SecuriVPN ISA

VPN encryptor for SECRET level IP communication

SecuriVPN ISA is a state-of-the-art IP encryption solution designed to secure classified communications against unauthorised access and eavesdropping. With high assurance and robust security features, it ensures the confidentiality and authenticity of sensitive data transmitted over unsecure IP networks. SecuriVPN ISA is the trusted choice for protecting information up to classification level SECRET.

Tailored for long-term communication privacy

Advenica's SecuriVPN ISA ensures long-term communication privacy by safeguarding all data transfer and key handling with quantum-secure algorithms and protocols. The encryption system renders vital network security functionalities such as authentication of information origin, integrity control, and anti-replay mechanisms.

Designed for the most challenging cybersecurity environments, the SecuriVPN ISA system empowers defence forces, government agencies and critical infrastructure to take the next step in protecting highly sensitive or classified systems and information. The solution involves future proof key management, versatile functions with high availability and the ability to communicate regardless of signal quality, providing ease of use as well as resilient communications.

Main benefits

- Quantum secure symmetric encryption algorithms are used to protect classified information at highest assurance level.
- Implements robust key management to securely generate, distribute, and manage encryption keys.
- Advanced remote administration through Three Domain Separation guarantees separation between sensitive data traffic and system administration.
- Scalable system from single point-to-point connection to networks with hundreds of devices offering several modes of operation and network topologies.
- National approvals on SECRET level available in several European countries.

Proven in multiple defence and civilian applications

For more than 20 years Advenica has protected defence and civilian information with high assurance encryption systems. The collective knowledge used in the SecuriVPN ISA system guarantees organisational readyness for most challenging cybersecurity environments.

Military Command and Control

SecuriVPN ISA facilitates timely information sharing in military operations where effective command and control is essential for mission success. From intelligence gathering and coordinating troop movements to directing support and planning logistics, it enables quick and decisive decision making. The SecuriVPN ISA system is suitable for installations ranging from data centres to tracked vehicles and naval applications, supporting specific military functions like radio silence and high latency scenarios.

Defence cooperation

Collaboration among defence, contractors, government agencies and allied partners, are essential to develop and deliver advanced defence capabilities. Whether collaborating on joint research projects, co-developing defence systems, or sharing threat intelligence and providing situational awareness, National Security entities can rely on SecuriVPN ISA to protect vital information across distributed networks.

Government agencies and diplomatic networks

Government bodies, including Ministry of Foreign Affairs and embassies, require secure communication channels to connect and exchange sensitive diplomatic correspondence, classified documents, operational information and strategic intelligence. SecuriVPN ISA serves as a trusted solution for securing interinstitutional and international communications, ensuring that national security remain confidential and protected from espionage and cyber threats.

Critical infrastructure protection

Critical infrastructure, such as transportation, power grids and water supply, is a prime target for cyber threats and attacks. SecuriVPN ISA protects critical infrastructure networks by encrypting sensitive data in transit over IP-based communication channels. SecuriVPN ISA ensures the continuity of critical infrastructure systems, ensuring operational resilience against nation sponsored attacks.

Product security

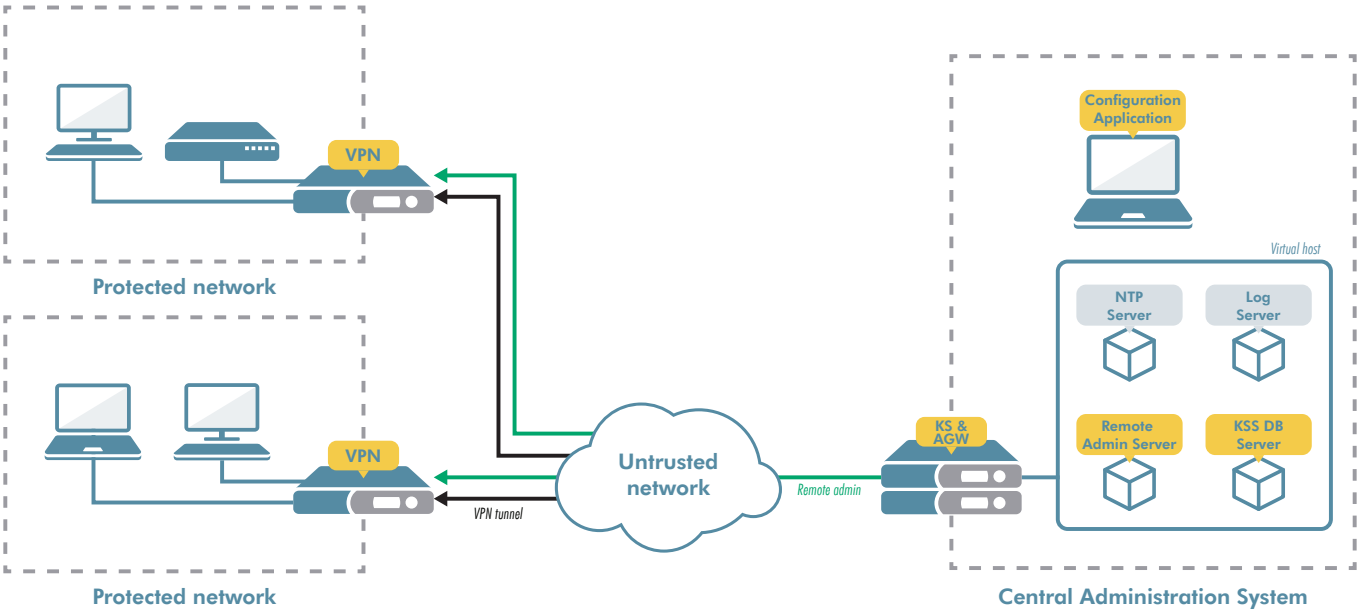
- Extensive secure key handling including designated key servers and remote key management and distribution
- Simple key management based on symmetrical encryption with dual algorithm support
- Selectable encryption algorithm (AES or Serpent) per VPN tunnel
- Replay protection
- Emergency erase of keys, remote or local
- Active and passive tamper resistance
- Hardware based encryption, red/black separation, root-of-trust and TRNG
- Design standards used:
  FIPS 140-3, Common Criteria EAL 4+

Device management

- Central Administration System (CAS) with redundancy option
- Secure administration enabled by Three Domain Separation and dedicated administration gateway (AGW)
- Smart cards for keys and configurations
- Secure local or remote firmware upgrade

Tactical features

- Designed to support tactical use-cases
- Silent mode reception to avoid detection
- Low band and jitter resilience
- Easy to declassify when not in operation
- Low power consumption to enable mobile scenarios



SecuriVPN system overview

VPN devices

Encryption devices protecting the traffic between the protected IP networks over the untrusted IP network using VPN tunnels.

Key Server System

Provides session keys for the VPN tunnels. Generation and distribution of session keys are performed by the Key Server device (KS device).

Remote Administration System

Delivers remote online supervision and administration of the encryption devices in the system. The Remote Administration System communicates to other devices through a Administration Gateway device (AGW device) which provides secure encrypted tunnels for management traffic.

Three Domain Separation

The Three Domain Separation technology provides separation between administrative and user data domains, providing administrators with a tool that allows management and control of VPN devices from a central location. At the same time, administrators cannot under any circumstances access user information that passes through a VPN device or information stored inside the secure network. The technology eliminates the threat of unauthorized disclosure of sensitive information by a VPN administrator.

Seamless network integration

SecuriVPN ISA is engineered to seamlessly integrate into modern environments supporting IPv6, DHCP, NAT, OSPF, Quality of Service, failover, and to support several modes of operation and concepts for network interconnection:

- Two-way tunnel or one-way tunnel
- Network modes: fixed, mobile and deployable
- Group Service: Effortlessly enable one network to provide IP services, such as servers, accessible to other networks within the group.
- Peer-to-Peer Service (P2P Service): Establish connections between networks within the group independently of any other network associations.
- Full Mesh Service: Forge connections and tunnels among all VPN devices within the system, ensuring comprehensive network coverage.
- Multicast Service: Customise multicast group services to listen to (Receiver) or send (Transmitter) information to a specific multicast address, or both (Transceiver).

Technical specification

Model specific	SecuriVPN ISA ED100FG	SecuriVPN ISA ED100FGP
Device type	VPN device, 19" rack	VPN device, portable
Device Size	442 x 44 x 272 mm 19" rack 1UE	257 x 44 x 272 mm
Device Weight	5,8 kg	4 kg
Ports	Optical 1000Base-SX (LC connectors)	Optical 1000Base-SX (LC connectors)
IP version	IPv4, IPv6	IPv4, IPv6
Performance	245 Mbps (full duplex, large frames)	245 Mbps (full duplex, large frames)
Power inlet	+11 - 13 VDC	+11 - 13 VDC
Power consumption	16W	16W
Power supply	Type: Internal 85-264 VAC (included) 10-66 VDC (optional) Dual power supply optional	Type: External 85-264 VAC (incuded)
Operating Temperature	-5 °C – +40 °C, 5 – 95% rel. H	-5 °C – +40 °C, 5 – 95% rel. H
Altitude	Max 2000 masl	Max 2000 masl
Pollution degree	2	2
MTBF	>75 000 h	>75 000 h

Cryptological system	SecuriVPN ISA
VPN characteristics	IPsec enhanced 512 unicast + 512 multicast tunnels NAT traversal Up to 150 Mbit linespeed 4000 keys
Cryptography	Symmetrical encryption: AES-256, Serpent-256 Asymmetric encryption: ECDH 521bit for enhanced key HMAC: SHA3-256 HASH: SHA-256
Key Management	Well-defined key hierarchy using black keys Perfect forward secrecy Session keys from Key Server System Authenticated session key exchange Enhanced IKE using ECDSA (521-bit) or RSA-PSS (1024-bit) signatures. Keys distributed on smart cards or through Central Administration

advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We empower countries, authorities, defence forces, critical infrastructure and businesses to secure society's most sensitive information. 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