gateprotect®
Next Generation Firewalls

Clarity · Perfection · Security

gateProtect GPX 800 | Designed for large enterprises

ISO standard 9241

„Next Generation UTM 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.

GPX 800 Next Generation UTM Appliances have extensive features including VLAN, Layer-8 technology, single sign-on, bridging, VPN SSL via x.509 certificates & VPN IPSec, IDS/ IPS, traffic shaping, antivirus, zero hour mail protection, web filtering and the very latest procedure-oriented eGUI® technology. VPN connection performance is greatly enhanced by the special ASIC Crypto accelerator chip.

Control of the user-based security policy - "Layer-8 Technology"
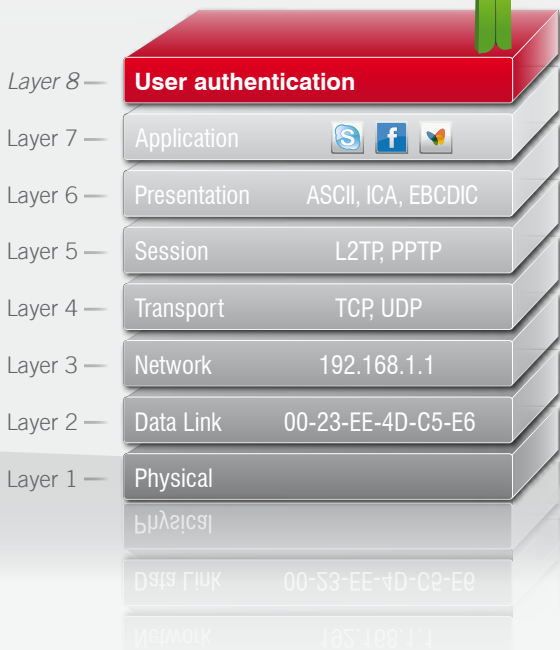
The "Layer-8 Technology" from gateProtect treats the user identity as the 8th layer of the OSI model

All gateProtect "Next Generation UTM Appliances" offer security and productivity at all levels and across all services – from layer 2 to layer 8 with identity-based policies.

Layer		
Layer 8	User authentication	
Layer 7	Application	
Layer 6	Presentation	ASCII, ICA, EBCDIC
Layer 5	Session	L2TP, PPTP
Layer 4	Transport	TCP, UDP
Layer 3	Network	192.168.1.1
Layer 2	Data Link	00-23-EE-4D-C5-E6
Layer 1	Physical	

User authentication

Clarity · Perfection · Security
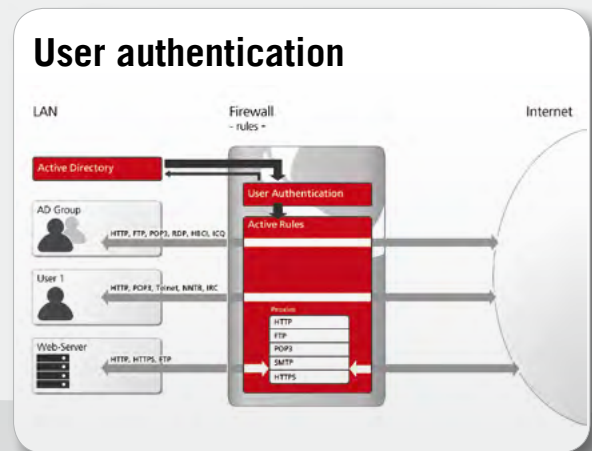
eGUI®
technology

gateProtect GPX 800 | ergonomic Graphical User Interface

The unique eGUI® technology revolutionizes the operation of "Next Generation UTM Appliances"

The greatest security risk facing modern IT networks relates to the fact that increasingly complex security functions are required in order to effectively block attacks. This inevitably leads to systems that are extremely complex to operate, which, in turn, means the risk of user errors increases exponentially. As a result of this, operation and configuration errors in IT systems are the cause of around 98% of all security vulnerabilities in companies nowadays. This risk, together with the constantly increasing amount of work that is required to manage IT security systems, means a whole new approach to the operation of professional security solutions is required.
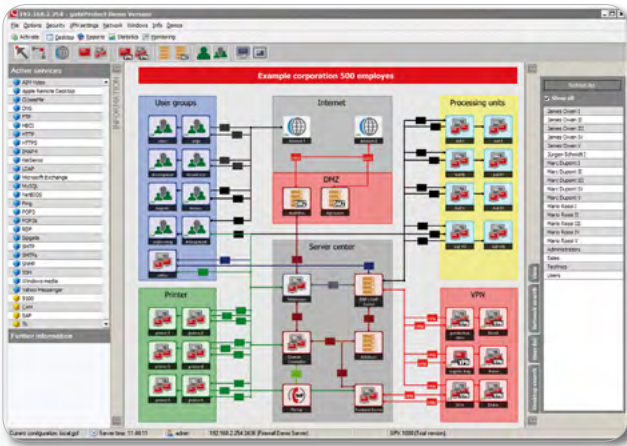

Central eGUI interface from gateProtect

eGUI®

The answer to these problems is the patented and unique eGUI® technology from gateProtect.

The interface concepts of the gateProtect competitors follow a "function-oriented" approach. However, this approach does not include the interaction between humans and machines. gateProtect therefore developed the eGUI® technology, which utilizes a "process-oriented" approach that includes the consequent implementation of the ISO Norm 9241 standard.

The program also provides a consistent layout, which only displays the specific information that the user actually requires for the current activity, no matter which application is being used.
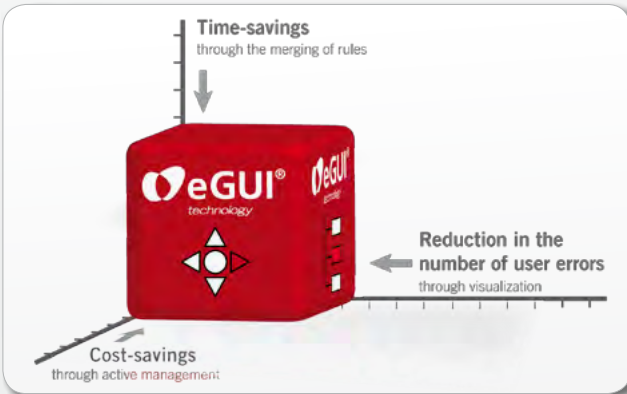
Benefits provided by the eGUI® interface

_Enormous time-savings through a reduction in the number of rules

_Reduction in the number of user errors thanks to the visualization of the entire network

_Reduced operating costs through active management

Initial configuration
(Firewall configuration, import and creation of users, UTM configuration, etc.)

gateProtect | **70% Time-savings**
Mitbewerber I
II
III
IV

Ongoing administration
(Configuration and changing of rules, creation of new users, UTM adjustments)

gateProtect | **80% Time-savings**
Mitbewerber I
II
III
IV

Familiarization phase
(Familiarization of new administrators or deputies, who should be able to configure the firewall)

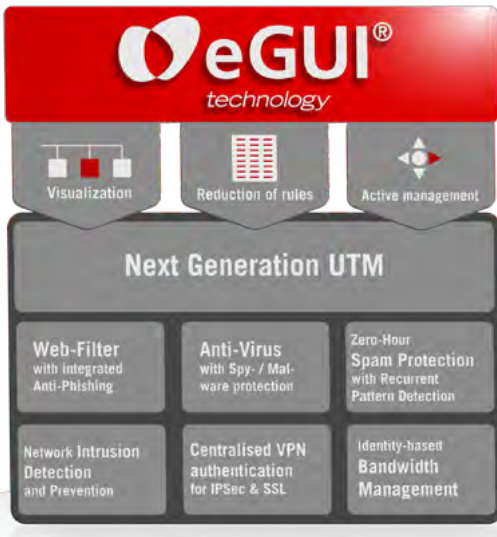gateProtect | **95% Time-savings**
Mitbewerber I
II
III
IV

Study from 2009, which compared the time required to configure firewalls from different providers

gateProtect GPX 800 | Cutting-edge security features

The combination of cutting-edge security features in a "Next Generation UTM Appliance"

The changing network security requirements of the market as well as companies necessitate the next generation of security systems. gateProtect combines a wide range of the most modern and innovative security functions in a single system, the gateProtect "Next Generation UTM Appliances".

Below you will find an overview of some of the next generation features from gateProtect (A complete list can be found on the last page):

• Web Filter with integrated Anti-Phishing
The gateProtect web filter, together with the gateProtect anti-virus and gateProtect spam protection features, provide a comprehensive level of protection against spyware, phishing, malicious site content and much, much more. The gateProtect web filter can be configured using 64 different categories, which can be combined flexibly in line with the specific requirements of the company and, therefore, provide a maximum level of protection.

• Anti-Virus with spy / malware protection and HTTPs Scan `VIEW 1`
In order to guarantee a comprehensive level of protection for the entire network, all e-mail and web traffic is scanned directly on the gateway using gateProtect's anti-virus solution. This even includes the scanning of **encrypted HTTPS pages**. As a result of this, serious threats or malware can be blocked from entering the network. The solution offers real-time protection for all common forms of spyware/malware, including viruses, worms, spyware, backdoors (trapdoors), Trojans and even keyloggers.

• Zero-Hour Spam Protection with Recurrent Pattern Detection
The zero-hour spam protection feature from gateProtect is a particularly powerful and extremely accurate solution. Unlike signature-based protection, this solution uses the **RPD technology** (recurrent pattern detection) that enables new spam mails to be detected before they actually start to spread. A recognition rate of more than 98% is achieved with a false positive rate of only 0,0006667 per mil.
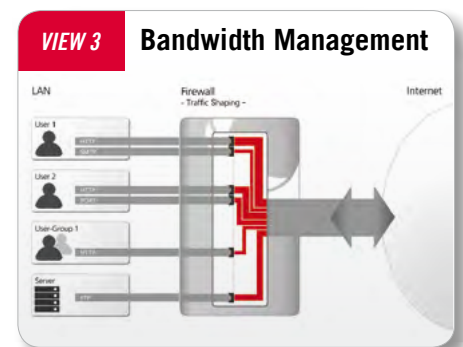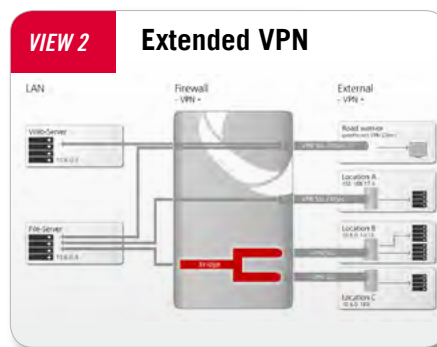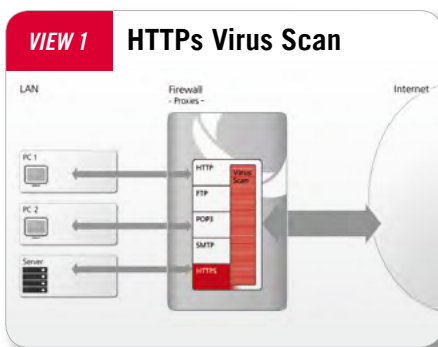
• Network Intrusion Detection and Prevention
The network intrusion detection and prevention system from gateProtect utilizes a signature-based approach to intrusion detection. The network traffic is checked continually using specific algorithms and attack patterns. This enables vulnerabilities in network protocols (such as TCP, UDP, IP, ICMP, SSL, SSH, HTTP and ARP) to be identified and, if required, protective measures to be taken immediately.

• Centralised VPN authentication for IPSec & SSL `VIEW 2`
gateProtect supports all common forms of site-to-site and client-to-site (road warrior) VPN connections via IPSec and SSL. Remote users can utilize all services when working via SSL without any restrictions. Furthermore, gateProtect also offers an SSL site-to-site solution with X.509 certificates, which can also work in bridge mode. This enables distributed corporate networks to be connected via the Internet using strong encryption, even if these networks utilize the same subnets.

• Identity-based Bandwith Management `VIEW 3`
The bandwidth management feature from gateProtect enables bandwidths to be defined at virtually any level, based on specific users, groups and applications. In combination with the quality of service and Internet failover functions, gateProtect's bandwidth management feature is the most comprehensive solution available on the market.

`VIEW 1` **HTTPs Virus Scan**

`VIEW 2` **Extended VPN**

`VIEW 3` **Bandwidth Management**

gateprotect®
Next Generation Firewalls

Clarity · Perfection · Security

gateProtect GPX 800 | Features and performance overview

Rear view

Performance
Note: In brackets (xx) for version a

Firewall throughput	UTM throughput	VPN IPSec throughput	IDS / IPS throughput
5 000 (3 500) Mbps	750 (500) Mbps	1 500 (1 000) Mbps *VPN ASIC Crypto acc.*	1 000 (830) Mbps

Hardware Specifications

Dimensions *DxWxH (mm)* 506 x 426 x 88	Weight 7,8 kg	Input Voltage AC 100-240	Consumption (Full load) 118 W	Operating Temperature C° 0~40

Network interfaces 8 Ports (7 Ports) 1 000 MBit: 8 (7)	Concurrent sessions 1 500 000 (1 350 000)	New sessions per second 20 000 (18 000)

Feature Specifications

▶ Firewall
- Stateful inspection
- Connection-tracking TCP/UDP/ICMP
- SPI and proxy combinable
- Time controlled firewall rules,
  content filter and internet connection
- IP-ranges, IP-groups
- Layer7-filter
- Port-ranges
- Self- and predefined ports
- Supported protocols:
  TCP, UDP, ICMP, GRE, ESP, AH

▶ Management
- eGUI Technology
  - ISO 9241 certified
  - visual feedback immediately supplied
    for each setting
  - self-explanatory functions
  - overview of all active services
  - overview of the whole network
  - Layer and zoom function
- Languages: English, German, French,
  Italian,Spanish, Turkish
- Role-based firewall administration
- Role-based statistic-client
- SSH-CLI
- Desktop configuration saved / restored
  separately from backup
- CLI on serial line
- Object oriented firewall configuration
- Direct Client Update function

▶ LAN / WAN-support
- Ethernet 10/100/1 000*/10 000* Mbit/s
- Twisted-Pair / Fibre-Optics
- MTU changeable (Ethernet/DSL)
- PPPoE, PPTPoE
- ISDN
- PPP-PAP, PPP-CHAP authentication
- Inactivity timeout
- Forced disconnect time
- Cablemodem, xDSL
- Concurrent connections
- Backup-connections
- Connection availability check
- Loadbalancing
- Time controlled internet connections
- Manual and automatic DNS assignment
- Multiple dyn-DNS support
- Supports 8 different dyn-DNS-services
- Source based routing
- Routing protocols RIP, OSPF

▶ User authentication
- Active Directory supported
- Active Directory groups integration
- OpenLDAP supported
- Local userdatabase
- Web-interface authentication
  (port changeable)
- Windows-client authentication
- Authentication on domain login
- Single sign on with Kerberos
- Single- and multi login
- Web-Landing-Page
- Login and logoff auditing
- User- and group statistics

▶ DHCP
- DHCP-relay
- DHCP-client
- DHCP-server (dynamic and fixed IP)

▶ DMZ
- Port forwarding
- PAT
- Dedicated DMZ-links
- DMZ-wizard
- Proxy supported (SMTP)

▶ VLAN
- Max. 4094 VLAN per interface possible
- 802.1q ethernet header tagging
- Combinable with bridging

▶ Bridge-mode
- OSI-layer 2 firewall-function
- Spanning tree (bride-ID, port-cost)
- Unlimited bridges
- Unlimited interfaces per bridge
- Combinable with VPN-SSL

▶ Traffic shaping
- Up- and download shapeable
- Multiple internet connection separately
  shapeable
- All services separately shapeable
- Maximum and guaranteed bandwidth
  adjustable
- QoS with TOS-flags supported
- QoS inside VPN connection supported

▶ Proxies
- HTTP (transparent or intransparent)
- Support for Radius-server, AD-server,
  local user-database
- HTTPS, FTP,POP3,SMTP,SIP
- Integrated URL-/ content-filter
- Integrated antivirus-filter
- Integrated spam-filter
- Time-controlled

▶ Antivirus
- HTTP, HTTPS, FTP, POP3, SMTP
- Scans compressed data and archives
- Scans ISO 9660-files
- Exceptions definable
- Manual and automatic updates

▶ Web-filter
- URL-filter
- Content-filter
- Block rules up to user-level
- Black-/ white-lists
- Im- / export of URL-lists
- File-extension blocking
- Category-based website-blocking
- Self definable categories
- Scan-technology with online-database
- Transparent HTTP-proxy support
- Intransparent HTTP-proxy support

▶ Antispam
- Online-scanner
- Scan-level adjustable
- Real-time-detection-center
- Black- / white-email-sender-lists
- Mail-filter
  - Black- / white-email-recipients-lists
  - Automatically reject emails
  - Automatically delete emails
  - AD-email-addresses import

▶ High availability
- Active-passive HA
- Synchronisation on single / multiple
  dedicated links
- Manually switch roles

▶ IDS/IPS
- Snort scan-engine
- 5000+ IDS-pattern
- Individual custom rules
- Security-level adjustable
- Rule groups selectable
- Exceptions definable
- Scanning of all interfaces
- Email on IDS events
- DoS, DDoS, portscan protection
- Invalid network packet protection

▶ Backup
- Remote backup creation
- Small backup files (kb)
- Remote backup restore
- Restore backup on installation
- Automatic and time based creation
  of backups
- Automatic upload of backups on FTP-
  or SCP-Server
- Auto-install-USB-stick with backup
  integrated

▶ Monitoring
- System-Info
- CPU- / memory usage
- Long-term-statistic
- HDD-status (partitions, usage, RAID)
- Network status (interfaces, routing, traffic,
  errors)
- Process-monitoring
- VPN-monitoring
- User-authentication-monitoring

▶ Logging, Reporting
- Email notification
- Logging to multiple syslog-servers
- Categorized messages
- Report in admin-client (with filter)
- Export report to CSV-files

▶ SNMP
- SNMPv2c
- SNMP-traps
- Auditing of:
  - CPU / Memory
  - HDD / RAID
  - Ethernet-interfaces
  - Internet-connections
  - VPN-tunnel
  - Users
  - Statistics, Updates
  - DHCP
  - HA

▶ Statistics
- IP and IP-group statistic
- Separate services
- Single user / groups
- TOP-lists (surfcontrol)
- IDS-statistics
- Traffic-statistics
- Antivirus- / antispam-statistics
- Defence statistics
- Export statistic to CSV-files

▶ VPN
- VPN-wizard
- Certificate-wizard

IPSec
- Site-to-site
- Client-to-Site (Road warrior)
- Tunnel-Mode
- IKEv1, IKEv2
- PSK
- X.509-certificates
- 3DES, AES (128, 192, 256)
  Blowfish (128, 192, 256)
- DPD (Dead Peer Detection)
- NAT-T
- Compression
- PFS (Perfect Forward Secrecy)
- MD5, SHA1, SHA2 (256, 384, 512)
- Diffi Hellman group
  (1, 2, 5, 14, 15, 16,17,18)
- export to One-Click-Connection
- XAUTH, L2TP

SSL
- Site-to-site
- Client-to-Site (Road warrior)
- Routing-Mode-VPN
- Bridge-Mode-VPN
- X.509-certificates
- TCP/UDP port changeable
- Compression
- specify WINS- and DNS-servers
- 3DES, AES (128, 192, 256)
  CAST5, Blowfish
- Export to One-Click-Connection

PPTP
- Windows-PPTP compatible
- Specify WINS- and DNS-servers
- MSCHAPv2

X.509 certificates
- CRL
- OCSP
- Templates
- Multi CA support
- Multi host-cert. support

▶ VPN-client
- IPSec-client
- SSL-client (OpenVPN)
- NAT-T
- AES (128, 192, 256), 3DES
  CAST, Blowfish
- X.509 certificates
- PSK
- One-Click-Connection
- Log-export

▶ Command Center
- eGUI Technology, ISO 9241 certified
- Monitor 500+ firewalls
- Active configuration of 500+ firewalls
- VPN connections centrally creatable
- Single- and group-backup
- Plan automatic backup in groups
- Single- and group update & licensing
- Create and apply templates on multiple
  firewalls
- Certificate based 4096 bit encrypted
  connections to the firewalls
- Display settings of all firewalls
- Role based command center user
  management
- VPN-monitoring

eGUI®
technology