

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*.

COPYRIGHT

Copyright © 2009 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

In this document ...

Overview Configuring McAfee Firewall Enterprise

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

McAfee Firewall Enterprise (Sidewin	nder) Admin Console						
File Tools Help							
🖳 📄 🦈 🎜 💽 🔞 🤅 Se	erver: fw10v191 Area: HTTP						
Firewalls							
aeonflux	Name	 Description 	tion	Туре	HTTP URL control	FTP URL control	HTTP req
with the management of the man	💝 default	default http application def	ense.	Combined	Off	Off	Off
B Policy	😺 SmartFilter Redirect	SmartFilter redirect for exp	lanations.	Server	On	Off	On
Rules							
😑 🤯 Application Defenses							
🖃 🌄 Defenses							
	<						>
HTTPS	New Modify Rename	Delete				Usage	Duplicate
Mail (Sendmail)							
Citrix							
	Name: default	Type: Combined 🗸	Description: default	http application	defense.		
😺 T120	(m. 4)					a set Care	a ablan
	Enforcements HTTP URL control	FTP URL control HTTP reque	ist HTTP reply MIME/	Virus/Spyware	Content control	omartFilter Con	lection
Oracle	Lindvoom province						
MS SQL	opsoleani proxies.						_
	Scheme 🛆	IP address	Port		Enabled		
SIP	ftp			no (han	dled natively)		
	http			no (han	dled natively)		
							_
🦉 Groups							
Geo-Location Settings							
TrustedSource	<						>
Virus Scanning							
IPS	New Modify De	lete					
E A Network	Destination ports allowed throu	jh	Destination por	ts allowed thro	ugh		
🗉 🙀 Maintenance	non-transparent HTTP proxy:		non-transparen	it HTTP proxy u	ising FTP:		
	80		21				
	443						
	1024-65535						
	New Modify De	lete	New	Modify D	elete		
	Allow non-transparent HTTP	5 traffic through the HTTP prox;	/				
		ті	cket:				

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



Connection: Edit Upstream Proxy Values	×
Scheme: http	
IP address: Or Port:	
Enabled	
Disabling the HTTP upstream proxy means that HTTP traffic will be handled locally by the firewall	
OK Cancel Help	

- **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

Rules: New R	ule		×
Name: Description:	[🗹 Enable
General Action:	⊙ Allow O Deny O Drop	Effective Times Time period: 	v
Service: Audit:	Standard (recommended)	Start on: 1/22/2009 12:00 AM Expire on: 1/22/2009 12:00 AM	
Source Burb:		Destination Burb: Endepilte Endepilt	V
NAT:	localhost (Host)	Redirect: Redirect port:	•
TrustedSour	rce TrustedSource Maliclous Suspicious Unverified Neut	Unverified, neutral and trusted traffic will match , (Range 29 to -255) ral Trusted	this rule.
- Inspection - Application	Defense: Vione> V	Ful	e are
IPS Signati	ure group: None>	Response mapping: default	
Authenticati	ion tor: <th>Allow users in the following groups: <Allow users in the following groups: Allow users in the following groups: Allow users in the following groups: allow users in the following groups: allow users in the following groups: https://www.sersin.com"/>https://wwww.sersin.comAllow</th> <th>Help</th>	Allow users in the following groups: < Allow users in the following groups: Allow users in the following groups: Allow users in the following groups: allow users in the following groups: allow users in the following groups: https://www.sersin.com"/>https://wwww.sersin.comAllow	Help

- **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

McAfee Firewall Enterprise (S		inder) Admin Console							
File Tools Help									
🖳 📄 🦻 🎜 💽 🔞	9	ierver: fw10v191 Area: Rule	s						
Firewalls	^	+ 📴 🖉 🔕 🐇 🗋 🛙	-) *9 🗐 I 🛛	🕈 🗖 🏦 🖡 🖡 Find:		🔍 Clear		📰 🛛 Activ	e Rules Columns
🖃 🔜 fw10v191 Dashboard		Name	Enabled Actio	n Service	Source Burb	Source	Destination Burb	Destination	Application Defense
🖼 📑 Monitor		- 🕀 📑 (1-14) Firewall Policy	4						~
Policy		📃 🔚 (1) HTTP redirect rule	😽 Allow	😰 http	internal	🕼 <any></any>	external	🕼 <any></any>	🌍 default 🔤
Rules		📃 🔤 (2) HTTPS redirect ru	😪 🛛 Allow	💿 https	internal	🕼 <any></any>	external	🕼 <any></any>	🍯 default 📃
Application Defenses		(3) Internet Services	Allow	🛛 📑 Internet Services	internal	🕼 <any></any>	external	🚯 <any></any>	🤪 default
Network Defenses		(4) VoIP SIP	Allow	🚯 sip	internal	🕼 <any></any>	external	🚯 <any></any>	🤪 default
IPS	-		Allow	🚯 h323	internal	🕼 <any></any>	external	🕼 <any></any>	🧳 default 🛛 💌
🗈 🙋 Network	~	<							>
					Ticket:				

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

Download area using the standard protocol http				
eicar.com	eicar.com.txt	eicar com.zip	eicarcom2.zip	
68 Bytes	68 Bytes	184 Bytes	308 Bytes	

- 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

McAfee [.]	Web Protection Service					
Request Blocked by McAfee Web Protection Service						
	URL	http://blockedsite.com/fullUrl				
	Reputation	127 (Malicious)				
	Categories	Spyware/Adware				
	Reason Blocked by defined policy.					
	If you think this page was blocked in error, please notify your administrator. Copyright 2008-2009 McAfee, Inc. All Rights Reserved.					

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.

