

## Allgemeines



Die FortiGate-60 ist ideal für den Einsatz im Smalloffice- Bereich gedacht. Die FortiGate-60 ist schnell installiert und über den browserbasierten Wizard einfach zu konfigurieren. Das Gerät bietet zwei WAN-Links für redundanten Internetzugang, einen separaten DMZ-Port sowie zwei USB-Ports für weitere Anschlussmöglichkeiten (z.B. Dial-up Modems, o.ä.).

## Performance

Firewall: 70 Mbps, 3 DES (168 Bit): 20 Mbps gleichzeitige Sessions: 50.000,  
VPN Tunnels: 40

## Anschlüsse

3 10/100 BaseTX-Ports (internes, externes Netz, DMZ) 1 RS232 Consolen-Port (9600)  
2 USB

## Anti-Virus

ICSA Labs zertifizierter Virus und Wurmschutz. Scant ein- und ausgehende E-Mail-Attachments (SMTP, POP3, IMAP) und den gesamten HTTP-Verkehr inklusive Web-basierter E-Mail.

## Web Content Filter

Der Administrator kann Schlüsselwörter definieren, auf die alle Webseiten gescannt werden. Sobald eine Webseite diese Schlüsselwörter enthält, wird sie nicht angezeigt. Ebenso können bestimmte URLs gesperrt werden. Cookies sowie ActiveX und Java Applets werden auf Wunsch ebenfalls gesperrt.

## Firewall

Stateful Inspection Firewall mit einfach zu konfigurierenden Regeln. Route- oder Transparent-Mode, Network Address Translation (NAT) und Port Address Translation. Interne Datenbank für die Benutzerauthentifikation. Über 20 Standard-Dienste wie z.B. HTTP oder FTP, zusätzlich benutzerspezifische Dienste und Dienst-Gruppen. Policy Schedules für die zeitliche Steuerung der Firewall. Virtual IP Mapping übersetzt öffentliche Adressen in interne Adressen. IP/MAC Binding verbindet IP-Adressen mit Ihren MAC-Adressen und verhindert somit IP-Spoofing.

## VPN

IPSec, PPTP und L2TP VPNs. Internet Key Exchange (IKE): Automatisch und manuell. Hardware-beschleunigte Verschlüsselung (DES, triple-DES, AES). IPSec und PPTP Client passthrough unterstützt.

## Intrusion Detection (IDS)

Real-Time Erkennung von über 1300 Attacken. Erkennt bekannte DoS (Denial of Service) und DDoS (Distributed Denial of Service) Attacken sowie bekannte Angriffe auf Schwachstellen der meisten Betriebssysteme und Applikations-Protokolle. Sendet bei einem Angriff Alarmmeldungen an bis zu drei E-Mail-Adressen.

## Logging

Sendet Log-Meldungen an einen Syslog-Host oder an ein NetIQ Webtrends Firewall Reporting Center. Verschiedene Logs für Traffic, Events und Attacken. Alle Logs können nach Schlüsselwörtern, Absender-/Empfängeradresse, Datum und Zeit durchsucht werden.

## Management

Policy Administration über ein einfach zu bedienendes grafisches Web-Interface. Wizard für die initiale Konfiguration. Remote Management verschlüsselt über HTTPS und SSH.

## Komponenten

Chassis, Stromkabel, AC-Adapter, LAN-Kabel, Manual, Quickstart-Guide.

Abmessungen 21,9 x 15,6 x 3,5 cm

Gewicht 0,68 kg

Stromversorgung 5 Volt, 3 Ampère

\*AES: Advanced Encryption Standard