McAfee Endpoint Security 10.6.0 - Firewall Product Guide

(McAfee ePolicy Orchestrator)

Contents

1 Product overview **5**

Overview of Endpoint Security 5
How Endpoint Security works 6
Overview of Firewall 7
Key features of Firewall 8
How Firewall works 9
Feature overview 9
How firewall rules work 10
How firewall rule groups work 11
Firewall stateful packet filtering and inspection 16
Using trusted networks to allow traffic automatically 20
Using trusted executables and applications to reduce false positives 20
Using the Firewall Catalog to reference existing items 20
Firewall protocols 20
How Adaptive mode affects Firewall 22
FAQ — McAfee GTI and Firewall 22
Firewall additions to McAfee ePO 23
Permission sets and Firewall 24
Client tasks and Firewall 25

2 Configuring Firewall **27**

Policies and Firewall 27
Enable and configure Firewall 28
Block DNS traffic 29
Define networks to use in rules and groups 29
Configure trusted executables 30
Get the signer distinguished name from McAfee ePO to use to specify trusted executables 30
Manage firewall rules and groups 31
Wildcards in firewall rules 32
Create connection isolation groups 32
Create timed groups 33
Use the Firewall Catalog 33
Tuning Firewall 34
Using Adaptive mode to create client rules automatically 35
Analyzing client data 36

3 Monitoring Firewall activity with McAfee ePO **39**

Dashboards, monitors, and Firewall 39
Queries, reports, and Firewall 40
Server tasks and Firewall 41
Roll up system or event data for Endpoint Security 42
Events, responses, and Firewall 43

4 Using Firewall on a client system **45**

Enable and disable Firewall from the McAfee system tray icon 45

Enable or view Firewall timed groups from the McAfee system tray icon 45

5 Managing Firewall on a client system 47

Enable and configure Firewall on a client system 47
Block DNS traffic on a client system 48
Define networks to use in rules and groups on a client system 48
Configure trusted executables on a client system 49
Get the signer distinguished name to specify trusted executables on a client system 50
Create and manage Firewall rules and groups on a client system 50
Create connection isolation groups on a client system 52
Create timed groups on a client system 53

6 Monitoring Firewall activity on a client system 55

Check the Event Log for recent activity 55
Firewall log file names and locations 55

1 Product overview

Contents

- *Overview of Endpoint Security*
- *How Endpoint Security works*
- *Overview of Firewall*
- *Key features of Firewall*
- *How Firewall works*
- *Feature overview*
- *Firewall additions to McAfee ePO*

Overview of Endpoint Security

McAfee® Endpoint Security is an integrated, extensible security solution that protects servers, computer systems, laptops, and tablets against known and unknown threats. These threats include malware, suspicious communications, unsafe websites, and downloaded files.

Endpoint Security enables multiple defense technologies to communicate in real time to analyze and protect against threats.

Endpoint Security consists of these security modules:

- **Threat Prevention** — Prevents threats from accessing systems, scans files automatically when they are accessed, and runs targeted scans for malware on client systems.
- **Firewall** — Monitors communication between the computer and resources on the network and the Internet. Intercepts suspicious communications.
- **Web Control** — Monitors web searching and browsing activity on client systems and blocks websites and downloads based on safety rating and content.
- **Adaptive Threat Protection** — Analyzes content from your enterprise and decides how to respond based on file reputation, rules, and reputation thresholds. Adaptive Threat Protection is an optional Endpoint Security module.

The Common module provides settings for common features, such as interface security and logging. This module is installed automatically if any other module is installed.

All modules integrate into a single Endpoint Security interface on the client system. Each module works together and independently to provide several layers of security.

See also

How Endpoint Security works on page 6
Overview of Firewall on page 7

How Endpoint Security works

Endpoint Security intercepts threats, monitors overall system health, and reports detection and status information. Client software is installed on each system to perform these tasks.

Typically, you install one or more Endpoint Security modules on client systems, manage detections, and configure settings that determine how product features work.

McAfee ePO

You use McAfee® ePolicy Orchestrator® (McAfee® ePO™) to deploy and manage Endpoint Security modules on client systems. Each module includes an extension and a software package that are installed on the McAfee ePO server. McAfee ePO then deploys the software to client systems.

Using McAfee® Agent, the client software communicates with McAfee ePO for policy configuration and enforcement, product updates, and reporting.

Client modules

The client software protects systems with regular updates, continuous monitoring, and detailed reporting.

It sends data about detections on your computers to the McAfee ePO server. This data is used to generate reports about detections and security issues on your computers.

TIE server and Data Exchange Layer

The Endpoint Security framework integrates with McAfee® Threat Intelligence Exchange (TIE) and McAfee® Data Exchange Layer (DXL) when using Adaptive Threat Protection. These optional products enable you to control file reputation locally and share the information immediately throughout your environment.

If the TIE server is not available, Adaptive Threat Protection queries McAfee® Global Threat Intelligence™ (McAfee GTI) for reputation information.

McAfee GTI

Threat Prevention, Firewall, Web Control, and Adaptive Threat Protection query McAfee GTI for reputation information to determine how to handle files on the client system.

McAfee Labs

The client software communicates with McAfee Labs for content file and engine updates. McAfee Labs regularly releases updated content packages.

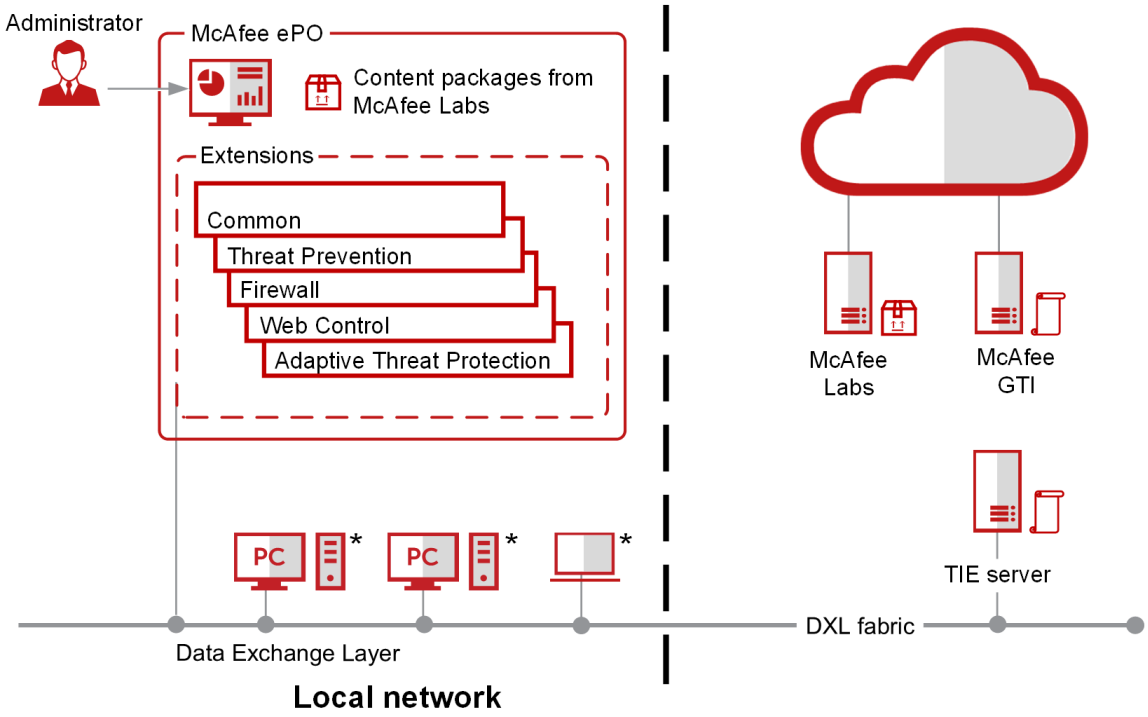


Figure 1-1 How it works

How your protection stays up to date

Regular updates of Endpoint Security protect your computers from the latest threats.

To perform updates, the client software connects to a local or remote McAfee ePO server or directly to a site on the Internet. Endpoint Security checks for:

- Updates to the content files that detect threats. Content files contain definitions for threats such as viruses and spyware, and these definitions are updated as new threats are discovered.
- Upgrades to software components, such as patches and hotfixes.

See also

Overview of Firewall on page 7
How Firewall works on page 9

Overview of Firewall

McAfee® Endpoint Security Firewall protects systems, network resources, and applications from external and internal attacks.

Firewall scans all incoming and outgoing traffic and compares it to its list of firewall rules, which is a set of criteria with associated actions. If a packet matches all criteria in a rule, the firewall acts according to the rule, blocking or allowing the packet through the firewall.

You use McAfee ePO to deploy and manage Firewall on client systems.

See also

Overview of Endpoint Security on page 5

Key features of Firewall

The key features of Firewall protect against threats, detect security issues, and correct false positives.

Protect

Protect your network and applications these Firewall features:

- **Rules** — Define the criteria Firewall uses to determine whether to block or allow incoming and outgoing traffic.
- **Rule groups** — Organize firewall rules for easy management, enabling you to apply rules manually or on a schedule, and to only process traffic based on connection type.
- **Stateful packet filtering and inspection** — Track network connection state and characteristics in a state table, allowing only packets that match a known open connection.
- **Reputation-based control** — Block untrusted executables, or all traffic from an untrusted network, based on reputation.

Detect

Detect security issues using these Firewall features:

- **Dashboards and monitors** — Display intrusion and detection events from McAfee GTI and Firewall.
- **Queries and reports** — Retrieve detailed information about Firewall, including client rules, errors, intrusion and block events, and save that information in reports.
- **Alerts** — Display alerts for blocked traffic, based on executable or network reputation.
- **Log traffic** — Log all blocked or allowed traffic.

Correct

Reduce or eliminate false positives using these Firewall features:

- **Adaptive mode** — Create rules automatically on the client system to allow legitimate activity.

  Once created, analyze client rules to decide which to convert to server-mandated policies.
- **Defined networks** — Define trusted networks to allow traffic from networks that your organization considers safe.
- **Trusted executables** — Maintain a list of safe executables to reduce false positives.
- **Firewall Catalog** — Define rules and groups to add to multiple policies, or networks and applications to add to firewall rules.
- **Client options** — Allow users to disable Firewall temporarily for troubleshooting.
- **Dashboards and monitors** — Monitor activity and intrusion detections, then use that information to tune Firewall settings.

How Firewall works

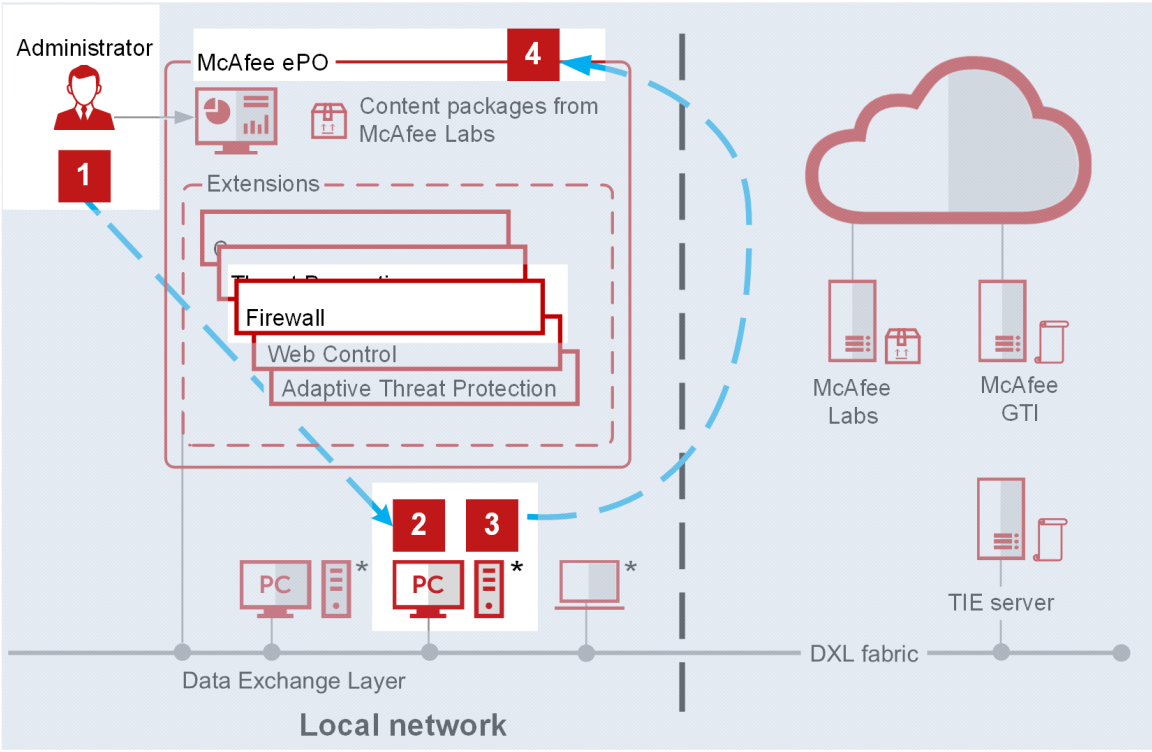
Firewall scans all incoming and outgoing traffic at the packet level and compares packets to the configured firewall rules to determine whether to allow or block the traffic.

1 The administrator configures firewall rules in McAfee ePO and enforces the policy to the client system.

2 The user performs a task that initiates network activity and generates traffic.

3 Firewall scans all incoming and outgoing traffic and compares packets to configured rules. If the traffic matches a rule, Firewall blocks or allows it, based on the rule criteria.

4 Firewall logs the details, then generates and sends an event to McAfee ePO.



* Client modules: Common, Threat Prevention, **Firewall**, Web Control, and Adaptive Threat Protection

Figure 1-2 How it works

See also

Predefined firewall rule groups in McAfee ePO on page 11
Predefined firewall rule groups on a client system on page 12
Firewall rule groups and connection isolation on page 14
Firewall stateful packet filtering and inspection on page 16

Feature overview

Contents

- *How firewall rules work*
- *How firewall rule groups work*
- *Firewall stateful packet filtering and inspection*
- *Using trusted networks to allow traffic automatically*

- *Using trusted executables and applications to reduce false positives*
- *Using the Firewall Catalog to reference existing items*
- *Firewall protocols*
- *How Adaptive mode affects Firewall*
- *FAQ — McAfee GTI and Firewall*

How firewall rules work

Firewall rules determine how to handle network traffic. Each rule provides a set of conditions that traffic must meet, and an action to allow or block traffic.

When Firewall finds traffic that matches a rule's conditions, it performs the associated action.

You can define rules broadly (for example, all IP traffic) or narrowly (for example, identifying a specific application or service) and specify options. You can group rules according to a work function, service, or application for easier management. Like rules, you can define rule groups by network, transport, application, schedule, and location options.

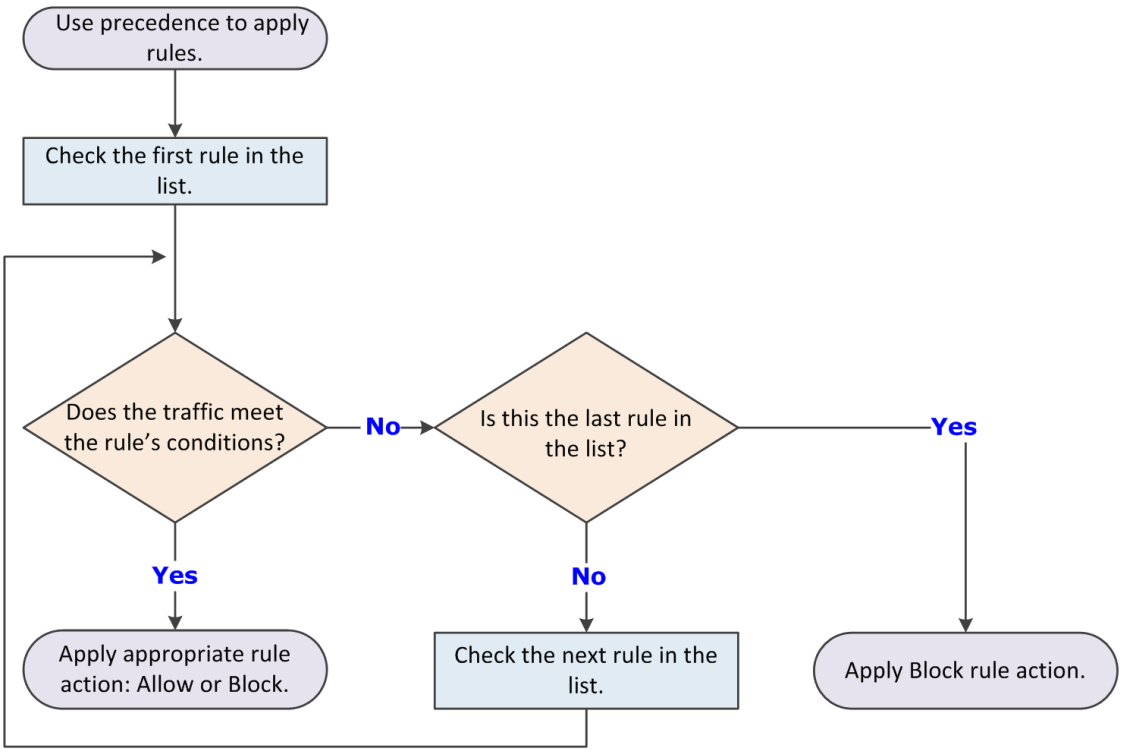
Firewall uses precedence to apply rules:

1. Firewall applies the rule at the top of the firewall rules list.

   If the traffic meets this rule's conditions, Firewall allows or blocks the traffic. It doesn't try to apply any other rules in the list.

2. If the traffic doesn't meet the first rule's conditions, Firewall continues to the next rule in the list until it finds a rule that the traffic matches.

3. If no rule matches, the firewall automatically blocks the traffic.



If Adaptive mode is activated, an Allow rule is created for the traffic. Sometimes the intercepted traffic matches more than one rule in the list. In this case, precedence means that Firewall applies only the first matching rule in the list.

Best practices

Place the more specific rules at the top of the list, and the more general rules at the bottom. This order makes sure that Firewall filters traffic appropriately.

For example, to allow all HTTP requests except from a specific address (for example, IP address 10.10.10.1), create two rules:

- **Block rule** — Block HTTP traffic from IP address 10.10.10.1. This rule is specific.
- **Allow rule** — Allow all traffic using the HTTP service. This rule is general.

Place the Block rule higher in the firewall rules list than the Allow rule. When the firewall intercepts the HTTP request from address 10.10.10.1, the first matching rule it finds is the one that blocks this traffic through the firewall.

If the general Allow rule is higher than the specific Block rule, Firewall matches requests against the Allow rule before finding the Block rule. It allows the traffic, even though you wanted to block the HTTP request from a specific address.

How firewall rule groups work

Firewall rule groups organize firewall rules for easy management. The software includes predefined rule groups with rules that allow needed services, such as McAfee ePO and DNS, to run.

Firewall rule groups don't affect the way Firewall handles the rules; the software processes rules from top to bottom.

Firewall processes the settings for the group before processing the settings for the rules it contains. If a conflict exists between these settings, the group settings take precedence.

You can create customized rule groups:

- **Timed groups** — Activate the group's settings manually or on a specified schedule.
- **Connection isolation groups** — Process only traffic that matches a defined connection type and group criteria.

See also

Using timed groups on page 13
Making groups location-aware on page 13

Predefined firewall rule groups in McAfee ePO

The predefined firewall groups include needed rules, such as core networking rules to allow McAfee applications.

Firewall group	Description
McAfee core networking	Contains the core networking rules provided by McAfee and includes rules to allow McAfee applications and DNS.  You can't change or delete these rules. You can disable some of the rules in this group by selecting the **Disable McAfee core networking rules** option in the Firewall Options. But, this might disrupt network communications on the client.
ePolicy Orchestrator server	Contains rules to allow McAfee ePO services to run.

Firewall group	Description
Basic networking (Required)	Contains rules to allow basic networking services, such as DNS, to run.
VPN	Contains rules to allow VPN services to run.
ICMP	Contains rules to allow all ICMP traffic.
Windows AD authentication	Contains rules to allow Windows Active Directory authentication.
NetBIOS	Contains rules to allow inbound and outbound NetBIOS services and sessions, and block untrusted NetBIOS services.
Web/FTP	Contains rules to allow outbound HTTPS and FTP services.
Mail clients	Contains rules to allow outbound mail services, such as POP.
Network tools	Contains rules to allow Remote Desktop (RDP) connections.

Predefined firewall rule groups on a client system

The predefined firewall groups include needed rules, such as core networking rules to allow McAfee applications.

If a firewall group has no rules defined, it appears in gray to indicate that the group is empty.

Firewall group	Description
McAfee core networking	Contains the core networking rules provided by McAfee and includes rules to allow McAfee applications and DNS. You can't change or delete these rules. You can disable some of the rules in this group by selecting the **Disable McAfee core networking rules** option in the Firewall Options. But, this might disrupt network communications on the client.
Admin-defined	Contains rules defined by the administrator at the management server. This group appears on the Endpoint Security Client only if the client system is managed by McAfee ePO. In this case, the group displays **Enabled** even if it contains no rules. These rules can't be changed or deleted on the Endpoint Security Client.
User-defined	Contains rules defined on the Endpoint Security Client. This group displays **Enabled** even if it contains no rules. Because these rules are created on the client system, these rules might be overwritten when the policy is enforced, depending on policy settings.
Adaptive	Contains client exception rules that are created automatically when the system is in Adaptive mode. This group displays **Enabled** even if Adaptive mode is not enabled and the group contains no rules. Once Adaptive mode is enabled, the group is populated with automatically generated rules. Because these rules are created on the client system, these rules might be overwritten when the policy is enforced, depending on policy settings.
Default	Contains default rules provided by McAfee. These rules can't be changed or deleted.

Using timed groups

Timed groups are Firewall rule groups that are active for a set time.

For example, a timed group can be enabled to allow a client system to connect to a public network and establish a VPN connection.

Depending on settings, groups can be activated either:

- On a specified schedule.
- Manually by selecting options from the McAfee system tray icon.

Making groups location-aware

You can make a group and its rules location-aware and create connection isolation.

Settings for **Transport** and **Executables** aren't available for connection isolation groups.

The Location and Network Options of the group enable you to make the groups network adapter-aware. Use network adapter groups to apply adapter-specific rules for computers with multiple network interfaces. After enabling location status and naming the location, parameters for allowed connections can include the following for each network adapter:

- **Location**:
  - Connection-specific DNS suffix
  - Default gateway IP address
  - DHCP server IP address
  - DNS server queried to resolve URLs
  - Primary WINS server IP address
  - Secondary WINS server IP address
  - Domain reachability (HTTPS)
  - Registry key

  If you specify more than one location-criteria parameter, all are applied to the location-aware group.

- **Networks** (local):
  - **Single IP address**
  - **Range**
  - **Subnet**

If two location-aware groups apply to a connection, Firewall uses normal precedence, processing the first applicable group in its rule list. If no rule in the first group matches, rule processing continues.

When Firewall matches a location-aware group's parameters to an active connection, it applies the rules in the group. It treats the rules as a small rule set and uses normal precedence. If some rules don't match the intercepted traffic, Firewall ignores them.

If this option is selected...	Then...
Enable location awareness	A location name is required.
Require that McAfee ePO is reachable	The McAfee ePO is reachable and the FQDN of the server has been resolved. To determine whether the McAfee ePO server is available, Firewall performs DNS and WINS queries for the McAfee ePO server name, which is registered with McAfee Agent. If both WINS and DNS fail to resolve the name, the McAfee ePO server is not available.
Local Network	The IP address of the adapter must match one of the list entries.
Connection-specific DNS suffix	The DNS suffix of the adapter must match one of the list entries.

If this option is selected...	Then...
Default gateway	The default adapter gateway IP address must match at least one of the list entries.
DHCP server	The adapter DHCP server IP address must match at least one of the list entries.
DNS server	The adapter DNS server IP address must match any of the list entries.
Primary WINS server	The adapter primary WINS server IP address must match at least one of the list entries.
Secondary WINS server	The adapter secondary WINS server IP address must match at least one of the list entries.
Domain reachability (HTTPS)	The specified domain must be reachable using HTTPS. To determine whether the domain is reachable, Firewall checks for the valid SSL certificate of the domain. The location-aware group criteria matches and the rules are applied only if the domain has a valid certificate.

Firewall rule groups and connection isolation

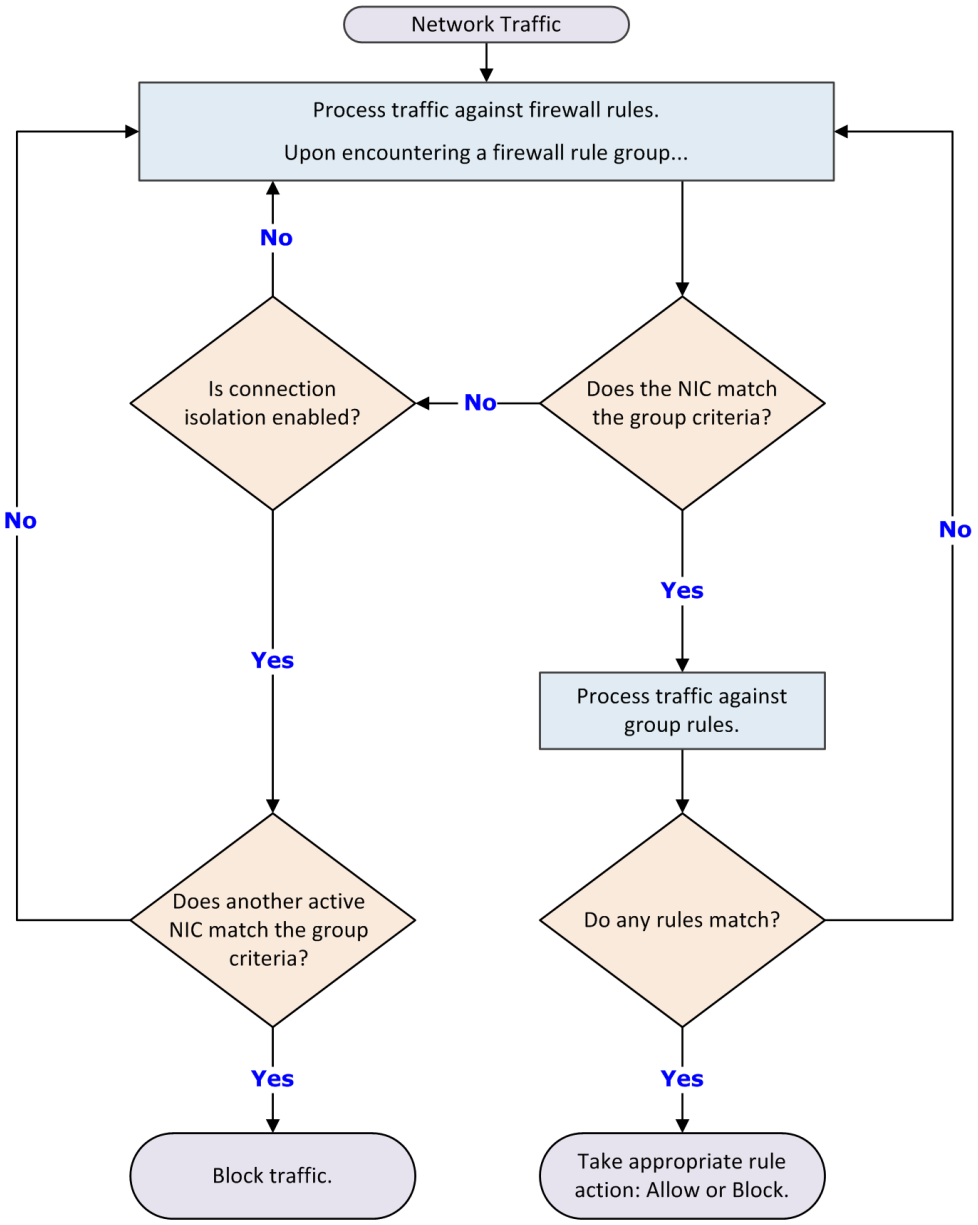
Prevent undesirable traffic from accessing a designated network by using connection isolation for groups.

When connection isolation is enabled for a group, and an active Network Interface Card (NIC) matches the group criteria, Firewall only processes traffic that matches:

- Allow rules above the group in the firewall rules list
- Group criteria

All other traffic is blocked.

Any group with connection isolation enabled can't have associated transport options or executables.



As examples of using connection isolation, consider two settings: a corporate environment and a hotel. The active firewall rules list contains rules and groups in this order:

1. Rules for basic connection
2. VPN connection rules
3. Group with corporate LAN connection rules
4. Group with VPN connection rules

Example: connection isolation on the corporate network

Connection rules are processed until the group with corporate LAN connection rules is encountered. This group contains these settings:

- Connection type = Wired
- Connection-specific DNS suffix = mycompany.com
- Default gateway
- Connection isolation = Enabled

The computer has both LAN and wireless network adapters. The computer connects to the corporate network with a wired connection. But, the wireless interface is still active, so it connects to a hotspot outside the office. The computer connects to both networks because the rules for basic access are at the top of the firewall rules list. The wired LAN connection is active and meets the criteria of the corporate LAN group. The firewall processes the traffic through the LAN but because connection isolation is enabled, all other traffic not through the LAN is blocked.

Example: connection isolation at a hotel

Connection rules are processed until the group with VPN connection rules is encountered. This group contains these settings:

- Connection type = Virtual
- Connection-specific DNS suffix = vpn.mycompany.com
- IP address = An address in a range specific to the VPN concentrator
- Connection isolation = Enabled

General connection rules allow the setup of a timed account at the hotel to gain Internet access. The VPN connection rules allow connection and use of the VPN tunnel. After the tunnel is established, the VPN client creates a virtual adapter that matches the criteria of the VPN group. The only traffic the firewall allows is inside the VPN tunnel and the basic traffic on the actual adapter. Attempts by other hotel guests to access the computer over the network, either wired or wireless, are blocked.

Firewall stateful packet filtering and inspection

Firewall provides both stateful packet filtering and stateful packet inspection.

Stateful packet filtering is the stateful tracking of TCP/UDP/ICMP protocol information at Transport Layer 4 and lower of the OSI network stack. Each packet is examined. If the inspected packet matches an existing firewall Allow rule, the packet is allowed and an entry is made in a state table. The state table dynamically tracks connections previously matched against a static rule set, and reflects the current connection state of the TCP/UDP/ICMP protocols. If an inspected packet matches an existing entry in the state table, the packet is allowed without further scrutiny. When a connection is closed or times out, its entry is removed from the state table.

Stateful packet inspection is the process of stateful packet filtering and tracking commands at Application Layer 7 of the OSI network stack. This combination offers a strong definition of the computer's connection state. Access to the application-level commands provides error-free inspection and securing of the FTP protocol.

See also

Firewall state table on page 18
Stateful protocol tracking on page 19

How stateful packet filtering works

Stateful filtering involves processing a packet against two rule sets: a configurable firewall rule set and a dynamic firewall rule set or state table.

The configurable rules have two possible actions:

- Allow — The packet is permitted and an entry is made in the state table.
- Block — The packet is blocked and no entry is made in the state table.

The state table entries result from network activity and reflect the state of the network stack. Each rule in the state table has only one action, Allow, so that any packet matched to a rule in the state table is automatically permitted.

The filtering process includes the following:

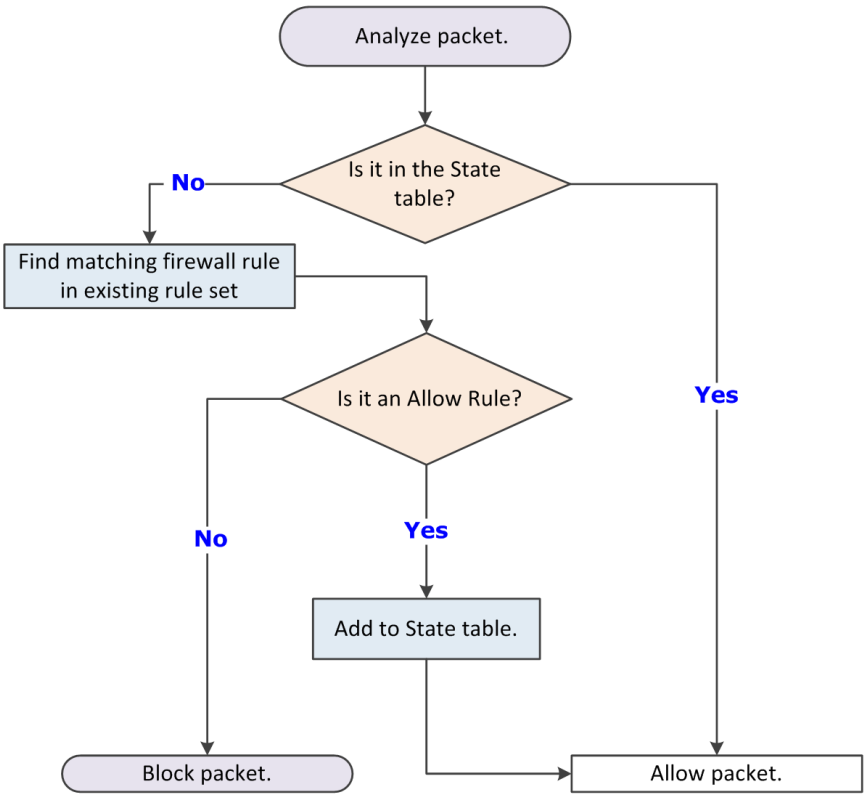
1 The firewall compares an incoming packet against entries in the state table. If the packet matches any entry in the table, the packet is immediately allowed. If not, the configurable firewall rules list is examined.

> A state table entry is considered a match if the Protocol, Local Address, Local Port, Remote Address, and Remote Port match those elements of the packet.

2 If the packet matches an Allow rule, it is allowed and an entry is created in the state table.

3 If the packet matches a Block rule, it is blocked.

4 If the packet doesn't match any configurable rule, it is blocked.



How stateful packet inspection works

Stateful packet inspection combines stateful filtering with access to application-level commands, which secure protocols such as FTP.

FTP involves two connections: *control* for commands and *data* for the information. When a client connects to an FTP server:

- The control channel is established on FTP destination port 21.
- An entry is made in the state table.

If Use FTP protocol inspection is enabled, the firewall performs stateful packet inspection on packets arriving through the FTP control channel on port 21.

With the control channel open, the client communicates with the FTP server. The firewall parses the PORT command in the packet and creates a second entry in the state table to allow the data connection.

When the FTP server is in active mode, it opens the data connection; in passive mode, the client initiates the connection. When the FTP server receives the first data transfer command (LIST), it opens the data connection toward the client and transfers the data. The data channel is closed after the transmission is completed.

The combination of the control connection and data connections is called a *session*. FTP dynamic rules are sometimes called *session rules*. The session remains established until its control channel entry is deleted from the state table. During the periodic cleanup of the table, if a session's control channel has been deleted, all data connections are then deleted.

Firewall state table

A firewall state table dynamically stores information about active connections allowed by firewall rules.

Each entry in the table defines a connection based on:

- Protocol — The predefined way one service talks with another; includes TCP, UDP, and ICMP protocols.
- IP addresses for local and remote computers — Each computer is assigned a unique IP address. IPv4, the current standard for IP addresses, permits addresses 32 bits long, whereas IPv6, a newer standard, permits addresses 128 bits long. Many operating systems, including Windows Vista and later, support IPv6. Firewall supports both standards.
- Port numbers for local and remote computers — A computer sends and receives services using numbered ports. For example, HTTP service typically is available on port 80, and FTP services on port 21. Port numbers range from 0–65535.
- Process ID (PID) — A unique identifier for the process associated with a connection's traffic.
- Timestamp — The time of the last incoming or outgoing packet associated with the connection.
- Timeout — The time limit (in seconds) after which the entry is removed from the table if no packet matching the connection is received. The timeout for TCP connections is enforced only when the connection isn't established.
- Direction — The direction (incoming or outgoing) of the traffic that triggered the entry. After a connection is established, bidirectional traffic is allowed even with unidirectional rules, provided the entry matches the connection's parameters in the state table.

Considerations for the state table

- If firewall rule sets change, all active connections are checked against the new rule set. If no matching rule is found, the connection entry is discarded from the state table.
- If an adapter obtains a new IP address, the firewall recognizes the new configuration and drops all state table entries with invalid local IP addresses.
- When the process ends, all entries in the state table associated with a process are deleted.

Stateful protocol tracking

Firewall monitors and handles connections based on the protocol.

Protocol	How protocol is handled
UDP	A UDP connection is added to the state table when a matching static rule is found and the action from the rule is Allow. Generic UDP connections remain in the state table as long as the connection isn't idle longer than the specified timeout period. These connections carry application-level protocols unknown to the firewall.
ICMPv4/v6	Only ICMP Echo Request and Echo Reply message types are tracked. In contrast to the reliable connection-oriented TCP protocol, UDP and ICMPv4/v6 are less reliable, connectionless protocols. To secure these protocols, the firewall considers generic UDP and ICMP connections to be virtual connections. Virtual connections are held only as long as the connection isn't idle longer than the timeout period specified for the connection. Set the timeout for virtual connections in the Firewall Options settings.
TCP	TCP protocol works on the S3-way handshake. **1** The client computer initiates a new connection, sending a packet to its target with a SYN bit set. **2** The target responds by sending a packet to the client with a SYN-ACK bit set. **3** The client responds by sending a packet with an ACK bit set and the stateful connection is established. All outgoing packets are allowed, but only incoming packets that are part of the established connection are allowed. An exception is when the firewall first queries the TCP protocol and adds all pre-existing connections that match the static rules. Pre-existing connections without a matching static rule are blocked. The TCP connection timeout is enforced only when the connection isn't established. A second or forced TCP timeout applies to established TCP connections only. A registry setting controls this timeout, which has a default value of one hour. Every four minutes the firewall queries the TCP stack and discards connections that TCP doesn't report.
DNS	Query/response matching makes sure that DNS responses are only allowed: • To the local port that originated the query • From a remote IP address that has been queried during the UDP Virtual Connection Timeout interval Incoming DNS responses are allowed if: • The connection in the state table hasn't expired. • The response comes from the same remote IP address and port where the request was sent.
DHCP	Query/response matching makes sure that return packets are allowed only for legitimate queries. Thus incoming DHCP responses are allowed if: • The connection in the state table hasn't expired. • The response transaction ID matches the one from the request.

Using trusted networks to allow traffic automatically

Trusted networks are IP addresses, IP address ranges, and subnets that your organization considers safe.

Defining a network as trusted causes Firewall to create an internal bi-directional Allow rule with remote network criteria set to the trusted network. Any traffic to and from the trusted networks is allowed.

Using trusted executables and applications to reduce false positives

Trusted executables are executables that have no known vulnerabilities and are considered safe.

Configuring a trusted executable creates a bi-directional Allow rule for that executable at the top of the Firewall rules list.

Maintaining a list of safe executables for a system reduces or eliminates most false positives. For example, when you run a backup application, many false positive events might be triggered. To avoid triggering false positives, make the backup application a trusted executable.

A trusted executable is susceptible to common vulnerabilities, such as buffer overflow and illegal use. Therefore, Firewall still monitors trusted executables and triggers events to prevent exploits.

The Firewall Catalog contains executables and applications. Executables in the catalog can be associated with a container application. You can add executables and applications from the catalog to your list of trusted executables. Once defined, you can reference the executables in rules and groups.

Using the Firewall Catalog to reference existing items

The Firewall Catalog simplifies the process of creating firewall rules and groups by enabling you to reference existing rules, groups, network options, applications, executables, and locations.

When referencing a catalog item, you create a dependent link between it and a firewall rule or group. Any change to the item in the catalog also changes the item wherever it is used. You can remove the dependency by breaking the link.

The Firewall Catalog, found in McAfee ePO under Policy, includes previously added firewall rule and firewall group items. You can add items individually to the catalog by linking items from firewall and rule groups. You can also import items from XML-format exports of Rules policies.

Firewall protocols

Firewall protection works at several layers of the network architecture, where different criteria are used to restrict network traffic. This architecture is built on the TCP/IP suite.

Link layer

The link layer protocol describes the media access control (MAC) method, and some minor error-detection facilities.

Ethernet LAN (802.3), wireless Wi-Fi (802.11x), and virtual LAN (VPN) are in this layer. Both firewall rules and groups distinguish between wired, wireless, and virtual links.

Network layer

The network layer protocols define whole-network addressing schemes, routing, and network control schemes.

It also supports arbitrary non-IP protocols, but can't detect any network or transport layer parameters for them. At best, this layer allows the administrator to block or allow these network layer protocols. The numbers associated with the non-IP protocols are based on the Ethernet numbers defined by the Internet Assigned Numbers Authority (IANA).

Firewall offers full support for IPv4 and IPv6 on Microsoft Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows 8, and Windows 10.

Transport layers

IP can be used as the network protocol for many transport protocols. In practice, four are commonly used:

TCP

TCP is a connection-oriented, reliable transport protocol. It guarantees that the data contained in network packets are delivered reliably, and in order. It also controls the rate at which data is received and transmitted. This control requires a certain amount of overhead, and makes the timing of TCP operations unpredictable when network conditions are suboptimal.

TCP is the transport layer for most application protocols. HTTP, FTP, SMTP, RDP, SSH, POP, and IMAP all use TCP.

TCP multiplexes between application-layer protocols using the concept of "ports." Each TCP packet contains a source and destination port number, from 0–65535. Usually, the server end of a TCP connection listens for connections on a fixed port.

Ports 0–1023 are reserved as "well-known ports." The IANA assigns numbers in this range to protocols. Most operating systems require a process to have special permissions to listen on one of these ports.

Firewall rules are constructed to block certain ports and allow others, limiting the activities that can occur on the network.

UDP

User Datagram Protocol is a connectionless best-effort transport protocol. It makes no guarantees about reliability or packet order, and lacks flow control features. In practice, it has some desirable properties for certain classes of traffic.

UDP is often used as a transport protocol for performance-critical applications. It is also used in real-time multi-media applications. A dropped packet causes only a momentary glitch in the datastream and is more acceptable than a stream that stops to wait for retransmission. IP telephony and videoconferencing software often uses UDP, as do some multi-player video games.

The UDP multiplexing scheme is identical to that of TCP: each datagram has a source and destination port, ranging from 0–65535.

ICMP

Internet Control Message Protocol, version 4 (ICMPv4) and version 6 (ICMPv6), is used as an out-of-band communication channel between IP hosts. It is useful in troubleshooting, and needed for the proper function of an IP network, because it is the error reporting mechanism.

IPv4 and IPv6 have separate, unrelated ICMP protocol variants. ICMPv4 is often called simply ICMP.

ICMPv6 is important in an IPv6 network. It is used for several critical tasks, such as neighbor discovery (which ARP handles in an IPv4 network). Users are discouraged from blocking ICMPv6 traffic if IPv6 is supported on their network.

Instead of port numbers, both versions of ICMP define message types. *Echo Request* and *Echo Reply* are used for ping. *Destination Unreachable* messages indicate routing failures. ICMP also implements a Traceroute facility, though UDP and TCP can also be used for this purpose.

Other transport protocols

IP supports over a hundred other transport protocols, but most are rarely used. The complete list of IANA-recognized protocols is at least minimally supported. Rules can be created to block or allow traffic over all IP transport protocols. But, the firewall doesn't support any multiplexing mechanism that these protocols might use.

Several are used to overlay other types of networks on top of an IP network (network tunneling). Some of these protocols (notably GRE, AH, and ESP) are used for IP encryption and VPNs.

See Protocol numbers for the IP protocol numbers.

Common unsupported protocols

There are several network protocols that Firewall doesn't support. Traffic belonging to these protocols, usually with an unparsable EtherType, is always blocked or always allowed, depending on the selection in the Options settings.

How Adaptive mode affects Firewall

In Adaptive mode, Firewall automatically allows all traffic that doesn't match an existing Block rule, and creates dynamic Allow rules for that non-matching traffic.

When Firewall is running normally, it continually monitors the network traffic that a computer sends and receives. Firewall allows or blocks traffic based on the rules. If the traffic can't be matched against an existing rule, it is automatically blocked.

You can create an explicit Allow rule for any traffic. For security reasons, incoming pings (ICMP traffic) are blocked in Adaptive mode unless an explicit Allow rule is created for it. Incoming traffic to a port that isn't open on the host is also blocked unless an explicit Allow rule is created for the traffic. For example, if the telnet service isn't running, incoming TCP traffic to port 23 (telnet) is blocked automatically.

Firewall displays the rules created on client systems through Adaptive mode, and enables you to save and migrate these administrative rules.

Stateful filtering

When Adaptive mode is applied with the stateful firewall, the filtering process creates a rule to handle the incoming packet:

1. The firewall compares an incoming packet against entries in the state table and finds no match, then examines the static rule list and finds no match.
2. No entry is made in the state table, but if the packet is a TCP packet, it is put in a pending list. If not, the packet is dropped.
3. If new rules are permitted, a unidirectional static Allow rule is created. If the packet is a TCP packet, an entry is made in the state table.
4. If a new rule isn't permitted, the packet is dropped.

FAQ — McAfee GTI and Firewall

Here are answers to frequently asked questions.

Firewall Options settings in the **McAfee GTI Network Reputation** section enable you to block incoming and outgoing traffic from a network connection based on McAfee GTI reputation.

What is McAfee GTI?

McAfee GTI is a global Internet reputation intelligence system that determines what is good and bad behavior on the Internet. McAfee GTI uses real-time analysis of worldwide behavioral and sending patterns for email, web activity, malware, and system-to-system behavior. Using data obtained from the analysis, McAfee GTI dynamically calculates reputation scores that represent the level of risk to your network when you visit a webpage. The result is a database of reputation scores for IP addresses, domains, specific messages, URLs, and images.

For frequently asked questions about McAfee GTI, see KB53735.

How does McAfee GTI work with Firewall?

Firewall uses the value of the **Incoming network-reputation threshold** and **Outgoing network-reputation threshold** options to create internal rules on the client system. If incoming or outgoing traffic matches these rules, Firewall queries McAfee GTI for the reputation of the source or destination IP address. Firewall uses this information to determine whether to block incoming or outgoing traffic.

- **Treat match as intrusion** — Treats traffic that matches the McAfee GTI block threshold setting as an *intrusion* and displays an alert.
- **Log matching traffic** — Treats traffic that matches the McAfee GTI block threshold setting as a *detection* and displays an event in the **Event Log** on the Endpoint Security Client. Firewall also sends an event to McAfee ePO.

What do you mean by "reputation"?

For each IP address on the Internet, McAfee GTI calculates a reputation value. McAfee GTI bases the value on sending or hosting behavior and various environmental data collected from customers and partners about the state of Internet threat landscape. The reputation is expressed in four classes, based on our analysis:

- **Do not block** (minimal risk) — This is a legitimate source or destination of content/traffic.
- **High Risk** — This source/destination sends or hosts potentially malicious content/traffic that McAfee considers risky.
- **Medium Risk** — This source/destination shows behavior that McAfee considers suspicious. Any content/traffic from the site requires special scrutiny.
- **Unverified** — This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is needed.

Does McAfee GTI introduce latency? How much?

When McAfee GTI is contacted to do a reputation lookup, some latency is inevitable. McAfee does everything possible to minimize this latency. McAfee GTI:

- Checks reputations only when the options are selected.
- Uses an intelligent caching architecture. In normal network usage patterns, the cache resolves most wanted connections without a live reputation query.

If Firewall can't reach the McAfee GTI servers, does traffic stop?

If McAfee GTI is not reachable, you can configure Firewall to either block all traffic by default or allow traffic unless firewall rules specifically block it.

Firewall additions to McAfee ePO

This managed product extends your ability to secure your network with these features and enhancements.

You must have appropriate permissions to access most features.

McAfee ePO feature	Addition
Actions	Actions that you can perform from the System Tree or use to customize automatic responses.
Client tasks	Client tasks that you can use to automate management and maintenance on client systems.
Dashboards	Dashboards and monitors that you can use to keep watch on your environment.
Events and responses	• Events for which you can configure automatic responses. • Event groups and event types that you can use to customize automatic responses.
Permissions sets	Endpoint Security Firewall, Endpoint Security Firewall Catalog, and Endpoint Security Firewall Client permission categories, available in all existing permission sets.
Policies	Options and Rules policy categories in the Endpoint Security Firewall product group.

McAfee ePO feature	Addition
Queries and reports	• Default queries that you can use to run reports. • Custom property groups based on managed system properties that you can use to build your own queries and reports.
Server tasks	Adds a predefined server task to the Server Tasks list in Automation.
Server tasks	Endpoint Security Firewall Property Translator server task that translates Firewall client rules in the client properties stored in the McAfee ePO database, and adds them to the Firewall Client Rules page.
Firewall Client Rules	Firewall Client Rules under Reporting displays firewall client rules created on a client system to allow activity that a firewall rules blocks.
Firewall Catalog	Firewall Catalog under Policy displays items in the Firewall Catalog and lets you edit, create, delete, and export them.

For information about these features, see the McAfee ePO documentation.

See also

Events, responses, and Firewall on page 43
Dashboards, monitors, and Firewall on page 39
Permission sets and Firewall on page 24
Policies and Firewall on page 27
Queries, reports, and Firewall on page 40
Server tasks and Firewall on page 41
Client tasks and Firewall on page 25

Permission sets and Firewall

Permission sets define rights for managed product functionality in McAfee ePO.

Firewall adds the Endpoint Security Firewall, Endpoint Security Firewall Client, and Endpoint Security Firewall Query permission groups to each permission set.

Permission groups define the access rights to the features. McAfee ePO grants all permissions for all products and features to global administrators. Administrators then assign user roles to existing permission sets or create new permission sets.

Your managed product adds these permission controls to McAfee ePO.

Permissions sets	Default permissions
Executive Reviewer Endpoint Security Firewall, Endpoint Security Firewall Client, and Endpoint Security Firewall Query	No permissions
Global Reviewer Endpoint Security Firewall, Endpoint Security Firewall Client, and Endpoint Security Firewall Query	No permissions
Group Admin Endpoint Security Firewall, Endpoint Security Firewall Client, and Endpoint Security Firewall Query	No permissions
Group Reviewer Endpoint Security Firewall, Endpoint Security Firewall Client, and Endpoint Security Firewall Query	No permissions

This managed product grants No Permissions by default.

Permissions must be granted for users to access or use permission-controlled features.

Table 1-1 Permissions required per feature

Feature	Required permissions
Automatic Responses	Automatic Responses, Event Notifications, Client Events
Client events and client rules	Systems, System Tree access, Threat Event Log
Dashboards and monitors	Dashboards, Queries
Policies	Endpoint Security Firewall: Firewall in the Endpoint Security Firewall permission group
Queries	Queries & Reports
Server tasks	Server Tasks
System Tree	Systems, System Tree access
Threat Event Log	Systems, System Tree access, Threat Event Log

For information about managing permission sets, see the McAfee ePO documentation.

Client tasks and Firewall

Automate management or maintenance on managed systems using client tasks.

Depending on your permissions, you can use default client tasks as is, edit them, or create new client tasks using McAfee ePO.

Firewall leverages the following default McAfee Agent client tasks.

Table 1-2 McAfee Agent default client tasks

Client task	Description
Product Deployment	Deploys McAfee products to client systems.
Product Update	Updates content files, engines, and all McAfee products automatically.

For information about client tasks and the Client Task Catalog, see the McAfee ePO documentation.

2 Configuring Firewall

Contents

- *Policies and Firewall*
- *Enable and configure Firewall*
- *Block DNS traffic*
- *Define networks to use in rules and groups*
- *Configure trusted executables*
- *Manage firewall rules and groups*
- *Use the Firewall Catalog*
- *Tuning Firewall*

Policies and Firewall

Policies let you configure, apply, and enforce settings for managed systems in your environment.

Policies are collections of settings that you create, configure, and apply, then enforce. Most policy settings correspond to settings that you configure in the Endpoint Security Client. Other policy settings are the primary interface for configuring the software.

Your managed product adds these categories to the Policy Catalog. The available settings vary in each category.

Table 2-1 Firewall categories

Category	Description
Options	Specifies options for the Firewall, including: • Turns on or off firewall protection. • Applies Adaptive mode for tuning. • Defines the domain name servers (DNS) to block. • Defines networks and trusted executables to use in rules and groups.
Rules	Specifies firewall rules, and groups of rules, that define what traffic is allowed and what is blocked. When DNS blocking is enabled in Options, this policy dynamically adds a rule near the top of the firewall rules list. This rule prevents resolving the IP address of the specified domain.

In addition, Firewall adds the Firewall Catalog. The Firewall Catalog simplifies firewall rule and group creation by enabling you to reference existing rules, groups, network options, applications, executables, and locations.

Customizing policies

Each policy category includes default policies.

You can use default policies as is, edit the My Default default policies, or create new policies.

Table 2-2 Firewall default policies

Policy	Description
McAfee Default	Defines the default policy that takes effect if no other policy is applied. You can duplicate, but not delete or change, this policy.
McAfee Default Server	Defines the default server Rules policy, which allows all server default services, such as Windows AD Authentication, Web/FTP, and mail servers, to accept client service requests. You can duplicate, but not delete or change, this policy.
My Default	Defines default settings for the category.

User-based policies

User-based polices (UBP) enable policies to be defined and enforced using McAfee ePO policy assignment rules with an LDAP server. These assignment rules are enforced on the client system for the user at log-on, regardless of the McAfee ePO group.

User-based polices are enforced when a user with a matching assignment rule logs on to the client system on the console. System-based polices (SBP) are enforced when two or more users are logged on to a system. Policy assignment rules take precedence over polices defined in the System Tree.

The user policy supersedes the system policy. All system policies apply and any user-based policy overrides the system policy.

Policy assignment rules are enforced only if the user logs on as the **interactive** user. The system policy, rather than the user policy, is enforced if the user logs on:

- With a **runas** command
- To a remote desktop or terminal service where the user's logon is not set to interactive

For more information about user-based policies and policy assignment rules, see the McAfee ePO Help.

Comparing policies

You can compare all policy settings for the module using the Policy Comparison feature in McAfee ePO. For information, see the McAfee ePO Help.

For information about policies and the Policy Catalog, see the McAfee ePO documentation.

See also

Use the Firewall Catalog on page 33
Enable and configure Firewall on page 28
Block DNS traffic on page 29
Configure trusted executables on page 30
Define networks to use in rules and groups on page 29
Manage firewall rules and groups on page 31

Enable and configure Firewall

Configure settings for Firewall to turn firewall protection on and off, enable Adaptive mode, and configure other Firewall options.

Task

1 Select **Menu** | **Policy** | **Policy Catalog**, then select **Endpoint Security Firewall** from the **Product** list.

2 From the **Category** list, select **Options**.

3 Click the name of an editable policy.

4 Select **Enable Firewall** to make the firewall active and change its options.

Host Intrusion Prevention 8.0 can be installed on the same system as Endpoint Security version 10.6. If McAfee Host IPS Firewall is installed and enabled, Endpoint Security Firewall is disabled even if enabled in the settings.

5 Click **Show Advanced**.

6 Configure settings on the page, then click **Save**.

See also

FAQ — McAfee GTI and Firewall on page 22
Block DNS traffic on page 29
Define networks to use in rules and groups on page 29
Configure trusted executables on page 30

Block DNS traffic

To refine firewall protection, create a list of FQDNs to block. Firewall blocks connections to the IP addresses resolving to the domain names.

Task

1 Select **Menu** | **Policy** | **Policy Catalog**, then select **Endpoint Security Firewall** from the **Product** list.

2 From the **Category** list, select **Options**.

3 Click the name of an editable policy.

4 Under **DNS Blocking**, click **Add**.

5 Enter the comma-separated FQDN of the domains to block, then click **Save**.

You can use the ***** and **?** wildcards. For example, *domain.com.

Duplicate entries are removed automatically.

6 Click **Save**.

See also

Enable and configure Firewall on page 28

Define networks to use in rules and groups

Define network addresses, subnets, or ranges to use in rules and groups, or define networks as *trusted*.

Task

1 Select **Menu** | **Policy** | **Policy Catalog**, then select **Endpoint Security Firewall** from the **Product** list.

2 From the **Category** list, select **Options**.

3 Click the name of an editable policy.

4 Click **Show Advanced**.

5 Under **Defined Networks**, click **Add Defined Network**.

6 Select the type from **Address type**, then enter a trusted IP address, subnet, or range in the **Address** field.

7 Select either **Trusted** or **Not trusted** from the drop-down menu.

- **Trusted** — Firewall allows all traffic to and from trusted networks.
- **Not trusted** — Defines networks for use in rules and groups. You can use networks defined as not trusted for the local or remote network criteria in a rule or group.

  Defining a network as not trusted adds those networks as exceptions to McAfee GTI rules in Firewall.

8 Click **Save**.

See also

Using trusted networks to allow traffic automatically on page 20
Use the Firewall Catalog on page 33
Enable and configure Firewall on page 28

Configure trusted executables

Define or edit the list of trusted executables that are considered safe for your environment.

Task

1 Select **Menu** | **Policy** | **Policy Catalog**, then select **Endpoint Security Firewall** from the **Product** list.

2 From the **Category** list, select **Options**.

3 Click **Show Advanced**.

4 Under **Trusted Executables**, click **Add**.

5 Configure the executable properties, then click **Save**.

6 Click **Save**.

Tasks

- *Get the signer distinguished name from McAfee ePO to use to specify trusted executables* on page 30
  The signer distinguished name (SDN) is required when you enable a digital signature check and add only files signed by a specified process signer.

See also

Using trusted executables and applications to reduce false positives on page 20
Use the Firewall Catalog on page 33

Get the signer distinguished name from McAfee ePO to use to specify trusted executables

The signer distinguished name (SDN) is required when you enable a digital signature check and add only files signed by a specified process signer.

Task

1 Select **Menu** | **Reporting** | **Threat Event Log**.

2 Click the Endpoint Security event to display details.

3 From **Endpoint Security**, select **Source Process Signer**, copy the details.

4 When specifying trusted executables, paste the **Source Process Signer** details to the **Signed by** field.

For example, the SDN required format is:

C=US, S=CALIFORNIA, L=MOUNTAIN VIEW, O=MOZILLA CORPORATION, OU=RELEASE ENGINEERING, CN=MOZILLA CORPORATION

Manage firewall rules and groups

Use a firewall rule group to create a set of rules with a single purpose.

For example, configure a group with rules to allow VPN connection. Groups appear in the rule list preceded by an arrow, which you can click to show or hide the rules in the group.

Task

1 Select **Menu** | **Policy** | **Policy Catalog**, then select **Endpoint Security Firewall** from the **Product** list.

2 From the **Category** list, select **Rules**.

3 Click the name of an editable policy.

4 Do any of the following.

To...	Steps
Add a firewall rule	Click **Add Rule** or **Add Rule from Catalog**.
Add a firewall group	Click **Add Group** or **Add Group from Catalog**.
Change an existing rule or group	Select the rule or group and click **Edit** under **Actions**.
Make a copy of a rule or group	Select the rule or group and click **Duplicate**.
Delete a rule or group	Select the rule or group and click **Delete**.
Add an item to the Firewall Catalog	Click **Add to Catalog** under **Actions**.
Move an item up or down in the list	Select the rule or group and click **Move Up** or **Move Down**.
Export all rule and group information in the policy to an XML file	Click **Export**. You can then import this file into the Firewall Catalog or to another policy.

5 Click **Save**.

Tasks

- *Create connection isolation groups* on page 32
  A connection isolation firewall rule group instructs Firewall to process only traffic that matches the defined connection type and group criteria.
- *Create timed groups* on page 33
  Create Firewall timed groups to restrict Internet access until a client system connects over a VPN.

See also

Wildcards in firewall rules on page 32
Create connection isolation groups on page 32
Define networks to use in rules and groups on page 29
Configure trusted executables on page 30
Use the Firewall Catalog on page 33

Wildcards in firewall rules

You can use wildcards to represent characters for some values in firewall rules. Wildcards match zero or more characters so that you don't have to specify an entire path or value, or set of values.

Firewall supports wildcards in blocked domains and executable paths only.

For paths of files, registry keys, executables, and URLs, use these wildcards.

Registry key paths for firewall group locations don't recognize wildcard values.

?	Question mark	A single character.
*	Asterisk	Multiple characters, excluding slash (/) and backslash (\). Use this character to match the root-level contents of a folder with no subfolders.
**	Double asterisk	Multiple characters, including slash (/) and backslash (\).
|	Pipe	Wildcard escape.

For the double asterisk (**), the escape is |*|*.

For values that normally don't contain path information with slashes, use these wildcards.

?	Question mark	A single character.
*	Asterisk	Multiple characters, including slash (/) and backslash (\).
|	Pipe	Wildcard escape.

Create connection isolation groups

A connection isolation firewall rule group instructs Firewall to process only traffic that matches the defined connection type and group criteria.

Task

1. Select **Menu** | **Policy** | **Policy Catalog**, then select **Endpoint Security Firewall** from the **Product** list.
2. From the **Category** list, select **Rules**.
3. Click the name of an editable policy.
4. On the **Rules** policy page, click **Add Group** or **Add Group from Catalog**.
5. Under **Description**, specify options for the group.
6. Under **Location**, select **Enable location awareness** and **Enable connection isolation**. Then, select the location criteria for matching.
7. Under **Networks**, for **Connection types**, select the type of connection (**Wired**, **Wireless**, or **Virtual**) to apply to the rules in this group.

   Settings for **Transport** and **Executables** aren't available for connection isolation groups.
8. Click **Save**.
9. Create new rules within this group, or move existing rules into it from the firewall rule list or the Firewall Catalog.
10. Click **Save**.

See also

Firewall rule groups and connection isolation on page 14
Making groups location-aware on page 13

Create timed groups

Create Firewall timed groups to restrict Internet access until a client system connects over a VPN.

Task

1 Select **Menu** | **Policy** | **Policy Catalog**, then select **Endpoint Security Firewall** from the **Product** list.

2 From the **Category** list, select **Rules**.

3 Click the name of an editable policy.

4 Create a Firewall group with default settings that allow Internet connectivity.

For example, allow port 80 HTTP traffic.

5 In the **Schedule** section, select how to enable the group.

- **Enable schedule** — Specifies a start and end time for the group to be enabled.
- **Disable schedule and enable the group from the McAfee system tray icon** — Allows users to enable the group from the McAfee system tray icon and keeps the group enabled for the specified number of minutes.

  If you allow users to manage the timed group, you can optionally require that they provide a justification before enabling the group.

6 Create a connection isolation group that matches the VPN network to allow needed traffic.

Best practice: To allow outbound traffic from only the connection isolation group on the client system, don't place any Firewall rules below this group.

7 Click **Save**.

See also

Using timed groups on page 13

Use the Firewall Catalog

The Firewall Catalog is a repository of items that you can use with Firewall. For example, you can define rule and groups to add to multiple policies or networks and applications to add to firewall rules.

You can add an item to or from the catalog while creating a firewall rule or group. When you add an item, you create a link between the item and the catalog — items inherits properties from items in the catalog. To break the inheritance and create a new independent item, click **Break Catalog Inheritance**.

Task

1 Select **Menu** | **Policy** | **Firewall Catalog**.

2 From the **Item type** drop-down list, select a catalog item.

3 Do any of the following on the Firewall Catalog page.

To...	Steps
Filter for an item.	Click **Show Filter Items**, enter filter criteria, then click **Set Filter**. Click **Clear** to return to the default view.
Change the view of items.	Select **Options**	**Choose Columns**, change the columns, then click **Save**.
Change an item.	Click the **Edit** link associated with the item.
Create and add an item to the catalog.	Click **New**.
Delete an existing item.	Click the **Delete** link associated with the item. If you delete an item with a dependent link, a new, independent copy of that item is placed with the linking rule or group.
Export a single item.	Click the **Export** link associated with the item.
Export all items of the catalog type.	Click **Export** in the upper-right corner of the page, then name and save the XML file.
Import items of the catalog type.	Click **Import** in the upper-right corner of the page, then locate and open the XML file with catalog data.

See also

Using the Firewall Catalog to reference existing items on page 20

Tuning Firewall

Tuning involves balancing intrusion prevention protection with access to required information and applications per group type. Tuning involves finding the right balance between protecting your environment from intrusions and allowing access to required information and applications.

During Firewall deployment, identify a few distinct usage profiles and create policies for them. The best way to achieve this goal is to set up a test deployment, then begin reducing the number of false positives and generated events. This process is called *tuning*.

You can reduce the number of false positives by creating:

- **Exception rules** — Mechanisms for overriding a setting in specific circumstances.
- **Trusted executables** — Executable processes that ignore all firewall rules.
- **Firewall rules** — Determine whether traffic is permissible, and block packet reception or allow or block packet transmission.

Automatic tuning using Adaptive mode

Automatic tuning removes the need to constantly monitor all events and activities for all users.

To help tune protection settings, place clients in *Adaptive mode*. In Adaptive mode, client rules are created automatically to allow legitimate activity. After client rules are created, analyze them and decide which to convert to server-mandated policies.

Often in a large organization, avoiding disruption to business takes priority over security concerns. For example, you might need to install new applications on some computers, and you might not have the time or resources to immediately tune them. You can place specific computers in Adaptive mode to profile a newly installed application, and forward the resulting client rules to the management server. You can then promote these client rules to an existing or new policy and apply the policy to other computers to handle the new software.

Systems in Adaptive mode have virtually no protection. For this reason, use Adaptive mode only for tuning an environment, then turn it off to tighten the system's protection.

1. Apply Adaptive mode for Firewall policies.
2. Review the lists of client rules.
3. Promote appropriate client rules to administrative policy rules.
4. After at least a week, turn off Adaptive mode.
5. Monitor the test group for a few days to make sure that the policy settings are appropriate and offer the wanted protection.
6. Repeat this process with each group of similar computers.

Manual tuning

Manual tuning requires direct monitoring of events and client rules that are created.

1. Monitor events for false positives and create exceptions or trusted applications to prevent these events from reoccurring.
2. Monitor network traffic and define trusted networks to allow appropriate network traffic.
3. Monitor the effects of the new exceptions, trusted executables, and trusted networks.
4. If these rules prevent false positives, keep network traffic to a minimum, and allow legitimate activity, add them to the policy.
5. Apply the new policy to a set of computers and monitor the results.
6. Repeat this process with each group of similar computers.

Using Adaptive mode to create client rules automatically

Place systems in Adaptive mode so that Firewall can create client rules automatically without user interaction.

Best practice: Enable Adaptive mode temporarily on a few systems only while tuning Firewall. Enabling this mode might generate many client rules, which the McAfee ePO server must process, negatively affecting performance.

Adaptive mode analyzes events first for the most malicious attacks. If the activity is considered regular and needed for business, Firewall creates client rules. By enabling Adaptive mode on representative clients, you can create a tuning configuration. You can then convert client rules to server-mandated policies. When tuning is complete, turn off Adaptive mode to tighten the system's protection.

Run client systems in Adaptive mode for at least a week. In this time, client systems encounter all normal activity, including scheduled activity, such as backups or script processing. As activity occurs, Firewall generates events and creates rules.

See also

FAQ — Adaptive mode on page 36

FAQ — Adaptive mode

Here are answers to frequently asked questions.

Adaptive mode is a setting that you can apply to Firewall when testing new rollouts. This mode enables the client system to automatically create rules that allow activity while preserving minimum protection against vulnerabilities. The following questions and answers can help you use this feature.

How do you turn on Adaptive mode?

Enable this option in the Firewall Options settings and apply this policy to the client.

How does Adaptive mode work with Firewall?

Adaptive mode creates rules on the client system that allow network packets not covered by existing firewall rules. Firewall client rules are created on a per-process basis. The processes associated with firewall client rules are based on path, file description, digital signature, and MD5 hash.

When is a rule not created automatically with Adaptive mode?

- There is no application associated with the packet when examined in the client activity log. Some of the most common examples include:
  - Incoming requests for services that aren't running, such as FTP or telnet
  - Incoming ICMP, such as an echo request
  - Incoming or outgoing ICMP on Windows Vista
  - TCP packets to port 139 (NetBIOS SSN) or 445 (MSDS), which might be required for Windows file sharing
  - IPsec packets associated with VPN client solutions
- There is already a rule that blocks or allows the packet.
- The applied Rules policy has a location-aware group with connection isolation enabled and the following is true:
  - An active NIC matches the group.
  - The packet is sent or received on a NIC that doesn't match the group.
- The packet isn't TCP, UDP, or ICMP.
- More than one user is logged on to the system, or no user is logged on to the system.

Analyzing client data

To tune your deployment, analyze client rules created in Adaptive mode, and events triggered by activity on the clients.

- From client rules data, you can:
  - See which rules are being created.
  - Aggregate rules to find the most common rules.
  - Move the rules directly to a policy for application to other clients.
- From event data, you can see firewall intrusions and McAfee® Global Threat Intelligence™ (McAfee GTI) block events. Drill down to the details of an event to see:
  - Which process triggered the event
  - When the event was generated
  - Which client generated the event

Use McAfee ePO queries and reports to gather information about client rules. Use the Threat Event Log to view all threat events that McAfee ePO receives from managed systems. Analyze the event and take the appropriate action to tune the Firewall deployment to provide better response to attacks.

See also

Manage Firewall client rules on page 37

Manage Firewall client rules

Tune and tighten security by reviewing Firewall client rules and moving them to a Rules policy.

Firewall client rules are created manually on a client or automatically in Adaptive mode.

For information about server tasks, see the McAfee ePO documentation.

Task

1. From the System Tree, click **Wake Up Agents**.

   The agent wake-up call collects the Firewall client properties, including client rules, from the client.

2. Select **Menu** | **Automation** | **Server Tasks**, then run the **Endpoint Security Firewall Property Translator** server task.

   When enabled, the Endpoint Security Firewall Property Translator task runs automatically every 60 minutes, scans the client properties for Firewall client rules, and adds them to the Firewall Client Rules page.

3. Select **Menu** | **Reporting** | **Firewall Client Rules**.

4. In the System Tree, select a group to display its details.

5. Review the client rules to determine which rules to promote to a **Rules** policy.

6. Move rules to a policy by selecting rules, clicking **New Firewall Rule**, then indicating the policy to move the rules to.

7. In the Firewall **Options** policy, deselect these options:

   - **Enable Adaptive mode**
   - **Retain existing user-added rules and Adaptive mode rules when this policy is enforced**

8. Enforce the updated **Options** and **Rules** policies.

The rules from the **Rules** policy replace the client rules that were created on the client system.

See also

Server tasks and Firewall on page 41

3 Monitoring Firewall activity with McAfee ePO

Contents

- *Dashboards, monitors, and Firewall*
- *Queries, reports, and Firewall*
- *Server tasks and Firewall*
- *Events, responses, and Firewall*

Dashboards, monitors, and Firewall

Keep watch on the status of your managed systems and any threats in your environment using your customizable dashboard.

Dashboards are collections of *monitors* that track activity in your McAfee ePO environment.

Default dashboards and monitors

The module provides default dashboards and monitors. Depending on your permissions, you can use them as is, modify them to add or remove monitors, or create custom dashboards using McAfee ePO.

Firewall includes the following default dashboard.

Table 3-1 Firewall dashboards and monitors

Dashboard	Monitor	Description
Endpoint Security: Firewall Dashboard		Status of Endpoint Security Firewall.
	Endpoint Security Firewall: Events from McAfee GTI	Number of Firewall intrusion or detection events from McAfee GTI.
	Endpoint Security Firewall: Events in the last 24 hours	Number of intrusion or detection events from Firewall in the last 24 hours.

In addition to the default Firewall dashboard, Firewall contributes monitors to several Common dashboards.

Table 3-2 Common dashboards and Firewall monitors

Dashboard	Monitor	Description
Endpoint Security: Compliance Status		Whether a technology is enabled (protection status).
	Endpoint Security Firewall: Compliance Status	Number of systems with Firewall protection enabled or disabled.
Endpoint Security: Installation Status		Whether a module is installed.
	Endpoint Security Firewall: Hotfixes Installed	Number of systems with Firewall hotfixes installed, including hotfix version numbers.

Custom dashboards

Depending on your permissions, you can create custom dashboards and add monitors using default Endpoint Security queries.

For information about dashboards, see the McAfee ePO documentation.

See also

Permission sets and Firewall on page 24

Queries, reports, and Firewall

Use queries to retrieve detailed information about the status of your managed systems and any threats in your environment. You can export, download, or combine queries into reports, and use queries as dashboard monitors.

Queries are questions that you ask McAfee ePO, which returns answers as charts and tables. *Reports* enable you to package one or more queries into a single PDF document, for access outside of McAfee ePO.

Similar information is available by accessing activity logs from the Endpoint Security Client on individual systems.

You can view query data only for resources where you have permissions. For example, if your permissions grant access to a specific System Tree location, your queries return data only for that location.

Default queries

The module adds default queries to McAfee Groups. Depending on your permissions, you can use them as is, modify them, or create custom queries from events and properties in the McAfee ePO database.

- Endpoint Security Firewall: Firewall Client Rules By Process
- Endpoint Security Firewall: Firewall Client Rules By Process/Port Range
- Endpoint Security Firewall: Firewall Client Rules By Process/User
- Endpoint Security Firewall: Firewall Client Rules By Protocol/System Name
- Endpoint Security Firewall: Compliance Status
- Endpoint Security Firewall: Count of Firewall Client Rules
- Endpoint Security Firewall: Errors
- Endpoint Security Firewall: Events from McAfee GTI in the last 6 months
- Endpoint Security Firewall: Events in the last 24 hours
- Endpoint Security Firewall: Hotfixes Installed
- Endpoint Security Firewall: Intrusion events in the last 24 hours
- Endpoint Security Firewall: Status
- Endpoint Security Firewall: Traffic block events in the last 24 hours

Custom queries

The module adds default properties to the Endpoint Security feature group. You can use these properties to create custom queries.

Feature Group	Result Type	Property (Column)	Property (Column)
Endpoint Security	Endpoint Security Firewall Systems	Additional Compliance Status Reason	Firewall Patch Version
		Compliance Status Reason	Firewall Rules Policy
		Endpoint Security Firewall client version	Firewall Service Running
		Endpoint Security Firewall Compliance Status	Firewall Status
		Firewall Adaptive Mode Status	Firewall Trusted Applications Policy
		Firewall Fault	Firewall Trusted Networks Policy
		Firewall Hotfixes	Install Directory (32 bit version)
		Firewall Last Policy Enforcement	Install Directory (64 bit version)
		Firewall License Status	Language
		Firewall Mode	Product Version
		Firewall Name Client UI Policy	Reboot Required
		Firewall Options Policy	
	Endpoint Security Firewall Properties	Language (Endpoint Security Firewall)	Product Version (Endpoint Security Firewall)
	Endpoint Security Platform Systems	Firewall Debug Logging Enabled	Firewall Event Filter Level

For information about queries and reports, see the McAfee ePO documentation.

See also

Permission sets and Firewall on page 24

Server tasks and Firewall

Automate server management or maintenance using server tasks.

Server tasks are scheduled management or maintenance tasks that you run on your McAfee ePO server. Server tasks enable you to schedule and automate repetitive tasks. Use server tasks to monitor your server and software.

Depending on your permissions, you can use default server tasks as is, edit them, or create new server tasks using McAfee ePO.

Default server tasks

Your managed product provides these server tasks. You can use server tasks as is, edit them, or create new ones.

Server task	Description
Endpoint Security Firewall Property Translator	Translates Firewall client rules in the client properties stored in the McAfee ePO database, and adds them to the Firewall Client Rules page. When enabled, the Endpoint Security Firewall Property Translator task runs automatically every 60 minutes and requires no user interaction. To see immediate feedback from actions on the client, run an agent wake-up call, then run this server task manually.

Custom server tasks

To create a custom server task, run the Server Task Builder and select from the **Action** drop-down list.

Server tasks	Description
Run Query	Runs default queries at a specified time and schedule.
Purge Threat Event Log	Purges threat event logs based on a query.
Export Policies	Downloads an XML file that contains the associated policy.
Export Queries	Creates a query output file that can be saved or emailed.
Roll Up Data	Rolls up system or event data from multiple servers at the same time. Select **Endpoint Security Firewall Rolled-Up Systems** or **Endpoint Security Rolled-Up Threat Events** for the **Data type**.

For information about server tasks, see the McAfee ePO documentation.

See also

Events, responses, and Firewall on page 43
Roll up system or event data for Endpoint Security on page 42
Permission sets and Firewall on page 24

Roll up system or event data for Endpoint Security

Compile data from multiple servers at the same time using McAfee ePO Roll Up Data server tasks.

Task

1. Select **Menu** | **Automation** | **Server Tasks**, then click **New Task**.
2. On the Description page, type a name and description for the task, and select whether to enable it, then click **Next**.
3. Click **Actions**, then select **Roll Up Data**.
4. From the **Roll up data from:** drop-down list, select one:
   - **All registered servers**
   - **Selected registered servers** — Select the servers you want, then click **OK**.
5. To roll up system data:
   a. For the Data Type, select **Managed Systems**.
   b. Select the **Additional Types: Configure** link, and select the Endpoint Security types you want to include.
6. To roll up event data:
   a. Click the **+** button at the end of the table heading to add another data type, then select **Threat Events**.
   b. Click **Additional Types: Configure**, and select the Endpoint Security types you want to include.

7 Schedule the task, then click **Next**.

8 Review the settings, then click **Save**.

Events, responses, and Firewall

Configure **Automatic Responses** to react to threat events.

The Threat Event Log is a log file of all threat events that McAfee ePO receives from managed systems.

In McAfee ePO, you can define which events are forwarded to the McAfee ePO server. To display the complete list of events in McAfee ePO, select **Menu** | **Configuration** | **Server Settings**, select **Event Filtering**, then click **Edit**.

Set up a Purge Threat Event Log server task to purge the Threat Event Log periodically.

For information about Automatic Responses and working with the Threat Event Log, see the McAfee ePO Help.

See also

Server tasks and Firewall on page 41

4 Using Firewall on a client system

Contents

- *Enable and disable Firewall from the McAfee system tray icon*
- *Enable or view Firewall timed groups from the McAfee system tray icon*

Enable and disable Firewall from the McAfee system tray icon

Depending on how settings are configured, you can enable and disable Firewall from the McAfee system tray icon.

These options might not be available, depending on how the settings are configured.

Task

- Right-click the McAfee system tray icon and select **Disable Endpoint Security Firewall** an option from the **Quick Settings** menu.

  When Firewall is enabled, the option is **Disable Endpoint Security Firewall**.

  Depending on settings, you might be prompted to provide your administrator with a reason for disabling Firewall.

Enable or view Firewall timed groups from the McAfee system tray icon

Enable, disable, or view Firewall timed groups from the McAfee system tray icon.

These options might not be available, depending on how the settings are configured.

Task

- Right-click the McAfee system tray icon and select an option from the **Quick Settings** menu.
  - **Enable Firewall Timed Groups** — Enables timed groups for a set amount of time to allow access to the Internet before rules restricting access are applied. When timed groups are enabled, the option is **Disable Firewall Timed Groups**.

    Each time you select this option, you reset the time for the groups.

    Depending on settings, you might be prompted to provide the administrator with a reason for enabling timed groups.

  - **View Firewall Timed Groups** — Displays the names of the timed groups and the amount of time remaining for each group to be active.

See also

Using timed groups on page 13
Create timed groups on a client system on page 53

5 Managing Firewall on a client system

Contents

- *Enable and configure Firewall on a client system*
- *Block DNS traffic on a client system*
- *Define networks to use in rules and groups on a client system*
- *Configure trusted executables on a client system*
- *Create and manage Firewall rules and groups on a client system*

Enable and configure Firewall on a client system

Configure settings for Firewall to turn firewall protection on and off, enable Adaptive mode, and configure other Firewall options.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Select **Enable Firewall** to make the firewall active and change its options.

Host Intrusion Prevention 8.0 can be installed on the same system as Endpoint Security version 10.6. If McAfee Host IPS Firewall is installed and enabled, Endpoint Security Firewall is disabled even if enabled in the settings.

4 Click **Show Advanced**.

5 Configure settings on the page, then click **Apply**.

See also

Enable and disable Firewall from the McAfee system tray icon on page 45
Block DNS traffic on a client system on page 48
Define networks to use in rules and groups on a client system on page 48
Configure trusted executables on a client system on page 49

Block DNS traffic on a client system

To refine firewall protection, create a list of FQDNs to block. Firewall blocks connections to the IP addresses resolving to the domain names.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Under **DNS Blocking**, click **Add**.

4 Enter the FQDN of the domains to block, then click **Save**.

You can use the ***** and **?** wildcards. For example, *domain.com.

Duplicate entries are removed automatically.

5 Click **Apply**.

See also

Enable and configure Firewall on a client system on page 47

Define networks to use in rules and groups on a client system

Define network addresses, subnets, or ranges to use in rules and groups, or define networks as *trusted*.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Click **Show Advanced**.

4 From **Defined Networks**, do any of the following:

To...	Steps
Define a network.	Click **Add** and enter the details for the trusted network. From the drop-down list: • Select **Yes** to define the network as trusted. Firewall allows all traffic to and from trusted networks. • Select **No** to define the network for use in rules and groups. You can use networks defined as not trusted for the local or remote network criteria in a rule or group. Defining a network as not trusted adds those networks as exceptions to McAfee GTI rules in Firewall.
Change a network definition.	For each column, double-click the item and enter the new information.
Delete a network.	Select a row, then click **Delete**.

5 Click **Apply**.

See also

Enable and configure Firewall on a client system on page 47

Configure trusted executables on a client system

Define or edit the list of trusted executables that are considered safe for your environment.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Click **Show Advanced**.

4 From **Trusted Executables**, do any of the following:

To...	Steps
Define a new trusted executable.	Click **Add** and enter the details for the trusted executable.
Change an executable definition.	For each column, double-click the item and enter the new information.
Delete an executable.	Select a row, then click **Delete**.

5 Click **Apply**.

Tasks

- *Get the signer distinguished name to specify trusted executables on a client system* on page 50
  The signer distinguished name (SDN) is required when you enable a digital signature check and add only files signed by a specified process signer.

See also

Enable and configure Firewall on a client system on page 47

Get the signer distinguished name to specify trusted executables on a client system

The signer distinguished name (SDN) is required when you enable a digital signature check and add only files signed by a specified process signer.

Task

1 Right-click an executable and select **Properties**.

2 On the **Digital Signatures** tab, select a signer and click **Details**.

3 On the **General** tab, click **View Certificate**.

4 On the **Details** tab, select the **Subject** field.

The SDN appears.

For example, Firefox has this SDN:

CN = Mozilla Corporation

OU = Release Engineering

O = Mozilla Corporation

L = Mountain View

S = California

C = US

The SDN fields appear in reverse order from the required format.

5 Copy the contents of the **Subject** field to a temporary location.

6 Edit the information to reverse the order of the elements, remove line breaks, and separate the elements with commas.

For example, the SDN required format is:

C=US, S=CALIFORNIA, L=MOUNTAIN VIEW, O=MOZILLA CORPORATION, OU=RELEASE ENGINEERING, CN=MOZILLA CORPORATION

7 When specifying trusted executables, paste the certificate details to the **Signed by** field.

Create and manage Firewall rules and groups on a client system

Use a firewall rule group to create a set of rules with a single purpose.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Firewall processes rules from top to bottom, regardless of whether they are in groups. The groups and rules appear in priority order in the **Firewall Rules** table. You can't sort rules by column.

Rules and groups that you configure from the Endpoint Security Client might be overwritten when the administrator deploys an updated policy.

Task

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Use these tasks to manage firewall rules and groups.

To do this...	Follow these steps
View the rules in a firewall group.	Click >.
Collapse a firewall group.	Click v.
Change an existing rule. You can change rules in the **User added** group only.	1 Expand the **User added** group. 2 Double-click the rule. 3 Change the rule settings. 4 Click **OK** to save your changes.
View an existing rule in any group.	1 Expand the group. 2 Select the rule to view its details in the bottom pane.
Create a rule.	1 Click **Add Rule**. 2 Specify the rule settings. 3 Click **OK** to save your changes. The rule appears at the end of the **User added** group.
Create copies of rules.	1 Select the rule or rules and click **Duplicate**. Copied rules appear with the same name at the end of the **User added** group. 2 Change the rules to change the name and settings.
Delete rules. You can delete rules from the **User added** and **Adaptive** groups only.	1 Expand the group. 2 Select the rule or rules and click **Delete**.

To do this...	Follow these steps
Create a group.	1 Click **Add Group**. 2 Specify the group settings. 3 Click **OK** to save your changes. The group appears in the **User added** group.
Move rules and groups in and between groups. You can move rules and groups in the **User added** group only.	To move elements: 1 Select elements to move. The grip appears to the left of elements that can be moved. 2 Drag and drop the elements to the new location. A blue line appears between elements where you can drop the dragged elements.

4 Click **Apply**.

Tasks

- *Create connection isolation groups on a client system* on page 52
  A connection isolation firewall rule group instructs Firewall to process only traffic that matches the defined connection type and group criteria.
- *Create timed groups on a client system* on page 53
  Create Firewall timed groups to restrict Internet access until a client system connects over a VPN.

See also

Create connection isolation groups on a client system on page 52
Create timed groups on a client system on page 53

Create connection isolation groups on a client system

A connection isolation firewall rule group instructs Firewall to process only traffic that matches the defined connection type and group criteria.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Under **RULES**, click **Add Group**.

4 Under **Description**, specify options for the group.

5 Under **Location**, select **Enable location awareness** and **Enable connection isolation**. Then, select the location criteria for matching.

6 Under **Networks**, for **Connection types**, select the type of connection (**Wired**, **Wireless**, or **Virtual**) to apply to the rules in this group.

Settings for **Transport** and **Executables** aren't available for connection isolation groups.

7 Click **OK**.

8 Create new rules within this group, or move existing rules into it from the firewall rule list.

9 Click **Apply**.

See also

Firewall rule groups and connection isolation on page 14
How firewall rule groups work on page 11

Create timed groups on a client system

Create Firewall timed groups to restrict Internet access until a client system connects over a VPN.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu , select **Settings**, then click **Firewall** on the **Settings** page.

3 Create a Firewall group with default settings that allow Internet connectivity.

For example, allow port 80 HTTP traffic.

4 In the **Schedule** section, select how to enable the group.

- **Enable schedule** — Specifies a start and end time for the group to be enabled.
- **Disable schedule and enable the group from the McAfee system tray icon** — Allows users to enable the group from the McAfee system tray icon and keeps the group enabled for the specified number of minutes.

  If you allow users to manage the timed group, you can optionally require that they provide a justification before enabling the group.

5 Click **OK** to save your changes.

6 Create a connection isolation group that matches the VPN network to allow needed traffic.

Best practice: To allow outbound traffic from only the connection isolation group on the client system, don't place any Firewall rules below this group.

7 Click **Apply**.

See also

How firewall rule groups work on page 11
Using timed groups on page 13

6 Monitoring Firewall activity on a client system

Contents

- *Check the Event Log for recent activity*
- *Firewall log file names and locations*

Check the Event Log for recent activity

The Event Log in the Endpoint Security Client displays a record of events that occur on the McAfee-protected system.

Task

1. Open the Endpoint Security Client.
2. Click **Event Log** on the left side of the page.

   The page shows any events that Endpoint Security has logged on the system in the last 30 days.

   If the Endpoint Security Client can't reach the Event Manager, it displays a communication error message. In this case, reboot the system to view the Event Log.
3. Select an event from the top pane to display the details in the bottom pane.

   To change the relative sizes of the panes, click and drag the sash widget between the panes.
4. On the **Event Log** page, sort, search, filter, or reload events.
5. Navigate in the Event Log.

   By default, the Event Log displays 20 events per page. To display more events per page, select an option from the **Events per page** drop-down list.

Firewall log file names and locations

The activity, error, and debug log files record events that occur on systems with Endpoint Security enabled.

All activity and debug log files are stored in the following default location:

%ProgramData%\McAfee\Endpoint Security\Logs

Each module, feature, or technology places activity or debug logging in a separate file. All modules place error logging in one file, EndpointSecurityPlatform_Errors.log.

Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection.

Table 6-1 Log files

Module	File name	Notes
Firewall	Firewall_Activity.log	
	Firewall_Debug.log	
	FirewallEventMonitor.log	Logs blocked and allowed traffic events, if configured.
Common	EndpointSecurityPlatform_Errors.log	Contains error logs for all modules.

By default, installation log files are stored here:

TEMP\McAfeeLogs, which is the Windows system TEMP folder.