



we secure YOUR network



network security  
network security

## CryptoGuard VPN family

The CryptoGuard VPN 5000 family is a flexible (cost-)effective security system, completely developed by Compumatica. It is deployed in highly sensitive areas. CryptoGuard VPN enables the secure and confidential communication within a single LAN and in protected linking of several LANs, even over public networks. Sensitive data is protected against unauthorized use during transportation over insecure public networks.

## Features CryptoGuard VPN

- Encryption on layer 2, 3 and 4
- Packet filter firewall, protocol, source-destination
- Black box transparent mode, not detectable
- Simple integration in existing networks
- IPsec encryption and authentication
- VPN mode: payload encryption, no data expansion
- Perfectly qualified for satellite communication
- Latency less than 1 ms.
- Algorithms: AES up to 256bit, 3DES
- Customization possible e.g. S-boxes and algorithms
- Strong pseudo random generator, hard- or software
- Redundancy based on OSPF or STP
- Support of VLANs
- Support of jumbo frames
- Security components: CF-card and smartcard
- Scalable throughput up to Gigabit connections
- Hardened Operating System (COS)

## Mobile communication

Compumatica offers several complementary solutions for remote communication.

Our CompuWall in combination with a Windows client. From everywhere in the world: working as in the office. All information can be available. If you combine CompuWall with our secure GSM encrypted voice, SMS and encrypted mail can be implemented.

CryptoGuard VPN Client is a software solution for the encrypted communication of a single PC or laptop with a central server or company network.

## CryptoGuard VPN 500

CryptoGuard VPN 500 is the smallest model of the CryptoGuard VPN product-range. It represents an cost-effective solution for individual PCs, small networks and servers. CryptoGuard VPN 500 provides the same features as the other models of the product-range.



Highest security for voice, data and video over IP

# VPN solutions for Intranet and Internet

## CryptoGuard VPN 5000

CryptoGuard VPN 5000 secures your Fast Ethernet network connections using standardized encryption algorithms (AES) and protocols (IKE and IPsec). Next to our proven CryptOn technology for secure key storage, CryptoGuard VPN 5000 supports smartcards as well. Networks with a capacity up to 100 Mbps full duplex are supported.

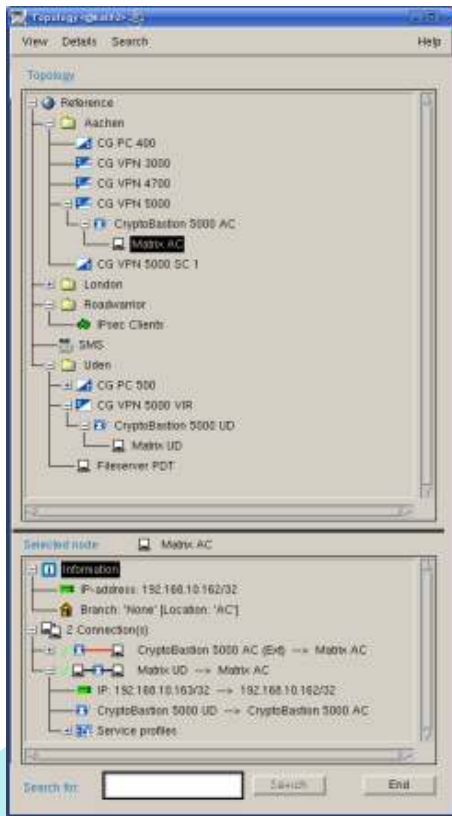
## CryptoGuard VPN 5000 Gigabit

CryptoGuard VPN 5000 Gigabit is the top model of our proven quality CryptoGuard VPN product-range. Apart from the usual security needs, CryptoGuard VPN 5000 Gigabit also meets the performance requirements of a Gigabit Ethernet network with throughput up to 1Gbps.

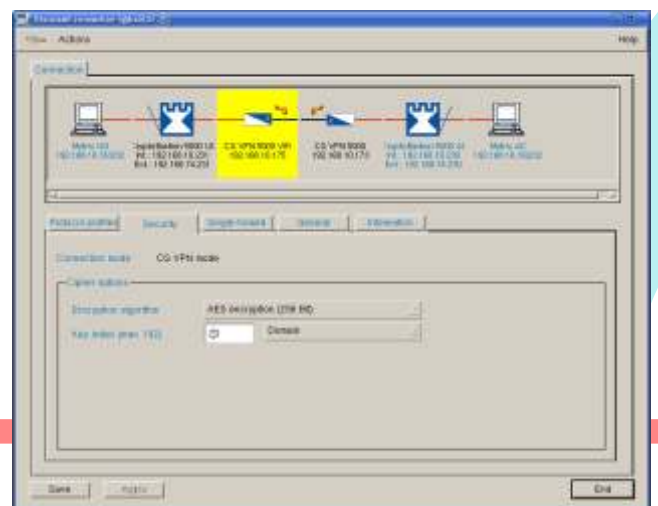
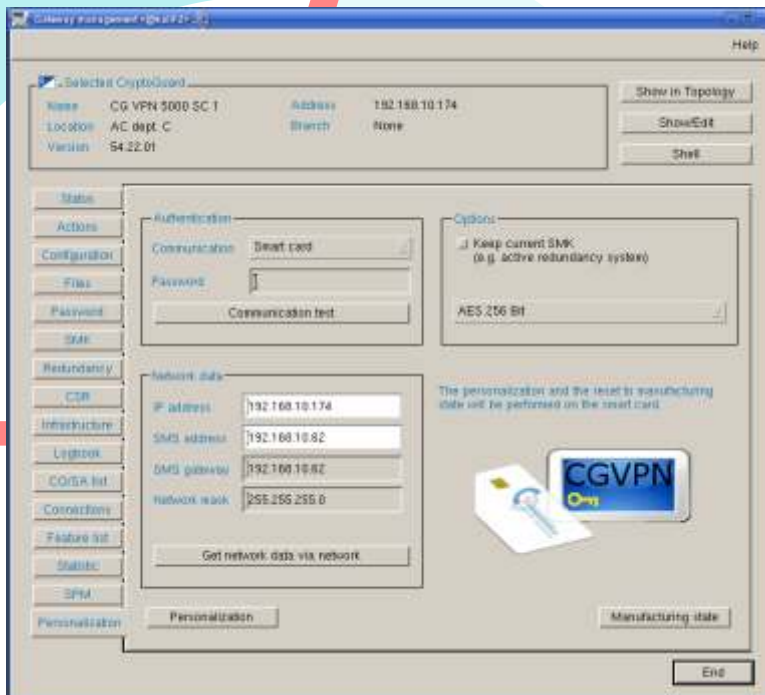


## Security Management Station

The Security Management Station (SMS) allows the central management of the several security components (CryptoGuard VPN, CryptoBastion) with versatile options and a user-friendly interface. The rules are defined in the SMS and the security components will be configured automatically, conform to the topological information. Furthermore, the SMS offers an intelligent key management system and several options to configure VPNs. To prevent a classic attack on firewall systems, the communication between the SMS and the security components is encrypted with modern algorithms. The SMS can easily be integrated in an existing network and enables virtual network computing all over the world. The SMS is "the heart and the brain" of the network security system.



## Central Security Management



## High-level overview

- Generation of secure connections using profile mechanisms
- Visualizing of connections
- Automatic rule generation with fault tolerance checking
- Intelligent, central and secure key management
- Hardware or software random generation
- Monitoring and alarm mechanisms
- SNMP interface
- Batch-job scheduling
- Redundancy mechanism

## Features

- Centralized Security Management
- Downward compatible up to the first release
- Unix based operating system
- Central data backup and restore
- Underlying high performance database
- Access control and role based administration
- Easy integration in existing network infrastructures
- Encrypted communication between SMS and security components





## CryptoBastion

The CryptoBastion as application level firewall separates the attached networks logically and physically. The entire network traffic between the connected subnets is checked and granted by this single entity.

Proxy applications for the most widespread services establish the connections for the desired services and protocols.

The versatile, modular CryptoBastion offers Unified Threat Management because of the newly implemented features:

- OpenVPN
- Host-IDS
- AntiVIRUS
- AntiSPAM
- SSL secured client as well as site2site access
- Every file system change will be reported
- Check for malware for HTTP(S), FTP, ESMTP and POP3
- Dispose unwanted mails for ESMTP and POP3

High availability through two CryptoBastion firewalls, either in active/active or active/passive mode, load balancing enabled selectively.

Misconfiguration is prevented by the applied principle

**"Everything is strictly prohibited, unless it's explicitly allowed."**

The screenshot displays the following information:

- Network:** med1.intern.computica.de
- Software version:** 5.40.0 (+2 updated)
- Local time:** Wed 10 Sep 2008 14:50:31 CEST
- Configured at:** Wed 03 Sep 2008 13:34:08 CEST
- Uptime:** 70 days, 23:50 (89 days, 6:32)
- License status:** will expire on 10/14/2008 (in 34 days)
- Token number:** 00000015
- Version:** 8207 from 09/10/2008
- Virus database:** 12:58:40

**Status:** Runlevel: ACTIVE

CPU:	8%
RAM:	33% of 499 MB
Swap:	0% of 793 MB
Number of processes:	84
Log partition:	2% of 36616 MB
Mail partition:	1% of 36817 MB
Quarantine:	15369
Bad mails:	3
requests:	0
deadletters:	0

**Current services configuration:**

- Virus scanner: **OK**, activated for services: HTTP, ESMTP, POP3, FTP
- Spam protection: **OK**, activated for services: ESMTP, POP3
- HTTP proxy: activated, 4 connection rules
- ESMTP proxy: activated, 4 connection rules
- FTP proxy: activated, 2 connection rules
- Telnet proxy: activated, 1 connection rule
- NNTP proxy: activated, 1 connection rule
- POP3 proxy: activated, 2 connection rules
- RTSP proxy: activated, 1 connection rule
- ICP relay: activated, 9 connection rules
- UDP relay: activated, 1 connection rule
- NETIO proxy: not activated
- Management proxy: activated, 3 connection rules
- OpenVPN: **OK**, 0 clients connected
- HA/Cluster: not activated
- SNMP: active

**Interface:**

Interface	Link	Speed
eth0	●	100Mb/s (Full)
eth1	●	100Mb/s (Full)
eth2	●	100Mb/s (Full)

## Strict and reliable Firewall security!

### CompuWall

is the flexible CryptoBastion stand-alone firewall solution with web management for security sensitive network administration. It combines a high security standard with outstanding performance. The CompuWall is managed via a SSL secured browser connection and provides an intuitive graphical user interface.

Configurable proxy applications are available for HTTP(S), FTP, Telnet, (E)SMTP, NNTP, POP3, RTSP, NET8, TCP/R and UDPR.

CompuWall features the special option to realize secure user authentication by means of mobile phone authentication, in addition to simple password, one time password, LDAP and/or RADIUS authentication.

### CryptoWall

is the high-end security solution in a multi-stage security environment. By applying different hard- and software modules, solutions can be customized individually. Security sensitive enterprises can choose from various active firewall elements, different platforms and operating systems, define proxies and equip the firewall system with extra functionalities. CryptoWall is based on tested-and-assured certified firewall components.

A CryptoWall consists of a combination of CryptoGuard VPN and CryptoBastion components.

Sharing data, voice, and video, internally and between companies and organizations has increased dramatically over the last years. The value of information is enormous and needs to be protected. Unauthorized access to data – accidentally or on purpose – must be prevented. Securing IP traffic by high level encryption is the solution to this problem. Creating security awareness at management and employee level is basic. It is advisable to separate the network and security responsibilities. For the network manager the availability and accessibility of the network will have priority. The security manager focuses on protecting data and unauthorized access. Managing both security and access by the same person can lead to conflicting interests and incidents. Security added to routers may seem easy and cheap, but is not optimal from a security point of view. Compumatica advises to use routers for network management and Crypto devices for data protection.

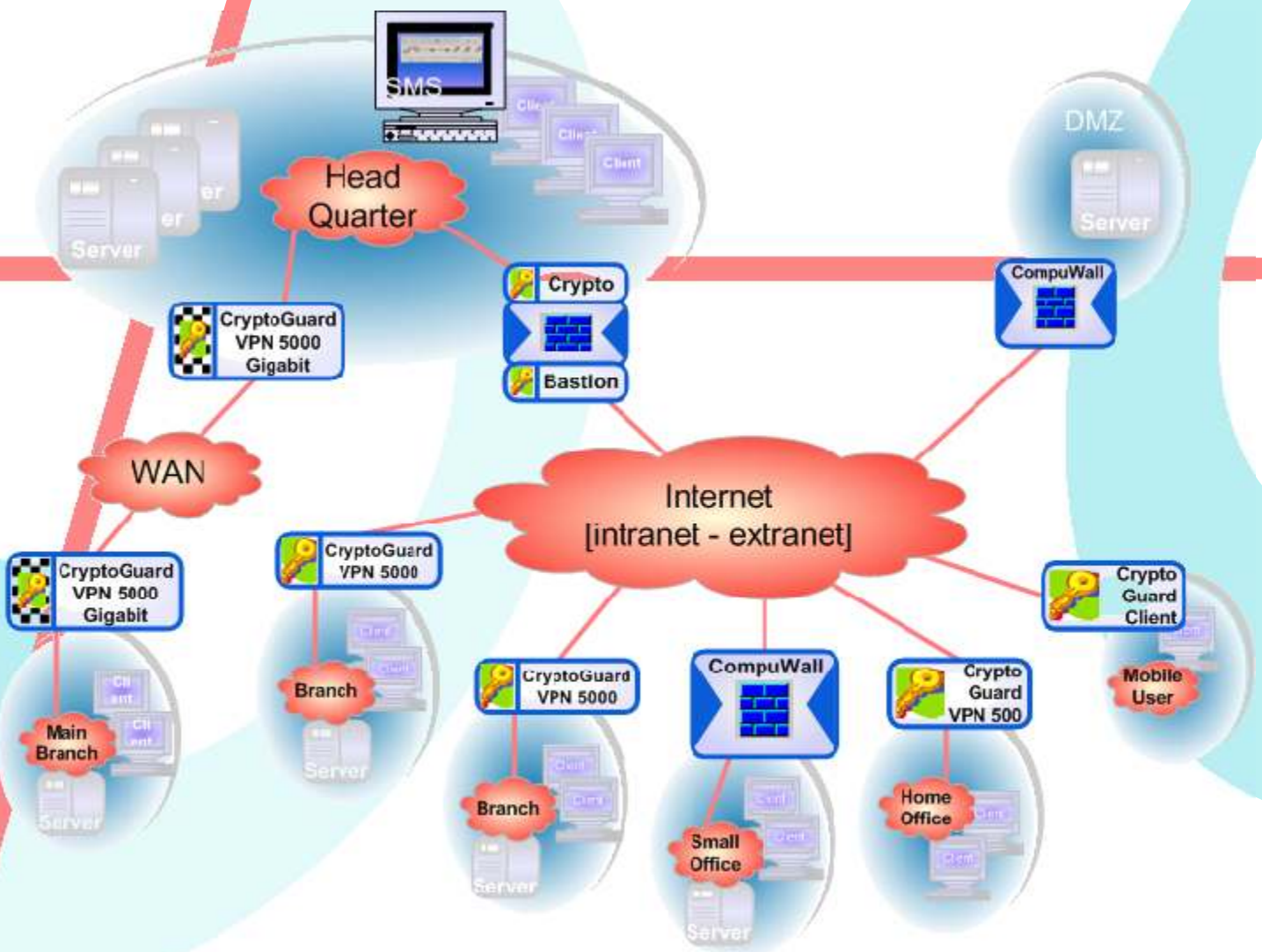
## Network security to perfection

CALEA, the US law for interception of all IP and telephone data, gives several organizations insight information of your data. Interception of IP traffic by worldwide telecommunication providers and governmental bodies makes sending of company (government) confidential data risky and dangerous. You never know who has access to your information.

Compumatica assures that all its products are backdoor free. Data, protected by the CryptoGuard, is invisible and unreadable for unauthorized people.



**CryptoGuard VPN 100 % backdoor free**



## CompuCrypt XL

Network connections that require high speed encrypted throughput use the CompuCrypt XL. The CompuCrypt XL is the newest security system of Compumatica. With the CompuCrypt XL it is possible to encrypt IP data, voice and video up to speeds of 10 Gbps. Default algorithm is AES key lengths 128, 192, 256 bits. Key material and all configuration data are stored on a smartcard by the CompuCrypt Management System. The CCM is a straight forward and easy to handle management system. Different models and features will be developed in the future.

## Compumatica GSM

Secure communication via GSM is more and more a need for management and international travelers.

Encrypted voice and SMS protect companies confidential information from interception. The unique combination of the Compumatica GSM with the CompuWall in your office encrypts and protects all your e-mail and log-in to your network. Standard AES 256 bits encryption is implemented. Specific S-boxes can be implemented.

Remote management by the Key Management System allows additional features.



## Special product versions – approvals

Apart from the commercial product portfolio, Compumatica provides an additional supply of country-specific encryption devices, special algorithms and S-boxes. This can be your own or developed by our crypto department. The products can furthermore be equipped as to comply with all TEMPEST stages as defined in SDIP 27 A,B or C.

## Approved for governmental use

The devices received the approval for "VS-NfD" from the German authorities, approved "Departementaal Vertrouwelijk" for Dutch authorities and "EU restricted" for the European Community.

## Approved for "NATO-Restricted"

Compumatica has also developed a variant which received the approval for the classification level "NATO-Restricted".

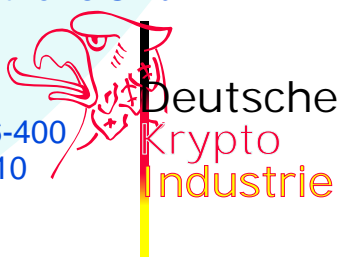
Compumatica secure networks – based in Germany and the Netherlands – is an independent private company with as main objective the securing of its customers' IP traffic.

Compumatica develops, produces and implements high level security solutions to all types of IP networks and customers. Customers may be a small organization with just a few countrywide connections or multinational companies with large worldwide networks.

Compumatica staff and products comply with high standards of reliability and quality. Every single product goes through a quality assurance phase in which it is subjected to thorough long-term tests. All Compumatica products are backward compatible for more than ten years. Herewith we guarantee our customers investment protection.

Customers of Compumatica are well named Top 500 companies as well as Governments of several countries who use our solutions to protect their critical data.

Compumatica secure networks GmbH  
Germanusstrasse 4  
52080 Aachen  
Germany  
Phone +49 (0)241 16 96-400  
Fax +49 (0)241 16 96-410  
www.compumatica.eu  
info@compumatica.eu



Compumatica secure networks bv  
Oude Udenseweg 29  
5405 PD Uden  
The Netherlands  
Phone +31 (0)413 334668  
Fax +31 (0)413 334669  
www.compumatica.eu  
info@compumatica.eu

