



FORUM SYSTEMS HANDS-ON TRAINING

LAB 12. THREAT MITIGATION – IDP RATE THROTTLING



FORUM SYSTEMS

A Crosscheck Networks Company

Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOST™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2014 Forum Systems, Inc. – All Rights Reserved.

Published: September 2014

Forum Systems Hands-on Training – Lab 12. Threat Mitigation – IDP Rate Throttling
D-ASF-SE-010029

Contents

Introduction.....	4
<i>Skill Level</i>	4
<i>Prerequisites</i>	4
<i>Lab Overview</i>	4
Building a REST Policy	5
Building the IDP Rule in Sentry.....	7
Testing the REST Policy	10
Additional Testing and More Reading.....	12
<i>BACK IT UP!</i>	12
<i>Additional Tests and Discussion Topics</i>	12
<i>Additional Information</i>	12
About Forum Systems.....	13

Introduction

Lab 12. Threat Mitigation – IDP Rate Throttling

Skill Level

This lab is Intermediate Skill Level. Some existing experience with Forum Sentry and SOAPSonar or completion of the Beginner Level labs is assumed.

Prerequisites

This lab requires the Forum Sentry Training Image, with a licensed copy of SOAPSonar Enterprise Edition.

Refer to the “FS_Training_Labs_v8-1_Introduction” document for information on the Forum Sentry Training Image and licensing SOAPSonar Enterprise Edition.

This lab assumes a basic understanding of building and testing a REST Policy in Sentry, as outlined in Lab 6.

Lab Overview

This lab focuses on threat protection IDP Rules (Intrusion Detection and Prevention) in Sentry. Specifically, throttling the number of requests allowed during a specific time period, based on the client IP.

IDP Rules in Sentry are firewall type rules that filter/block transactions based on a variety of criteria, including but not limited to: size, frequency, content, virus scanning, authentication/authorization failures, etc. Throughout the previous labs you may have received errors from Sentry that referenced some of the other default IDP Rules (e.g. Invalid WSDL Message, Invalid HTTP Message, Process Error, etc.).

In this lab we will build a new REST Policy for the OpenWeatherMap API. The setup is very similar to Lab 6. We will use a new listener for this new REST policy and we will apply rate throttling IDP rules to limit the client to 10 documents per minute.

This lab will provide instructions for creating custom IDP rules in Forum Sentry. Topics include:

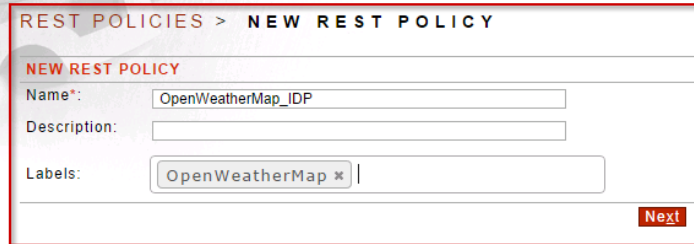
1. IDP Rules
2. IDP Actions
3. IDP Groups
4. Rate Throttling

Building a REST Policy

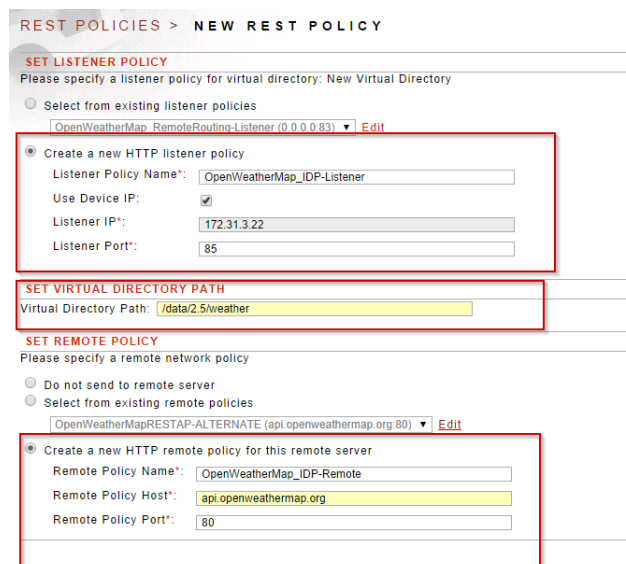
In this step we will build a new REST Policy in Sentry for the OpenWeatherMap API. This REST Policy will use a new network listener policy. For detailed instructions on building a REST Policy in Sentry, refer to Lab 6 of this series.

Follow the steps below to build a REST Policy in Sentry

1. Navigate to the Gateway→Content Policies→REST Policies page
2. Click New and create a REST Policy with the following criteria:
 - a. Name: OpenWeatherMap_IDP
 - b. Label: OpenWeatherMap



3. On the next screen, you are prompted to select existing remote policies or to build new listener and remote policies, and to enter the virtual path. Create new network policies rather than reusing any existing policies. Enter the following information to build the REST Policy for the OpenWeatherMap API:
 - a. Check the “Use Device IP” box
 - b. Set the listener port to: 85
 - c. Set the Virtual Directory Path to: /data/2.5/weather
 - d. Set the Remote Policy Host to: api.openweathermap.org
 - e. Set the Remote Policy Port to: 80
 - f. Click Finish



4. Access the Virtual Directory page by clicking the link “New Virtual Directory” and configure with the following criteria:
 - a. Name: OpenWeatherMap IDP
 - b. Filter Expression: .*
 - c. Scroll down and click Save
5. You have now successfully deployed the OpenWeatherMap REST API through Forum Sentry.

Building the IDP Rule in Sentry

In this step we will build a custom IDP Rule in Sentry for maximum document count. This rule will limit the number of documents (requests) per minute to 10. The rule will be enforced by client IP.

When the IDP threshold limit is reached, the client will be blocked for a period of 2 minutes. The client will be unable to access the service for a period of 2 minutes. After that period, the client IP will be allowed in again with the same limit of 10 documents per minute.

This will require building a custom IDP Action, a custom IDP Rule, and a custom IDP Group. Lastly, we will associate the custom IDP Group to the “OpenWeatherMap_IDP” REST Policy in Sentry.

Follow these steps to build a new IDP Action in Sentry.

1. Navigate to the IDP→IDP Policies→IDP Actions page.
2. Click New to create a new IDP Action. Configure the IDP Action with the following criteria:
 - a. Name: Block_for_2_Minutes
 - b. Prevention Settings: Abort processing of the document
 - c. Future Access Restrictions: Block and Lift restriction after 2 minutes
 - d. Leave all other defaults
 - e. Click Create

The screenshot shows the Sentry API Security Gateway interface. On the left is a sidebar with navigation links: GENERAL, Forum Systems, DIAGNOSTICS, GATEWAY, RESOURCES, IDP, IDP Blocking, IDP Policies, IDP Rules, IDP Actions (highlighted with a red box), IDP Schedules, IDP Clustering, ACCESS, SYSTEM, and PARTNERS. The main content area is titled 'IDP ACTION POLICIES > IDP ACTION DETAILS'. It contains several sections: 'IDP ACTION' with a 'Name' field set to 'Block_for_2_Minutes'; 'PREVENTION SETTINGS' with 'Abort processing of the document' checked; 'FUTURE ACCESS RESTRICTIONS' with 'Block' selected and 'Lift restriction after 2 minutes' checked; and 'ALERTS' with 'Log an alert' checked. Other options like 'Stealth Mode', 'Throttle at', and 'SNMP trap alert' are visible but not selected.

Follow these steps to build a new IDP Rule in Sentry.

1. Navigate to the IDP→IDP Policies→IDP Rules page.
2. Click New to create a new IDP Rule. Configure the IDP Rule with the following criteria:
 - a. Name: Max_Doc_10_Per_Minute
 - b. Criterion: Maximum document count
 - c. Value: 10
 - d. Period: Minute
 - e. Enforcement: Enforce by IP
 - f. IDP Action: Block_for_2_Minutes
 - g. Abort Message: BLOCKED 2 MINUTES
 - h. Leave all other defaults
 - i. Click Create

IDP RULE POLICIES > IDP RULE DETAILS

DETECTION SETTINGS

IDP Rule Name*: Max_Doc_10_per_Minute

Description:

Criterion: Maximum document count

THRESHOLD

Value: 10 KB

Period: Minute

ENFORCEMENT SETTINGS

☐ Enforce only on user group: LDAP-FS_LDAP Edit

☒ Enforce by IP

☐ Enforce by user

IDP ACTION

IDP Action: Block_for_2_Minutes Edit

Abort Message: BLOCKED 2 MINUTES

IDP SCHEDULE

IDP Schedule: Anytime Edit

Create

Follow these steps to build a new IDP Group in Sentry.

1. Navigate to the IDP→IDP Policies→IDP Groups page.
2. Click New to create a new IDP Group. Create the IDP Group with the following criteria:
 - a. Name: Custom_REST_Policy_IDP_Group
 - b. IDP Group Type: HTML Policy
 - c. Click Create
 - d. Add the custom IDP rule created in this lab to the IDP Group by checking the associated box to the left of the new rule under the Request column – this enables the rule for requests only
 - e. Leave all other defaults
 - f. Click Save

IDP GROUP POLICIES > IDP GROUP DETAILS

IDP GROUP DETAILS

IDP Group Name*: Custom_REST_Policy_IDP_Group

Description:

IDP Group Type: HTML Policy

REQUEST	RESPONSE	IDP RULE	CRITERION	THRESHOLD	USER GROUP	ENFORCE BY	IDP ACTION	IDP SCHEDULE
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Invalid HTTP Message	Document does not match any message type filter			Abort	Anytime	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Large Payload	Maximum payload size	25 MB		Abort	Anytime	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Large XML	Maximum XML document size	10 MB		Abort	Anytime	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Process Error	Document processing error			Abort	Anytime	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Virus Detected	Virus found			Abort	Anytime	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Authentication Failure	Authentication failed			Abort	Anytime	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Authorization Failure	Unauthorized access			Abort	Anytime	
<input type="checkbox"/>	<input type="checkbox"/>	Invalid SOAP Message	Document does not match any SOAP message			Abort	Anytime	
<input type="checkbox"/>	<input type="checkbox"/>	Max Archive Resource	Maximum caching depth	5 levels		Abort	Anytime	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Max_Doc_10_Per_Minute	Maximum document count	10 documents / Minute	IP	Block_for_2_Minutes	Anytime	
<input type="checkbox"/>	<input type="checkbox"/>	Un-Matching XML	Document does not match any XML filter			Abort	Anytime	
<input type="checkbox"/>	<input type="checkbox"/>	SOAP Rule Violation	SOAP rule violation			Abort	Anytime	

Create Save

Follow these steps to associate the new IDP Group to the “OpenWeatherMap_IDP” REST Policy in Sentry

1. Navigate to the Gateway→Content Policies→REST Policies page
2. Open the OpenWeatherMap_IDP REST Policy
3. Click the IDP Tab
4. Change the IDP Group to “Custom_REST_Policy_IDP_Group”
5. Click Save
6. Notice the custom IDP rule for 10 documents per minute is included

REST POLICIES > REST POLICY

REST POLICY

Policy Name: OpenWeatherMap_IDP

Virtual Directories
Task Lists
Settings
IDP Rules
Logging

IDP GROUP



IDP Group: Custom_REST_Policy_IDP_Group
Edit
Save

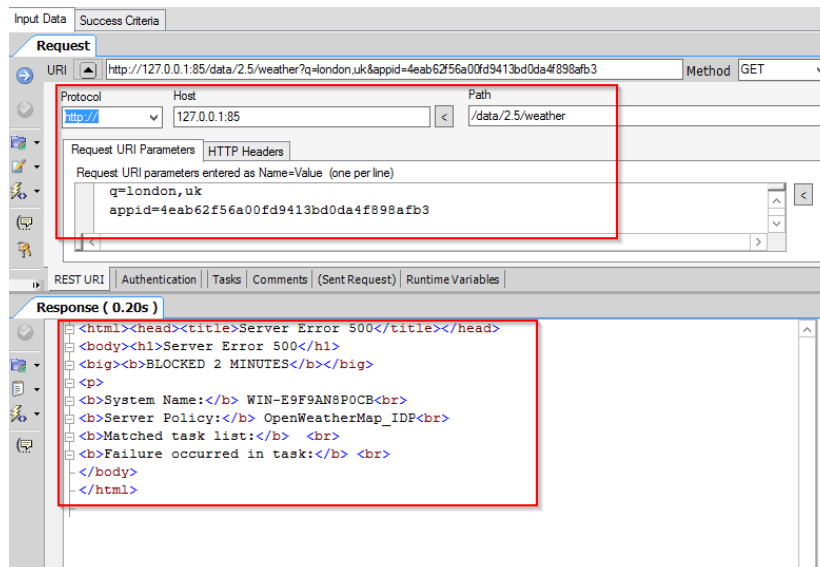
I/O	IDP RULE	IDP CRITERION	THRESHOLD	USER GROUP	ENFORCE BY	IDP ACTION	IDP SCHEDULE
♦♦	Invalid HTTP Message	Document does not match any message type filter				Abort	Anytime
♦♦	Large Payload	Maximum payload size	25 MB			Abort	Anytime
♦♦	Large XML	Maximum XML document size	10 MB			Abort	Anytime
♦♦	Process Error	Document processing error				Abort	Anytime
♦♦	Virus Detected	Virus found				Abort	Anytime
♦	Authentication Failure	Authentication failed				Abort	Anytime
♦	Authorization Failure	Unauthorized access				Abort	Anytime
♦	Max Doc 10 Per Minute	Maximum document count	10 documents / Minute	IP		Block for 2 Minutes	Anytime

Testing the REST Policy

Now that “OpenWeatherMap_IDP” REST Policy has been configured to allow 10 documents per minute, test the new IDP rule using SOAPSonar.

Follow the steps below to test max document IDP rule using SOAPSonar.

1. Launch SOAPSonar and build a new REST Project.
 - a. In the Project QuickStart menu choose Create a REST Project
 - b. Name the project “OpenWeatherMap_IDP”
2. Build the REST Test case in SOAPSonar using the information listed below. You’ll notice the Request URI field will update automatically.
 - a. **Protocol:** HTTP
 - b. **Host:** 127.0.0.1:85
 - c. **Path:** /data/2.5/weather
 - d. **Request URI Parameters / Name=Value pairs (one per line):**
q=London,uk
appid= 4eab62f56a00fd9413bd0da4f898afb3
3. Click the  to commit the settings.
4. Test the policy by sending the request using the  button.
 - a. You will receive a JSON formatted response with the weather data requested for the region entered
 - b. Send requests repeatedly (at least 11 requests) until you receive an error from Sentry.



- c. Your IP is blocked for 2 minutes. You can view the list of blocked IPs in Sentry and lift the restriction manually. Navigate to the IDP→IDP Blocking→IDP Blocking page
- d. View the list of blocked clients. You can select the blocked client and remove the

restriction manually

IDP BLOCKING						
Blocked						
<input type="checkbox"/>	USER/IP	COUNT	TRIGGER VALUE	IDP RULE	IDP GROUP	POLICY
<input type="checkbox"/>	127.0.0.1	1	11 documents / Minute	Max_Doc_10_Per_Minute	Custom_REST_Policy_IDP_Group	OpenWeatherMap_IDP
						EXPIRES
						2014/09/20 00:03
Throttled						
<input type="checkbox"/>	USER/IP	COUNT	TRIGGER VALUE	IDP RULE	IDP GROUP	POLICY
No items to display						
						Refresh Remove

END

Additional Testing and More Reading

BACK IT UP!

It is recommended that you export your REST Policy and/or your full Sentry configuration after completing this lab.

To export the REST policy, navigate to the REST Policies page, select the REST policy and use the GDM Export option to export the policy (and all dependencies) as a password encrypted FSG file. This can later be imported on the System→Configuration→Import/Export screen.

To export your full Sentry configuration, navigate to the System→Configuration→Import/Export screen and use the Export option in the center of the page to export the full Sentry configuration file as a password encrypted FSX file. This can later be imported on the same screen.

Backup your SOAPSonar project file by using the File→Save As option. All of your test cases will be saved in an .SSP file.

We recommend including the lab number in the name of the export files.

Additional Tests and Discussion Topics

1. After you are blocked, wait over 2 minutes and try the service again. Does it work?
2. Modify the different IDP Action, test the “Future Access Restriction” for Throttling.

Additional Information

For more information, review the following Forum Sentry Admin Guide:

1. IDP Policies Guide
2. REST Policies Guide

About Forum Systems

Forum Systems is the global leader in API and Cloud Security technology with industry-certified, patented, and proven products deployed in the most rigorous and demanding customer environments worldwide. Forum Systems has been an industry leader for over 12 years and has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP. Forum Systems security-first mindset enables trusted, network edge deployments of its technology for protecting critical enterprise transactions.

Our product technology is purpose-built and designed for mission-critical, enterprise-class scalable solutions where business solutions require the modern day security and identity enforcement protection, while enabling a scalable architecture and low-latency, high-volume throughput.

Forum Systems supports global enterprise customers across industries in commercial, government, and military sectors. Forum Systems technology provides the leading-edge of modern-day cyber-security innovation with integrated identity and SSO features that enable out-of-the box business solutions with point-and-click technology.

Forum's patented; FIPS 140-2 and NDPP certified hardware and virtual products make modern-day business communications secure by actively protecting and accelerating data exchange and API service access across networks and business boundaries. For more information, please visit www.forumsys.com.