

	Firebox T15/T15-W	Firebox T20/T20-W	Firebox T35/T35-W/T35-R*	Firebox T40/T40-W	Firebox T80	Firebox M270	Firebox M370	Firebox M470	Firebox M570	Firebox M670	Firebox M4800 Basiskonfiguration + 4 x 10 Gbit/s-Ports	Firebox M5800 Basiskonfiguration + 4 x 10 Gbit/s-Ports
Datendurchsatz und Verbindungen												
Firewall (UDP 1518)	400 Mbit/s	1,7 Gbit/s	940 Mbit/s	3,4 Gbit/s	4,7 Gbit/s	4,9 Gbit/s	8 Gbit/s	19,6 Gbit/s	26,6 Gbit/s	34 Gbit/s	49,6 Gbit/s	87 Gbit/s
VPN (UDP 1518)	150 Mbit/s	485 Mbit/s	560 Mbit/s	880 Mbit/s	1,4 Gbit/s	1,6 Gbit/s	4,6 Gbit/s	5,2 Gbit/s	5,8 Gbit/s	7,6 Gbit/s	16,4 Gbit/s	18,8 Gbit/s
AntiVirus	120 Mbit/s	328 Mbit/s	325 Mbit/s	623 Mbit/s	1,15 Gbit/s	2,1 Gbit/s	3,0 Gbit/s	3,5 Gbit/s	5,4 Gbit/s	6,2 Gbit/s	12,5 Gbit/s	22 Gbit/s
IPS (vollständiger Scan)	160 Mbit/s	271 Mbit/s	573 Mbit/s	510 Mbit/s	909 Mbit/s	2,3 Gbit/s	4,8 Gbit/s	5,7 Gbit/s	8,0 Gbit/s	10,4 Gbit/s	20 Gbit/s	33 Gbit/s
UTM (vollständiger Scan)	90 Mbit/s	154 Mbit/s	278 Mbit/s	300 Mbit/s	631 Mbit/s	1,6 Gbit/s	2,6 Gbit/s	2,1 Gbit/s	3,5 Gbit/s	4,2 Gbit/s	5,2 Gbit/s	11,3 Gbit/s
Schnittstellen	3 x 1 Gbit/s	5 x 1 Gbit/s	5 ^l x 1 Gbit/s	5 ^l x 1 Gb	8 x 1 Gbit/s**	8 x 1 Gbit/s**	8 x 1 Gbit/s**	8 x 1 Gbit/s**	8 x 1 Gbit/s**	8 x 1 Gbit/s**	8 x 1 Gbit/s Weitere Ports verfügbar***	8 x 1 Gbit/s und 4 x 10 Gbit/s Fiber Weitere Ports verfügbar***
I/O-Schnittstellen	1 Seriell / 1 USB	1 Seriell / 2 USB	1 Seriell / 2 USB	1 Seriell / 2 USB	1 Seriell / 2 USB	1 Seriell / 2 USB	1 Seriell / 2 USB	1 Seriell / 2 USB	1 Seriell / 2 USB	1 Seriell / 2 USB	1 Seriell / 2 USB	1 Seriell / 2 USB
Gleichzeitige Verbindungen	95.000	100.000	135.000	200.000	200.000	2.000.000	3.300.000	3.800.000	8.300.000	8.500.000	15.000.000	30.800.000
Neue Verbindungen pro Sekunde	2.400	8.500	6.800	18.000	25.000	40.000	51.000	82.000	115.000	140.000	254.000	328.000
VLAN-Support	10	10	50	50	75	100	300	400	750	1.000	1.000	Unbegrenzt
Limit für authentifizierte Anwender	200	200	500	500	500	500	500	Unbegrenzt	Unbegrenzt	Unbegrenzt	Unbegrenzt	Unbegrenzt
VPN-Tunnel												
VPN zwischen Standorten	5	10	25	30	60	50	100	250	500	750	5.000	Unbegrenzt
Mobile VPN IPSec	5	10	25	30	60	75	150	250	500	750	10.000	Unbegrenzt
WLAN												
Wireless Access Points (APs)	WatchGuard bietet eine umfassende Auswahl an Access Points, mit denen sich die Sicherheitsfunktionalitäten der Firebox-Plattform gezielt im WLAN nutzen lassen. Die Verwaltung dieser Access Points erfolgt entweder über die Cloud oder den in die Firebox integrierten Wireless Controller.											
Max. APs pro Modell†	4	4	20	20	20	20	20	20	20	20	20	20
Integriertes WLAN	Integriertes 802.11a/b/g/n erhältlich für Firebox T15-W. Integriertes 802.11a/b/g/n/ac erhältlich für Firebox T20-W, T35-W und T40-W											
Merkmale Betriebssystem												
Erweiterte Netzwerkfunktionen	Dynamisches Routing (BGP, OSPF, RIPv1,2) / SD-WAN dynamische Pfadauswahl / NAT: statisch, dynamisch, 1:1, IPSec traversal, Policy-basiertes PAT / Traffic-Shaping & QoS: 8 Priority Queues, DiffServ, Modified Strict Queuing / virtuelle IP-Adresse für Server-Lastausgleich											
Verfügbarkeit	Hochverfügbarkeit – aktiv/passiv und aktiv/aktiv für Clustering (nicht erhältlich bei drahtlosen Modellen) / VPN-Failover / Multi-WAN-Failover / Multi-WAN-Lastausgleich / Link Aggregation (802.3ad dynamisch, statisch, aktiv / Backup)											
Sicherheitsdienste												
Basic Security Suite	Anwendungskontrolle / Intrusion Prevention Service / WebBlocker / Gateway Antivirus / Reputation Enabled Defense / Network Discovery / spamBlocker / Standard-Support (24 x 7)											
Total Security Suite	Anwendungskontrolle / Intrusion Prevention Service / WebBlocker / Gateway Antivirus / Reputation Enabled Defense / Network Discovery / spamBlocker / APT Blocker / Threat Detection and Response / DNSWatch / IntelligentAV / Gold-Support (24 x 7 und optimierte Reaktionszeiten)											

* Die Firebox T35-R ist ein robustes, IP64-konformes Gerät für extreme Umgebungen.

** Die Firebox M470, 570 und 670 werden mit einem leeren Steckplatz ausgeliefert, der eines der folgenden Module aufnehmen kann: 4 x 10 Gbit/s Glasfaser, 8 x 1 Gbit/s Glasfaser oder 8 x 1 Gbit/s Kupfer.

***Die Datendurchsatzraten der Firebox-Modelle M4800 und M5800 wurden anhand der Basiskonfiguration + 4 x 10 Gbit/s-Ports bestimmt. Beide Modelle werden mit zwei leeren Steckplätzen ausgeliefert, die die folgenden Module in beliebiger Kombination aufnehmen können: 4 x 10 Gbit/s Fiber, 8 x 1 Gbit/s Fiber und 8 x 1 Gbit/s Kupfer, 2 x 40 Gbit/s Fiber.

† Nutzen Sie den Gateway Wireless Controller (GWC), um in Umgebungen mit geringer Client-Dichte und wenigen Störungen die maximale Anzahl empfohlener APs zu verwalten. Für anspruchsvollere Umgebungen wird eine Secure Wi-Fi- oder Total Wi-Fi-Lizenz empfohlen.

^l Optionen für Power over Ethernet (PoE): Firebox T40 (1) und T80 (2) enthalten integrierte PoE+-Ports.

Durchsatzraten werden mithilfe von Messungen an mehreren Anschlüssen ermittelt und variieren je nach Umgebung und Konfiguration. Der maximale Firewall-Datendurchsatz wurde entsprechend der RFC-2544-Methodik mit 1518-Byte-UDP-Paketen geprüft. Wenden Sie sich an Ihren WatchGuard-Händler oder rufen Sie WatchGuard unter der Nummer +49 700 92229333 direkt an wenn Sie Unterstützung bei der Auswahl des richtigen Modells benötigen. Online-Unterstützung erhalten Sie unter www.watchguard.com/sizingtool

Jede WatchGuard-Appliance umfasst die folgenden Funktionen:

Sicherheitsfunktionen

- Stateful Packet Firewall, Deep Packet Inspection, Anwendungsproxies: HTTP, HTTPS, FTP, DNS, TCP/UDP, POP3, POP3S, SMTP, IMAPS, Explicit Proxy
- Blockiert Spyware, DoS-Attacken, fragmentierte und schadhafte Pakete, Blended Threats und vieles mehr
- Analyse von Protokollabweichungen, Verhaltensanalyse, Mustervergleich
- Statische und dynamische Liste der blockierten Quellen
- VoIP: H.323 und SIP, Verbindungsaufbau und Sitzungsschutz

Logging & Reporting mit WatchGuard Dimension™

- Echtzeit-Protokollaggregation und -Berichterstattung für mehrere Appliances
- Geeignet für öffentliche & private Clouds
- Hohe Übersichtlichkeit durch intuitive und interaktive Visualisierungen
- Erkennen Sie Trends und Ausreißer und gewinnen Sie wichtige Einblicke in Ihren Netzwerkverkehr und Ihre Netzwerknutzung
- Mehr als 100 Berichte, unter anderem zur Einhaltung der PCI- und HIPAA-Vorgaben
- Möglichkeit zur Übermittlung von Berichten (PDF, CSV) per E-Mail
- Anonymisierung für die Einhaltung von Datenschutzrichtlinien

Managementsoftware

- Für das Management von WatchGuard-Appliances können die folgenden Komponenten verwendet werden:
- Dimension Command für die interaktive Verwaltung mehrerer Appliances in Echtzeit über einen Webbrowser
 - Weboberfläche für die Verwaltung einer einzelnen Appliance über einen Webbrowser
 - WatchGuard System Manager für die intuitive Verwaltung von Appliances über einen Windows-Client
 - Befehlszeilenschnittstelle (CLI) für den Direktzugriff per Skripten
 - Vereinfachte Konfiguration und Implementierung dank RapidDeploy

Benutzerauthentifizierung

- Transparente Active Directory-Authentifizierung (Single Sign-On)
- RADIUS, LDAP, Windows Active Directory, VASCO, RSA SecurID, internal database, SAML 2.0, SMS Passcode
- RSA SecurID® und VASCO
- Lokale Datenbank
- 802.1X für WLAN-Appliances (Firebox T15-W, T-35-W, T55-W)
- Microsoft® Terminal Services und Citrix XenApp -Umgebungen werden unterstützt

Support- und Wartungsoptionen

- Der in der Basic Security Suite enthaltene Standard-Support bietet eine Hardware-Garantie inklusive Geräte austausch, technischem Support rund um die Uhr und Software-Updates
- Ein Upgrade auf den Gold-Support – Bestandteil der Total Security Suite – beinhaltet neben sämtlichen Leistungsmerkmalen des Standard-Supports darüber hinaus optimierte Reaktionszeiten
- Weitere Informationen zu den Support-Stufen von WatchGuard und anderen Serviceoptionen finden Sie unter <https://www.watchguard.com/de/wgrd-international/support>



Netzwerkbedrohungen können jederzeit aus allen Richtungen kommen und Ihre Systeme lahmlegen, bevor Sie überhaupt von ihrer Existenz erfahren. Aufgrund ihrer einzigartigen Architektur und fundierten Abwehrmechanismen gegen Malware gelten die Netzwerksicherheitslösungen von WatchGuard als die intelligentesten, schnellsten und leistungsfähigsten auf dem Markt. Sie bieten IT-Experten dank universell einsetzbarer Sicherheits- und Visualisierungswerkzeuge für die Bedrohungserkennung eine komplette Kontrolle über ihre Netzwerke auf Enterprise-Niveau – unabhängig von Budget, Größenordnung oder Komplexität des Unternehmens.

Unser WLAN + Ihr Unternehmen = Endlose Möglichkeiten

Cloudveraltetes WLAN von WatchGuard wurde von Grund auf für Unternehmen aller Branchen und Größenordnungen konzipiert und bietet marktweit die beste Kombination aus Sicherheit, Leistung und Handhabbarkeit.

- **Patentierter WLAN-Sicherheit** gewährleistet den erforderlichen Schutz
- **Dieses WLAN wächst mit Ihren Anforderungen:** Es ermöglicht Ihrem Unternehmen eine einfache Skalierung von einzelnen Access Point (AP) bis zu einer unbegrenzten Anzahl – ohne Infrastrukturanforderungen
- **Umfangreiche Analysemöglichkeiten** liefern Echtzeit-Auswertungen des aktuellen Datenverkehrs und des Gesamtverlaufs in bedarfsgerecht konfigurierbaren Dashboards
- **Leistungsstarke Werkzeuge für den Dialog mit Kunden** bieten eine ansprechende Erfahrung beim WLAN-Gastzugang

WIRELESS ACCESS POINTS

Egal wo Sie Drahtlostechnik einsetzen – ob an dezentralen Standorten, für Gäste-WLAN, den Zugang zum Unternehmensnetz, öffentlichen Hotspots oder in Außenbereichen – bei WatchGuard finden Sie ein breites Sortiment von Access Points für sämtliche geschäftlichen Anforderungen sowie APs, die die neuesten 802.11ac Wave 2-Standards erfüllen.

Weitere Informationen zu unseren WLAN-Lösungen finden Sie unter www.watchguard.com/wifi

„Die Bereitstellung eines sicheren, zuverlässigen Hochleistungs-WLAN mit wesentlich höheren Übertragungsgeschwindigkeiten als 54 Mbit/s stellt für unsere Gäste, Besucher und in Besprechungsräumen einen echten Mehrwert dar.“

- WatchGuard-Kunde Fahyaz Khan, IT-Manager, Kensington Close Hotel

Über WatchGuard

WatchGuard® Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Mehr als 80.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen von WatchGuard profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält WatchGuard Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.com.

