

FortiADC Layer 7 Virtual Server with Content Rewriting Deployment Guide

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



Tuesday, January 8, 2019

L7VS content rewriting Deployment Guide

First Edition

TABLE OF CONTENTS

Change Log	4
Overview	5
Rewrite URL if URL and source IP match the configuration	9
Add new header to HTTP request if the HTTP request URL matches with the configuration	12

Change Log

Date	Change Description
1/8/2019	Initial release

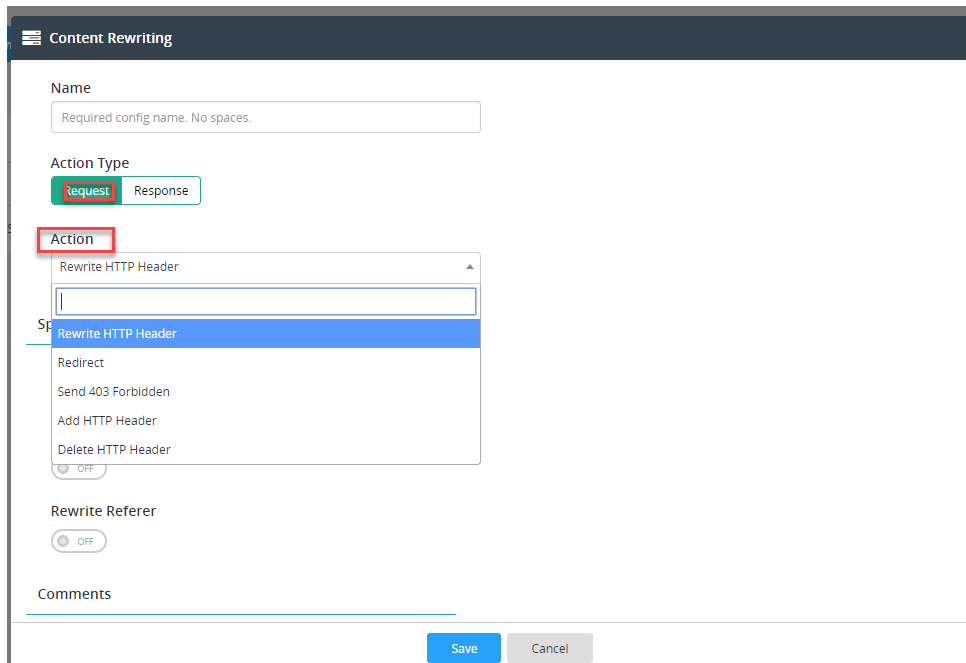
Overview

Layer 7 HTTP(S) Virtual server with content rewriting will allow you to rewrite HTTP request/response. This may be useful for:

- Redirecting HTTP to HTTPS
- External to internal URL translation
- Other security reasons

Rewrite action for HTTP requests include the following:

- Redirect
- Send 403 Forbidden
- Rewrite HTTP Header (including rewrite Host/URL/Referer)
- Add HTTP Header
- Delete HTTP Header



Rewrite action for HTTP response includes the following:

- Rewrite HTTP location
- Add HTTP header
- Delete HTTP header

Content Rewriting

Name

Action Type

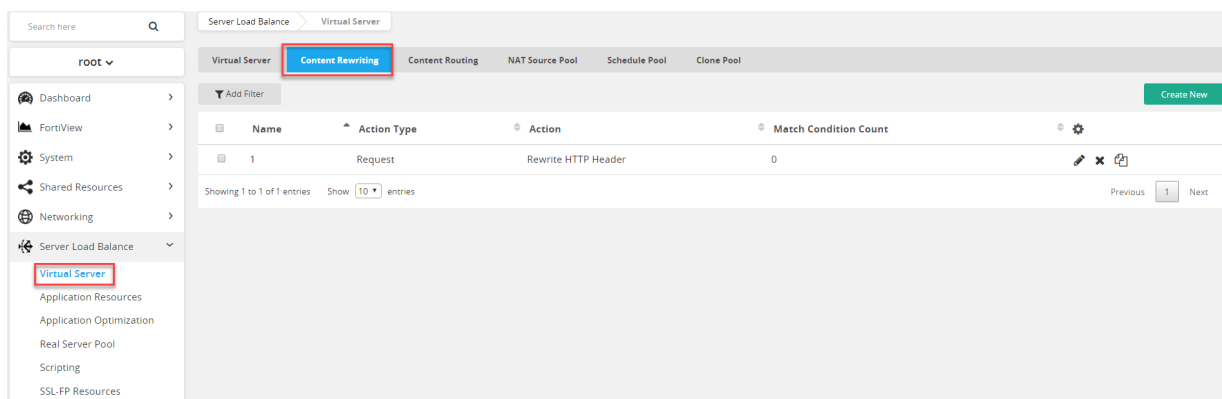
Action

Rewrite HTTP Location
 Add HTTP Header
 Delete HTTP Header

Example

To configure a content rewrite rule:

1. Go to Server Load Balance > Virtual Server
2. Click the Content Rewriting tab



3. Click Create New to display the configuration editor.
4. For each different action it will display the specific object to be rewritten.

Content Rewriting

Name

Action Type
 Request Response

Action

Specifics

Rewrite Host
 OFF

Rewrite URL
 OFF

Rewrite Referer
 OFF

Comments

5. After you save the content rewrite, you can edit it to set up the match condition. The match conditions include the following:

- HTTP Host header
- HTTP Request URL
- HTTP Referer Header
- Source IP Address
- HTTP Location Header

Content Rewriting

Name

Action Type
 Request Response

Action

Specifics

Rewrite Host
 OFF

Rewrite URL
 OFF

Rewrite Referrer
 OFF

Comments

Match Condition (Empty Match Condition will match anything)

ID	Object	Type	Content	Reverse	
No data available in table					

Showing 0 to 0 of 0 entries Show entries [Previous](#) [Next](#)

Content Rewriting

Edit Match Condition (Empty Match Condition will match anything)

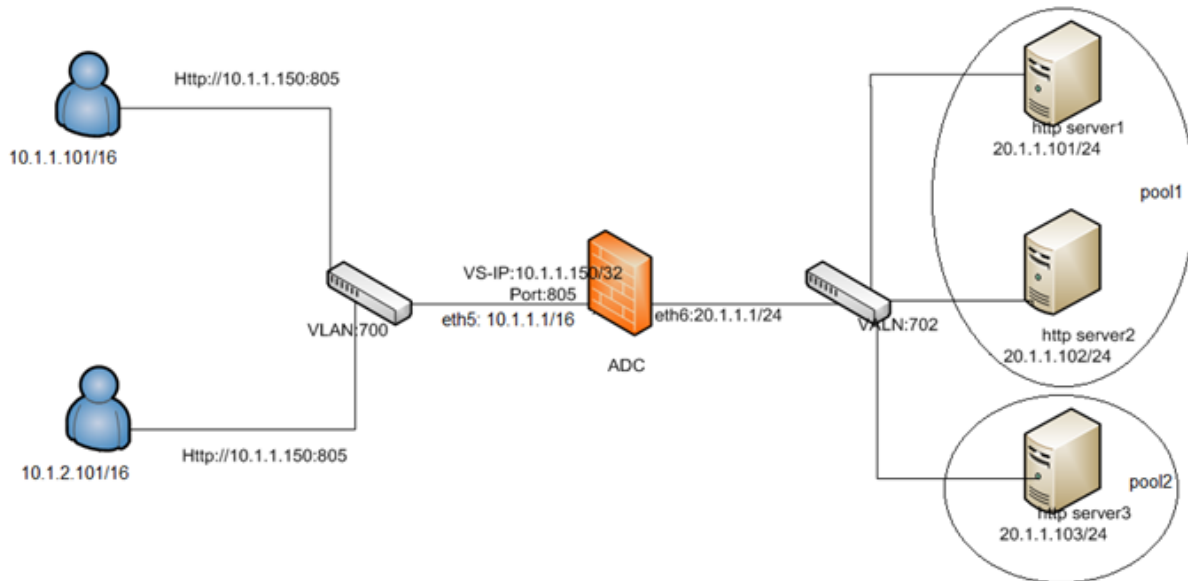
Object

- HTTP Host Header
- HTTP Request URL
- HTTP Referrer Header
- Source IP Address
- HTTP Location Header

Reverse
 OFF

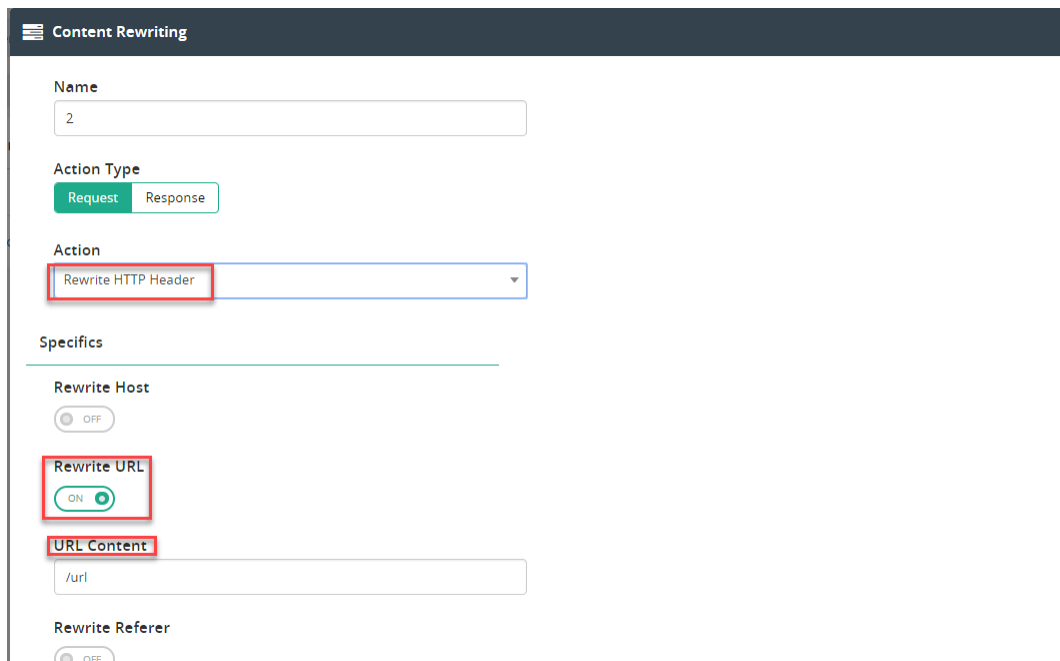
Ignore Case
 ON

Rewrite URL if URL and source IP match the configuration



Note: HTTP request from 10.1.2.0/24 to access index.html will rewrite to index.php

1. Select proper action when configuring content rewriting, and set the rewrite URL



2. Set match condition

Content Rewriting

Rewrite Referer

 OFF

Comments

Match Condition (Empty Match Condition will match anything)

Add Filter
Create New

ID	Object	Type	Content	Reverse	
1	Source IP Address	-	10.1.2.0/24	Disable	
2	HTTP Request URL	String	/index.html	Disable	

Showing 1 to 2 of 2 entries
Show entries
Previous Next

3. Bind content rewrite with Layer 7-HTTP Virtual Server

Rewrite URL if URL and source IP match the configuration

Virtual Server

Basic | General | Security | Application Optimization | Monitoring

Name
L7-HTTP-VS

Type
Layer 7 | Layer 4 | Layer 2

Status
Disable | **Enable** | Maintain

Address Type
IPv4 | IPv6

Traffic Group
default

Specifics

Schedule Pool
OFF

Content Routing
OFF

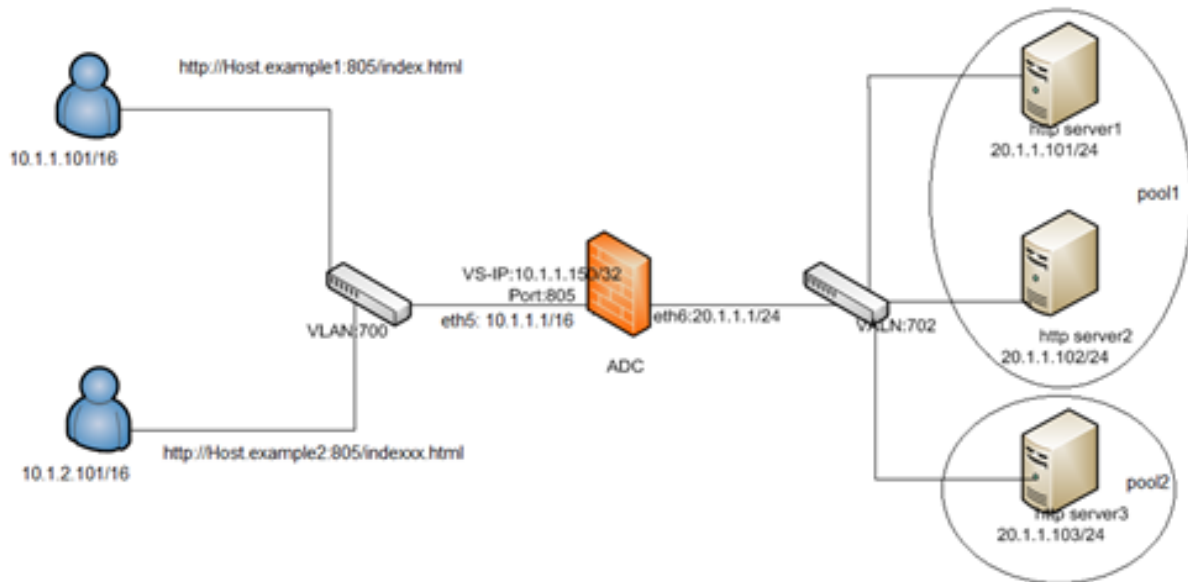
Content Rewriting
ON

Content Rewriting List

Selected Items	Available Items
rewrite-request	Create New

Add new header to HTTP request if the HTTP request URL matches with the configuration

Topology description



Note: HTTP request with Host Hosts.example2 will add test-header

1. Select proper action when configuring content rewrite, and set specifics



Content Rewriting

Name

rewrite-request

Action Type

Request

Response

Action

Add HTTP Header

Specifics

Header Name

test-header

Header Value

test-header-value

2. Set match condition

Content Rewriting

Edit Match Condition (Empty Match Condition will match anything)

Object
HTTP Host Header

Type
String Regular Expression

Content
Host.example2

Reverse
 OFF

Ignore Case
 ON

3. Bind content rewriting with the Layer 7-HTTP Virtual server

Add new header to HTTP request if the HTTP request URL matches with the configuration

The screenshot shows the 'Virtual Server' configuration page in the Fortinet GUI, with the 'Basic' tab selected. The configuration is as follows:

- Name:** L7-HTTP-VS
- Type:** Layer 7 (selected), Layer 4, Layer 2
- Status:** Enable (selected), Disable, Maintain
- Address Type:** IPv4 (selected), IPv6
- Traffic Group:** default

Under the 'Specifics' section:

- Schedule Pool:** OFF
- Content Routing:** OFF
- Content Rewriting:** ON
- Content Rewriting List:**
 - Selected Items:** rewrite-request
 - Available Items:** Create New

FORTINET®

High Performance Network Security



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.