability to perform detailed damage assessments in the event of a network compromise.</td>
</tr>
</tbody>
</table>
Solution Components

Software

CyberSecure Infrastructure Management System (IMS) is a software suite providing the management of essential operational components including equipment. The intuitively designed CyberSecure IMS dashboard allows users to visually monitor the health of the network and the history of events/alarms.

The IMS unified software suite enables monitoring of the physical infrastructure, and also delivers detailed event report to administrators and security personnel, as well as logs of the event and the response.

The IMS user interface dashboard provides users with a visual representation of the protected network along with views of the interceptors, showing alarm states for all circuits. This highly dynamic interface allows users to quickly see problem areas in real time and gives easy access to the reporting and mitigation tools, greatly simplifying alarm response and network restoration.

Hardware

The INTERCEPTOR from Network Integrity Solutions provides monitoring for up to four conduits per unit, allowing secure circuits to be monitored for physical intrusion, ensuring security without the need for cumbersome concrete encased conduit banks or expensive encrypers.

The CALIENT S320 Optical Circuit Switch enables the CyberSecure IMS to remotely shut down compromised circuits and reroute critical traffic, insuring that high value communications are not disrupted. This switching is performed at the physical level, transparent of the data and protocols on the fiber, and is not susceptible to exploitation by compromised circuits since the command and control is separated from the data plane.

Optical splitters, network analyzers and recorders allow analysis of traffic flowing over circuits that may potentially be compromised, allowing for precise damage assessment and mitigation.

About the CALIENT S320 Optical Circuit Switch

The S320 Optical Circuit Switch is a 320 port all-optical (OOO) switch that establishes, monitors and changes connections between single-mode optical fibers using Micro-Electro-Mechanical Systems (MEMS) optical switching.

The core of the S320 Photonic Switch is the MEMS Switch Module (MSM). High-quality mirrors and collimators and precise electrostatic control of the position of each mirror, enable typical switch times of 25 ms and optical loss that is typically less than 2.0 dB.
S320 hardware features:

- Small Size: 320 Ports (Tx/Rx pairs) in
- 7RU Chassis (LC Connectors)
- Low Power Operation: 45 Watts typical
- Ultra-low Latency: All-optical connectivity adds negligible latency.
- Scalable: Supports all data rates to 100 Gbps and beyond
- Reliable: Based on proven 3D MEMS design deployed in over 80,000 fiber terminations globally
- Simple to install, integrate and use: GUI-driven, EMS-ready, supports TL1, SNMP, CORBA, and OpenFlow
- Low loss: 2 dB typical insertion loss
- Built-in power monitoring: Every in/out fiber is monitored providing powerful network diagnostic capabilities

Summary — Infrastructure security for physical devices and network traffic

With the CyberSecure IPS approach it is possible for organizations to comprehensively and proactively protect the integrity of their physical networks as well as their network data. This solution provides both the software and hardware for customers to monitor their site and network equipment.

Next Steps

For more information on the CyberSecure IPS solution, please contact sales@calient.net.

About CALIENT

Headquartered in Santa Barbara, CA, CALIENT Technologies is the global leader in adaptive Optical Circuit Switching with systems that enable dynamic optical layer optimization in next generation data centers and software defined networks. CALIENT’s 3D MEMS switches have demonstrated years of reliability, with eight years of successful continuous operation. With more than 80,000 optical terminations shipped, CALIENT has one of the largest installed bases of Optical Circuit Switches worldwide. For more information, visit us at http://www.calient.net/, on Twitter and LinkedIn or contact us at marketing@calient.net.

About American Networking Solutions

American Networking Solutions (ANS) is a Veteran Owned Small Business (VOSB) based in the Washington, D.C. metropolitan area. We offer highly secure green technology solutions including the government approved CyberSecure IPS (Infrastructure Protection System).

For more information, visit http://www.americannetworkingsolutions.com.