Technical Note

Revision B

McAfee Firewall Enterprise 8.x

Using Firewall Enterprise with other McAfee products

This document explains the interoperability between McAfee® Firewall Enterprise (Firewall Enterprise) and other McAfee products.

- McAfee® Firewall Enterprise Control Center
- McAfee® ePolicy Orchestrator® Extension
- McAfee® Logon Collector
- McAfee® Endpoint Intelligence Agent
- McAfee® Event Reporter

Introduction

Firewall Enterprise integrates with a variety of McAfee products to provide additional functionality.

Table 1 McAfee products that integrate with Firewall Enterprise

Product	Function	Availability
McAfee Firewall Enterprise Control Center	Central management	Physical and virtual appliances available for purchase
McAfee ePolicy Orchestrator Extension	Status reporting	Software included with Firewall Enterprise
McAfee Logon Collector	Single sign-on	Software included with Firewall Enterprise
McAfee Endpoint Intelligence Agent	Per-connection metadata	Software included with Firewall Enterprise
McAfee Event Reporter	Security Information and Event Management (SIEM) solution	Physical and virtual appliances available for purchase

This document provides:

- Product overviews
- Requirements

- High-level setup steps
- Use scenarios

This document assumes you have a Firewall Enterprise appliance deployed in your network. For more information about Firewall Enterprise, see the *McAfee Firewall Enterprise Product Guide*.

See also

Find product documentation on page 2

Find product documentation

Review the product documentation for detailed information.

Task

1. Visit mysupport.mcafee.com.
2. In the **Self Service** section, click **Product Documentation**.
3. Select the appropriate product and version.
4. Download the document.

Download McAfee products

You can download McAfee products from the McAfee website.

Task

1. Visit www.mcafee.com/us/downloads.
2. Provide your grant number, then navigate to the appropriate product and version.
3. Navigate to the appropriate file and download it.

Review version compatibility information

Visit the KnowledgeBase for the latest information on McAfee firewall products and versions that interoperate with Firewall Enterprise.

Task

1. Visit mysupport.mcafee.com.
2. Log on with your user ID and password.
   - If you do not have an account but have received a grant number:
     - In the **User Login** section, click **New User**.
     - Complete the information and follow the prompts to set up your account.
   - If you do not have an account or grant number, contact Customer Service.
3. In the **Self Service** section, click **Search the KnowledgeBase**.
4. In the **Ask a Question** section, type `KB67462`, then click **Ask**.

McAfee Firewall Enterprise Control Center

McAfee Firewall Enterprise Control Center (Control Center) is an enterprise-class management tool that remotely manages, maintains, and monitors multiple firewalls.

Use Control Center to:

- Define and distribute access control rules to hundreds of firewalls
- Share configuration data among firewalls
- Configure virtual private network (VPN) connectivity
- Implement and selectively activate multiple security policies
- Manage software releases on all your firewalls
- Simplify routine administrative tasks
- Manage ongoing changes to your security policies
- Identify all changes made to policies across multiple firewalls
- Troubleshoot firewall issues

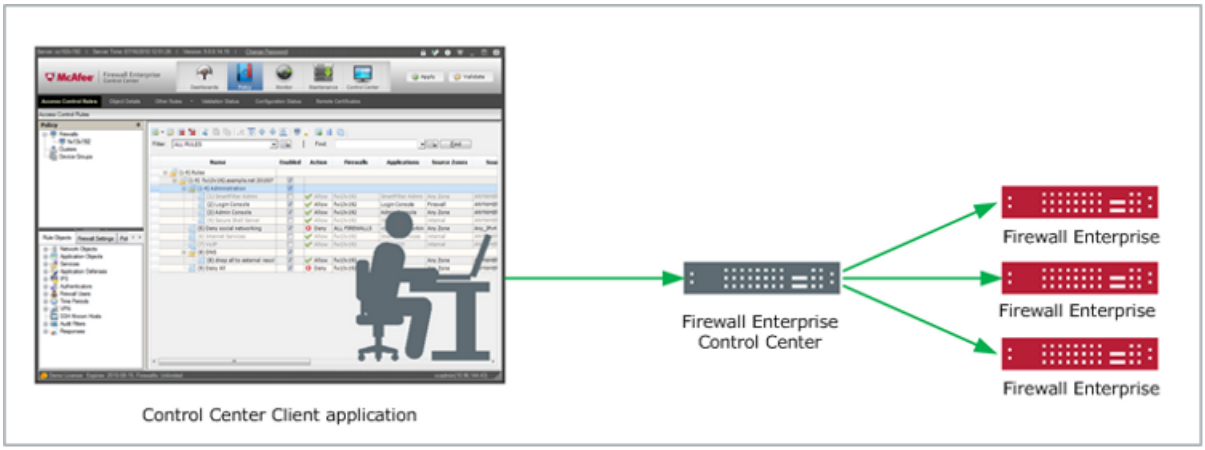

Figure 1 Managing multiple firewalls with Control Center

Availability

Two types of Control Center appliances are available for purchase or evaluation.

- **Physical** — Control Center physical appliances that run on McAfee hardware
- **Virtual** — McAfee® Firewall Enterprise Control Center, Virtual Appliance (Control Center, Virtual Appliance) that runs on the VMware ESXi hypervisor operating system

Requirements

To use Control Center, make sure you have these items.

- Control Center physical or virtual appliance

  If you use Control Center, Virtual Appliance, you also need a server running VMware ESXi.

- One or more Firewall Enterprise appliances
- Microsoft Windows-based computer to run the Control Center Client application

Set up Control Center

To set up Control Center, complete these high-level steps.

Task

1. Collect the documentation needed for setup.
   - (Physical appliance) *McAfee Firewall Enterprise Control Center Quick Start* (included with the shipment)
   - (Virtual appliance) *McAfee Firewall Enterprise Control Center, Virtual Appliance Product Guide*
   - *McAfee Firewall Enterprise Control Center Product Guide*
2. Deploy the Control Center appliance in your network; see the setup instructions in the product guide.
3. Start managing your firewalls using Control Center; see the firewall management instructions in the product guide.

See also

Find product documentation on page 2

Scenario: Consolidate individual firewall policies into a single security policy

In this scenario, assume you have multiple, independently managed Firewall Enterprise appliances deployed throughout your organization and you want to transition to a single security policy.

To achieve this goal, use Control Center to create a new unified policy that is based on your existing firewall policy.

1. Deploy a Control Center appliance in your organization as described in *Set up Control Center*.
2. Use Control Center to retrieve policy from your existing firewalls.
3. Use the Control Center policy cleanup tools to create a single policy that is based on the imported firewall policies.
   - **Merge Rules Wizard** — Combine access control rules that have common elements.
   - **Duplicate Rules Wizard** — Delete duplicate access control rules.
   - **Merge Objects Wizard** — Combine policy objects that have common elements.
   - **Unused Objects window** — View and delete unused policy objects.
4. Associate the new policy with the managed firewalls as appropriate.
5. Validate the new policy to make sure there are no errors.
6. Apply the new policy to the managed firewalls.
7. After your consolidated policy has been in place for an appropriate period of time, use the **Control Center Rule Usage Report** to determine which rules are unused and no longer needed.

McAfee Firewall Enterprise ePolicy Orchestrator Extension

The McAfee Firewall Enterprise ePolicy Orchestrator Extension (Firewall Enterprise ePolicy Orchestrator Extension) allows your McAfee ePO™ server to integrate with Control Center managed or Firewall Profiler managed Firewall Enterprise appliances.

You can view top-level data for multiple firewalls or drill down for detailed data on a firewall or the Control Center or Firewall Profiler that monitors it. You benefit from central visibility into:

- Firewall alerts
- Firewall health statistics
- Historical performance trends
- Tracking of version and patch levels
- Hosts and endpoints used in policies
- Host profile information directly from analytical tools

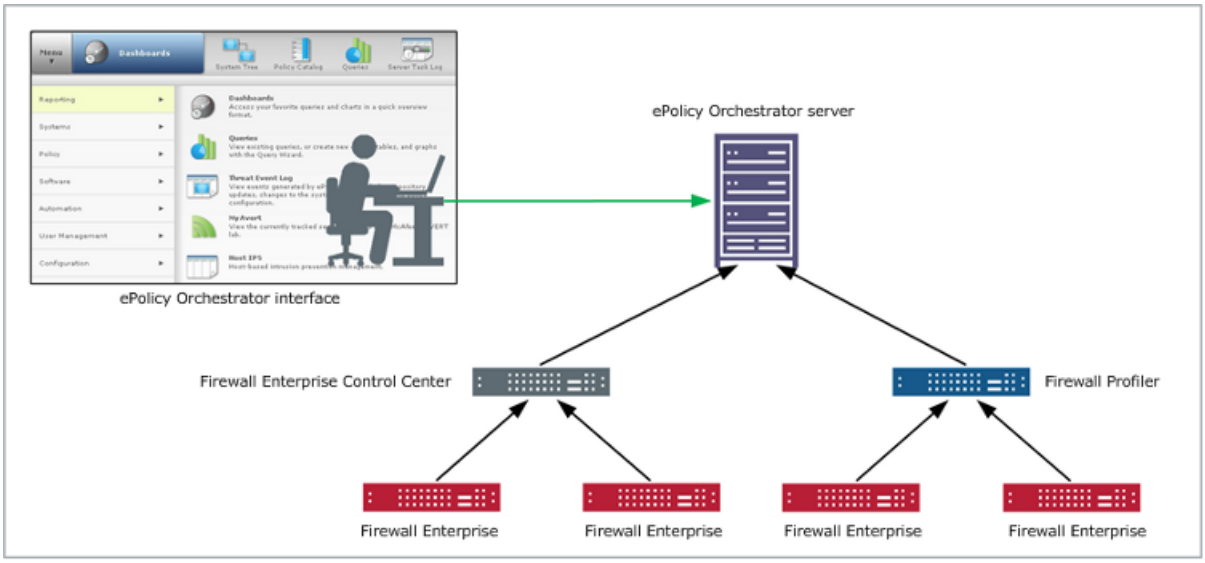

Figure 2 Integrating firewall status into McAfee ePO server

Availability

The Firewall Enterprise ePolicy Orchestrator Extension is included with Firewall Enterprise appliances and runs on the McAfee ePolicy Orchestrator platform.

Requirements

To use the Firewall Enterprise ePolicy Orchestrator Extension, make sure you have these items.

- McAfee ePO server
- One or both of these McAfee appliances:
  - Firewall Enterprise Control Center
  - Firewall Profiler
- One or more Firewall Enterprise appliances

Set up the Firewall Enterprise ePolicy Orchestrator Extension

To set up the Firewall Enterprise ePolicy Orchestrator Extension, you must have a McAfee ePO server and either a Control Center or Firewall Profiler deployed in your network.

Task

1. Download the Firewall Enterprise ePolicy Orchestrator Extension software. See *Download McAfee products*.
2. Download the *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*. See *Find product documentation*.
3. Follow the integration guide instructions to:
   - Install the Firewall Enterprise ePolicy Orchestrator Extension software on your McAfee ePO server.
   - Configure your Control Center or Firewall Profiler appliance.

See also

Find product documentation on page 2
Download McAfee products on page 2

Scenario: Troubleshoot a network outage

Assume that the Firewall Enterprise ePolicy Orchestrator Extension is deployed in your network, and your help desk staff has access to your McAfee ePO server for troubleshooting purposes. However, administrative access to the firewalls is limited to firewall administrators.

When an outage occurs, the help desk staff can use your McAfee ePO server to troubleshoot the situation and determine if the firewall is the cause before contacting firewall administrators. For example, a help desk worker can perform the following troubleshooting steps.

Task

1. Log on to the ePolicy Orchestrator console.
2. Determine if the Firewall Enterprise appliances are operational.
   a. In the ePolicy Orchestrator console, click **Dashboards**.
   b. Click the **Firewall Stats** tab.
   c. Examine the FWCC: Firewall Run Statuses query to determine if any firewalls are unresponsive.
   d. If any firewalls are unresponsive, click the pie chart to view their details.
3. View system resource information for the Firewall Enterprise appliances to determine if they are functioning normally.
   a. In the ePolicy Orchestrator console, click **Dashboards**.
   b. Click the **Firewall Resources** tab.
   c. Examine the firewall resource queries to verify that the firewalls are operating normally.
4. [Optional] View Firewall Profiler events to determine if firewall policy is being applied appropriately.
   a. In the ePolicy Orchestrator console, click **Dashboards**.
   b. Click the **Profiler Events** tab.
   c. Examine the Trend to Deny and Trend to Allow queries to determine if the firewalls are unexpectedly allowing or denying network traffic.

5 Take action based the troubleshooting results.

- If there is a firewall problem, contact a firewall administrator to resolve the issue.

  The firewall administrator can also expedite troubleshooting by leveraging the Firewall Enterprise ePolicy Orchestrator Extension to view endpoint information.

- If firewalls are not the cause, continue to investigate using ePolicy Orchestrator without contacting the firewall administrators.

McAfee Logon Collector

McAfee Logon Collector (Logon Collector) is a Microsoft Windows-based, distributed collector.

Logon Collector polls Microsoft Active Directory and domain controllers for user characteristics such as authentication status, group membership, and current IP address, and sends the information to other McAfee appliances.

- **Firewall Enterprise** — Uses the information provided by Logon Collector to control access based on user identity; users are not prompted for authentication by the firewall
- **Control Center** — Uses the information provided by Logon Collector to create user-based access control policy and apply it to Firewall Enterprise appliances
- **Firewall Profiler** — Uses the information provided by Logon Collector to correlate network traffic with user behavior

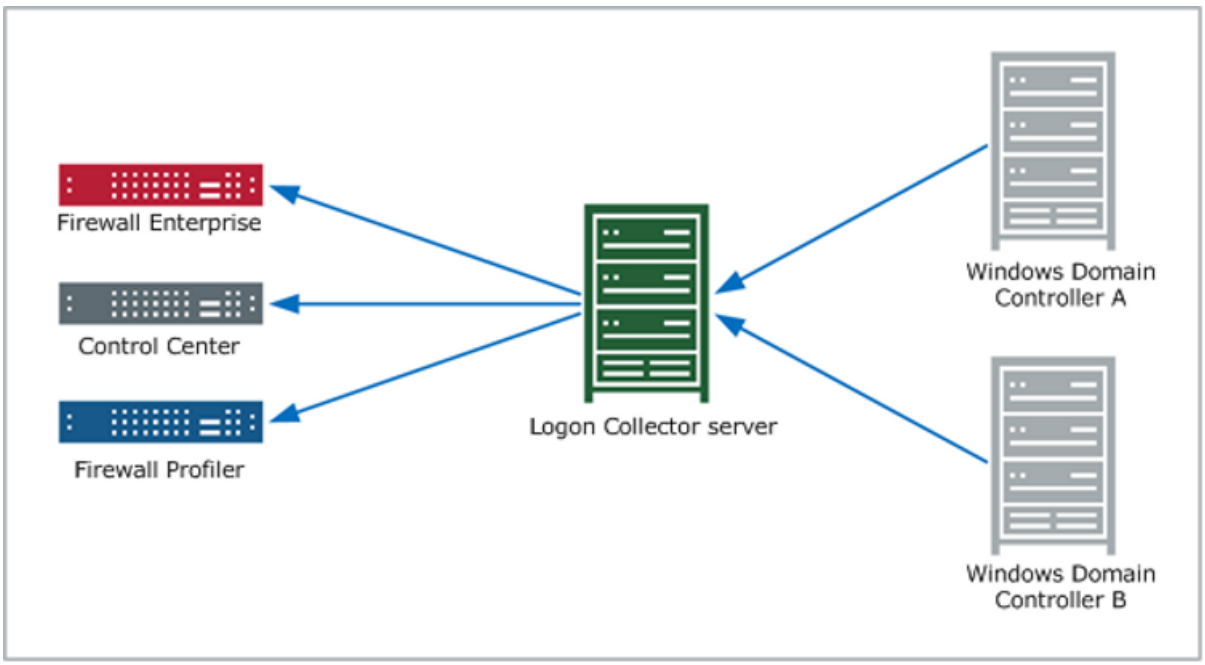

Figure 3 Providing user information with Logon Collector

Availability

The Logon Collector software is included with Firewall Enterprise, Control Center, and Firewall Profiler appliances.

Requirements

To use Logon Collector, make sure you have these items.

- Windows-based server to host Logon Collector
- One of these McAfee appliances:
  - Firewall Enterprise
  - Firewall Enterprise Control Center
  - Firewall Profiler

Set up Logon Collector

To set up Logon Collector, complete these high-level steps.

Task

1. Download the Logon Collector software.

   See *Download McAfee products*.

2. Download the *McAfee Logon Collector Product Guide*.

   See *Find product documentation*.

3. Follow the instructions in the *McAfee Logon Collector Product Guide* to install Logon Collector on a Windows-based server.

4. Configure your McAfee appliances to communicate with Logon Collector.

   For each appliance, see the product documentation for instructions:

   - **Firewall Enterprise** — *McAfee Firewall Enterprise Product Guide*
   - **Firewall Enterprise Control Center** — *McAfee Firewall Enterprise Control Center Product Guide*
   - **Firewall Profiler** — *McAfee Firewall Profiler Product Guide*

See also

Find product documentation on page 2
Download McAfee products on page 2

Scenario: Allow access to a user on a business trip

Assume that remote users access your organization's resources using a VPN that is authenticated by Microsoft Active Directory. Because remote users are often assigned dynamic IP addresses, it can be difficult to control what they access or determine what they have accessed in the past.

As shown by Figure 5, a user might use any number of IP addresses over a short business trip. Since you don't know what devices or IP addresses the remote user will use:

- How do you enforce access control policy for the remote user?
- How do you determine which resources have been accessed by the remote user?

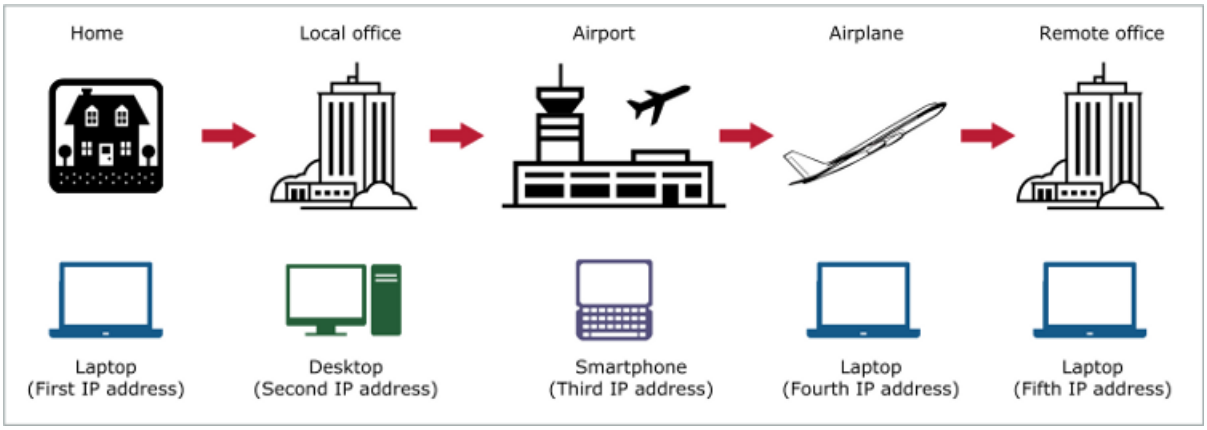

Figure 4 Identifying a user on a business trip

If Logon Collector is deployed in your network, it associates remote users with their IP address when they provide their Active Directory credentials to authenticate the VPN. Logon Collector then supplies this information to other McAfee products on your network.

- **Firewall Enterprise** — With the information provided by Logon Collector, you can create access control rules that allow and deny access based on users and the groups they belong to. Regardless of the dynamic IP addresses used by a remote user, the correct identity-based access control rules match.
- **Firewall Profiler** — With the information provided by Logon Collector, Firewall Profiler can visually display which resources were accessed by each user regardless of their IP address.

McAfee Endpoint Intelligence Agent

McAfee Endpoint Intelligence Agent (McAfee EIA) is a Windows-based endpoint solution that provides per-connection information to Firewall Enterprise.

When McAfee EIA is installed on a host system, the agent monitors the system for any outgoing connections. When a connection attempt is made, the agent sends information to Firewall Enterprise over an encrypted channel. Firewall Enterprise uses that information for policy decision making and auditing.

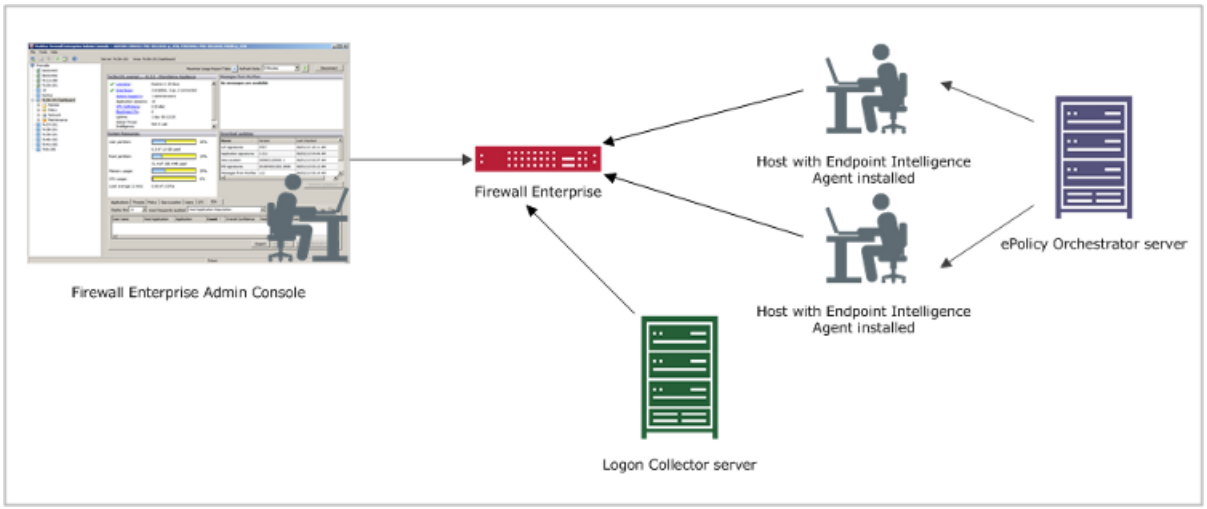

Figure 5 Using host metadata to enforce policy

Availability

The McAfee EIA software is included with Firewall Enterprise appliances.

Requirements

To use McAfee EIA, make sure you have these items.

- Host computers with McAfee EIA installed
- Endpoint Intelligence Manager (EIM)
- One or more Firewall Enterprise appliances (version 8.3.0 or later)
- Firewall Enterprise ePolicy Orchestrator Extension
- McAfee Logon Collector server

Set up McAfee EIA

To set up McAfee EIA, complete these high-level steps.

Task

1 Download the McAfee EIA software.

   See *Download McAfee products*.

2 Download the *McAfee Endpoint Intelligence Agent Product Guide*.

   See *Find product documentation*.

3 Configure the McAfee appliances to communicate with McAfee EIA.

For each appliance, see the product documentation for instructions:

- **Firewall Enterprise** — *McAfee Firewall Enterprise Product Guide*
- **ePolicy Orchestrator** — *Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*
- **McAfee Logon Collector** — *McAfee Logon Collector Product Guide*
- **Firewall Enterprise Control Center** — *McAfee Firewall Enterprise Control Center Product Guide*

4 Deploy McAfee EIA on your network.

See also

Find product documentation on page 2
Download McAfee products on page 2

Scenario: Blacklist an executable file of an allowed application

In this scenario, assume that you have McAfee EIA deployed on your network and Firewall Enterprise configured to use host metadata for auditing and policy enforcement. The firewall has executable file reputation, Global Threat Intelligence, and the classification list enabled.

Due to a known vulnerability, your company policy does not allow version 1.0.0.100 of the GoogleTalk instant messaging application. Though the GoogleTalk application is allowed on your network, you want to blacklist the executable file of the vulnerable version.

Perform these high-level steps to blacklist the GoogleTalk version.

1 Locate the MD5 hash value of GoogleTalk version 1.0.0.100.

2 On the firewall McAfee EIA classification list, add a blacklist executable entry.

3 Configure a firewall attack response.

McAfee Event Reporter

McAfee Event Reporter (Event Reporter) is a Security Information and Event Management (SIEM) solution for up to 25 McAfee devices in one location.

Event Reporter gathers data simultaneously from the devices through syslog and can process up to 1000 events per second. Use Event Reporter for:

- Event and flow data management, with Dynamic Aggregation options
- Tracking of appliance activity and status
- Firewall-specific and customizable reporting

- Event Correlation and alerting
- Granular forensics analysis

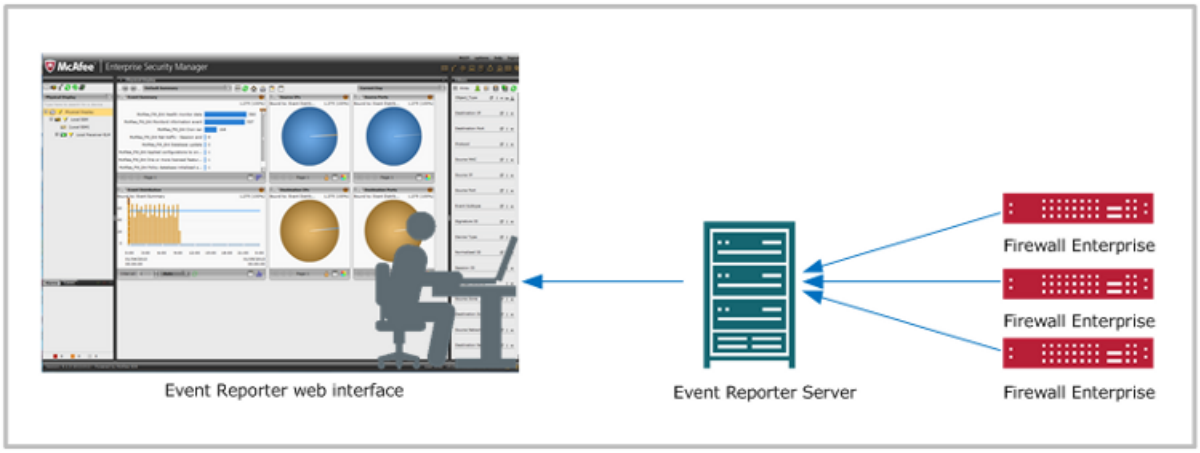

Figure 6 Managing firewall logs with Event Reporter

Availability

There are two types of Event Reporter appliances.

- **Physical** — Event Reporter physical appliances run on dedicated hardware.
- **Virtual** — VMware Player, VMware Server, or VMware Workstation software is required to host Event Reporter.

Requirements

To use Event Reporter, make sure you have these items.

- Linux-based server to host Event Reporter
- One or more Firewall Enterprise or Control Center appliances
- Computer with a web browser to access the Event Reporter web management interface

Set up Event Reporter

To set up Event Reporter, complete these high-level steps.

Task

1 Download the product documentation.
   - *McAfee Enterprise Security Manager ESMI Setup and Installation Guide*
   - *McAfee Reporter User Guide*
   - *McAfee Firewall Enterprise Product Guide*

2 Download the software.

3 Install the Event Reporter virtual machine on a VMware ESXi server.
   a Verify that your VMware machine meets the requirements.
   b If necessary, stripe the storage drive.

c Install the virtual Event Reporter.

d Configure the network interface on the virtual machine.

See the *McAfee Enterprise Security Manager ESMI Setup and Installation Guide* for more information.

4 Configure Event Reporter and add data sources.

a Configure the Event Reporter properties.

b Under the Local Receiver, add the firewall appliance as a data source.

You must select McAfee Firewall Enterprise (ASP)

c Choose a predefined view or create a custom view.

See the *McAfee Enterprise Security Manager Interface Reporter User Guide* for more information.

5 Configure the syslog audit for export to Event Reporter.

Audit or log source	Instructions
Firewall Enterprise	See the *McAfee Firewall Enterprise Product Guide* for more information.
Firewall Enterprise appliance archive	1 Make the raw Firewall Enterprise log data available on an FTP, SFTP, NFS, or CIFS share. 2 In Event Reporter, add a Firewall Enterprise data source. 3 Select the same **Data Retrieval** type as the share. 4 Complete the form with the rest of the necessary information. 5 After the archive has been processed, change the **Data Retrieval** type back to default.

See also

Find product documentation on page 2
Download McAfee products on page 2

Scenario: Correlate events and notify of suspicious behavior

Assume your Firewall Enterprise appliances are configured to export audit to Event Reporter, you created a correlation rule for IP addresses in Event Reporter, and you chose to be alerted by email.

A network event with the same source IP address comes in from China and the United States, and Event Reporter sends a notification email.

From the Event Reporter web interface, you can use various views to:

- Review all events generated by that IP address to see what else that IP address accessed over a period of time.
- Provide data needed for internal or external security audits.
- Report on these events for internal notification or compliance regulations.
- Send the event to case management for assignment and resolution.

Copyright © 2013 McAfee, Inc. Do not copy without permission.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.