



NGAF

Best Practices for Scenarios_Botnet Prevention

Version 8.0.17



Change Log

Date	Change Description
June 15, 2020	Document release.
Mar 18, 2021	Document Update
May 17, 2021	Document update.

CONTENT

Chapter 1 Scenario	1
1.1 Function Introduction.....	1
1.2 Testing URL.....	1
Chapter 2 Best Practice Recommendations.....	1
2.1 Endpoint Protection Policy Recommendations	2
2.2 Server Protection Policy Recommendations	3
Chapter 3 Precautions	4

Chapter 1 Scenario

1.1 Function Introduction

Traditional firewall and anti-virus software have limited effectiveness in anti-virus trojans. In the APT (Advanced Persistent Threat) scenario, traditional firewall and anti-virus software have weak detection and defense capabilities. Therefore, post-incident detection mechanism is needed to detect and Locate the infected machine of the endpoint to reduce the security risk of the endpoint. At the same time, the recorded logs require high traceability.

1.2 Testing URL

You can use following URL to test:

ifferfsodp9ifjaposdfjhgosurijfaewrrergwea.com

iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com

v.beahh.com

aqln.ws

mlmy.3322.org

www.iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com

clptiiybpip.cn

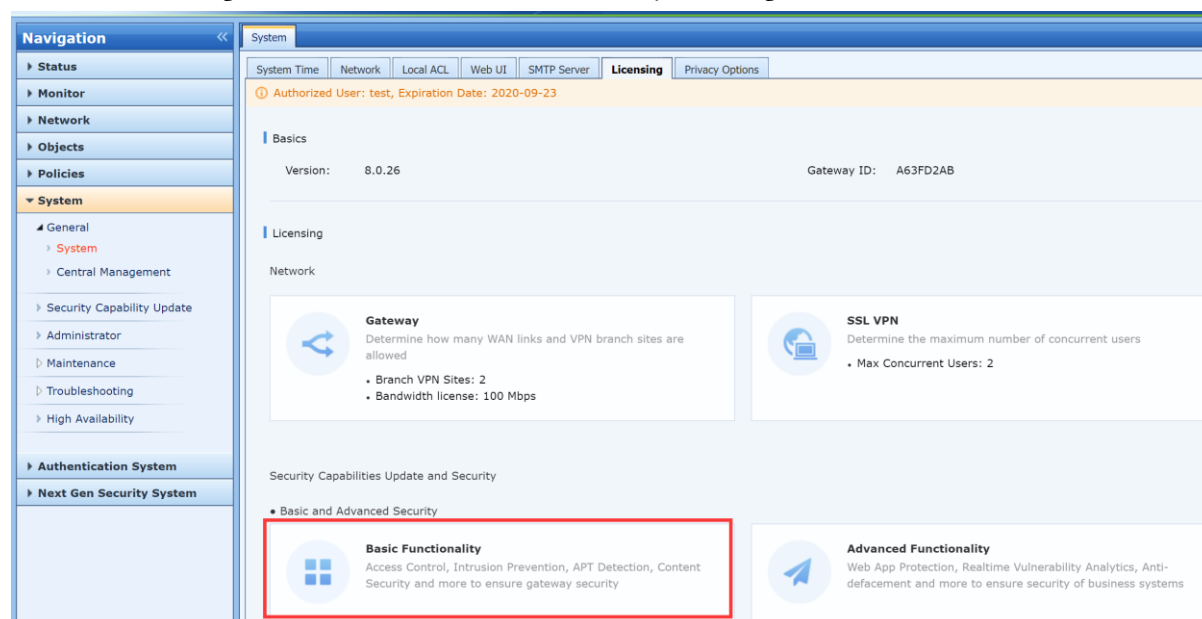
task.attendecr.com

bddp.net

cqogflioz.cn

Chapter 2 Best Practice Recommendations

Check the licensing to make sure that Basic Functionality licensing is enabled on the device.



Update the database to ensure that the database is updated to the latest time.

Botnet Prevention

No.	Database	Current Version	Latest Version	Update Svc Exp...	Auto Update	Operation
Neural-X Unknown Threat Database						
1	Unknown Threat Intelligence	2020-07-13 00:20:37	2020-07-13 00:20:37	2020-09-23	✓	
File Verification Model Database						
2	Sangfor Engine Zero File Verification Model Database	2020-05-17 18:00:00	2020-05-17 18:00:00	2020-09-23	✓	
Neural-X New Threat Databases						
3	URL Database	2020-06-16 09:00:00	2020-06-16 09:00:00	2020-09-23	✓	
4	Exploit Protection Database	2020-07-07 17:00:00	2020-07-07 17:00:00	2020-09-23	✓	
5	Application Ident Database	2020-05-09 11:55:59	2020-05-09 11:55:59	2020-09-23	✓	
6	WAF Signature Database	2020-07-05 15:00:00	2020-07-05 15:00:00	2020-09-23	✓	
7	Data Leak Protection	2018-02-16 18:00:00	2018-02-16 18:00:00	2020-09-23	✓	
8	Vulnerability Analysis Rule	2020-07-03 17:00:00	2020-07-03 17:00:00	2020-09-23	✓	
9	Anti-Virus Database	2020-05-19 11:00:00	2020-05-19 11:00:00	2020-09-23	✓	
10	Security Events	2020-07-06 11:00:00	2020-07-06 11:00:00	2020-09-23	✓	
Basic Databases						
11	Software Update	--	2020-06-24 00:00:00	Never expire	✓	
12	IP Address Database	2020-05-19 10:00:00	2020-05-19 10:00:00	Never expire	✓	
13	Threat Intelligence Database	2020-07-10 00:00:00	2020-07-10 00:00:00	Never expire	✓	

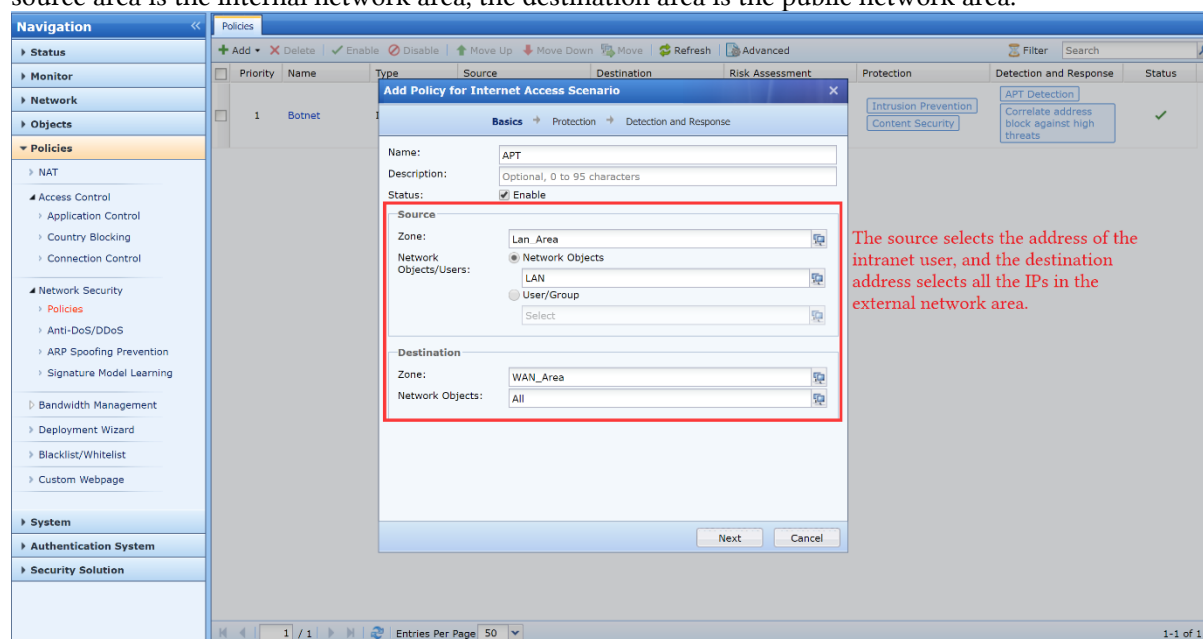
Botnet protection is recommended for both terminals and servers, both of which have the risk of infection.

Remarks: If there is a DNS server on the intranet and the intranet endpoint uses the intranet DNS for domain name resolution, the "Honeypot" technology must be enabled. Redirect malicious DNS requests, set as shown below:

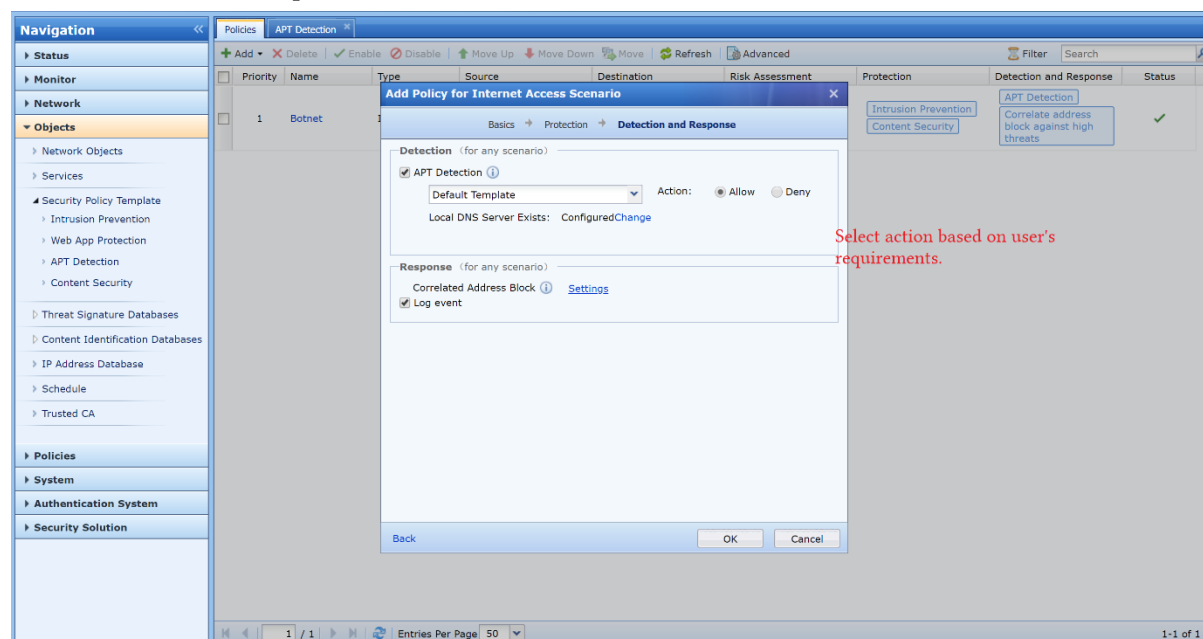
The screenshot shows the 'Botnet' policy configuration in the Sangfor SMS. The 'Advanced' tab is active, and the 'Settings' dialog box is open. The 'Honeypot Address' section is highlighted, showing the option 'Use Sangfor online honeypot address (recommended)' selected. A diagram illustrates the network setup with a client, a DNS proxy server, and a DNS server, showing how DNS requests are redirected to the honeypot address.

2.1 Endpoint Protection Policy Recommendations

Add policy and selection area, Endpoint protection direction selection needs to pay attention to the source area is the internal network area, the destination area is the public network area.

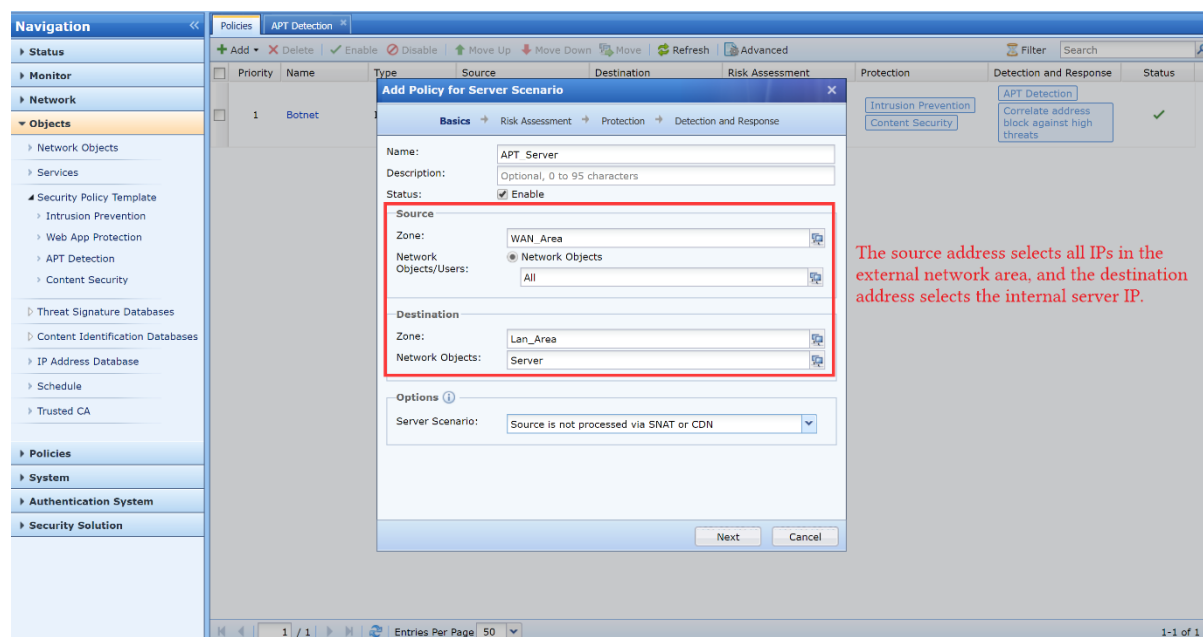


To enable the botnet function, use the "Default template" for the policy template, and select "Deny" for the action as the user requirements.

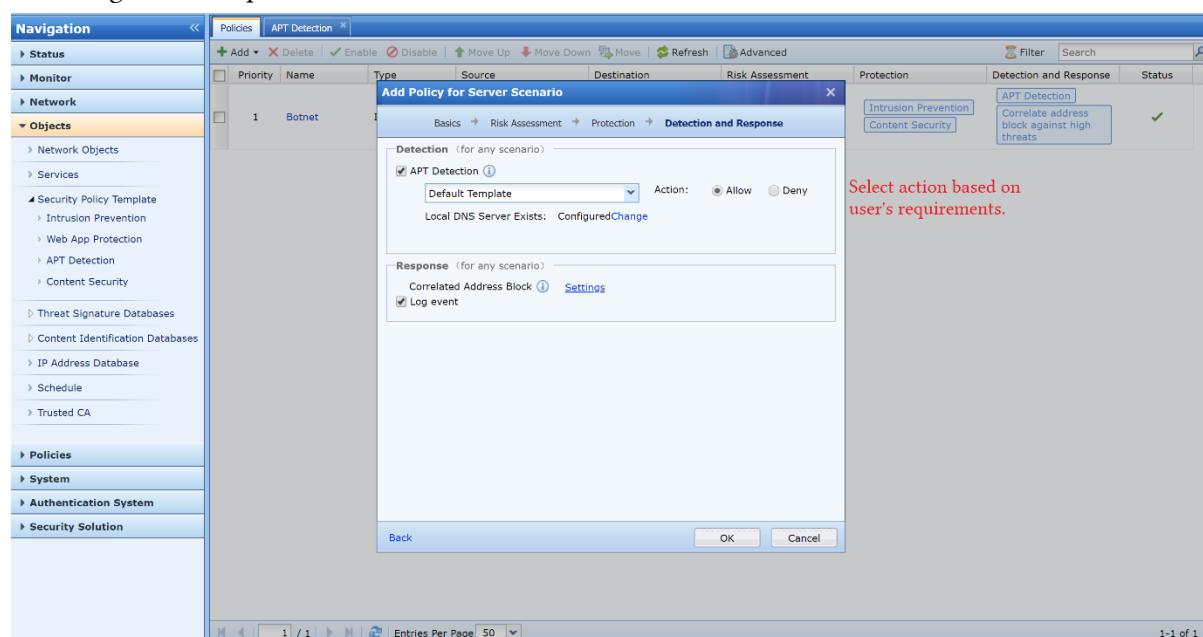


2.2 Server Protection Policy Recommendations

Add policy and selection areas are necessary. The direction of server protection needs attention that the source area is the external network and the destination area is the internal network area.



The policy template can use the "Default template", and the action can be selected as "Allow" or "Deny" according to user requirements.



Chapter 3 Precautions

The action of the botnet policy, no matter the "Policy for Server Scenario" or "Policy for Internet Access Scenario", the default action is "allow", if you want to turn on "Deny", you need to manually select;

The botnet function in the "Policy for Internet Access Scenario" can automatically reverse the area selected by the policy. For example, the source selected in the "Policy for Internet Access Scenario" is generally the external network area, and the destination area is the internal network area. Finally, for the identification and processing of botnets, the source is the internal network area and the target is the external network area;

The "Suspicious Traffic" function of the botnet does not block the behaviors that has been detected, and only records logs, and at the same time records the original data packets for later traceability.

Botnet Prevention

The screenshot displays the Sangfor security management console interface. On the left is a navigation pane with categories: Status, Monitor, Network, and Objects. Under Objects, there are sub-items: Network Objects, Services, Security Policy Template, Intrusion Prevention, Web App Protection, APT Detection (highlighted in red), Content Security, Threat Signature Databases, and Content Identification Databases.

The main area shows the 'APT Detection' configuration page. At the top, there are buttons for '+ Add', 'X Delete', and '+ Refresh'. Below is a table with columns 'No.', 'Name', and 'Protection'.

No.	Name	Protection
1	APT	Remote Access Trojan, Suspicious Traffic
2	Default Template	Remote Access Trojan
3	Anti-ransomware via bot reconnecting prevention	Remote Access Trojan

An 'Edit Template' dialog box is open, showing the configuration for the 'APT' template. It includes fields for 'Template Name' (APT) and 'Description'. Under 'Security Options', there are two checked items: 'Remote Access Trojan' and 'Suspicious Traffic Settings' (which is highlighted with a red rectangle and has an information icon). At the bottom of the dialog are 'OK' and 'Cancel' buttons.



SANGFOR

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