

## McAfee Firewall Enterprise Profiler

McAfee® Firewall Enterprise Profiler è un'appliance di rete che riceve i dati da McAfee® Firewall Enterprise (Sidewinder®), insieme ad altri flussi di dati di rete, per analizzare istantaneamente l'impatto sulla rete delle regole firewall. Con Profiler, sono sufficienti pochi minuti, invece che ore, per risolvere problematiche di rete o applicazioni legate al firewall, evitando attività manuali considerevoli con pochi semplici clic del mouse.



### Gestione dei set di regole per il firewall in modo semplice: McAfee Firewall Enterprise Profiler

La gestione dei set di regole per i firewall è una delle principali sfide e una delle principali attività che incide su budget e risorse in ambito IT. In base a una ricerca McAfee, gli amministratori dei firewall impiegano il 70% del proprio tempo a risolvere problemi di malfunzionamento delle applicazioni quando le regole firewall non sono sincronizzate con le modifiche che interessano la rete o le applicazioni. Ancor prima di iniziare a cercare di porre rimedio alle regole, gli amministratori impiegano troppo tempo ed energie semplicemente a cercare di stabilire se le regole firewall hanno avuto una qualche responsabilità nel causare l'interruzione del servizio.

McAfee Firewall Enterprise Profiler, un nuovo elemento della suite di gestione McAfee Firewall Enterprise, semplifica il compito di mantenere sincronizzate le regole firewall con le richieste aziendali in costante evoluzione che influenzano il rilascio di nuove applicazioni e aggiornamenti agli utenti.

Semplice da implementare e utilizzare, Profiler offre agli amministratori di rete e firewall visibilità automatica sul traffico associato alle modifiche nelle applicazioni e alle attività dell'utente sulla rete. Con queste informazioni, è possibile definire con precisione e rapidamente la causa originaria di qualsiasi interruzione nel servizio per individuare e risolvere rapidamente le problematiche del firewall.

### Migliori funzionalità di gestione del firewall

Le tradizionali soluzioni per la gestione del firewall forniscono informazioni solo sulle azioni negate del firewall, spesso solo con correlazione limitata a attività specifiche dell'utente. Sebbene quest'informazione sia preziosa, non fornisce quella conoscenza completa e in tempo reale necessaria per supportare attività quotidiane di troubleshooting del firewall.

McAfee Firewall Enterprise Profiler semplifica le attività quotidiane di gestione del firewall. Profiler riceve i dati tramite un feed live da McAfee

Firewall Enterprise e aggrega tali informazioni con i dati di flusso provenienti dalla rete. In questo modo, fornisce una reale visibilità sulle regole attive del firewall e sull'impatto che hanno sui processi e gli utenti sulla rete.

Profiler presenta la sua analisi in una visione d'insieme estremamente intuitiva che mappa in modo preciso gli oggetti in transito. Con pochi semplici clic del mouse, dalla visione d'insieme si può entrare nei dettagli necessari per comprendere l'ambiente di rete, inclusi nomi utente correlati, gruppi, ruoli e molto altro.

### Le caratteristiche di McAfee Firewall Enterprise Profiler

#### Solide funzionalità di analisi e troubleshooting

- Profiler correla gli eventi di rete con set di regole firewall, facilitando le attività quotidiane di troubleshooting e riducendo il tempo speso nella messa a punto e ottimizzazione dei set di regole.
- Le azioni di autorizzazione/rifiuto del firewall vengono presentate nel contesto del traffico complessivo di rete e utenti della rete:
  - » Profiler identifica e visualizza automaticamente le modifiche nel comportamento del firewall che potrebbero richiedere l'attenzione dell'amministratore.
  - » E' possibile visualizzare il comportamento del firewall nel suo contesto complessivo: chi (utenti e posizioni della fonte), cosa (servizi e applicazioni) e dove (posizione della destinazione) sulla rete, in base alle informazioni di flusso che riceve da router e switch.
- I report dettagliano le attività degli utenti, i servizi e le risorse in tempo reale e su un periodo di due settimane a rotazione.

#### Allarmi grafici visivi intuitivi

- Profiler identifica automaticamente le modifiche del traffico dovute alle policy del firewall, definendo con precisione gli elementi che richiedono attenzione.

**Specifiche dell'appliance McAfee Firewall Enterprise Profiler**

**Specifiche tecniche**

- CPU: (Quantità: 1) 2,33GHz Quad Core, 2x6 MB Cache, 5410
- HD: (Quantità: 2) Hard Drive 15K RPM SAS, 146 GB
- RAM: 4 GB
- Altezza: 4,26 cm
- Larghezza: 42,60 cm
- Profondità: 77,2 cm

- Le modifiche alle azioni del firewall vengono priorizzate automaticamente in base all'autorizzazione/rifiuto e cambiamenti dei volumi.
- Risposta rapida alla domanda più importante - è stato il firewall o no? - visualizzando le azioni del firewall in tempo reale:
  - » Una semplice visione grafica del traffico di rete complessivo tra ruoli utente e sistemi aziendali critici.
  - » Ricerca per utenti, gruppi, servizi e oggetti di rete del firewall.

- Profiler sfrutta i dispositivi e le infrastrutture di rete esistenti; non richiede agent host o dispositivi inline aggiuntivi per intercettare le autenticazioni del login; e non richiede attività di raccolta dei log successiva, che comporta un elevato lavoro manuale.
- Profiler sfrutta la directory delle risorse di McAfee ePolicy Orchestrator® per fornire una chiara comprensione del contesto in modo da risolvere rapidamente i problemi.
- Ogni appliance Profiler supporta fino a 5 appliance McAfee Firewall Enterprise a 500 MB e 3.000 (aggregati per tutti i firewall pertinenti) flussi al secondo (SU TUTTI PER I FLUSSI o 500 MB PER OGNI APPLIANCE).
- Profiler funziona perfettamente con Active Directory per l'acquisizione dell'identità e l'assegnazione dei ruoli.

**Interoperabilità perfetta con le infrastrutture di rete esistenti**

- McAfee Firewall Enterprise Profiler può essere implementato in circa 20 minuti (per firewall).
- L'implementazione fuori banda minimizza l'impatto sulla rete.



McAfee Firewall Enterprise Profiler visualizza tutte le azioni del firewall all'interno del contesto di rete anche per i set di regole più complessi. La dimensione della "bolla" dipende dall'attività totale: la bolla arancione mostra una tendenza al rifiuto; la bolla blu mostra una tendenza all'autorizzazione; quella grigia indica che non ci sono variazioni.

**Caratteristica**

**Vantaggio**

Avvisi in tempo reale che una normale comunicazione di rete dall'elaborazione ordini al database clienti si è interrotta	Rapida convalida dei problemi per una prioritizzazione; monitoraggio 24/7 per visualizzare rapidamente lo sviluppo dei problemi
Conferma se l'interruzione è o non è a livello di firewall	Rapido invio ai team responsabili di firewall, desktop o server/applicazione
Segnalazione dei motivi per cui il firewall sta tralasciando del traffico: è in violazione alle regole, contiene malware, ha una cattiva reputazione	Aggiornamento immediato delle configurazioni del firewall per ripristinare il servizio!
Esamina a più livelli cosa è stato cambiato per violare la regola firewall: posizioni dell'utente, posizione dell'applicazione, profilo granulare di applicazione/servizio o modifica della regola del firewall	
Conferma del ripristino della comunicazione attraverso il firewall in tempo reale	Conferma che l'incidente sia stato risolto

