SANGFOR

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 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:

ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

v.beahh.com

aqhln.ws

mlmy.3322.org

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

clptiiybpip.cn

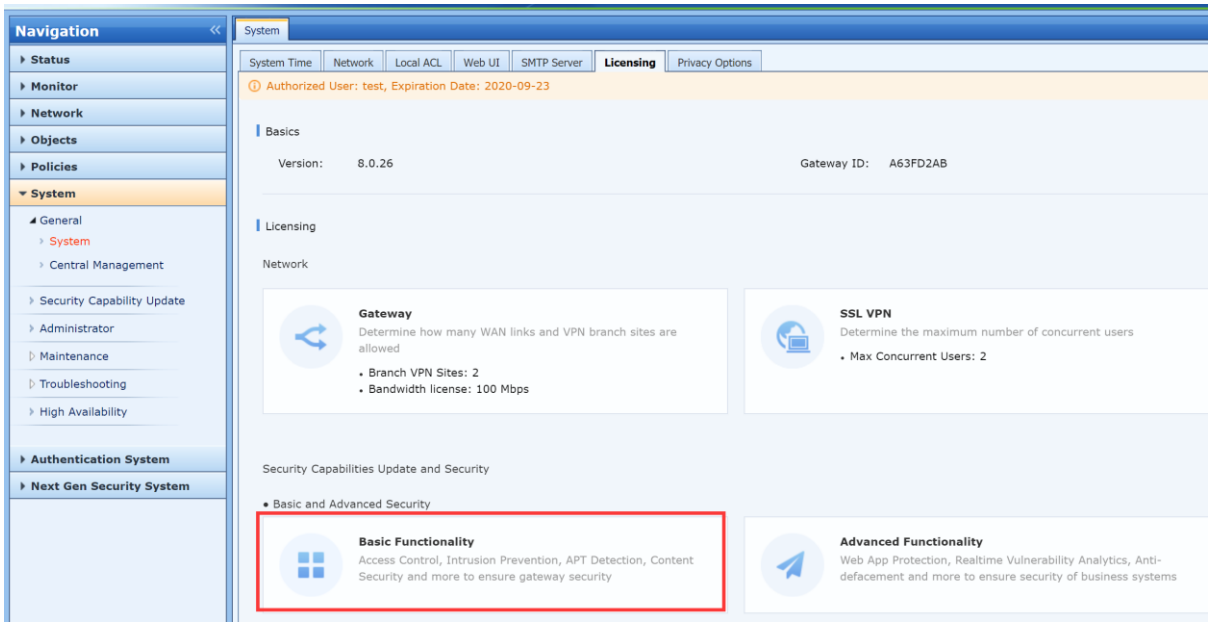
task.attendecr.com

bddp.net

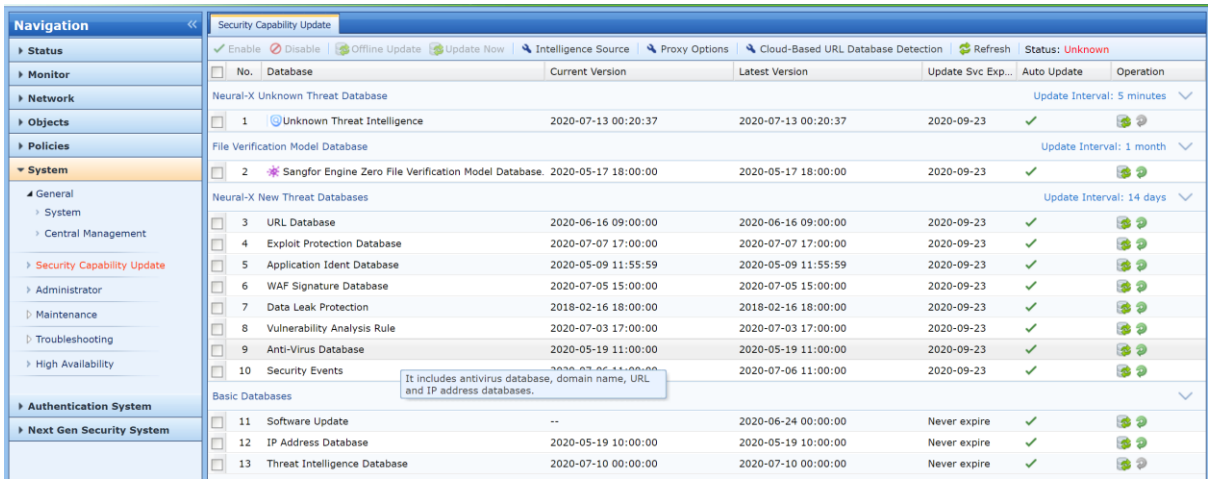
cqogflioz.cn

Chapter 2 Best Practice Recommendations

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

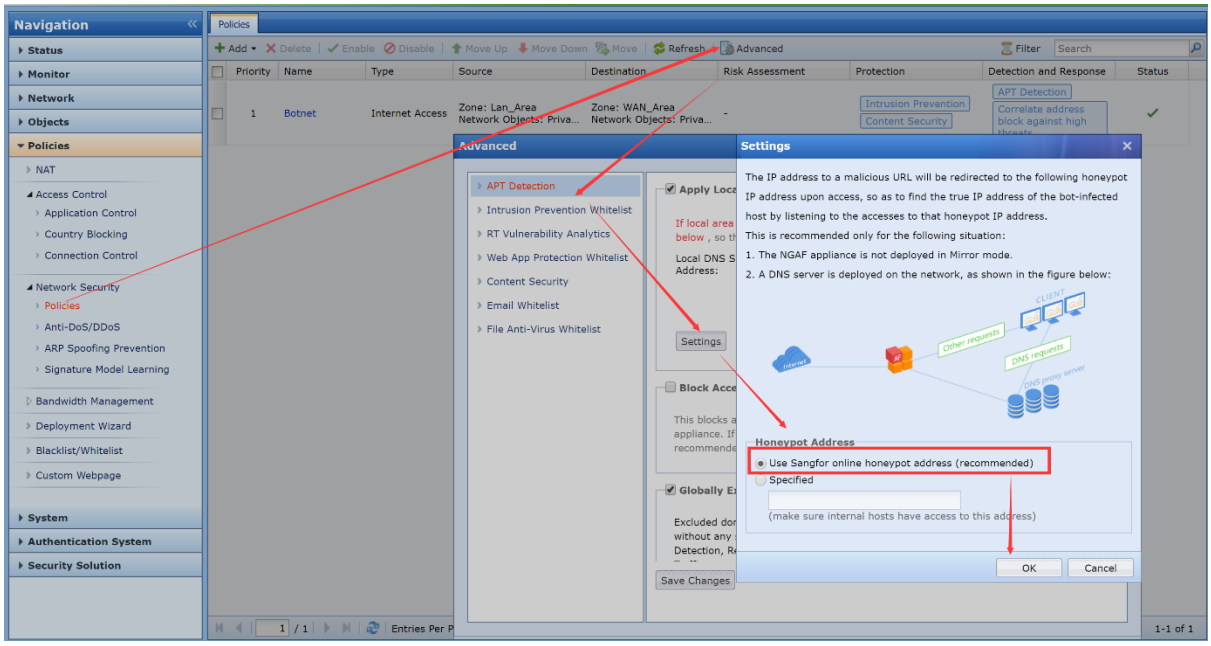


Update the database to ensure that the database is updated to the latest time.



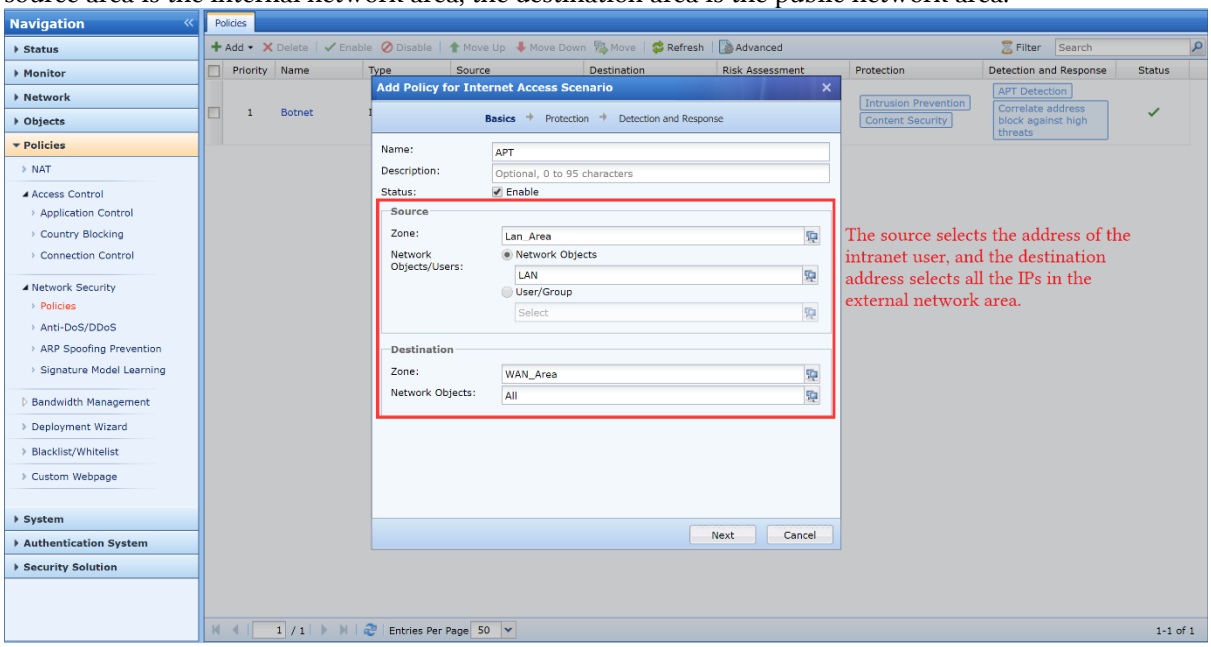
Botnet protection is recommended for both terminals and servers, both of which have the risk of infection.

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:

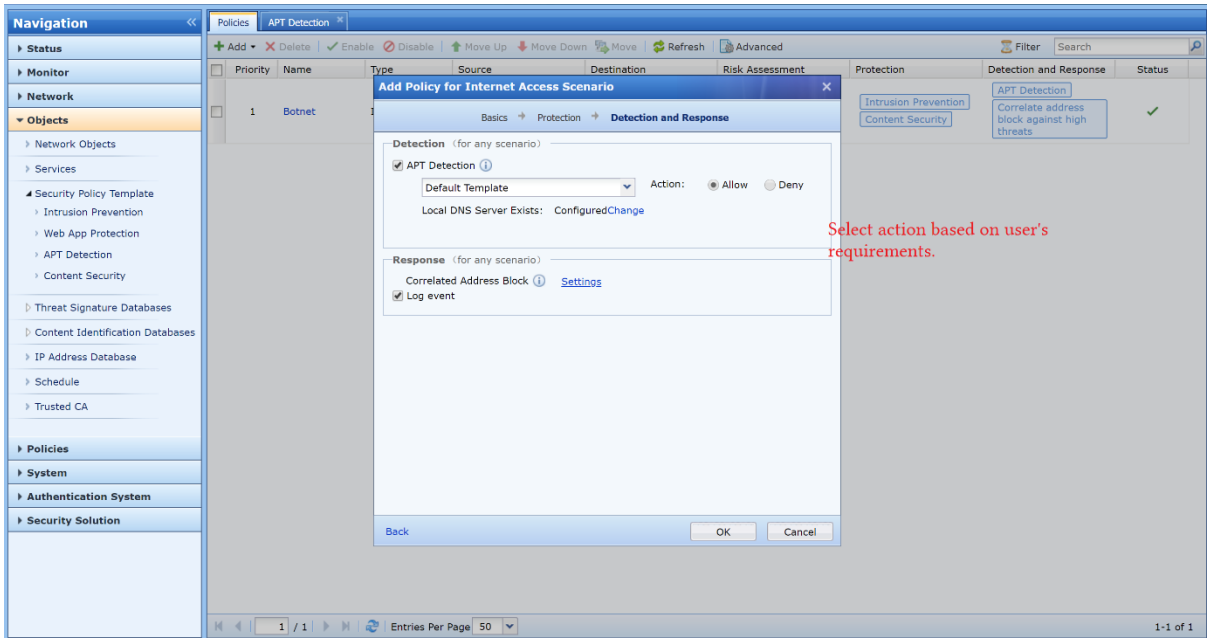


2.1 Endpoint Protection Policy Recommendations

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.

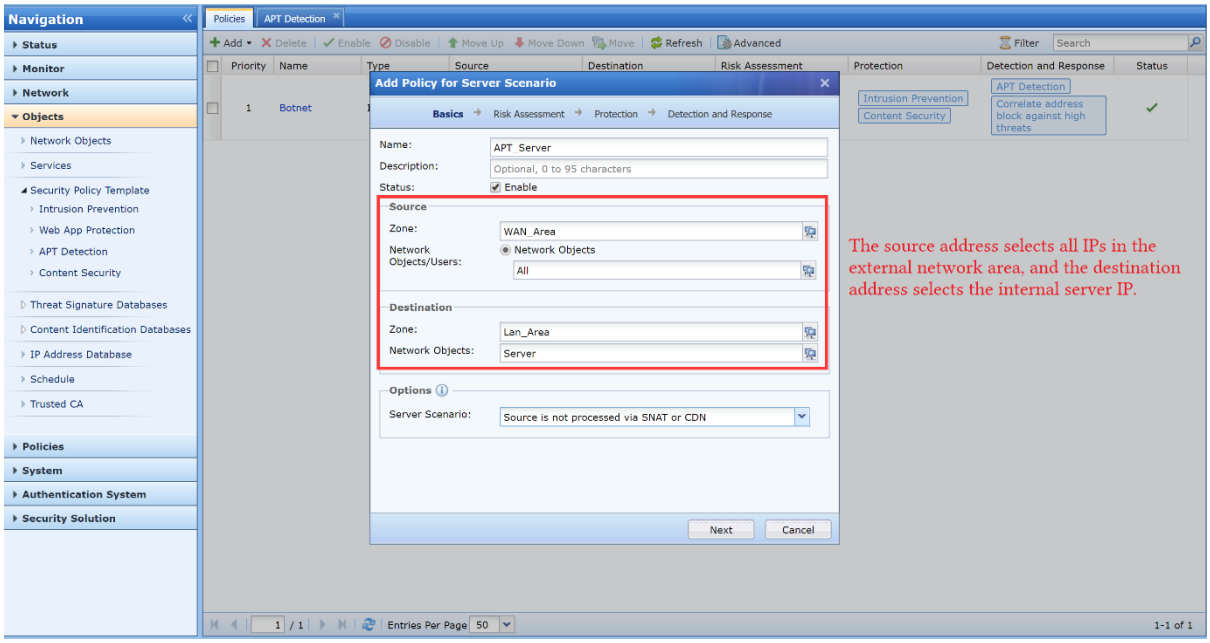


To enable the botnet function, use the "Default template" for the policy template, and select "Deny" for the action as the user requirements.

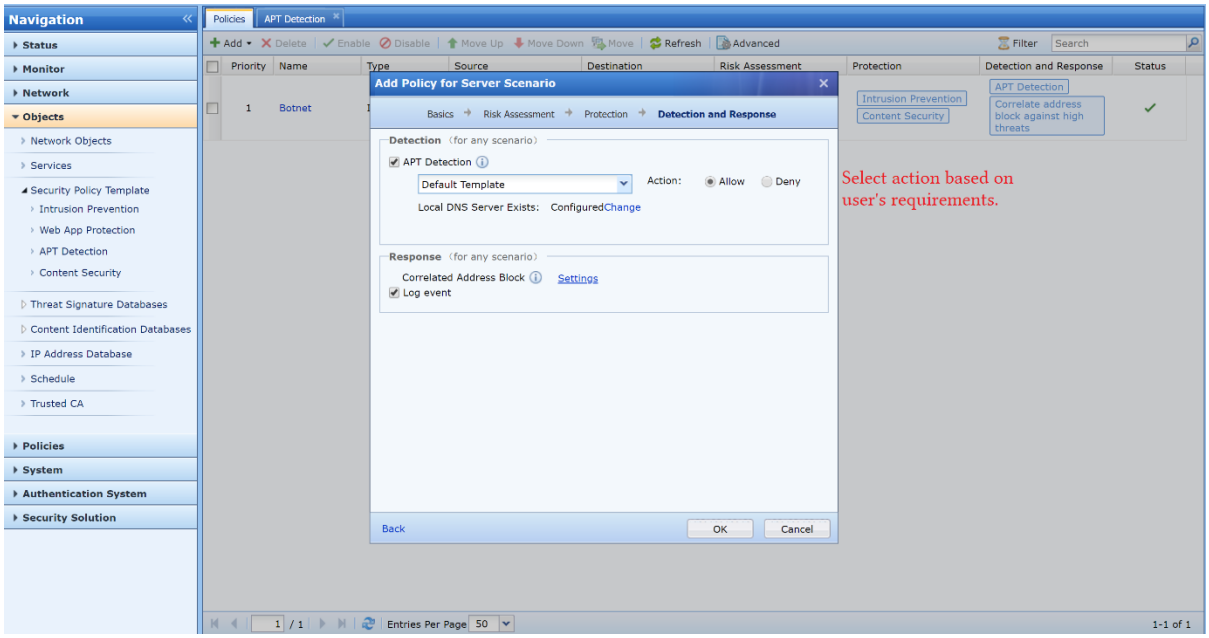


2.2 Server Protection Policy Recommendations

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