

Technical
WhitePaper

Enhancement of your VPN security system

Secure connections via shared infrastructures

Compumatica secure networks



OVERVIEW

NETWORK SECURITY

plays an important role for any company's IT management. For a better protected environment, security components have to be integrated into the firm network. A CryptoGuard VPN device fulfills these security demands in a both simple and efficient way.

Network Security today ranks high on the list of any company's concerns. Almost all of a company's relevant information is exchanged in electronic form via networks. Since the network technology used may assist attackers in many ways, these networks don't generally guarantee security or confidentiality.

For this reason, security has to be added to a company's networks. The pure security requirement can be fulfilled by integrating additional security devices into the existing network.

The CryptoGuard VPN is such a security device that can be easily integrated into an existing network, enforcing security and confidentiality.

The basic idea of a virtual private network (VPN) is to use the advantages of an open communication infrastructure in an economic way (e.g. the Internet) without taking the risks connected to that. A VPN should ensure that confidentiality of sensitive data is maintained during transmission over networks (LANs and WANs), so that only those persons or users authorized to access the sensitive data can do so.

VPN systems are integrated into the communication system in the form of black boxes or security sub-layers, together with an intelligent security management capability. A highly secure VPN can be realized by using the security components of the CryptoGuard VPN system.

The CryptoGuard VPN system consists of the Security Management Station (SMS), the central management station; the CryptoGuard VPN (CGVPN), a packet filter and encryption device; and the CryptoGuard VPN Client (CGClient), a packet filter and encryption client for Microsoft operating systems. Additionally to the CryptoGuard components, the CryptoGuard VPN system can be extended with the CryptoBastion, an application level firewall device.

Combining the two security systems CryptoGuard VPN and CryptoGuard VPN Client with the same management allows the user to create powerful network security solutions.

CRYPTOGUARD VPN SYSTEM

The basic philosophy of the CryptoGuard VPN device consists in the realization of a centralized system management. This concept requires that all information about the security system (e.g. CryptoGuard VPN device configurations, packet filter

definitions, System Master and Connection Keys, ...) is stored at the Security Management Station (SMS).

The Security Management Station (SMS) only distributes the parts of the management information required by a certain CryptoGuard VPN device as copies to this respective device. This is done in a secure (encrypted) way via the network or by smartcard.

**ADVANTAGES OF THE
CRYPTOGUARD VPN
SYSTEM**

- ✓ no additional software packages necessary
- ✓ clear demarcation between communication and security in a network
- ✓ flexibility of the CryptoGuard VPN devices

The CryptoGuard VPN system establishes a VPN in an existing network infrastructure without the need for adapting this structure. It consists of a centralized management (Security Management Station) and network security devices (CryptoGuard VPN).

The CryptoGuard VPN device itself is realized as black box solution that acts as an independent VPN gateway with additional packet filter functionality.

The advantages of an independent VPN gateway device are:

- CryptoGuard VPN devices fulfill the design criteria very well because they need no additional software packages or task settings.
- With separate CryptoGuard VPN devices, a clear demarcation is created between communication and security in a network.
- CryptoGuard VPN devices are flexible because they act as a security bridge.

The CryptoGuard VPN is a security device to realize a Virtual Private Network (VPN) by using encryption and filtering.

INTEGRATION STEPS

Integrating a CryptoGuard VPN device into the network occurs very easily during four phases (define, personalize, integrate and configure). The sequence of these phases is fixed; they have to be done step by step.

First the CryptoGuard VPN devices have to be **defined** at the SMS. For each CryptoGuard VPN device a name, an IP address and the associated network gateway resp. alternatively the IP address of the SMS has to be entered.

After entering these parameters at the SMS, the CryptoGuard VPN devices can be **personalized**. During the personalization phase all information the CryptoGuard VPN device needs to establish a secure network connection with the SMS is transferred to the smartcard (e.g. the System Master Key (SMK))

and net work parameters). The personalization can also be carried out per remote between SMS and smartcard.

Once this fundamental information is loaded, the CryptoGuard VPN device can communicate with the SMS in a secure (encrypted) way. This secure communication is done via the network, so the next step is to **integrate** the CryptoGuard VPN device into the network.

After integrating the CryptoGuard VPN devices into the network, the network will run the same as previously. This is because the behavior of the CryptoGuard VPN device in this phase (personalized and not configured) will be transparent for the network protocols and network mechanisms. The only thing the CryptoGuard VPN device does is to pass every network frame from one network connector to the other - nothing is changed in the traffic.

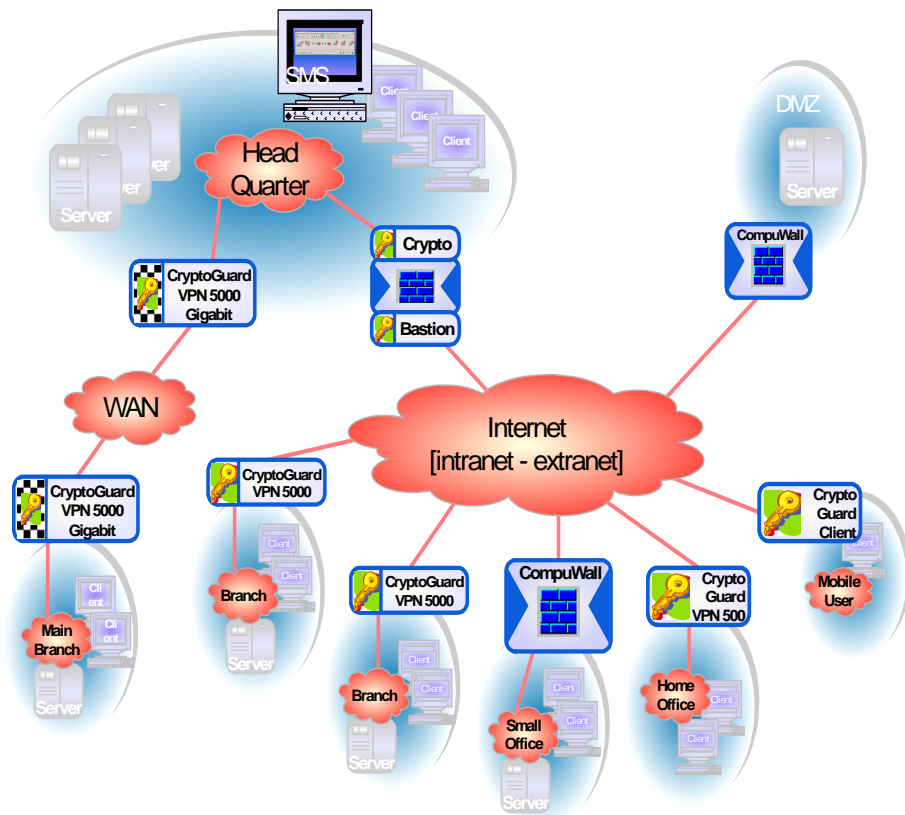
Next the CryptoGuard VPN device has to be **configured**. "Configuring" involves loading all configuration information required for daily use (e.g., filter rules (security policy), connection keys, logbook definitions and so on) into the CryptoGuard VPN device.

After completing the above steps, the CryptoGuard VPN device is integrated into the network and ready for use. A serial interface is available as further operational interface. For use as a packet filter no other CryptoGuard VPN devices are needed. For use as an encryption device, at least a second CryptoGuard VPN device is needed in the network to decrypt the encrypted frames.

The following figure shows a network after integration of the Security Management Station and several CryptoGuard VPN devices.

FOUR IMPLEMENTATION PHASES

1. Definition
2. Personalization
3. Integration
4. Configuration



CryptoGuard VPN devices are executable after their configuration even without intervention of the SMS. They support two independent security modes, IPsec/IKE and CryptoGuard VPN, which are specified in the following.

CRYPTOGUARD VPN MODE

The proprietary security and encryption mode of the CryptoGuard VPN device can be used in parallel to the IETF standard IPsec/IKE. (**Note:** only one of the two security modes is possible for a specific IP-source and IP-destination combination at one time).

After supplying the CryptoGuard VPN device with the needed connection keys and the security policy, a secure communication between two CryptoGuard VPN devices can be established. As encryption algorithms AES with a key length of up to 256 bits, 3DES, ADES and DES are supported. Although the CryptoGuard VPN Mode in general works with static encryption keys, there is a dynamic encryption of the network frames. This makes statistical analysis more complicated for the attacker and increases the security. As the used encryption

algorithm is length transparent, i.e., there is no data expansion through the encryption, the CryptoGuard VPN encryption will not generate any additional overhead on the network.

CRYPTOGUARD VPN MODE

- ✓ transparency towards the network
- ✓ encryption on several network protocol layers

Two important features of the CryptoGuard VPN Mode are the transparency of the CryptoGuard VPN device to the network and the ability to encrypt the network frame at different network protocol levels.

The transparency to the network results from the fact that in the CryptoGuard VPN Mode the encrypted network frames are sent to their original receiver addresses. They are not sent to another CryptoGuard VPN device (as, e.g., in IPsec/IKE Mode). The CryptoGuard VPN device doing the encryption is placed in front of the original recipient of the network frame. Based on its security policy, it automatically detects if there is a network frame to decrypt or not. If so, the network frame will be decrypted and sent to its recipient.

The encryption of the network frame can start at different positions within the frame. Depending on the customer's needs, the encryption can be done for MAC layer data (i.e., the entire IP frame), for IP layer data (the IP payload will be encrypted) or for TCP/UDP layer data (only the TCP/UDP payload will be encrypted). Which connection will be encrypted in which way is defined by the security policy.

IPSEC/IKE MODE

The CryptoGuard VPN devices can be run in two modes: The IPsec/IKE Mode works similarly like described for the CryptoGuard VPN Mode but the original frame length is modified when tunneling in the IPsec/IKE Mode, i.e. the IPsec/IKE Mode is in contrast to the CryptoGuard VPN Mode not length transparent. Furthermore, the following characteristics apply for the IPsec/IKE Mode:

IPSEC/IKE MODE

- ✓ not length transparent
- ✓ standardization
- ✓ interoperability with 3rd party products

The IPsec/IKE Mode of the CryptoGuard VPN device is an implementation of the VPN security standard defined by the IETF. The most important features of the IPsec/IKE Mode are the standardization of and interoperability with 3rd party products.

The CryptoGuard VPN device accepts the protocols ESP, AH, IPComp and IKE. Furthermore, it supports a number of algorithms for the ESP and AH protocol (e.g., ESP: AES with a key length of up to 256 bits, DES, 3DES, CAST; AH: MD5, SHA-1). The IKE protocol implementation supports authentications with PSKs (Pre-Shared Keys) and with RSA signatures. The algorithm for data compression supported by

IPsec is the deflate algorithm. Further IKE-/IPsec characteristics are Dead Peer Detection (DPD) and NAT-Traversal (NAT-T).

CHARACTERISTICS OF BOTH SECURITY MODES

Encryption and filtering in both modes are based on the security policy the user defines. The definition of the security policy has to be done centrally at the Security Management Station.

After defining the security policy at the SMS, the policies have to be transferred into the CryptoGuard VPN devices. Transferring the security policy from the SMS into the CryptoGuard VPN devices is done via the network in a secure and authenticated way, with no opportunity for someone to manipulate the transfer.

The smartcard is applied to securely store the System Master Keys (SMKs) of the CryptoGuard VPN device. The CryptoGuard VPN SMKs are used to establish a secure, authenticated connection between a CryptoGuard VPN device and the associated SMS. Additionally, the SMKs are used to guarantee the security of security-relevant data in the CryptoGuard VPN device.

Before establishing a secure communication between two CryptoGuard VPN devices, the associated connection keys and security policy have to be distributed to the devices. This is done automatically during the CryptoGuard VPN configuration phase by the SMS. The configuration phase is initiated by the SMS. The first step is a mutual authentication and the generation of a session key. The session key is used to secure the configuration session between the SMS and the CryptoGuard VPN device.

SECURITY APPROACHES

The CryptoGuard VPN device can operate in two different modes, corresponding to two security approaches.

The first approach is 'Everything that is not explicitly allowed is forbidden'. This means that if there is no rule for a specific protocol (e.g., "allow telnet traffic") in the CryptoGuard VPN device, then this protocol is not allowed. This mode is called 'Explicit Mode ON' or 'Firewall Mode' because in this setting a network frame is only passed through the CryptoGuard VPN device in plaintext (By-pass) if explicitly allowed.

The second approach is 'Everything that's not explicitly forbidden is allowed'. This means that every protocol is allowed for which there is no rule in the CryptoGuard VPN device. Thus,

e.g. all telnet traffic is possible in unencrypted form as long as no rule “encrypt telnet traffic” has been set up or until it has been blocked. This mode is called 'Explicit Mode OFF'.

The CryptoGuard VPN device has to be configured in one of these two modes. As with all other configurations, this can be done via the network by the SMS.

With these two possibilities a secure network can be achieved very easily without affecting other running protocols and network mechanisms (some known, some possibly unknown). One starts with 'Explicit Mode OFF' and then sets up and configures rule-by-rule. During the rule setup and configuration the network will for the most part operate as before; only the protocols and connections configured with the rules are affected. Once all known rules have been defined and configured, it is possible to switch to 'Explicit Mode ON' and then check to see if everything runs as expected.

LOGBOOK RECORDS AND SECURITY ALARMS

To get an overview of the network during the operational phase, the CryptoGuard VPN device supports logging of security relevant information in an internal logbook. The logbook can be read and deleted by the SMS. Additionally, the SMS includes several tools to analyze the logged security records. The logbook can be run in three different operating modes, depending on the chosen security policy.

Normally the "**Free Run Mode**" is used. In this mode the logbook operates like a ring buffer. If the logbook is full and there is a new security record, the oldest security record will be replaced by the new one. Thus old security records are lost if there is no save activity by the SMS to read the logbook.

The second mode is "**Single Shot**". This mode will only generate security records in the logbook if enough space is available. Thus, if the logbook is full, no new security records will be written and no old records will be deleted. Security records of new events will be lost.

The last mode is "**Block if Full**". This is normally only used in a highly secure network environment. If the logbook is full and no space is available for additional records, the CryptoGuard VPN device blocks all network traffic until the SMS has read and deleted the logbook. In this mode it is guaranteed that no security record will be lost.

Additionally, the "**Stroke Modus**" button may be activated. This means that the logbook entries are periodically retrieved by the SMS and deleted in the CryptoGuard VPN device as soon as

LOGBOOK

Depending on the chosen security policy different operation modes are available.

the available log book storage space is less than a particular level (e.g., 25%). After receiving this message, the SMS automatically retrieves the logbook. This prevents the loss of security records or blocking of the network traffic by the CryptoGuard VPN device.

Additionally to the security record mechanism, the CryptoGuard VPN device can send a security alert to the SMS each time a security-relevant event occurs. These events are the same as for the security records, but the mechanisms are independent and have to be configured separately.

SECURE SOFTWARE UPDATE

Updates to newer versions or to integrate bug fixes into the CryptoGuard VPN device can be done in the same way as ordinary configurations are done, i.e., by the SMS via the network in a secure way. To increase the security of this extremely security relevant event, the update or patch is protected by the SMS against integrity violations.

REDUNDANCY AND LOAD BALANCING FOR THE CRYPTOGUARD VPN DEVICE

The redundancy concept is based on two or more CryptoGuard VPN devices which are installed in parallel between two switches or routers. All CryptoGuard VPN devices have individual IP addresses and System Master Keys (SMKs) so that they are all accessible by the Security Management Station. All other configuration data is shared by all CryptoGuard VPN devices so that each CryptoGuard VPN device is able to process the network traffic. The CryptoGuard VPN devices have to be installed between switches/routers which are providing standardized redundancy mechanisms (e.g. Spanning Tree Protocol (STP) or Open Shortest Path First (OSPF)). The appropriate protocols have to be bypassed in clear (configured by means of the SMS). The transparency for the Spanning Tree Protocol can additionally be achieved by setting the parameter SPANTREE_MODE=BYPASS in the configuration file of each affected CryptoGuard VPN device.

Load balancing is performed by external network components based on standard load balancing mechanisms which are available in network components like routers (Open Shortest Path First (OSPF)) or load balancers. The appropriate protocols have to be bypassed in clear (configured by means of the SMS).

- | |
|---|
| <ul style="list-style-type: none">✓ REDUNDANCY CONCEPT✓ LOAD BALANCING |
|---|

CRYPTOGUARD VPN SAFETY AND SECURITY FEATURES

INDEPENDENCE OF THE CRYPTOGUARD VPN DEVICE

After installation and configuration, each CryptoGuard VPN device works independently in the network, i.e., the device needs no information about other CryptoGuard VPN devices within the security system. The most important benefit of this feature is, if one CryptoGuard VPN device in a network fails, it will have no influence on the operation of the others.

KEY CONCEPT

For the authentication of the CryptoGuard VPN devices in the SMS System Master Keys (SMK) are used to guarantee a secure communication between the CryptoGuard VPN device and the SMS and to serve for the security within the CryptoGuard VPN device itself.

SMKs are transferred into the CryptoGuard VPN device per smartcard during the personalization phase in a secure environment. Each CryptoGuard VPN device has its own unique SMKs, giving the system a higher security level and ensuring that the SMS can positively identify the CryptoGuard VPN device. As the SMKs are extremely security sensitive, they are stored on the smartcard. It is not possible for unauthorized persons to read the SMKs out of it or to use them.

As the integration steps showed, the SMKs are available at the CryptoGuard VPN devices before the configuration phase starts. The first step of the configuration phase is the authentication and establishment of a secure connection between the SMS and the CryptoGuard VPN device. During the authentication phase the CryptoGuard VPN device and the SMS exchange random numbers. These random numbers are used in combination with the SMKs of the CryptoGuard VPN devices to authenticate each other (challenge-response authentication). After a successful authentication the random numbers and the SMKs are used to calculate a dynamic session key for the SMS – CryptoGuard VPN device communication. Afterwards all data (e.g. configuration data) transferred between the SMS and the CryptoGuard VPN device is encrypted per AES algorithm with the negotiated dynamic session key.

Concerning the key concept for the CryptoGuard VPN Mode of the CryptoGuard VPN device the system is a pre-shared one. The concept is based on two types of keys: On the one hand

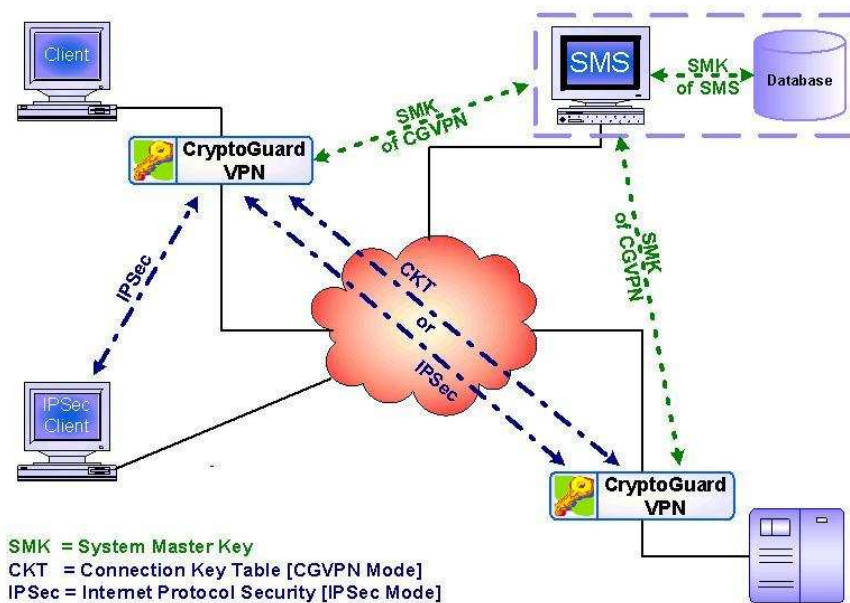
KEY CONCEPT

- ✓ **SYSTEM MASTER KEYS (SMKs)**
- ✓ **CONNECTION KEYS (CKs)**

each CryptoGuard VPN device receives individual **System Master Keys (SMK)** generated by the SMS. These SMKs are also used in the IPsec/IKE Mode. The key distribution has to be done in a secure way. On the other hand the CryptoGuard VPN Mode has **Connection Keys (CK)**.

This second kind of key, the Connection Key (CK), is used to secure the communication between the CryptoGuard VPN devices, i.e. to secure (encrypt) the payload of the network traffic. The CKs are transferred from the SMS to the CryptoGuard VPN device during the configuration phase. They are encrypted with the CryptoGuard VPN device's own SMK and stored in a secure way inside the CryptoGuard VPN device.

The following figure overviews the different use of SMKs and CKs in the CryptoGuard VPN system.

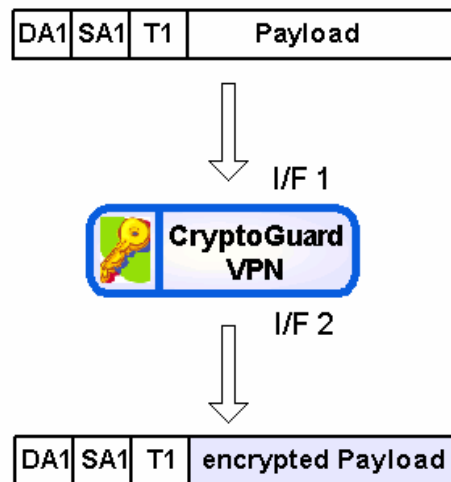


TRANSPARENCY

The CryptoGuard VPN device is designed as a Security Bridge, having two Ethernet / fast Ethernet network interfaces. Each network interface can individually be configured. Like an ordinary network bridge, the CryptoGuard VPN device works on the data link layer of the network and uses the network medium for the network frames. If it receives a network frame, this one will be transferred to the packet filter. The packet filter firstly tests the frame by means of a bridge algorithm to see if it is

intended for a receiver at another network interface. If not, the frame will be dropped; otherwise the received frame is further processed.

After processing (e.g. encrypting), the frame is transmitted to the second network interface, keeping its network addresses (depending of the layer that was encrypted) and its original frame length.



The above figure illustrates this mechanism for an Ethernet frame. The packet filter rule in the CryptoGuard VPN device is in this example defined such that the payload of all network frames with an Ethernet destination address DA1 and an Ethernet source address SA1 containing a payload of type T1 has to be encrypted (in reality, this could mean to encrypt all IP traffic between two network devices). Destination address, source address, filed type and the frame length remain unchanged.

PACKET FILTER OPPORTUNITIES AND ATTRIBUTES

The principle concept of the packet filter consists in that it tests the received network frames for a security policy, the Connection Control Table (CCT). If there is a match for a network frame in the CCT, this frame is processed as defined in the CCT.

After the filtering several possibilities are available for the further processing of a frame. If a network frame matches one of the rules in the CCT, the next step is to determine how to handle it:

**PROCESSING OF
NETWORK FRAMES**

- ✓ Encryption
- ✓ Blocking
- ✓ Bypassing

- **Encryption** of the matching network frame. This mode is independent of the "Explicit Mode". The CCT contains additional information indicating which part of the data of a network frame the CryptoGuard VPN device has to encrypt. Thus, the encryption can be done at different network layers, depending on the definition for this rule in the CCT. The encryption is length transparent, which means that there is no data overhead in the network by the CryptoGuard VPN Mode encryption. To give encrypted data with a higher security level, a dynamic component is used during the encryption, e.g. encrypting the same data more than once results in different cipher texts.
- **Blocking** the network frame matching the CCT. This processing mode can also be used to establish a simple firewall system with the CryptoGuard VPN Mode and only makes sense when used in combination with the "Explicit Mode OFF" feature.
- **Bypassing** the matching network frame in plain text through the CryptoGuard VPN device if the frame matches the CCT. This processing mode can be used to establish a simple firewall system with the CryptoGuard VPN device. This mode only makes sense when used in combination with the "Explicit Mode ON" feature.

MULTI NETWORK LAYER PROCESSING

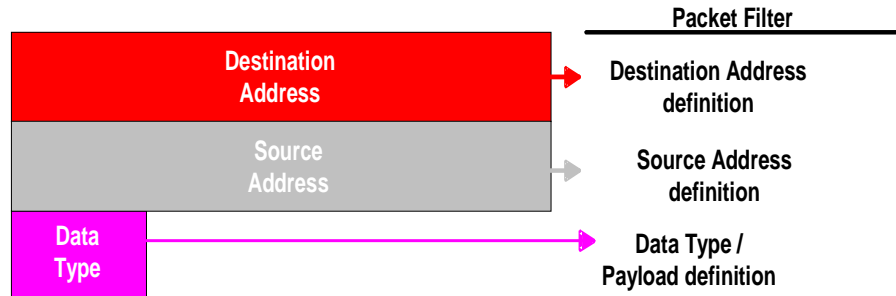
Filtering is possible on addresses, protocols, protocol attributes, weekdays and times of day. The addresses, protocols and protocol attributes always have to be seen in combination with the network layer (2, 3 or 4) that is used for this filter rule.

The next figures describe this behavior in more detail.

Layer 2 processing

At layer 2 filtering (and encryption) is possible for DIX2 network frames (also IEEE 802.3 and IEEE 802.2 network frames can be filtered/encrypted). The following figure shows a DIX2 network frame and the frame fields which can be analyzed by the packet filter. Encryption is possible for the MAC data part of the network frame.

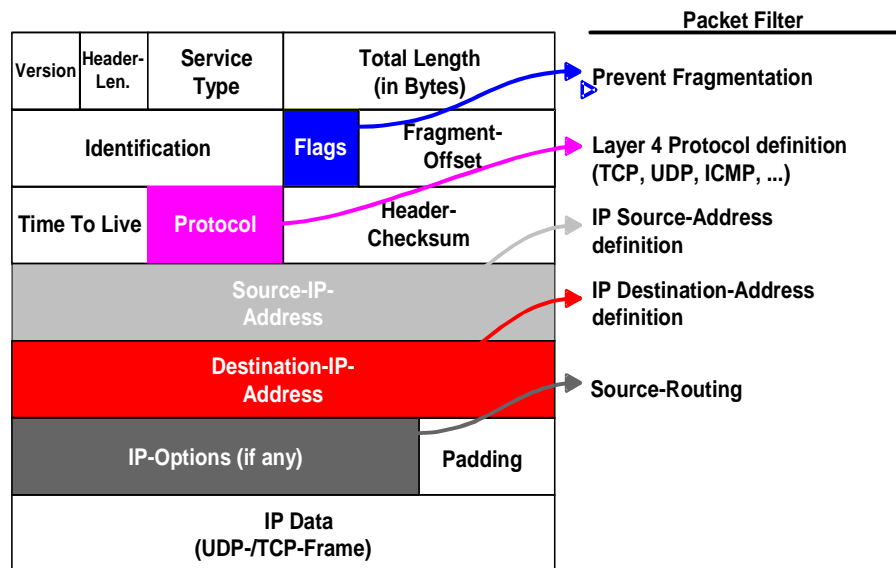
Ethernet MAC (DIX2)



Layer 3 processing

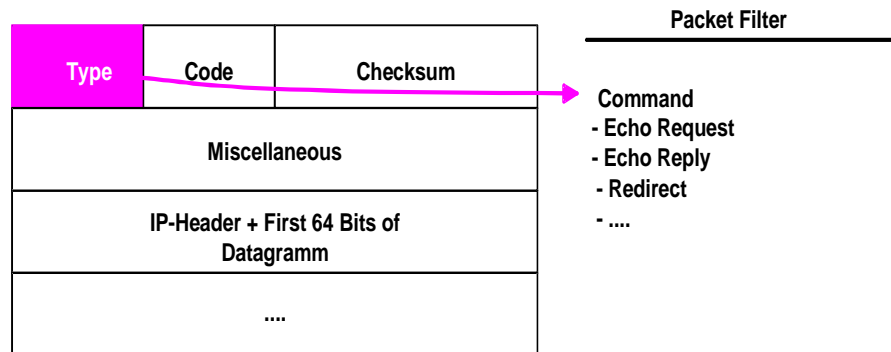
At layer 3 filtering is possible for IP and ICMP network frames. The following figure shows an IP network frame and the frame fields which can be analyzed by the packet filter. Encryption is possible for the IP data part of the network frame.

IP-Frame



The following figure shows an ICMP network frame and the frame fields which can be analyzed by the packet filter:

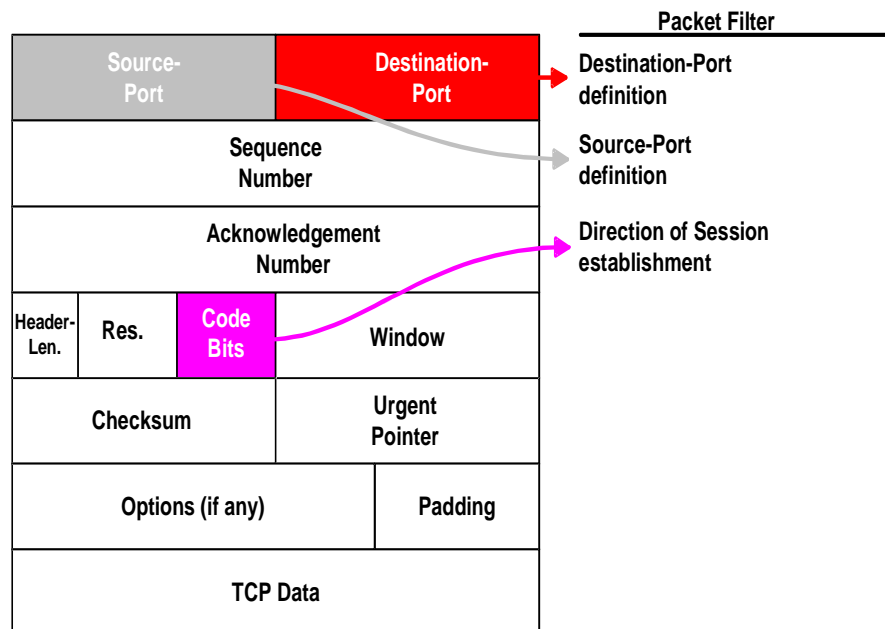
ICMP



Layer 4 processing

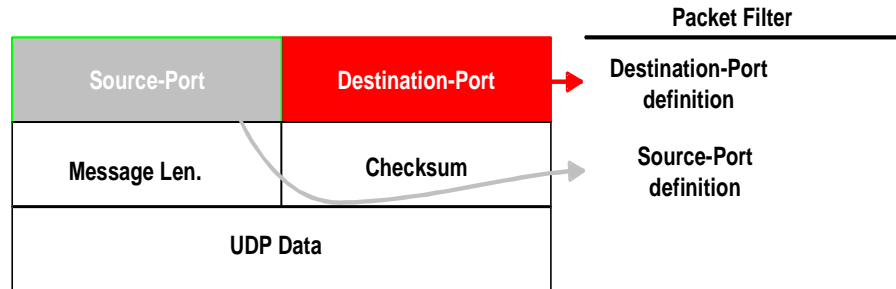
At layer 4 filtering is possible for TCP and UDP network frames. The following figure shows an TCP network frame and the frame fields which can be analyzed by the packet filter. Encryption is possible for the TCP data part of the network frame.

TCP-Frame



The following figure shows an UDP network frame and the frame fields which can be analyzed by the packet filter. Encryption is possible for the UDP data part of the network frame.

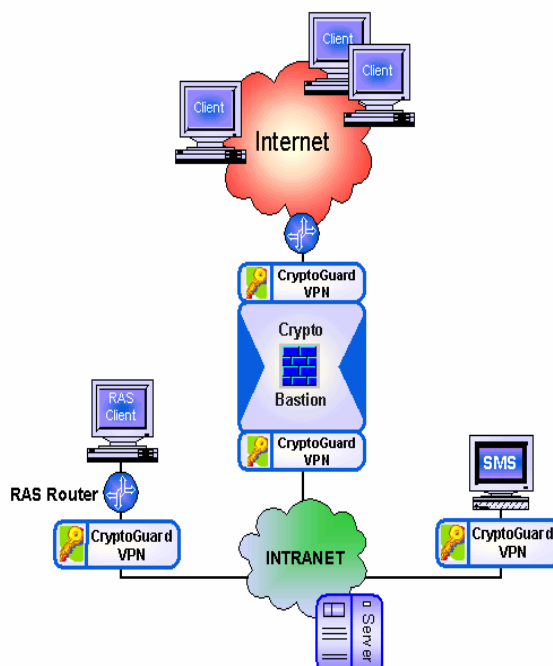
UDP-Frame



EXAMPLES OF PRACTICAL APPLICATIONS

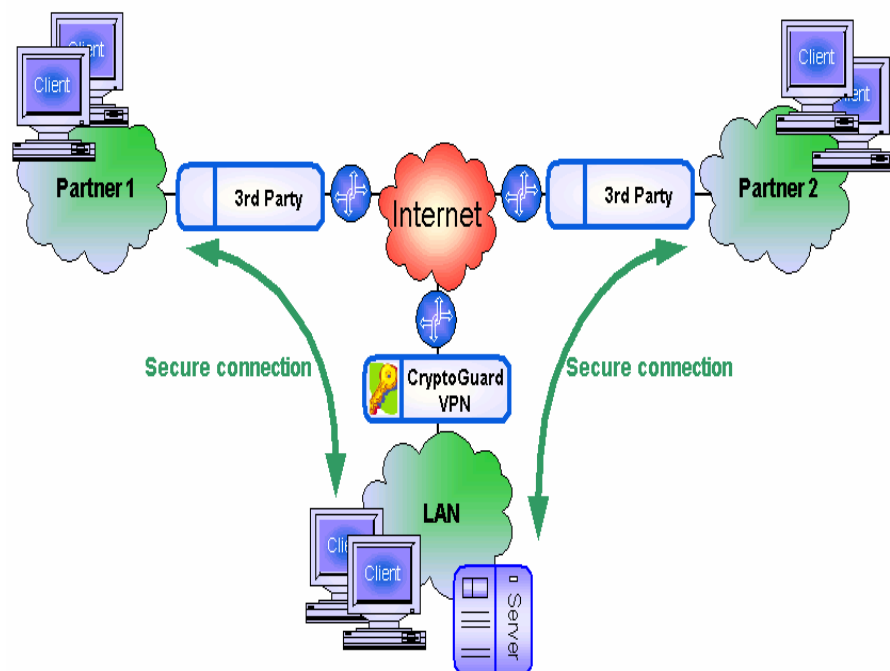
REMOTE ACCESS VPN

The following figure shows a typical "Remote Access (RAS)" VPN via an insecure network. The "Internet Clients" connect to the external CryptoGuard VPN device of the "High-Level Firewall System". The external CryptoGuard VPN devices act as VPN gateway for the clients. Another possibility for a RAS connection is the access from a "RAS Client" to a RAS router. The RAS router handles the network access and the following CryptoGuard VPN device realizes the secure communication. Typical applications in such an environment are data base access and central e-mail services.



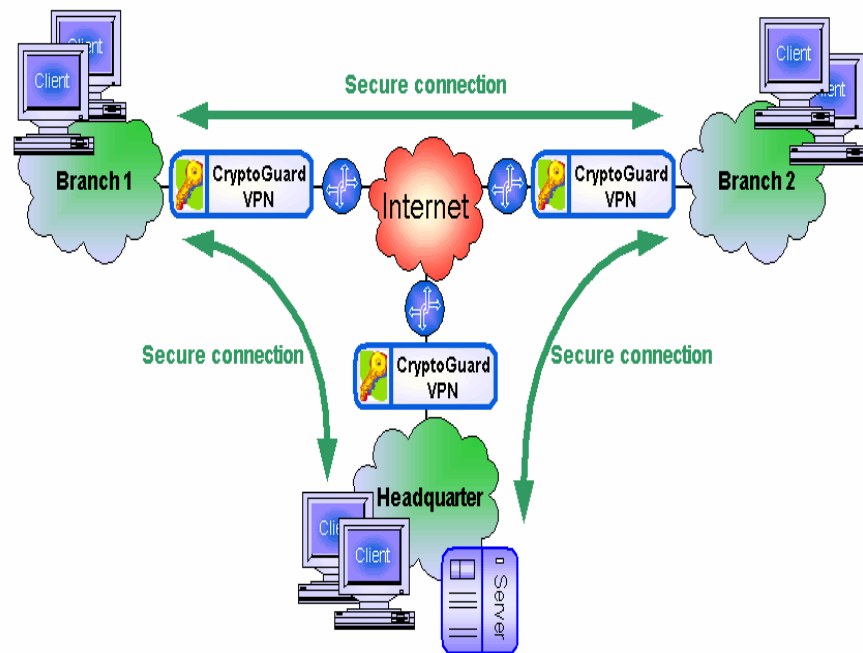
EXTRANET VPN

Extranet VPNs provide a secure and confidential data exchange between business partners. A secure tunnel is established between the VPN gateways of the partners. As each partner prefers a different VPN gateway product, all partners have to use a VPN standard. Today the standard is IPsec/IKE. An encrypted and authenticated tunnel is established between the 3rd party VPN gateways and the CryptoGuard VPN device. Typical applications in such an environment are access to price lists and technical datasheets using the WWW protocols. The following figure shows a simple example of an Extranet VPN.



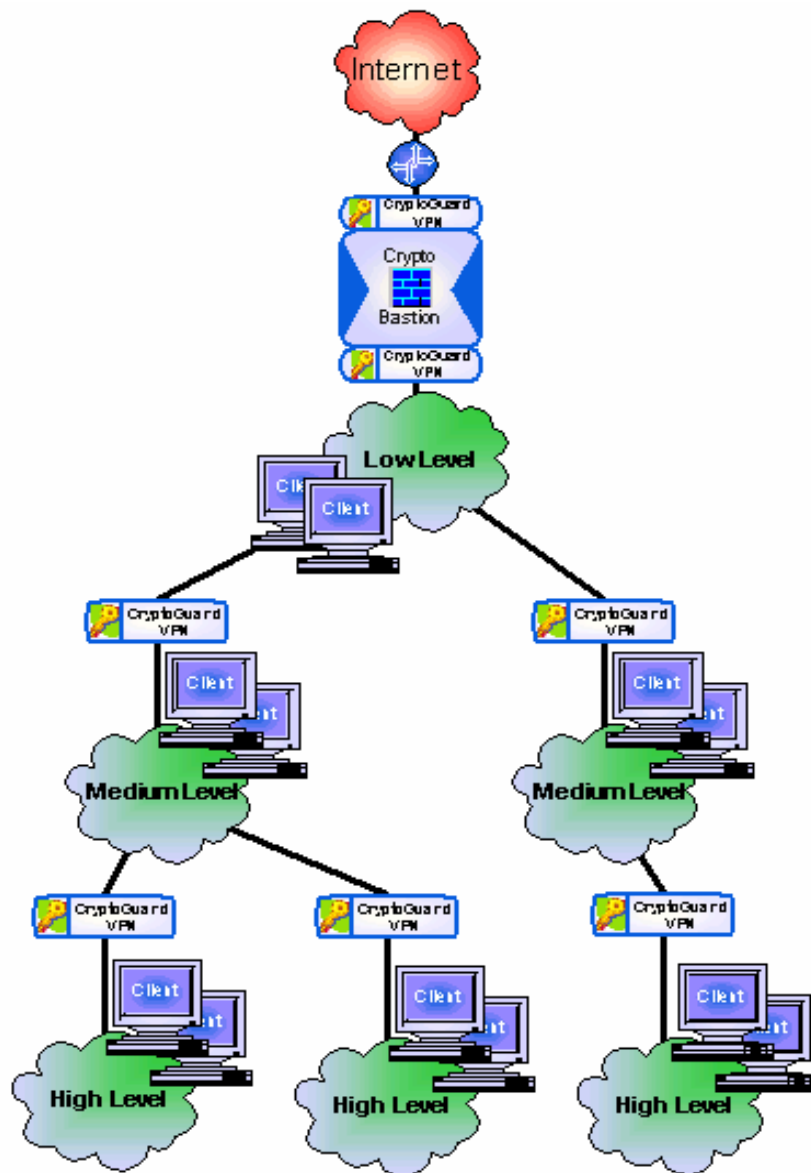
BRANCH OFFICE VPN

Branch Offices should be able to communicate without restrictions with the head office. Usually dedicated lines are used for this kind of connection. These lines are typically leased from a network provider. The provider guarantees the availability of the network, but not the security of the transferred data. To integrate security in the branch office connection, VPN gateways have to be situated at a point in front of the provider router. This guarantees security and confidentiality for the entire network traffic between the branch offices and the headquarters.



INTRANET VPN

An enterprise network can be divided into different areas such as the management, development or finance departments. The communication within an area is assumed secure, that between areas is assumed to be insecure. To secure the communication between the areas, the corporate network has to be examined more closely. What is seen is a collection of networks, connected in a defined structure. Security can be integrated into this network by implementing a VPN system. The following figure shows an example of such an Intranet VPN.



CONCLUSION

The basic VPN use cases given above demonstrate how easily a VPN can be established with the CryptoGuard VPN system. The CryptoGuard VPN system is independent of the existing network infrastructure. It supports standard VPN interfaces (IPsec/IKE) to 3rd party VPN components. The CryptoGuard VPN device can easily be extended with the CryptoBastion to a high-level firewall system.

ABBREVIATIONS

3DES	Triple D ata E ncryption S tandard: symmetric encryption algorithm defined in ANSI X9.52.
ADES	A lternating D ata E ncryption S tandard: mode of DES which is included in CryptOn. This modified algorithm uses extended keys with a length of 16 bytes and two different sets of s-boxes in parallel.
AES	A dvanced E ncryption S tandard: symmetric crypto system that has been announced as follower for DES resp. 3DES in 2000.
AH	A uthentication H header: IPsec authentication mechanism.
CCT	C onnection C ontrol T able: Security policy (filter rules and processing attributes) for the CryptoGuard VPN device.
CG VPN	C rypto G uard V PN: product to secure network communication.
CK	C onnection K ey: Key that is basically used for the encrypted communication between two CryptoGuard VPN devices.
CryptOn	Hardware module for encryption and secure key storage, product of the Compumatica secure networks.
DES	D ata E ncryption S tandard: Encryption algorithm defined by FIPS publication 46, 1977.
DH	D iffie- H ellman: Key exchange protocol, developed by Whitfield Diffie and Martin Hellman.
ESP	E ncapsulating S ecurity P ayload: IPsec encryption mechanism.
IETF	I nternet E ngineering T ask F orce: Organization that defines the standards used in the Internet.

IKE	I nternet K ey E xchange: A protocol defining how to exchange keys for IPsec communications.
IPComp	I P Payload C ompression Protocol
IPsec	I P security: A standard which defines various security services for traffic at the IP layer.
LAN	L ocal A rea N etwork: Any physical network technology that spans short distances (up to a few thousand meters).
OSPF	O pen S hortest P ath F irst
SA	S ecurity A ssociation
SK	S ession K ey: key that is calculated during authentication between SMS and CG VPN. The key is used for the encryption of the communication between SMS and CG VPN.
SMK	S ystem M aster K ey: Individual key of a CryptoGuard VPN device that is used to secure the communication between the device and the SMS and to secure the CryptoGuard VPN internal data.
SMS	S ecurity M anagement S tation
STP	S panning T ree P rotocol
VPN	V irtual P rivate N etwork: Method of communicating via a public network using encryption, so that only participants that share the necessary keys are able to communicate.
WAN	W ide A rea N etwork: Any physical network technology that spans large distances.

FURTHER INFORMATION

SHORT PROFILE

Compumatica secure networks – based in Germany and the Netherlands – is a fully independent private company with main task securing IP traffic of its customers. Compumatica develops, produces and implements high level security solutions for all types of IP networks and all types of customers. These can be small organizations with just a few countrywide connections up to international enterprises with world-wide networks. Compumatica staff and products meet high standards of reliability and quality. The products are based on systems that are approved, or even certified, according to the strict regulations of the BSI (in Germany) and the NLNCSA (in the Netherlands). Every single product goes through a quality assurance phase in which it is subject to a long-term test. All Compumatica products are backward compatible for more than ten years. Herewith we guarantee our customers investment protection. Our customers are well-known top 500 enterprises as well as government agencies and public organizations in different countries which protect their critical data with the aid of Compumatica systems.

As world-wide approved producer and system integrator *Compumatica secure networks* provides complete IT security solutions for networks of each size.

The security of your data is our mission – *we secure YOUR network.*

CONTACT DATA

Germany:

Compumatica secure networks GmbH
Germanusstraße 4

52080 Aachen

Phone +49 (0)241 16 96 400

Fax +49 (0)241 16 96 410

www.compumatica.eu



The Netherlands:

Compumatica secure networks bv
Oude Udenseweg 29

5405 PD Uden

Phone +31 (0)413 334 668

Fax +31 (0)413 334 669

www.compumatica.eu

