

# FIREBOX V

Erstklassige Netzwerksicherheit für Ihre virtuelle Umgebung



Unternehmen und Organisationen jeder Größe befassen sich mit dem Thema Virtualisierung, um einerseits Kosten sparen und andererseits die Effizienz, Flexibilität und Verfügbarkeit ihrer IT-Ressourcen steigern zu können. Doch Virtualisierung hat auch ihren Preis, schließlich sind virtuelle Umgebungen komplex in der Verwaltung und zudem anfällig gegenüber Sicherheitsbedrohungen. Genau darauf muss die IT-Abteilung vorbereitet sein. Hier kommt WatchGuard ins Spiel. Der Schutz entsprechender Anwendungen kann ab sofort über ein einziges Unified-Management-System garantiert werden – bei minimalem Aufwand. Denn mit WatchGuard FireboxV trifft Virtualisierung auf Best-in-Class-Netzwerksicherheit. Dank Echtzeitüberwachung, Multi-WAN-Unterstützung und skalierbaren Lösungen für Unternehmen jeder Größe steht Ihre virtuelle Umgebung der physischen in Sachen Sicherheit in nichts nach.

*Die virtuellen Lösungen von WatchGuard überzeugen mit herausragender Flexibilität bei der Bereitstellung. Knüpfen Sie ein Netzwerk aus interagierenden physischen und virtuellen Appliances, die alle über eine zentrale Plattform verwaltet werden. Die virtuellen Appliances von WatchGuard bieten die gleichen Sicherheits- und Netzwerkservices wie unsere physischen Appliances. Der Einsatz im Rahmen einer virtualisierten Infrastruktur erfolgt individuell – entweder nach Kunde, Abteilung oder Anwendung.*

## MAXIMALE FLEXIBILITÄT DANK VIRTUALISIERUNG DER URSPRÜNGLICHEN GATEWAY-FIREWALL

WatchGuard FireboxV schützt nicht nur den physischen, sondern auch den virtuellen „Rand“ des Rechenzentrums. So können Sie bequem Regeln umsetzen, um Daten aus der Unternehmensdatenbank von E-Mail-Diensten oder vertrauliche Personaldaten von den Finanzdaten anderer Geschäftsbereiche fernzuhalten – selbst wenn sich alles auf demselben Server befindet.

## DEUTLICH MEHR EFFIZIENZ DANK FIREWALL-KONSOLIDIERUNG

Hosting- bzw. Cloud-Dienstleister sowie Managed Security Service Provider können mehrere FireboxV-Instanzen auf Servern am Perimeter des Rechenzentrums bereitstellen. Diese virtuellen Firewalls werden separat betrieben, so dass für jeden Mandanten eigene SLA (Service Level Agreements) gelten können und Konfigurationsänderungen nur die jeweilige Firewall betreffen. Zur Verwaltung aller Instanzen dient eine einzige benutzerfreundliche Konsole.

## SCHLUSS MIT UNNÖTIGEN HARDWAREKOSTEN BEI DER ABSICHERUNG VIRTUELLER NETZWERKE – STANDORTKONSOLIDIERUNG

Wenn an einem größeren Standort oder in einem Geschäftsbereich verschiedene lokale Server (z.B. für Dateien, das Drucken oder Sprachanwendungen) zusammengefasst werden, lässt sich auf dem physischen Server eine virtuelle Firewall aufsetzen, die den Datenverkehr vom öffentlichen Internet fernhält. Die Verbindung zum Unternehmensrechenzentrum oder in die virtuelle Private Cloud erfolgt dann über einen sicheren VPN-Tunnel, was an den einzelnen Standorten Kosten spart – ohne Kompromisse bei der Sicherheit eingehen zu müssen.

## FUNKTIONEN UND VORTEILE

- Einsatz von virtuellen Appliances in der virtuellen Umgebung
- Virtuelle Infrastruktur mit führenden UTM-/NGFW-Funktionen und -Services
- Inklusive WatchGuard Dimension™, einer Public- und Private-Cloud-fähigen Visualisierungslösung, die Rohdaten umgehend in entscheidungsrelevante Sicherheitsinformationen umwandelt
- Einfach herunterzuladen, zu aktivieren, bereitzustellen und zu verwalten (zentrale Konsole, Weboberfläche, CLI)
- Unterstützt die Flexibilität und Verfügbarkeit von vSphere und Hyper-V
- Unterschiedliche Varianten für Organisationen jeder Größe
- Geeignet für Bildungseinrichtungen, Cloud/Hosting, Standortkonsolidierung
- Bereitstellung pro Kunde, Abteilung oder Anwendung

Modellname	Max. Anzahl CPU-Kerne	Benutzer	TDR-Host-Sensoren	Firewall (Mbit/s)	VPN (Mbit/s)	VPN-Nutzer
Small	2	50	50	2.000	400	50
Medium	4	250	150	4.000	1.500	600
Large	8	750	250	8.000	3.000	6.000
XLarge	16	1.500	250	Unbegrenzt	Unbegrenzt	10.000

**SICHERHEITSFUNKTIONEN**

Firewall	Stateful Packet Inspection, Deep Packet Inspection, Proxy-Firewall
Anwendungsproxies	HTTP, HTTPS, FTP, DNS, TCP/UDP, POP3, POP3S, SMTP, IMAPS, and Explicit Proxy
Angriffsschutz	DoS-Attacken, fragmentierte Pakete, komplexe Bedrohungen und vieles mehr
Filteroptionen	Browser Safe Search, YouTube für Schulen, Google for Business
Sicherheitsabonnements	APT Blocker, IPS, Gateway AV, WebBlocker, App Control, Data Loss Prevention, Reputation Enabled Defense, spamBlocker, Network Discovery, Threat Detection and Response, Access Portal

**MANAGEMENT**

Protokollierung und Benachrichtigungen	WatchGuard, Syslog, SNMP v2/v3
Benutzeroberflächen	Weboberfläche, skriptfähige CLI
Reporting	WatchGuard Dimension enthält über 100 vordefinierte Berichte sowie Übersichtsdarstellungen und Visualisierungswerkzeuge.

**NETZWERKFUNKTIONEN**

QoS	8 Priority Queues, DiffServ, Modified Strict Queuing
IP-Adresszuweisung	DHCP (Client)
NAT	Statisch, dynamisch, 1:1, IPsec traversal
Weitere Funktionen	Statisches Routing, Port-Unabhängigkeit

**VPN UND AUTHENTIFIZIERUNG**

Verschlüsselung	DES, 3DES, AES 128-, 192-, 256-bit
IPSec	SHA-2, IKE Pre-shared Key, Drittanbieterzertifikatimport, IKEv1/v2, Suite B
Single Sign-On	Windows, Mac OS X, mobile Betriebssysteme, RADIUS, SAML 2.0
Authentifizierung	RADIUS, LDAP, Windows Active Directory, RSA SecurID, interne Datenbank, SAML 2.0

**UMFASSENDE SICHERHEIT AUF ALLEN EBENEN**

Aufgrund ihrer einzigartigen Architektur und fundierten Abwehrmechanismen gegen Malware, Ransomware, Botnets, Trojaner, Viren, Drive-by-Downloads, Datenverlust, Phishing und mehr gelten die Netzwerksicherheitslösungen von WatchGuard als die intelligentesten, schnellsten und leistungsfähigsten auf dem Markt.

Funktionen und Dienste	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway Antivirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection and Response	✓	
DNSWatch	✓	
Access Portal	✓	
IntelligentAV	✓	
Dimension Command	✓	
Support	Gold (24x7)	Standard (24x7)

**VERSCHIEDENE KAUFOPTIONEN**

Die Flexibilität der integrativen WatchGuard-Plattform macht's möglich: Stellen Sie einfach die Sicherheitskomponenten zusammen, die Ihr Unternehmensnetzwerk tatsächlich benötigt. Dabei spielt es keine Rolle, ob Sie mit einer Grundsicherung beginnen oder umfassendere Maßnahmen zum Schutz Ihres Netzwerks etablieren möchten – wir stimmen unsere Sicherheitsdienste genau auf Ihre jeweiligen Anforderungen ab.

**BERATUNG UND SUPPORT DURCH EXPERTEN**

Mit jedem Firebox-Modell erhalten Sie ein Startabonnement für den Support. Der in der Basic Security Suite enthaltene Standard-Support bietet technischem Support rund um die Uhr und Software-Updates. Ein Upgrade auf den Gold-Support ist Bestandteil der Total Security Suite von WatchGuard.

Weitere Details erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter [www.watchguard.de](http://www.watchguard.de).