SANGFOR

NGAF

Best Practices for Configuration_Botnet Prevention

Version 8.0.35

Change Log

Date	Change Description
May 6, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Basic Configuration

Related documents:

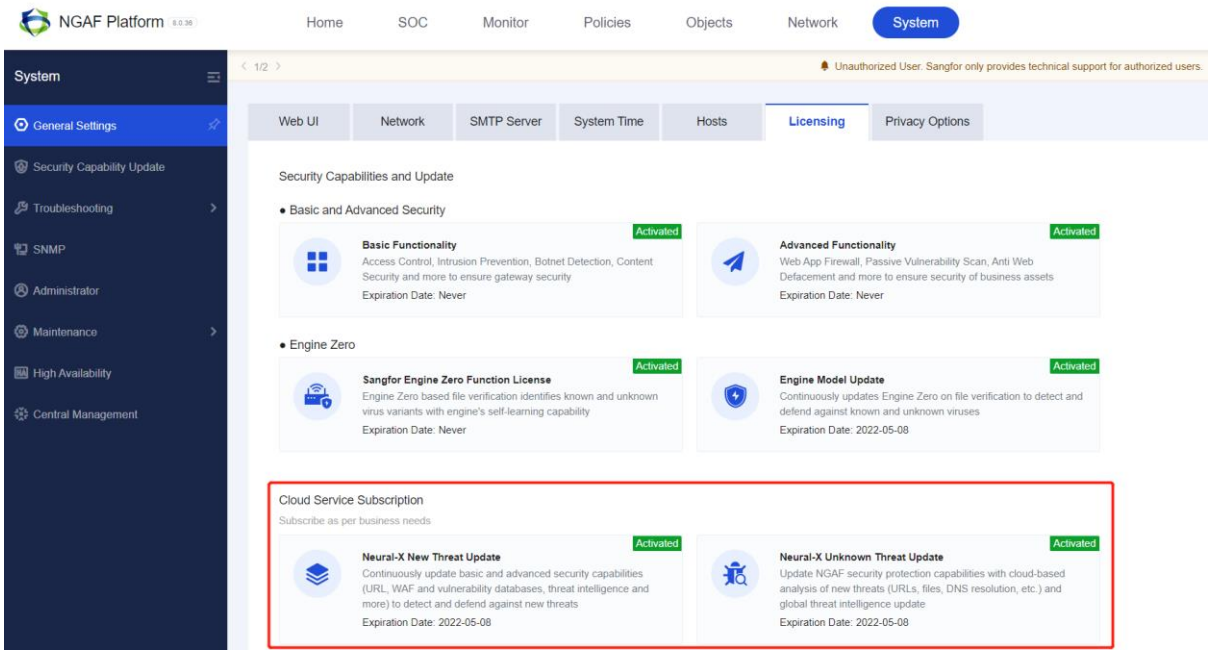
Best Practices for Configuration usually include selection of deployment mode, configuration ideas, information collection, function limitations, version differences. Regarding ***Botnet Prevention***, if you want to learn about general POC scenarios and detailed configuration steps, please refer to the following link:

https://community.sangfor.com/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=4594

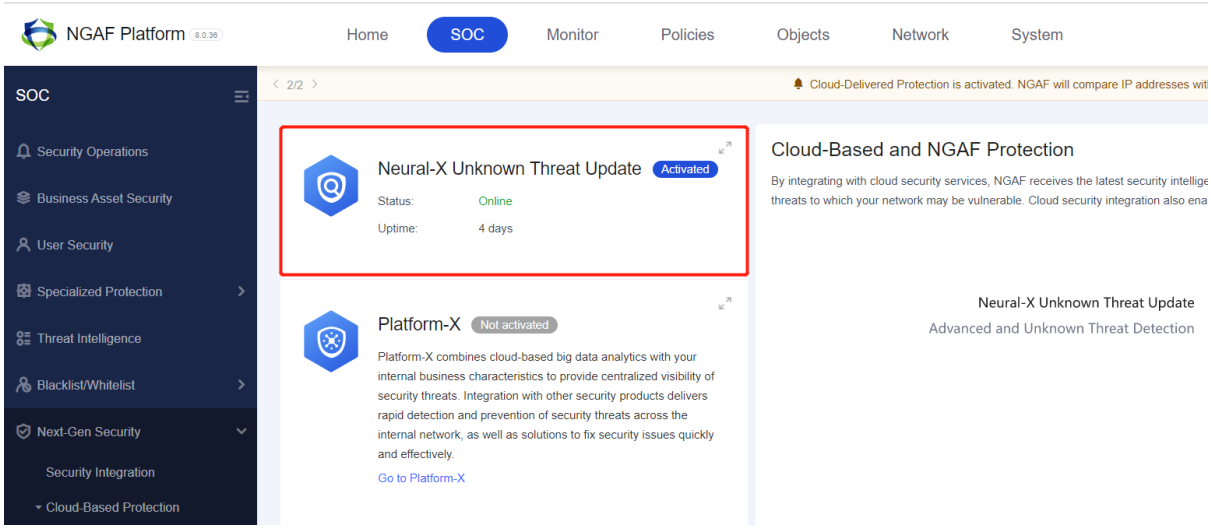
1.1 Basic

1.1.1 Confirm License and connectivity Validity

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



2. Check whether Neural-X's connectivity is normal.



1.1.2 Confirm the Topology and Traffic Direction

Check the deployment environment and network topology of NGAF, and confirm that the data flow of the source IP passes through NGAF

If there is an intranet DNS in the NGAF intranet direction: If the source IP of the botnet log is DNS IP, it may be caused by the access of the intranet computer

Whether the DNS server of the internal network is released to the outside: If the source host of the botnet log is the DNS IP, it may be generated by the external network accessing the internal DNS server

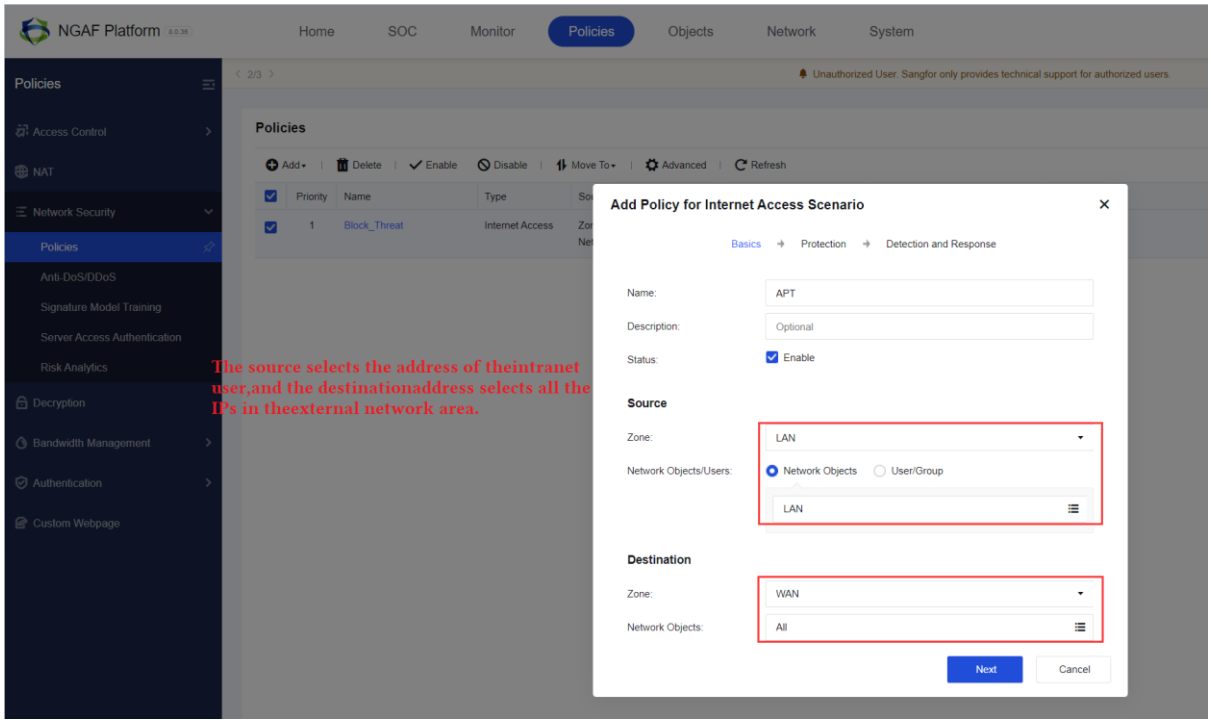
Whether there is a proxy device in the internal network: If there is an HTTP proxy device in the internal network or a device that has done SNAT, the source IP will be the internal network proxy device

Mail server: The mail server will send and receive mail on behalf of the client

1.2 Confirm the Requirements and Deployment

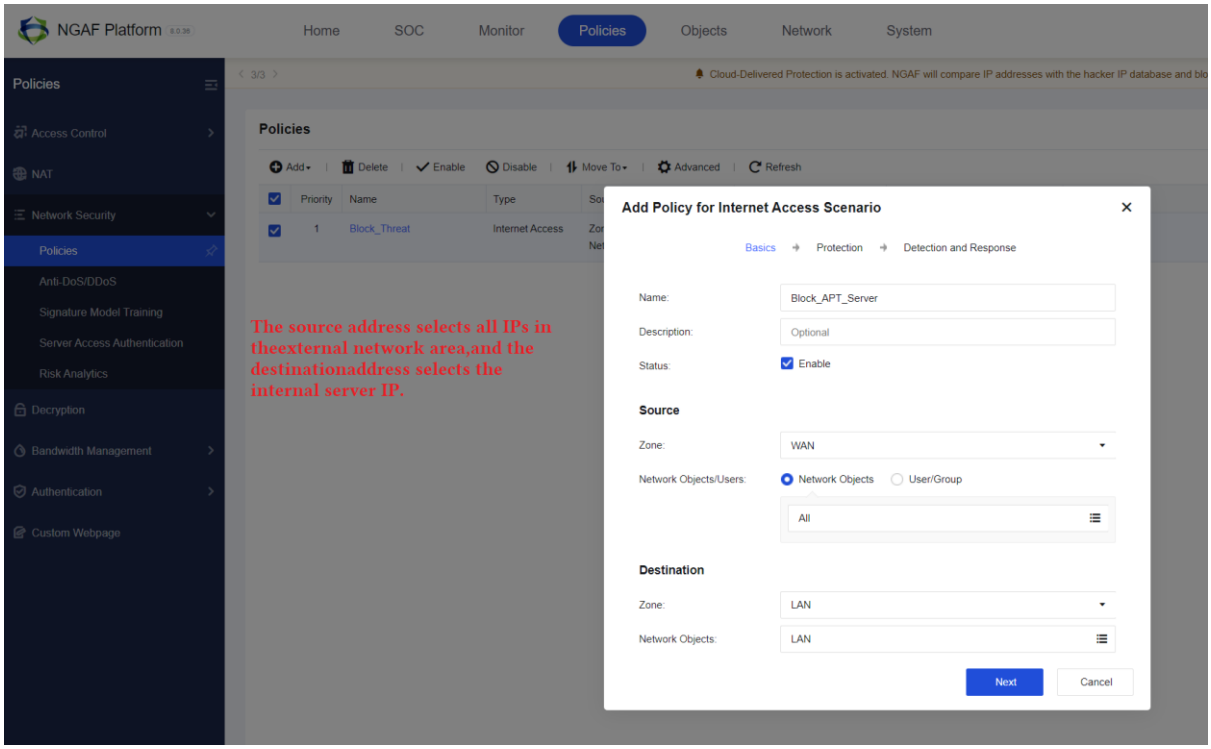
1.2.1 Host Protection

1. Host 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.



1.2.2 Server Protection

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.

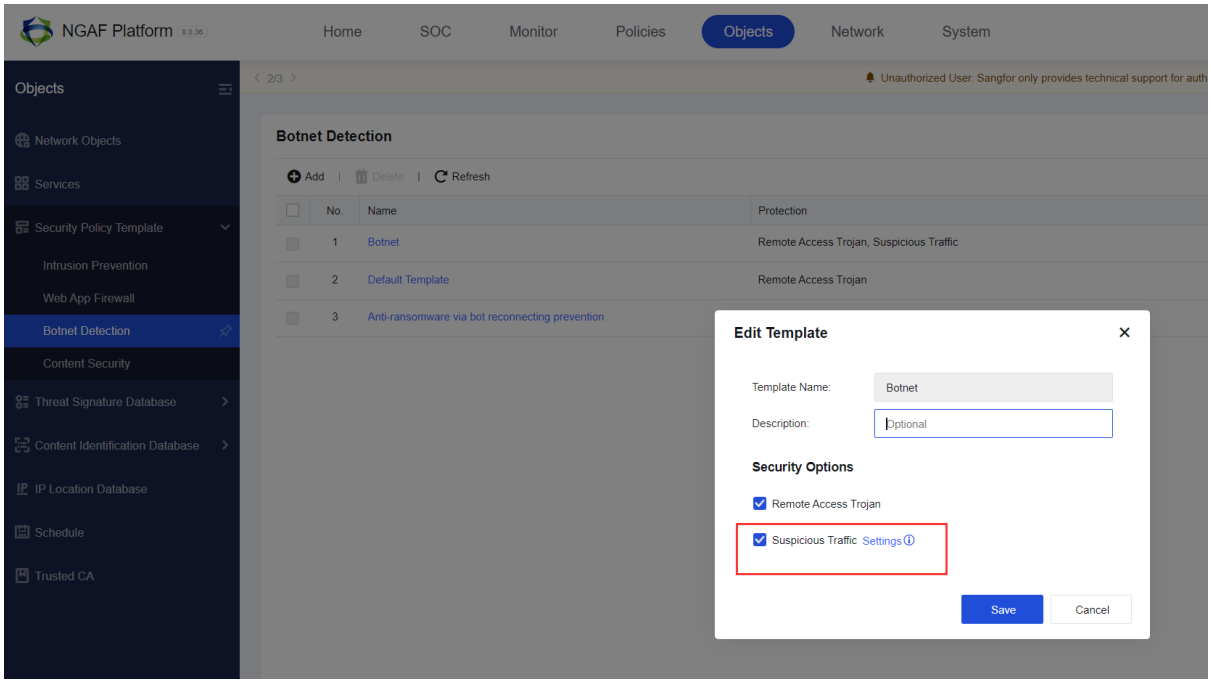


The action of the botnet policy, no matter the "Policy for Server Scenario" or "Policy for Internet Access Scenario ", the default action is "allow", if you want to turn on "Deny", you need to manually select;

The botnet function in the "Policy for Server Scenario" can automatically reverse the area selected by the policy. For example, the source selected in the "Policy for Server 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;

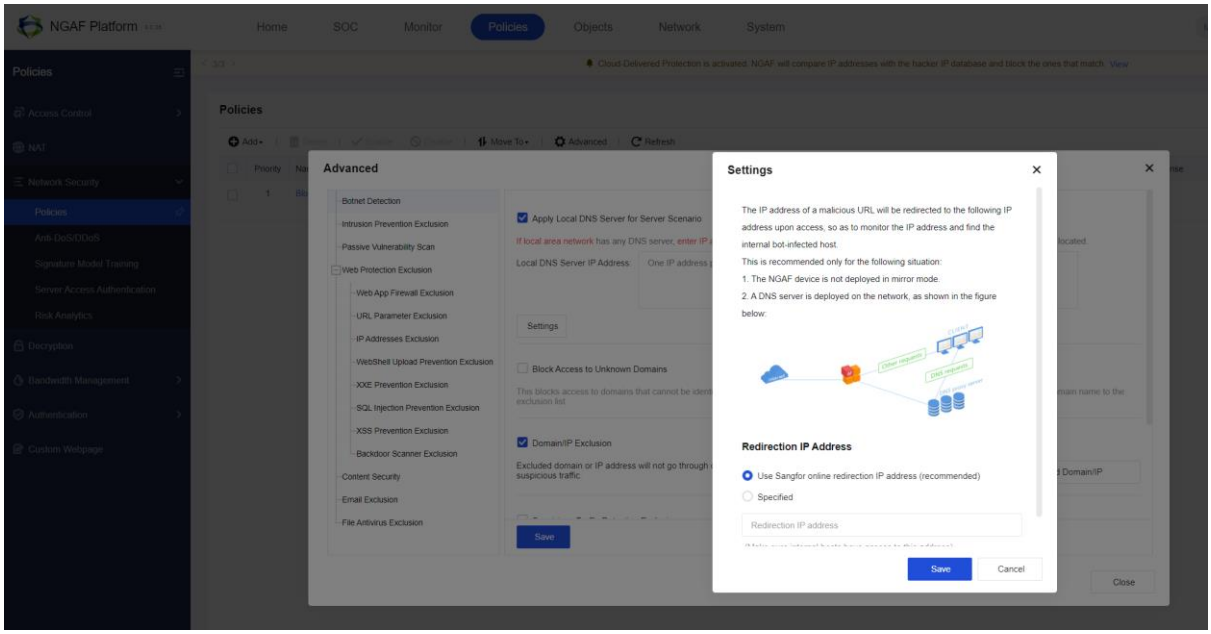
1.3 Best Practices for Configuration

1. 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.



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. For botnet URLs that have not been detected, you can go to https://wiki.sec.sangfor.com/ and https://www.virustotal.com/ to check online to ensure whether the URL is really a botnet.