

McAfee Firewall Enterprise Profiler

McAfee® Firewall Enterprise Profiler is a network appliance that receives data from McAfee® Firewall Enterprise (*Sidewinder*®), along with other network data flows, to instantly analyze how firewall rules are impacting the network. With Profiler, you spend minutes rather than hours resolving firewall-related network or application outages—replacing substantial manual effort with a few simple clicks.



Manage Firewall Rule-Sets the Easy Way: McAfee Firewall Enterprise Profiler

Managing firewall rule-sets is a major challenge and a major drain on IT time and budgets. According to McAfee research, firewall administrators spend up to 70 percent of their time fixing application outages that occur when firewall rules are out of synch with changes that effect the network or applications. Even before they can get around to fixing the rules, administrators spend far too much time and effort simply trying to determine whether firewall rules were actually responsible for causing the outage in the first place.

McAfee Firewall Enterprise Profiler, a new addition to the McAfee Firewall Enterprise management suite, simplifies the task of keeping firewall rules in synch with the constantly changing business demands that drive the delivery of new applications and updates to end users.

Easy to deploy and use, Profiler gives network and firewall administrators automatic visibility into the traffic associated with changes in applications and user activities across the network. With this information, you can quickly pinpoint the root cause of any outages to quickly troubleshoot and correct issues with the firewall.

Enhance Your Existing Firewall Management

Traditional firewall management solutions report only on denied firewall actions, often with only limited correlation to specific user activities. While this information is valuable, it doesn't provide the comprehensive, real-time knowledge you need to support day-to-day firewall troubleshooting.

McAfee Firewall Enterprise Profiler simplifies the daily tasks of firewall management. Profiler receives data over a live feed from McAfee Firewall

Enterprise and aggregates this information with flow data from across the network. In this way, it provides true visibility into all active firewall rules and the impact they have on processes and users across the network.

Profiler presents its analysis in a highly intuitive, at-a-glance view that accurately maps objects in transition. With a few simple clicks, you can drill down from the main view to all the details you need to understand your network environment, including related user names, groups, roles, and more.

Features of McAfee Firewall Enterprise Profiler

Robust analysis and troubleshooting capabilities

- Profiler correlates network events against firewall rule-sets, facilitating day-to-day troubleshooting and reducing the time you spend tuning and optimizing rule-sets
- Allow/deny actions of the firewall are presented in the context of all network traffic and network users:
 - » Profiler automatically identifies and displays changes in firewall behavior that may require your attention
 - » You can see firewall behavior in its full context: who (users and source locations), what (services and applications), and where (destination location) across the network based on the flow information it receives from routers and switches
- Reports detail the activities of users, services, and assets in real time and over a rolling two-week period

Intuitive visual alerts

- Profiler automatically identifies traffic changes due to firewall policy, pinpointing items that require attention

McAfee Firewall Enterprise Profiler Appliance Specifications

Technical Specifications

- CPU: (Qty: 1) 2.33GHz Quad Core, 2x6MB Cache, 5410
- HD: (Qty: 2) 146 GB, 15K RPM SAS Hard Drives
- RAM: 4GB
- Height: 1.67 in (4.26 cm)
- Width: 16.70 in (42.60 cm)
- Depth: 30.40 in (77.2 cm)

- Firewall action changes are automatically prioritized based on deny/allow and volume changes
- Quickly answer the most fundamental question—was it the firewall or not?—by visualizing firewall actions in real time:
 - » Get a simple yet robust visual view of all network traffic between user roles and critical business systems
 - » Search by users, groups, services, and firewall network objects
- Profiler leverages existing network devices and infrastructures; does not require host agents or additional inline devices to intercept login authentications; and does not require manually intensive, after-the-fact log collection
- Profiler leverages the McAfee ePolicy Orchestrator® asset directory to provide a clear understanding of the context so you can resolve issues quickly
- Each Profiler appliance supports up to five McAfee Firewall Enterprise appliances at 500 MB and 3,000 (aggregated across all relevant firewalls) flows per second (ACROSS ALL GIVE FOR FLOWS or 500MB EACH APPLIANCE)
- Profiler interoperates seamlessly with Active Directory for identity acquisition and role assignment

Seamless interoperability with existing network infrastructures

- McAfee Firewall Enterprise Profiler can be deployed approximately 20 minutes (per Firewall)
- Out-of-band deployment minimizes network impact



McAfee Firewall Enterprise Profiler displays all firewall actions in their network context even for the most complex rule-sets. The size of the “bubble” depends on total activity: orange shows a trend toward deny; blue shows a trend toward allow; gray indicates no change.

Feature	Benefit
Real-time alert that normal network communication from Order Processing to Customer database is disrupted	Enables quick validation of problems for prioritization; 24/7 monitoring can proactively see problems developing
Confirms that disruption is or is not at firewalls	Enables quick dispatch to firewall, desktop or server/application teams
Signals why the firewall is dropping traffic: violates rule, contains malware, bad reputation	Enables immediate update to firewall configurations to restore service!
Drills down on what changed to violate firewall rule: locations of user, location of application, granular profile of application/service, or firewall rule change	
Confirm restoration of communication through firewall in real-time	Verification that incident is resolved

