

Anonymous Proxy Detection

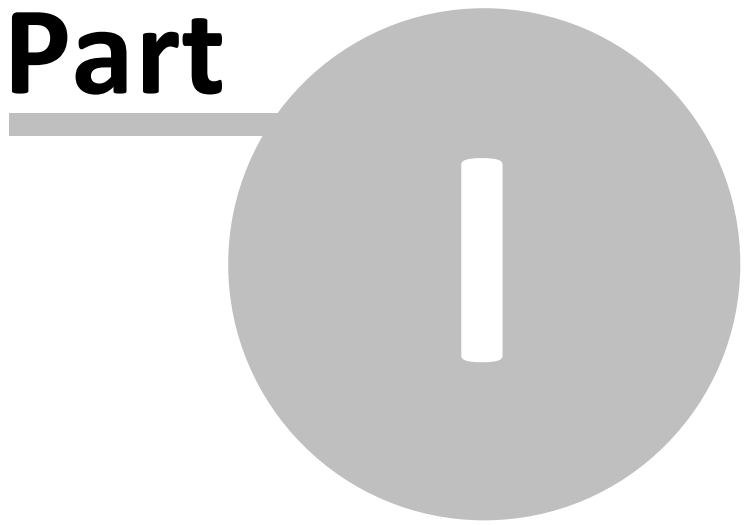
Exinda ExOS Version 6.3

© 2012 Exinda, Inc

Table of Contents

Part I Introduction	4
1 Using this Guide	4
Part II Overview	6
Part III Enabling Anonymous Proxy Detection	8
Part IV Controlling Anonymous Proxy Traffic	11

Part



1 Introduction

Anonymous Proxy Detection

Exinda Firmware Version: 6.3

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

1.1 Using this Guide

Throughout the manual the following text styles are used to highlight important points:

- Useful features, hints and important issues are called "notes" and they are identified in a light blue background.

Note: This is a note.

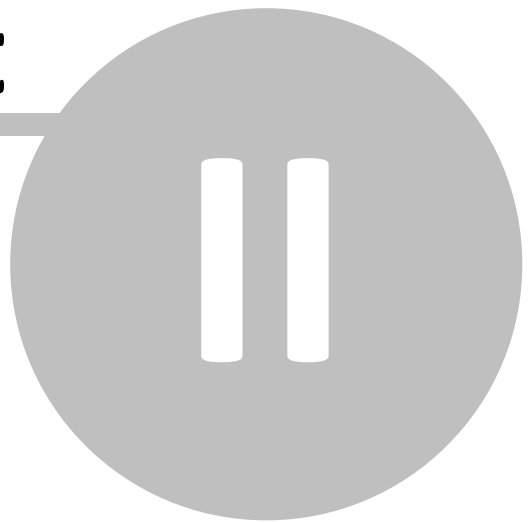
- Practical examples are presented throughout the manual for deeper understanding of specific concepts. These are called "examples" and are identified with a light green background.

This is an example.

- Warnings that can cause damage to the device are included when necessary. These are indicated by the word "caution" and are highlighted in yellow.

Caution: This is a caution.

Part



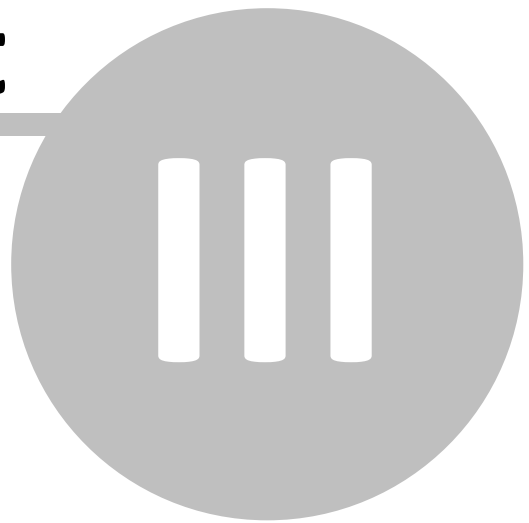
2 Overview

Anonymous Proxies are typically used to circumvent security policies, allowing users to access prohibited recreational, adult or other non-business sites by tunneling this traffic over a regular or encrypted HTTP session. Anonymous Proxies also provide anonymity - users accessing websites through an Anonymous Proxy can't easily be traced back to their original IP.

Starting with ExOS 5.3, Exinda appliances have built-in support for Anonymous Proxy detection. The Exinda appliance will receive daily updates from www.exinda.com containing updated Anonymous Proxy definitions, much like anti-virus applications receive daily threat updates.

This How to Guide explains how to enable Anonymous Proxy detection and how to monitor and control Anonymous Proxy traffic.

Part



3 Enabling Anonymous Proxy Detection

The Anonymous Proxy service is disabled by default. In order to enable this feature, navigate to Objects | Applications | Anonymous Proxy using the Web UI, Advanced mode.

Service: Running
Restart
Stop
Disable

Settings	
URL	http://www.exinda.com/ap/apdata.tar.gz
Last Check	2009/12/03 09:32:08 (57m 45s ago)
Last Update	2009/12/03 09:32:11 (57m 42s ago)
Status	Ok

The **renumerate** button refreshes the Anonymous Proxy list immediately

Renumerate

Figure 1: The form to configure and enable the Anonymous Proxy service.

This page allows you to start the Anonymous Proxy service and also check when the definitions were last updated. The 'Renumerate' button allows you to force the Anonymous Proxy service to fetch the latest definitions immediately.

Given that Anonymous Proxies are constantly changing, the Anonymous Proxy service will automatically retrieve the latest Anonymous Proxy definitions from the Exinda servers on a daily basis. If the Anonymous proxy service is stopped or disabled the last retrieved definitions will be used for detection of Anonymous proxy.

Note: In order to receive daily Anonymous Proxy definition updates, the Exinda appliance must be able to contact the www.exinda.com web servers and the appliance must also have valid software subscription.

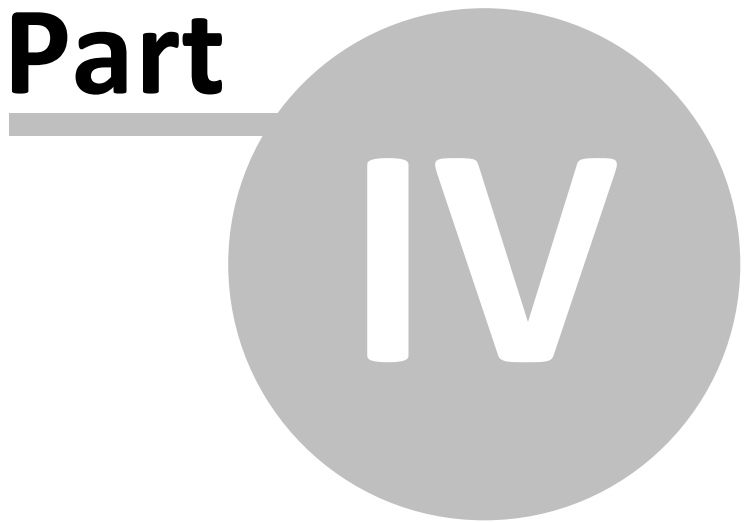
The Anonymous proxy ASAM is another component of the Anonymous Proxy detection. This works in combination with the Anonymous Proxy service and it is enabled by default. To disable this ASAM, navigate to System | Setup | Monitoring using the Web UI - Advanced mode. If the service is stopped and Anonymous proxy detection is no longer required, disabling the ASAM will clear the existing definitions.

ASAM	
HTTP	<input checked="" type="checkbox"/> Enable
Citrix	<input checked="" type="checkbox"/> Enable
Anonymous Proxy	<input checked="" type="checkbox"/> Enable

Apply Changes

Figure 2: The form to enable/disable the Anonymous Proxy ASAM.

Part



IV

4 Controlling Anonymous Proxy Traffic

Once the Exinda appliance identifies traffic as an Anonymous Proxy, it is classified as the "Anonymous Proxy" application. This means that any Anonymous Proxy traffic will show up in the real-time monitoring screen and other monitoring reports as "Anonymous Proxy".

Inbound Applications					Outbound Applications				
Application Name	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)	Application Name	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	177.348	52	129		Total	78.713	57	131	
HTTP	119.675	22	33	<div style="width: 33%;"></div>	HTTP	41.652	26	33	<div style="width: 33%;"></div>
IKE	26.096	7	17	<div style="width: 17%;"></div>	IKE	9.341	8	17	<div style="width: 17%;"></div>
HTTPS	15.154	4	10	<div style="width: 10%;"></div>	HTTPS	5.634	5	10	<div style="width: 10%;"></div>
IMAP-SSL	5.043	2	1	<div style="width: 1%;"></div>	ssdp	5.268	1	2	<div style="width: 2%;"></div>
Skype	3.448	4	36	<div style="width: 36%;"></div>	SSH	5.072	4	2	<div style="width: 2%;"></div>
SSH	2.672	5	2	<div style="width: 2%;"></div>	SMTP	3.791	2	2	<div style="width: 2%;"></div>
Anonymous Proxy	2.184	2	7	<div style="width: 7%;"></div>	Anonymous Proxy	2.745	2	7	<div style="width: 7%;"></div>
SMTP	1.806	4	2	<div style="width: 2%;"></div>	Skype	2.594	4	36	<div style="width: 36%;"></div>
ICMP	0.530	1	4	<div style="width: 4%;"></div>	IMAP-SSL	1.166	2	1	<div style="width: 1%;"></div>
BitTorrent	0.506	1	3	<div style="width: 3%;"></div>	ExindaCom	0.620	1	12	<div style="width: 12%;"></div>
DNS	0.130	0	1	<div style="width: 1%;"></div>	ICMP	0.376	0	4	<div style="width: 4%;"></div>
ExindaCom	0.104	0	12	<div style="width: 12%;"></div>	BitTorrent	0.328	1	3	<div style="width: 3%;"></div>
					DNS	0.105	0	1	<div style="width: 1%;"></div>

Figure 3: The Anonymous Proxy application is shown on the real-time monitoring screen.

It is also possible to create Optimizer Policies using the Anonymous Proxy application, like you would any other application. The Optimizer Policy configuration form below shows how to create an Optimizer Policy that will block Anonymous Proxies.

Add New VC Policy

Policy Name: Block Options: Discard only the first packet of a connection

VC Policy Number:

Schedule:

Action:

Policy Enabled:

Filter Rules:

VLAN	Host	Direction	Host	ToS/DSCP	Application
<input type="text"/>	<input type="text"/>	<input type="text" value="< - >"/>	<input type="text"/>	<input type="text"/>	Anonymous Proxy
<input type="text"/>	<input type="text"/>	<input type="text" value="< - >"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="< - >"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="< - >"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 4: Blocking Anonymous Proxies using the Optimizer.

Note: By default, the Anonymous Proxy application is part of the Recreational application group. This means that any policy that references the Recreational application group will also be referencing the Anonymous Proxy application. If you want to block Anonymous Proxies, the discard policy must be above any policy that references the Recreational application group.