



SANGFOR

NGAF

URL filtering abnormal Troubleshooting

Version 8.0.6

Change Log

Date	Change Description
Apr 26, 2019	URL filtering abnormal Troubleshooting

Content

Chapter 1 Application scenario	1
Chapter 2 Troubleshooting methods.....	1

Chapter 1 Application scenario

URL filtering does not take effect.

Chapter 2 Troubleshooting methods

1. Go to **System > Maintenance > Database Update** check if the URL Database is Latest Version.

No.	Database	Current Version	Latest Version
1	Sangfor Engine Zero File Verification Model Database	2018-11-15 Logs	2018-11-15
2	URL Database	2019-04-16 Logs	2019-04-16
3	Exploit Protection Database	2019-04-22 Logs	2019-04-22
4	Software Update	--	2019-02-19
5	Application Ident Database	2019-04-15 Logs	2019-04-15
6	WAF Signature Database	2019-04-10 Logs	2019-04-10
7	Data Leak Protection	2018-02-16 Logs	2018-02-16
8	Vulnerability Analysis Rule	2019-03-27 Logs	2019-03-27
9	IP address database	2019-04-15 Logs	2019-04-22
10	Threat Intelligence Database	2019-02-27 Logs	2019-02-27
11	Hot Threat Database	2019-04-26 Logs	2019-04-26
12	Security Events	2019-04-15 Logs	2019-04-15

2. Go to **Policies > Network Security > Policies** check if the policies is configured to Deny.

Basics Protection (for any scenario)

☐ Intrusion Prevention [i](#)

Default Template: Internet Access Scenario Action: ☐ Allow ☒ Deny

☒ Content security (file verification based on Sangfor Engine Zero) [i](#)

testPorn Action: ☐ Allow ☒ Deny

3. Go to **Objects > Security Policy Template > Content Security** check if the URL Filter is associated with the correct site, Check if the Schedule is ALL week.

Edit Template

Name: testPorn

Description:

Protection

☐ Email Protection(It will scan email body, filter email attachments and verify files based on Sangfor Engine Zero.)

Server Port: 25,110,143 [i](#)

Malicious Email Alert: It contains malicious content [i](#)

☒ URL Filter

Sites: testPorn [i](#)

☐ File Protection(It will filter files and verify file based on Sangfor Engine Zero.)

Schedule: All week

3. Do a separate test policy for a single test IP, move to the top to prevent multiple policy conflicts.
4. Go to **System > Troubleshooting** check if Start Bypass.
5. Go to **Policies > Blacklist/Whitelist** check if the whitelist matches the corresponding IP.
6. Capture packet to confirm whether the packet passes through the device in both directions.



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc