



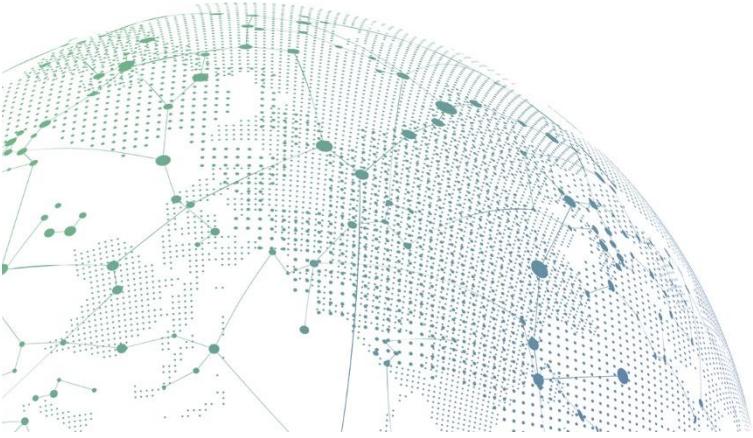
**SANGFOR**



## **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

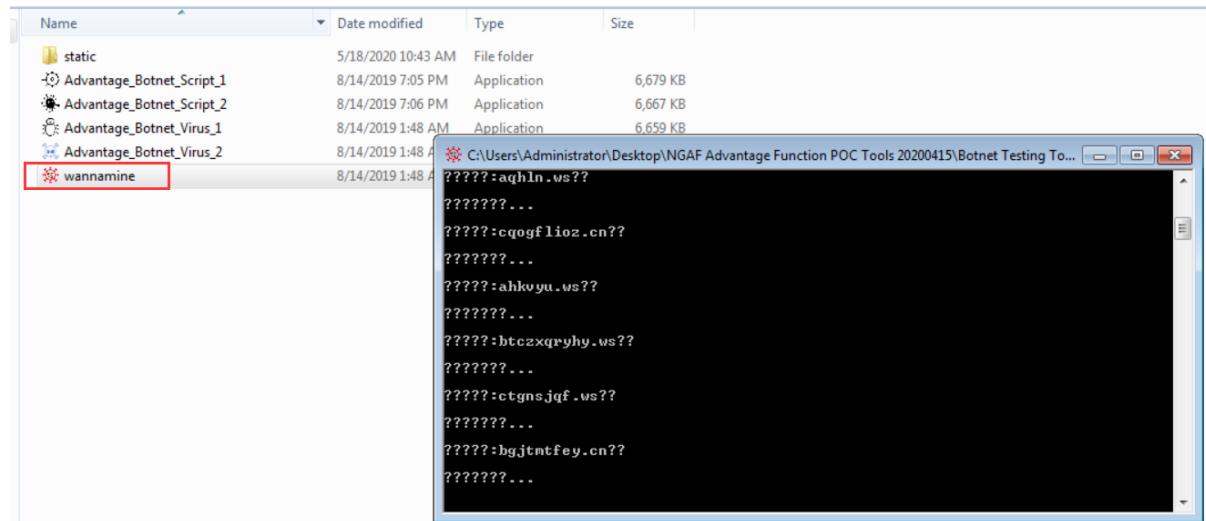
Neural-X adalah kontrol keamanan berbasis di cloud, yang mampu mengumpulkan dan menganalisa peristiwa keamanan secara keseluruhan, dan mampu mengidentifikasi ancaman yang tidak dikenali. Engine dari Sangfor Zero menggunakan kemampuan analisa yang kuat untuk menganalisa virus yang tidak dikenal.

## 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 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 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

## Unknown Threat Prevention By Engine Zero & Neural-X

### 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.

The screenshot shows the 'System' tab selected in the navigation bar. The 'Authorization' tab is active. In the main content area, there's a section titled 'Sangfor Engine Zero License' which includes a sub-section 'Sangfor Engine Zero Function License'. Below it is a section for 'Cloud Service Subscription' with two items: 'Neural-X New Threat Update' and 'Neural-X Unknown Threat Update'. Both the 'Neural-X New Threat Update' section and its sub-section 'Neural-X Unknown Threat Update' are highlighted with red boxes.

2. Pastikan Cloud-based Security Protection telah diaktifkan.

The screenshot shows the 'System' tab selected in the navigation bar. The 'Privacy Options' tab is active. In the main content area, there's a section titled 'Privacy Options' with a sub-section 'Join in User Experience Improvement Program'. Below it is another section with a checkbox 'Enable Cloud-based Security Protection' followed by two radio button options: 'Allow upload of unknown threats and updates of capabilities' and 'Allow update of capabilities'. The 'Enable Cloud-based Security Protection' checkbox and its options are highlighted with a red box.

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

The screenshot shows the Sangfor Engine Zero & Neural-X management interface. In the left navigation pane, 'System' is selected, and 'Security Capability Update' is highlighted. The main area displays several database tables:

- Security Capability Update:** Shows two entries: 'Unknown Threat Intelligence' and 'Sangfor Engine Zero File Verification Model Database'. Both have an 'Update Interval: 5 minutes'.
- Neural-X New Threat Databases:** A table with 10 entries, all with an 'Update Interval: 14 days'. The columns include No., Database, Current Version, Latest Version, Update Svc Exp..., Auto Update, and Operation.
- Basic Databases:** A table with 3 entries, all with an 'Update Interval: 1 month'. The columns include No., Database, Current Version, Latest Version, Update Svc Exp..., Auto Update, and Operation.

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.

The screenshot shows the Sangfor Engine Zero & Neural-X management interface. In the left navigation pane, 'System' is selected, and 'Security Capability Update' is highlighted. A modal dialog box titled 'Cloud-Based URL Database Detection' is open over the main table. The dialog contains the following options:

- Cloud-Based URL Detection:  Enable  Disable
- OK button
- Cancel button

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

```

Commands supported by console:
cls[clear](ctrl+l)           Clear
term(ctrl+c)                 End current program
vian                         View the interfaces on a VLAN and flag is not supported
mode_switch
arp                           Display ARP table cache entries. Command can be appended with flag -n
mii-tool                      Show connection status of each network interface
ifconfig                      View information of network interfaces and flag is not supported
switch-mac                    View forwarding table and flag is not supported
ping                          Check connectivity to a host. Command can be appended with flag -I
telnet                        Check connectivity to a port over Telnet protocol <host> <port>
ethtool                       Display Ethernet card settings and flag is not supported
ping6                         Check connectivity to a host by IPv6. Command can be appended with flag -I
route                         Show IP routing table and flag is not supported
traceroute                    Trace how packets are forwarded using traceroute <host>
tcpdump                       The command cannot be run with the -w, -W, -F, -r, -E, -m or -M flag, but can be run with the
                             flag -l, -nn or -c by default. -c flag supports up to 10000 packets

> telnet auth.sangfor.com 443
Resolving ...
118.143.122.154:443 connect OK

```

## 5. Konfigurasi Security Policy Template

**New**

**URL Database**

**Selected** 12 objects

- Online Shopping
- News Portal
- IT Related
- Education
- Religion
- Nonprofit Organization
- Science & Technology
- Web Application
- Illegality & Immorality**
- Life Related
- Finance
- Entertainment
- Policy & Law
- Business & Economy
- Network Security**
- Software Update**
- Malware**
- Malicious Script**
- Uncategorized

**Advanced Settings**

**Select File Signature**

No.	File Signature	File Extensions
1	Movie	*.rm *.rmvb *.avi *.asf *.wmv ...
2	Music	*.mp3 *.wma *.ogg
3	Image	*.jpg *.gif *.bmp *.tiff *.png
4	Text	*.cpp *.c *.txt *.h

8 entries selected

Sangfeng Engine Zero Based File Verification

File Signatures: Movie, Music, Image, Text, Compressed File, App

Protect downloads to internal servers

## Unknown Threat Prevention By Engine Zero & Neural-X

The screenshot shows the Sangfor management interface with the 'Policies' section selected in the navigation menu. The main pane displays a list of policies. One policy, 'Policy for Internet Access Scenario', is highlighted with a red box. The policy details are shown in the table:

Priority	Name	Source	Destination
1	ALL	Internet Access	Zone: Lan_Area Network Objects: LAN
2	Business	Server	Zone: WAN_Area Network Objects: All

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

The screenshot shows the Sangfor management interface with the 'Add Policy for Internet Access Scenario' dialog open. The 'Source' and 'Destination' sections are highlighted with a red box. The dialog fields are as follows:

Source	
Zone:	Lan_Area
Network Objects/Users:	<input checked="" type="radio"/> Network Objects LAN
	<input type="radio"/> User/Group Select
Destination	
Zone:	WAN_Area
Network Objects:	All

7. Konfigurasi security policy dan periksa apakah template terkonfigurasi sebelumnya

## Unknown Threat Prevention By Engine Zero & Neural-X

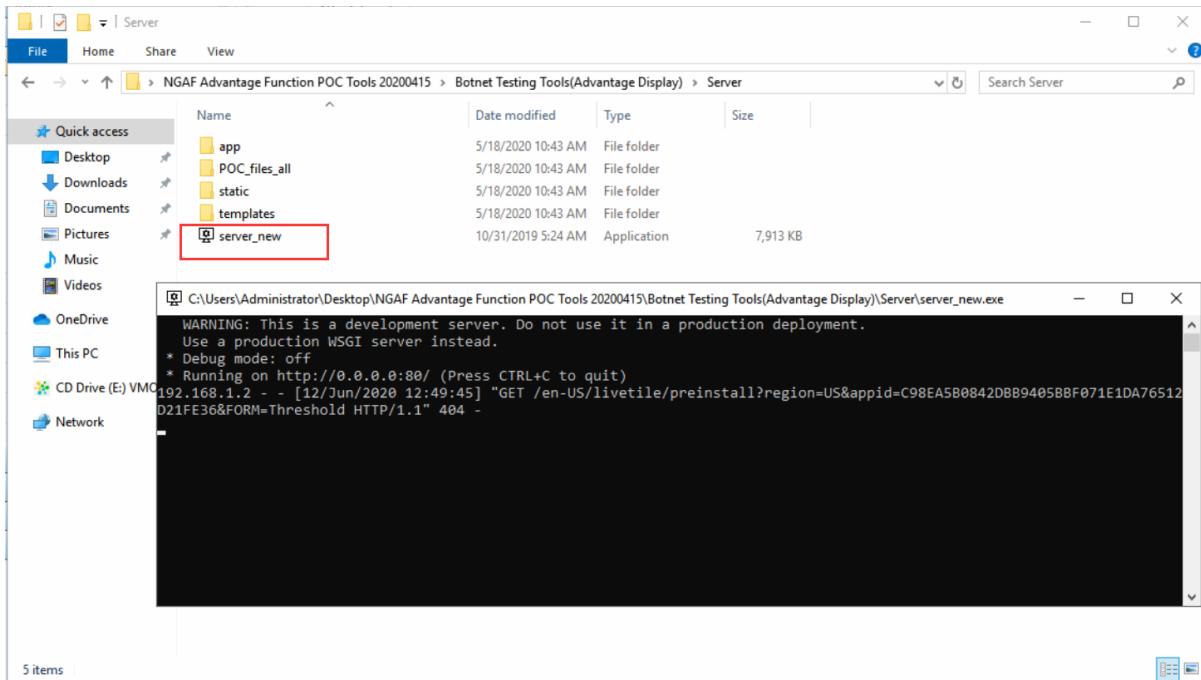
The screenshot shows two instances of the Sangfor management interface. The top instance is titled 'Add Policy for Internet Access Scenario' under the 'Protection' tab, specifically the 'Detection and Response' sub-tab. It displays a list of protection modules: Intrusion Prevention (unchecked), Content security (checked, with 'Content' selected, action Deny), and Bot, Anti-Virus, Default Template, Default Template\_Internet Access Scenario, Default Template\_Server Scenario, and Anti-ransomware via file downloading pr... (all unchecked). The bottom instance is also titled 'Add Policy for Internet Access Scenario' but under the 'Detection' tab. It shows APT Detection (checked, with 'APT' selected, action Deny) and a response section with Correlated Address Block (unchecked) and Log event (checked).

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.

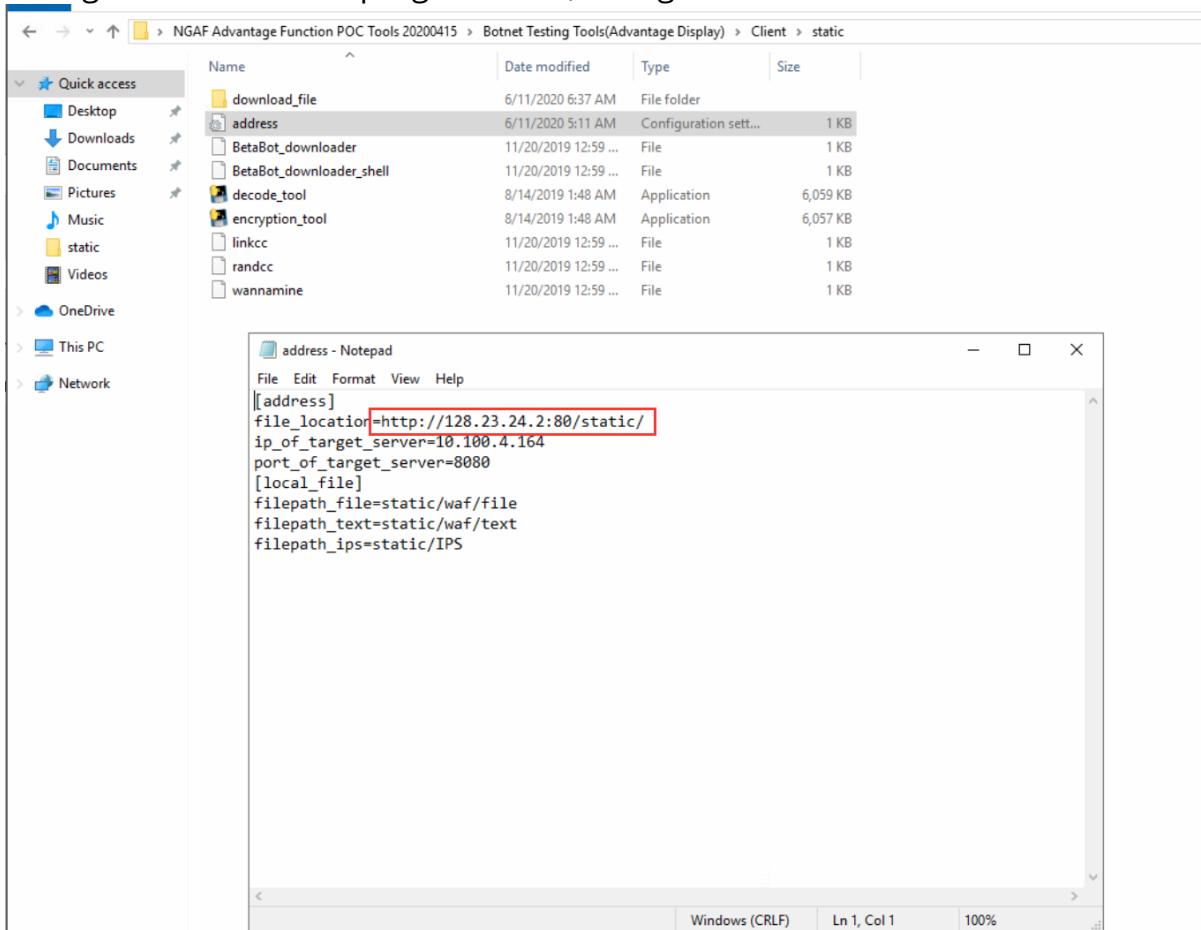
9. Penyerang menjebak pengguna LAN untuk memasukan perangkat USB yang tidak dikenal, sehingga memicu virus worm [Advantage\_Botnet\_Script\_2.exe] dan AF memblokir kerja yang mengirimkan trafik keluar menuju ke alamat domain yang berbahaya.

Jalankan Server\_new.exe pada PC Server:

## Unknown Threat Prevention By Engine Zero & Neural-X

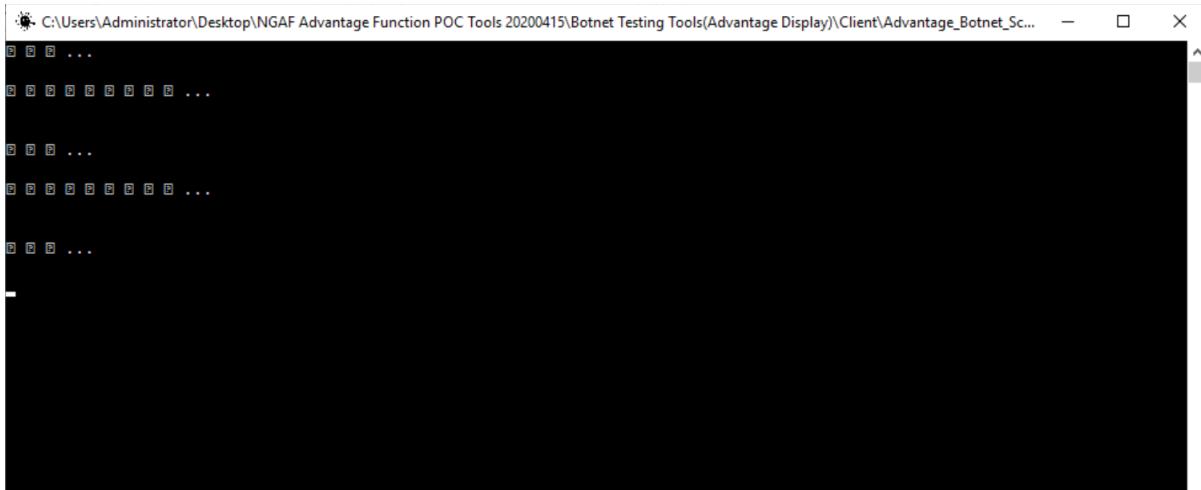


Konfigurasi alamat dari program klien, seting IP dari PC server dalam file:



Jalankan Advantage\_Botnet\_Script\_2.exe pada PC klien:

## Unknown Threat Prevention By Engine Zero & Neural-X



10. Anda dapat melihat dari log dalam report center.

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	Down...	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	Down...	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	Down...	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	Down...	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	Down...	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	Down...	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	Down...	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	Down...	Add	View	



**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