



SANGFOR



NGAF

Pedoman terbaik untuk Skenari_Unknown Threat Prevention By Engine Zero & Neural-X

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 Penjelasan Fungsi.....	1
1.2 Skenario:	1
1.3 Alat Pengujian	1
BAB 2 Rekomendasi Pedoman	1

BAB 1 Skenario

1.1 Penjelasan Fungsi

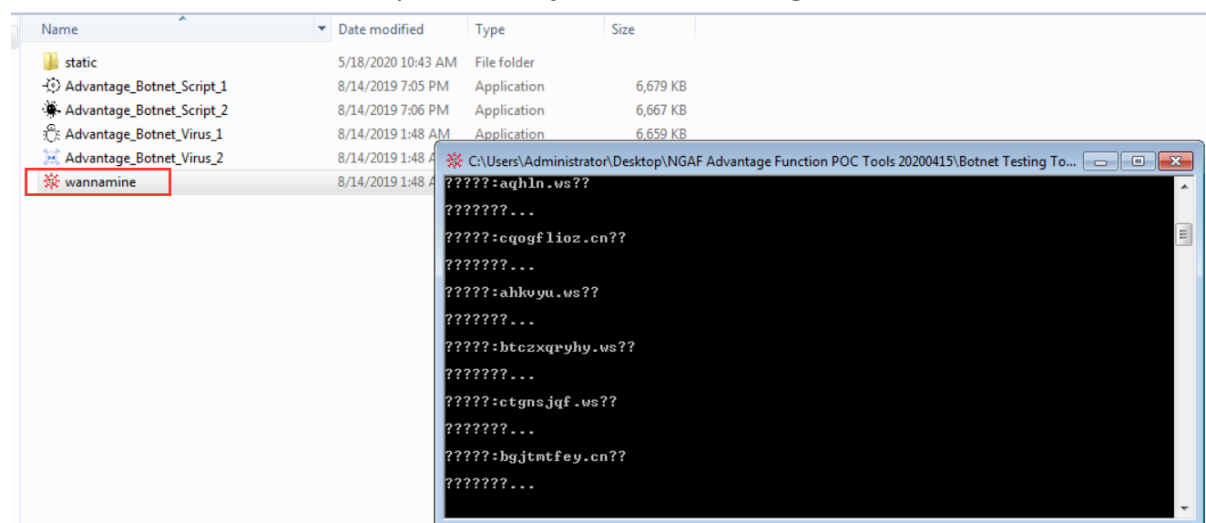
Neural-X adalah kontrol keamanan berbasis di cloud, yang mampu mengumpulkan dan menganalisa peristiwa keamanan secara keseluruhan, dan mampu mengidentifikasi ancaman yang tidak dikenali. Engine dari Sangfor Zero menggunakan kemampuan analisa yang kuat untuk menganalisa virus yang tidak dikenal.

1.2 Skenario:

Gunakan NGAF untuk menghubungkan Neural-X yang untuk melindungi keamanan jaringan pelanggan.

1.3 Alat Pengujian

1. Untuk menguji Botnet, anda dapat menggunakan **SANGFOR_NGAF_v8.0.17_Best Practice_Unknown Threat Prevention By Engine Zero & Neural-X.7z**, cari di PMO. Jalankan wannamine.exe di PC, wannamine.exe akan mencoba menggunakan DNS untuk mencari URL dari Botnet, tetapi sebenarnya tidak akan mengakses URL dari Botnet...



2. Ketika anda menjalankan program, mungkin akan terjadi kesalahan terkait api-ms-win-crt-runtime-l1-1-0.dll, Jadi disarankan untuk mengunduh **Visual C++ Redistributable Runtimes All-in-One** dan menginstall semua yang berkaitan dengan Visual C runtime libraries.

Catatan: Sistem Operasi yang berbeda akan muncul kesalahan yang berbeda. Anda dapat mencari solusi tersebut di Internet, akan tetapi biasanya kasus kesalahan tersebut adalah file Visual C Runtimes yang hilang.

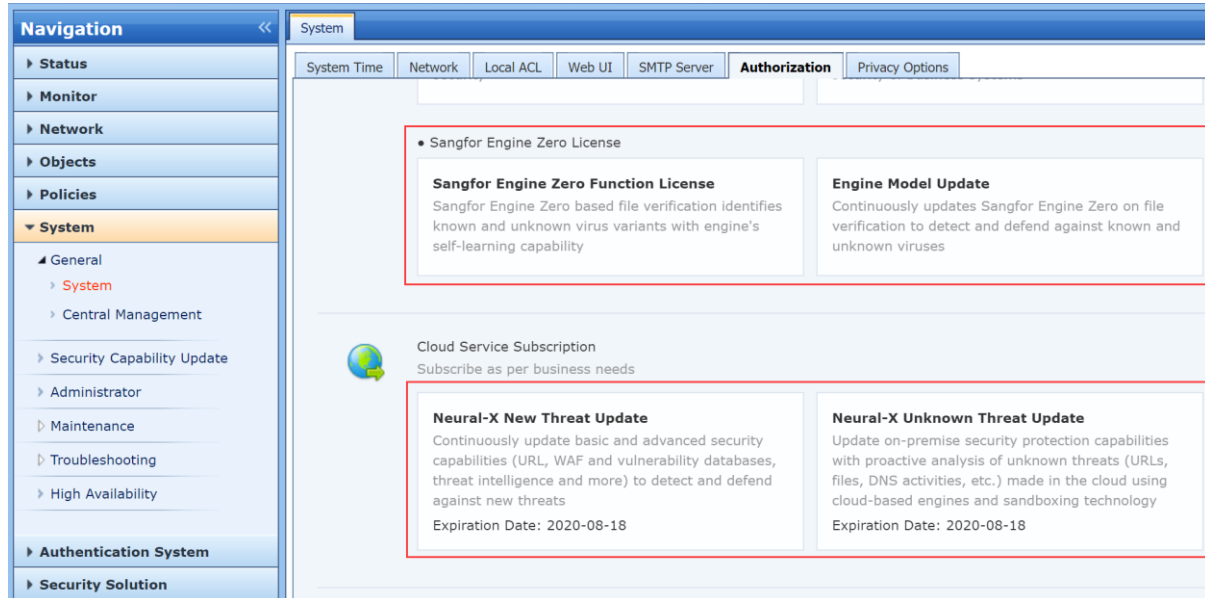
BAB 2 Rekomendasi Pedoman

Skenario:

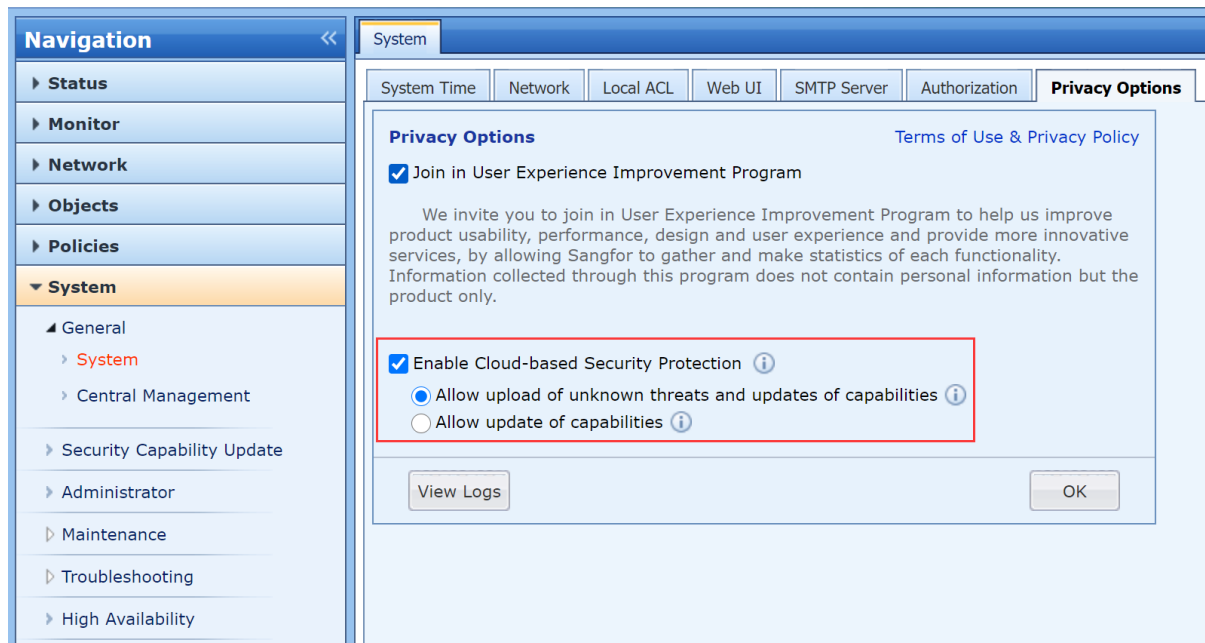
Pelanggan perusahaan manufaktur telah diserang oleh peretas untuk waktu yang lama, dan untuk ancaman yang tidak diketahui, firewall pelanggan sebelumnya tidak bekerja efektif untuk mengidentifikasi dan mencegahnya, dan pelanggan ingin menggunakan Sangfor NGAF untuk menangani ancaman yang tidak dikenal ini.

Konfigurasi:

1. Pastikan lisensi dari Neural-X dan Sangfor Zero Engine masih berlaku.

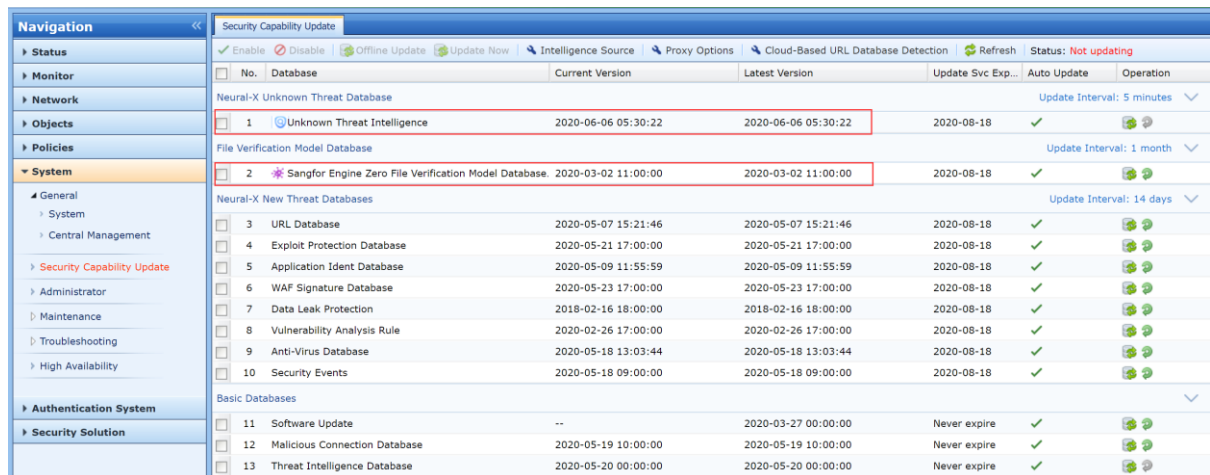


2. Pastikan Cloud-based Security Protection telah diaktifkan.



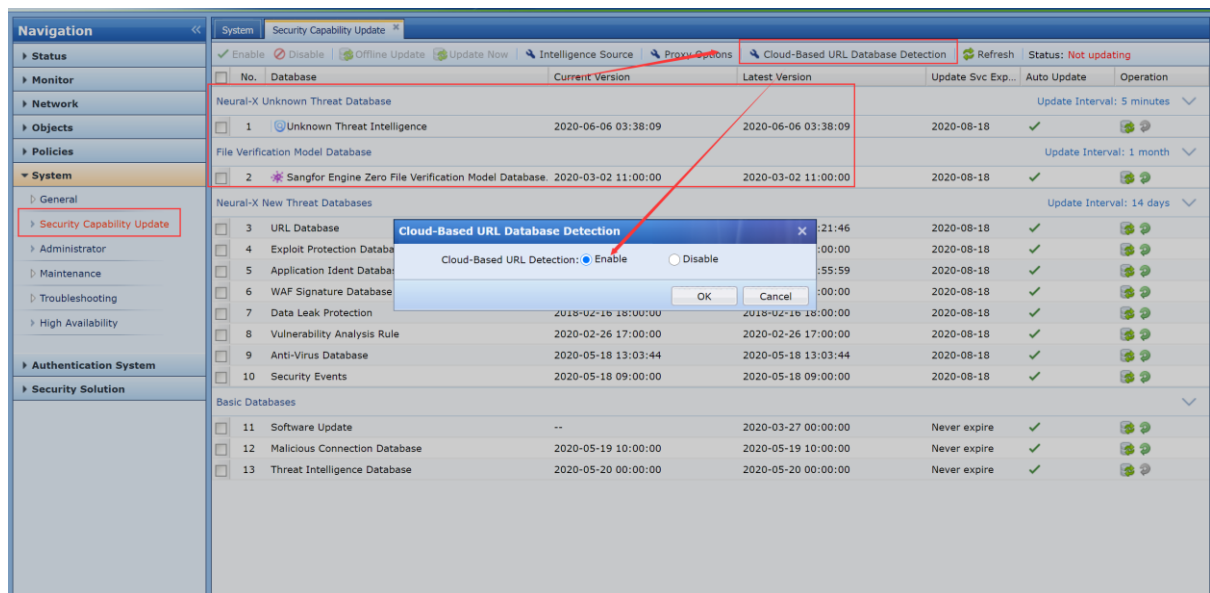
3. Pastikan unknown threat Intelligence database, Sangfor Zero Engine model, dan anti-virus database telah diperbaharui hingga versi yang paling terbaru.

Unknown Threat Prevention By Engine Zero & Neural-X



No.	Database	Current Version	Latest Version	Update Svc Exp...	Auto Update	Operation
Neural-X Unknown Threat Database						
1	Unknown Threat Intelligence	2020-06-06 05:30:22	2020-06-06 05:30:22	2020-08-18	✓	Update Interval: 5 minutes
File Verification Model Database						
2	Sangfor Engine Zero File Verification Model Database	2020-03-02 11:00:00	2020-03-02 11:00:00	2020-08-18	✓	Update Interval: 1 month
Neural-X New Threat Databases						
3	URL Database	2020-05-07 15:21:46	2020-05-07 15:21:46	2020-08-18	✓	Update Interval: 14 days
4	Exploit Protection Database	2020-05-21 17:00:00	2020-05-21 17:00:00	2020-08-18	✓	
5	Application Ident Database	2020-05-09 11:55:59	2020-05-09 11:55:59	2020-08-18	✓	
6	WAF Signature Database	2020-05-23 17:00:00	2020-05-23 17:00:00	2020-08-18	✓	
7	Data Leak Protection	2018-02-16 18:00:00	2018-02-16 18:00:00	2020-08-18	✓	
8	Vulnerability Analysis Rule	2020-02-26 17:00:00	2020-02-26 17:00:00	2020-08-18	✓	
9	Anti-Virus Database	2020-05-18 13:03:44	2020-05-18 13:03:44	2020-08-18	✓	
10	Security Events	2020-05-18 09:00:00	2020-05-18 09:00:00	2020-08-18	✓	
Basic Databases						
11	Software Update	--	2020-03-27 00:00:00	Never expire	✓	
12	Malicious Connection Database	2020-05-19 10:00:00	2020-05-19 10:00:00	Never expire	✓	
13	Threat Intelligence Database	2020-05-20 00:00:00	2020-05-20 00:00:00	Never expire	✓	

Cloud-Based URL Detection menggunakan kemampuan dari NGAF untuk mengenali URL secara tepat. Jika pelanggan ingin meningkatkan kemampuan pengenalan URL, harap pastikan fungsi ini telah diaktifkan.

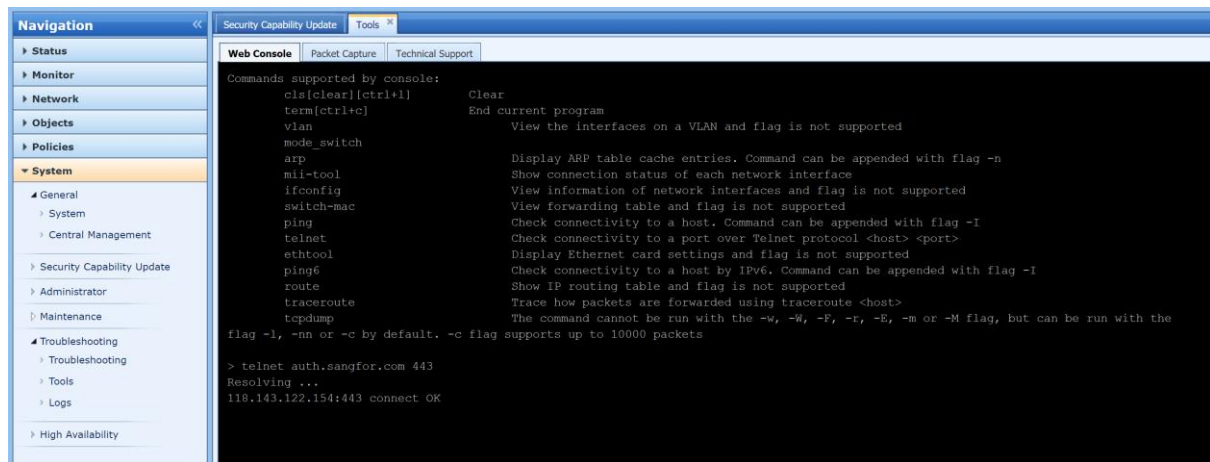


No.	Database	Current Version	Latest Version	Update Svc Exp...	Auto Update	Operation
Neural-X Unknown Threat Database						
1	Unknown Threat Intelligence	2020-06-06 03:38:09	2020-06-06 03:38:09	2020-08-18	✓	Update Interval: 5 minutes
File Verification Model Database						
2	Sangfor Engine Zero File Verification Model Database	2020-03-02 11:00:00	2020-03-02 11:00:00	2020-08-18	✓	Update Interval: 1 month
Neural-X New Threat Databases						
3	URL Database	2020-05-07 15:21:46	2020-05-07 15:21:46	2020-08-18	✓	Update Interval: 14 days
4	Exploit Protection Database	2020-05-21 17:00:00	2020-05-21 17:00:00	2020-08-18	✓	
5	Application Ident Database	2020-05-09 11:55:59	2020-05-09 11:55:59	2020-08-18	✓	
6	WAF Signature Database	2020-05-23 17:00:00	2020-05-23 17:00:00	2020-08-18	✓	
7	Data Leak Protection	2018-02-16 18:00:00	2018-02-16 18:00:00	2020-08-18	✓	
8	Vulnerability Analysis Rule	2020-02-26 17:00:00	2020-02-26 17:00:00	2020-08-18	✓	
9	Anti-Virus Database	2020-05-18 13:03:44	2020-05-18 13:03:44	2020-08-18	✓	
10	Security Events	2020-05-18 09:00:00	2020-05-18 09:00:00	2020-08-18	✓	
Basic Databases						
11	Software Update	--	2020-03-27 00:00:00	Never expire	✓	
12	Malicious Connection Database	2020-05-19 10:00:00	2020-05-19 10:00:00	Never expire	✓	
13	Threat Intelligence Database	2020-05-20 00:00:00	2020-05-20 00:00:00	Never expire	✓	

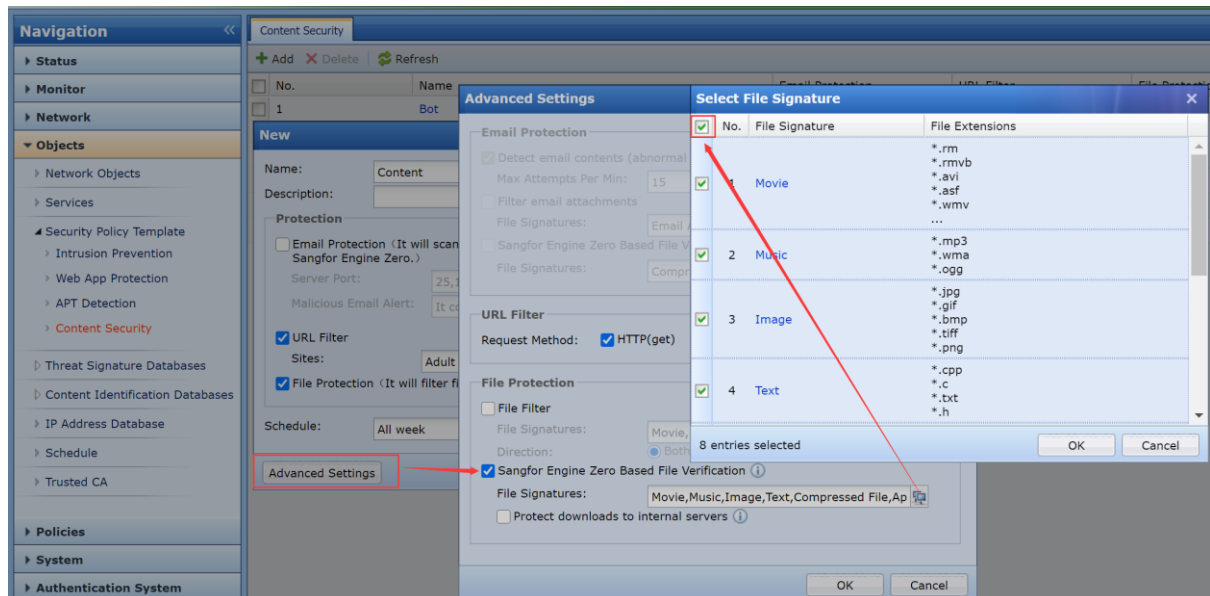
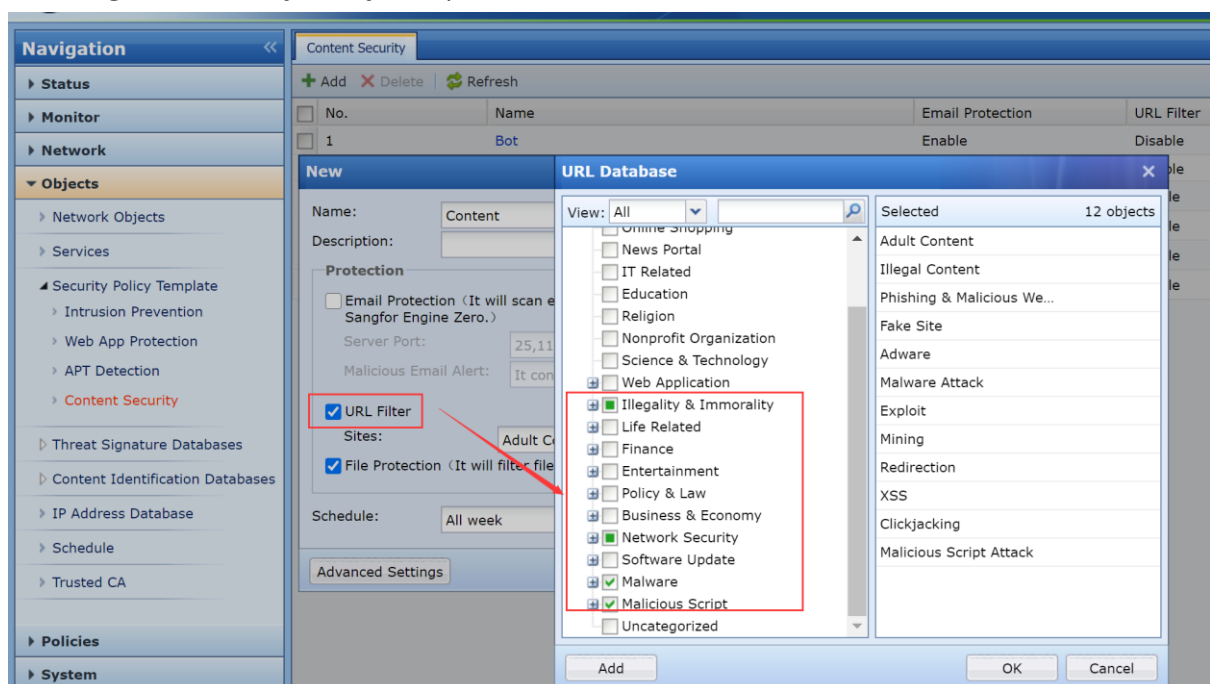
Cloud-Based URL Database Detection
Cloud-Based URL Detection: ☒ Enable ☐ Disable
OK Cancel

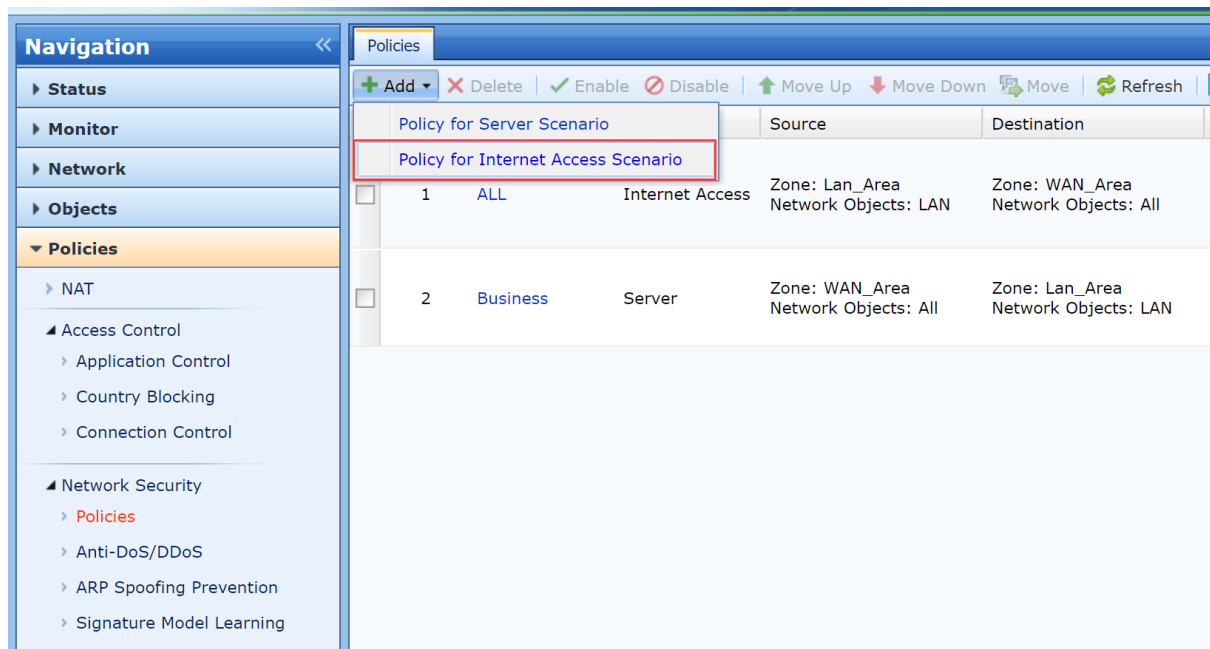
4. NGAF menggunakan Neural-X pada cloud untuk memperkuat kemampuan tingkat keamanan yang lebih kuat, sehingga harus terhubung ke cloud. Jadi anda perlu memeriksa apakah perangkat NGAF dapat mengakses alamat jaringan publik atau tidak, dan anda sebaiknya meminta pelanggan untuk tidak melakukan blok terhadap IP NGAF pada perangkat lainnya.

Unknown Threat Prevention By Engine Zero & Neural-X

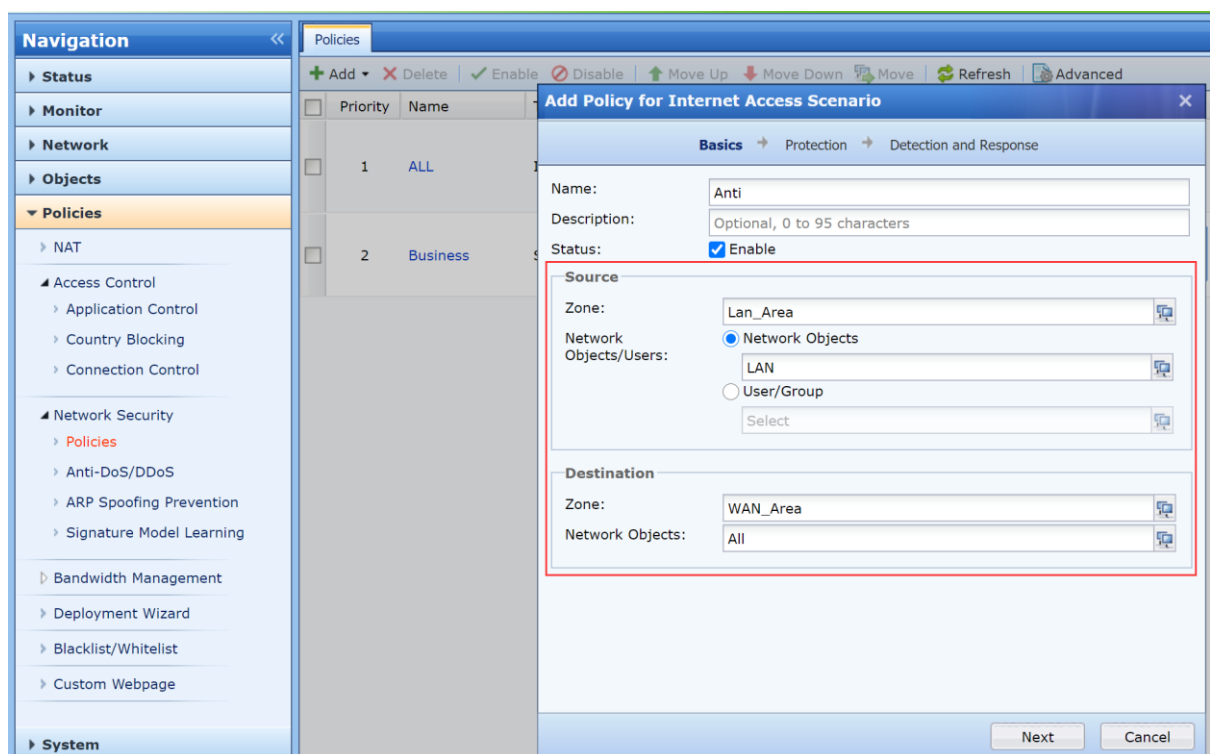


5. Konfigurasi Security Policy Template

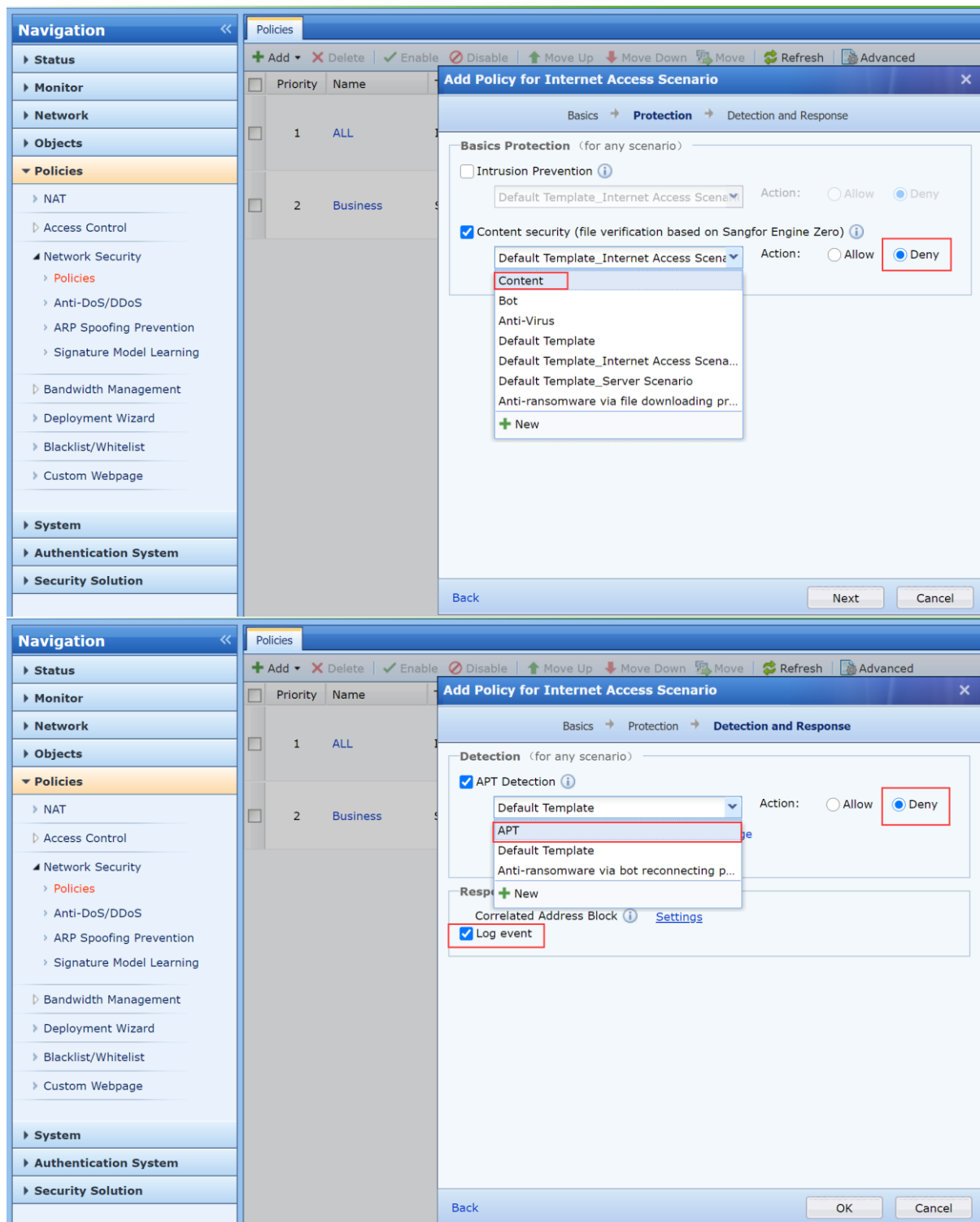




6. Pastikan zona asal/Source zone dan zona tujuan/ Destination Zone sudah benar



7. Konfigurasi security policy dan periksa apakah template terkonfigurasi sebelumnya

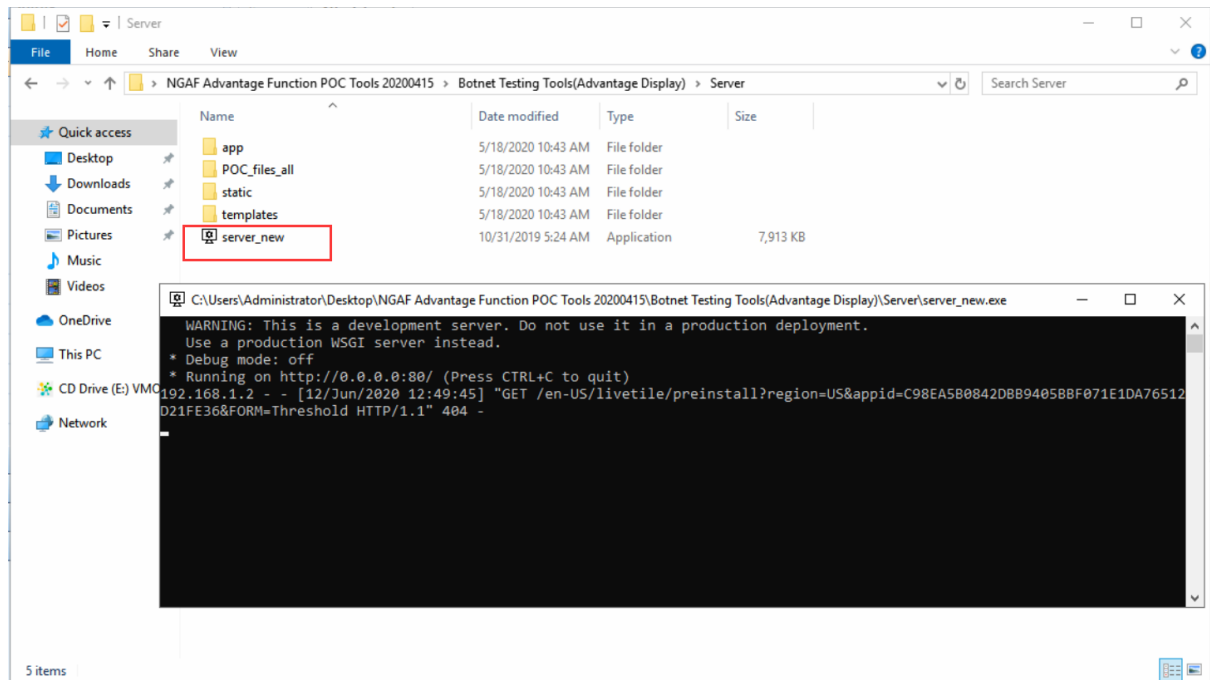


8. Contohnya, ketika sedang bertahan melawan botnet, host yang terjebak akan mengakses nama domain dalam jumlah yang besar, dan nama domain ini tidak terdapat dalam database lokal, maka Neural-X perlu digunakan untuk autentikasi penditeksian.

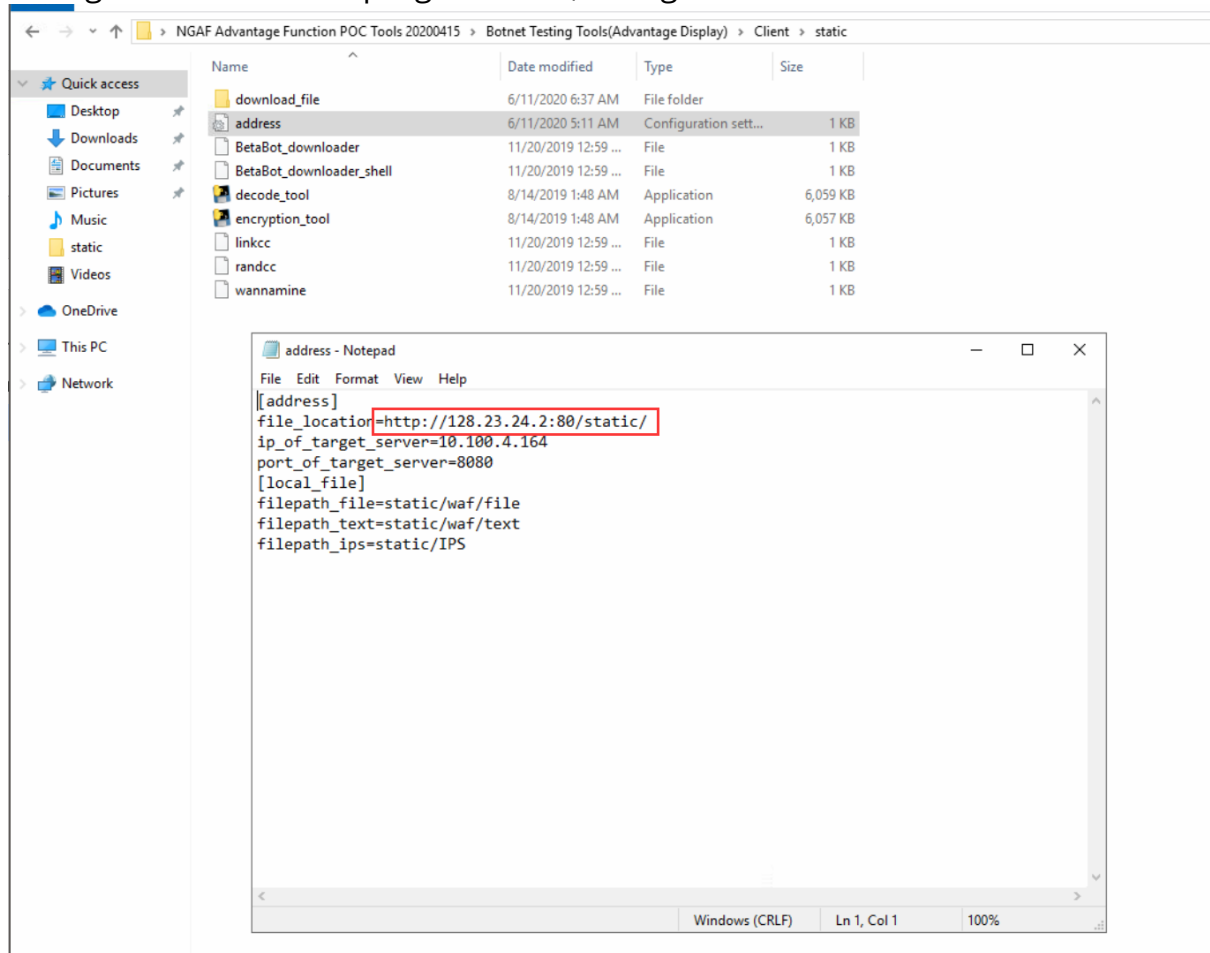
9. Penyerang menjebak pengguna LAN untuk memasukkan perangkat USB yang tidak dikenal, sehingga memicu virus worm [Advantage_Botnet_Script_2.exe] dan AF memblokir kerja yang mengirimkan trafik keluar menuju ke alamat domain yang berbahaya.

Jalankan Server_new.exe pada PC Server:

Unknown Threat Prevention By Engine Zero & Neural-X



Konfigurasi alamat dari program klien, seting IP dari PC server dalam file:



Jalankan Advantage_Botnet_Script_2.exe pada PC klien:



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