XIPHRA

HIGH ASSURANCE IP NETWORK ENCRYPTORS

APPLICATIONS

- SITE-TO-SITE AND INTEGRATED REMOTE ACCESS VPNS
- MANAGED SECURITY SERVICE PROVISION
- END TO END COMMUNICATIONS PRIVACY
- DATA SEPARATION

ENCRYPTORS FOR CRITICAL NATIONAL INFRASTRUCTURE AND THE ENTERPRISE

A Tripwire survey of Black Hat USA 2015 attendees, where leading information security researchers take the stage to share their latest work, revealed that 64% of respondents believe their organisations are potential targets for nation-state cyberattacks.

There are numerous published examples of breaches that are related to using general purpose routing and operating systems as the point of delivering IP network privacy. Having some of the widest attack surfaces, these solutions often end up relying upon the point of vulnerability to provide the security solution, and this evidently does not always end well.

The Xiphra range of application specific, dedicated IPSec VPN gateways is unique in providing hardware accelerated performance along with fully centralised policy and key management.

Delivers the only solution in its class for modular and scalable data in motion privacy and boundary protection, specifically designed for both self-managed deployments and the largest scale managed security service providers.

KEY BENEFITS

Suite B cryptographic algorithms (AES-256, EC-DH, EC-DSA & SHA-256) implemented in the Xiphra range have been deployed to protect sensitive data at the highest level.

Wide range of next generation hardware based IP encryption fits your needs today, and scales to meet the evolution of security policy and performance requirements for tomorrow. Includes both site-to-site and personal remote access encryptors.

Xiphra Management System (XMS) provides **the ultimate in cryptographic key management security,** with the Ultra Safe Keyper*Plus*. Keyper is the only networked HSM with FIPS 140-2 Level 4 validated cryptographic module, which has maintained this unrivalled level of certification for 15 years. Please see XMS datasheet for more information.

SPECIFICATIONS	PERSONAL ENCRYPTOR	OFFICE ENCRYPTOR	SITE ENCRYPTOR	CORE ENCRYPTOR
Pro	20 Mbps / 1 Tunnel	100 Mbps / 10 Tunnels	100 Mbps / 100 Tunnels	1 Gbps / 250 Tunnels
Enterprise	100 Mbps / 1 Tunnel	250 Mbps / 10 Tunnels	250 Mbps / 100 Tunnels	2.5 Gbps / 500 Tunnels
Ultimate	1 Gbps / 1 Tunnel	1 Gbps / 10 Tunnels	1 Gbps / 100 Tunnels	8 Gbps / 1500 Tunnels
Form Factor	Portable	Desktop	1U Rack Mount	1U Rack Mount
Interfaces	10 / 100 / 1000 Mb Ethernet	10 / 100 / 1000 Mb Ethernet	Modular Ethernet / fibre	Modular Ethernet / fibre
High Availability*	-	-	Hot Standby	Hot Standby
QoS*	-	-	Yes	Yes
Power	External PSU, USB 3.0	External PSU, PoE	Internal PSU	Dual Internal PSU

BEYOND SEMICONDUCTOR

AEP

Ultra ELECTRONICS

XIPHRA

XIPHRA ENCRYPTORS

FEATURE	BENEFIT
Hardware accelerated tunnel handling	Rapid tunnel setup optimises gateway transparency and application performance during IPsec path (re-) establishment
Diffserv based QoS support*	Support traffic prioritisation requirements for optimal use of available bandwidth
Latency of less than 6μs	Transparent to end users with the most demanding applications
IPv6 support*	Seamless integration with more efficient IPv6 based networks
Low power, high throughput	Purpose built application specific appliance minimises power consumption and heat emissions while maximising throughput and flexibility
Outbound NAT traversal	Automated negotiation across often troublesome NAT boundaries increases usability of secured communications
High Availability*	Hot standby provides service continuity despite IPSec path failure for core network elements
Remote feature upgrades	Unlocks features to evolve service with future requirements and security policy
LED indicators	At a glance device and activity status

SECURITY

FEATURE	BENEFIT
Suite B cryptographic algorithms	Globally recognised, publicly available standard for cryptography designed to support inter-agency and international collaboration through crypto interoperability. Suite B has been deployed to protect sensitive government data at the highest level
X509v3 based device authentication	Bullet proof authentication for the largest scale deployments, that eliminates key distribution challenges
Encrypted storage of credentials and other sensitive data	Protects against decipherment of protected data including firmware, configuration, keys, user credentials
Boot time authentication option	Ideal for portable and mobile use cases
CRL based device 'kill'	Compromise control for devices whose trust level has changed which guarantees peace of mind
Tamper evident labels	On demand verification that the device has not been tampered with
Perfect forward secrecy	Any ephemeral session key is not compromised even if one of the endpoint keys is somehow revealed

* Future release

Features and/or roadmap may be subject to change without notice.

Ultra ELECTRONICS

making a difference

BEYOND SEMICONDUCTOR

Ultra Electronics
AEP
419 Bridport Rd,
Greenford,
Middlesex UB6 8UA
Main Switchboard: +44 (0)1628 642 600
Email: info@ultra-aep.com
www.ultra-aep.com
www.ultra-electronics.com

Beyond Semiconductor
Brnčičeva ulica 41G
SI-1231 Ljubljana-Črnuče
Slovenia
Phone: +386 5 90 90 100
Email: info@beyondsemi.com
www.beyondsemi.com