GENERAL DYNAMICS
Mission Systems

TACLANE® Trusted Sensor (TTS) Software

Don't Just Protect Your Network – Know Your Network

NSA Approved

Use Classified Signatures on Unclassified Networks*

Augment commercial and public signatures based on latest intelligence

Intrusion Detection/Intrusion Prevention

Type 1 Protected Alert Reporting

Export and Fuse Data with SIEM for Local Action

Plaintext and Ciphertext Inspection

Sensor-Only Mode Configuration

Flow Analysis for Misuse and Exfiltration Capabilities

**Sensor-Only Mode*

Overview

Cyber attacks are advanced and more persistent than ever. Unprecedented growth in volume, sophistication and persistence of attacks on government and critical infrastructure networks are seen daily. Unclassified and government classified networks supporting critical missions are prime targets for cyber attacks. To withstand and operate in the presence of cyber attacks these networks need to be designed to be defensible at the boundary for confidentiality and infiltration. In these classified networks, system health and availability are crucial to support the needs of the mission. Network sensors, such as Intrusion Detection/ Protection Systems (IDS/IPS), provide critical system health to centralized Security Information and Event Management (SIEM) stations. Therefore the inclusion of sensing appliances into these sensitive networks has become essential to achieving the situational awareness of the network.

In response to these emerging and persistent threats, General Dynamics has developed TACLANE Trusted Sensor (TTS) software. The TTS software is a downloadable software option that can be used in several network topologies as an in-line HAIPE® sensor or as a separate secured network sensor, acting as an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS).

The in-line sensor capability supports sensitive networks by providing strong, Type-1 TACLANE encryption at the network boundaries enhanced with Deep Packet Inspection (DPI). Beyond a firewall's limited use of header filtering, DPI technology enables network elements to filter for malicious data within the traffic.

This in-depth inspection aids network administrators in understanding the overall system's health. DPI filtering affords administrators the ability to tune their network filtering based on either open standard or Government unique sets of finely detailed rule sets.

In the "Sensor Only Mode" secure inspection is provided like any IDS/ IPS with the added ability to use both open standard and Government classified rule sets and to issue Type 1 encrypted alerts. Since "Sensor Only Mode" can be used to monitor any network point, this will allow administrators to use classified rules on unclassified gateways to the Internet.

TTS is now available for TACLANE-FLEX (KG-175F), TACLANE-1G (KG-175G) and TACLANE-10G (KG-175X) network encryptors.

TACLANE Trusted Sensor (TTS) Software

IDS/IPS processing

- Analyze packets and react based on installed Open or Government unique Rules

REGEX formatted, Subset of SNORT 2.9 Syntax

- Rules sets are strongly protected inside the TACLANE
- Download unique PT and CT Rule files, at startup and dynamically

Alerts (RFC 5424 and RFC 5426 support)

- Syslog in user selectable reporting formats including {Syslog, Syslog-Common Event Format, and Unified-2 Format}

NetFlow reports (RFC 3954 support)

- Behavioral analysis information pertaining to the network of source destination packet and byte counts

Network Time Protocol (RFC 5905 support)

- Maintains time synchronized with an NTP server: used to timestamp Alerts and Netflow reports for forensic examination

Sensor Only Mode

- Supports specialized use case with DPI configuration: Sensor-Only IDS/IPS
- Secured alerts communicates with remote SIEM via HAIPE protocols
- Supports use of classified rules on unclassified networks

GEM™ Management

- Common management for encryption
- Rules Management, Deployment and Tasking, Alert Management, Analytics and Reporting

Virtual IDS/IPS

- Monitor remote network gateways from a single Cyber Aware TACLANE hub

Typical Use Cases

General Dynamics' TACLANE Trusted Sensor Software allows DPI inspection on both the Plaintext (PT) and Ciphertext (CT) interfaces as shown in Figure 1. Independent rule sets can be loaded into each DPI engine enabling administrators to target rules for each network. When threats are identified, several options for alert reporting are available including independent ports to independent SIEMs. This eliminates any 'tips and tells' to source of the cyber-attack so that the protected user network can begin understanding and reacting to the threat.

In addition, a new "Sensor Only Mode" (analogous to a tap in any network feed) provides secure inspection as shown in Figure 2. This mode acts like any commercial IDS/IPS with two exceptions: first, the TACLANE Trusted Sensor Software can inspect with both open rule sets and unique Government classified rule sets. Secondly, all alerts in this mode are Type-1 encrypted from the CT side of the TACLANE to the SIEM. This provides a secured 'T' connection to the alert management platforms. Since Sensor Only Mode can be used to monitor any network point, network administrator can now use classified rules on unclassified gateways to the internet.

For resource disadvantaged networks, such as devices on mobile platforms, the Trusted Sensor can be used to lower Size, Weight, and Power. As shown in Figure 3, mobile units with connections back to a tactical command post are securing their communications with a HAIPE tunnel. Only communications to and from the mobile platform can come from the tactical command center. Unlike architectures with separate encryption and IDS/IPS appliances, all traffic must come through the TACLANE Trusted Sensor Software before entering the command center. In this network architecture, the strong assurance mechanisms built into the Trusted Sensor enabled TACLANE in a command center can be relied on to virtualize the IDS/IPS on the mobile platform.

The TACLANE Trusted Sensor Software provides complete security by running seamlessly with our Suite A/B agility, HAIPE/IPMEIR agility and the optional Virtual LAN software feature. All packets are inspected - all packets are encrypted!

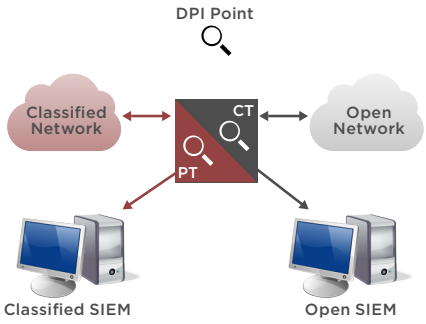

Figure 1: Content Aware TACLANE in a classically secured network

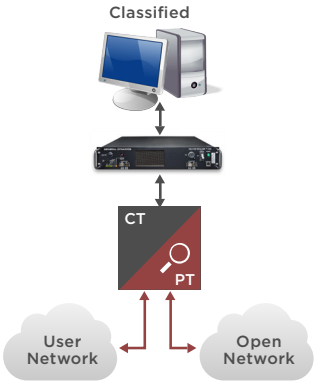

Figure 2: Content Aware TACLANE in Sensor Mode as an IDS or IPS

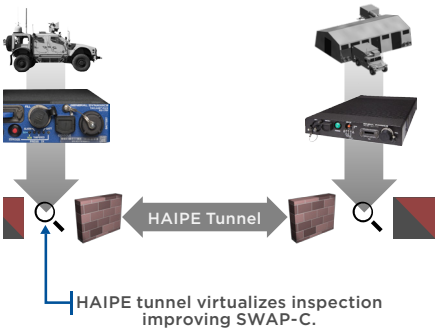

Figure 3: Content Aware TACLANE virtualizing inspection to resource disadvantaged/mobile endpoints

GENERAL DYNAMICS
Mission Systems

gdmissionsystems.com/cyber • infosec@gd-ms.com
Phone: 781-410-9400 • Toll-free: 888-Type1-4-U (888-897-3148) • Fax: 781-410-9863

D-TSSTAC-14-0418