

DEFEND
DIE
ZUR
ZEIT

DAS WOHL
BEWÄHRTESTE
UTM-GATEWAY
ZUR ZEIT!



DEFENDO RACK SERVER

GATEWAY APPLIANCE
ZUM SICHEREN
INTERNET ZUGRIFF
FÜR MITTELGROSSE
BIS GRÖSSERE LANS



- Dynamische Firewall
- Intrusion-Prevention
- VPN-Server
- Proxy-Server
- Webseiten-Filter
- Viren-Scanner
- Mail-Server
- Spam-Filter
- Greylisting
- Web-Mail
- DMZ-ready
- Voice-over-IP ready
- Ausfall-Cluster ready

LINOGATE
INTERNET TECHNOLOGIES

ALLES DRIN FÜR DEN SICHEREN INTERNET-ZUGANG

ALLE KOMPONENTEN FÜR INTERNET SICHERHEIT IN EINER BOX – ZUM SCHUTZ IHRES UNTERNEHMENS!



RACK SERVER

VERSIONEN

| | |
|----------------|----------|
| DEFENDO SMALL | 20 USER |
| DEFENDO MEDIUM | 50 USER |
| DEFENDO LARGE | 250 USER |

SPEZIFIKATIONEN

Plattform

19" EinbaufORMAT, 1 Höheneinheit
Intel Ci3 540 mind. 2,9 GHz,
2 GB RAM
mind. 250 GB 24x7 Festplatte
4 x 1000/100/10 Mbit LAN
Zusätzlich bei DEFENDO large:
Festplattenspiegelung und 4 GB RAM
Massangaben (B-H-T):
44 cm, 5 cm, 37/41 cm, Gewicht 6,8 kg

Konnektivität

ADSL / VDSL (ext. Modem erforderlich)
Ethernet
Tagged VLANs IEEE 802.1q
UMTS über optionalen USB-Stick
Policy-Routing nach Quelle, Ziel, Protokoll
Bandbreitenmanagement

- in Internet- und IPsec-Schnittstellen
- Konfiguration nach IP und Protokoll
- Quality-of-Service für VoIP
- Unterstützung von DSCP

Client für dynamisches DNS

Firewall

Grafische Statistiken
Konfigurierbarer Stateful-Inspection-Paketfilter
Network-Address-Translation (SNAT / DNAT)
Trust-Level-Konzept mit vier Vertrauensstufen
Verschiedenste Architekturen (z.B. DMZ),
Zeitabhängige Firewall-Regeln
Intrusion- Detection- / -Prevention System
mehrfach wöchentlich Signatur-Updates*

VPN-Server

Eigene Firewall-Regeln für VPN-Schnittstellen
IPsec-VPN-Server

- Verschlüsselung: AES und 3DES
- Authentifizierung: PSK und X.509-Zertifikate
- NAT-Traversal
- IKE-Fragmentation
- Dead-Peer-Detection
- XAUTH / ModeConfig
- L2TP über IPSEC

Open VPN Client und Server

- Verschlüsselung: AES und Blowfish
- Authentifizierung: X.509-Zertifikate

SSH TCP Portforwarding

- Verschlüsselung: AES
- Authentifizierung: RSA-Schlüssel
- gesicherter RDP-Stick für Clients erhältlich

Mail-Server / Mail-Relay

Eingehende E-Mails über SMTP, POP3, IMAP4
POP3 MultiDrop-Unterstützung
IMAP4-, POP3- und Web-Mail-Server
Verwendung als Mail-Relay für interne Mail-Server
TLS-Verschlüsselung
SMTP Authentifizierung als Server und Client
Anti-Spam

- Greylisting gegen Spam und Viren
- konfigurierbarer Spam-Mail-Filter
- Abfrage von RBL- und URIBL-Servern
- Plausibilitätsprüfungen im SMTP-Dialog
- Bayes-Filter

Filtern von Anhängen anhand Datei-Endung
HTML-Mail-Filter
Mail-Auto-Reply-Funktion

DEFENDO - DER TESTSIEGER

TRÄGT DAS QUALITÄTSSIEGEL



TeleTrust Quality Seal
www.teletrust.de/tsmig

Application-Level-Gateways / Proxies

Optional transparenter Zugriff auf Proxies
Web-Proxy für HTTP, HTTPS, FTP

- Konfigurierbares Caching von Webseiten
- Passwortgeschützter Zugriff auf das Internet
- Authentifizierung auch über NTLM und LDAP
- Statistik des gesamten Datenverkehrs
- Sperrung nach Datei-Endungen und Content-Type
- Verschiedene URL-Filterdatenbanken
- Gruppen- / IP-bezogene URL-Filter-Konfiguration
- Ausblendung aktiver HTML-Inhalte möglich

FTP-Proxy
HTTP / HTTPS-Reverse-Proxy

- Virtuelle Hosts
- Auswahl des Hintergrund-Servers nach URL-Pfad
- Optional Authentifizierung mit Client-Zertifikaten
- Zugriff auf MS Exchange (OWA, ActiveSync, OutlookAnywhere)
- Zugriff auf MS Remote-Desktop-Gateway
- Last-Verteilung
- Optional HTTP Strict-Transport-Security

SOCKS 4/5 Proxy
SIP-Outbound-Proxy
Transparenter POP3- / SMTP-Proxy
Caching-DNS-Forwarder

Viren-Scanner optional

Download-Virenscan in Web- und FTP-Proxy
Optional SSL-Interceptor für HTTPS-Virenscan
Virenprüfung aller ein- und ausgehenden E-Mails

Administration

Hierarchische IP-Gruppen; auch DNS basiert
Hierarchische Protokoll-Definitionen
Konfigurationsprofile mit Zertifikaten für

- Windows IPsec L2TP
- Windows OpenVPN
- iOS Exchange über Reverse-Proxy
- iOS XAuth IPsec
- DEFENDO / Orbiter IPsec

Benutzer-Import aus Active Directory

Weitere Komponenten

Web- / FTP-Server
Primary- und Secondary-DNS-Server
DHCP-Server; auch als Secondary einsetzbar
NTP-Zeitserver
SNMPv3-Server
Fail-Over-Cluster vorbereitet

* nur für Pflegevertragskunden

Technische Änderungen vorbehalten

LINOGATE
INTERNET TECHNOLOGIES

Döllgast Straße 6
86199 Augsburg
Deutschland
Fon: +49 (0)821 25 96 0
Fax: +49 (0)821 25 96 333

info@linogate.com
www.linogate.com