

## **TUXGUARD** ICM FIREWALL

TUXGUARD ICM FIREWALL 60  
TUXGUARD ICM FIREWALL 500  
VIRTUAL APPLIANCE



### DIE REVOLUTIONÄRE ICM-TECHNOLOGIE MIT NEXTGEN INSIDE

Die Intelligent Cyber Management (ICM) Firewalls mit NextGen inside von TUXGUARD schützen mit integriertem Cyber Defense Research und Realtime Cyber Security umfangreich und uneingeschränkt vor Cyberbedrohungen.

Phishing, Malware, Ransomware und anderer unerwünschter Datenverkehr und Angreifer werden analysiert, bereinigt und geblockt, bevor diese in Ihr Netzwerk gelangen.

Die ICM FIREWALLs mit NextGen inside und Realtime Cyber Security sind für den SMB- bis Enterprise-Markt designt – alles made in Germany 🇩🇪



Revolutionäre ICM Technologie



Realtime Cyber Security



Eigenes Cyber Defense Research



NextGen inside



IMD-, IPD-, IRD-Detection



100% Made in Germany & DSGVO-konform



Schutz für Unternehmen jeder Größe

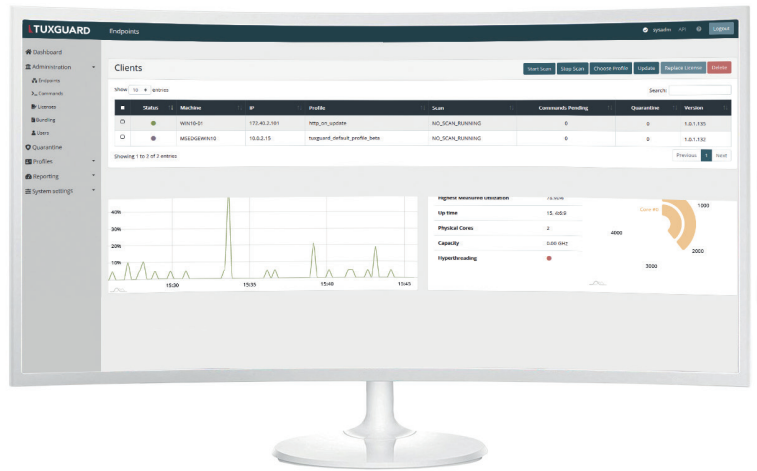


Dashboard mit Realtime-Daten

## NEHMEN SIE PLATZ IN IHREM REALTIME CYBER SECURITY COCKPIT!

Volle Kontrolle, Sichtbarkeit und Sicherheit – das Realtime Cyber Security Dashboard!

Das Dashboard dient Ihnen als Operation Center für die perfekte Übersicht zur Administration der TUXGUARD ICM FIREWALLS. So erhalten Sie alle wichtigen Informationen in Realtime und verwalten, steuern und kontrollieren zentral alle sicherheitsrelevanten Aufgaben.



Volle Kontrolle Realtime Cyber Security Dashboard



## TUXGUARD ICM FIREWALL 60

Ideal für Unternehmen mit bis zu 60 Arbeitsplätzen (konfigurationsabhängig) sowie als dezentrale Firewall oder Teil eines Filialnetzes nutzbar.

### TUXGUARD ICM FIREWALL 60

- ✓ TUXGUARD ICM Firewalls mit NextGen inside
- ✓ Erweiterten Sicherheitskomponenten IMD, IPD, IRD
- ✓ Realtime Cyber Security zum Schutz vor Phishing, Malware, Ransomware...
- ✓ Vollständige IPV6 Unterstützung
- ✓ VPN Gateway
- ✓ Nutzung als Hotspot
- ✓ Lüfterlose Firewall
- ✓ IPS
- ✓ TLS Encrypted Traffic Inspection
- ✓ Website Filtering
- ✓ QOS
- ✓ Anti Virus
- ✓ PIM 3rd Party

### Hardware

Bauart	Desktop
Prozessor	Intel Celeron 2C, 1.10GHz Prozessor
Memory	8 GB RAM
Ethernet Ports	3 x 10/100/1.000 Mbit
Storage	256 GB SSD (mSATA/SSD)
Kühlung	lüfterlos
Netzteil	12 V, 5 A, extern
Abmessungen	231 mm (B) x 44 mm (H) x 197 mm (T)
Gewicht	2,35 kg
Zertifizierungen	kgFCC, Class B/CE, Class B
Garantie	1 Jahr



## TUXGUARD ICM FIREWALL 500

Besonders geeignet für Unternehmen ab 60 - 500 Arbeitsplätze (konfigurationsabhängig) und als zentrale Firewall oder Teil eines großen Filialnetzes.

### TUXGUARD ICM FIREWALL 500

- ✓ TUXGUARD ICM Firewalls mit NextGen inside
- ✓ Erweiterten Sicherheitskomponenten IMD, IPD, IRD
- ✓ Realtime Cyber Security zum Schutz vor Phishing, Malware, Ransomware...
- ✓ Vollständige IPV6 Unterstützung
- ✓ VPN Gateway
- ✓ VoIP-Proxy
- ✓ Integration in Microsoft Active Directory
- ✓ Nutzung als Hotspot
- ✓ Cluster-Fähigkeit – Aktiv-Passiv
- ✓ IPS
- ✓ TLS Encrypted Traffic Inspection
- ✓ Website Filtering
- ✓ QOS
- ✓ Anti Virus
- ✓ PIM 3rd Party

### Hardware

Bauart	Desktop
Prozessor	Intel Atom 4C 2GHz
Memory	bis 64 GB (4 Bänke)
Ethernet Ports	6 x 10/100/1.000 Mbit, 2 x 10 Gbit
SFP+ Storage	mSATA (SSD)
Kühlung	Lüfter
Netzteil	12 V, 5 A, extern
Abmessungen	231 mm (B) x 44 mm (H) x 197 mm (T)
Gewicht	1,64 kg
Zertifizierungen	FCC/CE/RoHS
Garantie	1 Jahr

### TUXGUARD ICM VIRTUAL APPLIANCE

## Virtual Appliance

- ✓ TUXGUARD ICM Firewalls mit NextGen inside
- ✓ Erweiterten Sicherheitskomponenten IMD, IPD, IRD
- ✓ Realtime Cyber Security zum Schutz vor Phishing, Malware, Ransomware...
- ✓ Zentrale Firewall für besonderen Anforderungen wie z. B. für Branchen mit kritischen Infrastrukturen, Rechenzentren u. v. m.
- ✓ Skalierbar für alle Unternehmensgrößen
- ✓ Entwicklung, Programmierung, Produktion in Deutschland

### Kompatibilität

Arbeitet problemlos mit folgenden Virtual-Machine-Anbietern:



# TECHNISCHE INFORMATIONEN ICM FIREWALLS



ICM FIREWALL	ICM FIREWALL 60	ICM FIREWALL 500	Virtual Appliance
<b>HDN Cyber Defense</b>			
IMD - Intelligent Malware Domain Detection**	✓	✓	✓
IPD - Intelligent Phishing Detection**	✓	✓	✓
IRD - Intelligent Ransomware Detection**	✓	✓	✓
<b>Network</b>			
IPv4 und IPv6	✓	✓	✓
Link Aggregation (LACP)	✓	✓	✓
Multi-WAN mit Loadbalancing und Failover	✓	✓	✓
VLAN und VXLAN	✓	✓	✓
NTP	✓	✓	✓
Zugriffskontrolle	✓	✓	✓
<b>DHCP und DNS</b>			
DHCPv4 und DHCPv6 mit Relay und BOOTP Support	✓	✓	✓
Dynamic DNS	✓	✓	✓
Caching DNS mit Host/Domain Overwrites	✓	✓	✓
Zugriffskontrolle	✓	✓	✓
<b>Firewall</b>			
Statefull Inspection Firewall (SIF)	✓	✓	✓
Operation System Fingerprinting (OSFP)	✓	✓	✓
Network Address Translating (NAT)	✓	✓	✓
Regelbasierte Limitierung gleichzeitiger Verbindungen	✓	✓	✓
Packet Normalisation	✓	✓	✓
Protokollierung je Regel aktivierbar	✓	✓	✓
Policy Based Routing	✓	✓	✓
Gruppierungen via Aliase	✓	✓	✓
Kategorisierung von Regelketten	✓	✓	✓
DROP und EDROP	✓	✓	✓
GeoIP	✓	✓	✓
Verbindungsstatuskontrolle	✓	✓	✓
Pure Router Betrieb ohne Firewall	✓	✓	✓
Ausführliche Diagnosewerkzeuge	✓	✓	✓
<b>VPN</b>			
IPsec mit IKEv1, IKEv2, NAT-T, DPD	✓	✓	✓
OpenVPN	✓	✓	✓
WireGuard	✓	✓	✓
Stunnel	✓	✓	✓
<b>Traffic Shaper und QOS</b>			
Regelbasiertes Matching	✓	✓	✓
Bandbreitenmanagement	✓	✓	✓
Gemeinsame Nutzung von Bandbreiten	✓	✓	✓
Priorisierung	✓	✓	✓
Unabhängig von Firewallregeln	✓	✓	✓
<b>Traffic Shaper und QOS</b>			
Intelligent Ransomware Detection (IRD)	✓	✓	✓
Intelligent Maleware Domain Detection (IMD)	✓	✓	✓
Intelligent Phishing Detection (IPD)	✓	✓	✓
Deep Packet Inspection (DPI)	✓	✓	✓
SSL Fingerprinting	✓	✓	✓

\*HDN Cyber Defense ist ein Produkt der Hakdefnet GmbH

\*\*Leistungsdaten der Firewall sind abhängig von Anzahl der User und Konfiguration



ICM FIREWALL	ICM FIREWALL 60	ICM FIREWALL 500	Virtual Appliance
<b>Captive Portal (Gästenetzwerk, BYOD)</b>			
Mehrere Zonen	✓	✓	✓
Templates für eigene Corporate Identity	✓	✓	✓
Authentifizierung via LDAP, Radius, Local User Manager	✓	✓	✓
Vouchers und Tickets	✓	✓	✓
Splash Screen Only	✓	✓	✓
Timeouts und Welcome Back	✓	✓	✓
Bandbreitenmanagement	✓	✓	✓
Portal Bypass P	✓	✓	✓
Reporting in Echtzeit	✓	✓	✓
<b>Hochverfügbarkeit</b>			
Automatischer Hardware Failover	✓	✓	✓
Synchronisation Konfiguration	✓	✓	✓
Synchronisierter Verbindungsstatus	✓	✓	✓
<b>Monitoring</b>			
SNMP	✓	✓	✓
Netflow Exporter	✓	✓	✓
Netflow Analyser	✓	✓	✓
Netflow CVS Export	✓	✓	✓
<b>Zwei-Faktor-Authentisierung (2FA)</b>			
Time-based One-time Password (TOTP)	✓	✓	✓
Google Authenticator	✓	✓	✓
Für Captive Portal, Proxy, VPN und WebGUI	✓	✓	✓
<b>Email</b>			
Multidomain SMTP-Relay	✓	✓	✓
Adressumschreibung	✓	✓	✓
Header Checks	✓	✓	✓
<b>Email Spam und Maleware Filter</b>			
Geblockte Dateiendungen	✓	✓	✓
Graylisting	✓	✓	✓
SPF	✓	✓	✓
DKIM	✓	✓	✓
MX-Check	✓	✓	✓
Phishing	✓	✓	✓
Rate-Limits	✓	✓	✓
Spam Trap	✓	✓	✓
RBL	✓	✓	✓
SURBL	✓	✓	✓
Virensan	✓	✓	✓
<b>Virens Scanner</b>			
Internet Content Adaption Protocol (ICAP)	✓	✓	✓
ClamAV	✓	✓	✓
Für E-Mail	✓	✓	✓



ICM FIREWALL	ICM FIREWALL 60	ICM FIREWALL 500	Virtual Appliance
<b>Webproxy</b>			
HTTP, HTTPS, FTP und WebDAV	✓	✓	✓
SSH, SCP und SFTP	✓	✓	✓
Caching Proxy	✓	✓	✓
Multi-Interface	✓	✓	✓
Transparenter Modus	✓	✓	✓
TLS/SSL Inspection	✓	✓	✓
Automatische Konfiguration via WPAD/PAC	✓	✓	✓
Access Control Lists (ACLs)	✓	✓	✓
Blacklists	✓	✓	✓
Kategorienbasierter Webfilter	✓	✓	✓
Traffic Management	✓	✓	✓
Single-Sign-On (SSO) für LDAP, MS AD, Radius u.w.	✓	✓	✓
Virensan via ICAP	✓	✓	✓
<b>Reverse Proxy</b>			
HTTP, HTTPS und FTP	✓	✓	✓
SMTP, POP3 und IMAP	✓	✓	✓
TCP und UDP Datenströme	✓	✓	✓
Load Balancer und Failover	✓	✓	✓
WAF	✓	✓	✓
SNI Based Routing	✓	✓	✓
<b>Zertifikatsverwaltung</b>			
Integrierte Zertifikatsverwaltung	✓	✓	✓
Self-Signed	✓	✓	✓
Let's Encrypt	✓	✓	✓
<b>Weitere Dienste</b>			
Internet Group Management Protocol (IGMP)	✓	✓	✓
Radius	✓	✓	✓
Link Layer Discovery Protocol (LLDP)	✓	✓	✓
VOIP SIP Proxy	✓	✓	✓
<b>Firmware und Updates</b>			
REST-API	✓	✓	✓
Easy Upgrade	✓	✓	✓
Umfangreiche Dokumentation	✓	✓	✓

# TUXGUARD ICM FIREWALL 60 TUXGUARD ICM FIREWALL 500 VIRTUAL APPLIANCE



DIE REVOLUTIONÄRE ICM-TECHNOLOGIE  
FÜR ALLE UNTERNEHMENSGRÖSSEN.  
IN JEDER HINSICHT EIN GEWINN!

- TUXGUARD ICM Firewalls mit NextGen inside
- Erweiterten Sicherheitskomponenten IMD, IPD, IRD
- Realtime Cyber Security zum Schutz vor Phishing, Malware und Ransomware
- Geeignet für Firmen von bis zu 60/500 Arbeitsplätzen (konfigurationsabhängig)
- Vollständige IPV6 Unterstützung