# Datenblatt: UTM Firewalls

## DFL-260 / DFL-860

### NetDefend UTM Firewalls

- Hohe Durchsatzraten für VPN- und Firewall-Verkehr
- Intrusion Prevention System
- Anti-Viren-Schutz
- Web Content Filtering
- Hardware-Beschleuniger für hohen D
- Umfangreiche Routingfunktionalitäten
- Leistungsfähiges Traffic Management
- Proaktiver Schutz vor Bedrohungen von Innen

## Eigenschaften

- Firewall-Schutz auf Basis von Stateful Packet Inspection
- VPN-Server und VPN-Client Funktionalitäten zur verschlüsselten Anbindung von Standorten oder einzelner Mitarbeiter über das Internet
- Signatur-basiertes Intrusion Prevention System
- Integrierter Virenscanner von Kaspersky
- Dynamischer Web Content Filter
- Unterstützt transparenten Firewall-Modus für Implementation ohne Netzwerkänderung
- Unlimitierte Benutzeranzahl
- Application Layer Gateway für HTTP, FTP, SMTP, SIP und H.323
- Proaktive interne Netzwerksicherheit mittels D-Link ZoneDefense
- Content Filtering für Active X, Java Script und Cookies
- Blockieren bestimmter Peer-to-Peer und Instant Messenger Programme
- Benutzerauthentifizierung über RADIUS, LDAP, Active Directory, HTTP, HTTPS, XAUTH und PPP
- Outbound Traffic Load Balancing und WAN Failover
- Server Load Balancing
- Traffic Management für QoS Priorisierung und Bandbreitenreservierung
- Unterstützt 802.1q VLANs
- Policy Based Routing und dynamisches Routing mittels OSPF
- Management über objektorientierte Weboberfläche oder Command Line Interface

## Beschreibung

Gesetzliche Anforderungen und ein verantwortungsbewusstes Risikomanagement erfordern aufgrund der vielfältigen Bedrohungen für eine IT-Landschaft eine leistungsfähige IT-Sicherheitsarchitektur nach dem aktuellen Stand der Technik.
Mit der D-Link UTM Firewall-Familie können Sie leistungsfähige und gleichzeitig kosteneffektive IT-Sicherheitslösungen zum Schutz vor Sicherheitsbedrohungen von außen und von innen implementieren.

## Ihr Nutzen

### Schutz vor Bedrohungen von Außen

Als klassische Gateway-Firewall bieten beide Modelle umfangreichen Schutz vor Bedrohungen aus dem Internet oder aus anderen nicht vertrauenswürdigen Netzwerken. Neben der Paketfilter-Funktionalität sorgt insbesondere das Intrusion Detection und Prevention System mit seinen selbständig aktualisierten komponentenbasierten Signaturen für Schutz vor bekannten und sogar unbekannten Angriffen. Durch die Unified Thread Management-Funktionalität sind die Geräte darüber hinaus in der Lage mittels des integrierten Virenscanners und des dynamischen Web Content Filters das Herunterladen von schädlichen Dateien sowie das Laden unerwünschter Webseiten zu verhindern. Dazu können Unternehmen eine Blockade von Webseiten auf Basis von Kategorien wie z.B. Shopping oder Spiele veranlassen. Auf diese Weise können auch minderjährige Auszubildende gesetzeskonform vor jugendgefährdenden Inhalten geschützt werden.

### Schutz vor Bedrohungen von Innen

In IT-Sicherheitsstudien wird betont, dass 80% aller Angriffe gegen IT-Systeme nicht von außen sondern von innen aus dem Unternehmen gestartet werden. Die innovative ZoneDefense Funktionalität ermöglicht im Zusammenspiel mit D-Link xStack Switches eine sehr schnelle Isolation von Endgeräten, von denen schädlicher Netzwerkverkehr ausgeht, indem der zugehörige Switchport deaktiviert wird. Damit wird unter anderem verhindert, dass mit Schadcode befallene Notebooks nach Anschluss an das interne Netzwerk weitere Endgeräte angreifen und infizieren. Weiterhin kann eine Vielzahl von ggf. unerwünschten Applikationen wie Peer-to-Peer Software oder Instant Messenger blockiert werden und so eine entsprechende Sicherheitsrichtlinie technisch durchgesetzt werden.

# UTM Firewalls DFL-260 / DFL-860

## Ihr Nutzen

### Unified Thread Management

Unified Thread Management integriert alle am Gateway eines sicheren Netzwerks benötigten Mechanismen zur Abwehr von externen Bedrohungen in einem einzigen Gerät. Dazu gehören neben den klassischen Paketfilter- und Intrusion Detection/Prevention-Funktionalitäten auch das Scannen von Inhalten nach Viren und weiterem Schadcode sowie die Erkennung und Blockierung von Webseiten mit unerwünschten Inhalten. Durch die Integration all dieser Funktionen in einem Gerät verringert sich die Komplexität für die Inbetriebnahme und den Betrieb dieser Sicherheitsarchitektur erheblich. Dies ermöglicht eine signifikante Senkung der Betriebskosten.

### Intrusion Detection & Prevention System

Die in den UTM Firewalls genutzte IPS-Technologie basiert auf Komponenten-basierten Signaturen. Dadurch werden nicht nur bekannte Angriffsmuster erkannt, sondern auch unbekannte Variationen, die auf den gleichen Angriffmustern basieren. Die täglich aktualisierten Signaturen werden auf Basis eines weltumspannenden Netzes von Angriffssensoren erzeugt, die alle aktuellen Bedrohungen ermitteln und Ihnen so zeitnah Abwehrmechanismen dafür zur Verfügung stellen. Um die Netzwerkperformance bei dieser aufwendigen Analyse nicht zu beeinträchtigen, nutzt das IPS einen Hardwarebeschleuniger, mit dem die UTM Firewalls beeindruckende Durchsatzraten erreichen.

### Virusscanner

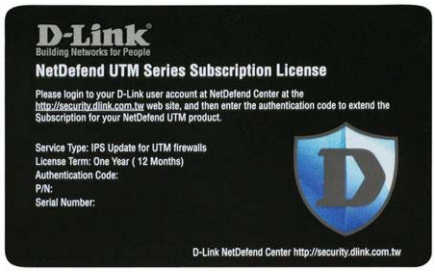
Der in den UTM Firewalls integrierte Virenscanner stammt von Kaspersky. Dieser renomierte Anbieter stell auch sicher, , dass die Firewalls stets mit aktuellen Virensignaturen versorgt werden. Um Verzögerungen durch den Virenscan zu minimieren, wird eine streambasierte Scantechnologie eingesetzt. Anstatt eine Datei zunächst komplett herunterzuladen und dann zu untersuchen, wird der Datenstrom, der die Datei enthält, IP-Paket für IP-Paket direkt untersucht und weitergeleitet. Dies ermöglicht das Scannen von Dateien beliebiger Größe und durch die Nutzung des integrierten Hardwarebeschleunigers geschieht dies besonders schnell.

### Dynamische Web Content Filter

Um den Zugriff auf Webseiten mit unerwünschten Inhalten zu verhindern, ist ein Web Content Filter integriert. Anhand von 32 Kategorien kann entschieden werden, welche Inhalte aus dem Web abrufbar sein sollen. Dazu greifen die UTM-Firewalls auf ein weltumspannendes Netzwerk von Datenbankservern mit Millionen von Einträgen zu, die ständig das gesamte Web kategorisieren. Darüber hinaus können zugelassene Webseiten von aktiven Inhalten wie z.B. ActiveX oder Java befreit werden, um den Zugriff auf erlaubte Inhalte sicherer zu gestalten.

### NetDefend UTM Subscriptions

Die Netdefend UTM Subscription Services sorgen dafür, dass Ihre UTM Firewalls stets Zugriff auf aktuelle Signaturen und Web Content Kategorien haben. Die Subscriptions können einzeln für die drei Funktionen IPS, Virenscanner und Web Content Filter abgeschlossen werden, so dass Sie nur für die Dienste bezahlen, die Sie wirklich nutzen. Beim Kauf einer UTM Firewall sind12-Monats-Lizenzen für IPS und den Virenscanner bereits enthalten, der Web Content Filter kann drei Monate kostenlos genutzt werden.




### Kostengünstige Weitverkehrsvernetzung mit VPN

Eine weitere wichtige Einsatzmöglichkeit für die UTM Firewalls ist die kostengünstige Vernetzung von Standorten sowie die Einwahl von Außendienstmitarbeitern über das Internet. Für die sicher verschlüsselten Verbindungen unterstützen die Geräte die Tunneling-Protokolle L2TP, PPTP und IPSec. Für Site-to-Site-VPNs wird die besonders effektive Hub & Spoke Topologie unterstützt. Durch die Nutzung standardisierter Protokolle können VPN-Verbindungen auch zu VPN-Servern und -Clients anderer Hersteller aufgebaut werden. Die Interoperabilität der D-Link-Produkte wurde von den anerkannten ICSA-Labs zertifiziert.

### Hochverfügbarkeit

Nicht nur Integrität, Vertraulichkeit und Authentizität gehören zu einer guten Sicherheitslösung, sondern auch die Verfügbarkeit. Deshalb unterstützen die Firewalls eine Vielzahl von Hochverfügbarkeitsfunktionen. Outbound Traffic Load Balancing und WAN-Failover ermöglichen die Nutzung von mehreren WAN-Verbindungen, so dass neben der Skalierbarkeit der Bandbreite die Anbindung ans Internet auch dann noch besteht, wenn eine Leitung ausgefallen ist. Server Load Balancing ermöglicht dagegen die Skalierung und Verfügbarkeitserhöhung von Servern hinter der Firewall, z.B. in einer DMZ.

# UTM Firewalls DFL-260 / DFL-860

## Ihr Nutzen

### Umfangreiche Netzwerkfunktionen

Durch die Unterstützung von VLANs und umfangreichen Routing-Funktionen wie z.B. OSPF kann beim Einsatz dieser Geräte oftmals auf einen zusätzlichen Router verzichtet werden. Dies verringert die Komplexität der Sicherheitsumgebung und reduziert Investitions- und Betriebskosten. Durch die integrierten Traffic Management-Funktionen werden Quality-of-Service-Anforderungen für Voice over IP oder andere zeitkritische Anwendungen durch die Firewalls mittels Priorisierung und Bandbreitenreservierung umgesetzt. Damit sind sowohl Sicherheit als auch Dienstqualität gleichermaßen gewährleistet.

## Technische Daten

### Firewall-System

- Transparenter Firewall-Modus
- NAT, PAT
- H.323 Traversal
- SIP ALG
- Zeitgesteuerte Regeln
- Application Layer Gateway

### Intrusion Detection & Prevention System (IDP/IPS)

- Automatisches Signatur-Update
- Schutz vor DoS und DDoS
- Angriffsalarmierung via Email
- Advanced IDP/IPS Subscription
- IP-Blacklist durch Schwellwert oder IDP/IPS

### Content Filtering

- HTTP: URL, Keyword
- Scripte: Java, ActiveX, Cookie, VB
- Email-Anteile: Blacklist, Keyword
- Nutzung einer externen Content-Filtering-Datenbank

### Anti-Virus

- Echtzeit-AV-Scanning
- Unlimitierte Dateigröße
- Scannen von VPN-Tunnel
- Unterstützt Virensignaturen von Kaspersky
- Automatisches Signatur-Update

### Blockierung von IM und P2P

**Unterstützte Applikationen:**
2 Find Mp3, Aimini, AOL Instant Messenger, ANts P2P, Ares P2P, Bit Torrent, Direct Connect, eDonkey, Gnutella, KaZaA, KCeasy, WinMX, iTunes, IRC, MSN Messenger, Yahoo! Messenger

### Layer 2-Funktionen

- DHCP-Server/-Client
- DHCP-Relay
- Policy-Based Routing
- IGMPv3

### Bandbreitenmanagement

- Policy-based Traffic Shaping
- Garantierte Bandbreite
- Maximale Bandbreite
- Bandbreite pro Priorität
- Dynamisches Bandbreiten-Balancing

### Traffic Load Balancing

- Outbound Load Balancing
- Traffic Redirect bei Fail-Over

### Virtual Private Network

- Verschlüsselungs-Algorithmen: DES, 3DES, AES, Twofish, Blowfish, CAST-128
- PPTP/L2TP Server
- Hub and Spoke
- IPSec NAT Traversal

### Benutzer-Authentifizierung

- Interne Datenbank
- RADIUS
- Microsoft Active Directory
- Webbasierte Authentifizierung
- Für IPSec-Authentifizierung: LDAP, XAUTH

### Management

- Consolen-Interface: RS-232
- Web-basierte Oberfläche über http und HTTPS
- Kommandozeile / SSH
- Firmware-Upgrade
- Backup & Restore der Konfiguration

### Logging und Monitoring

- Interne Protokollierung
- Externe Protokollierung zu einem Syslog-Server
- Email-Benachrichtigung
- SNMP v1, v2c

### Physikalische Eigenschaften

**Betriebstemperatur:** 0°C bis 40°C

**Lagertemperatur:** -20°C bis 70°C

**Relative Luftfeuchtigkeit (nicht kondensierend):**

- 5% bis 95%

**Emission (EMV)**

- FCC Class A
- CE Class A
- C-Tick

**Sicherheit**

- UL (nur DFL-260)
- LVD (EN60950-1)

ICSA labs CERTIFIED Firewall, Corporate
ICSA labs CERTIFIED IPSec
VPNC CERTIFIED Basic Interop
VPNC CERTIFIED AES Interop
FC CE UL LISTED ITE E141136 66F9 ACN 052 202 838

# UTM Firewalls DFL-260 / DFL-860

| Technische Daten | | DFL-260 | DFL-860 |
|---|---|---|---|
| | |  |  |
| Schnittstellen | | 1 Fast Ethernet WAN-Port<br>1 Fast Ethernet DMZ-Port<br>4 Fast Ethernet LAN-Ports | 2 Fast Ethernet WAN-Ports<br>1 Fast Ethernet DMZ-Port<br>7 Fast Ethernet LAN-Ports |
| Systemleistung | Firewall-Durchsatz | 80 MBit/s | 150 MBit/s |
| | VPN-Durchsatz | 25 MBit/s | 60 MBit/s |
| | Gleichzeitige Sessions | 12.000 | 25.000 |
| | Policies | 500 | 1.000 |
| Firewall System | Dynamisches Routing-Protokoll | – | OSPF |
| | Proaktive interne Netzwerksicherheit | – | ZoneDefense |
| Netzwerk | IEEE 802.1q VLAN | 8 | 16 |
| VPN | Dedizierte VPN-Tunnel | 100 | 300 |
| Traffic Load Balancing | Server Load Balancing | – | ☑ |
| Hochverfügbarkeit (HA) | WAN-Failover | ☑<br>(wenn DMZ-Port als WAN-Port konfiguriert ist) | ☑ |
| Stromanschluss | | Externes Netzteil | Externes Netzteil |
| Abmessungen | | 235 x162 x 36 mm<br>Desktop | 280 x 214 x 44 mm<br>Desktop |
| MTBF | | 21.571 Stunden | 36.879 Stunden |

## Garantie

5 Jahre

## Bestellinformationen

| **Artikelnummer**: | **Beschreibung**: |
|---|---|
| DFL-260/E | NetDefend UTM Firewall SoHo |
| DFL-860 | NetDefend UTM Firewall SMB |

## Zubehör

| **Artikelnummer**: | **Beschreibung**: |
|---|---|
| DFL260AV12 | DFL-260 12-Monate AV Lizenz |
| DFL260IPS12 | DFL-260 12-Monate IPS Lizenz |
| DFL260WCF12 | DFL-260 12-Monate WCF Lizenz |
| DFL860AV12 | DFL-860 12-Monate AV Lizenz |
| DFL860IPS12 | DFL-860 12-Monate IPS Lizenz |
| DFL860WCF12 | DFL-860 12-Monate WCF Lizenz |

## D-Link Kontaktinformationen


D-Link (Deutschland) GmbH
Schwalbacher Str. 74
D-65760 Eschborn
Fon: +49 (0)61 96 7799 0
Fax: +49 (0)61 96 7799 300
**www.dlink.de**

D-Link Schweiz
Glatt Tower, 2. OG, Postfach
CH-8301 Glattzentrum
Fon: +41 (0)44 832 11 00
Fax: +41 (0)44 832 11 01
**www.dlink.ch**

D-Link Österreich
Millennium Tower, Handelskai 94 - 96
A-1200 Wien
Fon: +43 (1)240 27 270
Fax: +43 (1)240 27 271
**www.dlink.at**




D-Link®
Building Networks for People