

XUTM Appliances for companies (up to 100 employees)

The GPO 250 is designed for companies with up to 100 employees and intended for installation in the server rack as a 2U appliance. Features include VLAN, single sign-on, bridging, VPN SSL via x.509 certificates + IPSec, spam protection with real-time detection, virus protection, intrusion detection, web filtering and process-oriented eGUI® technology.



eGUI®-Technology

The new eGUI® technology is remarkable for its ergonomic approach to the processing operation. The display, even of sometimes very different applications, is always consistent and delivers the information required by the user for the current operation only. A measure of the quality of the gateProtect operator concept are the principles governing the design of software dialogue, as formulated in ISO 9241, part 110.

Extended User Authentication

Most modern firewall systems support proxy-based user authentication. This means that only those services which work with proxies such as HTTP or FTP can be issued to specific users. The gateProtect firewall has rule-based Extended User Authentication. This allows any number of services to be assigned individually to one user or a group of users. These services can be provided with all the known additional options such as proxies or web filters. If a user logs on to the firewall from a computer, all the assigned services for the computer in question are enabled.

1. Web browser/UA Client:
logon is via an HTTPs connection.

2. Single sign-on:
Kerberos automatically passes the log-on to the domain to the firewall.

VPN Gateway (SSL with X.509 Certificates + IPSec)

gateProtect offers the most commonly used forms of current site-to-site and Road Warrior VPN connections via IPSec and SSL. Wizards and the eGUI® technology help with the management and set up of these connections. In addition, the firewall generates external configuration files when the VPN connections are created. These files can be used for setting up single click connections and also for site-to-site connections when importing on the firewall at a remote site.

Furthermore, gateProtect offers an IPSec and SSL site-to-site solution with X.509 certificates which can work in bridge mode as an option. For a normal bridge, two or more network cards are linked to form a logical network. gateProtect not only allows this for network cards but also for VPN-over-SSL connections. This makes it possible to treat remote computers exactly as if they were in the local network.

Failover

In order to safeguard the connection to the Internet, gateProtect offers the failover feature. A second emergency connection is set up in addition to the main connection. If the first main connection fails, the emergency connection is automatically established up and data traffic with the Internet is conducted via the new connection. This safeguards any current business processes, such as email despatch and reception.

Monitoring

In order to estimate the load on the firewall, it determines the status of the components, for example, the hard drive, the processor or similar relevant data, which it records and analyses permanently. It is possible to access this data with the administration client in order to respond rapidly in critical situations.

Bridging

Bridging makes it possible to introduce firewall functionality into an existing local network. The part of the network that requires protecting, for example the servers, are physically disconnected from the rest of the network and reattached via a bridge on the firewall.

Then access restrictions, proxies and virus scans, for example, can be set up between the physical networks. It is not necessary to make any changes to the networks themselves.

High Availability

The high availability of gateProtect firewall systems is based on an active/passive system where a secondary firewall is installed in parallel with the primary firewall. The secondary firewall synchronises itself constantly with the primary firewall using dedicated connections. It can therefore at any time take over the work of the primary firewall, should this fail, without any manual intervention.

Furthermore, the status of the primary firewall is monitored by different systems. If any problems are detected in the firewall, it switches itself off. The secondary firewall enables the synchronised configuration and can continue operating in the place of the primary firewall immediately. Downtime is minimised and problems can be dealt with under less pressure.

Features

Firewall

- _ Layer function
- _ Zoom function
- _ Single Sign-On (xUA)
- _ Packet filter
- _ NAT
- _ DHCP Server
- _ DMZ
- _ Bridging
- _ VLAN
- _ Application Level

High Availability

- _ High Availability (activ/passiv)

Internet

- _ Failover
- _ Webblocking
- _ Mail filter

Interception

- _ Syslog
- _ SNMP (Traps)
- _ IDS
- _ Monitoring
- _ Reporting
- _ Statistics (Statistics-Client)

Optional (UTM products)

- _ Spam filter
(CommTouch Technologie)
- _ Virus filter
(Kaspersky Technologie)
- _ Web filter
(Cobion / IBM Technologie)

Feature overview

Firewall technology

Firewall rules - timecontrolled
 Packet filter
 Adaptable Proxies
 VoIP-Proxy
 Bridging
 Stateful Inspection & Proxy combined
 NTP-Server/-Client
 Masquerading
 DynDNS

WAN

Support for xDSL and ISDN
 Support for TCP, UDP, ICMP, GRE, ESP, AH protocols
 Support for virtual IP addresses
 Support for DynDNS
 Failover
 QoS

eGUI®

Graphical Desktop (drag & drop)
 Layer function
 Zoom function

Management

Graphical Client (Data encryption with 4096 Bit)
 User management (specific rights for special settings)
 Role based administration
 Auditing able
 SSH-Support for CLI

Authentication/Authorisation

Active Directory (NT Domain)
 openLDAP + Kerberos
 Single Sign-On

Proxies

HTTP
 FTP
 POP3
 SMTP
 SIP (VoIP)

Security features

DMZ
 Web Blocking (URL)
 DHCP Client & Server
 NAT-Support
 Application Level
 High Availability

VPN protocols

PPTP
 SSL/TLS over X.509
 IPSec over X.509/IKE
 NAT-T

External VPN Client (IPSec & SSL)

Interception

SNMP
 Syslog
 IDS
 Monitoring
 Reporting
 Statistics
 Dedicated statistics client

Filter (optional)

Spam filter
 Content filter
 Virus filter

We do not offer an express or implied warranty for the correctness / up-to-dateness of the information contained here (which may be change at any time). Future products or functions will be made available at the appropriate time.

©2008 gateProtect AG Germany. All rights reserved.

Rear view
 GPA 250



Performance

FW throughput

1.1 Gbps

VPN throughput

140 Mbps

eMails per diem

25.000

Concurrent connections

250.000

Hardware Specification

CPU

INTEL® Celeron (2.0 GHz)

Board

MSI®

Memory

512 MB

Hard disk

160 GB HDD (24/7)

Network interfaces

4 Ports

100 MBit: 2

1.000 MBit: 2

Dimensions DxWxH (mm)

510 x 422 x 88

Noises (db)

59

* dependent from activated Proxys, IDS, Application Level & number of active vpn connections

eGUI®

GENI®