



Tactical Cybersecurity Solutions

with Cisco Technology

Gaps in Cyber at the Network Edge

Cyber has emerged as a new warfighting domain and the Department of Defense (DoD) is now considering cyber at the same level as traditional land, sea and air warfighting domain.



Limited Visibility into Cyber Threats - Cybersecurity technologies of yesterday are too large and expensive to deploy, leaving tactical networks ill-equipped with the mobility and scalability needed in a cyber warfighting environment. Without the right technologies in place, soldiers' views into the threat landscape can be restricted and even at times inaccurate, as real-time situational awareness of cyber threats is impaired.



Shortage of Cybersecurity Skills in Tactical Settings - A response to cybersecurity threats on the battlefield must come in real-time, as the difference between waiting hours and days versus seconds and minutes to respond could have dire consequences. Yet, the shortage of cyber specialists readily deployed and available in tactical environments makes real-time response difficult if not impossible. And even for tactical operators in the field, maintaining multiple systems can be overwhelming.



More Vulnerability at the Edge - The electronic footprints of current tactical networks are often easy to discover, and the closeness of adversaries in battlefield environments makes it easier for communications to be intercepted, which is all the more heightened given how tactical networks are traditionally dispersed. Internal and external cyber threats at the edge of the network challenge DoD when it comes to rapid detection and response.

A One-Stop Shop for Tactical Cybersecurity Solutions

PacStar now provides a one-stop shop for tactical cybersecurity solutions utilizing Cisco components. Solutions include:

PacStar Solutions



PacStar 400-Series

Leading-edge rugged, small form factor communications systems



PacStar Secure Wireless Command Post (Wi-Fi)

Small modular communications package for classified networks in deployed, expeditionary and tactical environments



PacStar IQ-Core® Software

Intuitive Communications Management



Cisco Technologies

Cisco Stealthwatch

Cisco Adaptive Security Virtual Appliance (ASAv)

Cisco 5921 Embedded Services Router (ESR)



PacStar 400-Series Modular Communications Solutions with Cisco Technologies

PacStar 400-Series family of small communications modules is designed to maximum capabilities and configuration flexibility, with the smallest SWaP possible. Including routing, switching, advanced network services, cybersecurity and more – in lightweight packaging solutions designed with a wide variety of power options. PacStar 400-Series includes a comprehensive selection of Cisco technologies for use in tactical cybersecurity solutions including pre-deployed tactical cyber sensors or advanced threat hunting solutions:



PacStar 451/455 Modules are high performance virtualized appliances for hosting multiple software applications in a compact, quick setup, rugged form factor. Both are based on Intel Core i5/i7 and Xeon processors, including a variety of port configurations, and feature SATA SSD storage. PacStar 451 offers up to 4 TB of storage, and PacStar 455 offers up to 32 TB raid protected storage. Both support a vast array of cybersecurity solutions and virtualized network functions.



PacStar 441 Small Router Module provides high-performance routing, switching and advanced network services for critical voice, data and video connectivity in a compact, quick setup, ultra-compact form factor. PacStar 441 is based on Cisco ESR 5915 and provides up to 4 ports of PoE LAN access.



PacStar 442/443 Switch Modules provide high-density network access ports for critical voice, data and video connectivity in a compact, quick setup, ultra-compact form factor. PacStar 442 is based on Cisco ESS 2020 and provides 10 ports. PacStar 443 provides 24 ports.

Supported Cisco Software



Cisco Stealthwatch

Use Stealthwatch to outsmart emerging threats with industry-leading machine learning and behavioral modeling. Detect advanced threats and respond to them quickly. Detect malicious patterns in encrypted traffic. Quickly detect zero-day malware, insider threats like command-and-control communications and data exfiltration, advanced persistent threats, and other sophisticated attacks. Store telemetry data for long periods. Use advanced analytics to conduct better investigations.

Most comprehensive visibility for effective security outcomes



Advanced
Threat
Detection



Accelerated
Threat
Response



Simplified
Network
Segmentation

Using existing network infrastructure



Cisco ASA v

The Adaptive Security Virtual Appliance brings full ASA firewall and VPN capabilities to virtualized environments to help safeguard traffic. Provides security technologies popular in US DoD tactical networks, in a PacStar supported tactical package.

Cisco ESR 5921

The Cisco 5921 Embedded Services Router (ESR) is designed to operate on small platforms. It extends the use of Cisco IOS into extremely mobile and portable communications systems. It also provides highly secure data, voice, and video communications to stationary and mobile network nodes across wired and wireless links.

Cisco ESR 5921 provides the same functionality as the hardware-based ESR 5915 – ensuring full interoperability and feature compatibility with the hardware ESR – but in a virtualized form factor.

PacStar 400-Series Tactical Hardware + Packaging Solutions

PacStar 400-Series hardware includes components that provide cybersecurity solutions with a minimum of SWaP.

Features:

- ★ **Integrated power supplies** that run on tactical radio batteries, wide range DC input and worldwide AC input
- ★ **Snap-together design** enables quick expansion with other PacStar 400-series products & quick reconfiguration of modules & chassis
- ★ **Continuous runtime** with hot swappable batteries
- ★ **Regulated 12 V DC output** supports powering other accessories
- ★ **Extensively MIL-STD 810G/461F/704D environmentally tested** for temperature, shock, and vibration and more
- ★ **Typical module weight:** 2.5 lbs.
- ★ **Typical module dimensions:** 5.3" x 7.1" x 1.6"

Selected by:

The U.S. Marine Corps
Networking On-the-Move
(NOTM) Program

U.S. Army's Transportable
Tactical Communications
(T2C2) Program

Module options:

- PacStar 441 Small Router Module
- PacStar 442/443 Small/Large Switch Modules
- PacStar 451 Small Server Module
- PacStar 455 Hyper-Convergence Module
- PacStar 461 RoIP Module
- PacStar 462 Voice FXS Module

Use your choice of modules alone or in PacStar flexible packaging solutions:

- PacStar Pelican™ Case Systems
- PacStar Smart Chassis
- PacStar Desktop Chassis
- PacStar Mini-Transit Case
- Rack Mount Systems

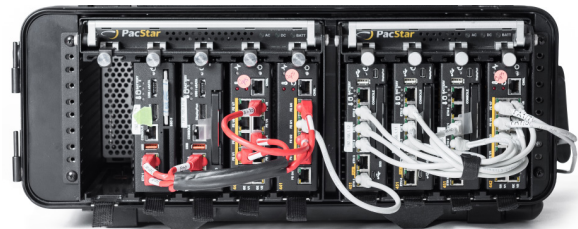


PacStar Secure Wireless Command Post (Wi-Fi)

PacStar Secure Wireless Command Post (Wi-Fi) is a small modular communications package that enables classified wireless and mobility for smartphones, tablets, and laptops in deployed, expeditionary and tactical environments. SWCP is an example solution providing extensive cybersecurity protection to tactical networks, utilizing Cisco technologies.

- ★ **Secure, converged, high-speed wireless infrastructure** capable of transmitting classified information, including multiple classified networks
- ★ **Complete, standalone system** including all cybersecurity components (PKI, VPN, Authentication Systems, etc.) necessary to deliver secure wireless access
- ★ **Expandable/modular system may be customized** with added networks or alternative component CSfC technologies
- ★ **Based on rugged, MIL-STD tested, PacStar 400-Series modules** and packages that optimize SWaP and maximize deployment flexibility

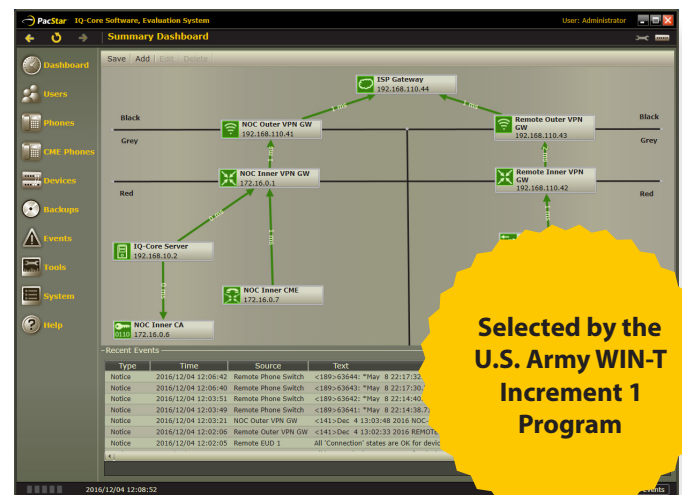
- ★ **Managed by PacStar IQ-Core Crypto Manager**, providing CSfC-specific capabilities including the management of PKI, digital certificates, and VPNs in accordance with NSA requirements



PacStar IQ-Core® Network Communications Manager

IQ-Core Network Communications Manager saves setup and configuration time, reduces errors and improves reliability of tactical networking solutions. It can overcome the added complexity and training burden imposed by network systems comprising multiple technologies. IQ-Core Software is optimized for Cisco technologies, with interoperability and extensive support for tactical and virtualized Cisco products.

- ★ **Intuitive User Interface**
Provides an intuitive user interface making communications set-up and operation quick, easy to learn and recall – improving mobility and reducing training time
- ★ **Reduces Configuration Errors**
Significantly reduces configuration errors, assisting organizations maintain uptime and compliance cybersecurity requirements
- ★ **Saves Time**
Automates complex, time consuming and error-prone tasks with powerful wizards with common user interfaces across hardware and software components
- ★ **Provides Situational Awareness**
Provides enhanced network situational awareness at the core and edge of the network with extensive real-time status, alerts, and auditing.
- ★ **Automates Cyber Defenses**
Improves cyber visibility, detects threats and automates responses – enabling units to embed cyber capabilities at the network edge
- ★ **Facilitates Remote Management**
Facilitates remote management with the ability to monitor, change device configurations and troubleshoot from anywhere in the world



- ★ **Simplifies Troubleshooting**
Simplifies troubleshooting through integrated tools for both entry-level and advanced network administrators, reducing reliance on contract Field Service Reps
- ★ **Streamlines Innovation**
Interoperates with a broad range of tactical and enterprise communications hardware and systems streamlining innovation and adoption of new COTS technologies at the edge
- ★ **Minimizes Complexity**
Enables deployment of advanced networking, unified communications, wireless technology, and cybersecurity while minimizing added operational complexity
- ★ **Field Proven**
Reduces acquisition risk because it's widely deployed, proven and certified for DoD use