

McAfee Firewall Enterprise (Sidewinder®)



Funzionalità per la sicurezza di McAfee Firewall Enterprise

Firewall

- Filtraggio stateful, di pacchetti e applicazioni complete
- Opzioni di distribuzione multiple, tra cui le appliance multi-firewall (un'appliance che gestisce fino a 32 firewall virtuali) e un' appliance firewall virtuale
- NAT (Network Address Translation)

Autenticazione

- Locale
- Active Directory
- LDAP (iPlanet, Open LDAP, Custom LDAP)
- RADIUS
- Windows Domain Authentication
- Windows NTLM Authentication
- Passport (single sign-on)
- Autenticazione complessa (SafeWord, SecurID)

Disponibilità elevata (HA)

- Attiva/attiva
- Attiva/passiva
- Failover di sessione stateful
- Monitoraggio IP remoto

Intelligence globale sulle minacce

- Servizio di reputazione globale di TrustedSource
- Filtraggio in base al rivelamento geografico

Filtraggio delle applicazioni cifrate

- SSH
- SFTP
- SCP
- SSL/HTTPS*

* Questi servizi sono acquistabili separatamente.

Le attuali problematiche dei firewall richiedono un nuovo concetto di protezione

I firewall rappresentano la prima linea di difesa di una società contro le minacce alla sicurezza e sono pertanto una componente indispensabile per ogni strategia di protezione della rete aziendale. Ma le minacce alla sicurezza delle aziende diventano di giorno in giorno più pericolose e imprevedibili, con attacchi a livello di applicazioni o che sfruttano vulnerabilità del Web 2.0 e con malware che evitano il rilevamento basato su firme. Gli eventi che attentano alla sicurezza sono in continuo aumento e sono dovuti per lo più all'uso di tecnologie di protezione tramite firewall ormai superate, che non sono in grado di fornire una valida protezione contro i nuovi vettori delle minacce. Allo stesso tempo, mentre gli amministratori dei firewall faticano a gestire e risolvere i problemi di diverse policy legacy del firewall i costi di gestione continuano a crescere.

Impennata dei costi di gestione

Va detto schiettamente che la gestione di più firewall ormai sorpassati è un'attività che richiede molto tempo e risorse. Le modifiche non coordinate alle applicazioni e alle rete provocano delle problematiche la cui soluzione necessita spesso ore o persino giorni. Gli amministratori non dispongono della necessaria visibilità sul comportamento degli utenti e faticano a rispondere in modo efficiente alle esigenze business in continuo mutamento. Per non parlare degli obblighi sempre più frequenti di dimostrare la conformità ai requisiti di auditing e alle normative: un'altra mansione piuttosto impegnativa che è resa ancora più laboriosa e costosa dalla carenza di utili strumenti di reporting.

In questo ambiente caratterizzato da minacce sempre diverse l'unico metodo per difendersi in modo proattivo è poter implementare in modo semplice e sicuro le modifiche firewall di cui necessita l'azienda. In altri termini, è necessario utilizzare una nuova soluzione firewall: McAfee® Firewall Enterprise (Sidewinder®).

Una tecnologia di protezione obsoleta non può bloccare le ultime minacce alla sicurezza

La vecchia tecnologia basata su regole e firme non è più sufficiente. Le nuove minacce si combinano in attacchi misti che sfruttano contemporaneamente diverse vulnerabilità. L'aspetto ancora peggiore di questi attacchi è la loro provenienza sia dall'interno che dall'esterno della rete, persino dai protocolli cifrati. Mantenere sotto controllo un ambiente di questo tipo non è mai stato così complicato, infatti con il crescere delle reti e della connettività anche le minacce si evolvono a velocità elevatissime. Senza un quadro completo delle minacce emergenti, gli amministratori perdono troppo tempo e fatica nel tentativo di mantenere il passo.

Presentazione di McAfee Firewall Enterprise

Con McAfee Firewall Enterprise e i prodotti ad esso correlati, gli amministratori possono iniziare immediatamente ad applicare regole per il firewall nel contesto business adeguato e a sfruttare le funzionalità centralizzate di gestione del firewall, reporting e creazione intuitiva delle regole. Inoltre, Firewall Enterprise offre un avanzatissimo grado protezione dalle minacce: funzionalità all'avanguardia come l'intelligence basata sulla reputazione, la protezione configurabile a livello di applicazione, l'ispezione del traffico cifrato, l'anti-virus, il filtraggio dei contenuti e il blocco preventivo degli attacchi di intrusione.

Gestione del firewall semplificata e conformità alla normative per accrescere l'agilità dell'azienda

McAfee Firewall Profiler, un'appliance separata della gamma di prodotti Firewall Enterprise, è progettata appositamente per l'esecuzione di alcune delle attività che impegnano maggiormente gli amministratori dei firewall: investigazione e risoluzione delle problematiche dei firewall. Definendo con esattezza e in tempo reale in che modo le regole del firewall interagiscono con utenti e applicazioni dell'azienda, Firewall Profiler consente agli amministratori di visualizzare l'impatto della creazione e della modifica di

Funzionalità per la sicurezza di McAfee Firewall Enterprise- Continua

Sistema di prevenzione delle intrusioni (IPS)*

- Oltre 10.000 firme
- Aggiornamenti automatici delle firme
- Firme personalizzate
- Gruppi di firme preconfigurati

Antivirus e spyware*

- Protegge da spyware, trojan e worm
- Euristiche
- Aggiornamenti automatici delle firme

Filtraggio Web*

- McAfee SmartFilter®
- Block Java, Active-X, JavaScript, SOAP

Antispam

- Servizio di reputazione globale di TrustedSource

SVPN

- IPsec certificato ICISA
- IKEv1 e IKEv2
- Cifratura DES, 3DES, AES-128 e AES-256
- Autenticazione SHA-1 e MD5
- Gruppi Diffie-Hellmann 1, 2 e 5
- Tunnel limitati da policy
- NAT-T
- Xauth

Visibilità e controllo dell'applicazione

- VoIP (SIP)
- SQL (Oracle, MS-SQL)
- Multimedia (H.323)
- SSH
- SMTP
- Citrix
- FTP
- HTTP
- HTTPS*
- IM/P2P
- Altri

McAfee SecureOS®

- McAfee Type Enforcement®
- Policy di sicurezza SO preconfigurate
- Partizionamento SO
- Separazione stack di rete

* Questi servizi sono acquistabili separatamente.

uno specifico set di regole per il firewall. La creazione e la risoluzione dei problemi delle regole che in passato richiedeva ore o giorni di lavoro si risolve ora con alcuni rapidi clic. Tutto ciò comporta un calo dei costi operativi e fornisce agli amministratori dei firewall l'opportunità di implementare delle nuove applicazioni in modo più veloce, reagendo più rapidamente alle esigenze specifiche delle loro società

La Admin Console di McAfee Firewall Enterprise semplifica la creazione delle policy

Una sicurezza affidabile deve essere configurabile in modo semplice. La Admin Console di Firewall Enterprise è un'interfaccia intuitiva con la quale gli amministratori possono creare regole e applicare difese in modo selettivo, ad esempio filtri delle applicazioni, firme IPS e filtraggio URL da un singolo schermo. Gli aggiornamenti per le nuove funzionalità software sono distribuiti automaticamente via Internet e ciò riduce le attività di manutenzione. La pianificazione può essere determinata con un solo clic del mouse. Inoltre, Firewall Enterprise presenta un record di segnalazioni CERT che non ha paragoni. L'attività non sarà mai interrotta da patch di sicurezza di emergenza e lo staff potrà lavorare senza distrazioni ai progetti strategici dell'azienda.

La gamma di prodotti Firewall Enterprise include degli strumenti aggiuntivi per semplificare la gestione: McAfee Firewall Reporter e McAfee Firewall Enterprise Control Center (*CommandCenter™*).

McAfee Firewall Reporter

Incluso gratuitamente, il tool Firewall Reporter trasforma i flussi di audit in informazioni attivabili. Questo premiato tool di gestione degli eventi di sicurezza (SEM) garantisce il monitoraggio centrale, gli allarmi correlati e il reporting. Genera in tutta semplicità oltre 800 report grafici che rappresentano il traffico di rete e contribuiscono a soddisfare i principali requisiti di conformità tra cui:

- Sarbanes-Oxley (SOX)
- Payment Card Industry (PCI) Security Standards Council
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)

McAfee Firewall Enterprise Control Center

Venduto separatamente, il Firewall Enterprise Control Center offre funzionalità di gestione delle policy firewall centralizzate per diverse appliance Firewall Enterprise. Questo tool ottimizza l'efficienza operativa, semplifica il controllo delle policy, perfeziona le regole, agevola l'aggiornamento del software e dimostra la conformità con le normative. È inoltre possibile confrontare le configurazioni delle policy su tutti i dispositivi gestiti da Control Center per garantire coerenza sulla rete. Solide funzioni per la gestione della configurazione permettono di individuare, tracciare e convalidare tutte le modifiche alle policy. Inoltre Control Center da ora si integra con McAfee ePolicy Orchestrator® (ePO™), offrendo a ePO la visibilità sui dati e i report che riguardano lo stato del firewall.

Visibilità in tempo reale sulle minacce globali ed eliminazione del traffico indesiderato

Firewall Enterprise elimina l'esposizione agli autori di attacchi sconosciuti grazie anche a due tecnologie esclusive: McAfee TrustedSource™, il primo sistema di reputazione globale del settore per i mittenti Internet e il filtraggio del rivelamento geografico che offre la visibilità geografica e la gestione delle policy in base al Paese di origine del traffico.

Approccio intelligente alle minacce globali

McAfee TrustedSource ha stabilito un nuovo standard per il rilevamento proattivo. Supportato da Avert Labs, l'azienda di ricerca delle minacce con l'offerta più completa, questo servizio in-the-cloud esamina il traffico non in base alla firme bensì in base al comportamento storico degli host e dei dispositivi basati su Internet. TrustedSource rifiuta le connessioni con i mittenti noti come pericolosi, pagine web infette, minacce miste e host divenuti zombie che distribuiscono malware, bloccando in modo efficace questi attacchi a livello del perimetro aziendale.

Bloccando questi attacchi, TrustedSource ferma anche oltre il 70 per cento del traffico indesiderato al margine della rete. Tutto ciò riduce il volume di traffico in entrata sui server di rete, risparmiando la larghezza di banda e accelerando i tempi di elaborazione.



Il sistema operativo McAfee SecureOS garantisce appliance potenti

McAfee Firewall Enterprise viene eseguito nel sistema operativo McAfee SecureOS a velocità elevata con tecnologia McAfee Type Enforcement brevettata che consente livelli impareggiabili di sicurezza della piattaforma. SecureOS ha un record di segnalazione CERT avanzato ed è implementato nelle reti internazionali più esigenti.

Opzioni di gestione e amministrazione

- IU grafica di Windows
- Console locale
- Riga di comando completa
- Backup e ripristino della configurazione del disaster recovery USB
- Veloci risoluzione dei problemi e analisi dell'impatto delle regole sul firewall con McAfee Firewall Profiler (venduto separatamente)

Logging, monitoraggio e reporting

- On-box logging
- Archiviazione ed esportazione dei log pianificata
- Software Extract Format (SEF) del log di Firewall Enterprise
- Formati di esportazione (XML, SEF, W3C, WebTrends)
- Syslog
- SNMP v1, v2c e v3
- SEM di McAfee Firewall Reporter inclusi

Networking e routing

- Routing dinamico (RIP v1 e v2, OSPF, BGP e PIM-SM)
- Route statiche
- 802.1Q VLAN tagging
- Client di DHCP
- Failover route di default
- QoS

Server sicuri

- Secure DNS (single o split)
- Secure Sendmail (single o split)

Appliance e hardware

- Garanzia upgrade per risposta in quattro ore per la maggior parte dei modelli
- Disponibili soluzioni di virtualizzazione e opzioni di appliance precise
- Processori single, core, dual-core e quad-core
- Accelerazione basata su ASIC
- HDD in configurazioni RAID
- Alimentazioni ridondanti

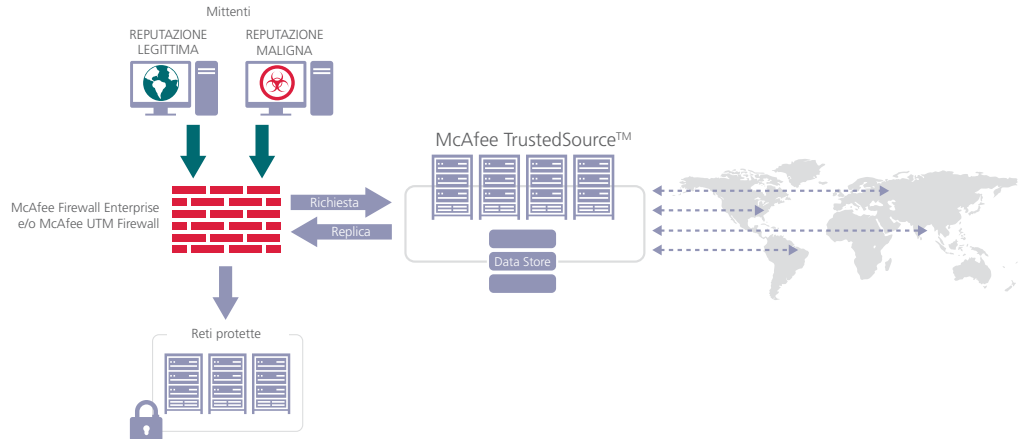
* Questi servizi sono acquistabili separatamente.

McAfee garantisce un supporto tecnico premiato

- Assistenza tecnica telefonica 24 x 7
- Assistenza tecnica 24 x 7 con ticketing basato su web e Knowledge Base

Rivelamento geografico

La funzionalità di rivelamento geografico di Firewall Enterprise limita ulteriormente le minacce globali consentendo il filtraggio del traffico in base a un codice Paese. Molte aziende sprecano larghezza di banda e risorse di sistema con traffico proveniente da Paesi o interi continenti con i quali non hanno alcun rapporto business ma attraverso cui si espongono in modo superfluo a rischi per la sicurezza. Il rivelamento geografico è utile per connettersi solo con il traffico globale che è direttamente correlato con le attività della propria azienda.



Visualizzazione e controllo delle applicazioni

Il crescente livello di organizzazione e tenacia dei cybercriminali fa sì che gli amministratori di rete debbano essere sempre più vigili nel proteggere reti, applicazioni e dati strategici per l'azienda. Le applicazioni, in particolare, rappresentano l'obiettivo principale degli hacker: almeno l'80 per cento dei nuovi attacchi si concentra sulle vulnerabilità applicative. I firewall legacy o quelli che utilizzano solo tecniche di stateful o deep inspection non sono in grado di proteggere l'azienda in modo adeguato.

Firewall Enterprise include tra le altre anche le funzioni di stateful e deep inspection ma in qualità di firewall a livello di applicazione Firewall Enterprise permette di aggiungere livelli di protezione più avanzati dove e quando desiderato, senza compromettere le prestazioni.

Per molti dei protocolli utilizzati più frequentemente sono disponibili controlli a livello applicativo, come:

- E-mail (SMTP)
- Web (HTTP e HTTPS)
- Multimedia (H.323)
- Oracle e MS-SQL
- Citrix
- VoIP/SIP (Voice over IP/Session Initiation Protocol)
- Secure Shell (SSH)
- File Transfer Protocol (FTP)

Soddisfazione dei requisiti PCI DSS

Lo standard PCI DSS (Payment Card Industry Data Security Standard) ora impone che le società che gestiscono le carte di credito implementino un firewall per l'applicazione. Firewall Enterprise consente di soddisfare tale requisito e protegge in modo proattivo i dati finanziari dei clienti dell'azienda.

Eliminazione dei punti deboli delle applicazioni cifrate

Molte aziende oggi cifrano una parte del traffico Internet per le comunicazioni con i partner commerciali o con i clienti o per le comunicazioni dei sistemi client/server. Sebbene la cifratura garantisca una protezione valida dei dati in transito, può anche rappresentare un'opportunità per i cybercriminali. La maggior parte dei firewall legacy non ispeziona il traffico cifrato e quindi non può proteggere contro i malware o utilizzare le firme di prevenzione delle intrusioni all'interno di questo tipo di traffico. Tutto ciò offre agli hacker un tunnel di accesso da cui sfruttare i server e le applicazioni aziendali.

Firewall Enterprise elimina questa vulnerabilità decodificando, filtrando e controllando il traffico Secure Socket Layer (SSH), Secure FTP (SFTP), Secure Channel Protocol (SCP) e Secure Socket Layer (SSL)/HTTPS. In questo modo vengono eliminati gli attacchi a sorpresa sui server web e delle applicazioni pur proteggendo l'integrità e l'autenticità dei messaggi cifrati.

Linea di prodotti McAfee Firewall Enterprise

La linea di prodotti Firewall Enterprise include le appliance più appropriate per le aziende di tutte le dimensioni, nonché prodotti complementari come McAfee Firewall Profiler, McAfee Firewall Enterprise Control Center e McAfee Firewall Reporter per facilitare le attività di gestione e ridurre i costi operativi. Tra le opzioni di distribuzione flessibili e ibride sono incluse appliance multi-firewall, appliance virtuali e appliance come McAfee Firewall Enterprise RM700 per ambienti più complessi. Per ulteriori informazioni, chiedete le schede tecniche specifiche di ogni prodotto.



Specifiche hardware

	410	510	1100	2100	2150	2150VX	4150
Formato	Small 1U	Small 1U	Enterprise 1U	Enterprise 2U	Enterprise 2U	Enterprise 2U	Enterprise 5U
Licenze utente illimitate	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Utenti consigliati	300	600	Medio-Grande	Medio-Grande	Grande	Grande	Enterprise
RAID	N/D	N/D	RAID 1	RAID 1	RAID 5	RAID 5	RAID 5
Alimentazione	Singola	Singola	Duale	Duale	Duale	Duale	Duale
Interfacce in rame (base/max)	8 – GB	8 – GB	8/14 – GB	8/20 – GB	8/20 – GB	20 – GB	14/24 – GB
Opzione interfaccia in fibra (max)	N/D	N/D	4	6	6	N/D	6
Opzione interfaccia 10 GB (max)	N/D	N/D	N/D	2	2	2	2
Decodifica e filtraggio SSL/HTTPS*	N/D	N/D	Sì	Sì	Sì	Sì	Sì
Conformità alle normative	FCC (solo USA) Class B, ICES (Canada) Class B, marchio CE (EN 55022 Classe B, EN55024, EN61000-3-2, EN61000-3-3), VCC (Giappone) Class B, BSMI (Taiwan) Class A, C-Tick (Australia/Nuova Zelanda) Class B, SABS (Sud Africa) Class B, CCC (Cina) Class B, MIC (Corea) Class B, UL 60950, CAN/CSA C22.2 No. 60950, IEC 60950						
Certificazioni	ICSA Labs IPSec VPN, Common Criteria EAL4+ con Application Protection Profile (l'unico firewall ad avere questo livello di EAL4+ certificazione), FIPS 140-2, Livello 2						
Prestazioni							
Velocità filtraggio pacchetti (TCP)	275 Mb/s	650 Mb/s	1,9 Gb/s	1,9 Gb/s	3,1 Gb/s	3,1 Gb/s	3,8 Gb/s
Velocità stateful	250 Mb/s	600 Mb/s	1,8 Gb/s	1,8 Gb/s	2,9 Gb/s	2,9 Gb/s	3,6 Gb/s
Connessioni contemporanee	100.000	500.000	1.000.000	1.000.000	1.600.000	1.600.000	2.000.000
Velocità filtraggio applicazioni	230 Mb/s	250 Mb/s	1,4 Gb/s	1,4 Gb/s	2,2 Gb/s	2,2 Gb/s	2,7 Gb/s
Velocità IPSec VPN	160 Mb/s	160 Mb/s	240 Mb/s	240 Mb/s	350 Mb/s	350 Mb/s	400 Mb/s
Dimensioni, peso, caratteristiche ambientali							
Larghezza	54,6 cm	54,6 cm	42,6 cm	44,43 cm	44,43 cm	44,43 cm	44,27 cm
Profondità	42,54 cm	57,6 cm	77,2 cm	74,4 cm	74,4 cm	74,4 cm	67,43 cm
Altezza	4,2 cm	4,2 cm	4,26 cm	8,64 cm	8,64 cm	8,64 cm	21,77 cm
Peso	11,8 kg	11,8 kg	16,3 kg	23 kg	28,85 kg	28,85 kg	45,36 kg
Dettagli alimentazione	345 W 110/220 V	345 W 110/220 V	Duale 670 W 110/220 V	Duale 750 W 110/220 V	Duale 750 W 110/220 V	Duale 750 W 110/220 V	Duale 930 W 110/220 V
Temperatura di esercizio	10° 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

