SANGFOR

NGAF

Best Practices for Configuration_Integrated Coorelation & Response with Endpoint Secure

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 ***Integrated Coorelation & Response with Endpoint Secure***, 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=4599

1.1 Basic

1.1.1 About License and Capacity

1. The correlation between NGAF and Endpoint Secure does not require authorization on NGAF. Just enable authorization on Endpoint Secure.

2. NGAF can be correlated with three kinds of Endpoint Secure. Please select the linkage method according to your needs. This article is based on the most commonly used local MGR.

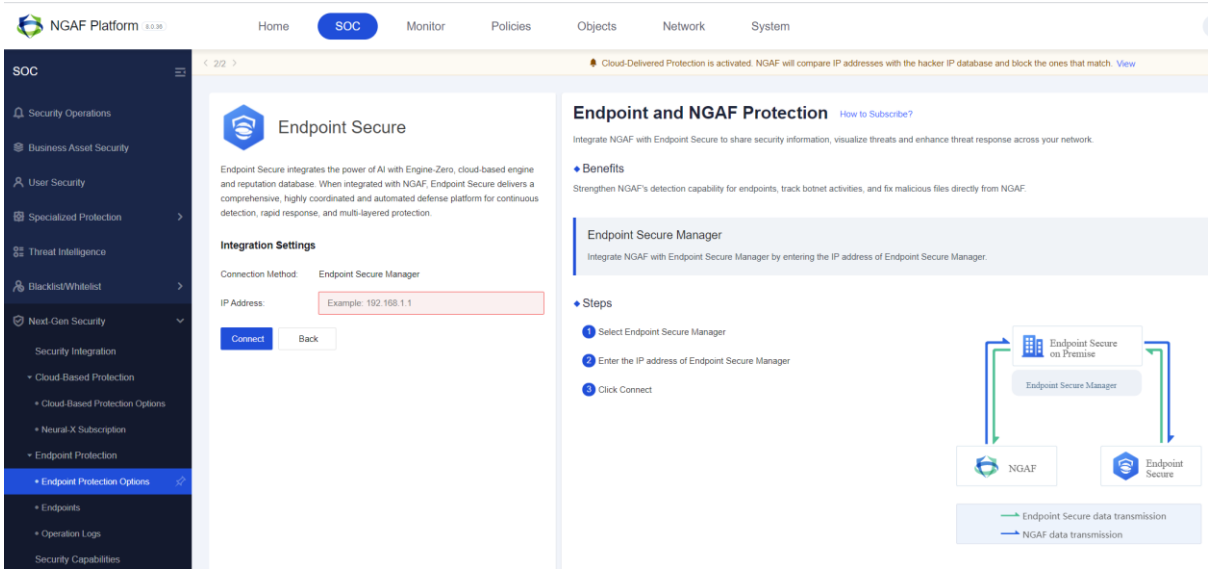
Starting from version 8.0.6, NGAF supports correlate with Local Endpoint Secure.

Starting from version 8.0.26, NGAF supports correlate with Endpoint Secure on NGAF.

Product	MGR Position	Where is Manage Page?	Applicable Scenario	Remarks
Endpoint Secure on NGAF	Cloud	NGAF	There are not enough resources to build a local MGR, and I don't want to maintain the MGR. If you don't want to manage Endpoint in the cloud, you only need to use basic scanning functions. Endpoint Secure's management page is integrated into the NGAF console.	It's simple to integrate with the NGAF page. Only main functions are included.
Endpoint Secure in Cloud	Cloud	Cloud	There are not enough resources to build a local MGR, and don't want to maintain the MGR. Able to accept Endpoint management in the cloud.	You need to log in to Platform-X and forward when managing ES Agent. This function is not available yet.
Endpoint Secure on Premises	Local	Local	Local deployment and maintenance of the MGR platform, and there are enough resources to build a local MGR.	

1.2 Confirm the Requirements and Deployment

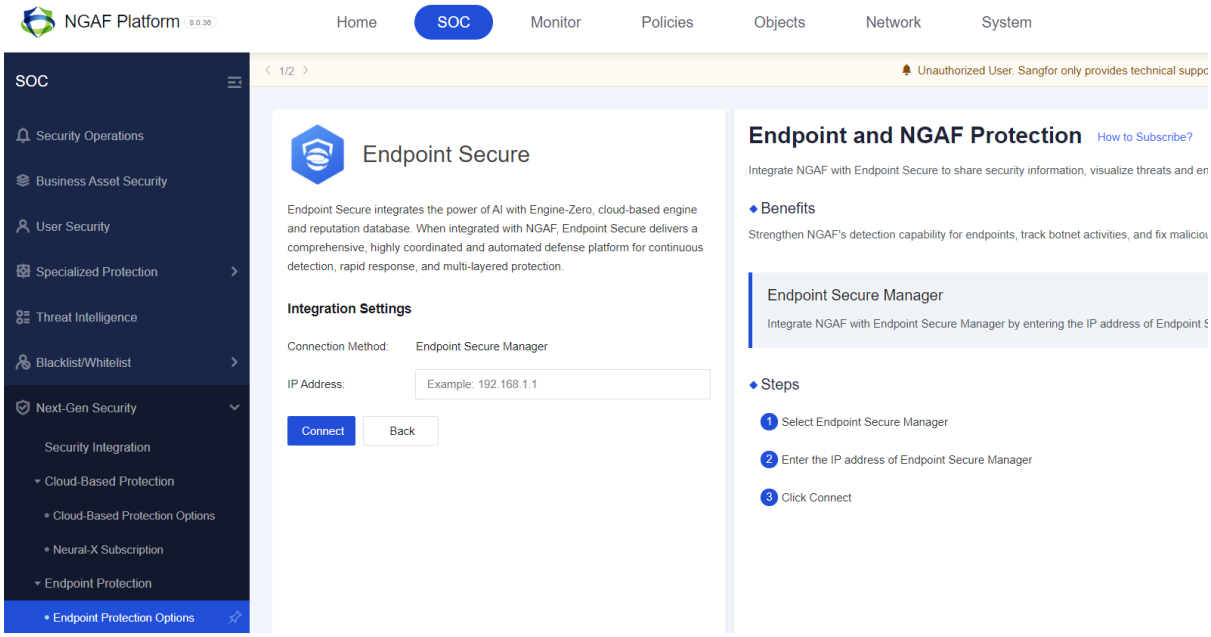
1. NGAF does not support non-443 ports used by Endpoint Secure, So please make sure that the port used by Endpoint Secure is port 443.



1.3 Best Practices for Configuration

1.3.1 Correlate NGAF with Endpoint Secure

1. For NGAF linkage, you only need to fill in the IP of the Endpoint Secure.



2. Failure to report botnet processes under NGAF- Endpoint Secure correlation. The possible reasons are listed below:

(1) It requires some time to see the result after virus samples are run. You are advised to wait half an hour and check again. NGAF reports detected botnet behaviors to Endpoint Secure at an interval instead of in real-time.

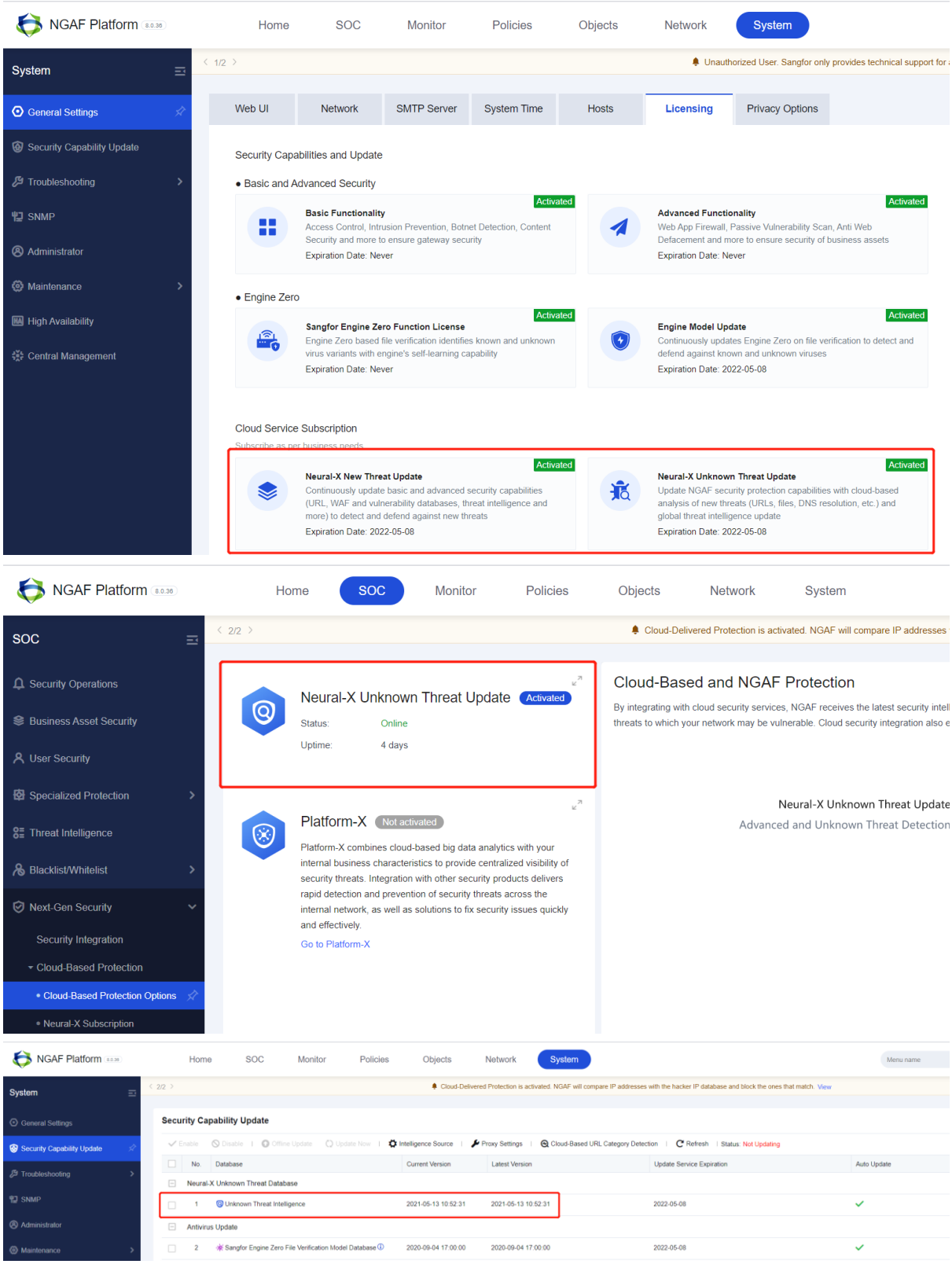
(2) Check whether the security policy is configured on NGAF, and whether the botnet detection is enabled, action set to **Allow** (not to **Deny**), and **Log event** checked.

1.3.2 Configure Security Policy in NGAF

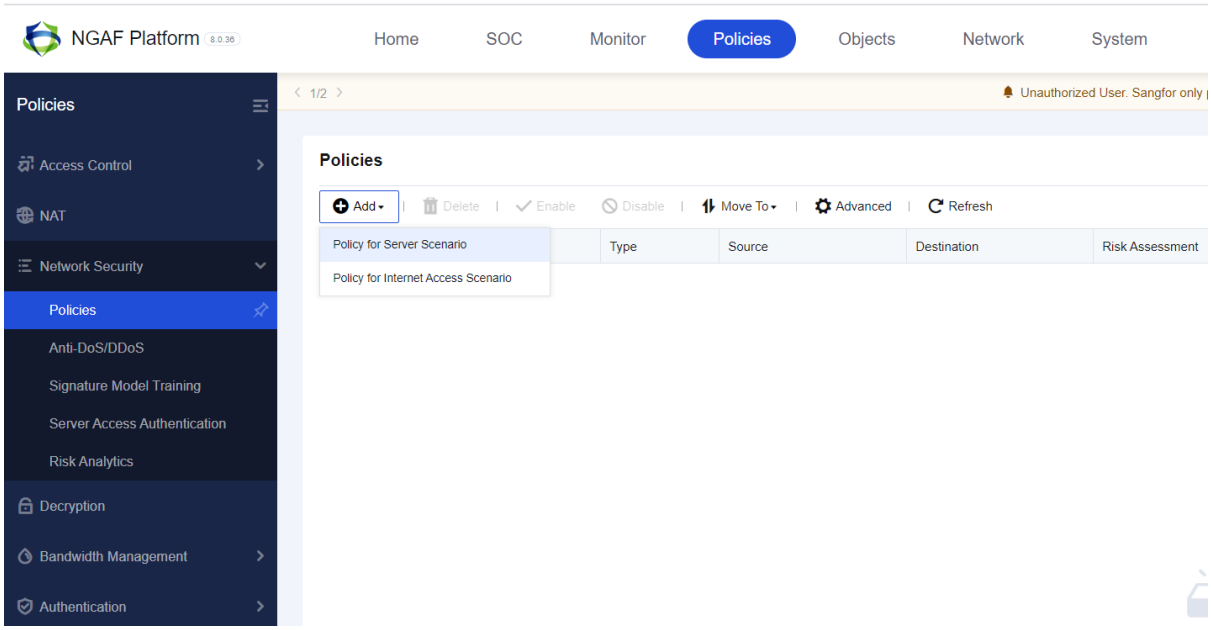
1. Only when NGAF detects a threat event can Endpoint Secure scan the endpoint's disk. Therefore, security policies must be configured on NGAF to ensure that NGAF can detect threats.

2. In order to ensure that NGAF has good threat detection capabilities, please ensure that NGAF has

enabled Neural-X Unknown Threat Update license and can access the Internet normally to update the latest threat intelligence.



3.Enable botnet detection for the **Policy for Server Scenario** and the **Policy for Internet Access Scenario**. Choose action **Deny** and check **Log event**, as shown below:



1.3.3 No Threat Detected

1.Failure to detect any virus under NGAF- Endpoint Secure correlation for virus-killing. The possible reasons are listed below:

(1) Verify that virus samples run in the quick killing directory. NGAF correlates with Endpoint Secure to issue the virus-kill task in quick killing mode instead of global killing mode. The quick killing mode only scans **/windows** and **/windows/system32**, as well as **/windows/system32/drivers** and its sub-directories.

2. NGAF does not detect any risky host. The possible reasons are listed below:

(1) Check whether all virus samples are run. Multiple virus samples are provided, and all these samples should be run.

(2) **Check whether the security policy is configured on NGAF**, and whether the botnet detection is enabled, action set to **Allow**, and **Log event** checked.

(3) Check whether the DNS resolution traffic and network traffic of the tested PC pass NGAF. The network traffic of the tested PC needs to pass NGAF.