

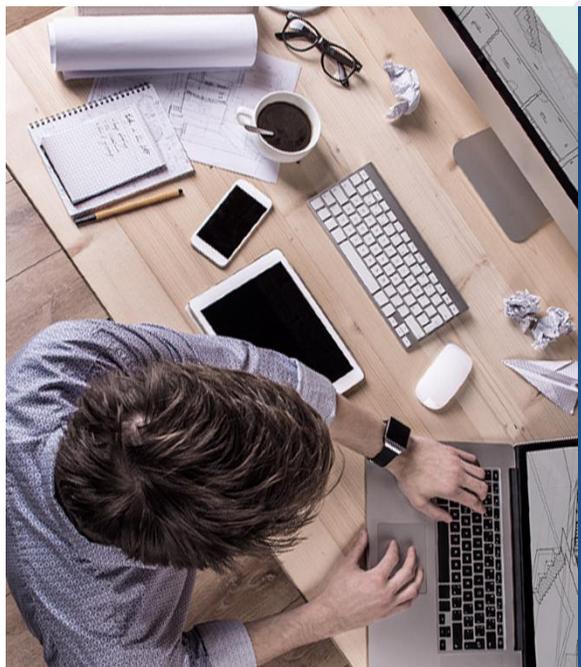


SANGFOR

Sangfor NGAF V8.0.6 Associate

Content security





- 1 Traffic Visibility
- 2 URL Filtering
- 3 File Filtering
- 4 Sangfor Engine Zero
- 5 Neural X

1. Traffic Visibility



Traffic visibility

Traditional packet filtering firewall control the packet filtering by ACL to make their network security.

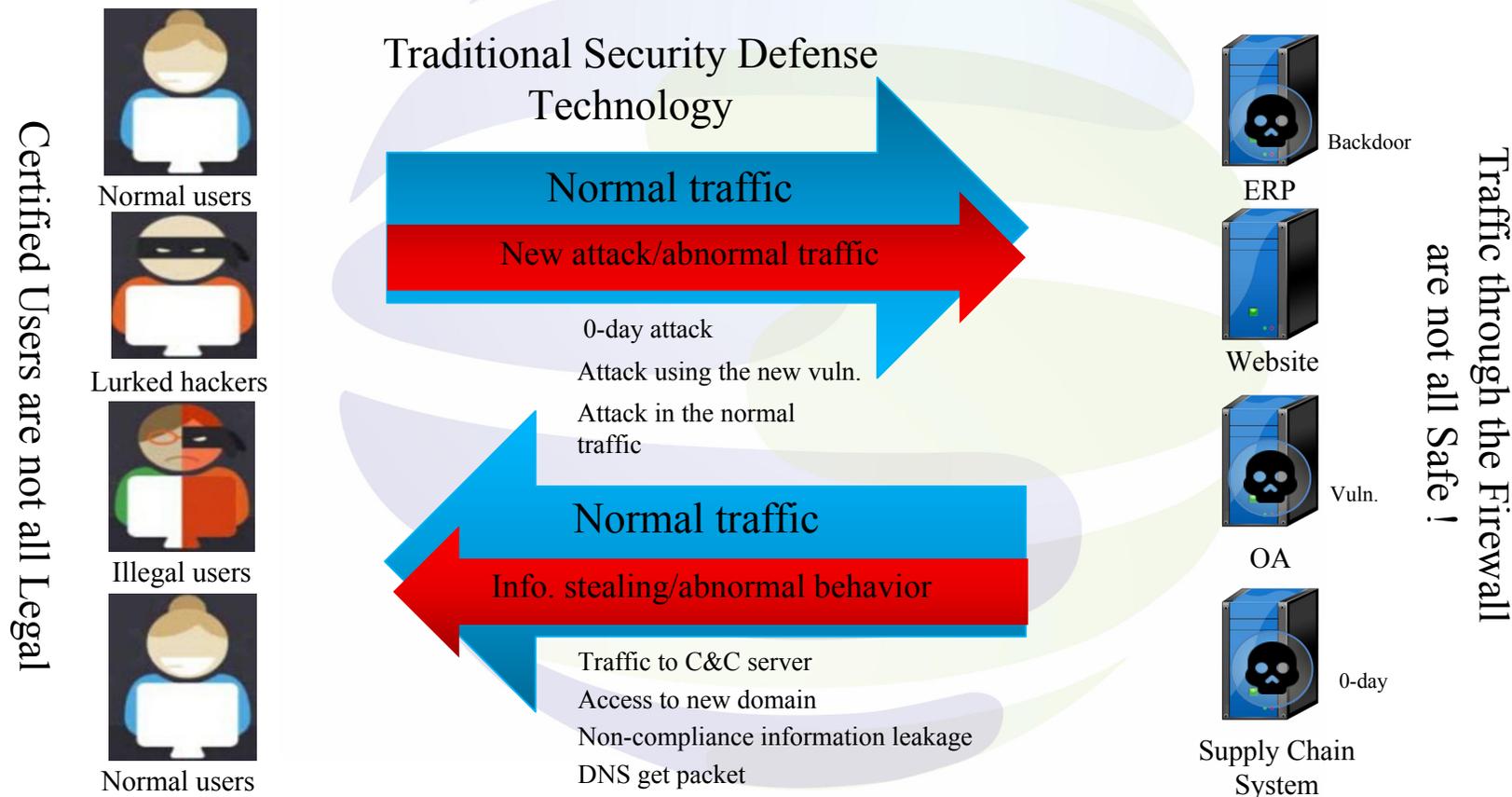
ACL control the traffic based on the source/destination IP, source/destination Port, protocol.



Is it safe enough
with ACL?

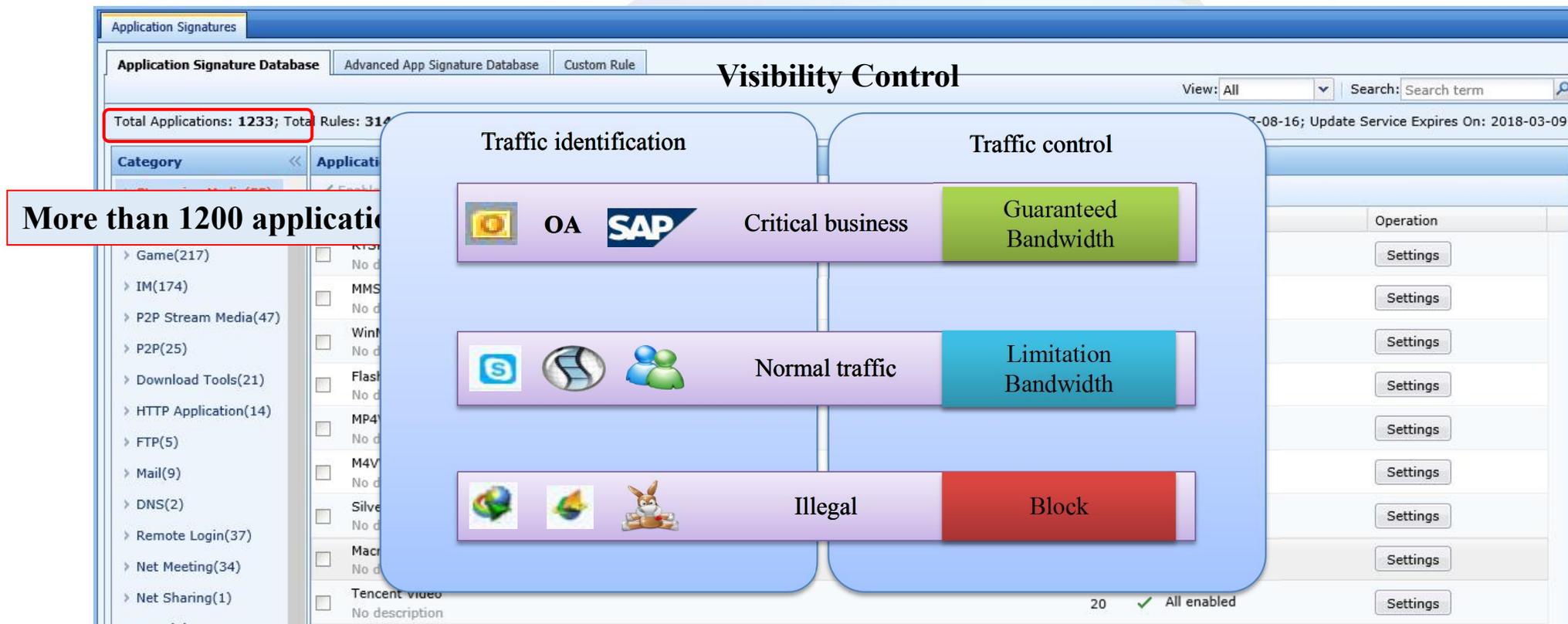
Traffic visibility

Many Invisible Security Risk in the Network



Traffic visibility

With the high identification rate application database, we can get all network traffic composition in time, making our traffic under our control and more security.



The screenshot displays the 'Application Signatures' interface with a 'Visibility Control' overlay. The interface shows a list of application categories on the left and a table of application signatures on the right. A red box highlights 'Total Applications: 1233; Total Rules: 314'. A callout box points to the application list with the text 'More than 1200 applications'. The 'Visibility Control' overlay is divided into two columns: 'Traffic identification' and 'Traffic control'. It lists three traffic categories with their corresponding control actions:

Traffic Identification	Traffic Control
 OA SAP Critical business	 Guaranteed Bandwidth
 Normal traffic	 Limitation Bandwidth
 Illegal	 Block

At the bottom of the overlay, it shows '20' and 'All enabled'. The background interface includes a search bar, a 'View' dropdown, and a 'Settings' button for each application signature.

2. URL Filtering



URL Filtering

What's the URL filtering?

NGAF identify the URL is allowed or denied by detecting the HTTP request, then take the corresponding action.

Why do we need URL filtering?

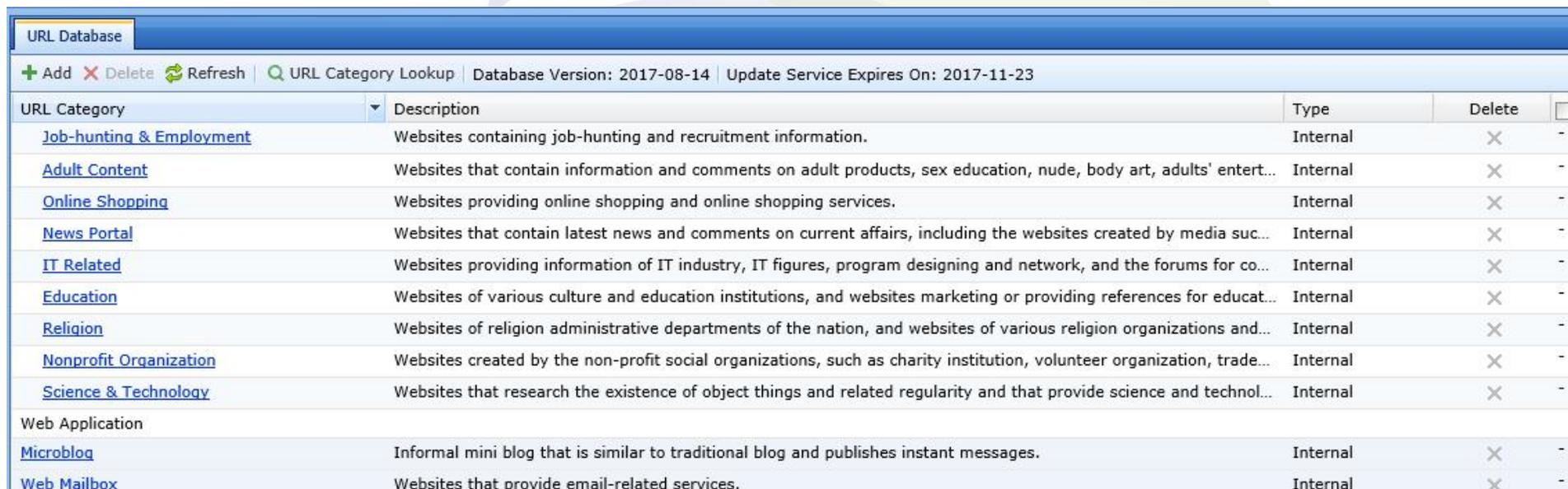
- Inappropriate content: Porn, adult content, drugs so on.
- Phishing and Malicious link, the website with the trojan, virus.
- Website unrelated with works: online video, game.



URL Filtering

URL database:

- More the 60 types;
- Millions of website;
- Update every two weeks
- URL category lookup
- Customize the URL



URL Database

+ Add X Delete Refresh URL Category Lookup Database Version: 2017-08-14 Update Service Expires On: 2017-11-23

URL Category	Description	Type	Delete	
Job-hunting & Employment	Websites containing job-hunting and recruitment information.	Internal	X	-
Adult Content	Websites that contain information and comments on adult products, sex education, nude, body art, adults' entert...	Internal	X	-
Online Shopping	Websites providing online shopping and online shopping services.	Internal	X	-
News Portal	Websites that contain latest news and comments on current affairs, including the websites created by media suc...	Internal	X	-
IT Related	Websites providing information of IT industry, IT figures, program designing and network, and the forums for co...	Internal	X	-
Education	Websites of various culture and education institutions, and websites marketing or providing references for educat...	Internal	X	-
Religion	Websites of religion administrative departments of the nation, and websites of various religion organizations and...	Internal	X	-
Nonprofit Organization	Websites created by the non-profit social organizations, such as charity institution, volunteer organization, trade...	Internal	X	-
Science & Technology	Websites that research the existence of object things and related regularity and that provide science and technol...	Internal	X	-
Web Application				
Microblog	Informal mini blog that is similar to traditional blog and publishes instant messages.	Internal	X	-
Web Mailbox	Websites that provide email-related services.	Internal	X	-

Content Security

URL filtering

Edit Template

Name: all url
Description:

Protection

Email Protection (It will scan email body, filter email attachments and verify files based on engine Zero.)
Server Port: 25,110,143
Malicious Email Alert: It contains malicious content.

URL Filter
Sites: Job-hunting & Employment, Adult Content, Online Shopping, News Portal, IT Related, Education, Religion, Nonprofit, Science & Technology, Life Related, Finance, Entertainment, Policy & Law, Business & Industry, Network Security, Software & Applications

File Protection (It will filter files and verify file based on engine Zero.)

Schedule: All week

Advanced Settings OK Cancel

URL Database

View: All

Selected: 6 objects

- All
 - Job-hunting & Employment
 - Adult Content
 - Online Shopping
 - News Portal
 - IT Related
 - Education
 - Religion
 - Nonprofit
 - Science & Technology
 - Illegality & Security
 - Life Related
 - Finance
 - Entertainment
 - Policy & Law
 - Business & Industry
 - Network Security
 - Software & Applications

Advanced Settings

Email Protection

Detect email contents (abnormal account, phishing emails)
Max Attempts Per Min: 15

Filter email attachments
File Signatures: Email Attachment Filter List

Engine Zero Based File Verification
File Signatures: Compressed File, Application Program, Antivirus

URL Filter

Request Method: HTTP(get) HTTP(post) HTTPS

File Protection

OK Cancel

URL filter is based on URL category

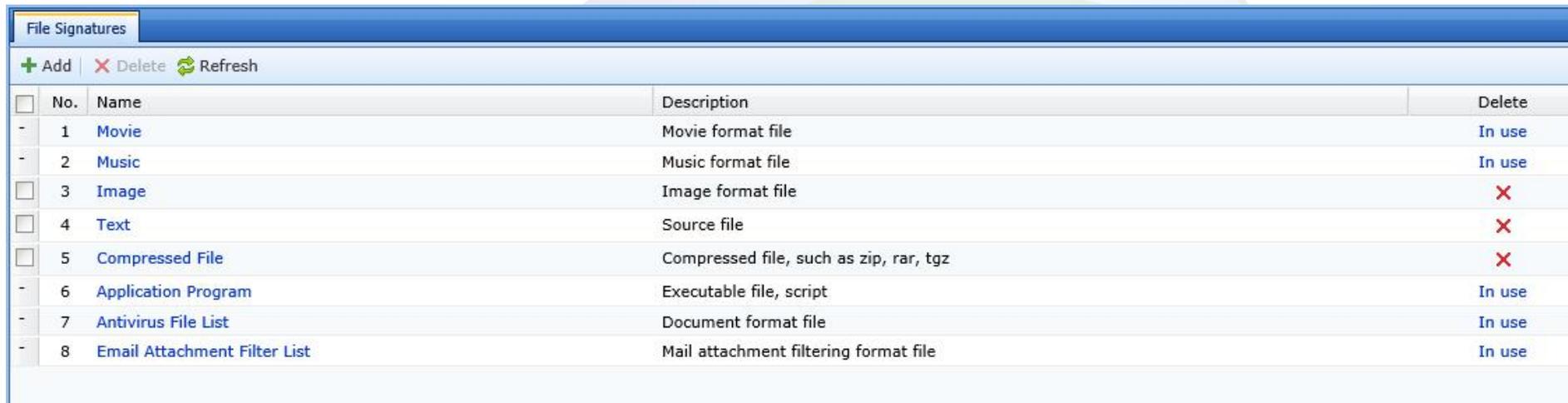
HTTP(get): Unable to visit certain websites
HTTP(post): Can open webpage but can't upload file
HTTPS: Select to enforce policy on https websites

3. File Filtering



File Filtering

Predefined common file signatures and could customize for file filtering and file virus scanning.

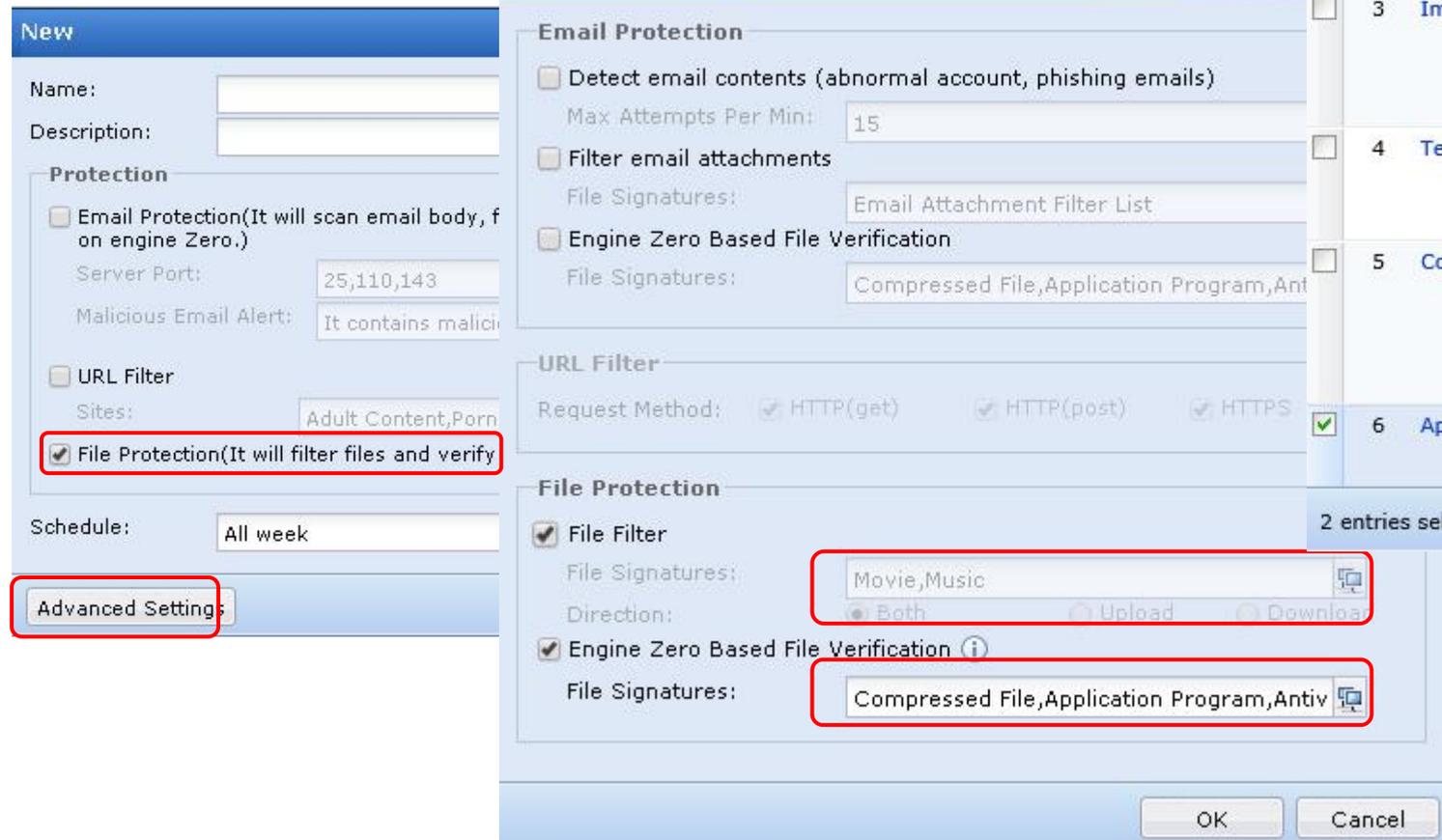


The screenshot shows a web interface for managing file signatures. At the top, there is a blue header with the title 'File Signatures'. Below the header, there are three action buttons: '+ Add', 'X Delete', and a refresh icon labeled 'Refresh'. The main content is a table with four columns: 'No.', 'Name', 'Description', and 'Delete'. The table contains eight rows of predefined file signatures. The 'Delete' column for rows 3, 4, and 5 shows a red 'X', while rows 1, 2, 6, 7, and 8 show 'In use'.

<input type="checkbox"/>	No.	Name	Description	Delete
-	1	Movie	Movie format file	In use
-	2	Music	Music format file	In use
<input type="checkbox"/>	3	Image	Image format file	X
<input type="checkbox"/>	4	Text	Source file	X
<input type="checkbox"/>	5	Compressed File	Compressed file, such as zip, rar, tgz	X
-	6	Application Program	Executable file, script	In use
-	7	Antivirus File List	Document format file	In use
-	8	Email Attachment Filter List	Mail attachment filtering format file	In use

Content Security

File protection



The screenshot displays the NGAF configuration interface for File Protection. The main window is titled "Advanced Settings" and includes sections for "Email Protection", "URL Filter", and "File Protection".

In the "File Protection" section, the "File Filter" checkbox is checked. The "File Signatures" field is set to "Movie,Music". The "Engine Zero Based File Verification" checkbox is also checked, with "File Signatures" set to "Compressed File,Application Program,Antiv".

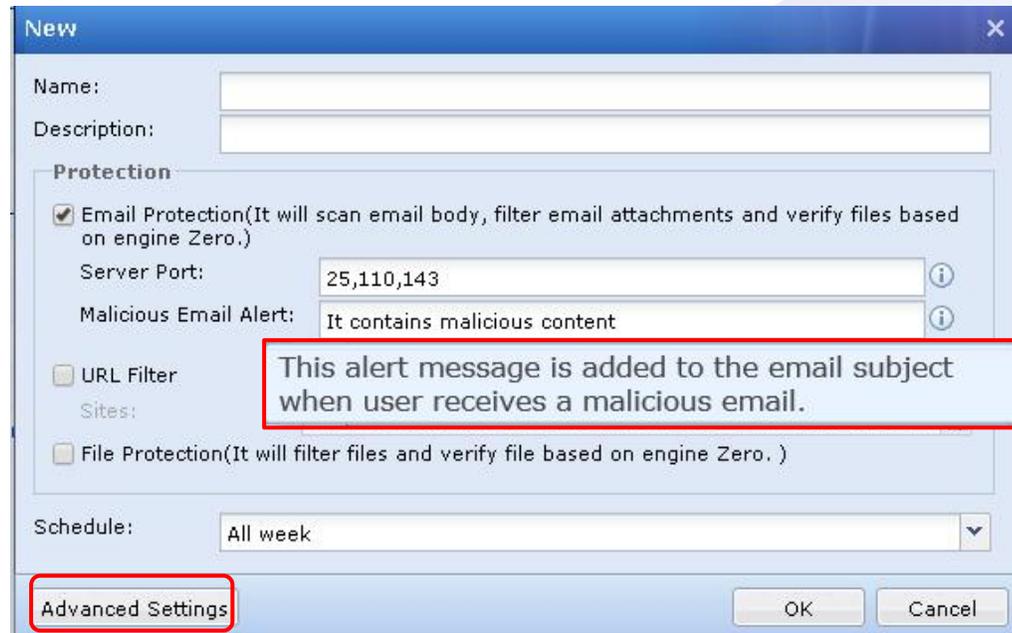
A "Select File Signature" dialog box is open, showing a list of file signatures and their corresponding file extensions. The "Application Program" signature is selected, and its file extensions are listed as bat, cmd, and com.

Red boxes highlight the "File Protection" section in the main window, the "File Signatures" field, the "Engine Zero Based File Verification" section, and the "Advanced Settings" button.

Filtering file and detecting the virus file in FTP/HTTP protocol. If filter some file type, NGAF don't detect the file contained virus or not.

Content Security

Email Security



Name:

Description:

Protection

Email Protection(It will scan email body, filter email attachments and verify files based on engine Zero.)

Server Port:

Malicious Email Alert:

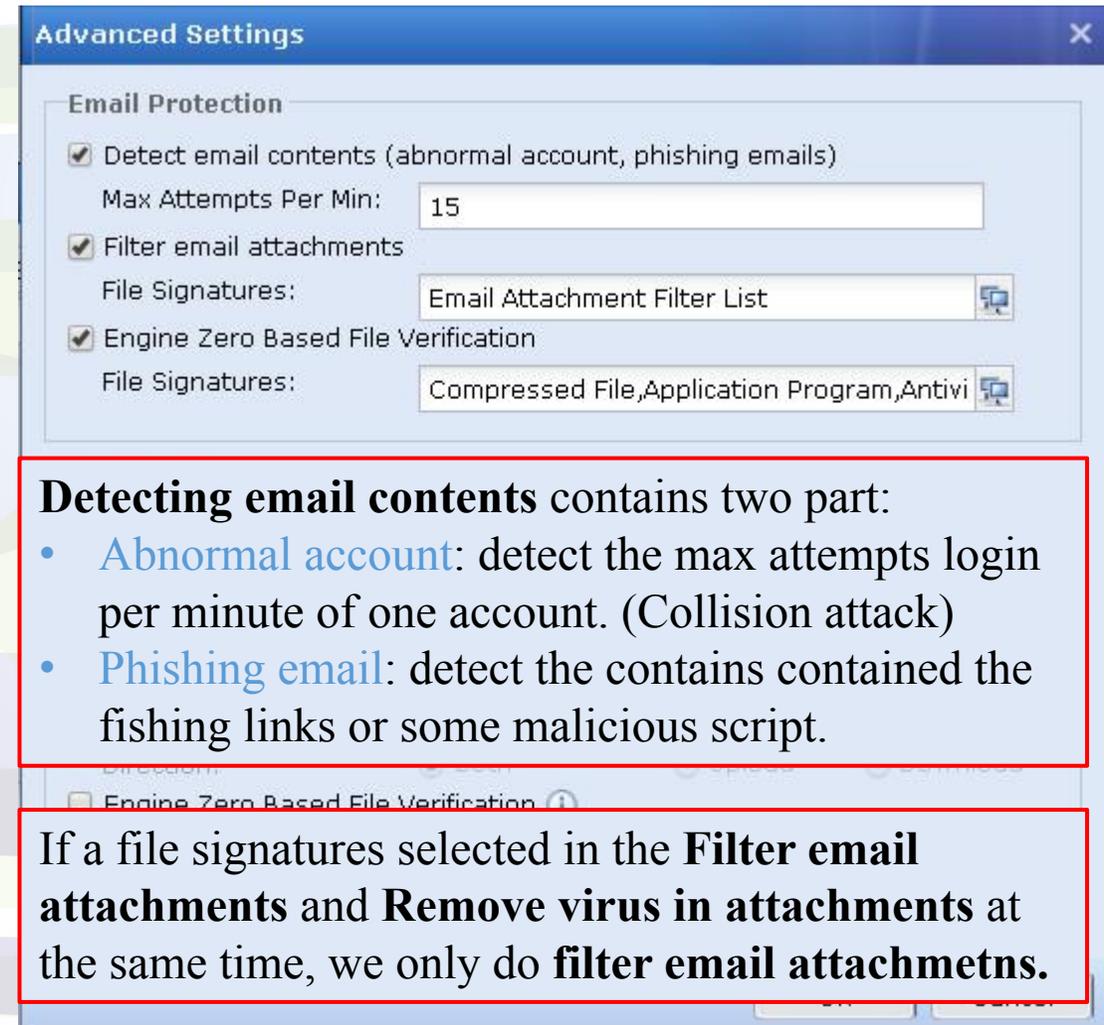
URL Filter

Sites:

File Protection(It will filter files and verify file based on engine Zero.)

Schedule:

Advanced Settings OK Cancel



Advanced Settings

Email Protection

Detect email contents (abnormal account, phishing emails)

Max Attempts Per Min:

Filter email attachments

File Signatures:

Engine Zero Based File Verification

File Signatures:

Detecting email contents contains two part:

- Abnormal account:** detect the max attempts login per minute of one account. (Collision attack)
- Phishing email:** detect the contains contained the fishing links or some malicious script.

If a file signatures selected in the Filter email attachments and Remove virus in attachments at the same time, we only do filter email attachmetns.

Precautions

- a. Content security policy support decryption, you should enable decryption Policy.
- b. Mail protection support mail attachments with virus, malicious link, XSS attack, file filter, Collision Attack.
- c. Mail protection default detect port 25,110,143, it can support other port by custom.
- d. When clients accept malicious mail, NGAF don't deny it even if the action of policy is deny, but NGAF will tamper the mail subject if the action of policy is deny.
- e. The log of HTTP/HTTPS download/upload, FTP download/upload is recorded in Application Control, not in Content Security Policy.

4. Sangfor Engine Zero



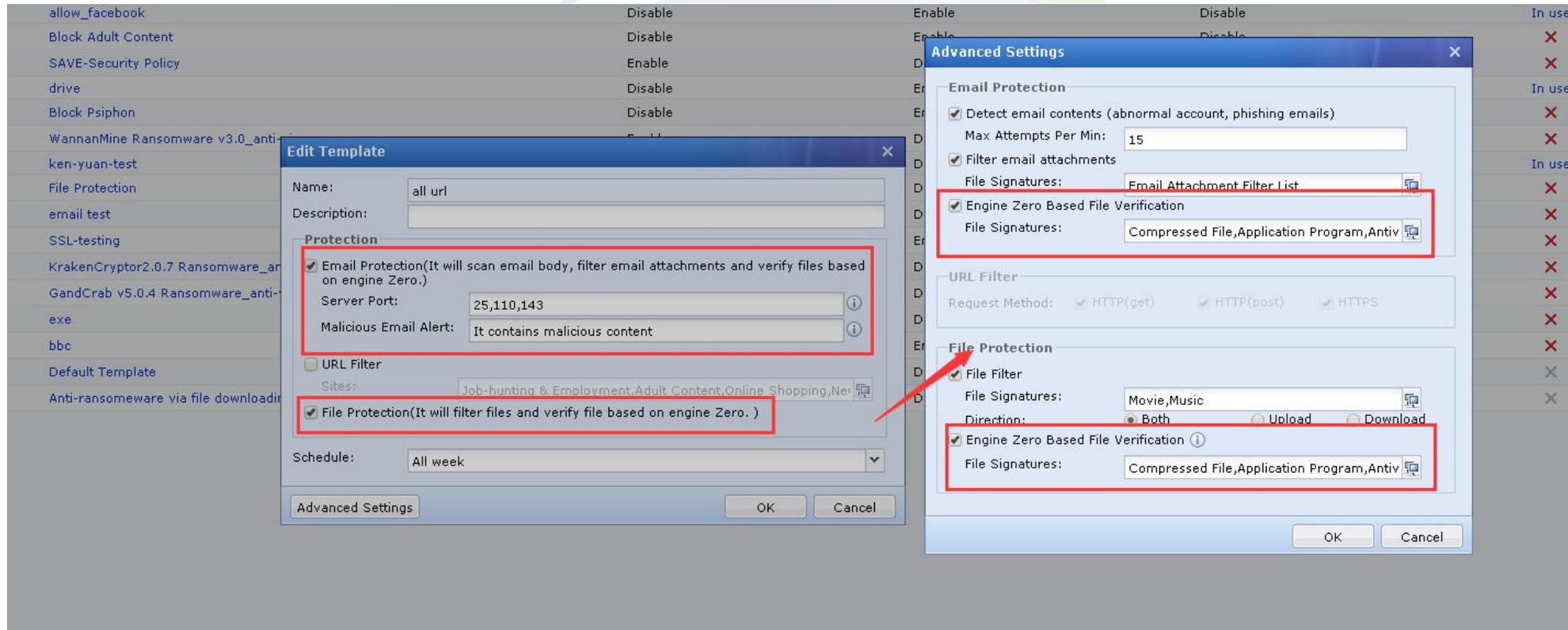
SAVE Engine

SAVE (Sangfor AI-based Vanguard Engine) is an artificial intelligence malicious file detection engine which this engine uses deep learning technology to analyze and synthesize hundreds of millions of original features, combined with the domain knowledge of security experts, and finally selects thousands of most efficient high-dimensional features for the identification of malicious files.

- Based on artificial intelligence technology, it **has powerful generalization ability** to identify unknown viruses or new variants of known viruses;
- The **detection effect of ransom virus has reached the industry leading level** , including WannaCry, BadRabbit and other viruses, and has a better detection effect on non-lesoviruses;
- **Cloud + device + end linkage** , relying on the security data of deep convincing security cloud brains, SAVE can continue to evolve, constantly update the model and improve detection capabilities, thus forming a perfect combination of local traditional engine, artificial intelligence detection engine and cloud killing engine.

Save Engine Configuration

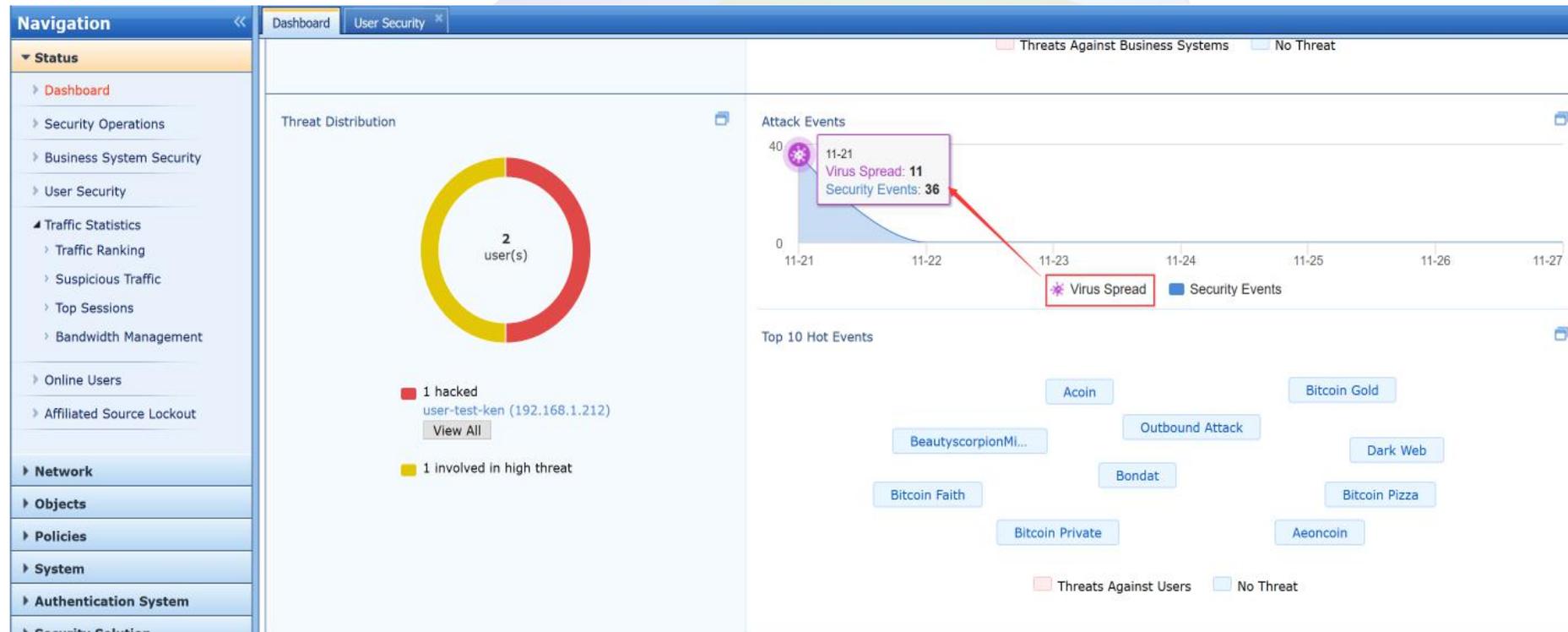
Configuration Path: Object > Security Policy Template > Content Security > Add



Note: Save Engine currently support to detect PE type file only like exe, object code, DLLs, FON Font files and etc.

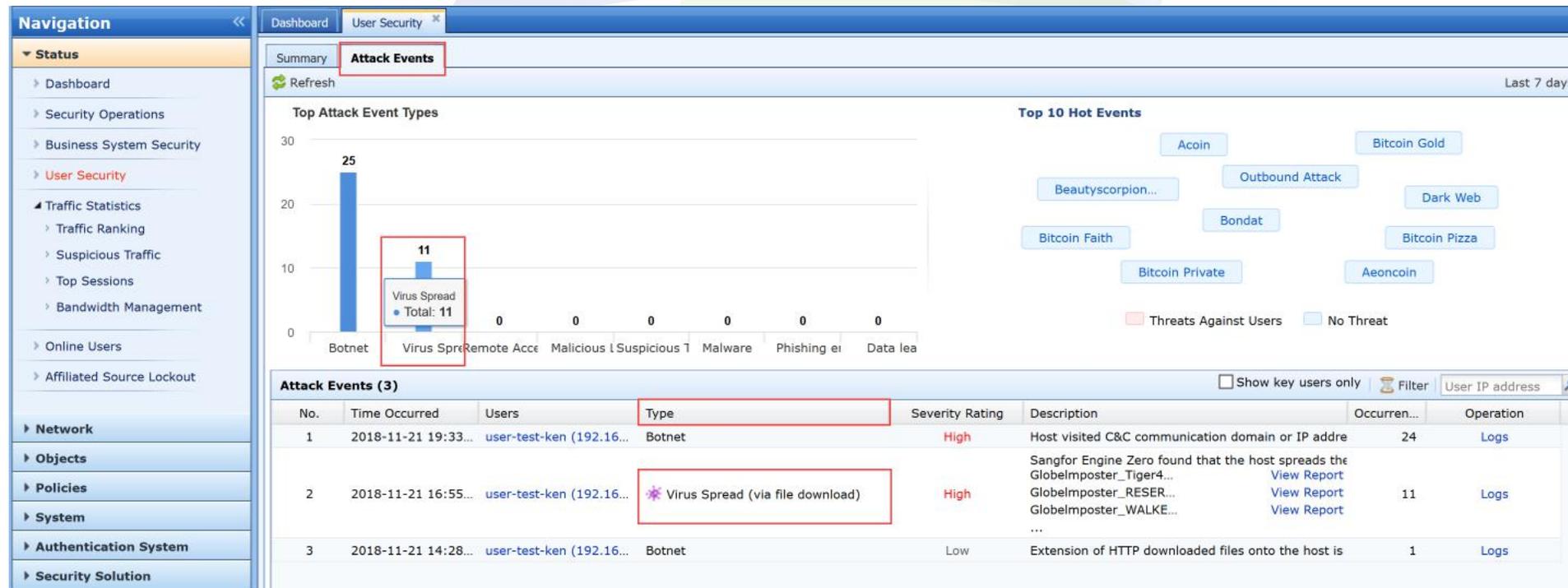
Placement and performance description

User security status of the Dashboard increases the virus spread icon



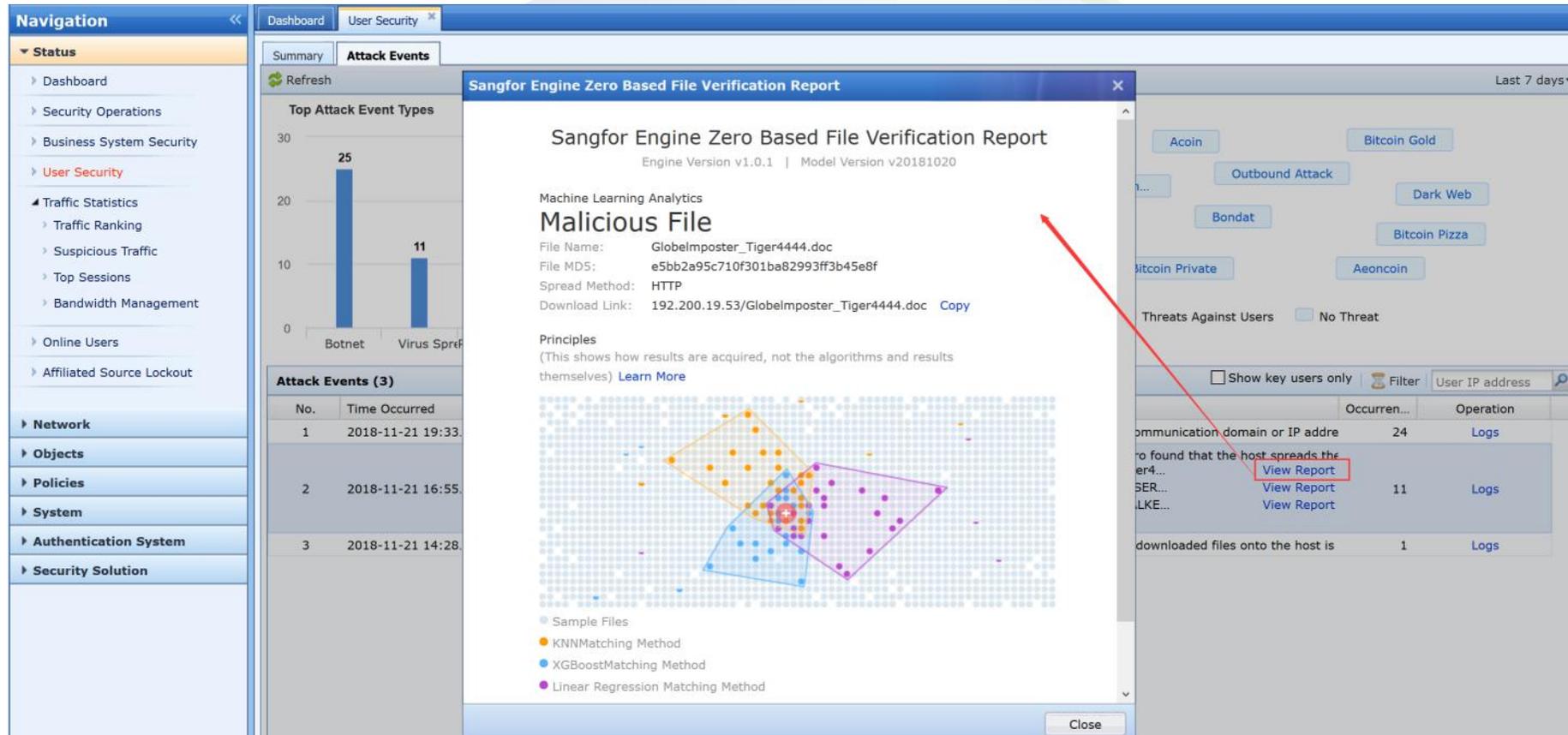
Placement and performance description

User Security - Attack Event, added Virus Propagation Histogram, Event type added virus propagation type.



Placement and performance description

Description added View Report about Virus Identification



The screenshot displays the Sangfor security dashboard with a 'User Security' tab selected. A 'Sangfor Engine Zero Based File Verification Report' window is open, showing details for a malicious file named 'Globelmposter_Tiger4444.doc'. The report includes a bar chart for 'Top Attack Event Types' (Botnet: 25, Virus Spread: 11), a table of 'Attack Events (3)', and a visualization of file matching methods. A red arrow points to the 'View Report' button in the table below the report window.

No.	Time Occurred
1	2018-11-21 19:33
2	2018-11-21 16:55
3	2018-11-21 14:28

	Occurren...	Operation
communication domain or IP address	24	Logs
no found that the host spreads the er4...	11	Logs
SER...	11	Logs
ILKE...	11	Logs
downloaded files onto the host is	1	Logs

5. Neural X



SANGFOR
深信服科技

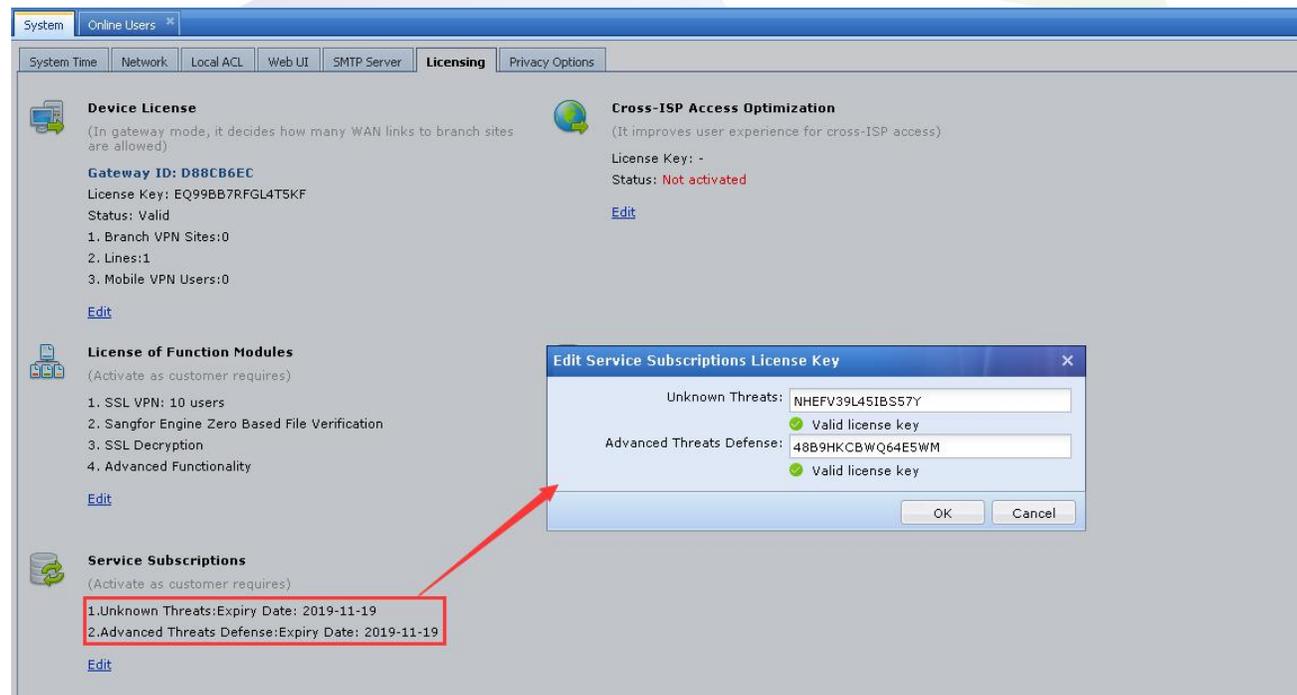
Neural X

- NGAF checks the passing data accordingly. When it finds that the local rule database cannot match, it uploads it to the Neural X to check whether it is risky data .
- The Neural X's rule database has more sources to continue to enrich the detection capabilities
- The local rule database of NGAF is limited in size, and there are hundreds of millions of rule databases on the cloud, so it cannot be delivered to the local rule database. In addition to a large number of rule databases, Neural X integrates many cloud detection engines. If some data cannot be matched by the rule database, it will detect the risk status through the detection engine. These cloud-based detection engines are also not available in NGAF for a short period of time.

Neural X Configuration



The Neural X does not need to be configured separately, and has the following three conditions .
The equipment version is AF8.0.5 and above;
The device can be connected to the Internet normally , and the data of the intranet user accessing the internet flows through the AF ;
The function serial number of the device Neural X has been normally turned on, System > General > Licensing, as shown below:



Neural X Precaution

1. The Neural X detection log takes about **6 minutes to 15 minutes to generate**, so you need to schedule the test time.
2. If you find that the DGA event is not generated, you can run the script several times, and each time you run the script, a DGA event will be generated.
3. AF only reports **200,000 gray domains every day**, so if the device with relatively large number of users, the report storage can be easily full. At this time, if you want to test again, you can only test it after restarting AF.
4. The Neural X 's disposal of the DGA domain name is **only analyzed and traced, and will not be intercepted** , so the user needs to check the terminal using the killing tool.

Thank you !

tech.support@sangfor.com

community.sangfor.com

Sangfor Technologies (Headquarters)

Block A1, Nanshan iPark, No.1001

Xueyuan Road, Nanshan District,

Shenzhen, Guangdong Province,

P. R. China (518055)

