RUCKUS ICX7400-SERVICE-MOD

IPsec VPN Encryption Service Module

BROCHURE

BENEFITS

HARDWARE-BASED ACCELERATION FOR IPSEC

- Programmable hardware technology to future-proof data protection, enabling more capabilities to be added as business needs evolve
- 10Gbps full duplex encryption/decryption
- Up to 100 tunnels per module

SECURITY AND DATA CONFIDENTIALITY

- IPsec extends crypto support to data traffic and introduces data confidentiality along with authentication
- Ideal for supporting IPsec for data traffic in federal, health care, financial and campus deployments

CSfC APPROVED

- Standards-based site-to-site IPsec VPN security to ensure end-to-end data integrity without the need for dedicated encryption appliances

SUPPORTED ALGORITHMS

SUPPORTED ALGORITHMS	ENCRYPTION	INTEGRITY	PRF	DH GROUP
IKEv2 Algorithms	AES-CBC-256	SHA-384	SHA-384	19
	AES-CBC-128	SHA-256	SHA-256	20
				14
Data path Algorithms (Suite B Crypto-graphics)	AES-GCM-256			
	AES-GCM-128			

ORDERING INFORMATION

PART NUMBER	DESCRIPTION
ICX7400-SERVICE-MOD	Service module for IPsec VPN encryption on ICX 7450

IPSEC VPN ENCRYPTION SERVICE MODULE

The ICX7400-SERVICE-MOD is an optional module on the Ruckus ICX 7450 switch that provides hardware-based acceleration for IPsec VPNs using Advanced Encryption Standards (AES). It leverages programmable hardware technology to future-proof data protection, enabling more capabilities to be added as business needs evolve.

Internet Protocol security (IPsec) is a suite of protocols that provide secure communication between devices at the network layer (Layer 3) across public and private networks. IPsec provides end-to-end security for data traffic by using encryption and authentication techniques that ensure data privacy. Encrypted packets are routed in the same way as ordinary IP packets.

The ICX7400-SERVICE-MOD module supports, with pre-shared authentication, the Suite-B-GCM-128 and Suite-B-GCM-256 user interface suites described in RFC 6379 and should interoperate with third-party equipment that supports Suite-B-GCM-128 and Suite-B-GCM-256. IPsec components include:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE)

IPsec introduces confidentiality and authentication services in the Ruckus Enterprise class switches. IPsec extends the crypto support to the data traffic and introduces data confidentiality along with the authentication.

The ICX 7450 switch with the integrated IPsec VPN service module consolidates network switching and encryption to provide unprecedented VPN deployment flexibility and cost savings. By initiating an IPsec tunnel from the switch for transporting selected traffic, organizations save the time and reduce the costs from having to install and manage encryption software on individual computers or deploy purpose-built encryption appliances.

The ICX 7450 also supports redundant service modules on a stack basis, insuring that, in the unlikely event of a service module failure, encryption could continue without interruption using another service module on the same switch or the same stack. Additional features include IPv4 and IPv6 support, PKI and X.509 based authentication, tunnel OSPF and BGP routing protocol packets, NAT Traversal, TCP MSS, VRF and jumbo frames are also supported with IPsec.

IPsec is only supported on the Ruckus ICX 7450 platform. To enable IPsec functionality, an ICX7400-SERVICE-MOD module must be installed on the device or stack. For further information about the installation procedure, refer to the hardware installation guide for Ruckus ICX 7450.

The ICX 7450 IPsec VPN Encryption Service Module is ideal for secure transport of sensitive data using standards-based and interoperable implementation providing industries such banking, law enforcement agencies, federal agencies, health care, and organizations requiring encryption for multi-site end-to-end secure data transfer.

WARRANTY

Ruckus ICX 7450 Switches and the IPsec VPN Encryption Services Module are covered by the Ruckus Assurance Limited Lifetime Warranty. For details, visit www.ruckuswireless.com/warranty.

RUCKUS ICX7400-SERVICE-MOD

IPsec VPN Encryption Service Module

BROCHURE

COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSFC) USE CASE

The time for Federal Agencies to ditch their outdated Type 1 encryptors has arrived. A simpler to manage and more cost-effective solution to securely transport classified and sensitive data is now available. The National Security Agency (NSA) Central Security Service's (CSS) Information Security Directorate (IAD) CSfC program has opened the door for Commercial off-the-shelf Systems (COTS) to provide the necessary cryptography to transport classified and sensitive US Government data which were historically only available from proprietary solutions.

INTERNET PROTOCOL SECURITY (IPsec)

IPsec is a suite of protocols that provide secure communication between devices at the network layer (Layer 3) across public and private networks.

IPsec provides end-to-end security for data traffic by using encryption and authentication techniques that ensure data privacy. IPsec enables authentication, confidentiality, data integrity and anti-replay protection between devices. There are many technical reasons that IPsec is the preferred security framework, but the main advantages of utilizing IPsec are:

- **Modularity**—It is not required to implement all of the protocols in the same way. Utilize the protocols in a way that best meets the applicable security requirements.
- **Interoperability**—IPsec is comprised of open standard protocols making it vendor agnostic, thereby deployable in a multivendor environment.
- **Flexibility**—IPsec encrypted packets are routed in the same way as ordinary IP packets and do not require re-architecting of the network infrastructure.

WHY CSfC?

From the NSA's Central Security Service:

"Commercial Solutions for Classified (CSfC) is a new way of delivering secure solutions leveraging industry innovation to deliver IA solutions quickly. It is founded on the principle that properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications."

This means that integrators can utilize CSfC comments to replace outdated Type 1 encryptors with a classified data designation up to Top Secret.

What is CSfC? In a nutshell a CSfC solution provides two layers of encrypted data protection. Two tunnels are created; an inner tunnel and an outer tunnel. The inner tunnel provides the protection of the client data, the outer tunnel provides the second layer of protection prior to the data being transmitted over a public or untrusted network.

The most preferred method of providing CSfC compliant data protection and the cornerstone of a CSfC Capabilities Package (CP) that employ Commercial National Security Algorithms (CNSA) is vendor (or manufacturer) diversity.

Per the NSA:

"Diversity is applied by using multiple layers, implemented with components that meet the CSfC vendor diversity requirements, which then reduce the likelihood that a single vulnerability can be exploited to reveal protected information."

This is not to say that a CSfC CP must be deployed as a multi-vendor layered solution. An update to the NSA's manufacturer diversity requirements states:

"The manufacturer diversity requirement for CSfC layered solutions has been modified to permit, subject to certain conditions, single-manufacturer implementations of both layers. The manufacturer must show sufficient independence in the code base and cryptographic implementations of the products used to implement each layer.

THE RUCKUS ICX 7450 IPSEC SERVICE MODULE

The Ruckus ICX 7450 is the industry's first stackable switching solution to leverage the advantages of site-to-site CSfC approved IPsec VPN security to ensure end-to-end data integrity without the need for dedicated encryption appliances. With up to 10 Gbps bi-directional data encryption capability the ICX 7450 IPsec Service Module can meet the most demanding encryption requirements.

System-level high-availability features, such as dual hot-swappable, load-sharing, and redundant power supplies, and hot-swappable fan trays offer another level of availability for the campus wiring closet, all in a 1 RU form factor.

BENEFITS

- Two layered solution interoperable with all other CSfC listed vendors
- Stackable switch form factor providing end user connectivity and encryptor in a single device
- Encryptor redundancy when deployed in a stacked configuration
- Supports multiple Communities of Interest utilizing Virtual Routing and Forwarding (VRF) technology for data and routing isolation
- Simplified deployment and operation

RUCKUS™ an ARRIS company

350 West Java Dr., Sunnyvale, CA 94089 USA

www.ruckusnetworks.com

18-10-A