



## Erweitern Sie den Zugriff auf alle Anwendungen oder Netzwerkressourcen von überall, und zwar ohne Beeinträchtigung der Sicherheit.

Auf der Suche nach sicheren Lösungen für den Remote-Zugriff sehen sich viele mittelständische Unternehmen heutzutage vor eine schwere Wahl gestellt. IPSec ist sehr schwierig zu implementieren und zu verwalten und der Support für Remote-Benutzer kann sich wegen unzuverlässiger Verbindungen, blockiertem Zugriff aufgrund von Problemen mit der Firewall-Durchlässigkeit sowie Kompatibilitätsproblemen beim Kunden als sehr komplex und kostspielig erweisen. Viele aktuelle SSL-VPN-Lösungen enthalten zudem Beschränkungen für Anwendungen und Protokolle und sind komplex in Einrichtung und Verwaltung. Als EDV-Administrator aber benötigt man eine zuverlässige Lösung.

Der Firebox<sup>®</sup> SSL Core<sup>™</sup> VPN-Gateway ist die VPN-Lösung, die universellen Zugriff auf alle Anwendungen oder Netzwerkressourcen bietet, und zwar ohne Stecker, Module oder Probleme mit der Client-Verwaltung – es sind keinerlei Extras erforderlich.

### Zuverlässiger universeller Zugriff

Mit zwei leistungsstarken Zugriffsmodi in einer Lösung können Sie die Reichweite Ihres Netzwerks auf einfachste Weise erweitern.

- **Secure Access Client-Modus.** Autorisierte Benutzer stellen ihre Verbindung über einen automatisch aktualisierten Web-Client her. Darüber erhalten sie dann Zugriff auf jede Anwendung oder Netzwerkressource, genau wie mit Ihrem Desktop-PC im Büro. Außerdem stehen ihnen Client-Failover-Funktionen zur Verfügung, dank derer Remote-Verbindungen stets aktiv bleiben.
- **Kiosk-Modus.** Autorisierte Benutzer können mit Hilfe webaktivierter Handhelds, Laptops, Desktops und Internet-Kiosks, deren Browser SSL in Java<sup>™</sup>- und Microsoft<sup>®</sup>-Windows<sup>®</sup>-Umgebungen unterstützen, sicher auf Webanwendungen, Citrix<sup>®</sup>-Server oder andere webbasierte Netzwerkressourcen zugreifen.

Unabhängig vom verwendeten Modus bietet das Firebox SSL Core VPN-Gateway Zugriff über jede Firewall und unterstützt alle wichtigen Betriebssysteme und Protokolle, einschließlich TCP, UDP (VoIP) und ICMP.

### Unerreichte Benutzerfreundlichkeit

Sie erhalten robusten, sicheren Zugriff direkt aus der Box, und das ohne zusätzliche Kosten, Neukonfigurationen, Entwicklungsarbeit oder administrative Probleme. So bleiben Sie jederzeit und überall im Geschäft.

- Für den universellen Zugriff auf Netzwerk und Anwendungen sind keine zusätzlichen Komponenten, Adapter oder spezielle Application Connectors nötig
- Es ist keinerlei Installation, Wartung oder Unterstützung von Clients notwendig – der Client wird bei der Verbindung zum Netzwerk automatisch aktualisiert
- Intuitive Schnittstellen sorgen für eine erhebliche Reduzierung des Zeitaufwands bei der Konfiguration und Verwaltung von Zugriffsrichtlinien
- Kein Unterschied zum Arbeiten mit dem Desktop-PC im Büro feststellbar. So kann der Benutzer ebenso produktiv arbeiten wie mit einer LAN-Verbindung

### Leistungsstarke Sicherheit

Das Firebox SSL Core VPN-Gateway bietet robuste Sicherheit zwischen Zugriffsgerät und Netzwerk, sowohl für verwaltete als auch für nicht verwaltete Geräte, und zwar über alle Protokolle.

- Vor der Freigabe des Netzwerkzugriffs wird der Sicherheitsstatus des Endpunkts geprüft, und zwar über Geräteattribute wie IP-Adressen, Firewall-Einstellungen, Betriebssystem, Patch-Level sowie den Status der Antivirus-Software
- Verschlüsselung: 196-Bit TLS unterstützt alle OpenSSL-Codes, darunter 3DES und RC4
- Verbirgt IP-Adressen von Remote-Netzwerken, um den Wurm-Traversal zu verhindern
- Sitzungs-Timeouts schützen vertrauliche Firmeninformationen vor nicht autorisierten Benutzern
- Über Sitzungen im Kiosk-Modus werden Bilder, aber keine Daten transportiert – es ist keine Löschung des Cache erforderlich
- Zusätzliche Sicherheitsfunktionen, wie die 2-Faktor-Authentifizierung und autorisierte digitale Zertifikate, machen Schluss mit Sicherheitsproblemen bei der Erweiterung des Netzwerkzugriffs
- Kann mit einer integrierten Firebox X Security Appliance implementiert werden, um Schutz vor netzwerk-, anwendungs- oder inhaltsbasierten Angriffen zu bieten

### Umfassende administrative Kontrolle

Mit der einfachen, aber detaillierten Zugriffssteuerung können Sie schnell und einfach den Benutzer- und Gruppenzugriff einrichten und verwalten, und zwar über einen einzigen zentralen Standort mit integrierter Protokollierung und Berichterstellung. Sie können:

- Zugriffsrichtlinien für Benutzer und Gruppen mit robustem Authentifizierungs-Support wie LDAP, Radius, Windows<sup>®</sup> Domain und RSA SecurID<sup>®</sup> zuweisen
- Den Netzwerkzugriff für Geräte über integrierte Endpunkt-Sicherheitsprüfungen steuern
- Erweiterte Netzwerkfunktionen wie IP-Pooling, optionales Split-Tunneling, Lastausgleich und dynamisches oder statisches Routing nutzen, um die benötigte Flexibilität für wachsende Netzwerktopologien zu erhalten

### Niedrigere Betriebskosten

Nutzen Sie das Beste aus IPSec und SSL VPN, aber ohne Einschränkungen und in einer einzigen Komplettlösung. Realisieren Sie erhebliche Kosteneinsparungen durch:

- Keine zusätzlichen Adapter, Application Connectors oder komplexen Netzwerkneukonfigurationen
- Keine Installation oder fortlaufende Pflege von Client-Software
- Intuitive Schnittstellen für EDV-Administratoren, die den Zeitaufwand für die Konfiguration und Verwaltung von Zugriffsrichtlinien reduzieren
- Integriertes Desktop-Sharing für SSL-verschlüsselten Support per Remote-Helpdesk
- Umfassendes Support-Paket der Sicherheitsexperten unseres LiveSecurity<sup>®</sup> Service

**TECHNOLOGIEVERGLEICH**

Funktionen	VPN IPSec	Andere SSL VPNs	Passerelle de VPN SSL Firebox-Core
Umfassender Netzwerkzugriff	✓	Beschränkt und kostspielig	✓
Unterstützung für alle Protokolle	✓		✓
Unterstützung für alle Applikationen	✓		✓
Kein Unterschied zum Bürobetrieb	✓		✓
Zugriff über jede Firewall		✓	✓
Zugriff ohne Clients von überall aus		✓	✓
Verhindert Wurm-Traversal		✓	✓
Zugriffskontrolle auf Anwendungsbasis		✓	✓
Automatisch aktualisierter, per Internet implementierter Client**			✓
Always-on-Funktion/Persistent Connection			✓
Es bleiben keine Daten auf dem öffentlichen Kiosk zurück		Extra	✓
Integriertes Desktop-Sharing			✓
Integrierte Endpunktsicherheit direkt aus der Box			✓
Unterstützt & optimiert den UDP-Verkehr, inklusive VoIP			✓

\* Im Kiosk-Modus haben autorisierte Benutzer Zugriff auf unterstützte webbasierte Anwendungen über webaktivierte Geräte, wie PDAs oder Smartphones, mit JVM-Version 1.2.4 oder höher, deren Browser SSL in Java- oder Windows-Umgebungen unterstützt. Zu diesen Anwendungen gehören Citrix® ICA, Remote Desktop, SSH, Telnet 3270 Emulator und VNC-Clients. Webanwendungen müssen Mozilla unterstützen.

\*\*Im Secure Access Client-Modus stellen autorisierte Benutzer Ihre Verbindung über einen automatisch aktualisierten, per Web implementierten Client her und können so auf beliebige Anwendungen oder Netzwerkressourcen zugreifen.

Technische Daten für den	Firebox SSL Core VPN-Gateway
Max. Tunneldurchsatz	75 Mbps
Max. VPN-Tunnel – gleichzeitig	205
Tunnel im Secure Access Client-Modus	205
Tunnel im Kiosk-Modus	3
Intel-basierter	1,2 GHz Prozessor
Sicherheits-Coprozessor	SafeNet SafeXcel-1141
Speicher – Compact Flash	64 MB
Speicher – RAM	256 MB
Aktive Netzwerkschnittstellen	2 x 10/100
Serielle Anschlüsse	1 DB9
Festplatte (enthalten)	40 GB
Netzteil	100-240 VAC Autosensing
Abmessungen in Zoll	H: 445mm, B: 426mm, T: 248mm
Gewicht	4,3 kg
LiveSecurity® Service	90 Tage (Erstabonnement)

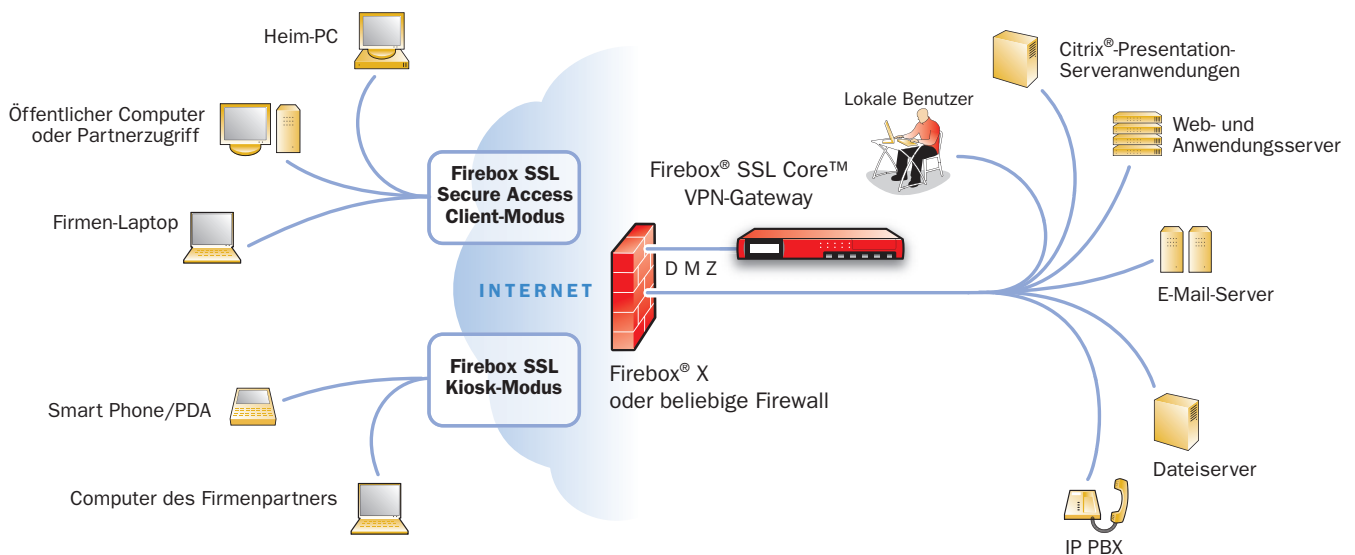
**Wann ist SSL VPN eine bessere Wahl als IPSec VPN?**

SSL VPN eignet sich bestens für Organisationen mit vielen mobilen Benutzern, die sich von verschiedenen Standorten aus ins Netzwerk einwählen.

- Bietet Mitarbeitern eine enorme Flexibilität beim Zugriff auf das Netzwerk von praktisch jedem Standort aus über webaktivierte Geräte wie Laptops, PDAs und Smartphones
- Ermöglicht es, bestimmte Bereiche Ihres Netzwerks unter Gewährleistung der Sicherheit Partnern, Beratern und Kunden zur Verfügung zu stellen
- Spart Zeit und Geld, denn der EDV-Administrator muss die Client-Software auf den Benutzergeräten nicht länger verwalten

**Firebox®-SSL-Bereitstellung**

Sicheren Zugriff erweitern - EDV-Supportkosten senken



Weitere Informationen finden Sie unter [www.watchguard.com/products/fb\\_ssl.asp](http://www.watchguard.com/products/fb_ssl.asp)

**ADRESSE:**  
WatchGuard Technologies Inc.  
Schellerdamm 16  
21079 Hamburg  
Germany

**WEB:**  
[www.watchguard.de](http://www.watchguard.de)  
**E-MAIL:**  
[germany@watchguard.com](mailto:germany@watchguard.com)

**GERMANY SALES:**  
+49 4068987610  
**FAX:**  
+49 4068987676

