McAfee
An Intel Company

McAfee Firewall Management

Comprehensive visibility, control, and reporting, plus streamlined and intuitive rule management to simplify next-generation firewall management

The more complex your organization, the more value you gain from visibility, control, and efficiency in firewall management. McAfee includes powerful, easy-to-use management software with every McAfee® Firewall Enterprise to help you know who is doing what when and be confident that firewall activities are not getting in the way of business. Optional McAfee Firewall Enterprise Control Center and McAfee ePolicy Orchestrator® (McAfee ePO™) software share information to minimize the complexity and compliance challenges of enterprise and multitenant installations. Available appliances ensure that protection and troubleshooting scale without impairing network traffic.

The Problem

"60% to 70% of all firewalls are misconfigured," rendering them "…worse than useless."

—Chris Christiansen, IDC

The Solution
McAfee Firewall Enterprise

Highlights

- Centralized policy and device management based on users and applications.
- Intuitive, reusable policies and tools that spotlight rule interactions, overlaps, gaps, and chances for optimization.
- Integrated dashboards, correlated and custom alerts, and real-time log viewing.
- Role-based administration and change controls.
- Logical separation of policies and configuration domains.
- Forensics and reporting included at no extra charge.
- Enterprise scalability and reliability.
- Log trending and analytics.
- Data sharing with endpoint systems through McAfee ePolicy Orchestrator software.
- More than 550 out-of-the-box reports.

Next-generation firewalls allow IT to permit safe, liberal use of social media and web applications while retaining visibility and fine-grained policy control for compliance. However, as organizations introduce more security—such as identity- and application-aware rules, content inspection, antivirus (AV), and intrusion prevention system (IPS)—these overlays can add complexity to firewall management unless firewall administrators also adopt more efficient management processes and tools.

With conventional firewalls, management has been the largest factor in the cost of ownership. Routine tasks consume endless hours. When there's a network outage, teams frantically piece together what happened, often striving to simply prove the firewall was not at fault.

As organizations take advantage of the security controls in next-generation firewalls, integrated tools and automation should reduce rule-set complexity and streamline incident response. Our McAfee firewall management solutions can help ensure your next-generation policy enforcement controls have the appropriate impact on your network, enabling valuable business services without hindering users or overwhelming operations.

More Confidence, Lower Cost
The McAfee firewall management solution combines management, reporting, and analytic tools for better visibility, effective security, and streamlined operations, including intuitive rule management. Solution components work together to lower firewall management effort and costs. McAfee covers the crucial facets of firewall management:

- *Firewall administration*—Enable fine-grained rules, audit operations, and centrally manage policies and configurations—all with highly intuitive management capabilities.
- *Trending, visualization, and analytics*—Monitor your firewall day to day, correlate data, and analyze real-time information flows within one environment.
- *Historic analysis and reporting*—Handle the long-term retention of firewall audit data and streamline compliance with 550+ reports.
- *Host integration*—Leverage McAfee ePO software to share host and firewall data.

Does Your Current Firewall Management Help You?

- Quickly identify who used what application.
- Write policies to control user access to applications.
- See rule interactions in advance.
- Easily identify rules that match traffic.
- Design and validate appropriate rules.
- Enable real-time content and security controls with a few clicks.
- Write fine-grained rules in your business' language: Users and apps.
- Maintain threat visibility as attacks emerge.
- View analytics, trending, and visualization of log data in a single environment.
- Quickly identify problems and find resolutions.
- Reduce policy size and complexity.
- Share data between network and host.
- Automate everyday workflows.
- Streamline compliance reporting.
- Optimize policies and clean up rules.
- Integrate the firewall with existing IT infrastructure, change processes, and organizational structures.

Command Line Controls

With McAfee, advanced users have the option of broad command line control:

- Full Unix shell and tool access.
- View all firewall log files, historic or real time.
- Fully configure or import policy.
- Access command line interface (CLI) at console or over SSH.

Firewall Administration

McAfee provides both local and centralized options for configuring, monitoring, and maintaining firewall devices and capabilities.

Local administration

The McAfee Firewall Enterprise Admin Console offers a basic environment for connecting to and managing one or more firewalls. This console makes it easy to implement policies that take advantage of all the options of the next-generation McAfee Firewall Enterprise. In one view, you enable granular, targeted security controls, constructing a single rule for each policy using the business language of applications and users.

A monitoring dashboard and one-click access to powerful network tools such as TCPdump, ARP, Ping, and nslookup bring together the core processes for managing individual firewalls. Full configuration and management capabilities are available at the command line as well.

Fine-grained control of applications and defenses

For each rule, a few clicks within one graphical user interface activate rich security controls, such as IPS, AV, geo-location, decryption, or reputation. You can permit use of potentially risky applications but impose protections that match the application's threat vectors. For example:

- Apply AV and IPS to web conferencing.
- Limit use of SSH and SSH tunneling to specific users and block port forwarding to prevent malicious traffic.
- Use geo-location to disallow and IPS to scan traffic to and from a dark portion of the web.
- Decrypt inbound traffic for content inspection, exempting based on policy, and re-encrypt.

As you draft each rule, you can control sub-capabilities of applications, such as games on websites, and restrict access and capabilities at the user level to match roles. Rules stay up to date as users change roles or leave the company. A search option helps you find applications, categories, and capabilities that your policy should reflect.

To reduce complexity and troubleshooting, this console presents rule interactions on a tab. The display highlights the rules and areas of each rule that could cause potential problems. You can immediately identify conflicts that could prevent your new rule from taking effect.
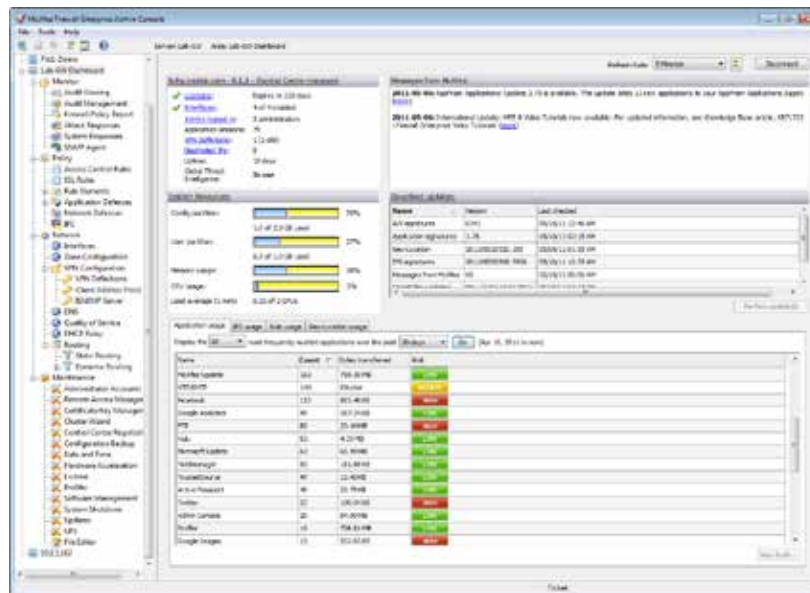

Figure 1. McAfee Firewall Enterprise Admin Console provides quick access and complete control over your firewalls.

Intuitive dashboard and real-time audit viewer

The firewall dashboard provides quick details on system status, allows simple confirmation and updating of security services, and highlights the latest number of applications discovered and policies in use over your chosen time span. Additionally, the real-time audit viewer within the console helps you keep abreast of active rules and troubleshoot issues. You can filter audit logs using predefined or custom filters, color code the results to accentuate threat events, and schedule automatic exporting of data to reporting systems, like McAfee Firewall Reporter or McAfee Security Innovation Alliance partner products.

Central administration

In environments with multiple firewalls, firewall administrators can use the local firewall administration console for full policy and device configuration, to set up and monitor dashboards, and to perform troubleshooting by viewing packet captures and logs in real time.

But how do you see the big picture? How do you capture economies of scale and reduce overlaps in rules, policies, and operations? The optional McAfee Firewall Enterprise Control Center dedicated or virtual appliance centralizes firewall management across multiple firewalls, boosting consistency and slashing maintenance effort. McAfee Firewall Enterprise Control Center helps you implement firewall security configuration settings, policies, and policy changes quickly, easily, and accurately across your entire firewall infrastructure. This integrated environment unites all of the McAfee firewall management tools.

Powerful yet simple rule creation, validation, and distribution

An enterprise security policy may require hundreds of rules deployed across a fleet of firewalls. Large policies with many rules are harder to manage and increase the chance of user error, which puts the network at risk.

The McAfee Firewall Enterprise Control Center environment helps you construct and optimize policies to minimize the number of rules, streamlining execution for better firewall performance. You can allow the traffic and inspections that you need, without extra checks that slow it down.

McAfee Firewall Enterprise Control Center includes graphical, fully integrated policy management tools that handle your entire enterprise network—from the edge to the core. The single rule policy concept available for local administration is enriched here to match the challenges of managing multiple systems, handling complex network topologies, and reusing rules. As you define powerful rules to take full advantage of filtering and protection features and act on applications and users, McAfee Firewall Enterprise Control Center helps you leverage these rules across your firewall infrastructure.

Drag-and-drop rule "objects" make it easy to configure, reuse, merge, optimize, troubleshoot, and clean up (remove unused) policies as you create specific configurations for each appliance in a multifirewall environment. To control access to specific systems, such as database servers, you can search by rules within objects, such as IP address or port. Just drag and drop the resulting rule objects to the correct rule fields to create or update access controls. Before you update the rule, just click to see if there are overlaps and confirm that the rule will fire.
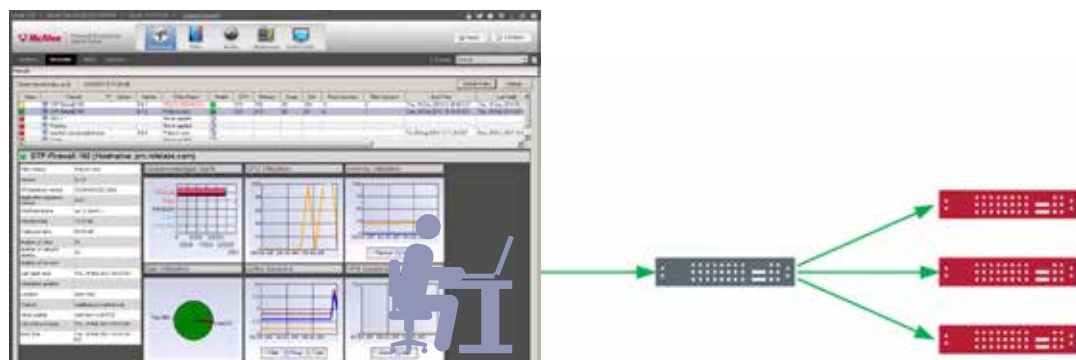

Figure 2. McAfee Firewall Enterprise Control Center centralizes and eases management of multiple firewalls.

McAfee firewalls leverage McAfee Logon Collector which simplifies discovery, logon, and authentication processes across all McAfee firewall management tools as well as McAfee Data Loss Prevention. This non-invasive process maps IP addresses to users for all types of traffic to enable user-based policies without requiring the user to authenticate to the firewall or use a protocol that supports authentication.

- Quickly discover who is using which application and check authentication status.
- Enforce user-based access control policies without a separate authentication step.
- Leverage users and groups in your Microsoft Active Directory.
- Enforce additional active authentication for users not logged in to the domain.
- Authenticate using captive portal, NTLM, Radius, LDAP, and Active Directory.

Cost-Effectively Manage Multiple Entities or Organizations

McAfee Firewall Enterprise Control Center helps managed service providers and organizations with multitenant management or reporting requirements administer the firewalls of multiple customers or separate entities.

- Create "domains" or "zones" that act as separate McAfee Firewall Enterprise Control Center instances—administrators only see the firewall and policies for their particular customer or entity.
- Separate configurations for several enterprises and hide information about an enterprise from administrators of other enterprises.
- Keep configuration simple and save time and effort with common rule objects; cross-enterprise policy objects can still be shared or reused by all domains.
- Role-based access control helps enforce change-control policies.

Search filters let you selectively view the rules for a particular firewall, firewall group, or the entire organization, and then easily modify those rules. Once defined, you can distribute rules to hundreds of firewalls, sharing them across logical enterprise groups, such as global, group, cluster, or local domains, or configuration domains, such as those offered by managed-service providers.

Optimized policies deliver better firewall performance and better security

Over time, rule sets tend to grow, overlap, and become ineffective, making it easier to make mistakes. To reduce the number of rules, our tools automate clean up. Wizards help you scan for, identify, and merge similar rules (a common set of parameters) and delete duplicate or unused rules to keep rule sets manageable.

For example, multiple administrators might create separate objects that have different names, but perform the same function. The "merge objects" command will look for this situation and clean it up with a single common object. Fewer rules to consider equals better performance.

Adaptive objects allow rule grouping and reuse

Administrators implement policies by defining intelligent objects once, and then reusing them whenever and wherever they make sense. With object grouping, you can do much more with a single rule and consolidate rule sets.

McAfee Firewall Enterprise Control Center supports many types of objects, including firewalls and firewall groups, hosts, networks, address ranges, applications, endpoint groups, and services, including geo-location objects.

McAfee Firewall Enterprise Control Center also gives you visibility into rule usage. You can identify the most used rules, least used rules, and rules that have not been matched by firewall traffic in the last 30 days. This real-world data lets you:

- Move most-used rules to the top of the rule list so traffic can be processed quickly.
- Investigate least-used rules to see if they are working as intended.
- Delete or disable unused rules that must be justified during audits.

You can even compare policy configurations on all of your McAfee Firewall Enterprise Control Center-managed devices to ensure consistency across your network. Robust configuration management

lets you centrally track, trace, and validate all policy changes.

Manage and monitor firewall software

For efficient and consistent updates, McAfee Firewall Enterprise Control Center can automatically detect when new releases and firmware are available on the McAfee site. Simply download the files you need and store them on McAfee Firewall Enterprise Control Center's Management Server for manual or automated installation. When you are ready to install, you can push new releases to one system or to hundreds simultaneously.

McAfee Firewall Enterprise Control Center displays the installation history for all managed firewalls along with the progress of the current deployment. If needed, you can restore a trusted device configuration in seconds with a few clicks of the mouse.

Complete access control with role-based administration and configuration domains

Some configuration changes are routine, while others are far-reaching. Role-based access allows you to exert centralized, consistent, policy-based control over distributed teams, determining which management functions can be viewed or changed based on each person's responsibilities. Role-based access can also ensure that only approved users create or validate rules, reducing the risk of unauthorized changes or rule conflicts breaking the firewall. Customers subject to Payment Card Industry Data Security Standard (PCI DSS) often employ role-based access to enforce change controls.

You can create any number of roles to address each organization's needs and privileges, associate rules with roles (to limit modifications), and establish priority protections for rules. Different roles could be defined to:

- Change only domain name system (DNS) entries.
- View event or audit logs.
- Create rules associated with a specific network service or protected server.

You might dictate that certain rules must always be at the top of the policy list and moved only by certain privileged users. Roles, like the rules you build, link to users and groups in LDAP and Active Directory so the system can auto-create or auto-deactivate users as they connect to McAfee Firewall Enterprise Control Center for the first time.

Trending, Visualization, and Analytics

After you have configured your firewalls, use your McAfee Firewall Enterprise Profiler for situational awareness about changing usage and threats and at-a-glance monitoring day to day. It helps you discover, visualize, and monitor application usage by user group and risk level.

With McAfee Firewall Enterprise Profiler's graphical displays, you spend minutes rather than hours planning changes, optimizing rules, and troubleshooting firewall-related network or application outages. McAfee Firewall Enterprise Profiler helps replace substantial manual effort and log viewing with a few simple clicks.

This software, included with your Firewall purchase or available in a dedicated appliance, takes feeds from the firewall, analyzes the data for visibility into how the firewall rules are affecting the network, and helps you detect changes in access patterns in real time.

Application discovery and real-time usage visualization

While McAfee Firewall Enterprise discovers the applications traversing the network, McAfee Firewall Enterprise Profiler visualizes those applications, both inbound and outbound. It also shows you how bandwidth is being used, by risk level and user group.

Dynamic displays highlight changes on the network, comparing timeframes and prioritizing events to help you detect alterations in access patterns that could signal a problem. You can track what happens for any time period at the firewall, characterizing users and assets based on real-time network activity and visualizing firewall deny/allow actions in context. This clarity lets you determine which applications are required and which are not, and create policies in the firewall that control access to applications. With data to back up decision-making, you can reduce cost in terms of bandwidth use, improve productivity, and tune rules or educate users to ensure usage matches organizational policies.

Threat and geographic visualization

Since many attacks are targeted and subtle, McAfee Firewall Enterprise Profiler gives you tools to determine if the systems protected by your firewalls are under attack, identify threats, confirm countermeasures are in place, and prioritize risks. The system highlights changes in risk so you can

Figure 3. Since crises seem to hit most often when you're away from the office, you can troubleshoot firewall events from any web browser.

Figure 4. Use Profiler to discover the applications your users are accessing and visualize the risk and network impact.

quickly take action and it dynamically adjusts risk ratings according to asset value, application risk, and identified threats.

McAfee Firewall Enterprise Profiler presents events correlated against firewall policy in the context of all firewall actions. To speed assessment, you see details for each event, including users, geographic location, and source and destination IP addresses and ports. The display lets you drill down to show specific users within the user group and look at the rule and the reason for a "deny" action. To verify that protective measures are working, you can see a report that shows security countermeasures applied by application.

Geo-location can be a strong indicator of risk. McAfee Firewall Enterprise Profiler can tell you the locations and sources of traffic and threats. Are you getting BitTorrent traffic from countries or regions where you do not do business? Are your hosts connecting to risky neighborhoods on the web? You can determine both the source and the destination of traffic—internal, external, or through a partner—searching by application and user group. You can drill into usage bubbles to see rules, IP addresses, users, and more and determine if traffic is business- or non-business-related.

Rapidly diagnose outages
During an application outage, filters help you quickly identify and scope the problem, digging into the root cause without leaving the firewall environment. You can drill down within bubble

charts to understand what users or specific applications are involved, for example TeamViewer or WebEx, and click through directly to investigate further.

Drill downs show users, countries involved, applications, usage levels, and the firewall rules that are allowing or blocking the particular applications. As you implement fixes, the real-time monitoring allows you to validate instantly that the rule set change had the desired effect on traffic, applications, or users.

Quick and direct reporting
McAfee Firewall Enterprise Profiler's graphical reports and reusable reporting objects help you convey information to others within your organization to guide actions and explain events or new requirements. Built-in reports cover pre-defined application and user-based topics, which let you document events and activities without going into another tool. Reports can reflect any level and any filtered or specific view in McAfee Firewall Enterprise Profiler. You can print, save, or export reports into PDF or CSV formats.

Proactive support to validate changes
Visibility into users, applications, and trends makes it possible to profile the impact of infrastructure changes. McAfee Firewall Enterprise Profiler lets you confirm that systems and traffic are back to normal and users have appropriate access to applications.

Available as a Virtual or Dedicated Appliance
A virtual Firewall Enterprise Profiler is included with every McAfee Firewall Enterprise product. In addition, many customers choose to purchase our dedicated Profiler appliance running on McAfee Linux. By operating on a dedicated appliance, out of band, the McAfee Firewall Enterprise Profiler can handle larger data sets, display real-time events, run troubleshooting queries, and let you explore rule sets without affecting on-going firewall or network performance.

Broad, Exhaustive Reporting

Application and identity-based reports	Reports identify the top applications going through the firewall and spotlight the individuals who are using those applications.
Global threat intelligence reputation report	Graphically see the spam that has been dropped at the network edge using reputation-based filtering.
Protocol and web usage	Provides a clear picture of protocol and web usage by user, department, and/or device. Identifies inappropriate usage including user activity associated with security appliance URL filtering.
Bandwidth usage	View bandwidth utilization by department, client, and application.
Regulatory compliance	Report templates take the pain out of regulatory compliance for Sarbanes-Oxley, PCI, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and the Federal Information Security Management Act (FISMA).
Configuration management	Document configuration change detail to prove that corporate networks are configured to government requirements.

Event Analysis and Reporting

Administrators use McAfee Firewall Enterprise Profiler daily to understand changing situations. They turn to McAfee Firewall Reporter to see the larger landscape of historical events and aggregate data for audit and compliance activities. Viewed within McAfee Firewall Enterprise McAfee Firewall Enterprise Control Center or from its own web-based GUI, McAfee Firewall Reporter centralizes audit streams, correlates alerts across devices, handles the longer-term retention of firewall audit data, and streamlines compliance.

Operator-focused reports

More than 550 reports cover all areas of the firewall including application and user based reports by geo-location, security zone, system health, and many other areas that provide comprehensive, device-specific information on individual or groups of firewalls. Reports are operator-focused to help you identify, investigate, correct, and close any issue. Visibility helps you secure the network, manage bandwidth requirements, and ensure appropriate usage.

Identity and application-based reports unlock the capabilities of your next-generation firewall, augmenting existing regulatory reports. Historical attack reports can show events categorized by hour, day, week, month, quarter, or current comparisons by each device, as well as across all devices.

Integrated and scalable

McAfee Firewall Reporter integrates with McAfee Firewall Control Center and is included with McAfee Firewall Enterprise. It scales to the largest environments to generate a complete picture of enterprise security events with no hours wasted in manual analysis of individual device logs.

McAfee ePolicy Orchestrator Platform Integration

Several McAfee firewall management tools integrate with the McAfee ePO platform to help network managers collaborate with enterprise security administrators, helpdesk teams, and auditors. For instance, the McAfee Firewall Enterprise Profiler sends trend and change data to McAfee ePO software that can trigger a helpdesk ticket. Integrations like these make it easier to understand the context of events for faster resolution and uncover the most pressing issues that require intervention.

McAfee Firewall Enterprise McAfee Firewall Enterprise Control Center, McAfee Firewall Enterprise Profiler, and McAfee ePO software can correlate host and firewall health data within the firewall management console. You can view top-level data for multiple firewalls or drill down for detailed data on a firewall or the McAfee Firewall Enterprise Control Center or Profiler appliance that monitors it. McAfee Firewall Enterprise Profiler can obtain host information from an event's drill down to comprehend the situation more quickly.

Get Started

By integrating, automating, and centralizing management activities throughout the firewall management workflow, McAfee offers crucial tools that will help you extract the maximum protection and compliance value out of your firewall investment, with the minimum of time and tedium. The McAfee firewall management tools work together to maximize operational efficiency, simplify policy control, and demonstrate regulatory compliance, while driving down management costs. Learn more at www.mcafee.com/firewall.

Technical Specifications

| Hardware Specs | Control Center Appliances | | | Profiler Appliance |
	C1015	C2050	C3000	P1000
Form Factor	1U	1U	1U	1U
Management Capability (Max)	15 Firewalls	50 Firewalls	100 or Unlimited* Firewalls	N/A
Network Interfaces (10/100/1000 copper)	2	2	2	2
Hard Drive	1 x 500GB SATA 7.2k	2 x 300GB SAS 10k	4 x 300GB SAS 10k	2 x 300GB SAS 10k
RAID	N/A	RAID 1	RAID 5	RAID 1
Optical Drive	None	8x DVD-ROM	8x DVD-ROM	8x DVD-ROM
Out of Band Management	Yes	Yes	Yes	Yes
Remote Access	No	Yes	Yes	Yes
Power Supply	Single 350W	Dual 650W	Dual 650W	Dual 650W
Power Consumption**	306W, 2.8A 110/220V	360W, 3.3A 110/220V	381W, 3.5A 110/220V	@110V, 360W, 3.3A
Dimensions	1.69"x17"x20" (HxWxD)	1.69"x16.9"x27.19" (HxWxD)	1.69"x16.9"x27.19" (HxWxD)	1.69"x16.9"x27.19" (HxWxD)
Weight	22 lbs.	31 lbs.	32 lbs.	31 lbs.
MTBF	130,494 hours	66,531 hours	61,423 hours	66,531 hours

 * C3000 features a license upgrade to allow management of an unlimited quantity of firewalls
** Power supplies are global power auto-sensing for 110-240V

VMware Player, VMware Server, or VMware Workstation software is required to host the Profiler virtual appliance.

McAfee Firewall Enterprise Control Center Appliances (from top down) are the C1015, C2050, and C3000

McAfee Firewall Enterprise Profiler Appliance, the P1000

McAfee®
An Intel Company