

SecuriVPN Central Administration

SecuriVPN Central Administration

SecuriVPN Central Administration is used to configure, supervise and control the SecuriVPN units. The Central Administration can be installed on one server or distributed over several dedicated servers, depending on the desired network architecture. With the Central Administration system it is possible to configure, administrate and monitor all systems from one central site. The Central Administration system can manage clusters of units for easy and effective configuration. It enables easy and secure system administration and allows the network management team to operate the system, exactly the way they want.

All parts of the SecuriVPN network can be administrated centrally using the Central Administration.

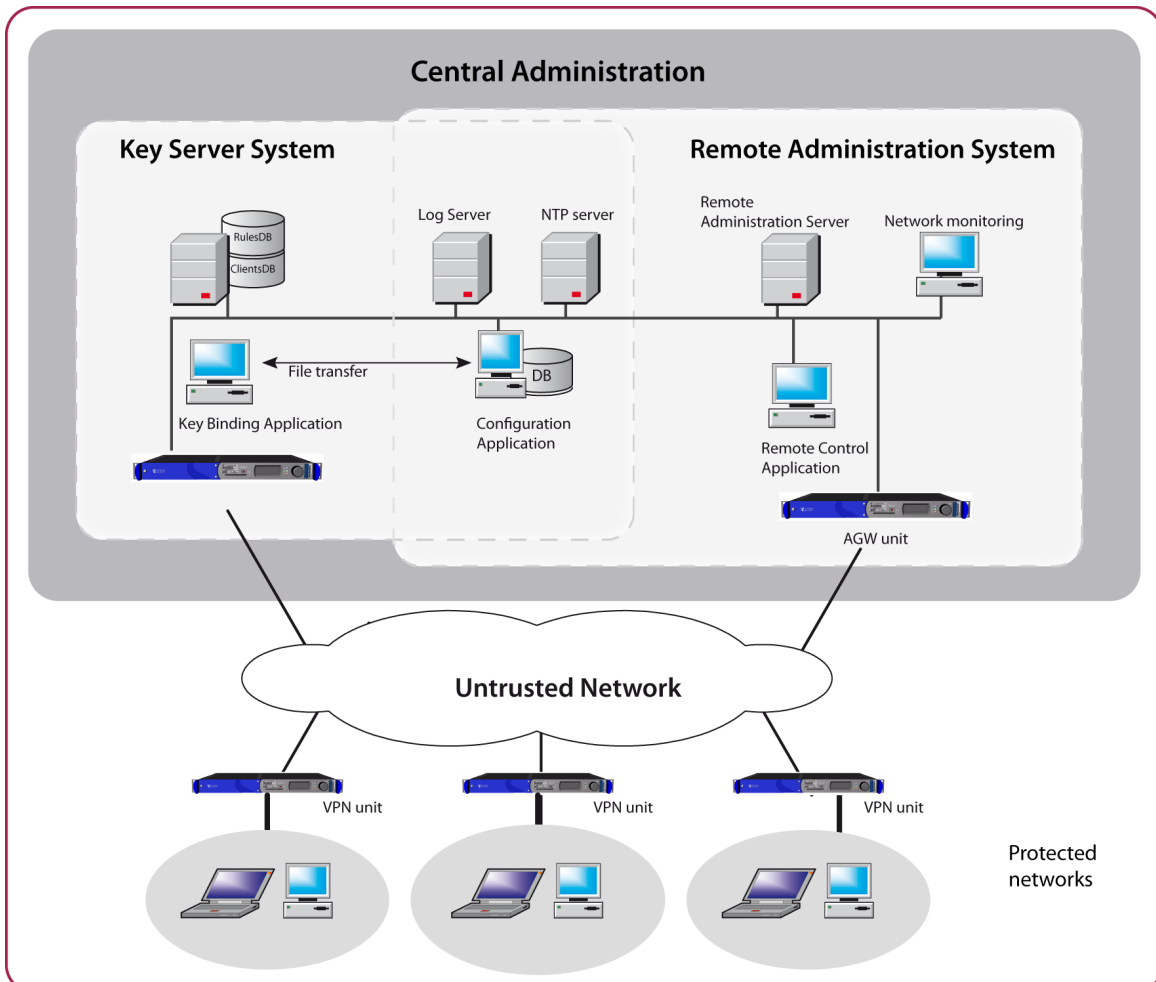
The configuration of the complete system is administrated in a central instance of the Configuration Application.

From the central site, the VPN units are remotely monitored and controlled using SNMP. Log events are collected into a central Syslog server and alarms (SNMP traps) are sent from the VPN units to a configured receiver. From the Remote Administration System configuration and firmware updates are sent online to the VPN units.

The central administration consists of two parts:

- Key Server System
- Remote Administration System

The Key Server System provides the session keys used for encryption of the end user traffic. The Remote Administration System is responsible for management and distribution of configurations and remote administration of the encryption units.



Remote Administration System

The Remote Administration System is used for management and distribution of configurations and remote administration of the encryption units. It consists of the following parts and features:

The Administration Gateway unit, an encryption unit protecting the management traffic. It also stores changed IP addresses of units that have made locally on the units and it provides time information to the VPN units.

Configuration Application, from a remote administration perspective, is used for publishing configuration files to the Remote Administration Server. The Configuration Application is further described above.

Remote Administration Server's responsibility is keeping the encryption units up-to-date with the correct configuration files and CRLs, and for handling manual remote control commands on behalf of the Remote Control Application.

Remote Control Application is an application used for issuing commands to encryption units. It is included in the Remote Administration Server distribution and accessibly using a web browser.

Remote Supervision Application is a standard SNMP management application. The MIB-files needed are supplied in the Network Management Extension product.

Log server, a standard log server where events from all of the system's encryption units are collected and stored.

The NTP server is providing time information to encryption units.

Administration network is a protected LAN with all the components of the Remote Administration System.

Supervision

From the Remote Administration System it is possible to supervise the encryption units using a third-party standard SNMP based network-monitoring application, such as HP Open View Network Node Manager. Several MIB files are used for describing the parameters available for reading, and in some cases writing to, the encryption units. The SNMP traffic is sent using the administrative tunnels to the VPN units (protected communication).

Distribution of configuration files and CRL's

From the Remote Administration System configuration files and Certificate Revocation Lists (CRLs) are distributed to VPN units over the untrusted network using the administration tunnels (protected communication).

Collecting log events from the units

It is possible to configure exactly which log events an encryption unit shall report. The VPN unit send batches of log events periodically over the untrusted network using the administration tunnels (protected communication).

Controlling units

From the Remote Administration System the Remote Control Application can control the encryption units. The application has a web interface and is operated from a standard web browser.

The administration tunnel is used by the Remote Control Application for sending remote control commands to VPN units (protected communication).

System time distribution

Central time may be distributed from the Remote Administration System using the administration tunnels (protected communication).

Updating firmware in the units

When a new firmware becomes available for a VPN unit it may be transferred from the Remote Administration System to the unit where it resides in storage until a command is given to install the new firmware.



Key Server System

The Key Server System provides session keys for the tunnels. The session keys are used for encrypting and authenticating the traffic. This system consists of the following parts:

Key Server unit (KS unit) generates and distributes the session keys to its clients (VPN units and AGW units). The communication between a client and the KS unit is protected by a master key. The KS unit has master keys for all of its clients loaded.

Key Server System database server contains databases of information for the KS unit about which clients that may communicate and the identity of the clients.

Key Binding Application is a software tool used for registering which client is using which master key.

The Configuration Application is shared with the Key Server System and the Remote Administration System. The Configuration Application is further described above.

The Log Server is also shared with the Key Server System and the Remote Administration System. In the Key Server System it collects and stores log events from the Key Server unit.

Session key generation

When a tunnel shall be established to another unit the initiating unit request a session key from the key server . If the communication is granted by the key server a new session ticket is generated and returned. The session key is then used for encryption of the end-user traffic sent over the tunnel. Session keys are also continuously renewed.

Security Control

Before the Key Server issues a session key it performs security checks to validate the request. These checks includes verification that the request is made using the correct master key and that the communication to the remote part is allowed according to the rule-set stored in the KSS database.

Configuration Application

The configurations for all units in the VPN system are made and maintained in one Microsoft Windows application called Configuration Application. Here the complete configuration of the system and the units are handled. When updates are made, the unit's individual configuration files are distributed online in the administration tunnels. Distribution can also be made manually using smart cards as transport media.



technologies adapted to your needs...

Key Server System

The Key Server System provides session keys for the tunnels. The session keys are used for encrypting and authenticate the traffic. This system consists of the following parts:

Key Server unit (KS unit) generates and distributes the session keys to its clients (VPN units and AGW units). The communication between a client and the KS unit is protected by a master key. The KS unit has master keys for all of its clients loaded.

Key Server System database server contains databases of information for the KS unit about which clients that may communicate and the identity of the clients.

Key Binding Application is a software tool used for registering which client is using which master key.

The Configuration Application is shared with the Key Server System and the Remote Administration System. The Configuration Application is further described above.

The Log Server is also shared with the Key Server System and the Remote Administration System. In the Key Server System it collects and stores log events from the Key Server unit.

Session key generation

When a tunnel shall be established to another unit the initiating unit request a session key from the key server . If the communication is granted by the key server a new session ticket is generated and returned. The session key is then used for encryption of the end-user traffic sent over the tunnel. Session keys are also continuously renewed.

Security Control

Before the Key Server issues a session key it performs security checks to validate the request. These checks includes verification that the request is made using the correct master key and that the communication to the remote part is allowed according to the rule-set stored in the KSS database.

Configuration Application

The configurations for all units in the VPN system are made and maintained in one Microsoft Windows application called Configuration Application. Here the complete configuration of the system and the units are handled. When updates are made, the unit's individual configuration files are distributed online in the administration tunnels. Distribution can also be made manually using smart cards as transport media.

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 AB

Box 11065

S-220 11 Lund, Sweden

Tel: +46 46 38 60 50

Fax: +46 46 38 60 55

E-mail: reqinfo@businesssecurity.com

URL: www.businesssecurity.com