

xUTM Appliances mit höchster Performance und Ausfallsicherheit

Die gateProtect Carrier Appliance GPX 1000 ist für unbegrenzt große Netzwerke ausgelegt. Die Appliance verfügt über einen leistungsstarken aktiv/passive HA Modus, sowie besonders schnelle Xeon Prozessoren, redundante Server Festplatten, sowie ein leistungsstarkes redundantes Netzteil. Bei der Hardware werden ausschließlich nur hochwertigste Server Hardware Komponenten verwendet. Diese Kombination von Redundanz sowie hochwertigster Hardware bringt eine Ausfallsicherheit von 99,97 %. Die Appliance wurde ausgelegt um auch spezielle Kundenanforderungen zu erfüllen. So lassen sich unter anderem optional z.B. Lichtwellenleiter Netzwerkkarten installieren oder weitere Festplatten im Raid Modus betreiben. Durch die Variabilität lässt sich die schon sehr hohe Grundperformance sowie Ausfallsicherheit nochmals kundenspezifisch steigern.



eGUI®-Technologie

Die neue eGUI® Technologie von gateProtect zeichnet sich durch ihre ergonomische Orientierung am Bearbeitungsprozess aus. Die Darstellung, auch verschiedenster Anwendungen, ist immer konsistent und liefert genau nur die Informationen, die der Anwender jeweils für den aktuellen Bearbeitungsprozess benötigt. Anhaltspunkte für die Qualität des gateProtect Bedienerkonzepts liefern die Dialogprinzipien zur ergonomischen Softwaregestaltung wie sie in der internationalen Norm ISO 9241, Teil 110 formuliert sind.

Extended User Authentifizierung

Die Mehrzahl heutiger Firewall-Systeme unterstützt eine proxybasierte User-Authentication. Das bedeutet, dass nur die Dienste, die mit Proxies wie z.B. bei HTTP oder FTP, arbeiten, benutzerspezifisch vergeben werden können. Die gateProtect Firewall verfügt über eine regelbasierte Extended User-Authentication. Hier können für einen Benutzer oder eine Benutzergruppe beliebig viele Dienste individuell zugeordnet werden. Diese Dienste können mit allen bekannten Zusatzoptionen wie Proxy oder Webfilter versehen werden. Meldet sich ein Benutzer nun von einem Rechner bei der Firewall an, so werden alle zugeordneten Dienste für den betreffenden Rechner freigeschaltet.

gateProtect bietet Ihnen zwei Möglichkeiten zur Anmeldung an der Firewall:

1. Mit Webbrowser/JAIClient:
Die Anmeldung erfolgt über eine HTTPS-Verbindung.
2. Mit Single Sign-On:
Kerberos gibt automatisch die Anmeldung an die Domäne an die Firewall weiter.

VPN-Gateway (SSL mit X.509 Zertifikaten + IPsec)

gateProtect bietet die gängigsten Formen von heutigen Site-to-Site und Road Warrior VPN-Verbindungen via IPsec und SSL. Wizards und die eGUI® Technologie unterstützen die Verwaltung und Erstellung solcher Verbindungen. Zusätzlich generiert die Firewall bei der Einrichtung von VPN-Verbindungen externe Konfigurationsdateien. Diese können sowohl bei der Einrichtung von Single-Click-Connections, als auch für den Import auf der Firewall an einem entfernten Ort für Site-to-Site Verbindungen verwendet werden.

Darüber hinaus bietet gateProtect eine IPsec-, sowie eine SSL Site-to-Site Lösung mit X.509 Zertifikaten, die optional auch im Bridgmodus arbeiten kann. Bei einer normalen Bridge werden zwei oder mehrere Netzwerkkarten so zusammengeschaltet, dass sie ein logisches Netzwerk bilden. gateProtect erlaubt dies nicht nur für Netzwerkkarten, sondern zusätzlich auch für VPN-over-SSL Verbindungen. Dadurch ist es möglich, Rechner an anderen Standorten genauso zu behandeln, als wären sie vor Ort im lokalen Netzwerk.

Traffic Shaping & QoS / Up- & Download

Das Traffic Shaping von gateProtect ist eine der umfangreichsten Implementierungen am Markt. Für jedes Objekt auf dem Desktop lassen sich Maximal- und Mindestbandbreiten festlegen. Darauf aufbauend kann dann für die einzelnen Dienste der Traffic beeinflusst werden. Dadurch kann die Verteilung der Bandbreite bis in jede Detailtiefe konfiguriert werden. Eine weitere Besonderheit der gateProtect Lösung ist die Priorisierung von Datenpaketen im VPN Tunnel mittels QoS. Dies ist wichtig für zeitkritische Anwendungen, bei denen eine Verzögerung unerwünscht ist. So kann z.B. bei gateProtect über einen VPN-Tunnel mittels VoIP störungsfrei telefoniert werden und zwar unabhängig von der Auslastung des Tunnels z.B. durch RDP oder Datendownloads.

Hochverfügbarkeit

Die Hochverfügbarkeit von gateProtect Firewall Systemen basiert auf einem Aktiv/Passiv-System. Hierbei wird parallel zur primären Firewall eine sekundäre Firewall installiert. Diese synchronisiert sich fortwährend über dedizierte Verbindungen mit der primären Firewall. Sie ist damit jederzeit in der Lage bei Ausfall der primären Firewall, deren Arbeiten nahtlos und ohne manuellen Eingriff zu übernehmen.

Des Weiteren wird der Zustand der primären Firewall durch verschiedene Systeme überwacht. Werden dabei Probleme innerhalb der Firewall festgestellt, schaltet sie sich ab. Die sekundäre Firewall gibt daraufhin die synchronisierte Konfiguration frei und kann so direkt anstelle der primären Firewall weiterarbeiten. Die Ausfallzeiten werden dadurch minimiert und aufgetretene Probleme können in aller Ruhe beseitigt werden.

HTTPs Scan

Das Scannen von HTTPs-Traffic auf der Firewall ist bei den meisten Mitbewerbern nicht möglich. Diesen Umstand macht sich diverse Schadsoftware, wie Trojaner und Viren, zu Nutze und kommt durch diese offene Tür unbehelligt ins interne Netz. Als einer von wenigen Herstellern schließt die xUTM Appliance von gateProtect diese Tür. Sie kann auch in verschlüsselten HTTPs Verbindungen den Datenverkehr auf Viren und andere Schadsoftware scannen. Hierfür wird auf der Firewall der Datenstrom entschlüsselt, analysiert und, wenn keine Viren gefunden wurden, anschließend verschlüsselt wieder versandt.

Load Balancing

gateProtect erlaubt es durch sein Load Balancing den Datenverkehr mit dem Internet auf verschiedene Leitungen zu verteilen. Die Firewall entscheidet dann bei jedem Verbindungsaufbau, welche Internetleitung verwendet wird. In der Regel wird eine solche Verteilung nach Protokollen vorgenommen. gateProtect ermöglicht es darüber hinaus jeder einzelnen Verbindung eine Leitung zuzuordnen. Auf diese Weise kann die Nutzung der Internetverbindungen bis in kleinste Detail geplant und optimiert werden.

Features

Firewall

- Layer Funktion
- Zoom Funktion
- Single Sign-On (xUA)
- Paketfilter
- NAT
- DHCP-Server
- DMZ
- Bridging
- VLAN
- Application Level

Hochverfügbarkeit

- High availability (activ/passiv)
- Redundantes Netzteil
- Raid (Hardware „HotSwap“)

Internet

- Fallover
- Webblocking
- Mail-Filter
- Concurrent connections
- Load Balancing
- Traffic shaping

Interception

- Sys-Log
- SNMP (Traps)
- IDS
- Monitoring
- Reporting
- Statistik (Statistic-Client)

Optional (UTM Produkte)

- Spam-Filter
(Commtouch Technologie)
- Virus Filter
(Kaspersky Technologie)
- Web-Filter
(Cobion / IBM Technologie)

Die Funktionen in der Übersicht

Firewall technology

Firewall rules - timecontrolled
 Packet filter
 Adaptable Proxys
 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
 Concurrent connections
 Load Balancing
 Traffic Shaping & QoS

eGUI®

Graphical Desktop (drag & drop)
 Layer function
 Zoom

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 SignOn

Proxys

HTTP
 FTP
 POP3
 SMTP
 SIP (VoIP)
 HTTPS

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
 Sys-Log
 IDS
 Monitoring
 Reporting
 Statistics
 Dedicated statistics client

Filter (optional)

SPAM filter
 Content filter
 Virusscan

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.

Performance*

FW throughput

4.5 Gbps

VPN throughput

300 Mbps

eMails per diem

500.000

Concurrent connections

2.000.000

Hardware Spezifikation

CPU

XEON Quad Core (2.0 GHz)

Board

INTEL®

Memory

4096 MB

Hard disk

2x 160 GB HDD (24/7)
 Hardware Raid (HotSwap)

Power supply

Redundant

Network interfaces

10-12 Ports
 100 MBit: 0
 1.000 MBit: 10-12

Dimensions DxWxH (mm)

662 x 422 x 88

Noises (db)

69

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



gateProtect AG Germany
 Valentinskamp 24
 20354 Hamburg
 Germany

Tel.: +49 (0) 1805 - 428 377
 Fax: +49 (0) 1805 - 428 332
 Vertrieb: sales@gateprotect.de
 Allgemein: info@gateprotect.de

www.gateprotect.de