BUSINESS SECURITY

SecuriVPN® Arana

Approved for Secret UE / EU Secret

Secure IP communication system for the world's most demanding customers

Network communication infrastructures of today touch all parts of the modern society and constitute a critical foundation in national economy, public safety as well as national and international security. The possibility to enable instantaneous communication and information exchange increases the productivity and effectiveness of your organization. Protection of the data you are sending is crucial, otherwise it is not possible to achieve the necessary trust and confidence for conducting business.

Business Security can offer you a full solution that secure both information and communication.

With the SecuriVPN systems you can communicate over an untrusted network without the risk of eavesdropping or manipulation of your system. Whether you need to protect network communication in the long term (for instance between embassies) or in the short term (supporting events gathering a large number of people such as large scale sporting events, political summits, natural disaster crisis management or sending out a battle group), the SecuriVPN system can fulfil your communication requirements.

Business Security can offer you a network and infrastructure design that fulfils all your needs and covers all your security requirements thanks to our expertise in creating security systems for the worlds most demanding customers.

SecuriVPN connects, encrypts and protects IP networks, including all IP based communication such as phone calls, faxes, email and file transfer, from, to and within your organisation. The system includes all components needed for a successful network administration and secure communication, such as VPN units, key servers, administration gateway, network management system, remote management system, key server system and key production system.

SecuriVPN system solution

SecuriVPN

SecuriVPN is a general purpose VPN system connecting several protected IP networks securely through an untrusted network. The data traffic between the protected networks is tunnelled on the IPsec level using symmetric 256 bits encryption and pre-shared or session keys.

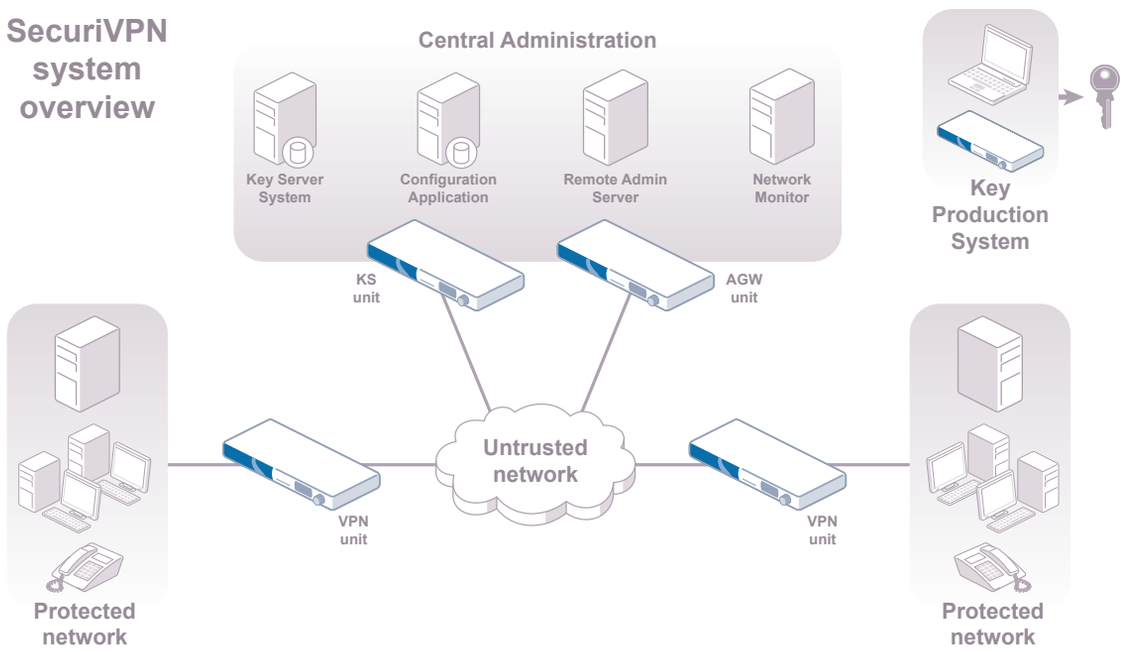
The security mechanisms providing the secure tunnelling in SecuriVPN are basically stand-alone units with dedicated hardware in combination with strong algorithms, communication protocols, keys and key management. The level of security of these mechanisms is chosen to withstand attackers that are highly motivated, have considerable amount of resources in form of money, equipment and time available, have knowledge of the interior design of the system and are highly skilled.

From a network viewpoint the SecuriVPN's main building block, the VPN units, are the default gateway for the protected networks and routes the IP traffic to the other protected networks using the configured tunnels. The protected networks may consist of a single host to large routed networks consisting of up to 16 different networks. The untrusted network may introduce delays, packet reordering and packet drop, but otherwise the untrusted network is invisible from the protected networks.

SecuriVPN places no restriction of the topology employed for the connection of the protected networks. It is possible to use SecuriVPN in topologies ranging from pure star topology, sometimes called hub-and-spoke, to full mesh networks where all protected networks may communicate directly.

Typical Applications:

- Protecting any networks that handles EU classified information.
- Protecting networks that handles nationally classified information (after national approvals)
- Connecting branch officies to a central site e.g. embassies.
- Full mesh networks used by battle groups
- Protection of radio-based networks
- Protection on single radio or satellite links
- Managed VPN solutions
- Public safety systems
- Protection of support/administration networks controlling vital infrastructure, eg power plants, electric supply networks etc.



Solutions for secure communication

Network administration

The administration of the VPN system is made centrally. The configuration of the complete system is administrated in a central instance of the Configuration Application. From the Configuration Application the configurations for the individual units are generated and distributed online in administration tunnels. The configurations for the units contain all required parameter settings.

From the central site called Remote Administration System, the VPN units are remotely monitored and controlled. Log events and alarms are collected into central servers. From the Remote Administration System configuration and firmware updates are sent online to the VPN units.

The untrusted network may be any routed or switched IP network. The quality of the network may range from fixed high bandwidth networks such as private networks, to Internet, to networks containing paths that are carried over satellite, to very low bandwidth networks carried over short wave IP radio. Parameter settings in the configuration adopt to these different network situations.

For mobile situations, where the protected network is moved from one location to another, the VPN unit registers its new IP address within the Remote Administration System. This allows other units to find the relocated unit without change of their configurations.

When the same information needs to be spread from one protected network to several others it is suitable to use multicast addressing. In SecuriVPN it is possible to configure tunnels that securely connect several protected networks using multicast addressing. Any multicast connected protected network may send and receive multicast traffic to and from all the other connected protected networks. As with unicast addressing, the transport of multicast traffic over multicast tunnels is invisible to the hosts on the protected networks. For flexibility it is possible to use a combination of multicast IP address and UDP port as definition of a multicast tunnel. It is also possible to configure a mapping between the multicast address used on the protected network to another address used on the untrusted network.

Security administration

The administration of the security settings and keys are made with the Key Production System, Key Server System and locally on the units. The pre-shared keys are generated and administrated in the Key Production System. The keys are distributed in encrypted form to the units on PIN-protected smart cards. The keys may also be distributed to the units from the Remote Administration System using the administration tunnels (option).

The Key Server System generates session keys to be used as the key for the actual data encryption on the tunnels. Each tunnel is given a unique session key, only shared between the two participating VPN units. The key is automatically replaced after a certain amount of data or period of time. The key server only distributes session keys to the units that are allowed to communicate according to the configured tunnels in the system. This gives an extra layer of security.

Scalability

SecuriVPN is scalable, both with the number of protected networks that may be connected but also with the network and security architecture. There are two major ways of downscaling the system. First, it is not necessary to deploy the Remote Administration System if it is acceptable to reduce the central control and supervision of the system.

The second step to downscale the system is to use only manually distributed pre-shared group keys instead of relying on session keys from the Key Server System.

SecuriVPN system solution

Reliable system
Business Security is a trusted European security solution provider, providing top of the class certified solutions, approved by independent evaluation organisations.

Complete and flexible
The system includes all components that are needed for successful network administration without the risk of loosing your data. The necessary building blocks consist of encryption units, key servers, administration gateways, network management system, key production and key management systems.

Easy to learn, easy to use
The system is designed for efficiency and effectiveness. The usability goal is to make it easy for your network management team to operate the system, exactly the way they want to. A team of experts will guide you with expertise in installation, management, support and maintenance of your system, as well as knowledge transfer within the area of information security.

IP standards compliant
The SecuriVPN system is designed according to IP networking standards. It will therefore be easy to deploy into your existing network infrastructure.

Standard platform
Business Security knows the communication security market and the solutions fulfil all major needs for a demanding end-user. The SecuriVPN system is flexible and modular in its design, also meeting custom-design requirements. SecuriVPN Arana is approved for Secret UE / EU Secret.

High availability
The system has been designed for harsh environments and high availability. The exceptional track record includes field deployment in the Nordic Battle Group.

Attractive TCO, Total Cost Ownership
The combination of innovative security technology and security management gives a unique solution that reduces daily maintenance and support. The system requires a minimum of user assistance since all components are optimised with a high level of usability and easy update support.

High performance
You can grow with SecuriVPN into the future. After many years of development Business Security can deliver a high-speed solution without compromising data security. Future development will bring even more high performance solutions.

Regulatory Compliance
- CE
- FIPS 140-2 Level 3 conformant
- Tempest EU/SWE MIL-STD up to classification level Top Secret
- Common Criteria EAL 4+
- Secret UE / EU Secret approved

Company Profile

Business Security AB is an independent Swedish company and manufacturer of secure encryption solutions for data, voice, fax, video and the Internet. We develop leading-edge encryption solutions for government entities and organizations with very stringent security requirements such as military departments, law enforcement agencies, multinational corporations and banks. So far, Business Security has delivered trusted security solutions to more than 40 countries worldwide.

BUSINESS SECURITY

Business Security AB
Box 11065
S-220 11 Lund, Sweden
Tel: +46 46 38 60 50
Fax: +46 46 38 60 55
E-mail: reqinfo@businessecurity.com
URL: www.businessecurity.com