



Firewall & VPN Appliance genuscreen

Facts & Features

Definition:

The firewall & VPN appliance genuscreen features a stateful packet filter and a VPN gateway to defend your network against threats from the Internet. In addition, sensitive systems in large company networks need extra protection. The genuscreen firewall was developed for exactly these requirements. Furthermore, this solution allows the easy and efficient implementation of secure and high-performance VPN tunnels.

Easy integration: genuscreen completely preserves the existing network structure. The bridging mode permits insertion of the solution in the network where areas need extra protection without changing a single IP address.

Typical Use:

- Safeguarding the internal LAN against unauthorized access from outside (e.g. Internet)
- Structuring an intranet in such a way as to establish domains with different protection schemes
- Safe data transfer through high-performance VPN tunnels

Throughput Volume:

Up to 8.370 Mbit/s firewall throughput with a single genuscreen system, more performance possible with clusters

Customer Service:

- Customer service directly from the manufacturer
- Security system management
- Hotline service / update service
- Free hardware support for three years from date of purchase
- Comprehensive training courses



Reasons to Choose genuscreen:

- Certification to CC EAL 4+
- Approval for the encrypted transfer of classified data of the German level RESTRICTED
- Easy integration via the bridging function
- Packet filter with stateful tracking, DOS protection, spoofing protection and filtering on the basis of TCP flags
- Setup of high-performance VPN tunnels with reliable encryption
- Fully IPv6 capable
- Bandwidth management with ALTQ (Alternative Queuing) for reliable performance of preferred protocols
- High availability and user-defined throughput volume using clusters
- User-friendly GUI-based administration
- Central management of numerous solutions

Reasons to Choose genua:

- Leading German specialist for IT security
- Founded in 1992 – implementation of numerous major projects for industrial, government, and military organizations



Firewall

Stateful packet filter	State of the art firewall for manageable rulesets
Bridging firewall	Invisible firewall on the data link layer (layer 2)
Network Address Translation (NAT)	Masquerade networks behind one address
Quality of Service (QoS)	Guarantee service priorities
Queuing (traffic shaping)	Bandwidth management to control traffic volume
Traffic redirection	Forward public services to internal services
Filter criteria	Filtering decision can be based on IP address, network protocol, port, interface, flags and state
Filter action	Choice of packet handling: pass, block, drop
DDoS protection	Proxy for the TCP handshake protects services against TCP SYN floods often used by DDoS attacks
Spoofing protection	Block forged packets
Packet normalisation	Reassemble fragmented packets, generate random IP identification, enforce IP header settings such as TTL and MSS
Enhanced protection	Privileged separation, sandboxing

Virtual Private Network (VPN)

SSHid	VPN on the protocol layer (layer 4, TCP)
IPsec	VPN on the network layer (layer 3)
Bridging IPsec	VPN on the link layer (layer 2)
L2TP	Support for Android, Windows, iOS, Mac OS X (layer 2)

IPsec VPN

General	
NAT-Traversal (NAT-T)	Supports connections between NATed devices
NAT for VPN	Connect locations with overlapping network ranges
High availability (sasync)	Synchronise security associations between multiple appliances to minimize failover outage
High performance replay protection	Increased replay windows
Operation Modes	
Tunnel mode	Entire IP packet is encrypted and encapsulated
Transport mode	Only the payload is encrypted
Network mode	Supports routing protocols such as OSPF over VPN connections
Layer 2 bridging	Use IPsec to connect two locations on layer 2
Transparent IPsec router	Encrypt your WAN traffic without changing your topology
IKEv2	Connect mobile or third party devices
L2TP	Support for Android, Windows, iOS, Mac OS X (layer 2)
Authentication	
RSA	De facto public-key standard
Elliptic curves	Fast key exchange
Pre-shared keys	Manually exchange secret pair of keys
PKI (X.509)	Use a certificate authority (CA) to verify keys
Algorithms	
Encryption	AES-128, AES-192, AES-256, 3DES, Blowfish, CAST

SSHid VPN

General	
Single TCP connection	Outgoing only, no problems with firewalls or NAT
Comes with NAT	Connect locations with overlapping network ranges
No interlinking	Easily prevent unwanted traffic
Compression	Increase net throughput
Operation Modes	
Bidirectional	Like any other VPN
One-direction	Offer centralised services to hundreds of branch offices (e.g. SAP)
Semi-bidirectional	E.g. allow printing at the branch office from central SAP server



Networking

General	
Redundant network access	Multiple uplinks
DNS	Enabling local DNS caching
UMTS/WLAN option	External UMTS or WLAN interface
NTP client	Obtain time from NTP servers
DHCP server	Automatically assign IP address to clients
DHCP relay	Forward DHCP queries to central DHCP server
VLAN	Supports virtual LANs to separate networks
Trunking	Aggregate multiple network interfaces on one virtual interface
PPPoE	DSL uplinks
IPv6	
Native IPv6	Fully IPv6 ready
Tunnelling	Use tunnelling to cross legacy IPv4 networks
NAT64	NAT between IPv4 and v6
Routing	
Policy based routing	Based on IP addresses/networks
Static routes	For small and easy setups
OSPFv2, v3	Popular routing protocol among large corporate networks
Virtual routing domains	Separate routing domains on one appliance
RIP	Routing Information Protocol
MPLS/LDP	Multiprotocol Label Switching/ Label Distributing Protocol

High Availability

Active-active with load balancing	Distribute load on several appliances depending on the source/destination IP address
Link aggregation	LACP: easy integration in a redundant/high-performance switch setup
Hot standby	Reserve appliance for automatic failover

Monitoring

System	System status (memory, load)
VPN	Supervise VPN connection status
NetFlow export	Monitor network traffic with the NetFlow protocol
SNMP, SNMPv3	Retrieve information via SNMP GET requests, or send SNMP TRAPs

Extensibility

Optional modules	Cache (DNS, HTTP), URL filter
------------------	-------------------------------

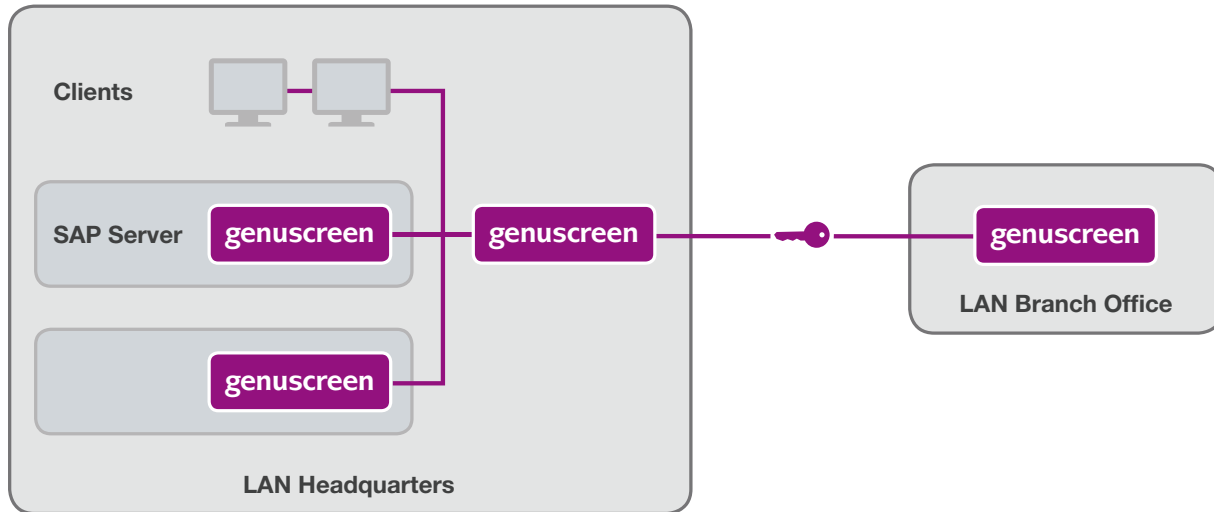
Administration

General	
Web GUI	Powerful web-based user interface secured with TLS/SSL (HTTPS)
Online help	Instant help via user interface
Shell access	Local using console or serial interface, remotely using SSH
Cronjobs	Schedule jobs at specific times
Flexible configuration	Easily modify/add files to the system
USB update	Fix inaccessible systems with an USB stick
Patch Management	
GUI	Get and install patches via GUI
Automatic updates	Automate the process of fetching updates for the appliance
Patch rollback	Return to previous patch level
Logging	
Syslog	Use a third party syslog server to store logs
Hard drive	Use appliance hard drive for storage, if available
Memory	Logs are recorded in memory
Central	Use genucenter to concentrate the logs on one system
Debugging	
Network	Powerful command-line-tools: tcpdump, traceroute, ping, etc.
Firewall	Monitor firewall states, rules and logs
VPN	VPN connection status overview and problem analysis
Root shell	The shell offers full root access
Central Management	
Central Management	Easy administration of several (hundred) systems with Management Station genucenter



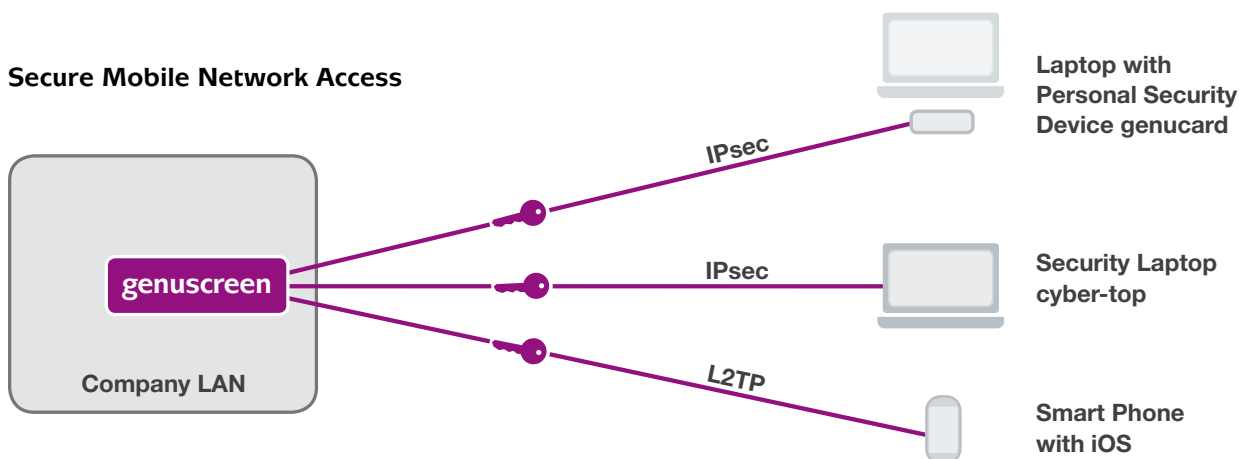
Application Examples

Setting up Security Zones



Users of company networks frequently have excessive authorizations and permissions. To enhance the internal security, the LAN should be separated into individual zones. The genuscreen firewall provides all necessary features for network protection. In the illustration above, an SAP server, HR department data and a branch office are separated from the internal LAN using genuscreen firewalls. Clients from the internal LAN no longer have access to data of others departments. The branch office network also is physically separated, and its users have only access to LAN areas of the headquarters that are explicitly allowed.

Secure Mobile Network Access



The genuscreen firewall & VPN appliance establishes encrypted and authenticated connections across public networks by combining the layer 2 tunneling protocol (L2TP) with the IPsec VPN technique. This means that with the native support of L2TP in smart devices using the Android, iOS and Mac OS X operating systems mobile users are able to connect to company networks without first installing additional software. Employees are therefore able to gain the advantages of “Bring your own device” – at a high security level.

Further information:
www.genua.eu/genuscreen