



- **Leistungsstarke Sicherheit** für Niederlassungen und Kleinunternehmen
- **Zuverlässige, flexible Netzwerkoptionen** gewährleisten Schutz und Konnektivität für Niederlassungen und Kleinunternehmen
- **Einfach zu konfigurierende VPN-Tunnel** bieten vollständigen Netzwerkzugriff für Niederlassungen und mobile Benutzer
- **Einfache Verwaltung und Priorisierung** des Netzwerkverkehrs über QoS-Einstellungen (Quality of Service)
- **Integrierte, intuitive Verwaltung der Sicherheitsfunktionen** für eine einfache Administration
- **Skalierbare Lösungen und Modell-Upgrades** schützen Ihre Investitionen in die Sicherheit
- **Ein globales Team aus Sicherheitsexperten** steht Ihnen jederzeit zur Seite

Effektiver Schutz für Niederlassungen und Kleinunternehmen

Durch die Integration bewährter SOHO- und Edge-Sicherheitsfunktionen mit einer neuen hochleistungsfähigen Hardware-Plattform bieten Firebox X Edge Security Appliances von WatchGuard leistungsstarken Netzwerkschutz für Kleinunternehmen und Niederlassungen. Das System, das als eigenständige integrierte Security-Appliance oder VPN-Endpunktlösung eingesetzt werden kann, wartet mit Funktionen wie Stateful-Packet-Firewall, VPN und URL-Filtering sowie einer modernen Netzwerk- und Datenverkehrsverwaltung auf. Die Konfiguration der Upgrade-fähigen Edge-Modelle lässt sich wahlweise und sehr benutzerfreundlich über eine intuitive Online-Benutzeroberfläche oder zentral mit WatchGuard System Manager® ausführen. Mit unserem marktführenden LiveSecurity® Service stellen wir dazu noch das umfassendste Support- und Wartungspaket der Branche.

Umfassende Netzwerkfunktionen

Zuverlässige, flexible Netzwerkfunktionen garantieren dauerhaften Schutz und Konnektivität für Kleinunternehmen und Niederlassungen.

Sichere und effiziente Verkehrsverwaltung

- Sicherheit für mehrere externe IP-Adressen
- Unterstützung für Dynamisches NAT, 1:1 NAT und PAT (Port Address Translation)
- Kürzere Betriebsausfallzeiten durch WAN-Failover

Zuverlässiger, konfigurierbarer QoS

- Über die Konfiguration weisen Sie kritischem Datenverkehr, wie VoIP, die benötigte Priorität und entsprechende Bandbreite zu

Sicherer Zugriff auf Netzwerkressourcen

Mit VPN-Tunneln und verschlüsselten Verbindungen garantiert die Firebox X Edge sicheren und umfassenden Zugriff auf wichtige Netzwerkressourcen für Niederlassungen und mobile Benutzer.

Flexible Wireless-Sicherheit

Die Firebox X Edge Wireless Appliances verfügen über einen 802.11b/g Wireless Access Point mit WPA- und WEP-Sicherheitsoptionen, über den firmenfremde Personen kontrolliert auf das Internet zugreifen können, ohne die Netzwerksicherheit zu gefährden.

Benutzerfreundlichkeit

Die Firebox X Edge, die über eine intuitive, benutzerfreundliche Webschnittstelle verwaltet wird, lässt sich im Handumdrehen installieren und konfigurieren und bietet somit beste Benutzerfreundlichkeit für Profis und Einsteiger.

Ausweitung des UTM-Schutzes auf den Netzwerkrand

Indem Sie die Leistungsstärke Ihrer UTM-Lösung (Unified Threat Management) über die Firebox X Edge auf Ihre Niederlassungen ausweiten, profitieren auch Ihre Firebox Edge Anwender von den Funktionen der Firebox® X Core™

und Firebox® X Peak™ Appliances wie Zero-Day-Angriffsschutz, Antivirus, Anti-Spam und Intrusion Prevention und damit einer optimalen Netzwerksicherheit.

Zentrale Verwaltung für mehrere Niederlassungen

Als Endpunkte Ihres Firebox X Core oder Firebox X Peak Netzwerks implementierte Firebox Edge Appliances können zentral über WatchGuard System Manager (WSM) verwaltet werden. Dieser bietet eine vereinfachte VPN-Verwaltung und Konfiguration und ermöglicht die Erstellung von VPN-Tunneln in drei einfachen Schritten, das Pushing von Appliance-Softwareupdates auf alle verwalteten Edge-Geräte und die Einrichtung einheitlicher Sicherheitsrichtlinien für das gesamte Netzwerk. Weiterhin enthalten sind eine umfassende Protokollierung, flexible Sicherheitsrichtlinien und Tools zur Echtzeit-Überwachung.

Besserer Schutz vor Bedrohungen aus dem Internet

Mit WebBlocker, einem integrierten URL-Filtering-Dienst der Firebox X, kontrollieren Sie die Internetverbindung und den Zugriff auf Webinhalte.

- Schützen Sie Ihr Netzwerk vor gefährlichen Webinhalten wie Spyware und Phishing-Sites sowie Attacken von unseriösen Websites
- Steuern Sie die Internetnutzung, um Haftungsansprüche zu vermeiden bzw. die Mitarbeiterproduktivität zu steigern

Schutz Ihrer Investitionen

Bei steigenden Ansprüchen können Sie beliebig Lizenzen oder Netzwerk- und Sicherheitsfunktionen hinzufügen – und zwar ohne Ihre Hardware austauschen zu müssen.

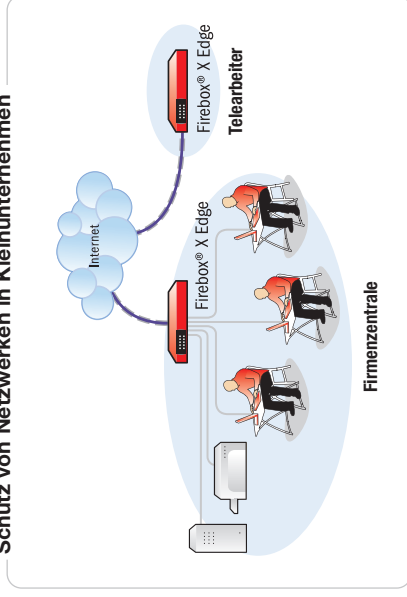
- Wenn Sie mehr Kapazität benötigen, führen Sie ein Upgrade auf ein höherwertiges Modell durch. Dazu müssen Sie nur einen einfachen Lizenzschlüssel erwerben und installieren
- Auf die gleiche Weise fügen Sie weitere VPN-Lizenzen für mobile Benutzer hinzu
- Mehr Schutz vor Bedrohungen aus dem Internet und risikoreichem Websurfing bietet dazu unser URL-Filtering-Dienst

Bester Schutz und robuste Konnektivität für Netzwerke von Kleinunternehmen

Das Verwalten eines Netzwerks in einem Kleinunternehmen ist eine echte Herausforderung. Angesichts der Vielzahl an Bedrohungen aus dem Internet brauchen Sie soliden Schutz für Ihr Netzwerk, den aber ein einfacher Router nicht bieten kann. Zudem sehen sich Kleinunternehmen nicht selten den gleichen Problemen ausgesetzt wie Großfirmen, wie eine Vielzahl anspruchsvoller Anwendungen, hohes Verkehrsaufkommen sowie mobile Benutzer. Und auch wenn bei einer solchen Firma die Ressourcen traditionell begrenzt sind, soll es eine Lösung sein, die sowohl benutzerfreundlich als auch erschwinglich ist und eine gewisse Zukunftssicherheit bietet.

Die Lösung: Firebox X Edge von WatchGuard – perfekt für Netzwerke von Kleinunternehmen.

Schutz von Netzwerken in Kleinunternehmen



Warum die Firebox X Edge für Kleinunternehmen Sinn macht

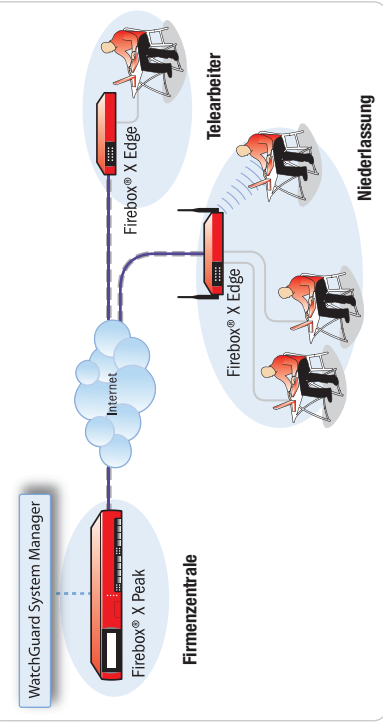
- **Einfache Installation und Verwaltung** über eine intuitive Online-Benutzerschnittstelle. Auch EDV-Einsteiger können die Appliance im Handumdrehen installieren und konfigurieren
- **Robuste Sicherheit direkt aus der Box** mit intelligenten Standardeinstellungen und Konfigurationsassistenten für optimalen Schutz vom ersten Tag an
- **Zuverlässige, flexible Netzwerkoptionen** für eigenständige Büros, inklusive erweiterter Funktionen wie 1:1 NAT, Dynamisches NAT, PAT (Port Address Translation) und Support für mehrere externe IP-Adressen
- **Verkehrsverwaltung und QoS (Quality of Service)** gewährleisten die benötigte Bandbreite für missionskritischen Verkehr, wie z. B. VoIP
- **Kürzere Betriebsausfallzeiten** dank WAN/WAN-Failover bei einer Unterbrechung der Verbindung zum primären WAN-Port
- **Wireless-Sicherheit und Guest Services** bieten kontrollierten Internetzugang für firmenfremde Personen, und zwar ohne Gefährdung des Netzwerks
- **Schutz von Benutzern und Netzwerk** vor Bedrohungen aus dem Internet – mit WebBlocker, dem URL-Filtering-Dienst von WatchGuard
- **Sicherer Zugriff auf wichtige Netzwerkkressourcen** für Telearbeiter über Offsite-Workstations, und zwar per VPN-Tunnel und Authentifizierung für mobile Benutzer
- **Mehr Kapazität und Netzwerk-/Sicherheitsfunktionen** bei wachsenden Anforderungen, und zwar ohne Austausch der bestehenden Hardware. Ein einfacher Lizenzschlüssel (per Download verfügbar) genügt, um Ihre Firebox Edge in eine noch leistungsfähigere Appliance zu verwandeln
- **Das Expertenteam** unseres preisgekrönten LiveSecurity® Service hält Sie auf dem Laufenden und bietet Unterstützung bei neuen Bedrohungen

Schutz der Netzwerkumgebung

Die Erweiterung der robusten Netzwerksicherheit von Ihrer Firmenzentrale auf Niederlassungen sollte Ihre EDV-Abteilung keine zusätzlichen Ressourcen kosten. Sie benötigen den gleichen leistungsstarken Schutz am Netzwerkrand, müssen aber gleichzeitig in der Lage sein, das gesamte System zentral verwalten zu können. Um maximale Effizienz und niedrige Betriebskosten zu ermöglichen, sollten alle Komponenten Ihrer Sicherheitslösung dazu noch nahtlos miteinander integriert sein. Erst dadurch ist es möglich, einheitliche Sicherheitsrichtlinien für das gesamte Netzwerk einzurichten, die sich global per Mausclick aktualisieren lassen. Außerdem müssen die Kabel- oder Wireless-Appliances in der Firmenzentrale und in der Niederlassung über moderne Netzwerkfunktionen verfügen, die eine Priorisierung des innerbetrieblichen Datenverkehrs mit der entsprechenden Bandbreite ermöglichen.

Die Lösung: Firebox X Edge von WatchGuard – sie ermöglicht die effiziente Ausweitung der Leistungskraft Ihrer Firebox X Core oder Firebox X Peak von der Firmenzentrale auf Ihre Niederlassungen.

Schutz von Niederlassungen und Telearbeiter-Sites



Warum die Firebox X Edge für Niederlassungen Sinn macht

- Die **UTM** -Funktionen Ihrer Firebox X Core oder Peak Appliance, inklusive echtem Zero-Day-Angriffschutz, können auf die Filialen Ihres Netzwerks ausgedehnt werden, um leistungsstarken, mehrschichtigen Schutz zu bieten
- **Die zentrale Konfigurationsverwaltung** über WatchGuard System Manager (WSM) der Firebox X Core oder Peak Appliance ermöglicht eine einfache Administration Ihrer Niederlassungen
- **Sicherung der innerbetrieblichen Konnektivität** durch VPN-Tunnel für Niederlassungen. Mit WSM erstellen Sie VPN-Tunnel in drei einfachen Schritten per Drag&Drop und verschwenden keine kostbare Zeit für Installation und Wartung
- **Appliance-Softwareupdates** per WSM Push. Damit stellen Sie sicher, dass auf allen Edge-Remote-Appliances die gleiche Version installiert ist und Sicherheitsrichtlinien schnell und einheitlich implementiert werden können
- **Moderne Netzwerkfunktionen** der Firebox X Edge: 1:1 NAT, Dynamisches NAT, PAT (Port Address Translation) sowie Support für mehrere externe IP-Adressen und damit zuverlässige, flexible Netzwerkoptionen
- **QoS mit dynamischer Verkehrsverwaltung** gewährleistet, dass Bandbreite sinnvoll verwaltet und missionskritischem Verkehr, wie z. B. VoIP, die notwendige Priorität eingeräumt wird
- **Firmenfremden Personen kann ohne Gefährdung der Netzwerksicherheit** über Wireless Guest Services und den Wireless Access Point der Firebox Edge Appliance kontrollierter Zugriff aufs Internet gewährt werden

Technische Daten	Firebox® X10e WG50010	Firebox® X10e-W WG50011* WG50012**	Firebox® X20e WG50020	Firebox® X20e-W WG50021* WG50022**	Firebox® X55e WG50055	Firebox® X55e-W WG50056* WG50057**
Modell-Upgrade	auf X20e oder X55e	auf X20e-W oder X55e-W	auf X55e	auf X55e-W	--	--
Firewall-Durchsatz***	100 Mbps	100 Mbps	100 Mbps	100 Mbps	100 Mbps	100 Mbps
VPN-Durchsatz***	35 Mbps	35 Mbps	35 Mbps	35 Mbps	35 Mbps	35 Mbps
URL-Filtering	Optional	Optional	Optional	Optional	Optional	Optional
Serielle Ports	1	1	1	1	1	1
Schnittstellen 10/100	6	6	6	6	6	6
Sicherheitszonen (enthalten)	2	2	2	2	2	2
Gleichzeitige Sitzungen	6.000	8.000	8.000	8.000	10.000	10.000
Unterstützte Knoten (LAN IPs)	15 (Upgrade auf 20 möglich)	30	30	30	Unbegrenzt	Unbegrenzt
VPN-Tunnel für Niederlassungen	5	15	15	15	25	25
VPN-Tunnel für mobile Benutzer (inkl./max.)	1/11	5/25	5/25	200	5/55	5/55
Obergrenze für die Local User Authentication DB	200	200	200	200	200	200

*Verfügbar in Nordamerika

**Verfügbar außerhalb von Nordamerika

***Durchsatzraten variieren je nach Umgebung und Konfiguration

Funktionen

Sicherheitsfunktionen

- Stateful-Packet-Firewall
- Malformed Packet-Schutz
- Liste statisch geblockter Sites
- URL-Filtering

VPN

- Verschlüsselung (DES, 3DES)
- IPSec
 - SHA-1, MD5
 - IKE - Pre-Shared Key, Firebox-Zertifikat
- IPSec Passthrough
- PPTP Passthrough
- Dead Peer Detection (RFC 3706)
- Hardware-basierte Verschlüsselung

Benutzerauthentifizierung

- XAUTH
- LDAP
- Windows® Active Directory
- Lokale Authentifizierung
- Windows® NT
- Windows® 2000
- Windows® 2003

IP-Adresszuweisung

- Static
- Dynamische DNS
- PPPoE-Client
- DHCP-Server
- DHCP-Client
- DHCP-Relay

Redundanzfunktionen

- WAN-Failover
 - WAN-Failover-Ports - 1

Verkehrsverwaltung- und Priorisierung

- Verkehrspriorisierung
- QoS (Quality of Service)
 - 4 Prioritäts-Warteschlangen (Stufen)

Moderne Netzwerkfunktionen

- Statisches NAT
- Dynamisches NAT
- 1:1 NAT
- IPSec NAT Traversal
- Richtlinien-basierte PAT (Port Address Translation)
- Bis zu 8 externe IP-Adressen
- Statisches Routing – bis zu 100

Protokollierung/Berichterstellung

- Syslog
- WebTrends®-kompatible Berichte (verfügbar für WSM-Benutzer)
- HTML-Berichte (verfügbar für WSM-Benutzer)
- Verschlüsselter Protokollkanal (verfügbar für WSM-Benutzer)

Management-Software

- WatchGuard System Manager (WSM) v8.3.1 oder höher
- Win32 Management-Schnittstelle

Appliance-Software

- v8.x oder höher

Wireless-Sicherheitsfunktionen

- Wireless Guest Services
- 802.11b/g
- WPA, WEP-Schlüssel

Support & Wartun

- 1-Jahres-Hardware-Garantie
- 90 Tage LiveSecurity® Service Abonnement

Abmessungen/Leistungswerte

Abmessungen Appliance	
Kabelmodell	18,8 x 16,5 x 36 cm
Wireless-Modell (bei ausgezogener Antenne)	26,9 x 16,5 x 18,5 cm
Abmessungen Verpackung	
Kabelmodell	33,8 x 30,2 x 11,2 cm
Wireless-Modell	33,8 x 30,2 x 11,2 cm
Gewicht Appliance	
Kabelmodell	0,8 kg
Wireless-Modell	0,9 kg
Gesamtgewicht	
Kabelmodell	1,5 kg
Wireless-Modell	1,7 kg
WEEE-Gewicht	
Kabelmodell	0,9 kg
Wireless-Modell	1 kg

Spannung	100-240 VAC Autosensing
Stromverbrauch	USA: 12 Watt Restliche Länder: 172 Kal/min oder 0,68 BTU/min
Rack-fähig	Ja

Umgebungsbedingungen

Betriebstemperatur	0-45° C
Ruhefemperatur	-10-70° C
Betriebsfeuchte	10 - 85%
Ruhefeuchte	5 - 90% nicht-kondensierend bei 55° C
Nicht periodische Schwingungen (Ruhezustand)	7 - 28 Hz 0,001 bis 0,01 G2 pro Hz
Mechanischer Schock (Betrieb)	20 G mit 11 ms Dauer 1/2 Sinuswelle
WEEE/RoHS-konform	Ja



Beratung und Support durch Experten

Unser LiveSecurity Service ist das umfassendste Support- und Wartungspaket der Branche. Ein globales Team aus Sicherheitsexperten bietet Ihnen jegliche Unterstützung für eine bessere Verwaltung Ihrer Netzwerksicherheit. Zum Leistungsumfang gehören Softwareupdates, technischer Support durch unsere Experten, aktuelle Sicherheitswarnungen, vorzeitiger Hardwareaustausch sowie Selbsthilfe-Ressourcen wie Schulungen, Zertifizierungen und Lernprogramme. Unternehmen mit missionskritischen Internetanforderungen können zudem unseren Premium-Service in Anspruch nehmen.

RoHS-konforme Hardware-Plattformen

Produkte der Firebox X Edge e-Serie erfüllen die Anforderungen der RoHS-Direktive (Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment), die am 1. Juli 2006 in Kraft tritt.

WatchGuard wird auch weiterhin seine Ressourcen und Firmenrichtlinien dazu einsetzen, möglichst umweltschonende Produkte herzustellen.

Weitere Informationen zur Firebox X Edge finden Sie unter www.watchguard.com/appliances.

ADRESSE: WatchGuard Technologies Schellerdamm 16 21079 Hamburg Germany · WEB: www.watchguard.com · E-MAIL: germany@watchguard.com · GERMANY SALES: +49 40 689876 10 · FAX: +49 40 689876 76

Für die Richtigkeit/Aktualität der hierin enthaltenen Informationen (die jederzeit geändert werden können) wird weder eine ausdrückliche noch eine konkludente Garantie übernommen. Zukünftige Produkte oder Funktionen werden zum gegebenen Zeitpunkt zur Verfügung gestellt.
©2006 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard Logo, Firebox, LiveSecurity, Core, Peak und Stronger Security, Simply Done sind in den USA und/oder anderen Ländern entweder Markenzeichen oder eingetragene Markenzeichen von WatchGuard Technologies, Inc. Alle anderen Markenzeichen oder Markennamen sind Eigentum ihrer jeweiligen Besitzer. FileID: WGCE66389_061506