

Klarheit · Perfektion · Sicherheit



gateprotect[®]
xUTM Appliances

Unternehmen

Command Center

xUTM Appliances

eGUI® Technologie

Appliance-Übersicht

Features

www.gateprotect.de

Willkommen bei gateProtect

IT-Sicherheit ist zurecht eines der vorrangigen Managementthemen unserer Zeit. Die Szenarien von Bedrohungen für Unternehmensdaten in IT-Netzwerken sind vielfältig und ständig kommen neue hinzu. Ein hochtechnologisches Problem, dem die Administratoren im Sicherheitsmanagement nur mit hoch entwickelten Systemen auf neuestem Stand der IT-Technologie begegnen können.

Das größte Sicherheitsrisiko heutiger IT-Netzwerke besteht jedoch darin, dass zur effektiven Abwehr von Angriffen immer mehr hochkomplexe Sicherheitsfunktionen integriert werden müssen, was auch die Bedienung dieser Systeme immer komplexer und aufwändiger macht. Bedienungs- und Einstellungsfehler von Firewall Systemen sind daher heute zu 95 % der Grund von Sicherheitslücken in den IT- Systemen der Unternehmen.

Die in den gateProtect-Laboren entwickelte und patentierte eGUI® Technologie (ergonomic Graphic User Interface) löst mit seiner neuartigen ergonomischen Benutzeroberfläche genau dieses Problem.

gateProtect hat sich auf die Entwicklung und Vermarktung von konsequent benutzerorientierten HighEnd-Lösungen für IT-Sicherheit spezialisiert. Das gateProtect Command Center und die xUTM Appliances vereinigen alle modernen Sicherheits- und Netzwerkfeatures in einem System.

gateProtect-Systeme steigern effektive Sicherheit und Effizienz im IT-Management um ein Vielfaches.

Inhalt

Unternehmen	Seite 4-7
Command Center	Seite 8-9
xUTM Appliances	Seite 10-17
eGUI® Technologie	Seite 18-21
Appliance-Übersicht	Seite 22
Features	Seite 23



*Dennis Monner
CEO gateProtect*

gateProtect steigert Effizienz und IT-Sicherheit

Die gateProtect Aktiengesellschaft Germany ist führender Hersteller von IT-Sicherheitslösungen im Bereich Netzwerksicherheit. Im Fokus stehen Firewall-Systeme, xUTM Appliances, Network Management Systeme sowie VPN-Clients.

Die Lösungen von gateProtect vereinigen modernste Sicherheits- und Netzwerkfeatures wie Firewall, Bridging, VLAN, Single Sign-On, Traffic Shaping, QoS, IPSec/SSL (X.509), IDS/IPS, Web filter, Virus filter, Realtime Spam Detection und HTTPS Proxy in einem System.

Die Besonderheit aller gateProtect-Produkte, über die technischen Highlights hinaus, liegt in der einzigartig ergonomischen Bedienbarkeit der

Systeme. gateProtect ist weltweit der einzige Hersteller, der durchgängig die Richtlinien der ISO-Norm 9241 umsetzt.

Mit der einmaligen und patentierten eGUI® Technologie (ergonomic Graphic User Interface) sowie dem neuen Command Center V2 setzt gateProtect neue Maßstäbe bei der Konfiguration und Verwaltung von global gemanagten IT-Security-Systemen.

Die neuartige eGUI® Technologie führt zu einer erheblichen Erhöhung der effektiven IT-Sicherheit in Unternehmen und gleichzeitig zu einer enormen Effizienz-Steigerung bei der laufenden Wartung der Systeme. Daraus folgt für gateProtect-Kunden eine merkliche Einsparung bei den Betriebskosten.



Sie finden eine Vielzahl weiterer Referenzen auf unserer Website: www.gateprotect.de

Kunden und Referenzen

32 000 Installationen in Europa belegen das Vertrauen in die Marke gateProtect auf breiter Basis. Zu den deutschen Kunden zählen namhafte Unternehmen und Institutionen wie der TÜV Thüringen, E.ON Energie, Mercedes-Benz, Galileo Satelliten

Systeme, Die Bahn, Kneipp-Werke, Constantin Film, Technische Universität Dresden und viele weitere.

Als Kernzielgruppe wendet sich gateProtect an mittelständische Unternehmen aller Branchen.



Konsequente Nutzerorientierung auch beim Support

Aufgrund der eGUI® Technologie hat gateProtect 90 % weniger Supportaufkommen, als dies bei Mitbewerberprodukten der Fall ist. Aus dieser Situation heraus kann gateProtect eine am Markt unerreichte Supportqualität gewährleisten.

So werden Supportleistungen bei gateProtect direkt im Hause und durch eigene Mitarbeiter erbracht. Dafür stehen gateProtect-Kunden jederzeit hochqualifizierte und laufend geschulte Netzwerkad-

ministratoren zur Verfügung. Nur so lässt sich eine gleich bleibend hohe Supportqualität garantieren. Der Kundensupport erfolgt je nach Servicevertrag telefonisch 7 Tage die Woche, 24 Stunden am Tag mit Reaktionszeiten von 0 – 2 Stunden (24/7).

Insgesamt resultiert das gateProtect-Supportsystem in einem europaweit unerreichten Serviceniveau.

*Mitarbeiter des
technischen Supports*



IT Security made in Germany

gateProtect ist Gründungsmitglied der vom Bundesministerium für Wirtschaft und Technologie geförderten Initiative „IT Security made in Germany“ (ITSMIG.e.v.).

Die Initiative „IT Security made in Germany“ ist ein Zusammenschluss deutscher Firmen aus dem Bereich IT-Sicherheit. Mitglieder sind namhafte Firmen der deutschen IT-Sicherheitswirtschaft wie Siemens, Avira, Genua, gateProtect und andere.

Das gemeinsame Ziel ist, in direkter Zusammenarbeit mit dem Bundesministerium und den Mitgliedern, die Wahrnehmung deutscher IT-Kompetenz auf internationaler Ebene weiter auszubauen und gemeinsame Auslandsmärkte effizient zu nutzen. Die Initiative wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) gefördert und

arbeitet als Public Private Partnership (PPP). Organisation und Management liegen beim Fraunhofer-Institut für Sichere Informationstechnologie SIT. Weitere Informationen finden Sie unter: www.itsmig.de



**Bundesministerium
für Wirtschaft
und Technologie**

*Mitarbeiter des gateProtect-
Entwicklungslabors*





Selbstverpflichtung zur Abhörsicherheit

Der potenzielle Kunde von Produkten aus dem Bereich IT-Sicherheit fragt sich: Wie viel Sicherheit bietet das Produkt? Muss ich mit versteckten Zugangsmöglichkeiten oder mit geschwächten Verschlüsselungsmechanismen rechnen? Muss ich davon ausgehen, dass das Produkt Elemente enthält, die ich nicht kontrollieren kann?

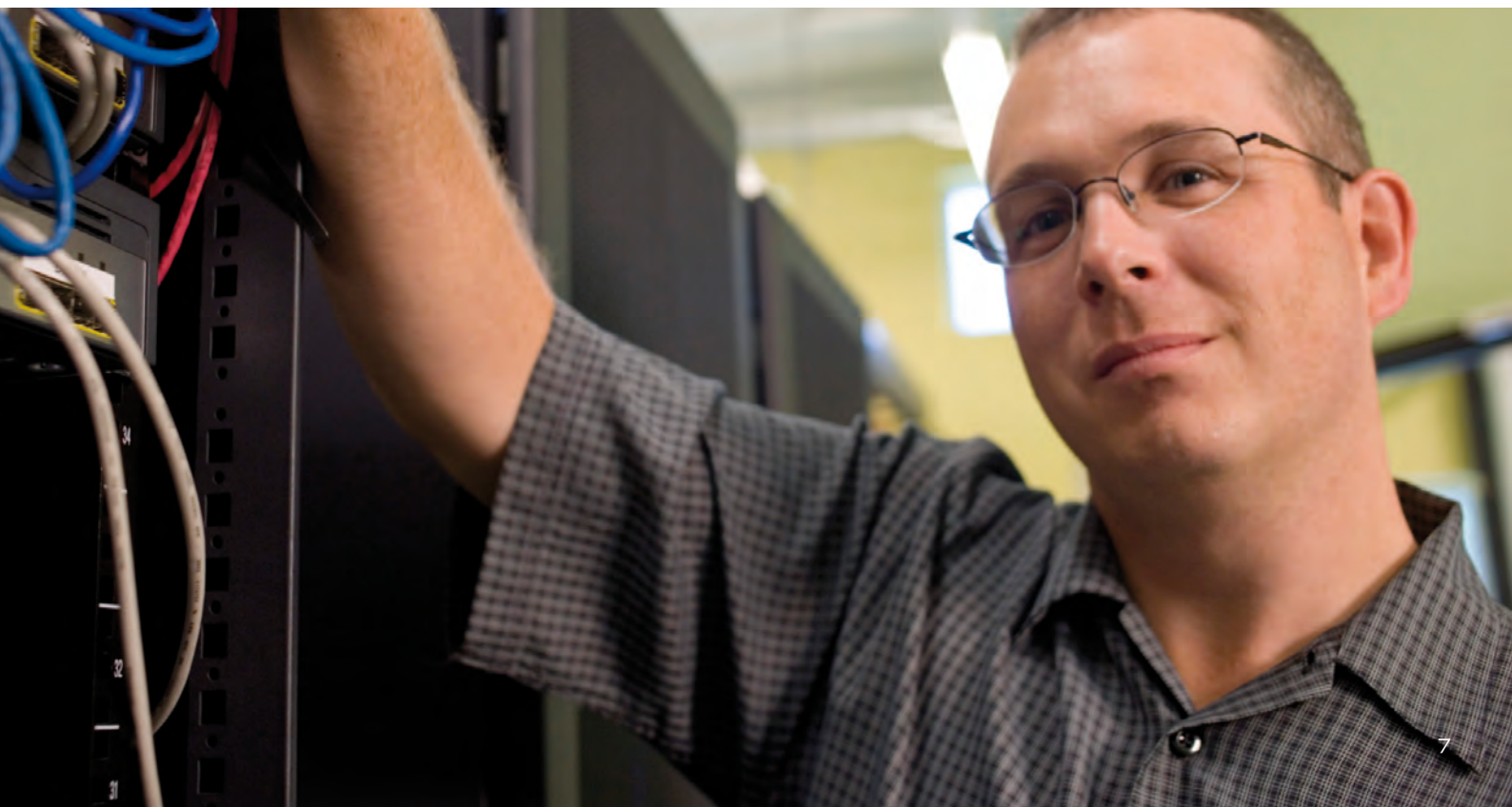
Die Rechtslage in der Bundesrepublik Deutschland ist klar: Es ist den Unternehmen erlaubt, IT-Sicherheitsprodukte mit beliebig starker Verschlüsselung und ohne versteckte Zugangsmöglichkeiten herzustellen und zu vertreiben.

Ausgewählte Mitglieder der Initiative „IT Security made in Germany“ nutzen diese Chance. gateProtect hat sich explizit zu Produkten ohne versteckte Zugangsmöglichkeiten bekannt und die entsprechende Selbstverpflichtung unterzeichnet. Darin heißt es unter anderem:

1. Wir verpflichten uns, ausschließlich Sicherheitsprodukte ohne versteckte Zugangsmöglichkeiten herzustellen.
2. In unseren Produkten sind keine verdeckten Zugangskennungen und Zugangsmechanismen enthalten, die Dritten einen vom Kunden nicht kontrollierten Zugriff auf das Computersystem ermöglichen oder sicherheitsrelevante Funktionalitäten deaktivieren.
3. Unsere Produkte bewirken keine verdeckte Übertragung von Kryptoschlüsseln oder Teilen von Schlüsseln oder Zugangskennungen.



*Abhörsicherheit
wird garantiert*





*Weltweite Verwaltung,
Konfiguration und Überwachung
beliebig vieler gateProtect
xUTM Appliances*

Command Center

Das Command Center ermöglicht die zentrale Verwaltung, Konfiguration und Überwachung von bis zu 500 gateProtect xUTM Appliances bzw. Firewall-Systemen.

Alle gateProtect Appliances, von der GPO 75 bis zur GPX 2500, können zentral über das Command Center verwaltet und konfiguriert werden. Dies ist besonders für Unternehmen wichtig, die mehrere Firewall-Systeme im Einsatz haben oder größere Rollouts planen.

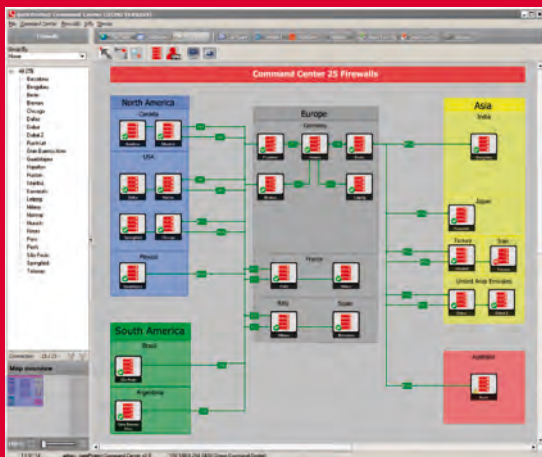
Das neue Command Center erhöht die effektiv erreichbare Sicherheit um ein Vielfaches und führt

gleichzeitig zu einer enormen Effizienz-Steigerung bei der laufenden Wartung der Systeme. So können auch die relativen Betriebskosten deutlich gesenkt werden.

Mit der einmaligen, integrierten eGUI® Technologie (ergonomic Graphic User Interface) setzt gateProtect neue Maßstäbe bei der Konfiguration und Verwaltung von global gemanagten IT-Security-Systemen.

Die wichtigsten Funktionen im Überblick

- Zentrale Übersicht aller Firewall-Systeme**
- Sofortiger direkter Zugriff auf jede einzelne Firewall**
- Automatisches und zentrales Erstellen von Backups aller angebotenen Firewall-Systeme**
- Zentrales Einspielen von:**
 - Updates auf x-beliebige Firewall-Systeme
 - Standardkonfigurationen auf ausgewählten Firewall-Systemen (bei größeren Rollouts)
 - Lizenzschlüsseln und ihrer Verwaltung
- Zentrale Konfiguration von neuen Standorten via VPN (VPN Wizard)**
- Überwachung aller VPN-Verbindungen und zentrales Trennen von Verbindungen bei Bedarf**
- Zoom-Funktion: Detailansicht jedes einzelnen Firewall-Systems**
- Zentrale Überwachung des Funktionszustands sowie der Auslastung aller Firewall-Systeme**
- Zentrale Benachrichtigung und Kategorisierung von Alarmzuständen**



Detailansicht jedes einzelnen Firewall-Systems

Zentrale Überwachung des Funktionszustands sowie der Auslastung aller Firewall-Systeme

Zentrale Benachrichtigung und Kategorisierung von Alarmzuständen

Die gateProtect xUTM Appliances:
GPO 75, GPO 125, GPA 250,
GPA 400, GPX 800, GPX 1000,
GPZ 2500



xUTM Appliances

Die Lösungen von gateProtect vereinigen modernste Sicherheits- und Netzwerkfeatures wie Firewall, Bridging, VLAN, Single Sign-On, Traffic Shaping, QoS, IPSec/SSL (X.509), IDS/IPS, Web filter, Virus filter, Realtime Spam Detection, HTTPS Proxy in einem System.

Eine detaillierte Übersicht der gesamten Features der xUTM Appliances finden Sie unter www.gateprotect.de/features

Feature Highlights der gateProtect xUTM-Systeme

- _Extended User Authentication (xUA)
- _Extended VPN (xVPN)
- _VPN Client
- _Traffic Shaping & QoS / Up- und Download
- _HTTPS Scan

Integrierte Unified Threat Management Tools

- _Viren-Schutz
- _Content filtering
- _Spam-Schutz

Extended User Authentication

für alle Dienste, nicht nur HTTP

Hochverfügbarkeit

mit Synchronisation über unterschiedliche Kanäle

Load Balancing

am Gateway, Aufteilung der Dienste

Traffic Shaping & Quality of Service

auch in VPN-Tunneln

Virus filter

mit echtem HTTPS Scan

Spam filter

mit Realtime Detection

Web filter

Effektive Kombination aus URL & Content filtering

Extended VPN

alle Dienste über SSL verfügbar

Extended User Authentication (xUA)

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, benutzer-spezifisch 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.

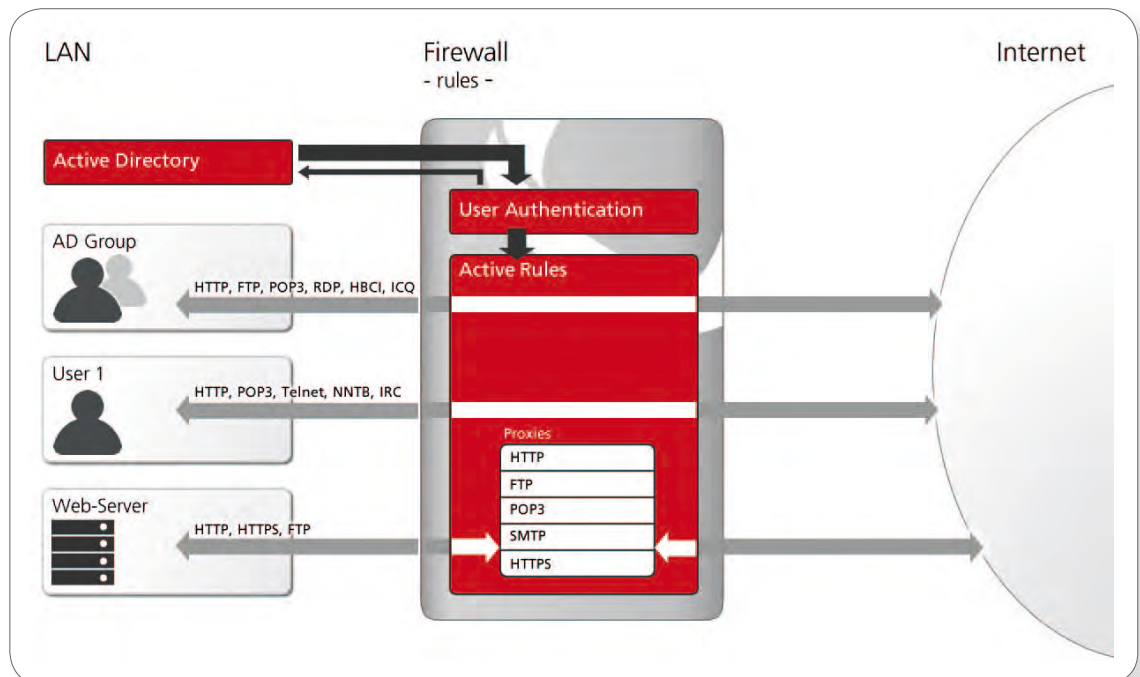
Meldet sich ein Benutzer nun von einem Rechner aus bei der Firewall an, so werden alle zugeordneten Dienste für den betreffenden Rechner freigeschaltet.

gateProtect bietet Ihnen zwei Möglichkeiten zur Anmeldung an der Firewall:

1. Mit Web-Browser/UA Client: Die Anmeldung erfolgt über eine HTTPS-Verbindung.
2. Mit Single Sign-On: Kerberos gibt automatisch die Anmeldung an der Domäne an die Firewall weiter.

Die Extended User Authentication von gateProtect überzeugt durch

- Freigabe von Diensten bis auf Benutzerebene
- Individuelle Konfiguration der Dienste bis auf Benutzerebene
- Konfiguration der Dienste für Benutzer- und Active Directory Gruppen
- Freigabe von Diensten auch im Intranet
- Zukunftssicherheit, weil auch zukünftige Dienste konfigurierbar sind
- Single Sign-On durch Kerberos bei Anmeldung an der Windows-Domäne
- Browser-Login für Betriebssystemunabhängigkeit



Schematische Darstellung xUA

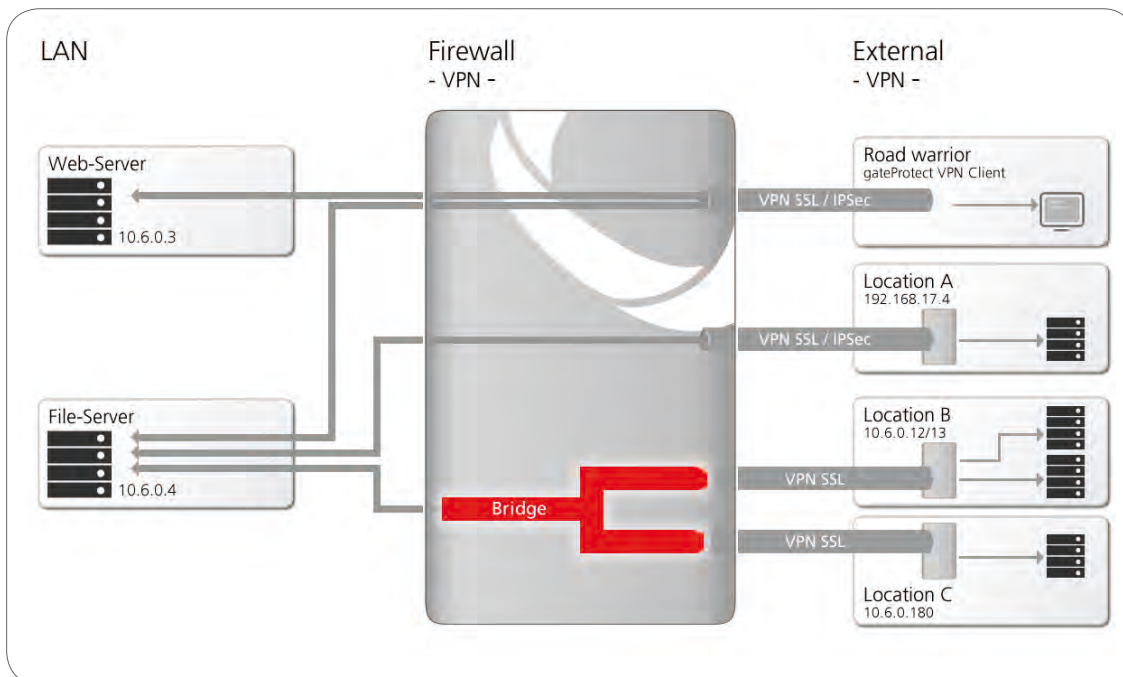
Extended VPN (xVPN)

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 Bridge-Modus 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.

Die Vorteile des gateProtect xVPN

- _Hoher Sicherheitsstandard im SSL-Modus durch Verwendung von X.509 Zertifikaten
- _Einfachste Anbindung entfernter Netzwerke durch Nutzung des Bridge-Modus
- _Volle Kompatibilität auch zu Fremdsystemen, da alle gängigen Standards unterstützt werden
- _Single-Click-Connection für einfache Einrichtung von Road Warrior-Verbindungen und Heimarbeitsplätzen
- _Schnelle und unkomplizierte Einrichtung durch eGUI® Technologie



Schematische Darstellung xVPN

VPN-Client

gateProtect hat für die Anbindung von Laptops und Heimarbeitsplätzen einen eigenen VPN-Client entwickelt. Dieser unterstützt sowohl IPSec als auch VPN-over-SSL.

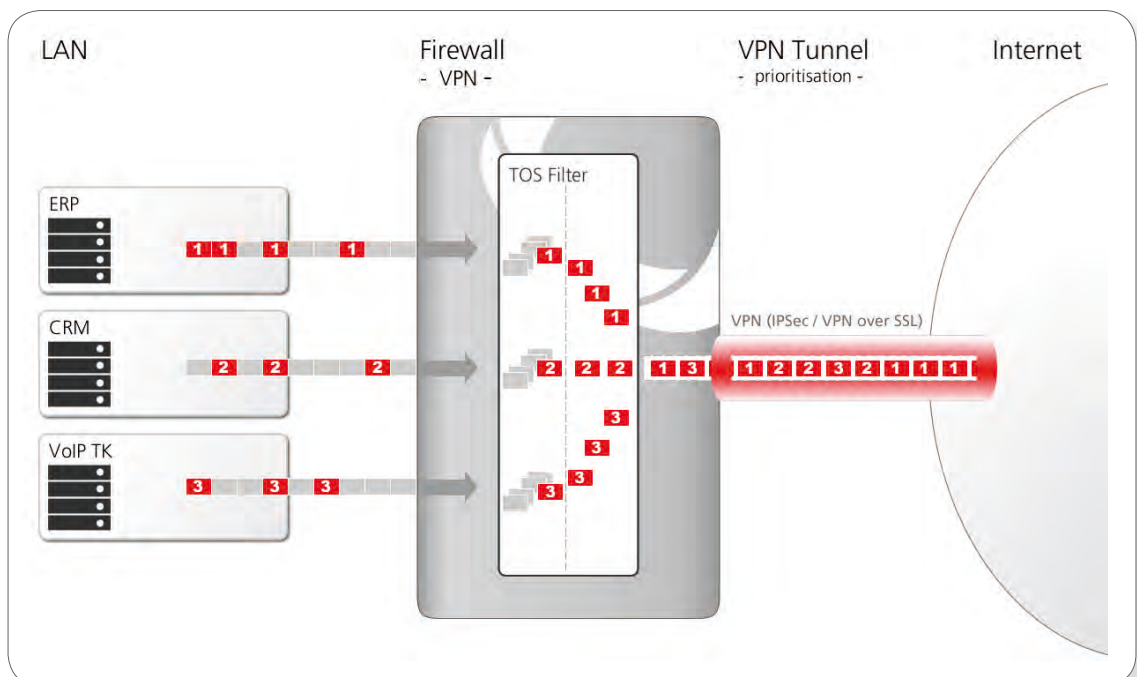
Viele Anbieter arbeiten nur webbrowserbasiert. Im SSL-Modus erlaubt der gateProtect VPN-Client uneingeschränkten Zugriff auf alle Dienste durch den VPN-Tunnel, sofern diese im Regelwerk erlaubt sind. Dadurch lassen sich eine Vielzahl von Applikationen wie z.B. Terminalserver auch durch einen SSL-VPN-Tunnel bedienen.

Durch Verwendung von X.509 Zertifikaten erreicht gateProtect bei VPN-over-SSL Verbindungen einen ähnlich hohen Sicherheitsstandard wie zertifikatsbasierte IPSec-Verbindungen. Jedoch kann hier die deutlich höhere Flexibilität des VPN-over-SSL-Tunnels genutzt werden.

Der VPN-Client unterstützt die von gateProtect entwickelte Single-Click-Connection. Im Zusammenspiel mit der Konfigurationsdatei, die aus der Firewall exportiert wird, kann durch einen einzigen Mausklick der VPN-Tunnel aufgebaut werden.

Die Vorteile des gateProtect VPN-Clients

- _ Hoher Sicherheitsstandard durch X.509 Zertifikate bei VPN-over-SSL
- _ Hohe Kompatibilität durch IPSec und VPN-over-SSL
- _ Nutzbarkeit aller Dienste durch den VPN-over-SSL-Tunnel
- _ Perfekte Zusammenarbeit mit gateProtect Firewalls
- _ Einfache Installation durch Single-Click-Connection



Schematische Darstellung QoS im VPN-Tunnel

Traffic Shaping & QoS / Up- & Download

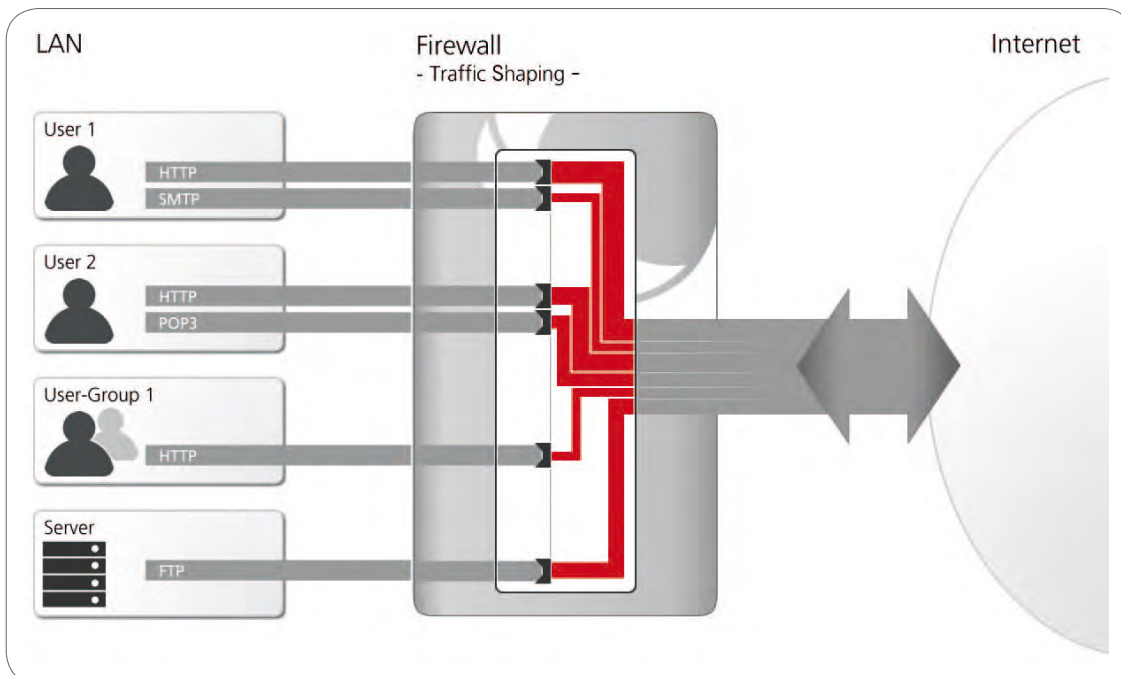
Das Traffic Shaping von gateProtect ist eine der umfangreichsten Implementierungen am Markt. Für jedes Objekt auf dem Konfigurationsdesktop (Benutzer, Rechner, Gruppen usw.) lassen sich Maximal- und Mindestbandbreiten festlegen. Darauf aufbauend kann dann für die einzelnen Dienste der Traffic beeinflusst 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.

gateProtect Traffic Shaping & QoS im Vergleich zum Wettbewerb

_umfangreiche Konfigurationsmöglichkeiten bei Traffic Shaping
_Quality of Service in VPN-Tunneln

_Traffic Shaping-Einstellungen in beliebiger Detailtiefe
_Shaping von Up- und Download



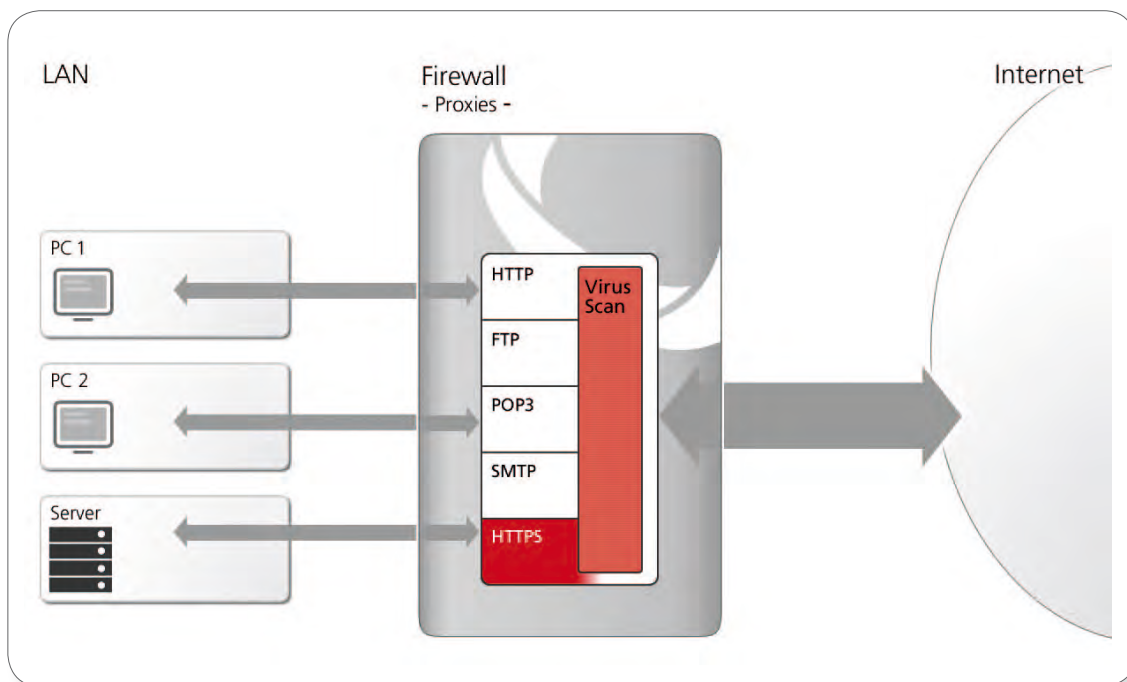
Schematische Darstellung xTS

HTTPS Scan

Das Scannen von HTTPS-Traffic auf der Firewall ist bei den meisten Anbietern nicht möglich. Diesen Umstand machen sich diverse Schadsoftwares, wie Trojaner und Viren, zu Nutze und kommen durch diese offene Tür unbehelligt ins interne Netz.

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.

Als einer der wenigen Hersteller schließt gateProtect mit seinen xUTM Appliances diese



Schematische Darstellung
HTTPS Scan



UTM-Produkte

gateProtect hat im Bereich Viren- und Spam-Schutz, sowie Content filtering international renommierte Hersteller als Partner gewonnen. Durch eine direkte OEM-Partnerschaft wird die Aktualität der Produkte garantiert. Diese Produkte sind als fester Bestandteil der Firewall integriert und werden aktiv durch die eGUI® Technologie unterstützt.



Virus Filter

Die renommierte Antiviren-Software ist weltweit für ihre hervorragende Technologie und kurzen Reaktionszeiten auf neue Viren bekannt. Das Team der Virus Analysten bietet die schnellsten Releases von Sicherheitsupdates schon während dem Ausbruch neuer Viren.

Web Filter

Die GlobalView Web Filtering Lösung ermöglicht aufgrund der einzigartigen „in the cloud“ Infrastruktur eine bisher nicht dagewesene Abdeckung des gesamten Webs.

Spam Filter

Die Anti-Spam-Engine erreicht durch ihre einzigartige Technologie und die Beobachtung des weltweiten Mailverkehrs in Outbreak Detection Centern eine überdurchschnittlich hohe Spamerkennungsrate von über 97 % bei minimaler False Positive Rate.



*Perfekte Ergonomie in der
Mensch-System-Interaktion
mit dem gateProtect eGUI®*

ergonomic Graphic User Interface

Mit eGUI®, der ergonomischen grafischen Benutzeroberfläche bringt gateProtect Bedienungs-sicherheit und -effizienz auf ein bisher unerreichtes Niveau.

Das Risiko von Sicherheitslücken durch Einstellungsfehler und ein ständig wachsender Arbeitsaufwand im Management von IT-Sicherheitssystemen machen einen völlig neuen Denkansatz notwendig.

Die Antwort ist die patentierte eGUI® Technologie von gateProtect.

Die in der internationalen ISO-Norm 9241 als Ergonomie der Mensch-System-Interaktion beschriebenen Zusammenhänge und Anforderungen bildeten das Lastenheft dieser gateProtect-Entwicklung.

Als weltweit einziger Anbieter hat gateProtect alle sieben Gestaltungsgrundsätze der ISO-Norm vollständig erfüllt. Mit der in allen Produkten integrierten eGUI® Technologie erzielt gateProtect höchste Verlässlichkeit und eine vielfach gesteigerte Geschwindigkeit in allen Arbeitsvorgängen der Administration.



eGUI® Technologie und ISO-Norm 9241

Das größte Sicherheitsrisiko heutiger IT-Netzwerke besteht darin, dass zur effektiven Abwehr von Angriffen immer mehr hochkomplexe Sicherheitsfunktionen integriert werden müssen. Dies führt unweigerlich dazu, dass die Bedienung dieser Systeme ebenfalls sehr komplex wird und das Risiko von Bedienerfehlern exponentiell stark steigt. Der Grund liegt in den vielfältigen gegenseitigen Abhängigkeiten der Einstellungen, die in den gängigen Administrationskonsolen kaum oder nur sehr unübersichtlich dargestellt werden können.

Bedienungs- und Einstellungsfehler von IT-Sicherheitssystemen sind daher heute zu 95 % der Grund von Sicherheitslücken in den Unternehmen.

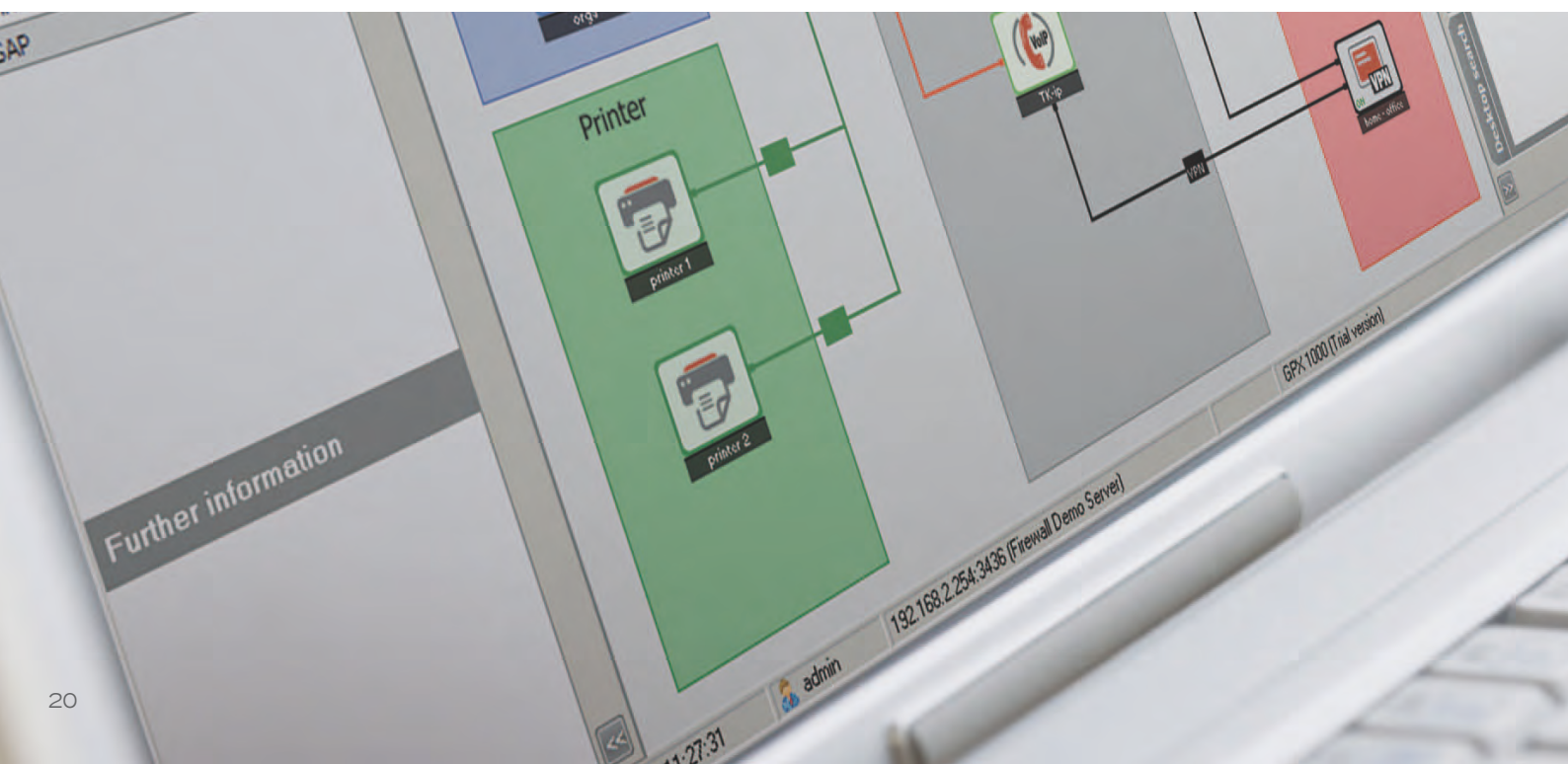
Die in den gateProtect-Laboren entwickelte eGUI® Technologie (ergonomic Graphic User Interface) löst dieses Problem. Die neuartige Benutzeroberfläche zeichnet sich durch ihre ergonomische Orientierung am Bearbeitungsprozess aus. Die Darstellung, auch verschiedenster Anwendungen, ist immer konsistent und liefert genau nur die Informationen, die der Anwender jeweils für den aktuellen Bearbeitungsprozess benötigt.

Anhaltspunkte für die Qualität des gateProtect-Bedienerkonzepts liefern die Prinzipien zur Ergonomie der Mensch-System-Interaktion wie sie in der internationalen Norm ISO 9241, Teil 110 formuliert sind.

Einige Vorteile der eGUI® Oberfläche

- Sofortiges visuelles Feedback jeder Einstellung
- Selbsterklärende Funktionen
- Zentrale Übersicht aller aktiven Dienste
- Sofortiger Überblick der gesamten Netzwerkkonfiguration
- Layer- und Zoom-Funktion für Netzwerke bis 10 000 User

eGUI®
ergonomic graphic
user interface



Die sieben Gestaltungsgrundsätze nach DIN EN ISO 9241 Teil 110

1. Aufgabenangemessenheit

„Ein Dialog ist aufgabenangemessen, wenn er den Benutzer unterstützt, seine Arbeitsaufgabe effektiv und effizient zu erledigen.“

2. Selbstbeschreibungsfähigkeit

„Ein Dialog ist selbstbeschreibungsfähig, wenn jeder einzelne Dialogschritt durch Rückmeldung des Dialogsystems unmittelbar verständlich ist oder dem Benutzer auf Anfrage erklärt wird.“

3. Steuerbarkeit

Ein Dialog ist steuerbar, wenn der Benutzer in der Lage ist, den Dialogablauf zu starten sowie seine Richtung und Geschwindigkeit zu beeinflussen, bis das Ziel erreicht ist.“

4. Erwartungskonformität

„Ein Dialog ist erwartungskonform, wenn er konsistent ist und den Merkmalen des Benutzers entspricht, z.B. seinen Kenntnissen aus dem Arbeitsgebiet, seiner Ausbildung und seiner Erfahrung sowie den allgemein anerkannten Konventionen.“

5. Fehlertoleranz

„Ein Dialog ist fehlertolerant, wenn das beabsichtigte Arbeitsergebnis trotz erkennbar fehlerhafter Eingaben entweder mit keinem oder mit minimalem Korrekturaufwand seitens des Benutzers erreicht werden kann.“

6. Individualisierbarkeit

„Ein Dialog ist individualisierbar, wenn das Dialogsystem Anpassungen an die Erfordernisse der Arbeitsaufgabe sowie an die individuellen Fähigkeiten und Vorlieben des Benutzers zulässt.“

7. Lernförderlichkeit

„Ein Dialog ist lernförderlich, wenn er den Benutzer beim Erlernen des Dialogsystems unterstützt und anleitet.“

Als weltweit einziger Anbieter hat gateProtect alle sieben Gestaltungsgrundsätze der ISO-Norm vollständig erfüllt. Mit der in allen Produkten integrierten eGUI® Technologie erzielt gateProtect höchste Verlässlichkeit und eine vielfach gesteigerte Geschwindigkeit in allen Arbeitsvorgängen der Administration.



gateProtect Appliance-Übersicht

Die xUTM Firewall Appliances der gateProtect AG bieten ein Höchstmaß an Flexibilität und beinhalten alle gängigen Sicherheitsfeatures.

Trotz des Einsatzes modernster Sicherheitstechnologien sind die xUTM Appliances im täglichen Einsatz besonders einfach zu bedienen.

0-Serie

GPO 75

10 User*

✓ 4 LAN



Performance throughput

Firewall	200 Mbps
VPN	50 Mbps
concurrent connections	50.000

GPO 125

25 User*

✓ 4 LAN



Performance throughput

Firewall	200 Mbps
VPN	70 Mbps
UTM	35 Mbps
concurrent connections	150.000

A-Serie

GPA 250

100 User*

✓ 4 LAN



Performance throughput

Firewall	800 Mbps
VPN	120 Mbps
UTM	90
concurrent connections	300.000

GPA 400

250 User*

✓ 6 LAN



Performance throughput

Firewall	1.4 Gbps
VPN	190 Mbps
UTM	140 Mbps
concurrent connections	500.000

X-Serie

GPX 800

500 User*

✓ 8 LAN



Performance throughput

Firewall	3.0 Gbps
VPN	1.000 Mbps
UTM	500 Mbps
concurrent connections	1.000.000

GPX 1000

1 000 User*

✓ 12 LAN



Performance throughput

Firewall	5.0 Gbps
VPN	1.500 Mbps
UTM	700 Mbps
concurrent connections	1.300.000

GPZ 2500

10 000 User*

✓ 18 LAN



Performance throughput

Firewall	9.0 Gbps
VPN	2.500 Mbps
UTM	1.100 Mbps
concurrent connections	2.500.000

Die Features in der Übersicht

xUTM Appliance	GP0 75	GP0 125	GPA 250	GPA 400	GPX 800	GPX 1000	GPZ 2500
eGUI* (ergonomic Graphic User Interface)							
Central configuration desktop	x	x	x	x	x	x	x
Layer-Function	x	x	x	x	x	x	x
Zoom-Function	-	-	x	x	x	x	x
High availability							
High availability (Active-Passive)	-	x	x	x	x	x	x
Redundant power supply	-	-	-	-	-	x	x
Redundant disks (Raid)	-	-	-	-	-	x ¹	x ¹
Firewall							
LAN	4	4	4	6	8	12	18
Patch Management	x	x	x	x	x	x	x
Certificate Management (CRL, OCSP)	x	x	x	x	x	x	x
Packet filter	x	x	x	x	x	x	x
NAT	x	x	x	x	x	x	x
DynDNS	x	x	x	x	x	x	x
DHCP-Server	x	x	x	x	x	x	x
DMZ	x	x	x	x	x	x	x
User authentication	x	x	x	x	x	x	x
Single-SignOn	x	x	x	x	x	x	x
QoS	x	x	x	x	x	x	x
Bridging	x	x	x	x	x	x	x
V-LAN	x	x	x	x	x	x	x
Routing (RIP v2, OSPF)	x	x	x	x	x	x	x
Application Level	-	x	x	x	x	x	x
Traffic Shaping	-	x	x	x	x	x	x
Internet							
Failover	-	x	x	x	x	x	x
Webblocking	-	x	x	x	x	x	x
Mailfilter	-	x	x	x	x	x	x
Concurrent connections	-	-	x	x	x	x	x
Load Balancing	-	-	x	x	x	x	x
Proxies							
HTTP	-	x	x	x	x	x	x
FTP	-	x	x	x	x	x	x
POP3	-	x	x	x	x	x	x
SMTP	-	x	x	x	x	x	x
SIP (VoIP)	-	x	x	x	x	x	x
HTTPS	-	-	-	x	x	x	x
VPN							
Site to site							
SSL (X.509 certificates)	x	x	x	x	x	x	x
SSL (X.509 certificates) + Bridgemode	x	x	x	x	x	x	x
IPSec (X.509 certificates, PSK, XAUTH, L2TP)	x	x	x	x	x	x	x
Road warrior							
IPSec (X.509 certificates, PSK, XAUTH, L2TP)	x	x	x	x	x	x	x
SSL (X.509 certificates)	x	x	x	x	x	x	x
PPTP	x	x	x	x	x	x	x
Interception							
Sys-Log	x	x	x	x	x	x	x
SNMP (Traps)	-	x	x	x	x	x	x
IDS	-	x	x	x	x	x	x
Monitoring	-	x	x	x	x	x	x
Reporting	-	x	x	x	x	x	x
Statistics	-	x	x	x	x	x	x
Statistics Client	-	x	x	x	x	x	x
Optional (UTM Products)							
Virus filter	-	opt.	opt.	opt.	opt.	opt.	opt.
Spam filter	-	opt.	opt.	opt.	opt.	opt.	opt.
Web filter	-	opt.	opt.	opt.	opt.	opt.	opt.

x¹ - Hardware „Hotswap“

Was können wir für Sie tun?



gateProtect AG Germany
Valentinskamp 24
20354 Hamburg
Germany

Tel.: +49 (0) 1805 - 428 377 (12 Cent./Min.)
Fax: +49 (0) 1805 - 428 332 (12 Cent./Min.)
Vertrieb: sales@gateprotect.de
Allgemein: info@gateprotect.de
www.gateprotect.de

Ihr gateProtect Vertriebspartner