



# NGAF

## Best Practices for Configuration\_Botnet Prevention

Version 8.0.35



## Log Perubahan

Tanggal	Deskripsi Perubahan
6 Mei 2021	Rilis dokumen.
17 Mei 2021	Pembaruan dokumen.

# DAFTAR ISI

Chapter 1 Konfigurasi Dasar.....	错误!未定义书签。
1.1 Dasar .....	1
1.1.1 Konfirmasi Lisensi dan Validitas Konektivitas .....	1
1.1.2 Konfirmasi Topologi and Pengarahan Traffic.....	2
1.2 Konfirmasi Persyaratan dan Deployment.....	2
1.2.1 Proteksi Host.....	2
1.2.2 Proteksi Server.....	3
1.3 Praktik yang Disarankan untuk Konfigurasi .....	4

# Bab 1 Konfigurasi Dasar

Dokumen terkait:

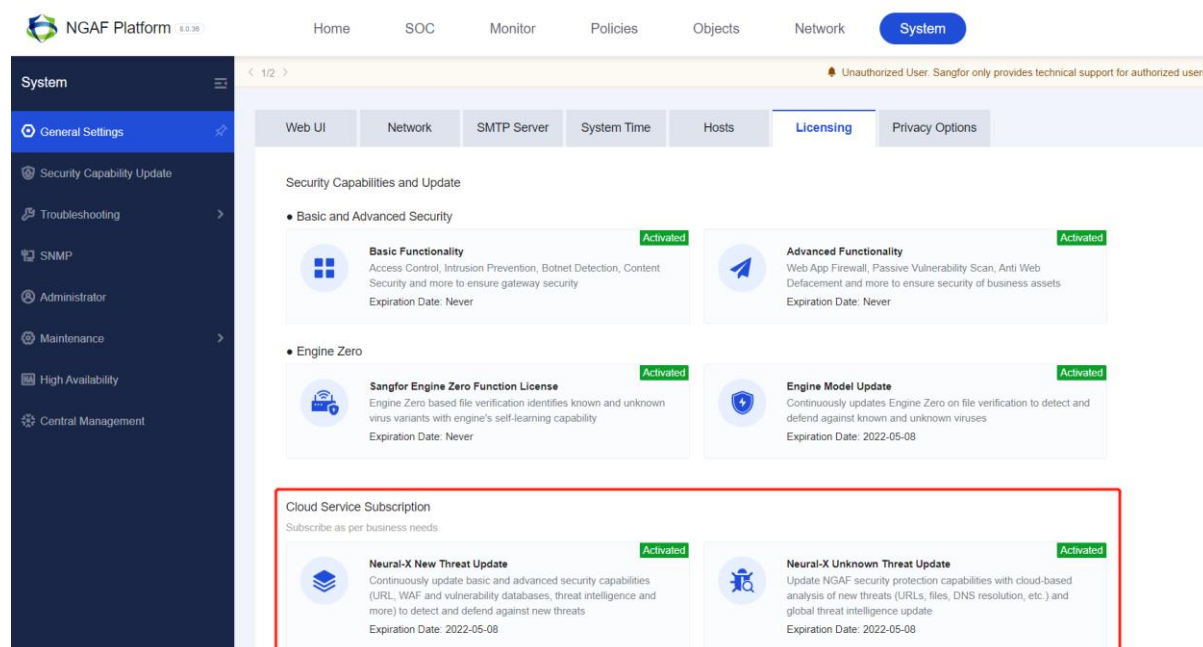
Praktik Terbaik untuk melakukan konfigurasi biasanya mencakup pemilihan mode deployment, ide konfigurasi, pengumpulan informasi, batasan fungsionalitas, perbedaan versi. Mengenai **Pencegahan Botnet**, jika anda ingin mempelajari skenario POC umum dan langkah-langkah konfigurasi terperinci, silakan merujuk ke tautan berikut:

<https://sangforltd.sharepoint.com/:w/s/PMO/EW03kzit4TNEMLXBJjig1HcBIWhppn9RFAG-QuzE64qPvw?e=BJI4Js>

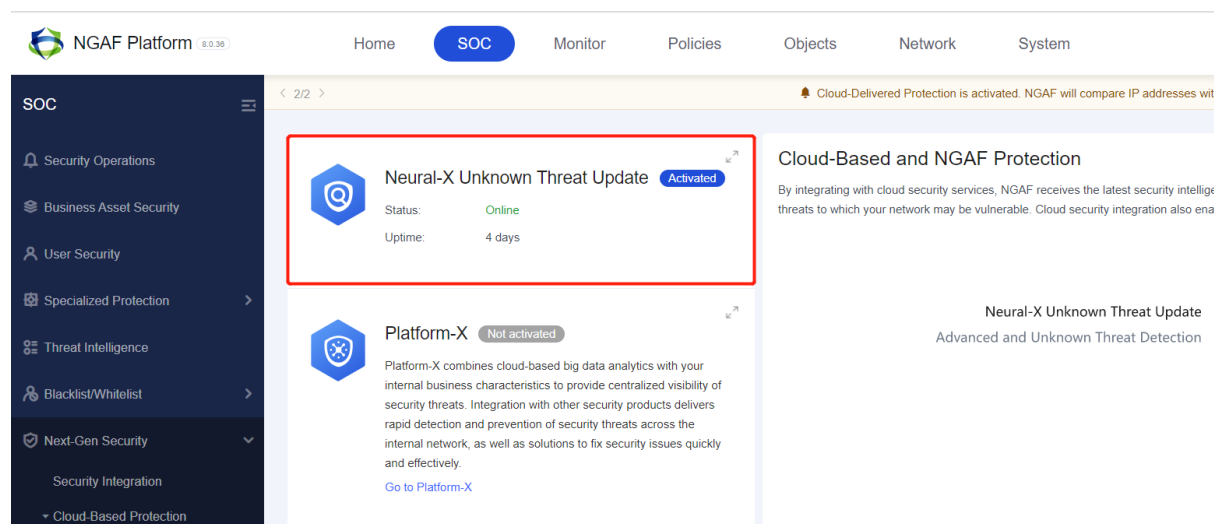
## 1.1 Dasar

### 1.1.1 Konfirmasi Lisensi dan Validitas konektivitas

1. Periksa lisensi untuk memastikan bahwa lisensi Fungsi Dasar diaktifkan pada perangkat.



2. Periksa jika konektivitas Neural-X normal.



### 1.1.2 Konfirmasi Topologi dan Arah Traffic

Periksalah pada lingkungan penerapan dan pada topologi jaringan NGAF, dan berikan konfirmasi bahwa aliran data dari IP sumber telah melewati NGAF.

Jika ada DNS intranet di arah NGAF intranet: Jika IP sumber log botnet adalah IP DNS, kemungkinan disebabkan oleh akses komputer intranet.

Apabila server DNS dari jaringan internal dilepaskan ke luar: Jika host sumber log botnet adalah IP DNS, itu mungkin dihasilkan oleh jaringan eksternal yang mengakses server DNS internal.

Apabila ada perangkat proxy di jaringan internal: Jika ada perangkat proxy HTTP di jaringan internal atau perangkat yang telah melakukan SNAT, IP sumber akan menjadi perangkat proxy jaringan internal.

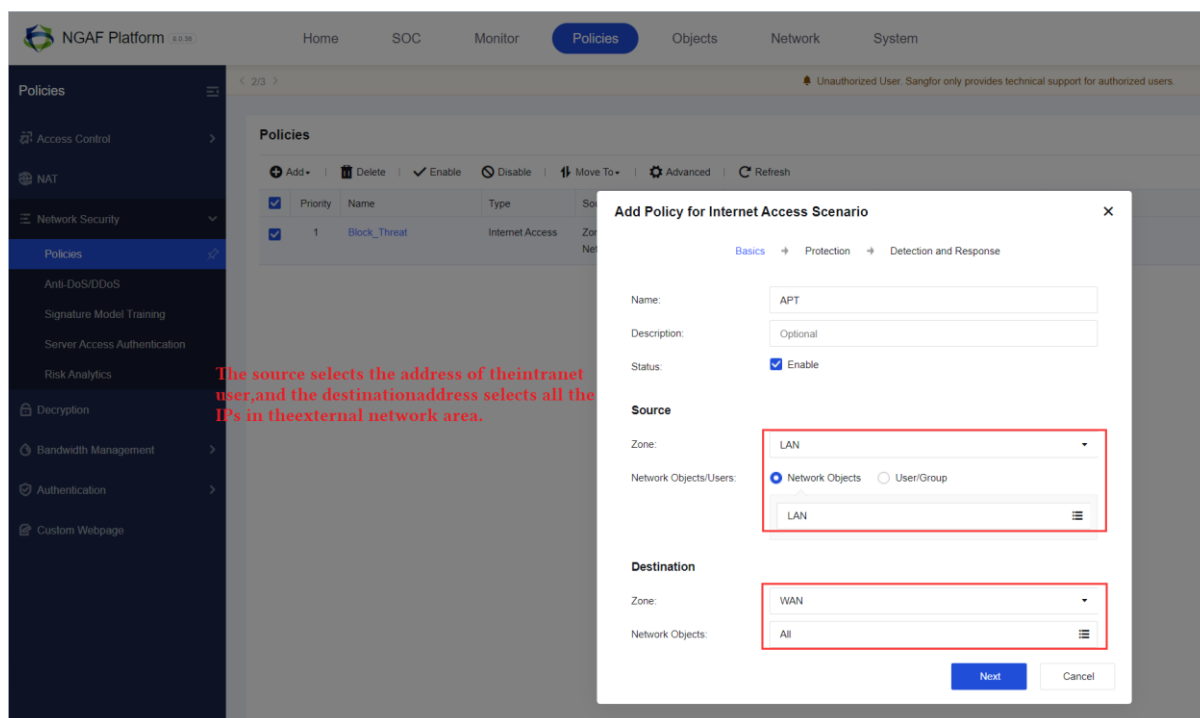
Server email: Server email akan mengirim dan menerima email atas nama klien.

## 1.2 Konfirmasi Persyaratan dan Deployment

### 1.2.1 Proteksi Host

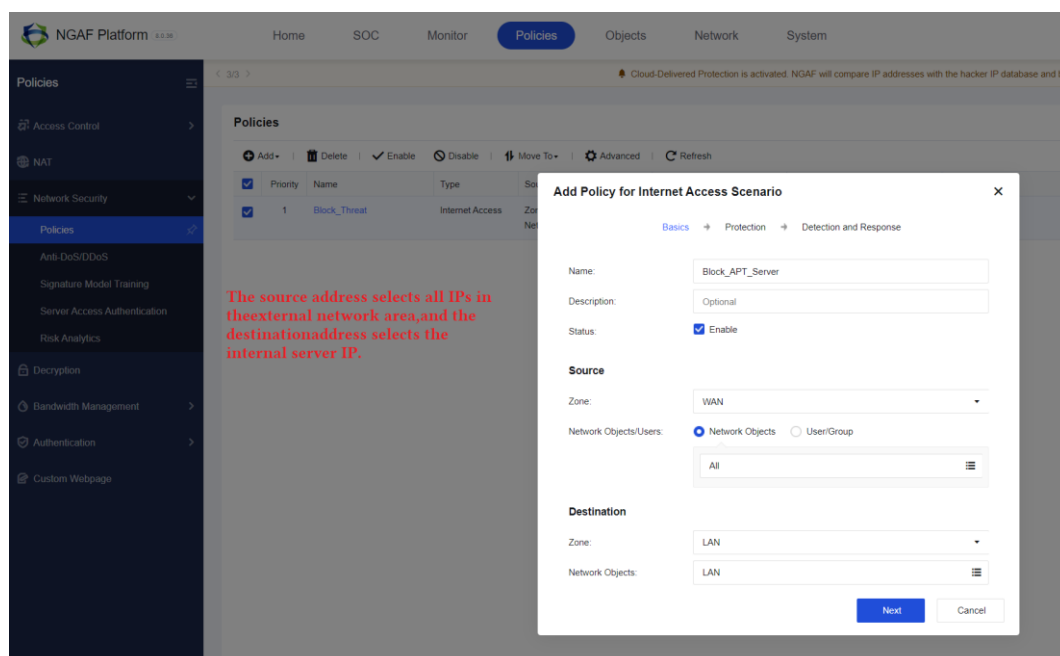
1. Rekomendasi Proteksi Host Policy. Menambahkan policy dan selection area, arah pemilihan proteksi Endpoint perlu memperhatikan source area adalah area jaringan internal, destination area adalah area jaringan publik.

## Konfigurasi Pencegahan Botnet Praktik yang Disarankan



### 1.2.2 Proteksi Server

2. Rekomendasi Proteksi Server Policy. Menambahkan policy area dan selection area sangat diperlukan. Arah proteksi server perlu diperhatikan bahwa source area adalah external network dan destination area adalah internal network area.



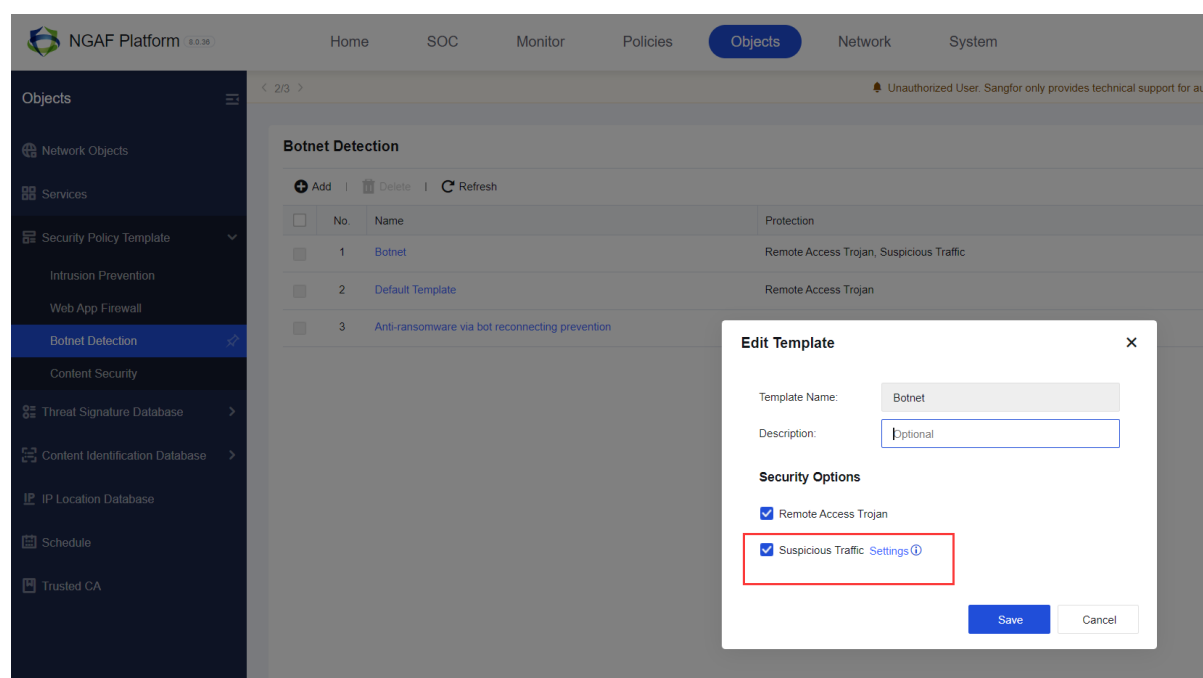
Tindakan default dalam kebijakan botnet, baik "Policy for Server Scenario" atau "Policy for Internet Access Scenario" adalah "Allow". Jika Anda ingin mengaktifkan "Deny", maka Anda harus memilih secara manual;

## Konfigurasi Pencegahan Botnet Praktik yang Disarankan

Fungsi botnet dalam "Policy for Server Scenario" dapat secara otomatis membalikkan area yang dipilih oleh kebijakan. Misalnya, source yang dipilih dalam "Policy for Server Scenario" umumnya adalah area jaringan eksternal, dan destination area adalah area jaringan internal. Terakhir, untuk identifikasi dan pemrosesan botnet, source-nya adalah internal network area dan targetnya adalah external network area;

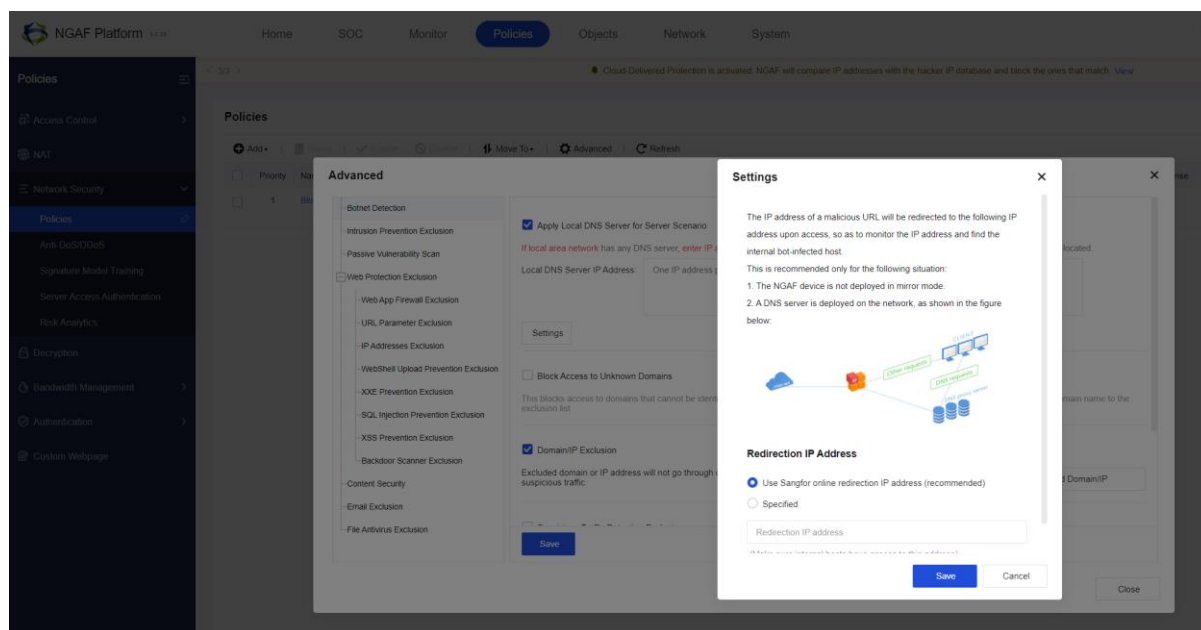
### 1.3 Praktik yang Disarankan untuk Konfigurasi

1. Fungsi "Suspicious Traffic" dari botnet adalah dengan tidak membatasi perilaku yang telah terdeteksi, dan hanya mencatat, dan pada saat yang sama merekam paket data asli untuk keterlacakannya nanti.

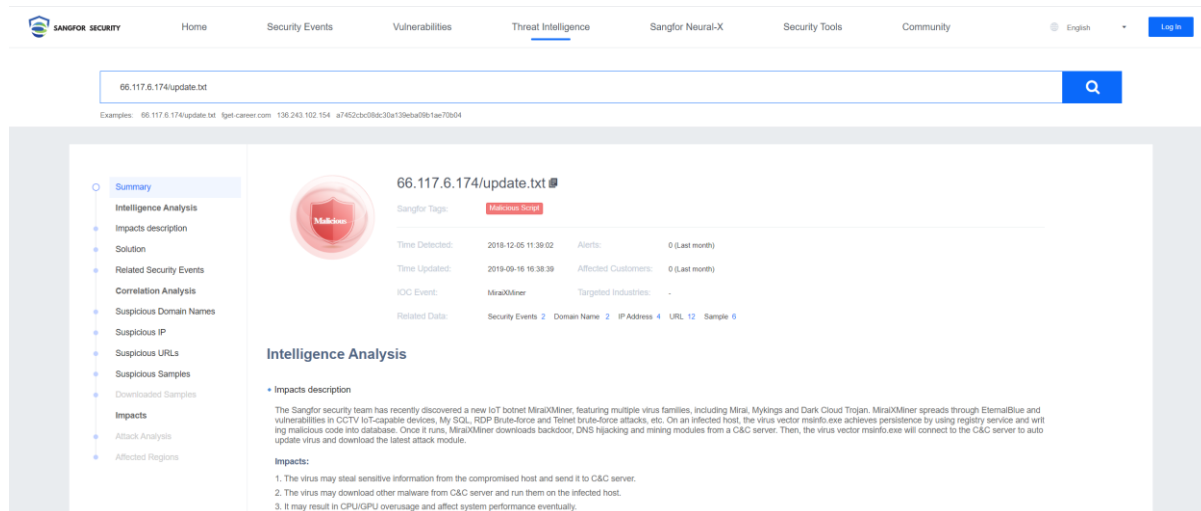


Catatan: Jika ada server DNS di intranet dan endpoint intranet menggunakan DNS intranet untuk resolusi nama domain, teknologi "Honeypot" harus diaktifkan. Arahkan ulang permintaan DNS berbahaya, atur seperti yang ditunjukkan di bawah ini:

## Konfigurasi Pencegahan Botnet Praktik yang Disarankan



2. Untuk URL botnet yang belum terdeteksi, Anda dapat mengunjungi <https://wiki.sec.sangfor.com/> dan <https://www.virustotal.com/> untuk memeriksa secara daring apakah URL tersebut benar-benar botnet.







**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