McAfee®

Application Note

Configuring McAfee® Firewall Enterprise for McAfee Web Protection Service

This document explains how to configure McAfee Firewall Enterprise (Sidewinder®) to redirect all web traffic to Web Protection Service.

Web Protection Service supports explicit and transparent proxy options. For more information about each, including advantages and disadvantages, refer to the ***McAfee Web Protection Service Product Guide****.*

In this document ...

Overview

There are a variety of ways to redirect your web traffic to McAfee® Web Protection Service. This document explains the transparent proxy option and provides instructions for configuring McAfee Firewall Enterprise *(Sidewinder®)* to redirect port 80 traffic.

Note: You must use McAfee Firewall Enterprise version 7.0.1 or later.

For more information about the redirection options, including advantages and disadvantages, refer to the *McAfee Web Protection Service Product Guide*, available from the Support tab of the Web Protection Service application.

Configuring McAfee Firewall Enterprise

This procedure explains how to configure McAfee Firewall Enterprise to transparently send web traffic to the Web Protection Service Data Center (proxy.securewebbrowsing.com) over port 80.

Note: For end users, cookie-based authentication (login pages) is supported.

Set up the Application Defenses

Begin by setting up the HTTP and HTTPS Application Defenses.

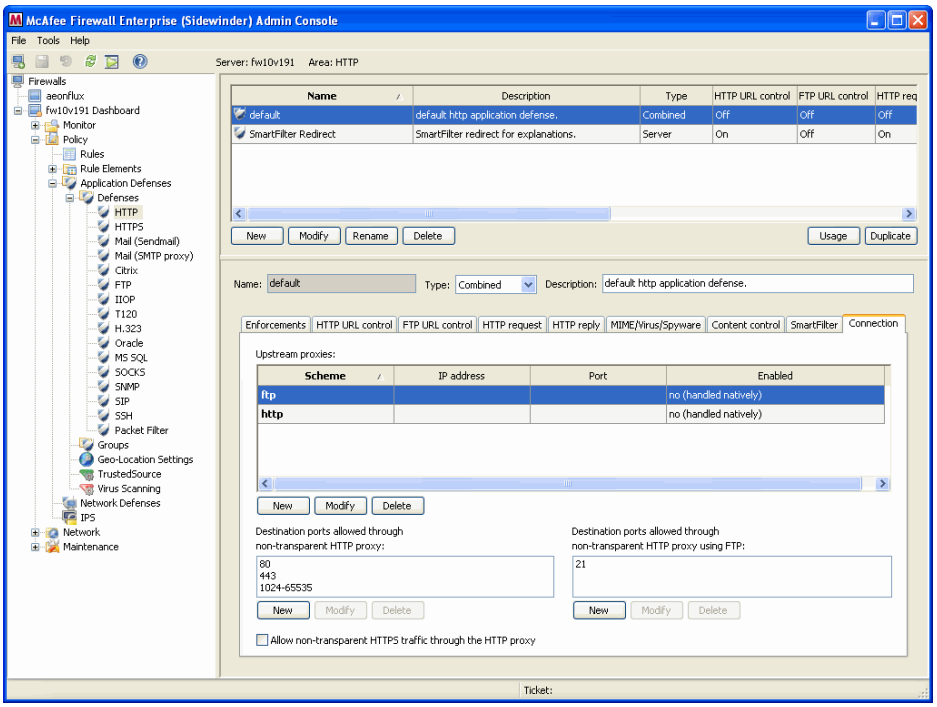
Set up the HTTP Application Defense

Follow these steps to set up the HTTP Application Defense.

1. Select **Policy > Application Defenses > Defenses**.
2. Select **HTTP**; the default Application Defense appears highlighted. (If you do not want to use the default, create a new Application Defense and select it.)

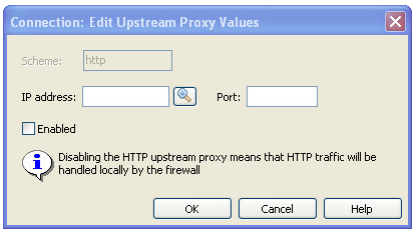
3 In the bottom pane, click the **Connection** tab (Figure 1).

Figure 1 Modify HTTP Application Defense window



4 In the Upstream proxies section, select **http**, then click **Modify**. The Edit Upstream Proxy Values window appears (Figure 2).

Figure 2 Edit Upstream Proxy Values window



5 Complete the following information:

a IP address

- Type **proxy.securewebbrowsing.com** and click the **DNS Lookup** icon.
- Once the result displays, click **OK** to automatically update the IP address field.

Note: Alternately, you can determine the IP address from the Web Protection Service application. Click the **Support** tab **> Run Proxy Test**. Copy the IP address for your best result and paste it in the IP address field.

b Port – Type **80**.

c Enabled – Select this checkbox.You may need to wait a few minutes for this change to take effect.

6 Click **OK**, and save your changes.

Set up the HTTPS Application Defense

Follow these steps to set up the HTTPS Application Defense.

1 Select **Policy > Application Defenses > Defenses**.

2 Select **HTTPS**; the default Application Defense appears highlighted. (If you do not want to use the default, create a new Application Defense and select it.)

3 In the bottom pane, click the **Connection** tab (similar to Figure 1).

4 In the Upstream proxies section, select **http** (there is no HTTPS option in this step).

5 Click **Modify**. The Edit Upstream Proxy Values window appears (Figure 2).

6 Complete the following:

a IP address

- Type **proxy.securewebbrowsing.com** and click the **DNS Lookup** icon.
- Once the result displays, click **OK** to automatically update the IP address field.

Note: Alternately, you can determine the IP address from the Web Protection Service application. Click the **Support** tab **> Run Proxy Test**. Copy the IP address for your best result and paste it in the IP address field.

b Port – Type **80**.

c Enabled – Select this checkbox.

7 Click **OK**, and save your changes.

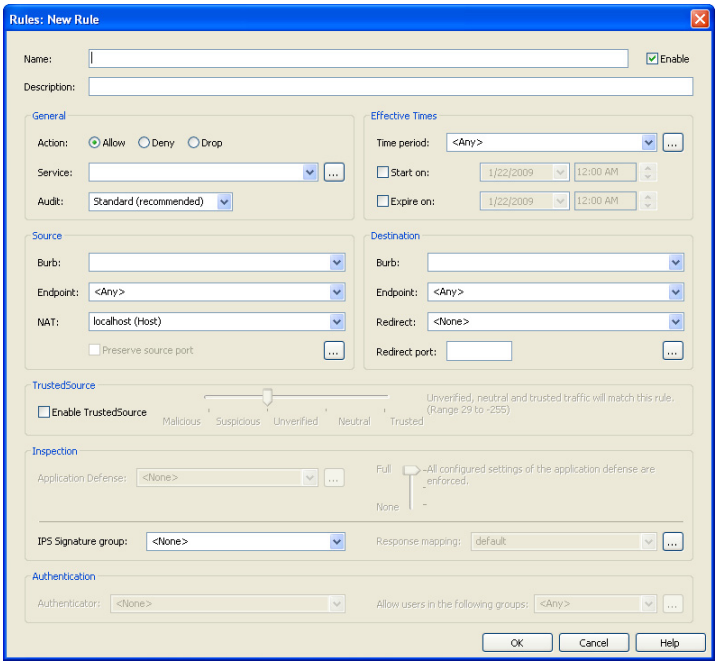
Create the HTTP and HTTPS rules

Complete these steps to create an HTTP rule, then repeat the steps to create an HTTPS rule.

1 Select **Policy > Rules**.

2 Click **New Rule** [+]. The New Rule window appears (Figure 3).

Figure 3 New Rule window



3 Complete the following information:

a **Name** – Type a name for the rule.

b **Description** – Type a description for the rule.

c **Action** – In the General section, select **Allow**.

d **Service** – In the General section, use the drop-down arrow to select one of the following:

- If you are creating the HTTP rule, select **http (HTTP Proxy)**.
- If you are creating the HTTPS rule, select **https (HTTPS Proxy)**.

e **Burb (Source)** – In the Source section, use the drop-down arrow to select **internal**.

Note: If your users (web clients) are located in a different burb, select that burb instead.

f **Burb (Destination)** – In the Destination section, use the drop-down arrow to select **external**.

g **Application Defense** – In the Inspection section, use the drop-down arrow to select one of the following:

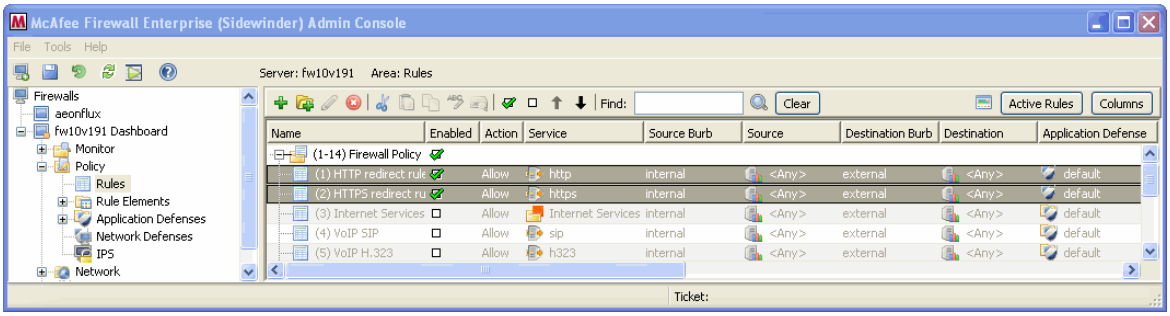
- If you are creating the HTTP rule, select the HTTP Application Defense you set up earlier (*Set up the HTTP Application Defense* on page 3).
- If you are creating the HTTPS rule, select the HTTPS Application Defense you set up earlier (*Set up the HTTPS Application Defense* on page 5).

4 Click **OK**.

5 Prioritize the rule as follows (Figure 4):

- **HTTP** – If you are prioritizing the HTTP rule, select and drag it to the top of the rules list.
- **HTTPS** – If you are prioritizing the HTTPS rule, select and drag it to the top of the rules list under the HTTP rule.

Figure 4 Prioritized rules



6 Save your changes.

Verify the configuration

Based on your service, select one of the following methods to make sure your traffic is being properly filtered:

- **Web Protection Service *with* malware protection** – Verify using either of the following procedures.
- **Web Protection Service *without* malware protection** – Follow the *Verify using Web Protection Service* procedure.

Verify using EICAR

[Conditional] If your Web Protection Service includes malware protection, follow these steps (if not, see *Verify using Web Protection Service*):

1. Navigate to www.eicar.org.
2. Click **Anti-Malware Testfile** at the top right portion of the window.
3. Scroll to the bottom of the window. Under the **Download area using the standard protocol http** banner, click any of the links (Figure 5).

Figure 5 EICAR links

4. Click **Run**.
5. An alert indicates that your web traffic is now being redirected through Web Protection Service (Figure 6).

Figure 6 Malware block

Note: If you used HTTPS to download the EICAR file, you will not receive an alert in this instance.

Verify using Web Protection Service

To verify your configuration:

1. In Web Protection Service, click the **Allow & Block Lists** tab.
2. From the Block List toolbar, click **Add URL**. The New URL dialog appears.
   a. In the URL field, type **www.example.com**.
   b. Click **Save**.
3. Open a browser and try to browse to **www.example.com**. An alert indicates that your web traffic is now being redirected through Web Protection Service (Figure 6).

   Note: You may need to wait a few minutes for this change to take effect.

700-2046-00

McAfee®