genua
A Bundesdruckerei Company

genuscreen

Firewall and VPN Appliance

Technical Information

genua A Bundesdruckerei Company

Table of Contents


1 genuscreen: Firewall and VPN Appliance

Data exchange between various locations via the Internet is cost effective and easy, but must be reliably protected from eavesdroppers and prying eyes. In much the same way, your network also needs to be shielded from Internet hazards. A major requirement is providing secure zones for especially sensitive systems within large networks. Our Firewall & VPN Appliance genuscreen was developed exactly for this purpose – a security solution that creates strongly encrypted virtual private networks (VPN) for data communication via public networks. Sensitive information can be transferred via these connections with high security.

In addition, the high performance genuscreen firewall strictly filters data traffic at the interfaces, and only forwards expressly permitted connections. All other requests are dropped without exception.

The Firewall & VPN Appliance genuscreen has been officially tested to comply with the highest security standards. It has been approved for the encrypted transmission of data up to the German classification level Restricted, and certified to the level EAL 4+ according to Common Criteria (CC).

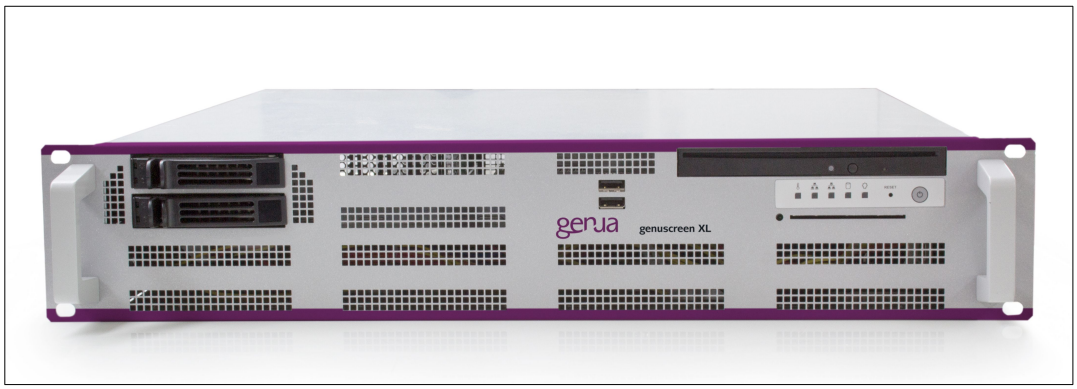

Fig. 1: Rack server solution genuscreen XL

On the following pages you will find a summary of the functions and possible applications for the Firewall & VPN Appliance genuscreen.

2 Firewall

genuscreen offers a stateful packet filter.

2.1 Features of the Packet Filter

Stateful Tracking

Individual connections are examined according to a number of criteria. These include:

- the number of connections per source IP address
- the number of connections over a given time period
- the number of source IP addresses that make connections

DOS Protection

Incomplete TCP connections are made from an IP address during a denial of service attack. genuscreen protects against DOS attacks by only forwarding packets that have been transmitted after a full TCP connection has been established.

Spoofing Protection

Attackers using false source IP addresses can carry out attacks on networks without revealing their true location. Alternatively, they can obtain access to network services that are reserved for particular IP addresses. The genuscreen firewall provides you with the possibility of protecting yourself from such attacks.

TCP Flag Filtering

TCP packets can be checked and filtered on the basis of the TCP flags.

Global IPv6 Switch

This function allows all IPv6 traffic to be blocked.

2.2 Packet Normalization

Some applications – but also attackers – generate IP packets that cannot be clearly interpreted. One example is a self-excluding combination of flags in a TCP header, such as SYN and RST or SYN and FIN.

Packet normalization is used to clean up packet contents and ensure that there is no ambiguity when interpreting the contents on the receiver side.

TCP packets with invalid flag combinations are thrown away and fragmented packets combined. Packet normalization provides a defense against a number of types of attack, such as IP fragmentation attacks that are made using overlapping fragments.

Some of the most important packet normalization functions are:

- fragmented packets are combined
- duplicated fragments are discarded
- overlapping fragments are cut off
- time stamps in TCP headers are modulated with a random number

2.3 Network Address Translation (NAT)

The number of public IP addresses under the IPv4 protocol that are still free is becoming less and less. It is therefore necessary to use private IP addresses in internal networks. However, so that the Internet can be used for communication these private addresses need to be translated into public ones using a NAT process (Network Address Translation).

NAT is implemented in the Firewall & VPN Appliance genuscreen, which supports the following functions:

Redirection

Redirection makes it possible for incoming traffic to be sent to a machine behind a NAT gateway. This enables services to outside – i.e. to the Internet – to be provided.

1:1 Mapping

A 1:1 mapping can be defined between an internal IP address and an external one in order to, for example, explicitly bind the service of a web server from the internal network with its external address.

2.4 Dynamic Protocols

One feature of dynamic protocols is dynamic port allocation. This means that a connection will not always be allocated to a particular port. This can lead to problems with NAT, amongst others, because the dynamically allocated ports cannot be assigned to already established connections. In addition, this can also mean that a larger port range needs to be opened, thereby creating a potential security weakness. genuscreen supports specific dynamic protocols in order to avoid this problem. These include:

- SIP for VoIP
- FTP for data transfer

3 VPN – Virtual Private Network

The genuscreen can establish high performance VPN networks to allow secure data transmission across the Internet, only using strong encryption algorithms and long encryption keys.

The genuscreen provides the following methods of establishing VPN networks:

- Transport mode by genua
- VPN tunnel with IPSec in bridging mode
- Connection of mobile devices using L2TP or IKEv2
- VPN tunnel for TCP connections via SSH

3.1 IPSec in Routing Mode (Layer 3)

The Firewall & VPN Appliance genuscreen can be used as a Layer 3 based IPSec gateway. The connection can be established using NAT traversal if the genuscreen is behind a NAT router. UDP port 4500 is used for the VPN connection with NAT traversal. Partners can communicate without a direct, transparent IP connection having to be established.

ISAKMP/OAKLEY is used for the Internet Key Exchange (IKE) between genua appliances.

With IPSec, a Security Association (SA) is negotiated for each combination of host and network. This means that a large number of hosts/networks will result in many more SAs, each of which will tie up resources at the VPN gateway. Alternatively, if it is necessary to

reduce the number of SAs, an IPSec connection can be established and operated through an IP-in-IP tunnel (gateway-to-gateway) in transport mode.

In network mode the communicating partners are no longer addressed individually by the genuscreen but grouped together behind the target gateway. This considerably reduces the number of Security Associations that have to be negotiated and results in both improved performance and scalability.

3.2 IPSec in Bridging Mode (Layer 2)

genuscreen can be set up to function as a VPN gateway without long downtimes and configuration changes to the logical IP address structure. This is done using the bridging mode, where genuscreen is (invisibly) integrated into an existing network on Layer 2 and transferred data is transparently encrypted.

3.3 Connection of Mobile Devices Using L2TP and IKEv2

genuscreen is able to receive VPN-connections of mobile clients using L2TP and IKEv2. This allows for the trouble-free connection of smart-phones and tablets to your networks. All connections to genuscreen are permanently secured by IPsec.

3.4 VPN over SSH Port Forwarding (Layer 4)

SSH (Secure Shell) allows the tunneling of additional authenticated and encrypted TCP connections.

The algorithms that are used in the genuscreen for authentication and encryption are cryptographically strong and just as secure as those used in IPSec. In addition, the SSH protocol can be much more flexibly used than IPSec for example, for connections through firewalls and NAT routers.

On the one hand, the manual aspect of establishing SSH connections increases the unlikelihood of misuse while on the other SSH only allows TCP connections to be forwarded through specifically enabled tunnels. However, the absence of “routed” connections gives SSH a security advantage over IPSec.

It is also interesting that overlapping networks with the same IP range can be coupled quite straightforwardly using SSH VPN connections.

4 Additional Features

4.1 Bridging

One of the main features of the Firewall & VPN Appliance genuscreen is the simple integration in existing network topologies via bridging.

In its bridging mode, the genuscreen is invisibly integrated into a network on layer 2 without other changes being required in the existing LAN structure. This means that neither existing logical address schemes need to be resolved, new IP addresses allocated nor routing settings changed.

The simple integration allowed by the bridging function applies for use of the genuscreen as a firewall and as a VPN gateway. This in turn means that invisible barriers against attackers can be implemented. genuscreen can also be used as an invisible gateway for the encrypted exchange of data. The full functionality of the firewall or VPN gateways is retained when the genuscreen is in bridging mode.

4.2 Different Topologies

The network topology is crucial for the performance, as well as the reliability of a network: Only if alternate paths between the nodes exist, full functionality is retained when individual connections break down.

genuscreen allows you to realize the network topology suitable for your infrastructure, for example fully meshed or star (even using multiple central gateways).

4.3 SIP Module for Securing IP-Based Communication

The Session Initiation Protocol (SIP) plays a key role in Voice-Over-IP communication, which is being widely introduced as a requirement of developments such as All-IP. As these new technologies also bring new attack vectors with them, IT security has to develop comprehensive solutions to guarantee secure operation. The SIP module is available as a genuscreen option. It uses a rigorous specialized test procedure to ensure data communication is only allowed after the connection has been fully analyzed and found to be secure. The SIP module can also be used for SSL/TLS connections. The module uses Session Border Control (SBC) functions to prevent attacks against telephones and telephone systems, and allows the implementation of security guidelines. In addition, the SIP module ensures interoperability of systems that for example use different encryption standards, as well as simplifying certificate administration.

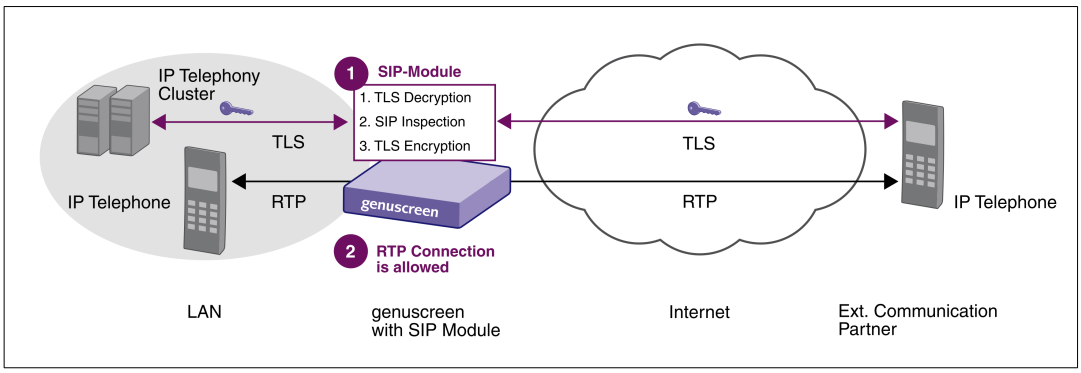

Fig. 2: Checking encrypted SIP with the genuscreen

4.4 Bandwidth Management (QoS)

The firewall can also handle spoken communication and secure the widely used SIP VoIP protocol. Since reliable performance is key for VoIP, our product features highly refined bandwidth management.

However, VoIP is not the only application for which the smart management of the available bandwidth is indispensable. genuscreen can prioritize important protocols in the data transfer on demand.

The bandwidth of the network connection is divided into different queues. Depending on certain criteria (source address, target address, port, protocol) the traffic is allocated to the different queues. Varying priorities can be assigned to these queues, which makes it possible to process interactive traffic (such as SIP), before non time-critical traffic (such as web traffic).

4.5 Virtual Routing

genuscreen supports virtual routing and thereby multiple instances of a routing table on a single item of hardware. The routing instances are independent of one another so identical or overlapping IP addresses can be used – clearly separated from one another and without conflicts.

This means that, for example, a single genuscreen can be used to route a number of networks with the same IP range into different virtual routing domains (VRDs). Individual VRDs are strictly separated from one another so that, for example, an administration interface can be reliably isolated and access from other domains prevented, even in the event of a configuration error.

4.6 High Availability

genuscreen can flexibly scale and realize high availability solutions.

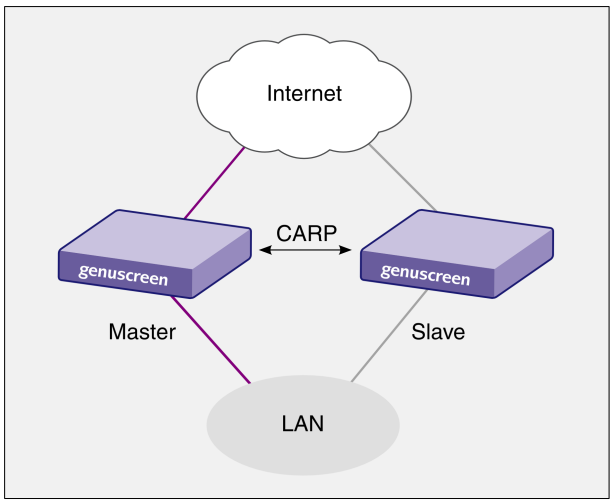

Fig. 3: genuscreen in hot standby operation

Hot Standby Operation

Master-slave configurations with two or more appliances are used to avoid downtime, making the exchange of an appliance possible without loss of function. The Common Address Redundancy Protocol (CARP) is used to control the interfaces: Should the master fail then

the or rather a slave will take over the virtual CARP address of the master. The takeover time of less than two seconds is extremely short.

4.7 Forward Compatibility with IPv6 Integration

The rapid growth of the Internet and the restrictions that come with the IPv4 protocol lead to bottlenecks that should be reduced with IPv6. With the increase in address capacity the chance was also taken to adapt the Internet protocol to modern requirements.

The changeover of the Internet to IPv6 is underway and will accelerate in coming years. In between times there are areas in the Internet that can only be reached with IPv6, others that can be reached with both protocols and large areas that are exclusively based on IPv4.

This has implications for your IT infrastructure: For example, firewall filter rules have to be rewritten for IPv6. The behavior of a firewall that cannot explicitly handle IPv6 traffic cannot be exactly predicted.

genuscreen takes account of these developments and can securely handle both IPv4 and IPv6 protocols. With genuscreen you are investing in a product that corresponds with today's standards – and those of tomorrow.

4.8 Suitable for Almost any Operational Environment

Encompassing such enterprise features as logging on syslog servers, and monitoring using SNMPv3 or Netflow, genuscreen is suited for operation in large corporate networks.

An interesting feature for smaller networks: genuscreen offers a separate DHCP server allowing you to assign dynamic IP addresses to client computers – no additional hardware necessary.

5 System Management

5.1 Central Management via genucenter

The configuration and administration of any number of genuscreen appliances can be carried out with the simple to operate genucenter Central Management Station user interface.

The genucenter has the following features:

Rollout Management

The rollout management provided by the genucenter enables the initial set-up of a large number of systems with a particular configuration and software.

Central Configuration and Software Management

genucenter provides a central source for software and configuration updates. These are either loaded from genuscreen automatically (pull) or on request (push) and allow the simple and comfortable administration of a large number of systems.

- Central Configuration Management
  The genucenter user interface provides a summary of the current configuration of the systems. Profiles can be used to allow systems with the same purpose to be configured at the same time.
- Central Software Management
  genucenter allows systematic updates of individual devices.

Central Monitoring

genucenter can monitor individual genuscreens, clearly presenting the following information:

- accessibility
- problems
- system state

Central Logging for all genuscreens

- genucenter offers a central database for saving configuration, state and log information of all appliances as well as for their analysis. The possibility of securing the database and restoring it is provided by a backup function.

Multi-client capability

- genucenter is multi-client capable, allowing for the creation of system groups with diverse deployment characteristics.

Reliability

- genucenter allows for redundancy, in order to apply updates and changes to the configuration without experiencing down times.

5.2 Decentralized Management

Naturally, it is also possible to administer every genuscreen separately. In this case, the administrator has the following possibilities:

Configuration via web interface

- The genuscreen can configured and administered via a secure https based connection and a well laid out and comfortable web interface.

Direct access

- Alternatively, the genuscreen can be configured using a SSH connection and console interface.

5.3 Analysis and Debugging

Full access to genuscreen is always possible via a secure SSH connection, allowing administrators to use a number of analysis, tracing and debugging tools. genuscreen comes with a number of tools for recognizing and analyzing network and system problems.

These include:

- tcpdump for traffic analysis
- IPSec debugging
- Network debugging
- Network probing
- Analysis in local networks
- Detailed log analysis

6 Certification and Approval

6.1 Certification

genua applies for certification according to international standards for important products, in order to demonstrate the quality of the security functions that have been implemented. This also means that the products can be used in environments with the highest security requirements.

The Firewall & VPN Appliance genuscreen 5.0 has been certified according to Common Criteria (CC) at the EAL 4+ level. Testing at the German Federal Office for Information Security (BSI) involved handing over comprehensive documentation and the source code as well as extensive tests – and it provides our customers with the assurance that they are buying a top quality security solution.

6.2 Approval

In contrast to certification, approval cannot be applied for by the manufacturer. Approval procedures are started by the state, when members of a public authority wish to use a product. The application is made by a public sector consumer and the approval is processed and granted by the BSI.

Genuscreen 7.4 has been granted approval by the BSI for encrypted data transfer with IPSec up to the German VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) level, and for the NATO Restricted, and RESTREINT UE/EU RESTRICTED levels. According to the new directive for classified information (Verschlusssachenanweisung), the approval includes the firewall functions in addition to the VPN.

Please feel free to contact us for further information about certification and approval. We will be pleased to offer you more comprehensive information.

7 Hardware

We supply different hardware models – from the maintenance-free model without cooling fan and hard disk through to a range of rack-mounted server solutions. You will find more detailed hardware information under www.genua.de/genuscreen.

8 Application Scenarios

8.1 genuscreen as a Zone Firewall

Many company networks are connected to the Internet via an Internet firewall, with the internal LAN having a largely flat hierarchy and no further security transitions. In such situations many of the internal users often have more permissions than they actually need. A considerable improvement in the internal security can be achieved when the LAN is divided up into physically separated zones. This can be achieved using the genuscreen.

The existing network structure can be fully retained if a bridging packet filter is used as a firewall. The firewall is simply integrated at the appropriate point in the network to separate off the zone.

A number of possible applications are shown in the following diagram. Here a SAP-Server, the personnel department and a subsidiary are each separated from the internal LAN by a genuscreen firewall. This scenario means, for example, that clients from the internal LAN are no longer able to access the data from the personal department. The subsidiary network is physically separated and its users can only perform tasks in the central internal network that they have been specifically allowed. This, of course, also applies for users of the internal LAN.

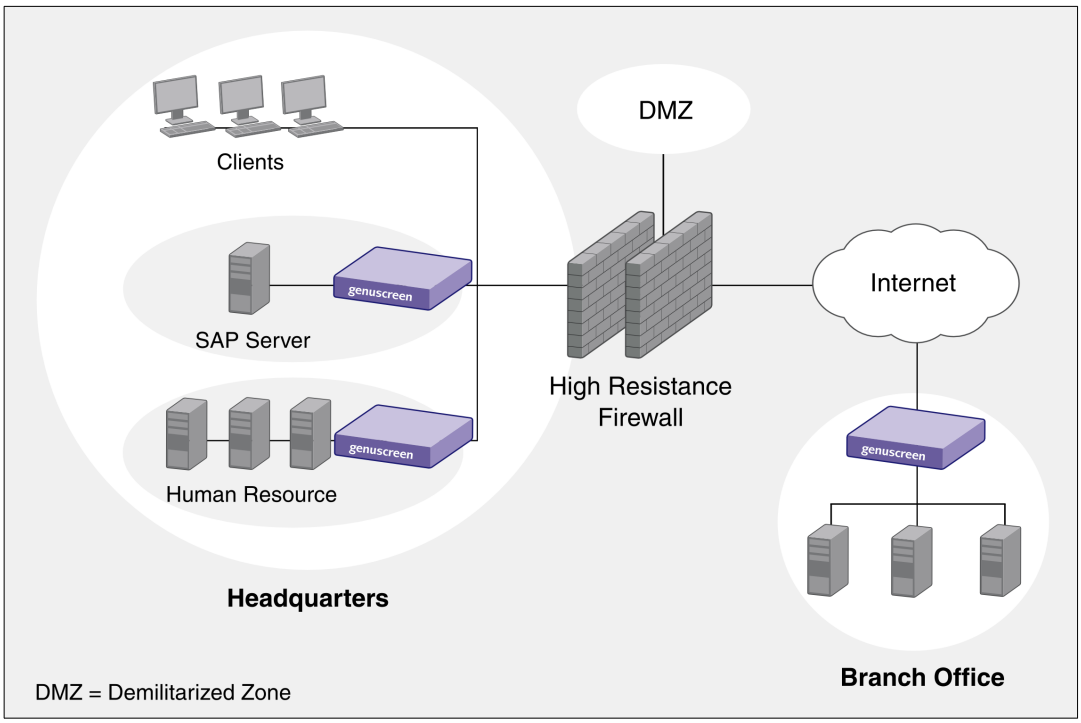

Fig. 4: Creating zones with genuscreen

8.2 Transparent Coupling Through an Encrypted Network

The configuration of a VPN almost always involves a considerable effort. It is not only the settings for the VPN gateway or those of the network itself but the changes in the logical IP address structure of the affected LANs that have to be implemented. The following steps have to be taken when a network that is to be able to communicate through a VPN gateway:

- new default (VPN) gateways defined
- IP addresses set for the gateway
- possibly new network masks set

This means that the network will not be reachable over a longer period of time or that connections within the network cannot be established.

Implementing genuscreens as bridging VPN gateways provides a solution to this problem.

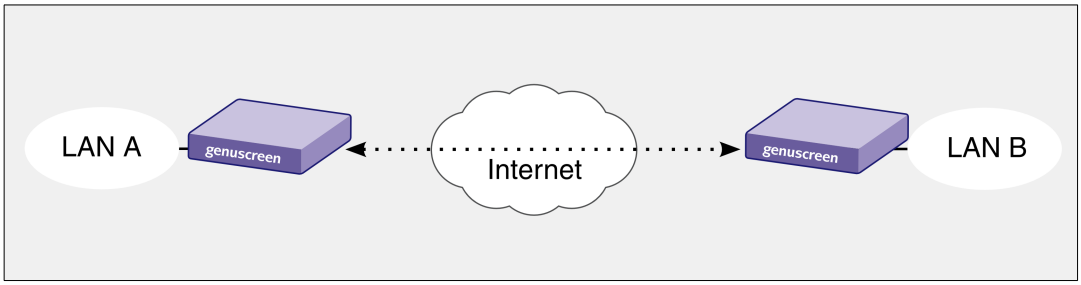

Fig. 5: genuscreen as bridging VPN gateway

The advantage: The result is a full-fledged VPN connection between LAN A and LAN B. This connection is completely transparent for both networks and does not require any configuration in LAN A or LAN B. Therefore an encrypted connection can quickly be established through public or unencrypted networks.

8.3 Using the Network Mode to Avoid a SA Bottleneck

Data that is important for VPN relationships is exchanged in a Security Association (SA), including:

- a security identifier – an unambiguous 32-bit number
- a key for encrypting the data
- the number of packets that have already been exchanged via this SA

A SA is normally established between all networks or hosts. A SA bottleneck can easily be formed when communication occurs between numerous partners as each permutation of network/hosts requires its own SA. This leads to, amongst other things, a decrease in performance at the VPN gateways, as the negotiation of SAs requires a lot of computing time. SAs are administered in the Kernel, in the SAD (Security Association Database).

As SAs are renegotiated at very short intervals, many SAs will be duplicated, with the duplicates also having to be continually renewed. The length of time that a SA is valid can be increased but this brings a security risk and a reduction in the level of security.

This situation is shown graphically in the diagram below. Three networks are shown, each behind its own VPN gateway. SAs have to be negotiated and administered for all networks – that is, for the relationships A1-B1, A1-B2, A1-B3, A2-B1 etc. This results in 18 SAs per gateway.

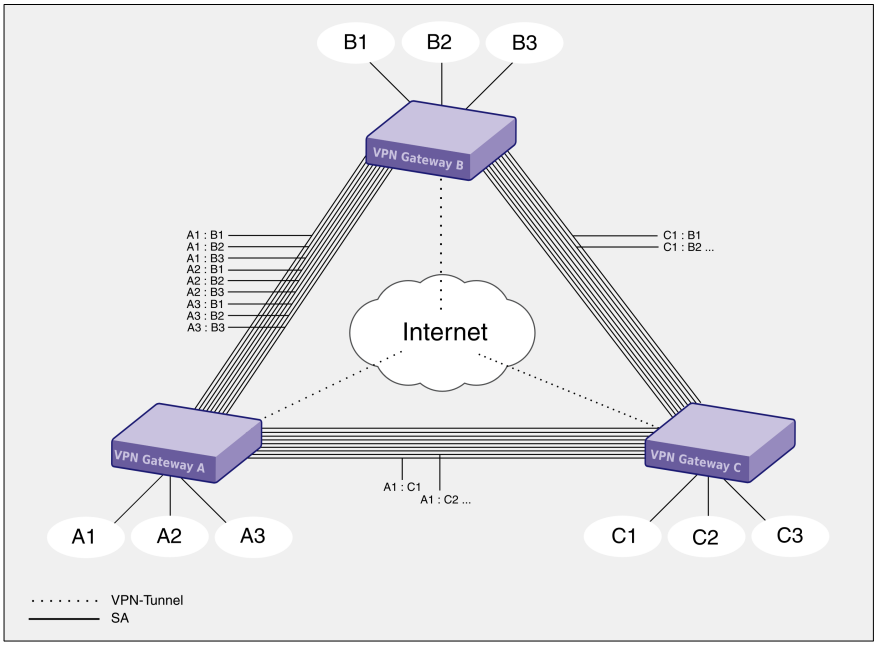

Fig. 6: Example of a SA bottleneck

genuscreen allows such SA circles to be avoided as it negotiates with other gateways and not with individual VPN partners. This means that in the example scenario described above only three relationships need to be negotiated and maintained and not 27. This is shown graphically in the next diagram and provides a clear advantage for organizational structures that are strongly or fully meshed.

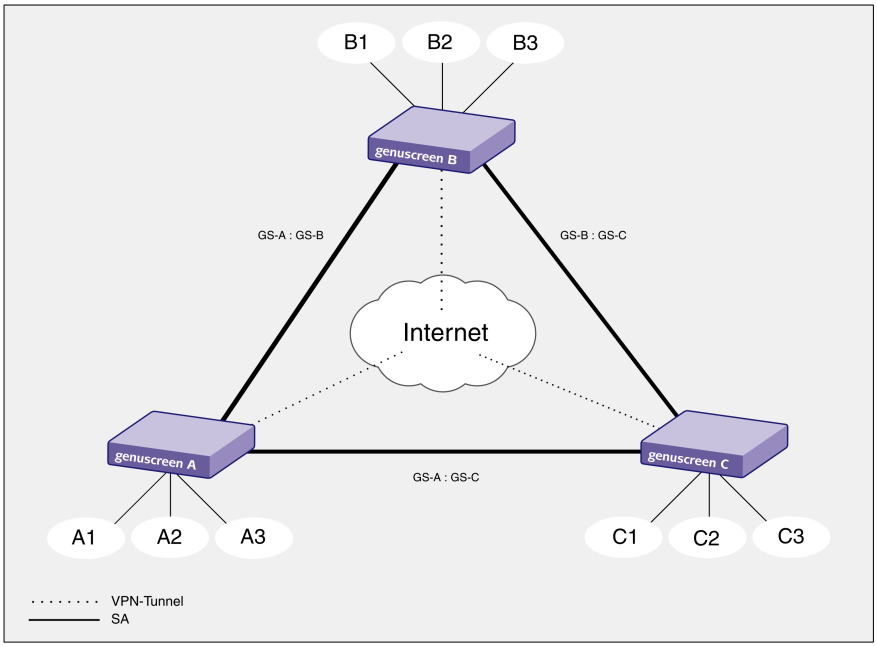

Fig. 7: Avoiding a SA bottleneck using genuscreen

8.4 Operation in Classified Environments

The Firewall & VPN appliance genuscreen is approved for processing and transferring encrypted data with IPSec up to NATO Restricted and UE Restraint Restricted levels.

9 Support

9.1 Introduction

Installation and configuration service: genua and its specialist sales partners will support you if you wish during the installation, configuration and commissioning of your Firewall & VPN Appliance genuscreen and Central Management Station genucenter. At the same time your administrators will be given thorough instructions in the use and maintenance of the system.

9.2 Training

genuscreen Specialist Training: This training provides administrators with detailed information about the construction and functioning of the Firewall & VPN Appliance genuscreen as well as knowledge of the configuration options and how operational systems can be monitored.

9.3 Software Support for Operational Systems

Update Service: The Firewall & VPN Appliance genuscreen is under continual development, with new versions incorporating current developments and useful new functions appearing regularly. Intermediate versions may also be released if necessary.

Our update service ensures that the newest versions will automatically be delivered to you and that you will have access to our full patch data base.

Hot-line Service: In addition to our update service, we provide e-mail and telephone support in German and English. You can use our hot-line for any questions related to the genuscreen. If required, we can provide telephone hot-line support 24 hours a day, 7 days a week.

Security System Management: This service covers the ongoing monitoring and maintenance of customers' IT and security systems, via strongly encrypted Internet connections.

9.4 Hardware Support for Operational Systems

Next Business Day Exchange-Service: In the event of a hardware defect, customers within Germany will receive a technically identical device in exchange for their defective one on the next working day. The services rendered and the conditions of service can be found in the genua GmbH General Terms of Contract.

9.5 Support from Sales Partners

Support Services from Sales Partners: Many authorized genua sales partners provide extended support options such as an on-site hardware exchange service within a guaranteed time.

10 Contact and Sales

genuscreen and genucenter can be purchased from authorized dealers and genua. You will find a current list of our partners under:

https://www.genua.de/en/partner/partner-search.html

Our sales staff will be pleased to direct you to your nearest sales partner.

GS-WP-0720-10-E

Our Contact Information:

genua GmbH, Domagkstr. 7, 85551 Kirchheim, Germany
tel +49 89 991950-0, fax +49 89 991950-999, info@genua.eu, www.genua.eu

11 Glossary

IPsec	Internet Protocol Security – a security protocol that provides a high degree of confidentiality, authentication and integrity for communication over IP networks. IPsec can be used to establish virtual private networks (VPNs).
OSI-Modell	Open System Interconnection Model – a layer model for communication between information processing systems, which allows the functioning of network protocols to be characterized.
PFL	Packet Filter – a firewall that applies filter rules based on IP addresses and port numbers. If a connection is allowed by the filter rules then the PFL will allow the connection data to pass in a manner similar to that of a router. A PFL can only repel attacks at the IP level when additional security measures are applied. Such additional protection can be provided by so-called “stateful inspection”. A classical PFL cannot access application data and therefore cannot recognize attacks, for example, from viruses occurring at the application level.
SIP	The Session Initiation Protocol is a communications protocol for signaling and controlling multimedia communication sessions in applications of Internet telephony.
SMTP	Simple Mail Transfer Protocol – a network protocol for the exchange of e-mails in computer networks.
SSH	Secure Shell – a network protocol which can be used to establish an encrypted network connection to a remote computer.
TCP	Transmission Control Protocol – a connection and stream orientated network protocol that provides reliable transfer.
Transport Mode	Transport Mode allows two hosts to directly communicate with each other over the Internet. It uses IPsec to ensure the authenticity and integrity of the data, which is encrypted to ensure that it cannot be read by unauthorized third parties. However, the source and target of the data flow cannot be masked as the communication takes place over an open network.
Tunnel Mode	Tunnel mode is used when at least one of the computers involved is not being addressed directly but is being used as a security gateway. In this situation, the communication partner behind the

	gateway remains anonymous. If data is exchanged between two networks through their security gateways then it is not possible to determine which computers are communicating with each other. Authentication, integrity control and encryption can be used here.
VPN	Virtual Private Network – a technology enabling an external computer to be connected to a local network using the Internet as a transport medium and providing encrypted data transfer.