

McAfee Firewall Enterprise-Appliance

Vollständige Bewertung und Eindämmung aller neuen Bedrohungen und Schwachstellen

Die immer zahlreicher werdenden Unternehmensanwendungen sowie die breite, sich schnell wandelnde Angriffsfläche von Web 2.0 erfordert einen neuen Ansatz bei der Firewall-Sicherheit. Die ersten Firewalls waren auf Ports, Protokolle und IP-Adressen beschränkt. Die heutigen, verbesserten McAfee®-Firewalls der nächsten Generation ermöglichen mithilfe ihrer visuellen Analyse- und Benutzeridentifizierungsfunktionen sowie durch effiziente und wirksame Regeln die zuverlässige Erkennung, Steuerung, Visualisierung und Absicherung sowohl neuer als auch vorhandener Anwendungen. Darüber hinaus haben wir zur Erkennung komplexer Bedrohungen innerhalb dieser Anwendungen eine präventive Bedrohungsentelligenz integriert, die mehrere Überprüfungsverfahren in einer kostengünstigen und leicht zu verwaltenden Appliance vereint.

Funktionen von McAfee Firewall Enterprise

McAfee AppPrism™: Anwendungs-erkennung und -steuerung, einschließlich:

- Paket- sowie zustands- und vollständig anwendungsbezogene Filterung
- Vollständige Anwendungserkennung und -steuerung
- Mehrere Ausbringungsoptionen, einschließlich Multi-Firewall-Appliances (bei denen eine Appliance bis zu 32 virtuelle Firewalls verwalten kann), McAfee Firewall Enterprise for Riverbed, McAfee Firewall Enterprise for Crossbeam sowie eine virtuelle Firewall-Appliance
- Network Address Translation (NAT)

McAfee AppPrism-Kategorien

- Anonymisierer / Proxies
- Authentifizierungsdienste
- Webbasierte Unternehmensanwendungen
- Content-Management
- Unternehmensüberwachung
- Datenbank
- Verzeichnisdienste
- E-Mail
- Verschlüsselte Tunnel
- ERP (Enterprise Resource Planning) / CRM (Customer Relationship Management)
- File-Sharing
- Computerspiele
- Instant Messaging
- Infrastrukturdienste
- IT-Dienstprogramme
- Software für mobile Systeme
- P2P-Netzwerk (Peer-to-Peer)
- Austausch von Foto-/Videodaten
- Fern-Administration
- Remote Desktop / Terminaldienste
- Social Networking
- Software- und System-Updates
- Speicherplatz
- Streaming-Medien
- Symbolleisten und PC-Dienstprogramme
- Voice over IP (VoIP)
- VPN
- Webmail
- Internet-Nutzung
- Internet-Konferenzen

Firewalls sind normalerweise immer genau so stark oder schwach wie die Richtlinien, die Sie definieren. Dabei hängt die effektive Sicherheit Ihrer für die heutigen komplexen Web 2.0-Daten entwickelten Richtlinien wesentlich von einem umfassenden Verständnis ab. Und dieses Verständnis zu entwickeln, ist unter Umständen schwierig. Sie benötigen eine unmittelbare Transparenz, die weit über Ports und Protokolle hinausgeht, und die Ihre vielschichtigen Web-Anwendungen und zahlreichen Benutzer ebenso einschließt wie die ausgefeilten Bedrohungen, denen diese ausgesetzt sind.

Konnten Sie es sich früher noch leisten, auf neue Signaturen zu warten, so erfordert die rasant fortschreitende Entwicklung heutiger Bedrohungen eine präventive, vorhersehbare Risikodiagnose. Dazu müssen zahlreiche Eigenschaften wie Quellen-Reputation, Inhalte und Verhalten bewertet werden, um schädigende Folgen feststellen zu können, bevor eine neue Bedrohung als solche bestätigt wird.

Es reicht nicht mehr aus, eine Bedrohung vorherzusagen zu können. Eine exakte und rechtzeitige Blockierung erfordert den gemeinsamen und kontrollierten Einsatz unterschiedlicher Produkte.

Diese Anforderungen sowie der Ruf nach Compliance-Nachweisen lassen die Arbeitsbelastung der Netzwerk-Teams ansteigen. Andererseits werden die Budgets immer weiter eingeschränkt. Irendetwas muss sich ändern.

Die größte Firewall-Innovation seit 15 Jahren

Mit der Version 8 von McAfee Firewall Enterprise hat McAfee die Firewall neu erfunden. Drei Innovationen bieten einen bisher unerreichten Schutz zu einem geradezu sensationellen Preis. Wir kombinieren vollständige Transparenz und Anwendungssteuerung mit reputationsbasierten Bedrohungsdaten und dem Schutz vor vielseitigen Angriffen. Damit steigern wir

Ihre Netzwerksicherheit und senken gleichzeitig Ihren Verwaltungsaufwand sowie Ihre Kosten.

Die Firewall-Lösung umfasst die McAfee Firewall Enterprise-Appliance-Familie: McAfee Firewall Enterprise Profiler, McAfee Firewall Enterprise Control Center und McAfee Firewall Reporter.

Das schwächste Glied in der Kette der Netzwerksicherheit ist heute die Anwendungsschicht. Also haben wir unsere in zahlreichen Hochsicherheitsumgebungen zuverlässig eingesetzte Firewall mit einer umfassenden Anwendungserkennung und -steuerung kombiniert. Damit können Sie nun Ihre neuen und bestehenden Web 2.0-Anwendungen vor den Risiken des Datenverlusts und des Netzwerkmissbrauchs sowie vor schädigenden Angriffen schützen. Mithilfe der McAfee-Technologie stellen Sie sicher, dass Ihre Netzwerkanwendungen ausschließlich zum Wohl Ihres Unternehmens eingesetzt werden.

Erkennung

Die McAfee AppPrism-Technologie nutzt den innovativen McAfee Firewall Enterprise Profiler, um sämtliche Datenströme und Anwendungen zu erkennen, die gerade im Einsatz sind. Wichtige ebenfalls bereitgestellte Zusatzinformationen sind Quelle, Bandbreite und Ziel der Daten. Durch die Untersuchung verschlüsselter anwendungsbezogener Daten können Schlupflöcher beseitigt werden, die vorzugsweise von Datendieben und anderen Angreifern verwendet werden.

Kontrolle

Die detaillierte Kontrolle ermöglicht die umfassende Umsetzung der an unternehmerische Anforderungen angepassten Richtlinien. Konnten diese Richtlinien früher nur an IP-Adressen, Ports oder Protokollen ausgerichtet werden, so besteht nun die Möglichkeit, Benutzernamen mit Verantwortlichkeiten und bestimmten Anwendungen zu verknüpfen.

Funktionen von McAfee Firewall Enterprise (Forts.)

Authentifizierung

- Lokal
- Microsoft Active Directory
- Transparente Identitäten für Active Directory (McAfee Logon Collector)
- LDAP (Sun, OpenLDAP, Custom LDAP)
- RADIUS
- Microsoft Windows-Domänenauthentifizierung
- Microsoft Windows NTLM-Authentifizierung
- Passport (Single Sign-On)
- Starke Authentifizierung (SecurID)
- Unterstützt CAC-Authentifizierung

Hochverfügbarkeit

- Aktiv/aktiv
- Aktiv/passiv
- Zustandsbezogenes Sitzungs-Failover
- IP-Remote-Überwachung

Global Threat Intelligence

- Bewertung von Netzwerkverbindungen mit McAfee Global Threat Intelligence™
- Standort-Filterung
- McAfee Labs™

Verschlüsselte Anwendungsfilerung

- SSH
- SFTP
- SCP
- Bidirektionale HTTPS-Entschlüsselung und erneute Verschlüsselung

Eindringungsschutzsystem (IPS)

- Über 10.000 Signaturen
- Automatische Signatur-Updates
- Anwendungsspezifische Signaturen
- Vorkonfigurierte Signatur-Gruppen

Viren- und Spyware-Schutz

- Schutz vor Spyware, Trojanern und Würmern
- Heuristik
- Automatische Signatur-Updates

Web-Filterung

- Integrierte McAfee SmartFilter®-Filterung und -Verwaltung
- Blockiert Java, Active-X, JavaScript und SOAP

Spam-Schutz

- Bewertung von Netzwerkverbindungen mit McAfee Global Threat Intelligence

VPN

- IKEv1 und IKEv2
- DES-, 3DES-, AES-128- und AES-256-Verschlüsselung
- SHA-1- und MD5-Authentifizierung
- Diffie-Hellmann-Gruppen 1, 2 und 5
- Richtlinieneingeschränkte Tunnel
- NAT-T
- Xauth

Sie können Nutzungsregeln für Anwendungen anhand bestimmter Attribute entwickeln:

- Betriebliche oder private Nutzung
- Benutzeridentität
- Integrierte Anwendungssteuerung
- Whitelists
- Standort-Filterung

Benutzeridentität

Ohne Transparenz oder Steuerung der Benutzer und der von ihnen verwendeten Inhalte können Firewalls keinen Schutz vor Port-wechselnden, flexiblen und gezielten Anwendungen bieten. McAfee Firewall Enterprise verwendet benutzerbezogene Regeln sowie Anwendungssteuerung.

Sobald ein Benutzer eine Verbindung herstellt, überprüft das System in Echtzeit anhand der bestehenden Benutzerverzeichnisse dessen Zugangsrechte. Die Firewall setzt daraufhin umgehend die dieser Benutzeridentität zugewiesenen Richtlinien um, welche dann explizit den Zugang zu einer bestimmten Anwendung ermöglichen.

Durch die Verfolgung der einzelnen Benutzer können die Regeln heutigen betrieblichen Anforderungen entsprechend ausreichend detailliert erstellt werden. Dabei sind identitätsbasierte Regeln in betrieblicher Hinsicht sehr sinnvoll. Immer mehr Unternehmen stützen sich bei der Zugangssteuerung zunehmend auf Identitäts-Management und die einheitliche Verwendung von Benutzerverzeichnissen. Änderungen der Benutzerdaten werden dabei nur einmal eingegeben und dann verteilt. Auch bei einer Änderung des Benutzerkreises bleiben die Sicherheitsrichtlinien aktuell.

Integrierte Anwendungssteuerung

Eine integrierte Anwendungssteuerung ermöglicht die Anpassung der Benutzerrechte innerhalb einer Anwendung. So können Sie beispielsweise den Zugang zu Yahoo gestatten, Yahoo IMs aber sperren. Oder Sie können die IM-Funktionen nur einer bestimmten Benutzergruppe gestatten, wie beispielsweise Support- und Vertriebsmitarbeitern, oder dies nur an bestimmten Standorten freischalten, z. B. in der Unternehmenszentrale.

Eine andere Möglichkeit besteht darin, durch die Angabe bestimmter Nutzungszeiten eine angemessene betriebliche Nutzung zuzulassen oder bestimmte Anwendungen zu blockieren. So könnte MySpace während der Mittagspause für den Kundendienst freigeschaltet werden, während Finanzanwendungen für Mitarbeiter tabu sind, die sich am Wochenende über VPN anmelden.

Zahlreiche Bedrohungen nutzen die weitmaschigen Sicherheitsfunktionen der Webseiten sozialer Netzwerke und verbergen ihre Schaden bringende Fracht hinter schicken Applikationen. Mit McAfee können Sie die sinnvollen Bestandteile von Webseiten wie Facebook freigeben und gleichzeitig das Risiko durch problematische Anwendungen auf diesen Webseiten minimieren.

Whitelists

Eine weitere Einschränkung der Nutzung von Anwendungen kann mithilfe von Whitelists erreicht werden, die lediglich die Daten von bestimmten Anwendungen zulassen, die als erforderlich oder angemessen betrachtet werden. Im Gegensatz zu langen Blacklists reduzieren Whitelists die Anzahl der Regeln, die erstellt und verwaltet werden müssen.

Standort-Filterung

Botnets werden mithilfe der Anwendungen beliebter sozialer Netzwerke verbreitet. Deshalb wird es immer wichtiger, Schaden verursachende Anwendungen zu blockieren, die mit bestimmten Standorten kommunizieren möchten. Durch die Standort-Filterung können Sie diese Kontakte sperren und Ihre Daten gegen unberechtigten Zugriff schützen. Außerdem verhindern Sie damit, dass Ihre Systeme für unlautere Zwecke missbraucht werden.

Wir ermöglichen die detaillierte Steuerung und vereinfachen gleichzeitig die Entwicklung der zugehörigen Regeln. Tatsächlich bekommen Sie mit jeder Ansicht immer genau eine Richtlinie. Dabei stellt eine einfach zu nutzende Konsole alle Optionen dar, mit denen Ihre Regeln effizient verwaltet und weitere Schutzfunktionen eingerichtet werden können. Dieses einheitliche Modell wird im Laufe der Zeit und abteilungsübergreifend besonders sinnvoll, da auch Abhängigkeiten und Überschneidungen einzelner Regeln hervorgehoben werden. Mögliche Probleme werden farblich markiert. Dadurch können Fehler vermieden und die Leistung verbessert werden.

Visualisierung

Es ist Zeit, die Verwaltung von Risiken durch die Verwaltung von Regel zu ersetzen. McAfee Firewall Enterprise Profiler vereinfacht die Bewertung der Netzwerkdaten, so dass Sie neue Anwendungen schnell und problemlos hinzufügen können. Unsere intuitive visuelle Analyse ermöglicht die unmittelbare Messung der Effizienz jeder einzelnen Regeländerung. Auf diese Weise können Sie Ihre Richtlinien optimal einstellen.

Umfangreiche grafische Tools fassen die Aktivitäten der einzelnen Anwendungen nach Benutzeridentität, Standort und Nutzungsgrad in Echtzeit zusammen. Sie können auf einen Blick sehen, wer welche Anwendungen nutzt. Durch diese integrierte Ansicht können Sie die sonst Stunden in Anspruch nehmenden Vorsichtsmaßnahmen, Experimente und Fehlersuchen mit einigen wenigen Mausklicks erledigen. Für einige Benutzer besteht der größte Vorteil darin, dass sie sofort sehen können, ob ein Problem wirklich durch die Firewall entstanden ist, und dann der Sache auf den Grund gehen können.

McAfee SecureOS®-Betriebssystem

Funktionen

- McAfee Type Enforcement®-Technologie
- Vorkonfigurierte Sicherheitsrichtlinien für das Betriebssystem (OS)
- Betriebssystem-Abschottung
- Netzwerk-Stack-Trennung

McAfee Firewall Enterprise Control Center

- Grafische Benutzeroberfläche von Windows
- Lokale Konsole
- Vollständige Befehlszeile
- Sicherung und Wiederherstellung der USB-DR-Konfiguration
- Schnelle Problembeseitigung und Auswirkungsanalyse für Firewall-Regeln mithilfe von McAfee Firewall Enterprise Profiler

Protokollierung, Überwachung und Berichterstellung

- On-Box-Protokollierung
- Geplante Protokollarchivierung und -exportierung
- McAfee Firewall Enterprise-Protokoll im Software Extract-Format (SEF)
- Mehrere Exportformate (XML, SEF, W3C, WebTrends)
- Syslog
- SNMP Version 1, 2c und 3
- Sicherheitsereignis-Management mit McAfee Firewall Reporter

Netzwerk- und Routing-Funktionen

- IPv6-konform
- Dynamisches Routing (RIP Version 1 und 2, OSPF, BGP und PIM-SM)
- Statische Routes
- 802.1Q VLAN-Tagging
- DHCP-Client
- Standardrouten-Failover
- QoS

Sichere Server

- Secure DNS (einzeln oder gesplittet)
- Secure Sendmail (einzeln oder gesplittet)

Appliances und Hardware

- Upgrade-Gewährleistung mit bis zu 4-Stunden-Reaktion für die meisten Modelle
- Virtualisierungslösungen und Rugged Appliance-Optionen erhältlich
- Einfache sowie Dual-Core- und Quad-Core-Prozessoren
- ASIC-basierte Beschleunigung
- RAID HDD-Konfigurationen
- Redundante Netzteile

Technischer Support

- Technischer Telefon-Support rund um die Uhr
- Technischer Support mit internetbasiertem Ticketing und KnowledgeBase rund um die Uhr

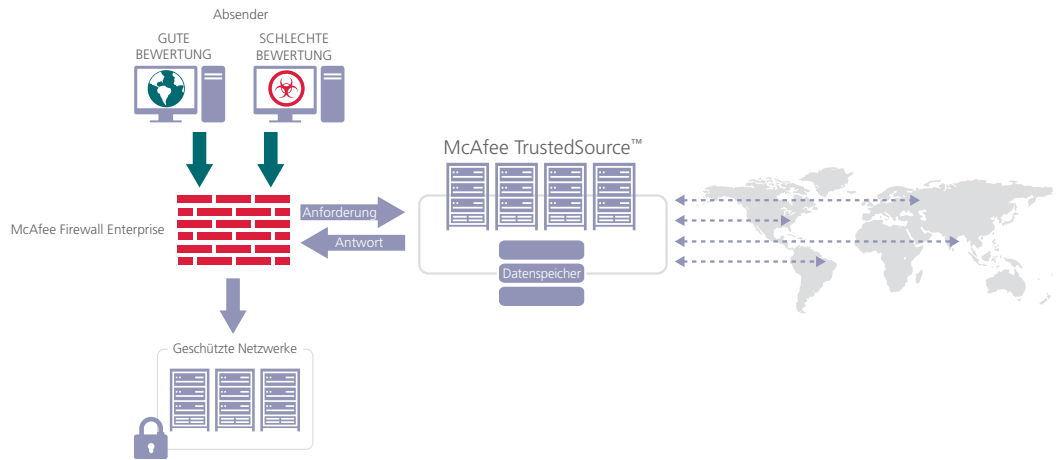


Abbildung 1: McAfee Global Threat Intelligence von McAfee TrustedSource erlaubt oder sperrt Netzwerkverkehr abhängig von der Reputation.

Schutz

McAfee AppPrism unterstützt Sie dabei, die von anwendungsbezogenen Bedrohungen ausgehenden Risiken zu verringern und dabei gleichzeitig die Bandbreite im Unternehmen optimal einzusetzen. Hinter McAfee AppPrism steht die Leistung der McAfee Labs™. Unsere Bedrohungsforscher können mithilfe der Bedrohungsdaten kontinuierlich die Risiken bei 31 Anwendungskategorien, von Anonymisierern bis zu Video- und Foto-Sharing-Programmen, erkennen und bewerten.

Durch die Zuweisung dynamischer Reputations-Daten zu Webseiten, Absendern und Standorten erreichen wir eine Blockierung von durchschnittlich 70 Prozent aller unerwünschten Daten – lange bevor Sie diese überhaupt zu Gesicht bekommen. Dadurch sind wir sogar in der Lage, die schwer zu erkennenden Botnet-Befehlskanäle aufzuspüren.

Einzige Firewall mit Reputations-Analyse und Global Threat Intelligence

Nur McAfee bietet eine Firewall mit integrierter Reputations-Technologie, und dabei stellt diese nur einen Bestandteil der McAfee Global Threat Intelligence dar. Bei McAfee arbeiten über 400 Sicherheitsforscher an der Untersuchung von web-, spam- und anfälligkeitsbasierten Bedrohungen, Host- und Network Intrusion, Malware und Verfahren zur Richtlinien Einhaltung. Diese Bandbreite ermöglicht die Einstufung jeder neuen Bedrohung und Anfälligkeit.

Ihre Bemühungen sowie die von über 100 Millionen Sensoren weltweit gesammelten Daten bieten eine vorausschauende Risikoanalyse in Echtzeit, mit der Sie vor neu auftretenden mehrstufigen Bedrohungen geschützt werden können.

Im Gegensatz zu früheren Firewalls, die auf Signaturdateien basierten, halten Sie die automatisierten Bedrohungsdaten der McAfee Labs stets auf dem

Laufenden, ohne dass Sie die Firewall abschalten müssen. Im Hinblick auf die steigende Bedrohung durch Aktivitäten wie Operation Aurora stellt McAfee Global Threat Intelligence den ausgereiftesten Schutz dar, den Sie für Geld kaufen können. Diese Technologie unterstützt Sie bei der Schwachstellenminimierung, vermeidet Vorschriftenverletzungen und senkt die Kosten für Problembeseitigung.

Vielseitige Sicherheit in einer integrierten Appliance

Einer der Gründe, aus dem sich unsere Kunden für McAfee entscheiden, ist unser umfassendes Sicherheits- und Compliance-Portfolio. Diese Leistung stellen wir Ihnen jetzt unmittelbar zur Verfügung. Angesichts der komplexen Bedrohungen in Web 2.0-Anwendungen, mehrstufigen gezielten Angriffen und Phishing setzt McAfee Firewall Enterprise nun auf wesentliche kombinierte Schutzmechanismen, die in jeder Firewall-Appliance integriert sind.

Früher waren Firewalls auf Zugriffssteuerung und Segmentierung beschränkt. Ein angemessener Schutz erforderte dabei Investitionen in die Implementierung und Verwaltung mehrerer unterschiedlicher Produkte. Heute enthält ein Paket:

- Vollständige Anwendungserkennung und -steuerung dank McAfee AppPrism
- Eindringungsschutz
- Globale Reputations-Analyse
- URL-Filterung mit McAfee SmartFilter-Technologie
- Verschlüsselte Anwendungsfilerung
- Viren-, Spyware- und Spam-Schutz

Unsere Erfahrungen beim Aufbau mehrstufiger Lösungen tragen dazu bei, dass wir alle diese Schutzfunktionen ohne Leistungs- oder Produktivitätseinschränkungen bereitstellen können – ohne Zusatzkosten.

Produktlinie von McAfee Firewall Enterprise

Die Firewall Enterprise-Produktlinie enthält Appliances für Unternehmen jeder Größe sowie begleitende Produkte wie McAfee Firewall Enterprise Profiler, McAfee Firewall Enterprise Control Center und McAfee Firewall Reporter. Diese Produkte ermöglichen zusammen die Optimierung der Verwaltungsvorgänge sowie die Reduzierung der Betriebskosten. Zu den flexiblen Hybrid-Delivery-Optionen zählen physische Appliances, Multi-Firewall-Appliances, virtuelle Appliances sowie Lösungen für Riverbed Steelhead-Appliances. Die McAfee Firewall Enterprise for Crossbeam-Lösung, die auf Crossbeam X-Series-Hardware ausgeführt wird, bietet Sicherheitsperformance auf Netzbetreiber-Niveau mit bis zu 40 Gbit/s. Weitere Informationen erhalten Sie von Ihrem Vertriebsmitarbeiter.

Detaillierte Steuerung leicht zu handhaben

Zuverlässige Sicherheit muss auch leicht konfigurierbar sein. Dank der intuitiven Verwaltungskonsolle von McAfee Firewall Enterprise können Administratoren mit nur einem Bildschirm Regeln erstellen und selektiv Verteidigungsmaßnahmen wie Anwendungsfilter, IPS-Signaturen und URL-Filterung bereitstellen. Neue Funktions-Updates der Software werden automatisch über das Internet ausgebracht, was den Wartungsaufwand verringert. Zur Festlegung des Zeitplans genügt ein einziger Mausklick.

Die McAfee Firewall Enterprise-Produktlinie enthält weitere Tools zur Vereinfachung der Verwaltung: McAfee Firewall Reporter und McAfee Firewall Enterprise Control Center.

Firewall Reporter ist im Lieferumfang von McAfee Firewall Enterprise enthalten und wandelt Audit-Datenströme in umsetzbare Daten um. Dieses mehrfach ausgezeichnete SEM-Tool (Sicherheitsereignis-Management) bietet eine zentrale Überwachung sowie eine korrelierte Warn- und Berichtsumgebung. Sie können Ihre Netzwerkdaten völlig problemlos mithilfe von über 500 grafischen Berichten darstellen und damit zur Einhaltung aller wichtigen gesetzlichen Bestimmungen beitragen.

McAfee Firewall Enterprise Control Center ist als zusätzliches Tool erhältlich und bietet zentralisiertes Firewall-Richtlinien-Management für mehrere McAfee Firewall Enterprise-Appliances. Dies ermöglicht die Maximierung der betrieblichen Effizienz, die Vereinfachung der Richtlinienkontrolle, die Optimierung von Regeln und Software-Updates sowie den Nachweis der Einhaltung gesetzlicher Bestimmungen. Sie können sogar die Richtlinienkonfigurationen aller mit McAfee Firewall Enterprise Control Center verwalteten Geräte vergleichen, um die Konsistenz im gesamten Netzwerk sicherzustellen. Das leistungsfähige Konfigurations-Management ermöglicht die zentrale Suche, Verfolgung und Validierung aller Richtlinienänderungen.

Darüber hinaus kann McAfee Firewall Enterprise Control Center jetzt auch in McAfee ePolicy Orchestrator® (McAfee ePO™) integriert werden, um auf diese Weise zusätzliche Transparenz der Firewall-Status und -Berichte zu bieten.

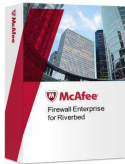
Sicherste Firewall-Hardware-Plattform

Die Kernkomponente von McAfee Firewall Enterprise ist das sehr schnelle und hochsichere Betriebssystem McAfee SecureOS. Geschützt wird dieses Betriebssystem mithilfe der patentierten McAfee Type Enforcement-Technologie, die eine unübertroffene Plattformsicherheit bietet. Dies ist möglicherweise der Grund, weshalb McAfee SecureOS von CERT eine einzigartige Bewertung erhalten hat: Es war nie erforderlich, für diese Software einen Notfall-Sicherheitspatch herauszugeben.

Die vorkonfigurierte Betriebssystem-Sicherheitsrichtlinie regelt das System so ab, dass die Funktionen des Betriebssystems nicht von Angreifern unterbrochen werden können.

Durch diese zusätzlichen Sicherheitsmaßnahmen konnten wir eine Firewall entwickeln, die erstmals die Zertifizierung „Common Criteria EAL 4+“ und die Protection Profile-Compliance des US-Verteidigungsministeriums erhielt.

Durch den Einsatz unserer Innovationen und hochentwickelten Sicherheitsverfahren schützt McAfee Firewall Enterprise weltweit 15.000 Netzwerke, unter anderem von mehreren tausend Regierungsbehörden und Fortune 500-Unternehmen sowie von sieben der zehn führenden Finanzinstitute. Lassen Sie Ihr Unternehmen von uns schützen.



Virtuelle Firewall zum Schutz Ihrer virtuellen Infrastruktur



WAN-Optimierung und Sicherheit für Niederlassungen mit einem einzigen Gerät



Crossbeam X-Series Firewall-Leistung gesteigert auf 40 Gbit/s

Hardware-Spezifikationen ¹	S1104	S2008	S3008	S4016	S5032	S6032	S7032-XX
Formfaktor	1U Klein	1U	1U	1U Enterprise	2U Enterprise	2U Enterprise	2U Enterprise
Unbegrenzte Anwenderlizenzen	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Empfohlene Anwenderzahl	200	300	600	Mittel bis groß ³	Mittel bis groß ³	Groß ³	Groß ³
RAID	-	-	-	Ja	Ja	Ja	Ja
Max. Anzahl von Netzwerkmodulen	-	-	-	1	3	3	2 ⁴
1 Gb-Kupferschnittstellen (grundl./max.)	4	8	8	8/16	8/32	8/32	8/16 ⁴
Option für 1 Gbit-Schnittstelle (max.)	-	-	-	8	24	24	8 ⁴
Option für 10 Gbit-Schnittstelle (max.)	-	-	-	6	18	18	4 ⁴
Beschleunigung zur verschlüsselten Filterung	-	-	Integriert	Integriert	Integriert	Integriert	-
Out-of-Band-Verwaltung (z. B. Status, Temperatur, Spannung und Einschaltzustand)	Nur serielle Konsole	Nur serielle Konsole	Ja	Ja	Ja	Ja	Ja
Einhaltung gesetzlicher Bestimmungen	BSMI (Taiwan), MIC/KCC (Korea), C-Tick (Australien/Neuseeland), VCCI (Japan), FCC (USA), UL (USA), CSA (Kanada), ICES (Kanada), CE (EU), GOST R (Russland), CCC (China), SABS (Südafrika), IRAM (Argentinien), NOM (Mexiko)						
Leistung¹							
Leistung der Firewall (max.) ²	750 Mbit/s	1,0 Gbit/s	4,0 Gbit/s	9,0 Gbit/s	12,0 Gbit/s	15,0 Gbit/s	12,0 Gbit/s
Bedrohungsschutz ²	250 Mbit/s	1,0 Gbit/s	2,0 Gbit/s	3,0 Gbit/s	5,0 Gbit/s	6,0 Gbit/s	5,0 Gbit/s
McAfee AppPrism ²	250 Mbit/s	1,0 Gbit/s	2,0 Gbit/s	7,5 Gbit/s	10,0 Gbit/s	12,0 Gbit/s	10,0 Gbit/s
Gleichzeitige Verbindungen ²	200.000	500.000	750.000	1.500.000	3.000.000	4.000.000	3.000.000
Neue Verbindungen pro Sekunde ²	5.000	15.000	20.000	35.000	50.000	70.000	50.000
IPSec VPN-Durchsatz (AES) ²	60 Mbit/s	250 Mbit/s	350 Mbit/s	400 Mbit/s	450 Mbit/s	500 Mbit/s	450 Mbit/s
Max. Anzahl von IPSec-VPN-Tunneln ²	250	1.000	2.000	4.000	8.000	10.000	8.000
Abmessungen, Gewicht, Umgebungen							
Breite	42,93 cm	42,93 cm	42,93 cm	43,8 cm	48,04 cm	48,04 cm	48,04 cm
Tiefe	21,59 cm	71,12 cm	71,12 cm	61,87 cm	76,21 cm	76,21 cm	76,21 cm
Höhe	4,32 cm	4,32 cm	4,32 cm	4,32 cm	8,71 cm	8,71 cm	8,71 cm
Gewicht	4,96 kg	11,34 kg	11,34 kg	9,98 kg	13,61 kg	13,61 kg	13,61 kg
Stromversorgung	100 W 110/220 V	350 W 110/220 V	350 W 110/220 V	Redundant 400 W 110/220 V	Redundant 750 W 110/220 V	Redundant 750 W 110/220 V	Redundant 750 W 110/220 V
Betriebstemperatur	0 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C

¹ Sämtliche Spezifikationen und Leistungsdaten beruhen auf den Baureihe S dieser Appliances.

² Die V8-Leistungsdaten stellen die maximalen, unter optimalen Testbedingungen gemessenen Leistungen der Systeme dar. Tatsächliche Ausbringung und verwendete Richtlinien können zu anderen Leistungsdaten führen.

³ Wenden Sie sich an Ihren McAfee-Vertreter, um die richtigen Größen für Ihre Bedürfnisse zu ermitteln.

⁴ Es werden maximal zwei Netzwerkmodule (beliebiger Typ) und maximal ein 10 Gbit-Netzwerkmodul (mit maximal 4 enthaltenen Transceivern) unterstützt.

