

GPA 500 - Next Generation UTM Appliance

The gateprotect GPA 500 Next Generation UTM appliance has been tailored for medium-sized companies that value, besides high standards of security and reliability, also especially good performance. The comprehensive Unified Threat Management enables cost-efficient all-round protection combined with best performance. Thanks to the application of the eGUI technology, the GPA 500 can be administered quickly and easily. A multitude of up-to-date and powerful security features in the area of anti-virus, Intrusion Prevention or Application Control offer reliable protection against malware, spam, Trojans, DoS, phishing and other attacks. The combination of all defense mechanisms in one device thus renders cost-intensive investments into several separate solutions unnecessary.

The latest hardware is suited for mounting in server cabinets and includes six network interfaces that can be individually configured. The consequent use of high-quality server components in the GPA 500 enables high transfer rates above average, providing for comprehensive UTM security combined with top-performance.

Likewise, the connection of external branches via VPN as well as the use as an endpoint for the connection to further locations may be realized without problems by means of the GPA 500. Thanks to the flexible possibilities of application, the good performance and the excellent price-performance ratio, the GPA 500 is the right choice for small and medium-sized companies that wish to protect their network environment in a reliable matter, but at a favorable price.



SecurITy
made
in
Germany

Specifications

GPA 500

Interfaces

1 GbE Ports

6xRJ45 (front)

System Performance*

Firewall throughput (MBit/s)

2 100

VPN IPSec throughput (MBit/s)

320

UTM throughput (MBit/s)

300

IPS throughput (MBit/s)

400

Dimensions

H x W x D (mm)

44 x 426 x 238

Gross Weights (kg)

3

Power

Input Voltage (V)

AC 100-240

Full load power consumption (W)

41 W

Environmental

Operating Temperature (°C)

0 ~ 40

Storage Temperature (°C)

-10 ~ 70

Relative Humidity (Non condensing)

20 ~ 90 %

Hardware Certification



* System performance depends on application level and number of active VPN connections. We do not offer an express or implied warranty for the correctness /up-to-dateness of the information contained here (which may be changed at any time). Future products or functions will be made available at appropriate time.

©2013 gateprotect AG Germany. All rights reserved.

FEATURE OVERVIEW

Next Generation UTM / Next Generation Firewall Appliances

The Next Generation UTM Appliances from gateprotect are characterized by optimal scalability, security and performance. Thanks to a unique and patented eGUI® Technology, gateprotect sets standards when it comes to the configuration of modern security systems.

gateprotect's eGUI® Technology raises operating security and efficiency to a previously unattained level. Furthermore, gateprotect is the only manufacturer worldwide to implement the ISO NORM 9241 standard. gateprotect was recently honored with the Frost & Sullivan Best Practices Award 2011.



"gateprotect provides UTM products that stand-out from the competition due to their ease-of-use and security effectiveness. The gateprotect ergonomic graphical user interface (eGUI) provides the most intuitive and effective visual UTM management interface available in the marketplace."

Frost & Sullivan, August 2011

Feature Specifications

MANAGEMENT

- Role based Firewall Administration
- SSH-CLI
- Desktop configuration saved / restored separately from backup
- Object oriented firewall configuration
- Direct Client Update function



Ergonomic Graphic User Interface

- ISO 9241 compliant
- Immediate visual feedback for each setting
- Self-explanatory functions
- Overview of all active services
- Overview of the whole network
- Layer and zoom function

USER AUTHENTICATION

- Active Directory / OpenLDAP support
- Local User database
- Web-interface authentication
- Windows-client authentication
- Single sign on with Kerberos
- Single- and Multi login
- Web Landing page

TRAFFIC SHAPING / QOS

- Multiple Internet connections separately shapeable
- All services separately shapeable
- Maximum and guaranteed bandwidth adjustable
- QoS with TOS-flags support
- QoS inside VPN connection support

HIGH AVAILABILITY

- Active-passive HA
- State synchronization
- Single and Multiple dedicated links support
- Stateful Failover

BACKUP & RECOVERY

- Small backup files
- Remote backup & restore
- Restore backup on installation
- Automatic and time based backups
- Automatic upload of backups on FTP- or SCP-Server
- USB Drive recovery option

LAN / WAN-SUPPORT

- Ethernet 10/100 MBits/s
- Gigabit Ethernet
- MTU changeable (Ethernet/DSL)
- PPP-PAP, PPP-CHAP authentication
- Inactivity timeout / Forced disconnect time
- xDSL
- Multi WAN support
- WAN failover
- Loadbalancing
- Time controlled internet connections
- Manual and automatic DNS assignment
- Multiple dynDNS support
- Source based routing
- Routing protocols RIP, OSPF
- DHCP
- DMZ

VLAN

- 4094 VLAN per interface
- 802.1q ethernet header tagging
- Combinable with bridging

Bridge-mode

- OSI-Layer 2 firewall function
- Spanning tree (bride-ID, port-cost)
- Unlimited interfaces per bridge
- Combinable with VPN-SSL

LOGS, REPORTS, STATISTICS

- Email Reporting
- Logging to multiple syslog-servers
- Logs in admin-client (with filter)
- Export to CSV-files
- IP and IP-group statistics
- Separate services
- Single user / groups
- TOP-lists (Surfcontrol)
- IDS- / Traffic-statistics
- Application Control traffic statistics
- Antivirus- / Antispam-statistics
- Defence statistics

MONITORING

- System Info (CPU, HDD, RAM)
- Network (interfaces, routing, traffic, errors)
- Processes
- VPN
- User Authentication

SNMP

- SNMPv2c
- SNMP-traps
- HA*

UNIFIED THREAT MANAGEMENT

Web-filter

- URL-Filter with safe search enforcement
- Content Filter
- Block rules up to user-level
- Black-/ White lists
- Import / Export of URL lists
- File Extension blocking
- Category based website-blocking
- Self definable categories
- Scan technology with online-database
- Intransparent HTTP-proxy support

Application Control

- Layer 7 Packet filter (DPI)
- Filter Applications instead of ports
- Detection & Control of Skype, Bittorrent and others as well as Web 2.0 Applications like Facebook

Antivirus

- Kaspersky Anti-Virus Engine
- Complete Protection from all malware
- HTTP, HTTPS
- Client-to-Site (Road Warrior)
- FTP, POP3, SMTP
- Exceptions definable
- Manual and automatic updates

Antispam

- Scan-level adjustable
- Real-time Spam Detection
- GlobalView Cloud using Recurrent Pattern Detection (RPD)
- Mail Filter
 - Black- / White lists
 - Automatically reject/delete emails
 - AD Email address import

Intrusion Prevention

- Individual custom rules
- Security-level adjustable
- Rule groups selectable
- Exceptions definable
- Scanning of all interfaces
- DoS, portscan protection
- Malicious network packet protection

Proxies

- HTTP (transparent or intransparent)
- HTTPS
- Support for Radius server, AD server, local user database
- FTP, POP3, SMTP, SIP
- Time-controlled

VPN

- VPN wizard
- Certificate wizard
- Site-to-Site
- Client-to-Site (Road Warrior)
- PPTP
- Export to One-Click-Connection

X.509 certificates

- CRL
- OCSP
- Multi CA support
- Multi Host-cert support

IPSec

- Tunnel mode
- IKEv1, IKEv2
- PSK / Certificates
- DPD (Dead Peer Detection)
- NAT-T
- XAUTH, L2TP

SSL

- Routing mode VPN
- Bridge mode VPN
- TCP/UDP
- Specify WINS- and DNS-Servers

COMMAND CENTER

- Monitor & Active Configuration of 500+ firewalls
- Central Configuration and Monitoring of VPN Connections
- Single and group backup
- Plan automatic backup in groups
- Single and group update & licensing
- Create configuration templates and apply on multiple firewalls
- Certificate Authority
- Certificate based 4096 bit encrypted connections to the firewalls
- Display settings of all firewalls
- Role based User Management

