SecuriVPN® ISA

Quantum-secure encryption

High assurance

SecuriVPN ISA meets the highest demands on both security and assurance. It is analysed, designed and implemented so that it prevents intrusion, data leakage and manipulation of information worthy of protection. For the customer to facilitate, Advenica encloses distinct recommendations on how the product needs to be managed to maintain the high security level.

Advantages

- Dual algorithms (HW dependant)
- Simple key management based on symmetrical encryption
- Red/black separation in hardware
- High availability with multiple redundancy options
- Receive-only mode
- Support dynamic routing
- Emergency erase
- Supports various networks such as ad-hoc and fully-meshed
- Full traceability is provided through both local and central logging

Advenica's quantum-secure IP encryption system, SecuriVPN ISA, was originally developed for tactical and strategic defence use. The system can aid any organisation with the need to protect information up to classification level SECRET. It has been proven to provide versatile encrypted communications.

Tailored for long-term communication privacy

Long-term communication privacy is ensured by unique technology developed by Advenica. All IP communication, data transfer and key handling is protected by quantum-secure algorithms and protocols. The system renders vital network security functionalities such as authentication of information origin, integrity control, and anti-replay mechanism.

Simple future-proof key management, high-availability features and ability to communicate over both low and high quality transmission layers, provides ease of use as well as resilient communications. Features include:

- High-availability including failover and dual Central Administration System (CAS)
- Secure administration enabled by Three Domain Separation and dedicated administration gateway (AGW) with its own VPN tunnel
- Scalable from single point-to-point connection to secure networks with hundreds of devices
- Extensive key handling including designated key servers and remote key management and distribution

Three Domain Separation

To eliminate the risk of unauthorised disclosure of classified information by rouge administrative staff, Advenica has developed a technology to separate classified information and transport networks from device administration, called Three Domain Separation. The patented Three Domain Separation technology introduces a third domain, the administration domain, in addition to the traditional Red/Black domain separation. Thus, classified information from the protected (RED) domain cannot be accessed from the administration domain. The Three Domain Separation technology effectively reduces the insider threat within the organisation.

SecuriVPN® Technical data

Quantum-secure encryption.

VPN basics
- IPsec enhanced
- 512 unicast + 512 multicast tunnels
- NAT traversal
- Up to 150 Mbit linespeed
- 4000 keys

Modes of Operation
- Two-way tunnel
- One-way tunnel
- Network modes: fixed, mobile and deployable

Ports
- Optical 1000Base-SX (LC connectors) or Electrical 100Base-TX (RJ45)

Encryption Algorithms in hardware
- AES 256
- Custom algorithms

Device authentication
- X.509 certificates and CRLs
- Symmetric keys

Device management
- Front panel user interface
- Local configuration port
- Smart cards
- Secure in-band remote management, utilising Three Domain Separation
- Secure local or remote firmware upgrade

Key Management
- Session keys from Key Server System
- Authenticated Session key exchange
- Enhanced IKE using RSA-PSS signatures (2048-bit)
- Keys distributed on smart card or through Central Administration

Monitoring & Log handling
- Local interface for log output
- Remote management with event secure syslog
- SNMP remote monitoring and control

High Availability and QoS
- Up to 10 devices in parallel per site
- QoS, DiffServ
- Up to 336 hours key backup
- Failover installation

Security Features
- Hardware based random number generator
- Red/black separation in hardware
- Emergency erasure of keys
- Tamper evident chassis
- Active and passive tamper resistance
- POST (Power On Self Test)
- Replay protection
- Auto detection of local red/black circuit
- Separate administration domain

Regulatory Compliance
- CE
- Tempest EU/SWE

Power source (dual)
- 85-264 VAC (standard)
- 10-66 VDC (optional)
- Dual power supply optional
- Power consumption: 16W

Operating Temperature
-5 °C – +40 °C, 5 – 95% rel. H

Pollution degree
2

Max altitude
2000 masl

Physical Dimensions
Device Size
442 x 44 x 272 mm (19" rack device)
257 x 44 x 272 mm (portable device)
Device Weight
4-5,8 kg

Models
- ED100 19" rack device (height 1U)
- Front Connector Module (option)
- ED100P portable device

MTBF
>75 000 h

advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED