SANGFOR

NGAF

Best Practices for Scenarios_Unknown Threat Prevention By Engine Zero & Neural-X

Version 8.0.17

Change Log

Date	Change Description
June 15, 2020	Document release.
Mar 18, 2021	Document Update.
May 17, 2021	Document update.

CONTENT

Chapter 1 Scenario

1.1 Function Description

Neural-X is a security brain in the cloud, capable of collecting and analyzing global security events, and being able to identify unknown threats. The Sangfor Zero engine can use its powerful analysis capabilities to analyze unknown viruses.

1.2 Scenario:

Use NGAF to link Neural-X to protect customers' network security.

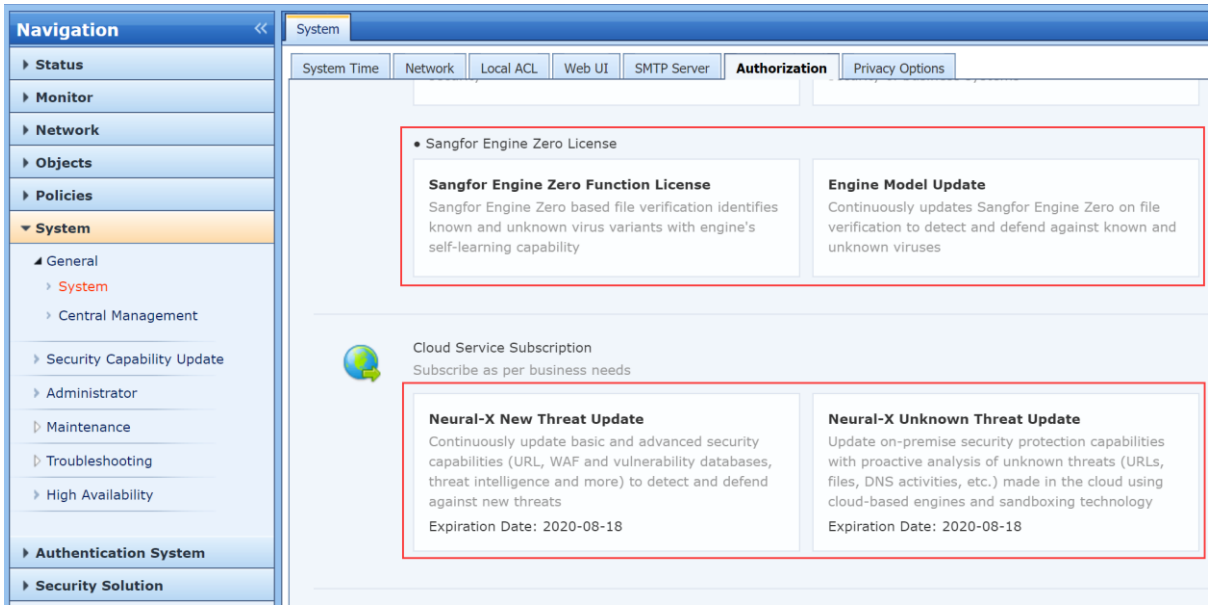
Chapter 2 Best Practice Recommendations

Scenario:

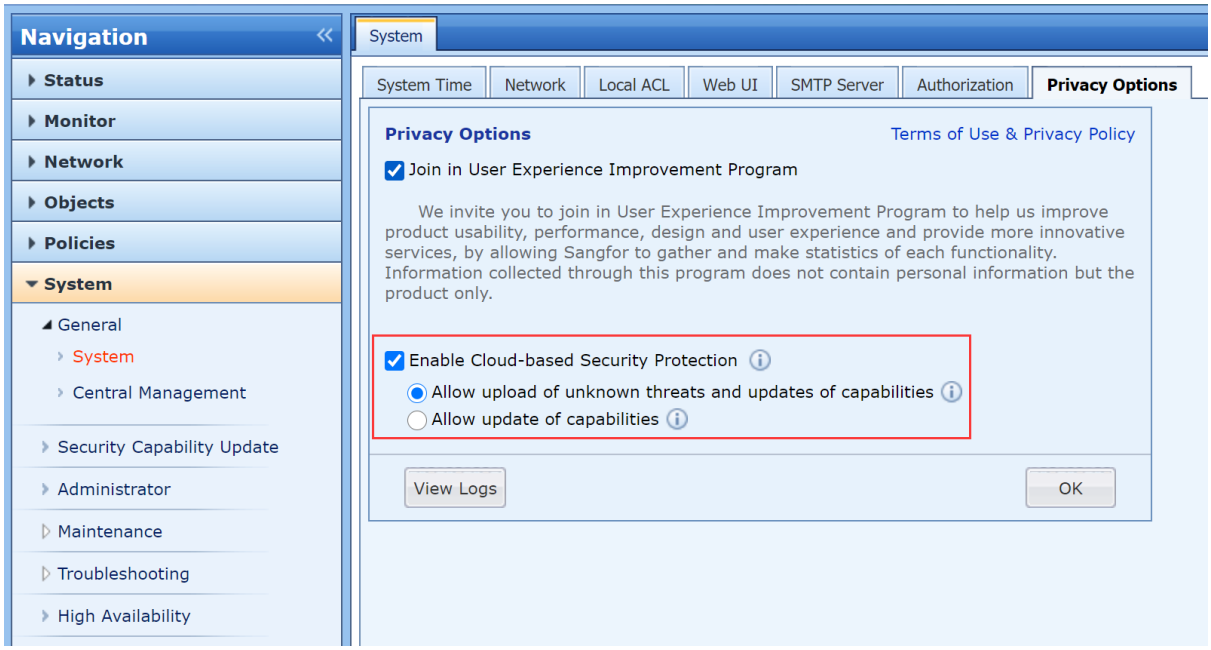
A manufacturing customer has been attacked by a hacker for a long time, and for unknown threat, the customer's previous firewall cannot effectively identify and intercept it, and wants to use Sangfor NGAF to deal with the unknown threat.

Configuration:

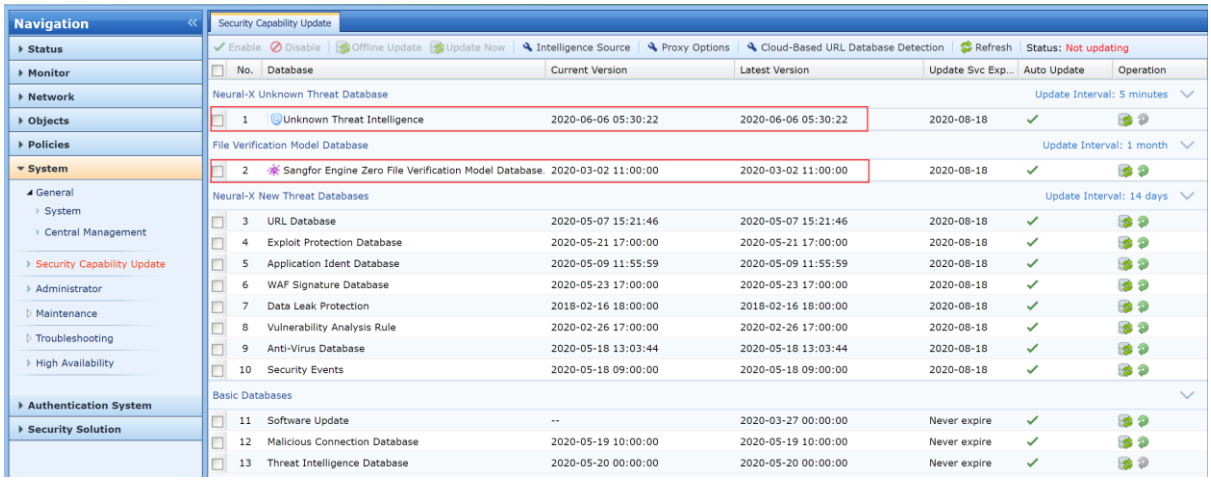
1. Ensure the license status of Neural-X and Sangfor Zero Engine is valid.



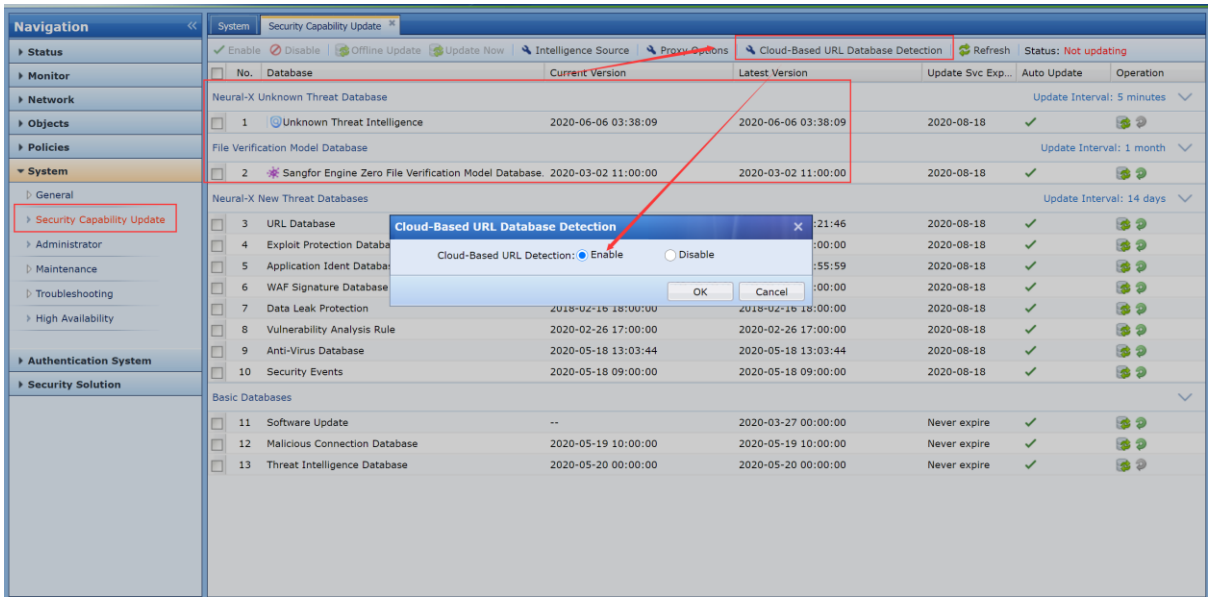
2. Make sure that Cloud-based Security Protection is enabled.



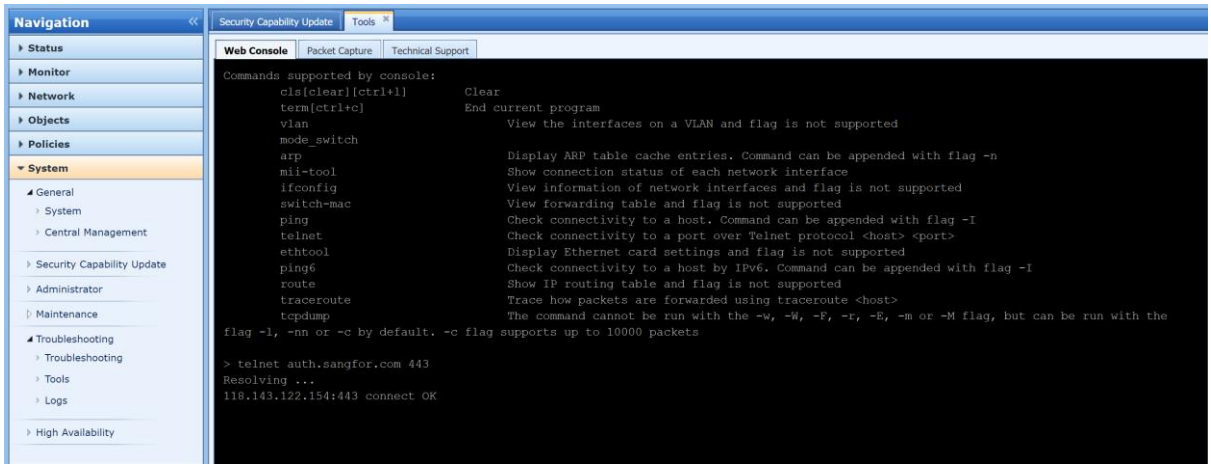
3. Ensure that the unknown threat Intelligence database, Sangfor Zero Engine model, and anti-virus database are all updated to the latest version.



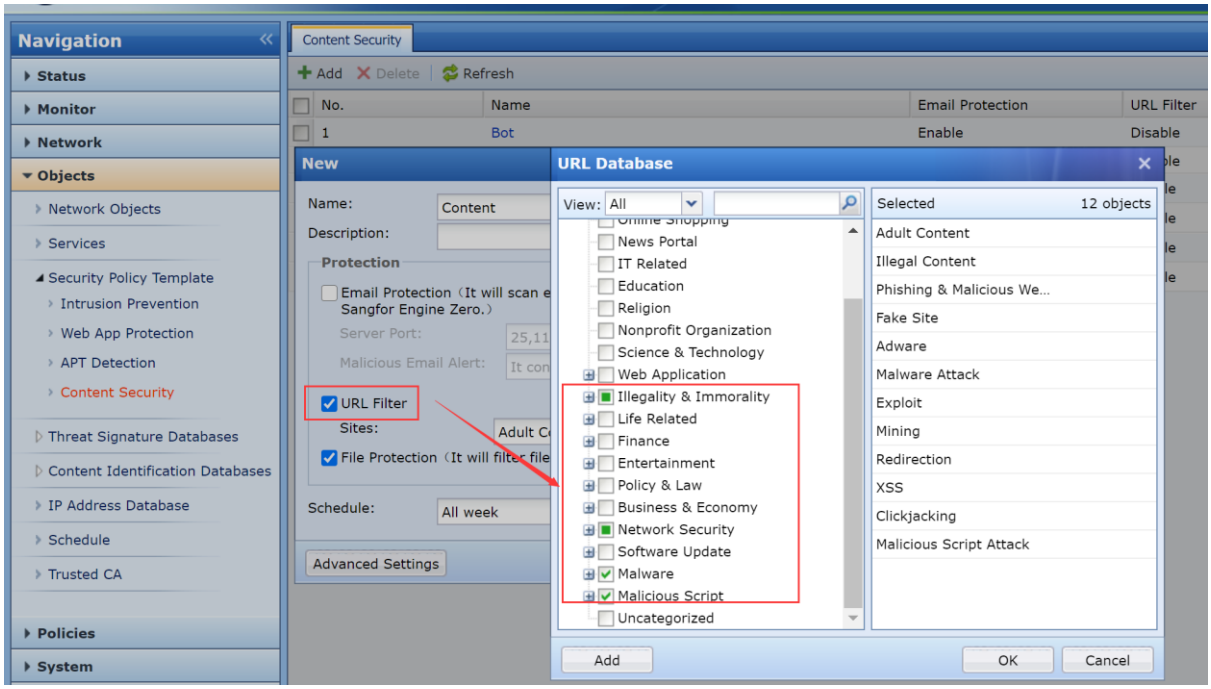
Cloud-Based URL Detection is used to strengthen NGAF's ability to recognize URLs. If customers want to enhance URL recognition capabilities, please ensure that the function is turned on.

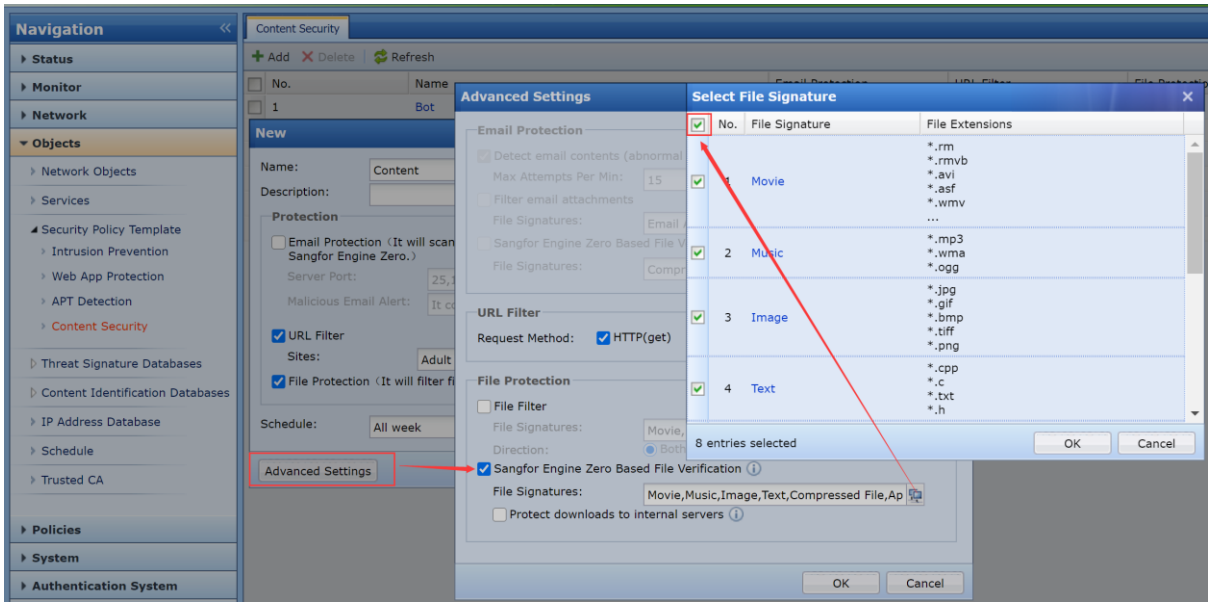


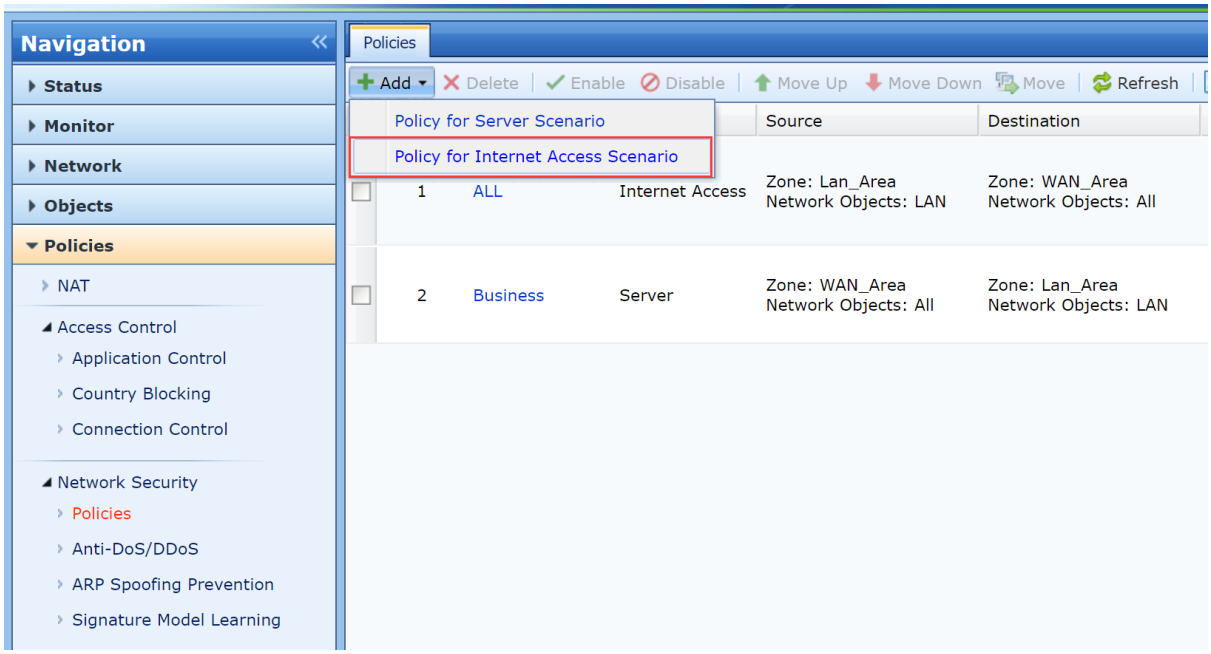
4. NGAF uses Neural-X in the cloud to strengthen its security capabilities, so it must be connected to the cloud. So you need check whether the NGAF device can access the public network address, and you'd better ask customer not block NGAF's IP in other device.



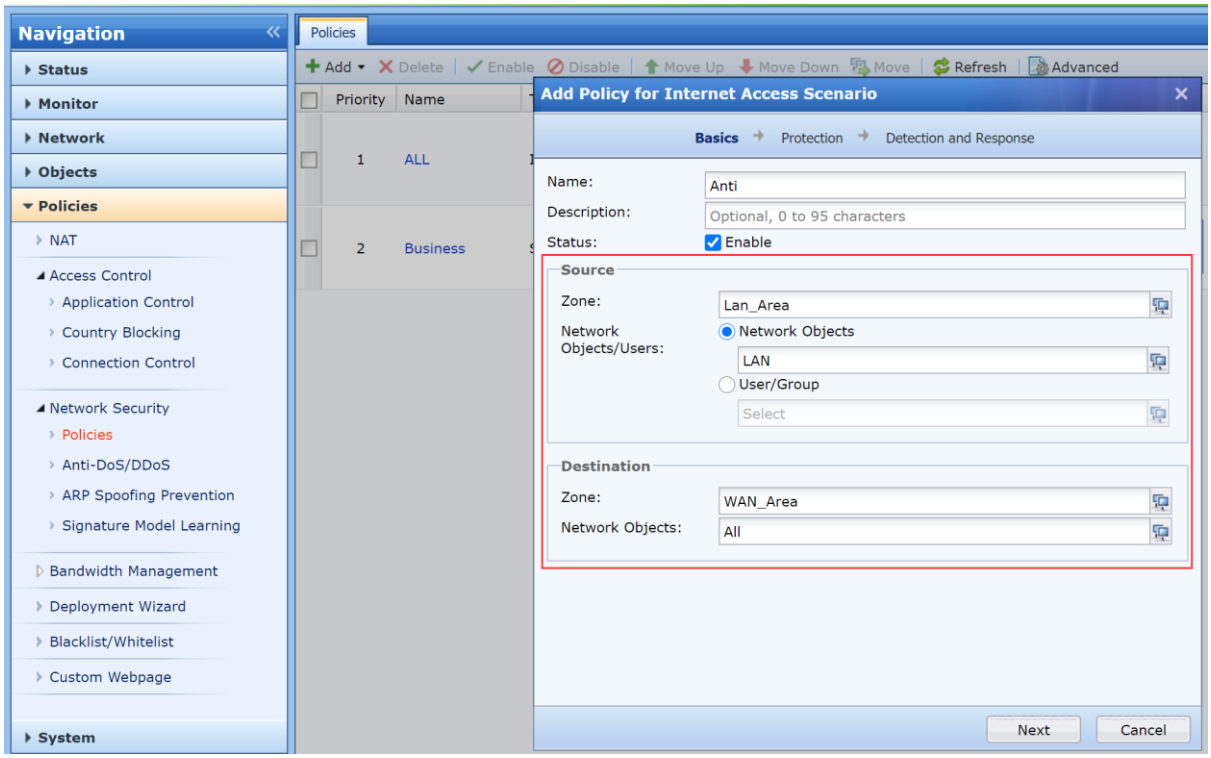
5.Configure Security Policy Template


Navigation
Status
Monitor
Network
Objects
Network Objects
Services
Security Policy Template
Intrusion Prevention
Web App Protection
APT Detection
Content Security
Threat Signature Databases
Content Identification Databases
IP Address Database
Schedule
Trusted CA
Policies
System
Content Security
Add
Delete
Refresh
No.
Name
Email Protection
URL Filter
1
Bot
Enable
Disable
New
Name:
Content
Description:
Protection
Email Protection (It will scan e
Sangfor Engine Zero.)
Server Port:
Malicious Email Alert:
URL Filter
Sites:
File Protection (It will filter file
Schedule:
All week
Advanced Settings
URL Database
View: All
Selected
12 objects
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
Adult Content
Illegal Content
Phishing & Malicious We...
Fake Site
Adware
Malware Attack
Exploit
Mining
Redirection
XSS
Clickjacking
Malicious Script Attack
Add
OK
Cancel

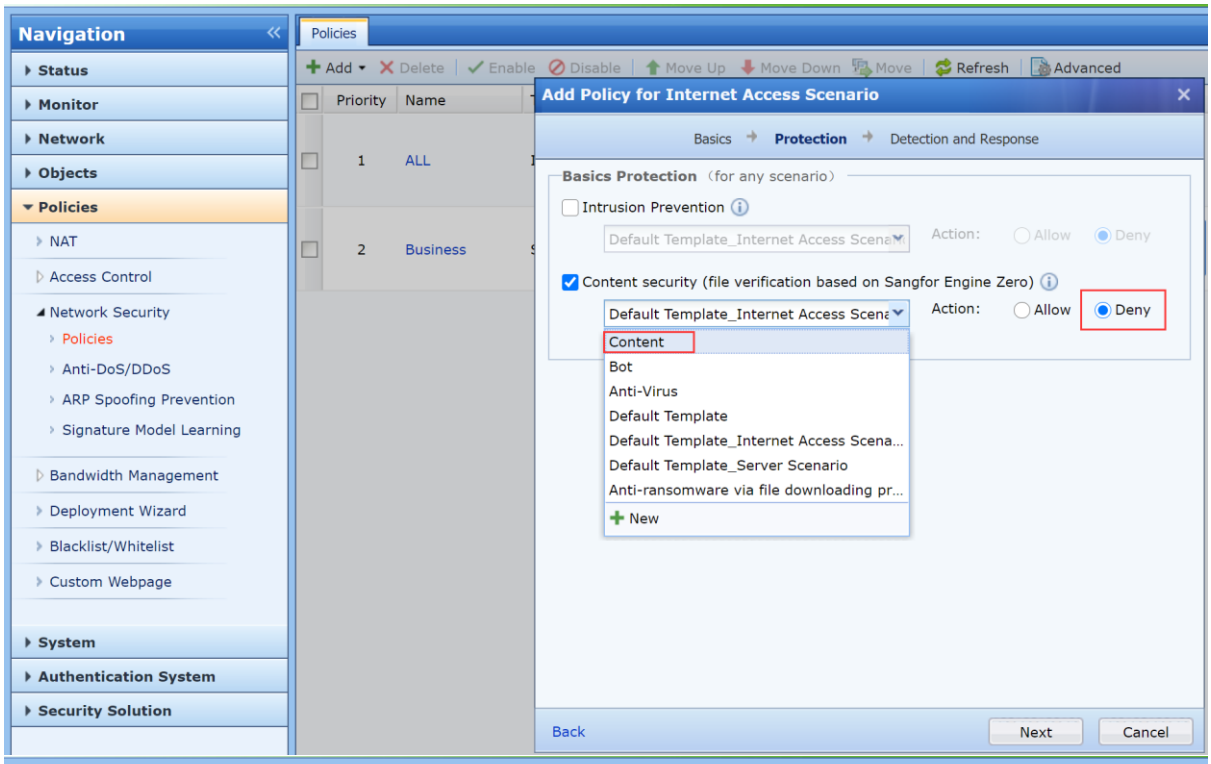

Navigation
Status
Monitor
Network
Objects
Network Objects
Services
Security Policy Template
Intrusion Prevention
Web App Protection
APT Detection
Content Security
Threat Signature Databases
Content Identification Databases
IP Address Database
Schedule
Trusted CA
Policies
System
Authentication System
Content Security
Add
Delete
Refresh
No.
Name
1
Bot
New
Name:
Content
Description:
Protection
Email Protection (It will scan
Sangfor Engine Zero.)
Server Port:
Malicious Email Alert:
URL Filter
Sites:
Adult
File Protection (It will filter fi
Schedule:
All week
Advanced Settings
Advanced Settings
Email Protection
Detect email contents (abnormal
Max Attempts Per Min:
15
Filter email attachments
File Signatures:
URL Filter
Request Method:
HTTP(get)
File Protection
File Filter
File Signatures:
Direction:
Both
Sangfor Engine Zero Based File Verification
File Signatures:
Movie,Music,Image,Text,Compressed File,Ap
Protect downloads to internal servers
OK
Cancel
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
OK
Cancel

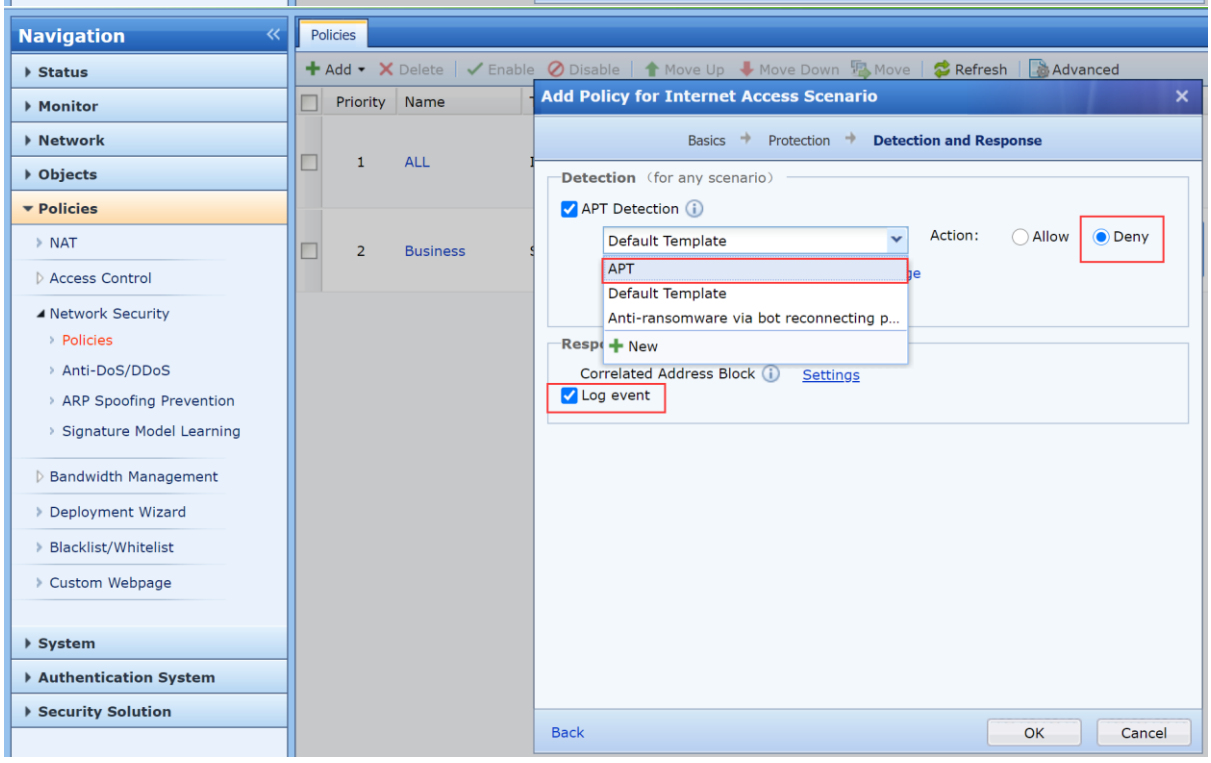


6. Ensure that the Source zone and Destination Zone is correct



7.Configure security policy and check the template you configured before.

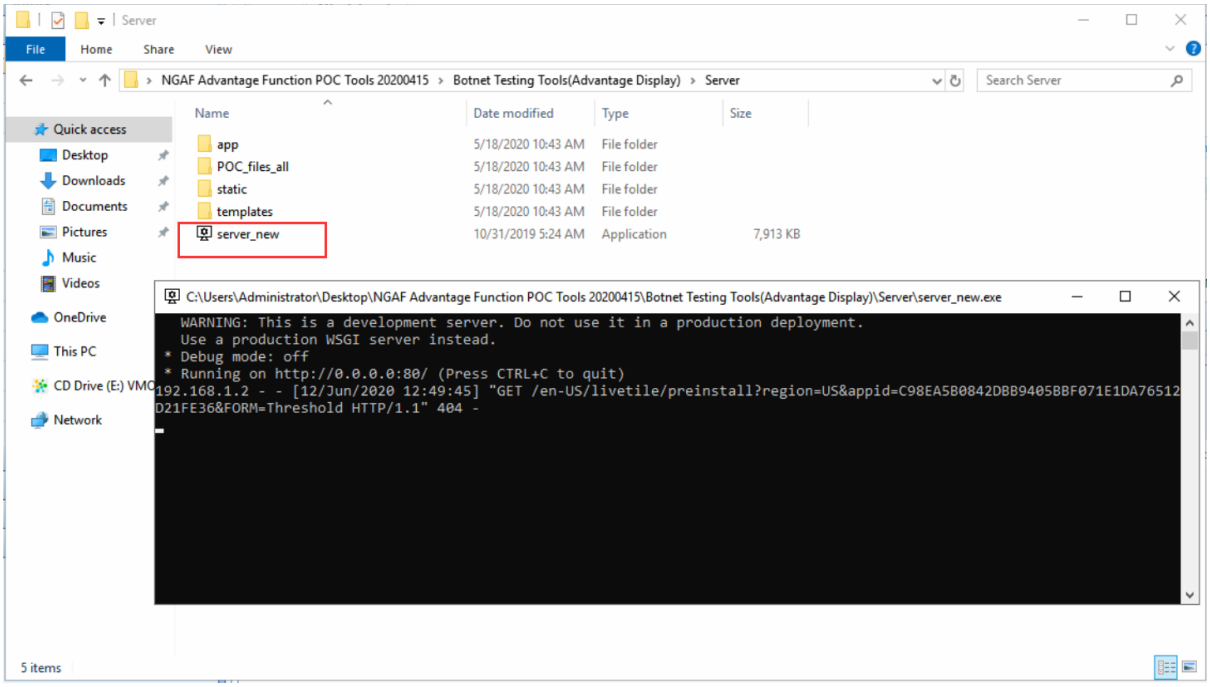




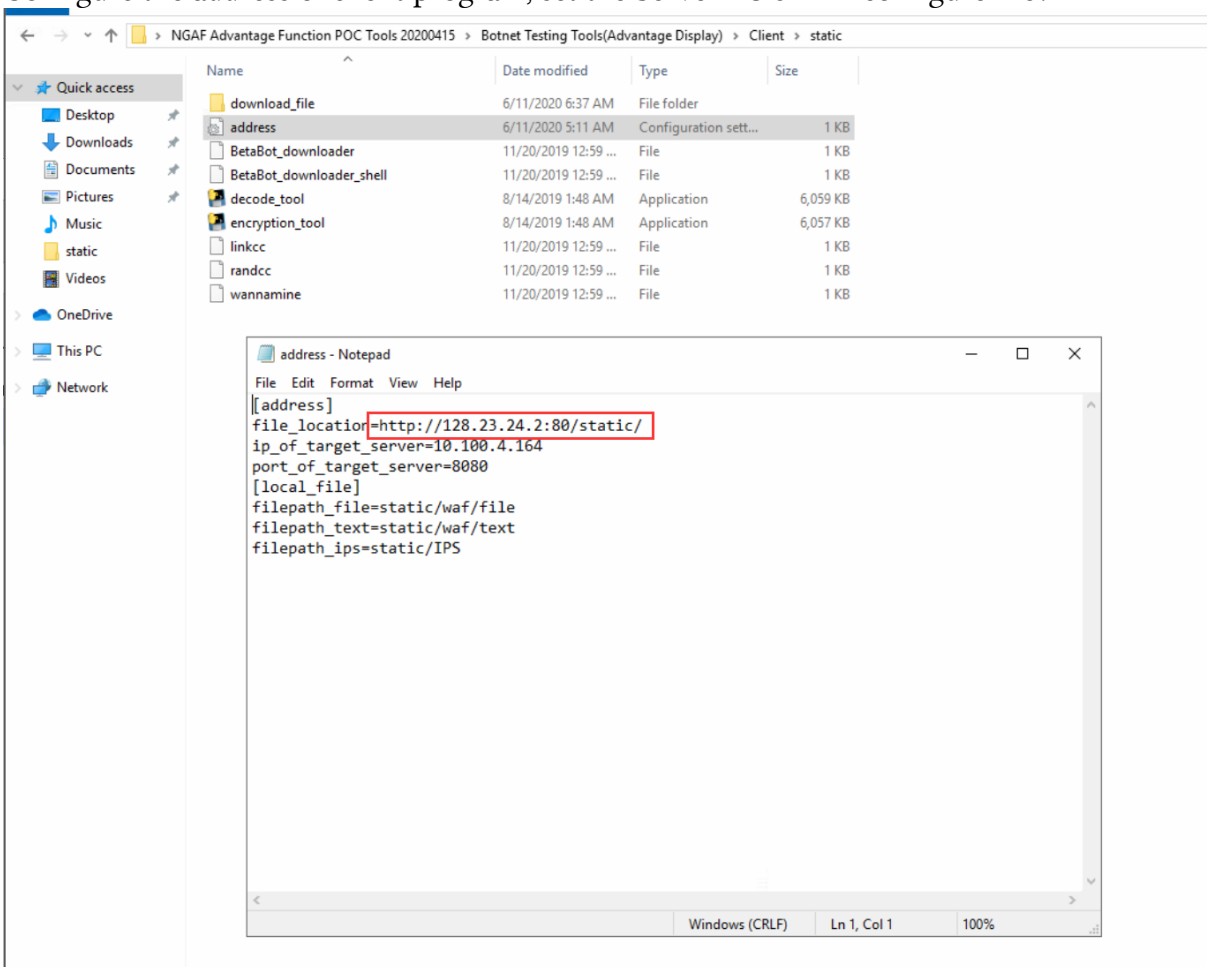
8. For example, when defending against botnets, the trapped host will access a large number of domain names, and these domain names are not included in the local database, then Neural-X needs to be used for authentication detection.

9. The attacker traps the LAN user to insert unknown USB device, so as to trigger the worm virus [Advantage_Botnet_Script_2.exe] and the AF blocks the work that send traffic out to the malicious domain name address.

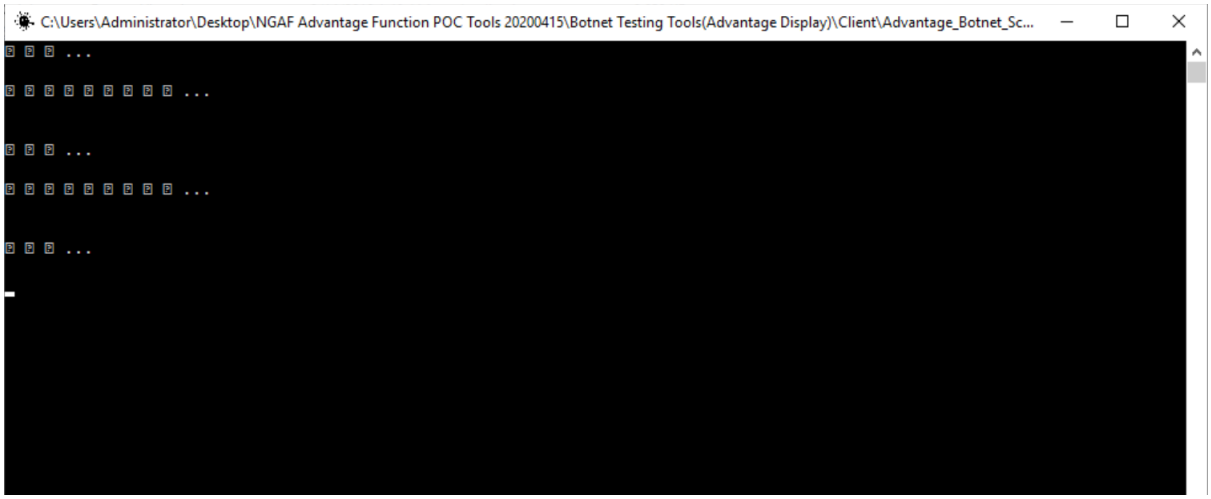
Run Server_new.exe in Server PC:



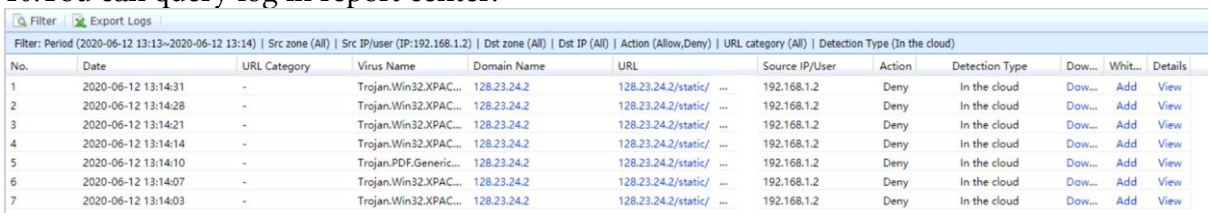
Configure the address of client program, set the Server PC's IP in configure file:



Run Advantage_Botnet_Script_2.exe in Client PC:



10.You can query log in 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