gateprotect®
xUTM Appliances

Clarity · Perfection · Security

GPO 125 Office Appliance

Office-Serie

The entry-level solution to Unified Threat Management

The GPO 125 is designed for companies with 10-25 employees. The xUTM appliance is intended to stand-alone and is also suitable for use separately from the rack.

Like all the large gateProtect solutions, the GPO 125 includes the new eGUI® technology and can also be operated and configured with the Command Center. You will be the owner of a fully functional, powerful xUTM appliance with unlimited gateProtect VPN clients.

eGUI®
ergonomic graphic user interface

---

eGUI®-Technology

The new eGUI® technology from gateProtect 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:
2. logon is via an HTTPs connection.

3. 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 as if they were in the local network.

Proxies (HTTP, FTP, POP3,SMTP, SIP)

The gateProtect firewall offers proxies for HTTP, SMTP, POP3, FTP and SIP. All the data conducted via these proxies is checked for viruses, spam, appropriate content or non-permitted content and then passed on to the user. This prevents unwanted data reaching the internal network via the permitted access routes.

Application Level (Deep Packet Inspection)

gateProtect allows application level filters to be installed in the data flow on the firewall. These check the data passing through e.g. HTTP for correct syntax. If the prescribed syntax is violated, the application level filter blocks the connection. This ensures that the data flowing through permitted connections conforms to rules and prevents an abuse of the enabled connection.

VLAN

A virtual LAN allows several logical networks to be operated in a single physical network. To do this, every data packet carries a flag on the basis of which it is assigned to a VLAN. The gateProtect xUTM appliance recognises this assignment. This means that rules can generated on the firewall for these virtual networks in exactly the same way as for normal networks. gateProtect relieves the administrator of any special management of these VLANS and improves efficiency.

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
_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

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

Authentification/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

Performance

FW throughput
100 Mbps

VPN throughput
40 Mbps

eMails per diem
5.000

Concurrent connections
250.000

Hardware Specification

CPU
AMD (500 MHz)

Memory
256 MB

Hard disk
2,5", 80GB

Network interfaces
4 Ports
100 MBit: 4
1.000 MBit: 0

Dimensions DxWxH (mm)
152 x 245 x 36

Noises (db)
30

Rear view
GPO 125

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

eGUI®

gateprotect®
xUTM Appliances