



NGAF

Pedoman terbaik untuk Skenario Botnet Prevention

Versi 8.0.17



Data Perubahan

Tanggal	Keterangan Perubahan
June 15, 2020	Rilis Dokumen
Mar 18, 2021	Pembaruan Dokumen
May 17, 2021	Pembaruan Dokumen

DAFTAR ISI

BAB 1 Skenario	1
1.1 Perkenalan Fungsi	1
1.2 Pengujian URL.....	1
BAB 2 Pedoman yang disarankan	1
2.1 Rekomendasi Policy Proteksi pada Endpoint.....	3
2.2 Rekomendasi Policy Proteksi pada Server	4
Chapter 3 Perhatian.....	5

BAB 1 Skenario

1.1 Perkenalan Fungsi

Piranti anti-virus dan firewall pada umumnya memiliki keterbatasan efektifitas dalam mendeteksi trojan. Pada skenario APT (Advanced Persistent Threat), Antivirus dan Firewall biasa memiliki tingkat deteksi dan pertahanan yang lemah. Oleh sebab itu, sistem pendeteksi secara dini diperlukan untuk mendeteksi dan mengenali mesin yang terinfeksi untuk memperkecil resiko yang terjadi pada komputer pengguna. Pada saat yang sama, sejarah dari data perubahan sangat penting untuk melakukan penelusuran.

1.2 Pengujian URL

Anda dapat menguji melalui URL berikut:

ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

v.beaahh.com

aqhln.ws

mlmy.3322.org

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

clptiiybpip.cn

task.attendecr.com

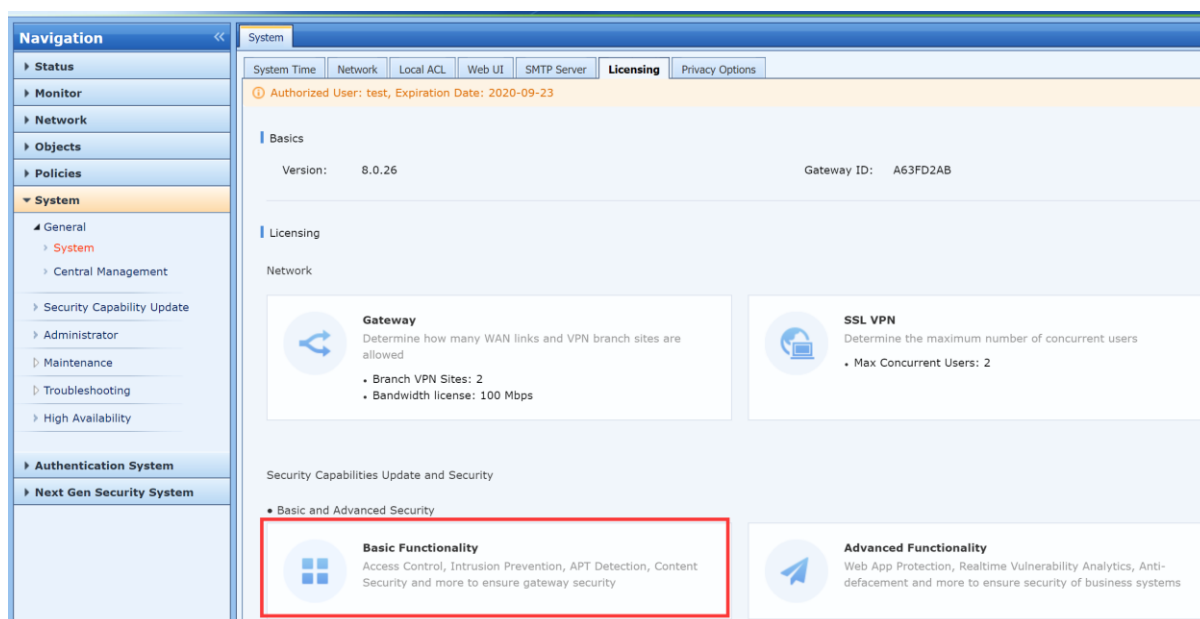
bddp.net

cqogflio.cn

BAB 2 Pedoman yang disarankan

Lakukan pengecekan lisensi untuk memastikan Fungsi lisensi telah diaktifkan pada perangkat.

Botnet Prevention



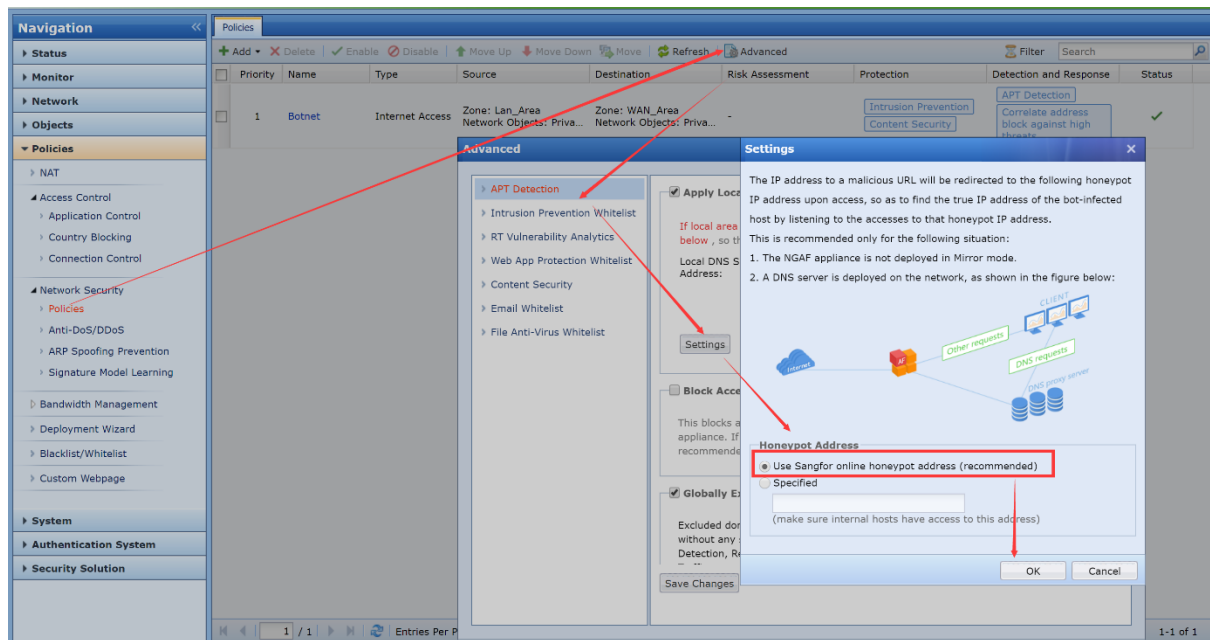
Pastikan database telah diperbarui hingga pembaruan terbaru.

The screenshot shows the 'Security Capability Update' configuration page. The table below lists the databases and their update status.

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	✓	Update Interval: 5 minutes
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	✓	Update Interval: 1 month
Neural-X New Threat Databases						
3	URL Database	2020-06-16 09:00:00	2020-06-16 09:00:00	2020-09-23	✓	Update Interval: 14 days
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	✓	

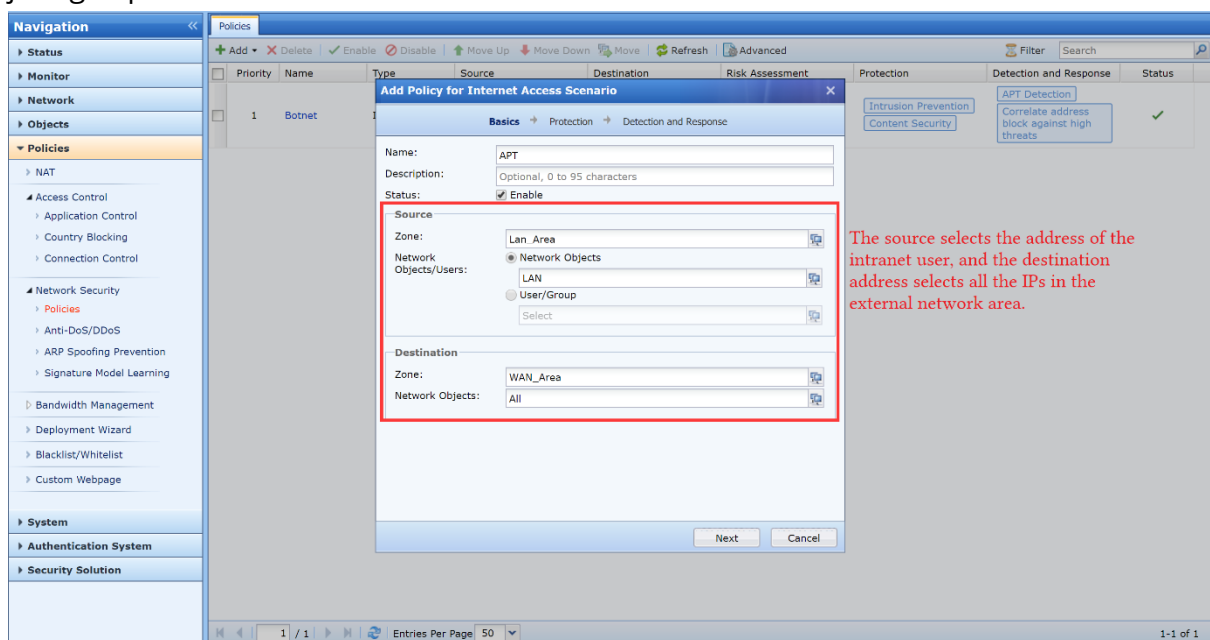
Proteksi Botnet direkomendasikan untuk server dan workstation, keduanya memiliki resiko terinfeksi yang sama.

Catatan Penting: Jika memiliki DNS server dalam intranet dan pengguna intranet menggunakan DNS dari intranet untuk nama domain yang digunakan, "Honeypot" adalah teknologi yang harus di aktifkan. Meneruskan permintaan DNS dengan cara sebagai berikut dibawah ini:

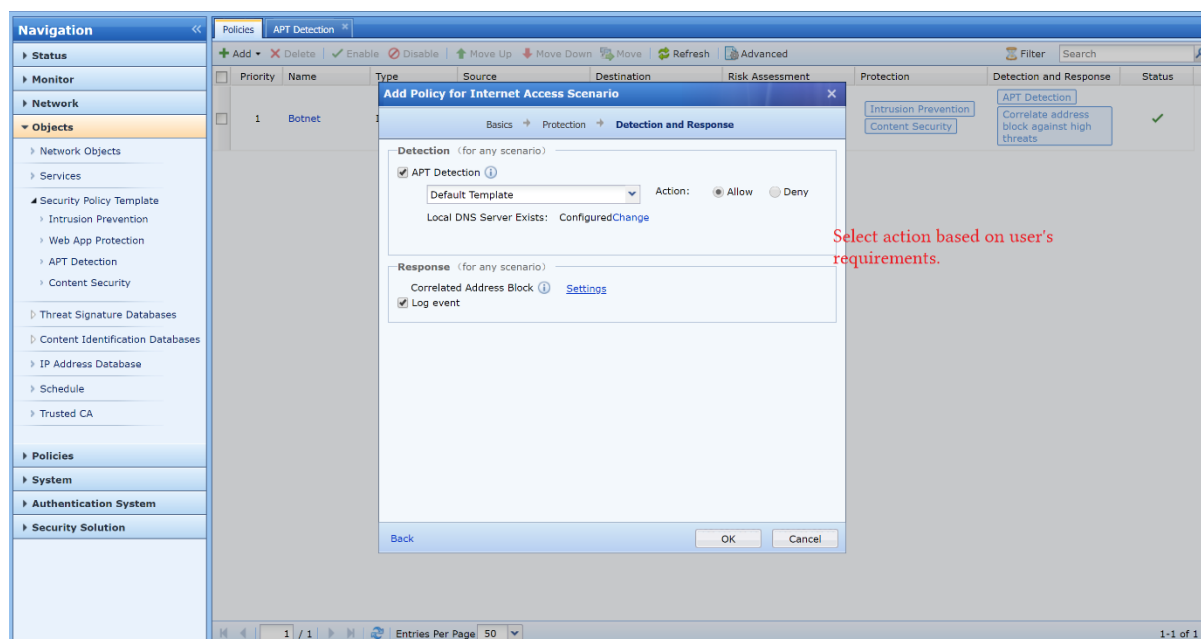


2.1 Rekomendasi Policy Proteksi pada Endpoint

Tambahkan area dan policy, Proteksi Enpoint dibutuhkan memilih arahan untuk memperhatikan area asal adalah area internal jaringan, area tujuan adalah area jaringan publik.

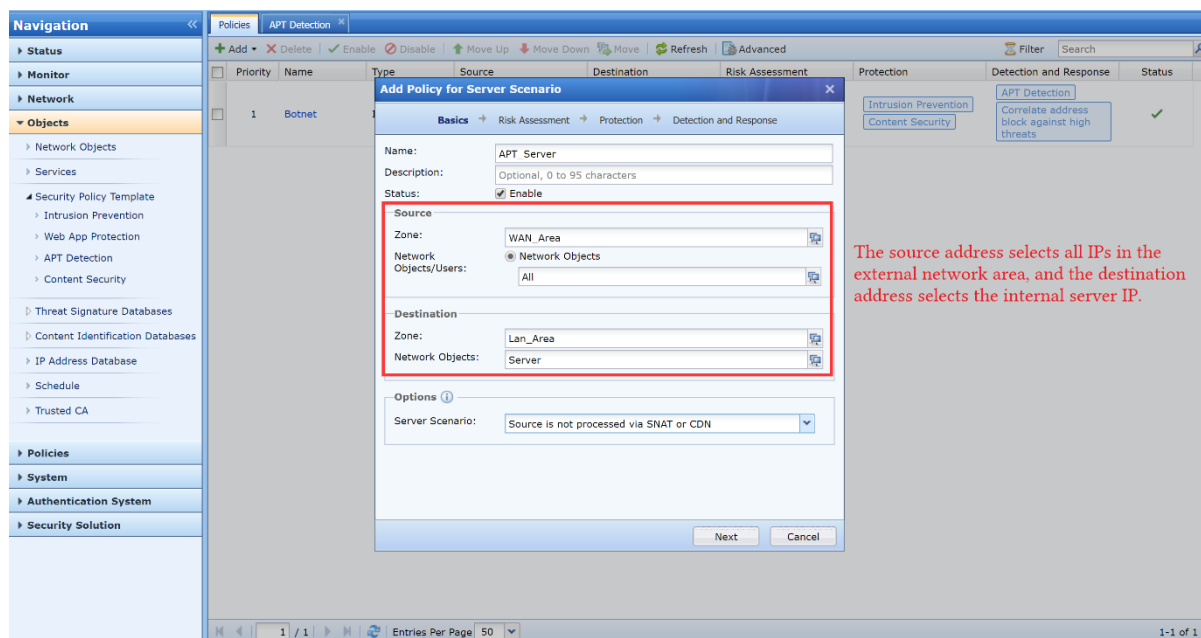


Untuk mengaktifkan fungsi botnet, gunakan "Default template" untuk policynya dan "Deny" untuk aksi sebagai kebutuhan melakukan pertahanan yang dibutuhkan.

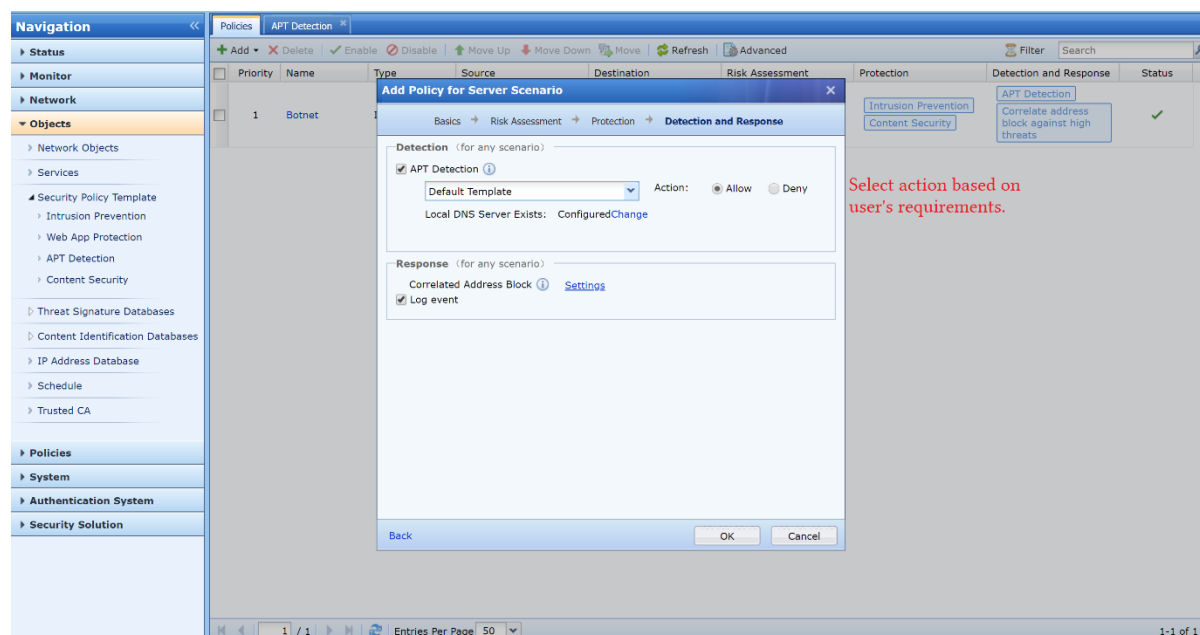


2.2 Rekomendasi Policy Proteksi pada Server

Tambahkan policy dan pilih area yang diperlu diproteksi. Proteksi Server dibutuhkan memilih arahan untuk memperhatikan area asal adalah area internal jaringan, area tujuan adalah area jaringan publik.



Untuk mengaktifkan fungsi botnet, gunakan "Default template" untuk policynya dan "Deny" untuk aksi sebagai kebutuhan melakukan pertahanan yang dibutuhkan.

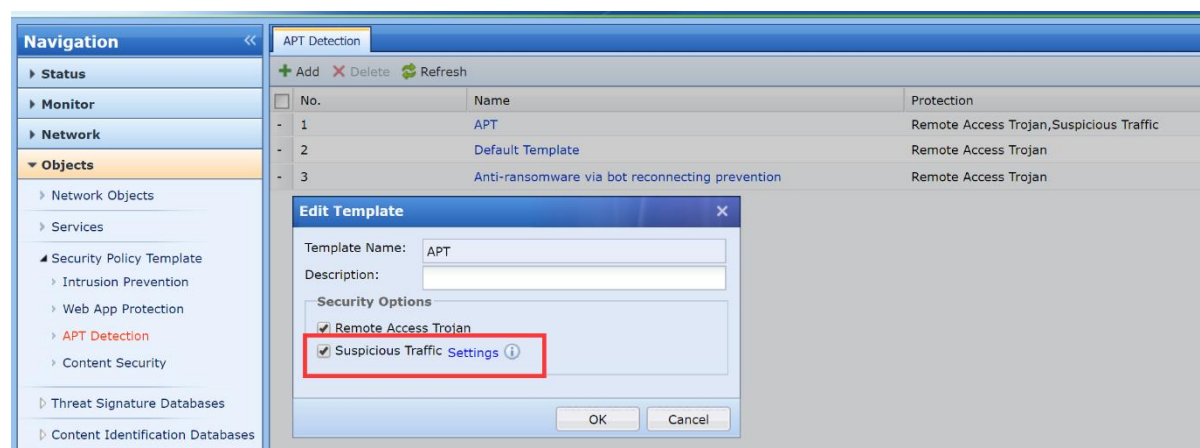


Chapter 3 Perhatian

Aksi dari policy botnet, Skenario akses untuk "Policy for Server Scenario" atau "Policy for Internet Access Scenario", pada dasarnya adalah "allow", jika anda ingin merubahnya menjadi "Deny", anda perlu memilihnya secara manual;

Fungsi botnet dalam "Policy for Internet Access Scenario" dapat secara otomatis tersedia pada area yang telah dipilih melalui policy. Contohnya, area yang dipilih dalam "Policy for Internet Access Scenario" adalah semua external network area, dan tujuan area adalah internal network area. Tujuannya untuk mengidentifikasi dan proses dari botnet, sumber adalah internal network area dan yang menjadi target adalah external network area;

Fungsi "Suspicious Trafik" dari botnet tidak melakukan blok terhadap perlakuan yang tidak biasa, ia hanya melakukan diteksi, dan hanya menyalinnya dalam log dan pada saat yang sama pencatatan paket data original untuk nantinya dilakukan penelusuran.





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