



Enhancing “SIPRNet-to-Battalion” Deployments

This is a representative case study of a typical SIPRNet-to-Battalion deployment across a major U.S. Army base, and the cost and O&M impact that INTERCEPTOR can have on future deployments.

Overview

With the evolution and expansion of network-centric operations, Army commanders and their staffs now require constant situational awareness and the ability to access the collaborative environment made possible by SIPRNet to develop knowledge about the enemy, environment and potential contingencies that may arise during deployment. SIPRNet access enables units to conduct operational planning and allows intelligence personnel the means to leverage the larger Distributed Common Ground System (DCGS) community and to understand potential threats well in advance of deployment.

Under the Installation Infrastructure Improvement and Modernization Program (I3MP), the Army is upgrading the base-level infrastructure for both outside plant and in-building NIPR and SIPR networks. Due to the scope of the I3MP program and the SIPRNet-to-Battalion mandate, SIPRNet access is being expanded to a large number of buildings on each installation – requiring extensive deployment of in-line network encryptors and/or Protected Distribution Systems (PDS) to protect the national security information.

SIPRNet Protection Requirements

For years, the traditional Army approach for protecting the few SIPRNet networks on a base has been to use encryptors or concrete-encased duct banks for outside plant building-to-building connections, and a hardened PDS carrier (EMT, etc) for in-building Local Area Networks (LANs). With SIPRNet growing from just a few buildings with access to I3MP’s pervasive deployment of up to 150+ buildings across the base, the cost and complexity of these traditional protection methods has increased dramatically—with a direct impact on the total cost of ownership (TCO) of the network for the U.S. Army. Even with the cost and performance implications for a typical I3MP deployment (see chart on back), the Army had limited options to help enhance or accelerate SIPRNet deployments....until now.

New Optical Technology + New SIPRNet Protection Solution

Army installations and I3MP contractors are now able to leverage and install a different type of network security system that significantly reduces the cost and complexity of SIPRNet deployment. Used by other military, intelligence, and government agencies since 2003, the INTERCEPTOR Optical Network Security System was formerly approved for use by the U.S. Army in October 2008 for both outside plant building-to-building SIPRNet connections and in-building LANs.

INTERCEPTOR, categorized as an Hardened Protected Distribution System by NSA via NSTISSI 7003, works by placing a monitoring signal on a few fibers within the cables that will carry SIPRNet or JWICS—essentially turning those monitored fibers into sensors along the ENTIRE length of the cable, protecting ALL of the fibers in the cable (up to 144 fibers).

For SIPRNet-to-Battalion deployments and I3MP upgrades at Army installations, the newly-approved INTERCEPTOR solution offers EXTENSIVE savings for both Initial deployment and total cost of ownership – with no limitations on availability of bandwidth for the warfighter...ever!

Network Integrity
SYSTEMS

We Bring Security To Light™
877.NIS.4PDS

Once INTERCEPTOR is installed and monitoring a SIPRNet connection, if the cables are tampered with or someone attempts to access ANY of the fibers inside the SIPRNet cable, INTERCEPTOR immediately senses the activity and notifies the pre-defined IT and/or security personnel. As a physical layer device, INTERCEPTOR does not touch, process or route the network data, therefore it eliminates any potential bandwidth bottlenecks or performance limitation and allows Army units to immediately and fully utilize the full line-rate speed from their current or future network equipment...up to and beyond 10GBps. Interceptor is also a commercial off-the-shelf product that does not require COMSEC authorization, saving time and headaches in the procurement process and a significant reduction in lead-time from months to days or weeks. The technology installs easily and quickly with minimal disruption to base or building operations and personnel, enabling fast accreditation on either new or existing cables.

The cost for INTERCEPTOR to provide a single protected SIPRNet circuit to each building (same number of available circuits as in-line network encryptors) is about 50% less than encryption and 75% less than concrete encasement (detailed results below). However, INTERCEPTOR is not just protecting the single circuit (2 fibers) like an encryptor does, but ALL of the fibers inside of the cable...with unlimited bandwidth. So if INTERCEPTOR is protecting a 48-fiber cable providing SIPRNET access to a building, then there is a potential to have up to 24 protected circuits feeding that building. INTERCEPTOR offers unparalleled scalability with no additional cost investment. To provide the same level of scalability with encryptors would cost over \$240,000 compared to approximately \$20,000 for INTERCEPTOR, and would provide less than 4MB of bandwidth per connection.

Based on the representative deployment criteria (defined below), each Interceptor for SIPRNet deployment to 150 facilities would have cost approximately \$675,000, again, a 50% savings over encryption and a 75% savings over hardened PDS. However, depending on the density of the buildings, INTERCEPTOR can also be used where up to four separate building links are protected by a single INTERCEPTOR port – allowing a single INTERCEPTOR unit to protect up to 12-16 cables for high-density deployments. Using this type of a point-to-multipoint protection scheme with INTERCEPTOR would increase the cost savings dramatically.

| COMPARISON OF VARIOUS SECURITY SOLUTIONS | | | | |
|---|---|---|---|--|
| CONSIDERATIONS | ENCRYPTION STANDARD | ENCRYPTION HIGH-SPEED | CONCRETE ENCASEMENT | INTERCEPTOR ALARMED PDS |
| COST | | | | |
| NUMBER OF BUILDINGS | 150 | 150 | 150 | 150 |
| NUMBER OF UNITS PER BUILDING | 1 | 1 | | .25 |
| TOTAL NUMBER OF UNITS REQUIRED | 150 | 150 | | 38 |
| COST PER UNIT | \$10,000 | \$30,000 | | \$18,000 |
| AVERAGE DISTANCE FROM POP TO BUILDINGS (METERS) | | | 200 | |
| TOTAL LENGTH OF ENCASEMENT (METERS) | | | 30,000 | |
| TOTAL COST | \$1.5 MM | \$4.5 MM | \$3.0 MM | \$675,000 |
| OTHER CONSIDERATIONS | | | | |
| BANDWIDTH | < 1 MB | < 10 MB | UNLIMITED | UNLIMITED |
| DISRUPTION TO BASE | NONE | NONE | <ul style="list-style-type: none"> • CONSTRUCTION • ROAD CLOSURES • NOISE | NONE |
| STEPS TO ACCREDITATION | <ul style="list-style-type: none"> • COMSEC AUTHORIZATION • LEAD TIME | <ul style="list-style-type: none"> • COMSEC AUTHORIZATION • LEAD TIME | <ul style="list-style-type: none"> • MAJOR CONSTRUCTION • ONE YEAR OF AGGRESSIVE WORK | <ul style="list-style-type: none"> • COTS PRODUCT • 4-8 WEEKS DELIVERY • PLUG AND PLAY • SET-UP OF 38 UNITS IN 2 WEEKS |
| TIME TO ACCREDITATION | 6-12 MONTHS | 12-18 MONTHS | 12 MONTHS | 2-3 MONTHS |
| MAINTENANCE | PKI MANAGEMENT | PKI MANAGEMENT | DAILY VISUAL INSPECTIONS | NONE |

The Bottom Line...INTERCEPTOR Impact:

>50% Savings • 10Gb+ Throughput • Unlimited Scalability • Accreditation in <3 Months