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 Penjelasan Fungsi

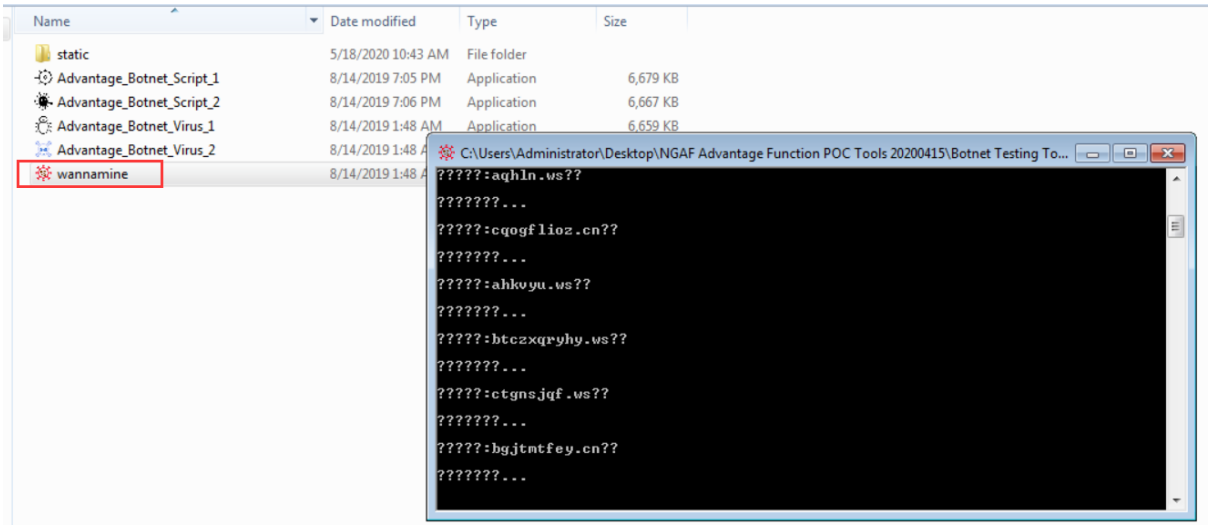
Neural-X adalah kontrol keamanan berbasis di cloud, yang mampu mengumpulkan dan menganalisa peristiwa keamanan secara keseluruhan, dan mampu mengidentifikasi ancaman yang tidak dikenali. Engine dari Sangfor Zero mengunakan kemampuan analisa yang kuat untuk menganalisa virus yang tidak dikenal.

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 memcoba 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 disarangkan 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.

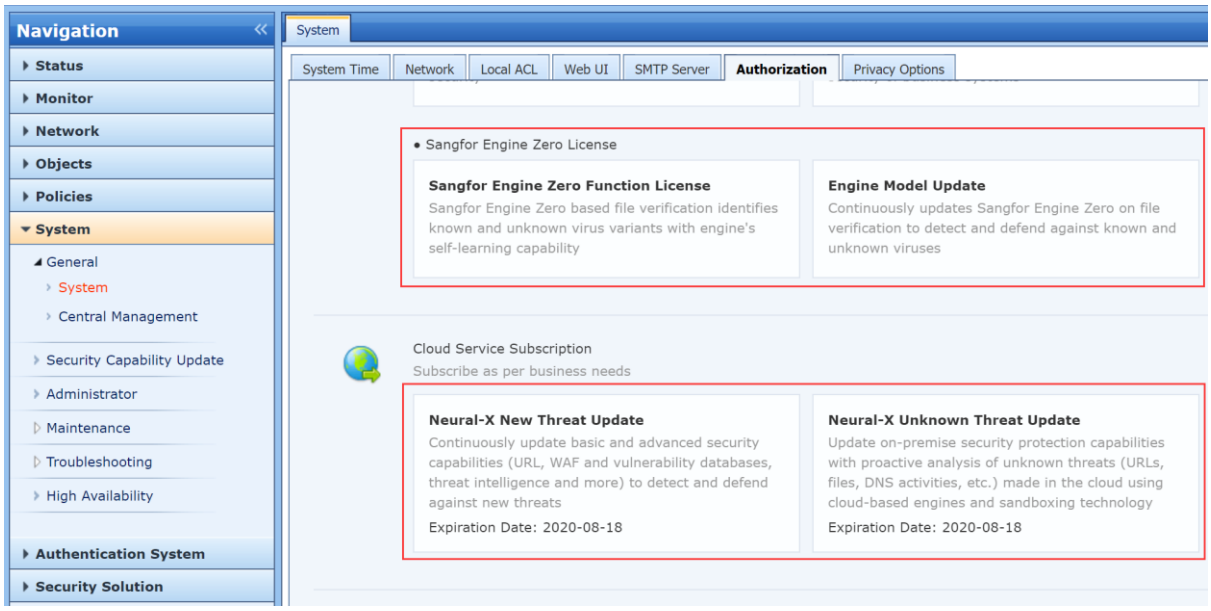
BAB 2 Rekomendasi Pedoman

Skenario:

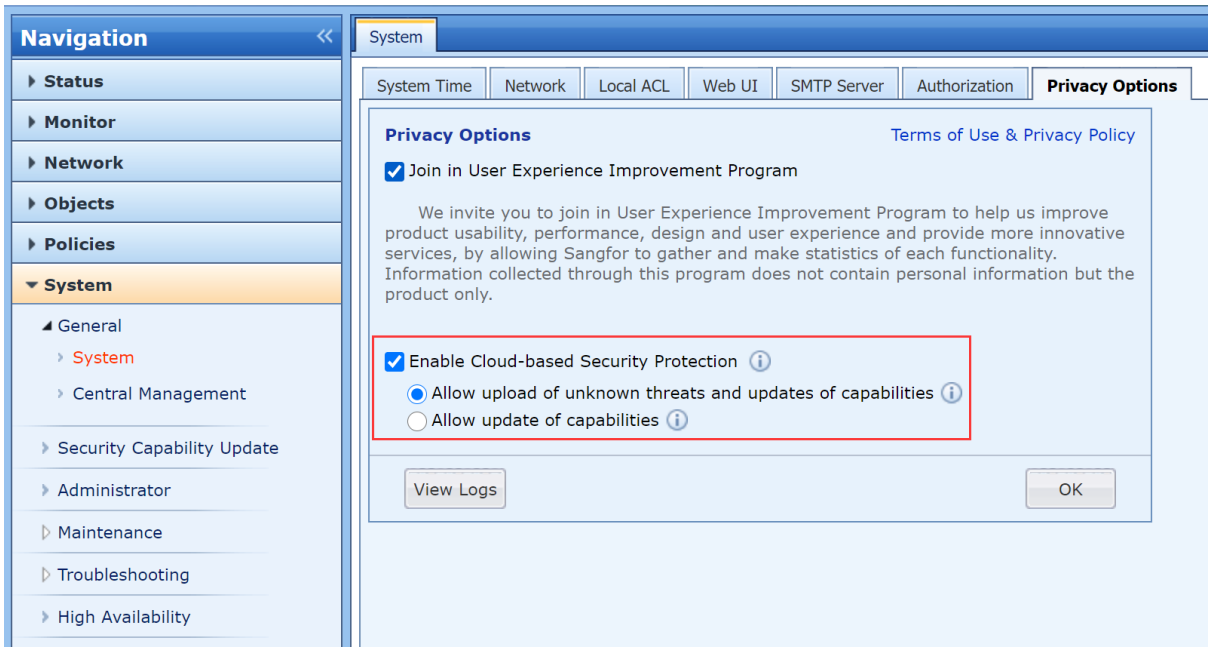
Pelanggan perusahaan manufaktur telah diserang oleh peretas untuk waktu yang lama, dan untuk ancaman yang tidak diketahui, firewall pelanggan sebelumnya tidak bekerja efektif untuk mengidentifikasi dan mencegahnya, dan pelanggan ingin menggunakan Sangfor NGAF untuk menangani ancaman yang tidak dikenal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

Konfigurasi:

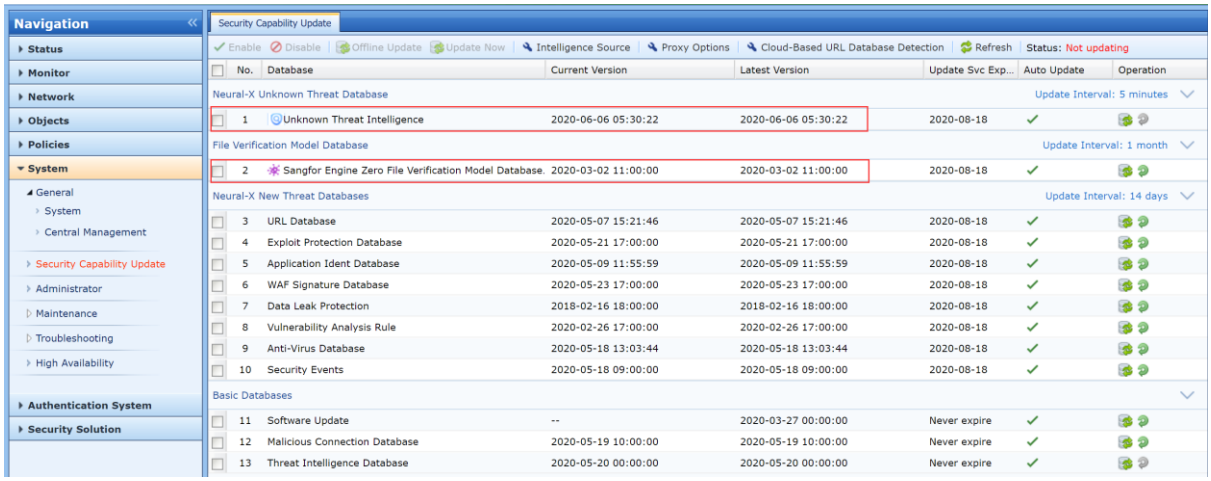
1. Pastikan lisensi dari Neural-X dan Sangfor Zero Engine masih berlaku.



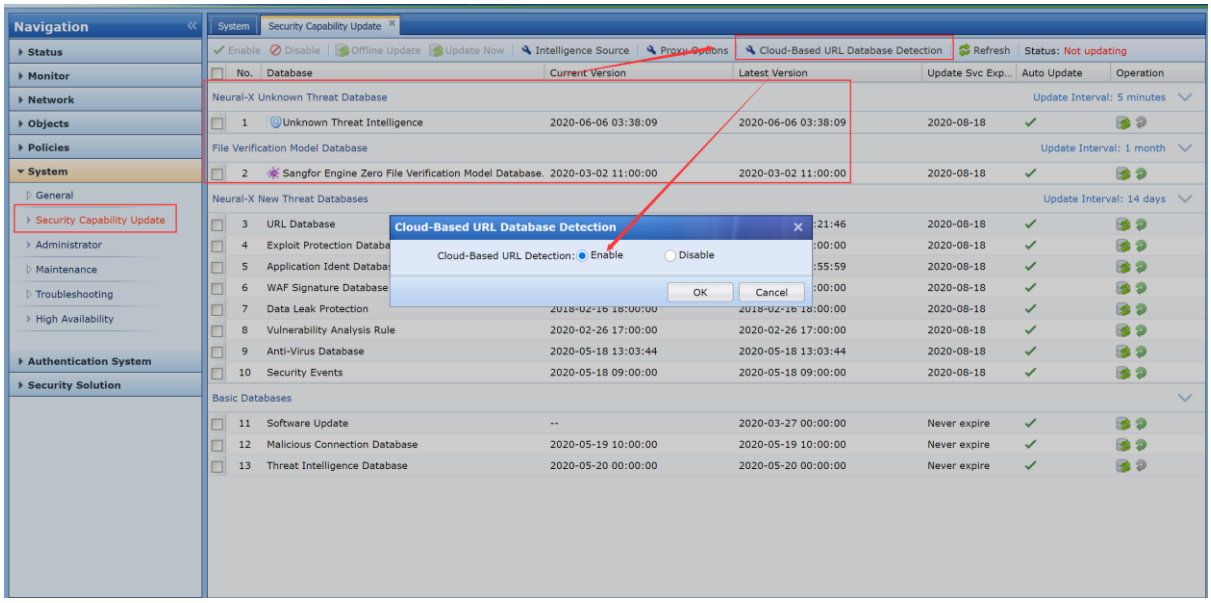
2. Pastikan Cloud-based Security Protection telah diaktifkan.



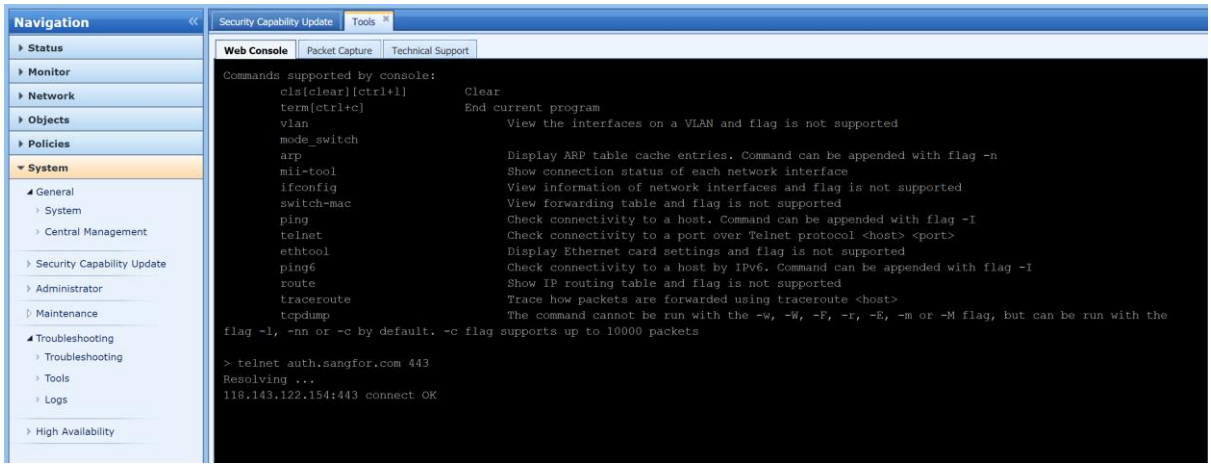
3. Pastikan unknown threat Intelligence database, Sangfor Zero Engine model, dan anti-virus database telah diperbaharui hingga versi yang paling terbaru.



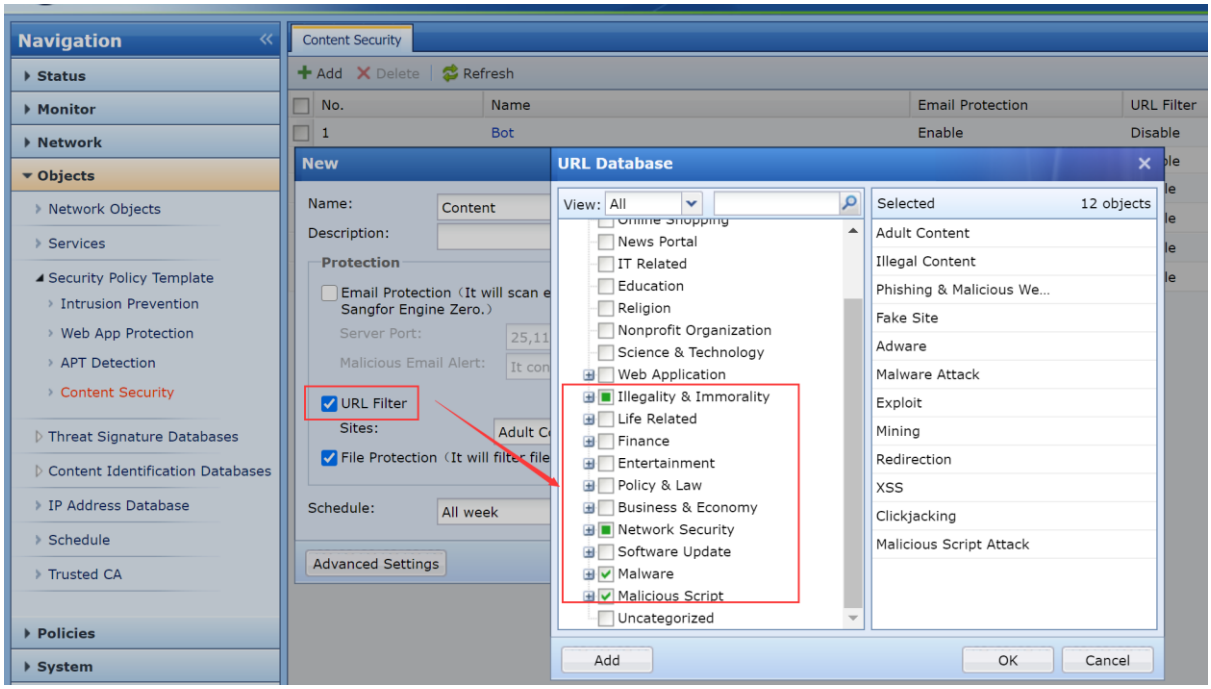
Cloud-Based URL Detection menggunakan kemampuan dari NGAF untuk mengenali URL secara tepat. Jika pelanggan ingin meningkatkan kemampuan pengenalan URL, harap pastikan fungsi ini telah diaktifkan.

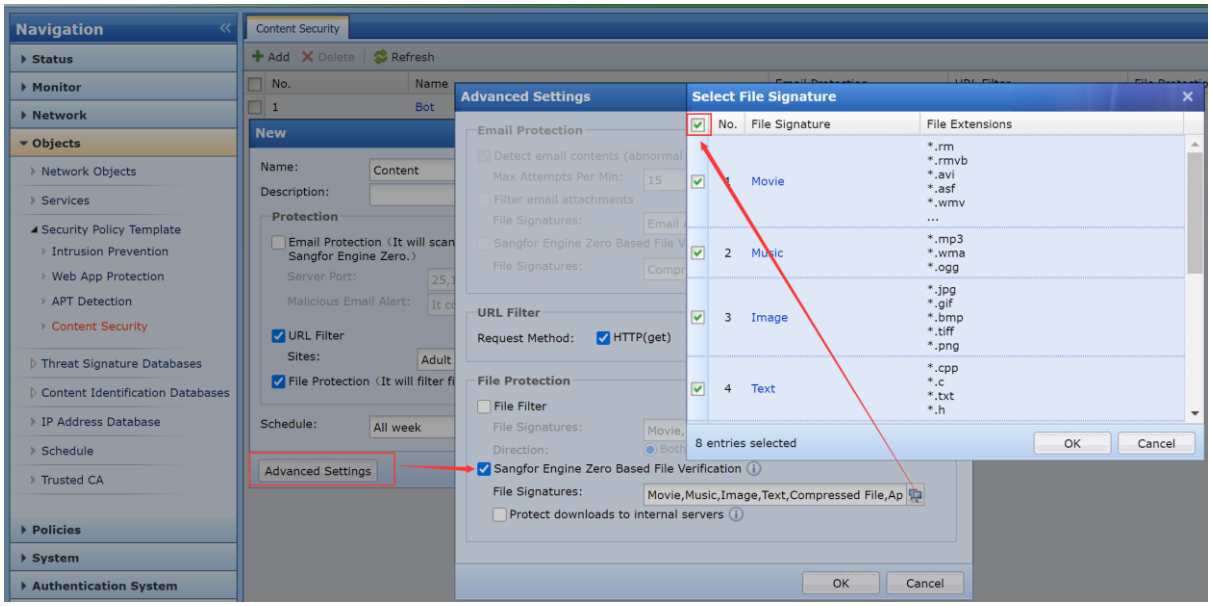


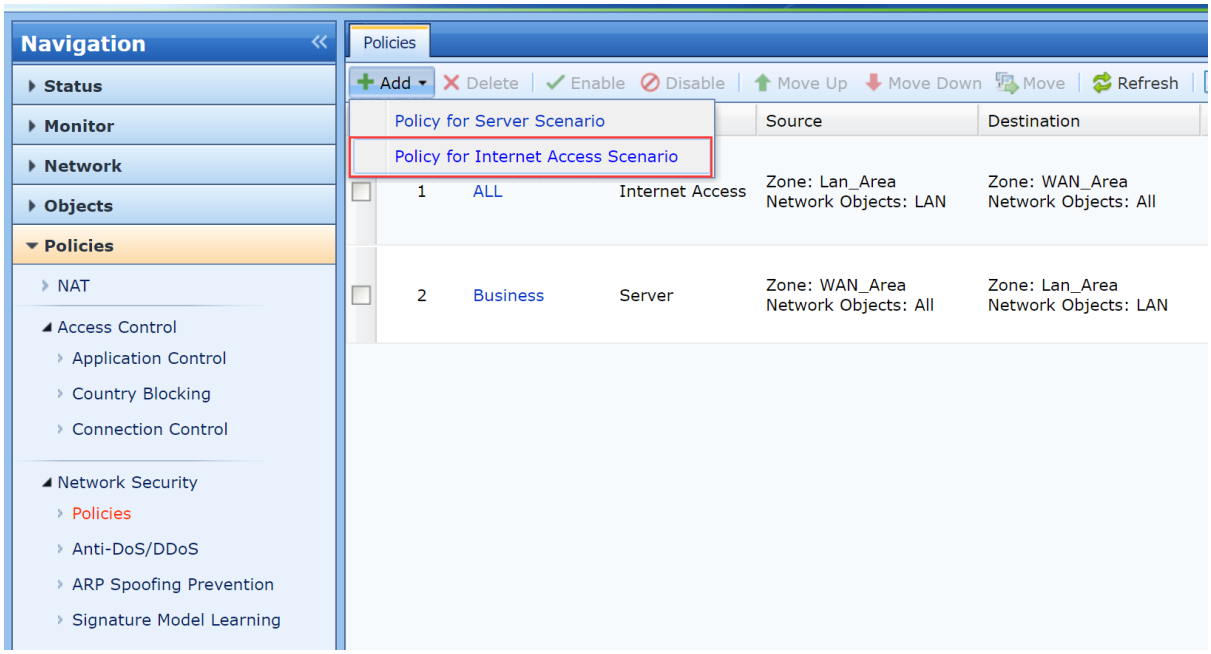
4. NGAF menggunakan Neural-X pada cloud untuk memperkuat kemampuan tingkat keamanan yang lebih kuat, sehingga harus terhubung ke cloud. Jadi anda perlu memeriksa apakah perangkat NGAF dapat mengakses alamat jaringan publik atau tidak, dan anda sebaiknya meminta pelanggan untuk tidak melakukan blok terhadap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



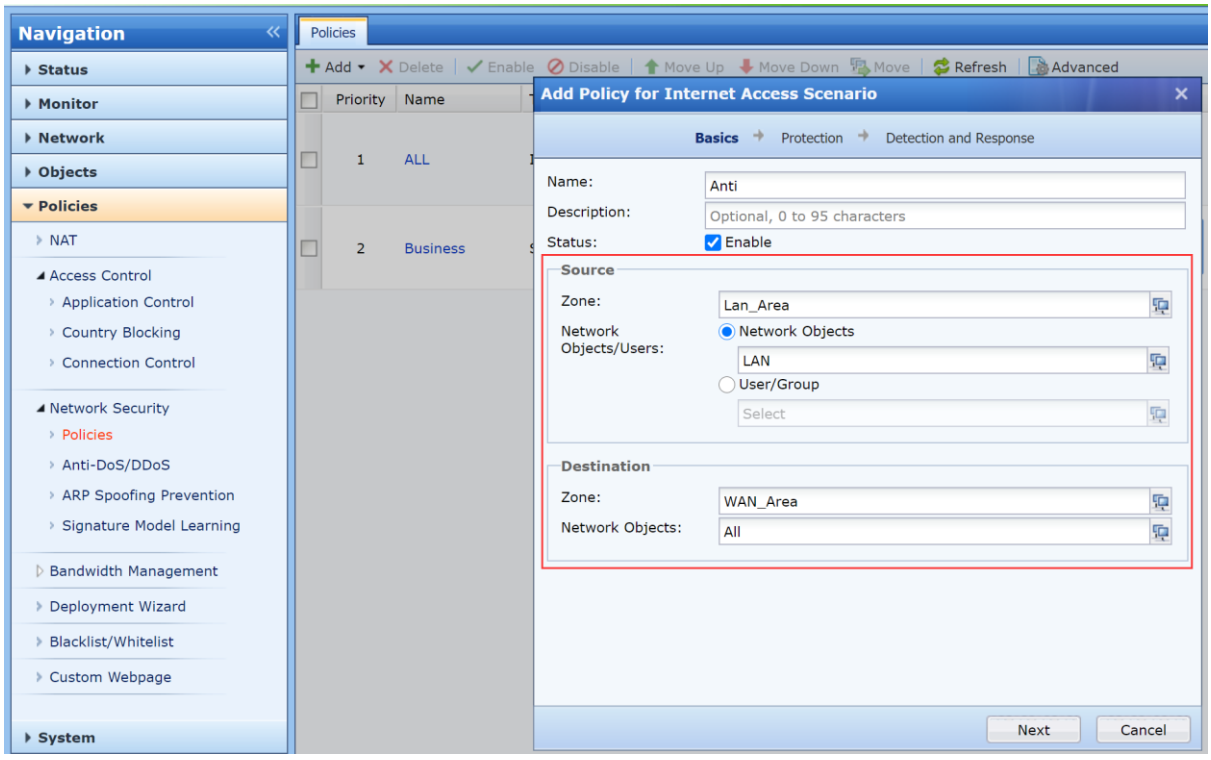
5. Konfigurasi Security Policy Template



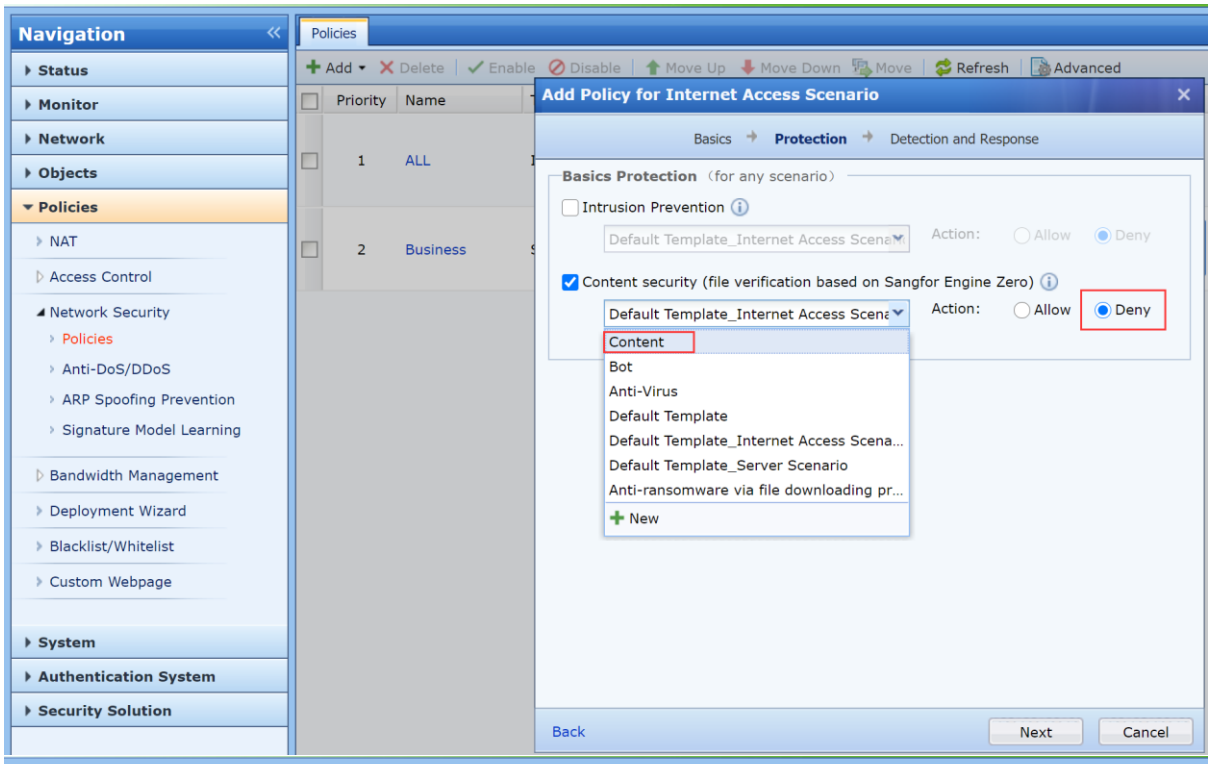


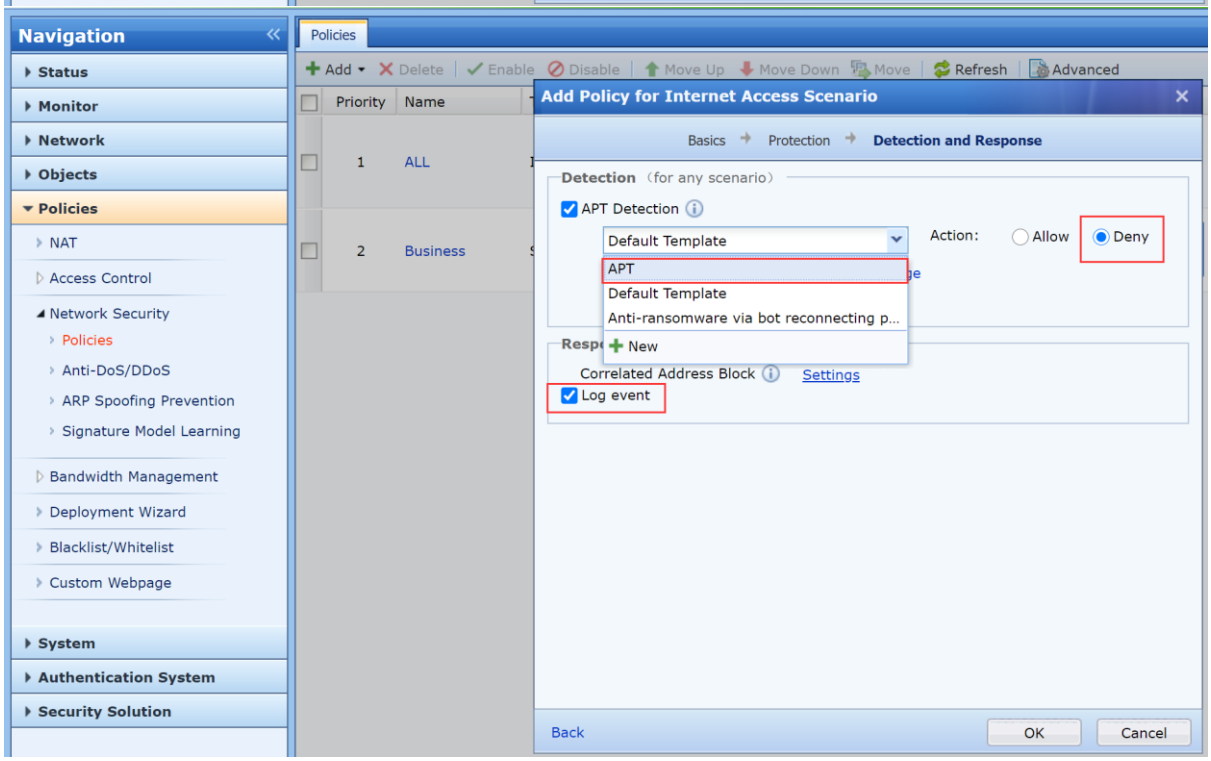


6. Pastikan zona asal/Source zone dan zona tujuan/ Destination Zone sudah benar



7. Konfigurasi security policy dan periksa apakah template terkonfigurasi sebelumnya

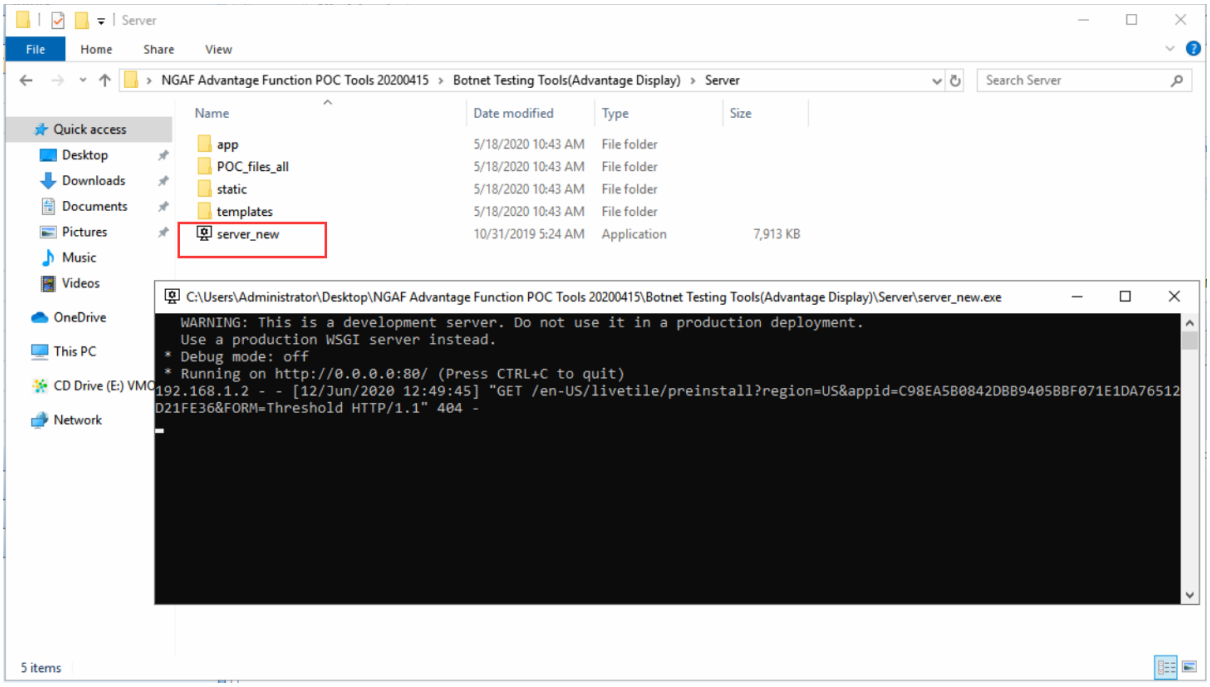




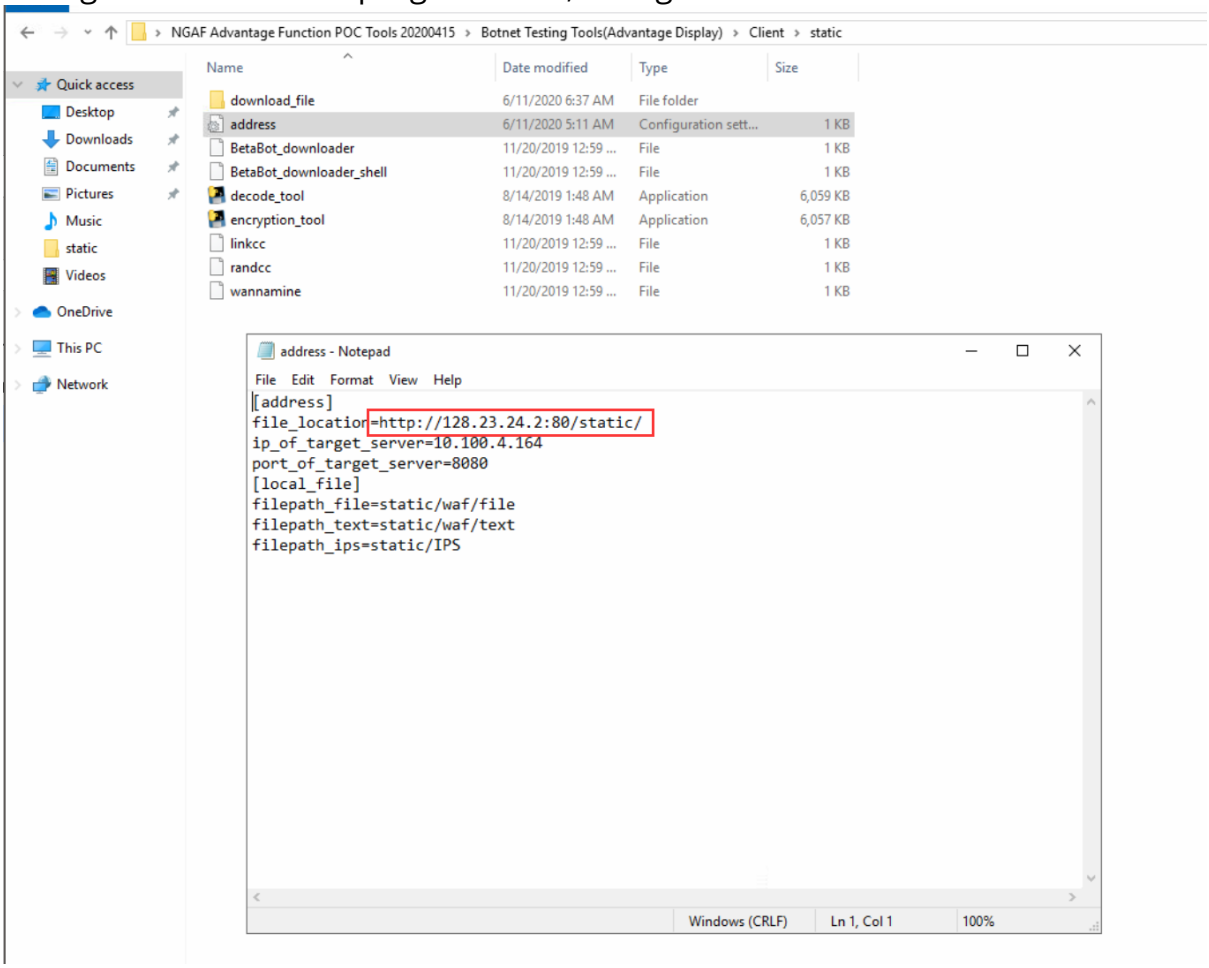
8. Contohnya, ketika sedang bertahan melawan botnet, host yang terjebak akan mengakses nama domain dalam jumlah yang besar, dan nama domain ini tidak terdapat dalam database lokal, maka Neural-X perlu digunakan untuk authentikasi penditeksian.

9. Penyerang menjebak pengguna LAN untuk memasukan 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.

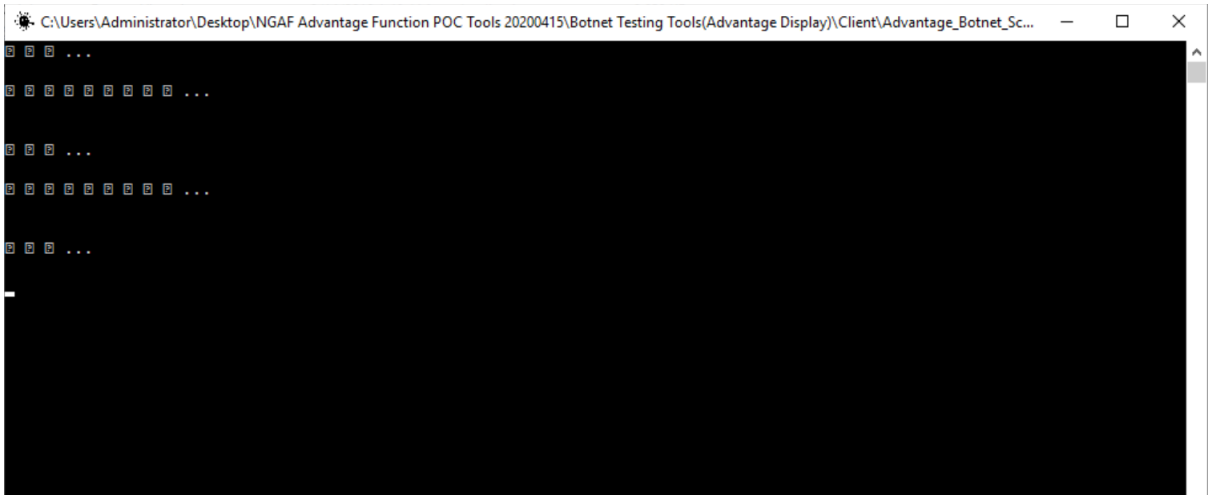
Jalankan Server_new.exe pada PC Server:



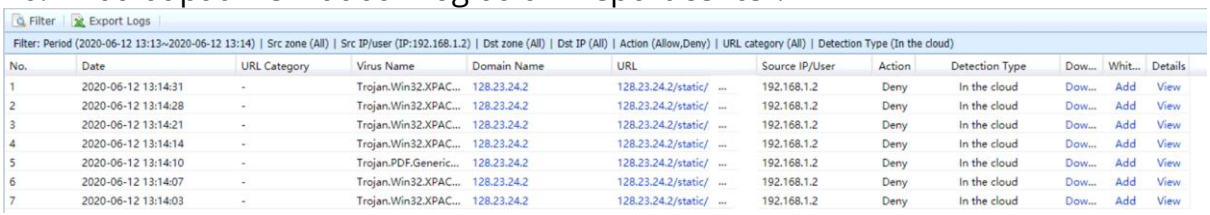
Konfigurasi alamat dari program klien, seting IP dari PC server dalam file:



Jalankan Advantage_Botnet_Script_2.exe pada PC klien:



10. Anda dapat melihat dari log dalam report center.



Filter | Export Logs

Filter: Period (2020-06-12 13:13~2020-06-12 13:14) | Src zone (All) | Src IP/user (IP:192.168.1.2) | Dst zone (All) | Dst IP (All) | Action (Allow,Deny) | URL category (All) | Detection Type (In the cloud)

No.	Date	URL Category	Virus Name	Domain Name	URL	Source IP/User	Action	Detection Type	Dow...	Whit...	Details
1	2020-06-12 13:14:31	-	Trojan.Win32.XPAC...	128.23.24.2	128.23.24.2/static/ ...	192.168.1.2	Deny	In the cloud	Dow...	Add	View
2	2020-06-12 13:14:28	-	Trojan.Win32.XPAC...	128.23.24.2	128.23.24.2/static/ ...	192.168.1.2	Deny	In the cloud	Dow...	Add	View
3	2020-06-12 13:14:21	-	Trojan.Win32.XPAC...	128.23.24.2	128.23.24.2/static/ ...	192.168.1.2	Deny	In the cloud	Dow...	Add	View
4	2020-06-12 13:14:14	-	Trojan.Win32.XPAC...	128.23.24.2	128.23.24.2/static/ ...	192.168.1.2	Deny	In the cloud	Dow...	Add	View
5	2020-06-12 13:14:10	-	Trojan.PDF.Generic...	128.23.24.2	128.23.24.2/static/ ...	192.168.1.2	Deny	In the cloud	Dow...	Add	View
6	2020-06-12 13:14:07	-	Trojan.Win32.XPAC...	128.23.24.2	128.23.24.2/static/ ...	192.168.1.2	Deny	In the cloud	Dow...	Add	View
7	2020-06-12 13:14:03	-	Trojan.Win32.XPAC...	128.23.24.2	128.23.24.2/static/ ...	192.168.1.2	Deny	In the cloud	Dow...	Add	View