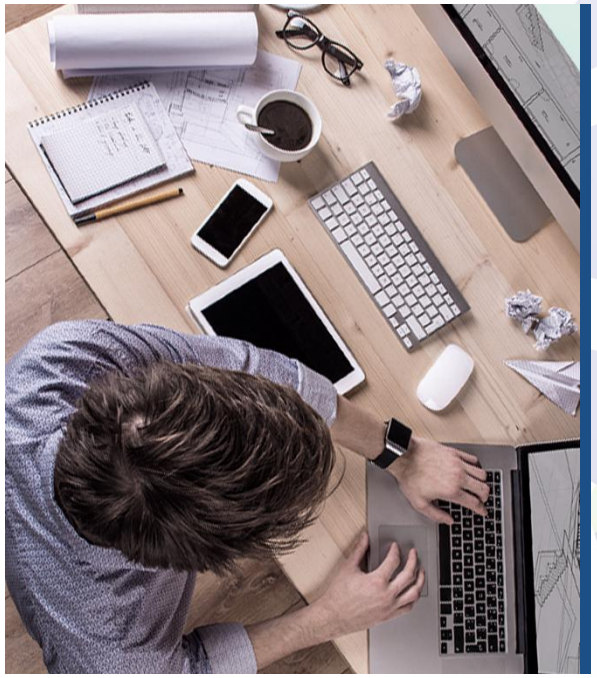
SANGFOR

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

SANGFOR
深信服科技

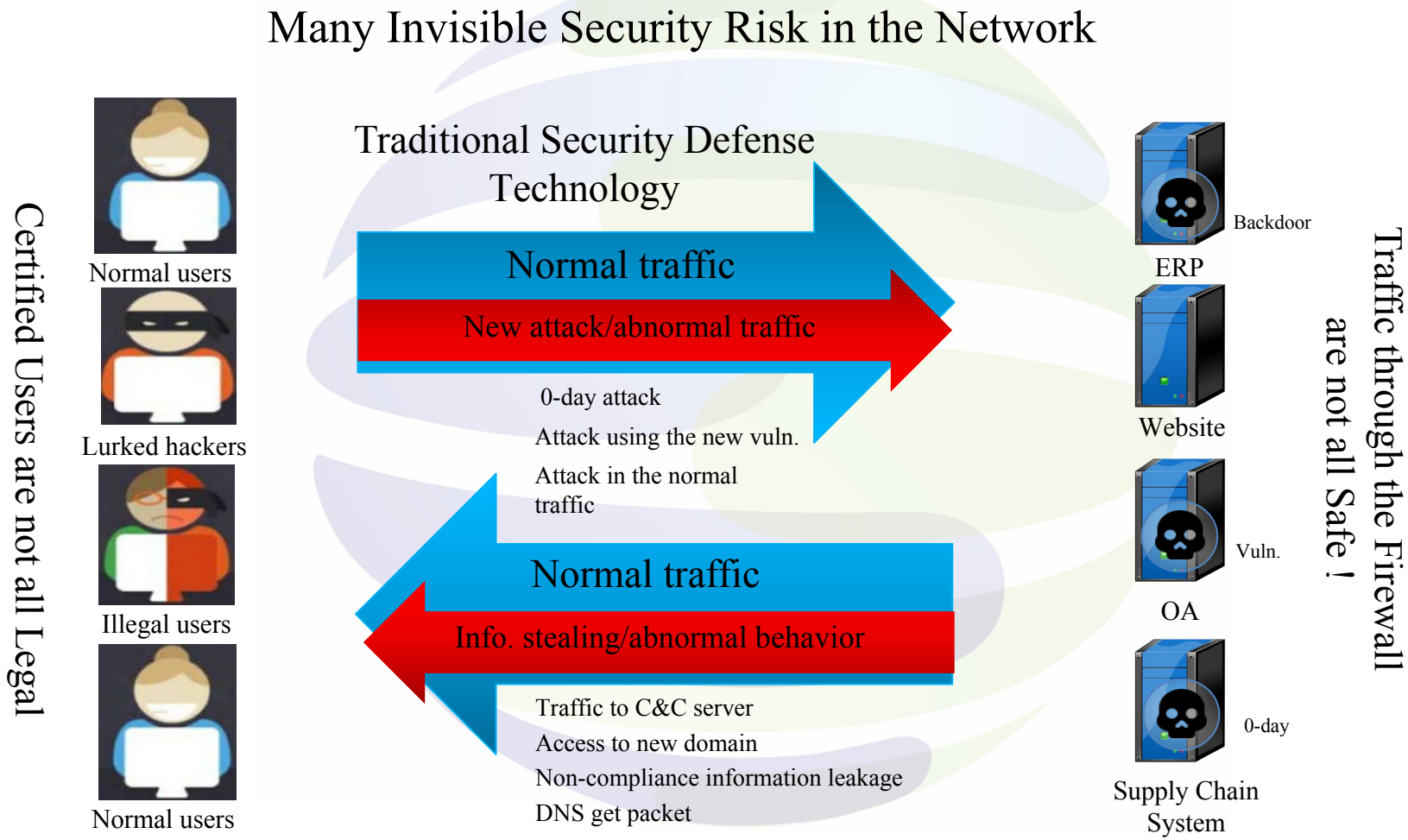
Traffic visibility

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.

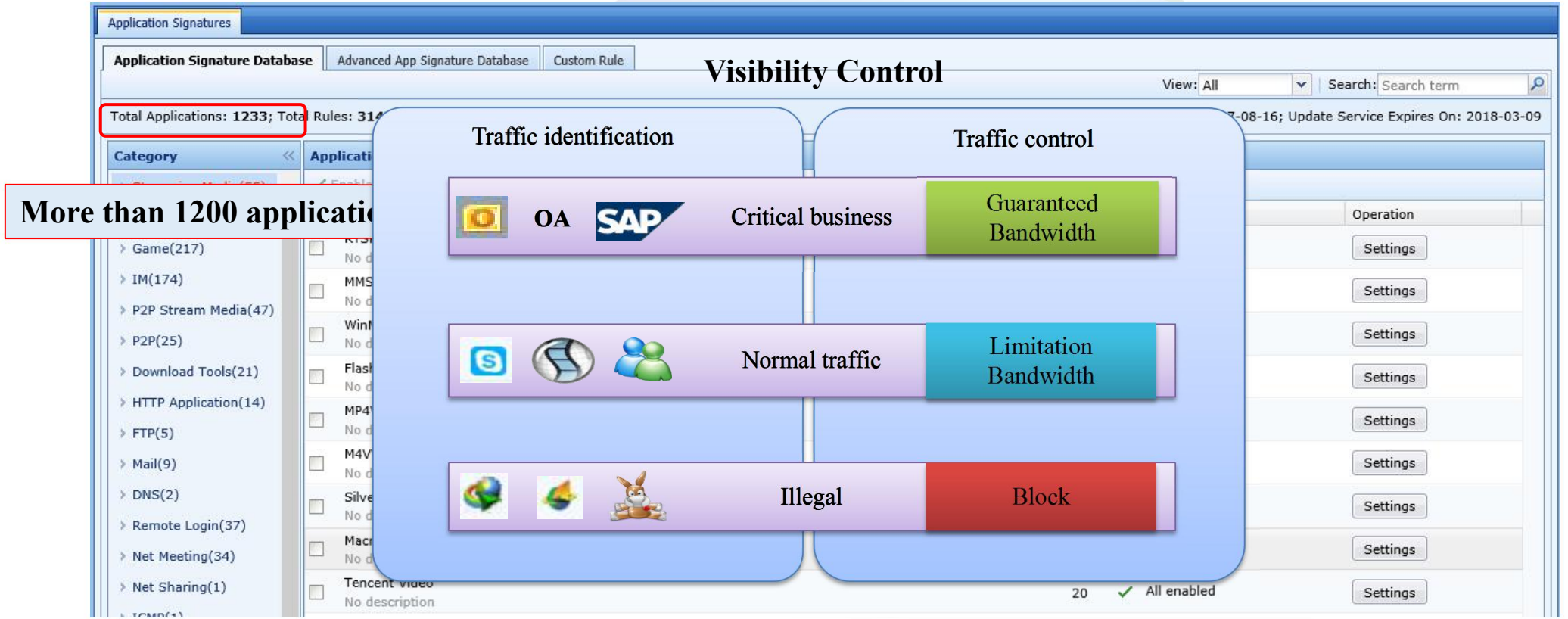
Is it safe enough
with ACL?

Traffic visibility



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.



2. URL Filtering

SANGFOR
深信服科技

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?

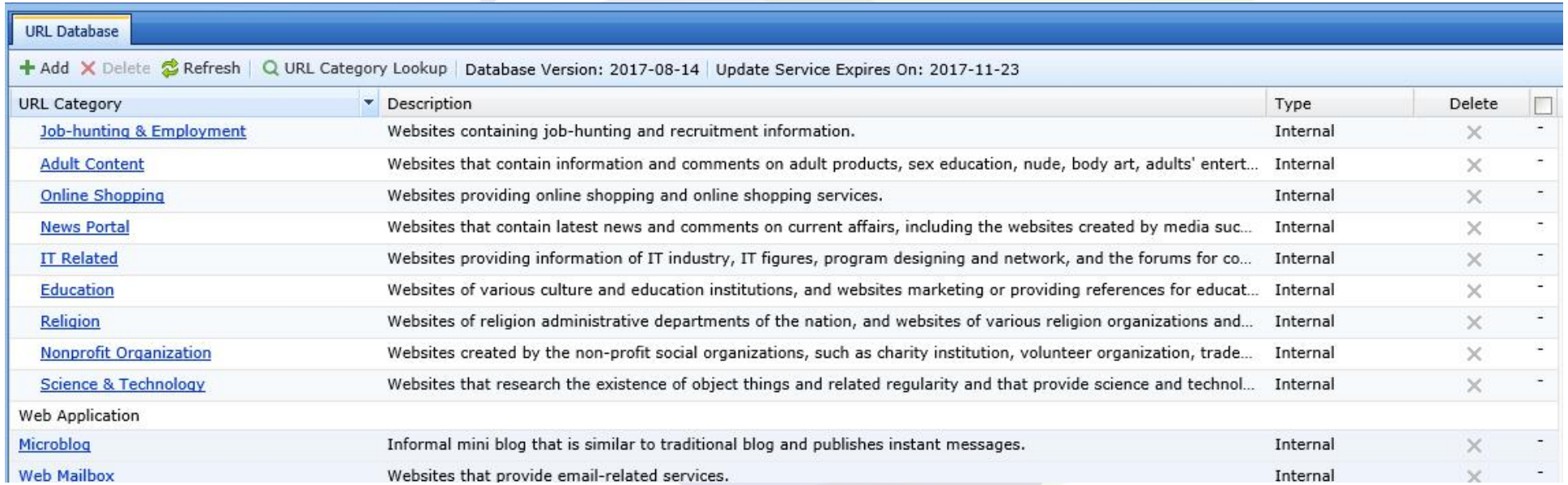
- Inappropriate content: Porn, adult content, drugs so on.
- Phishing and Malicious link, the website with the trojan, virus.
- Website unrelated with works: online video, game.

URL Filtering

URL database:

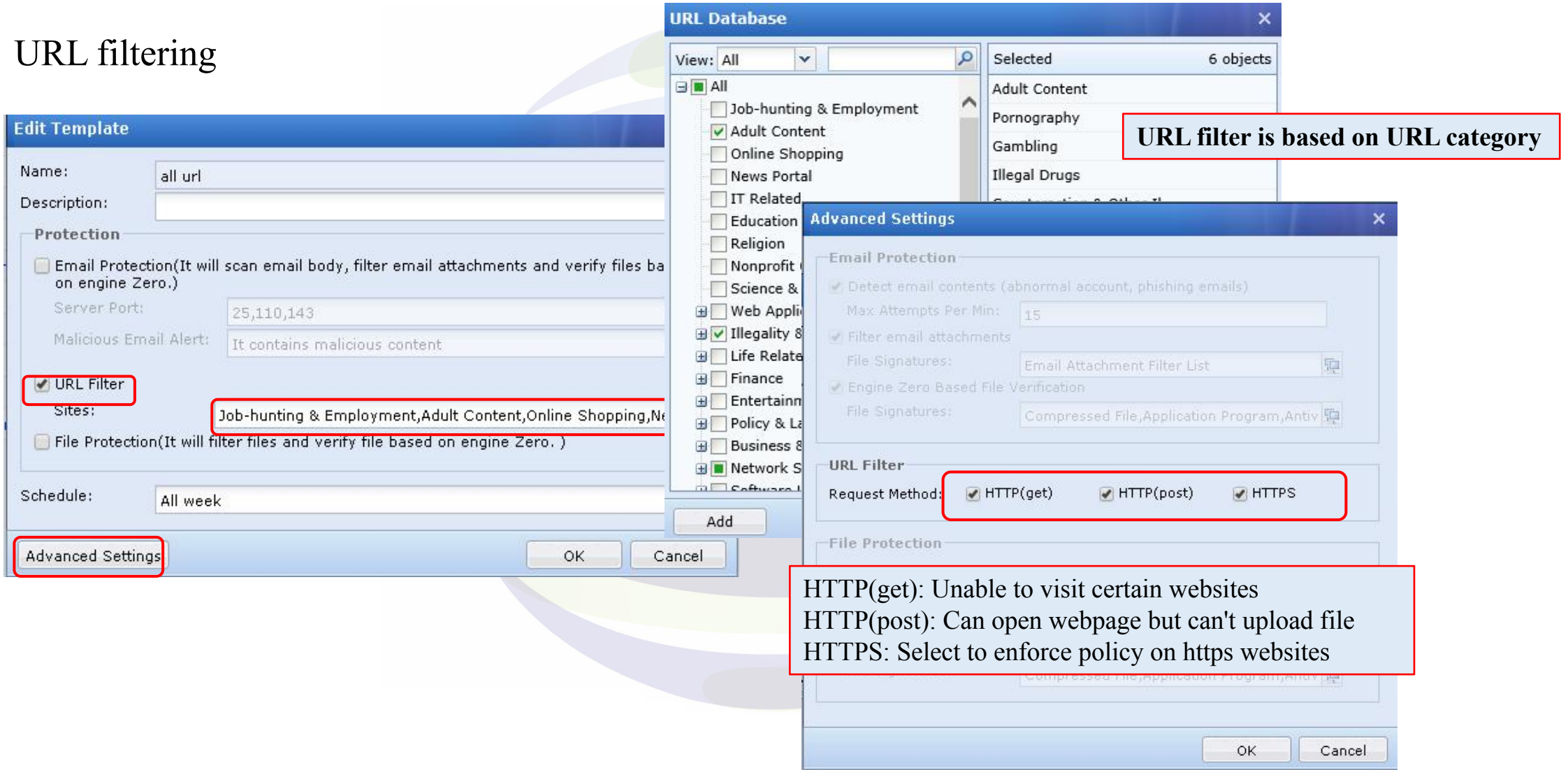
- More the 60 types;
- Millions of website;
- Update every two weeks

- URL category lookup
- Customize the URL



Content Security

URL filtering



3. File Filtering

SANGFOR
深信服科技

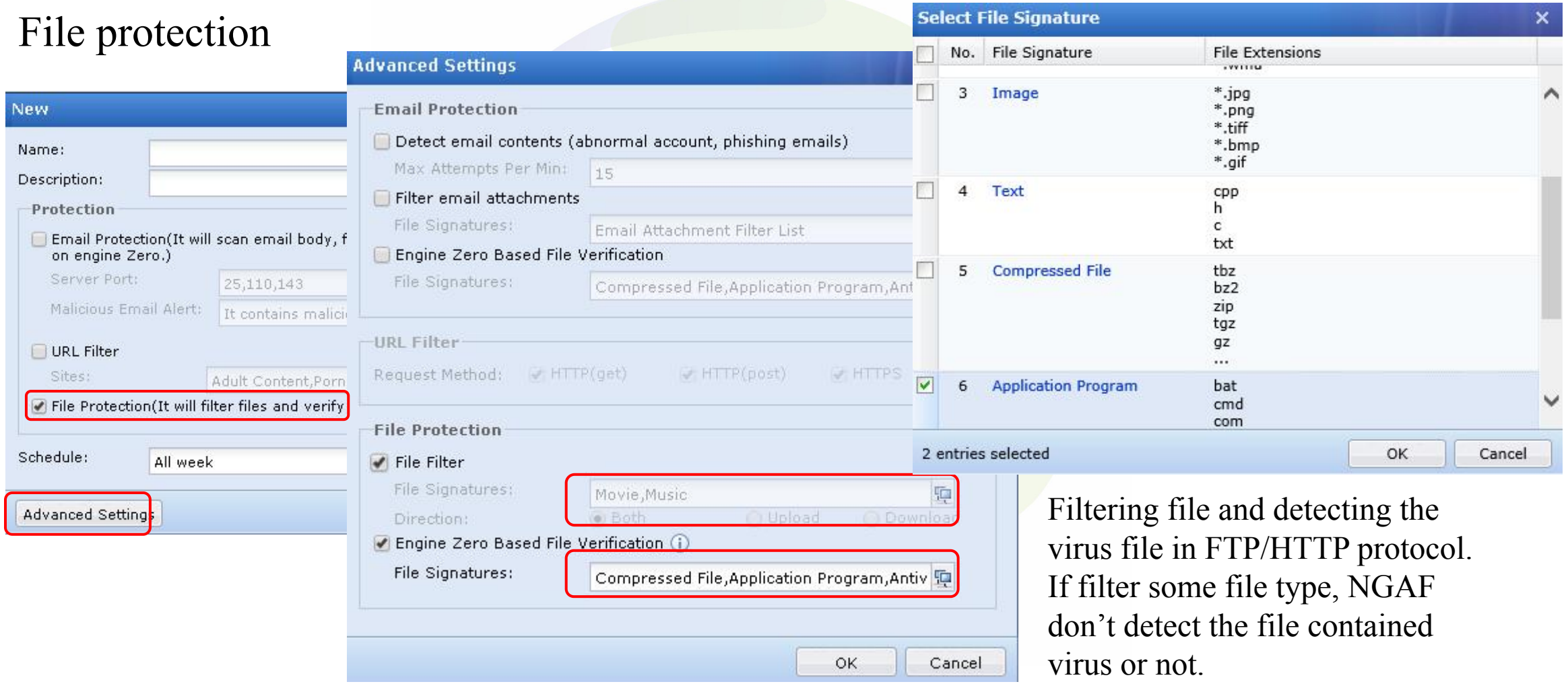
File Filtering

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

No.	Name	Description	Delete
1	Movie	Movie format file	In use
2	Music	Music format file	In use
3	Image	Image format file	✕
4	Text	Source file	✕
5	Compressed File	Compressed file, such as zip, rar, tgz	✕
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

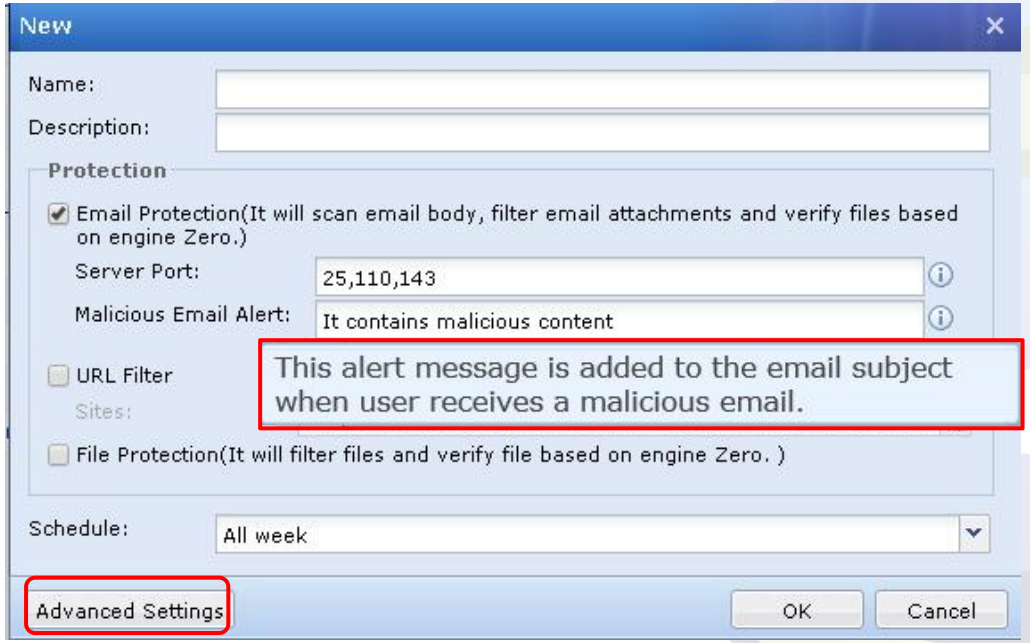
File protection

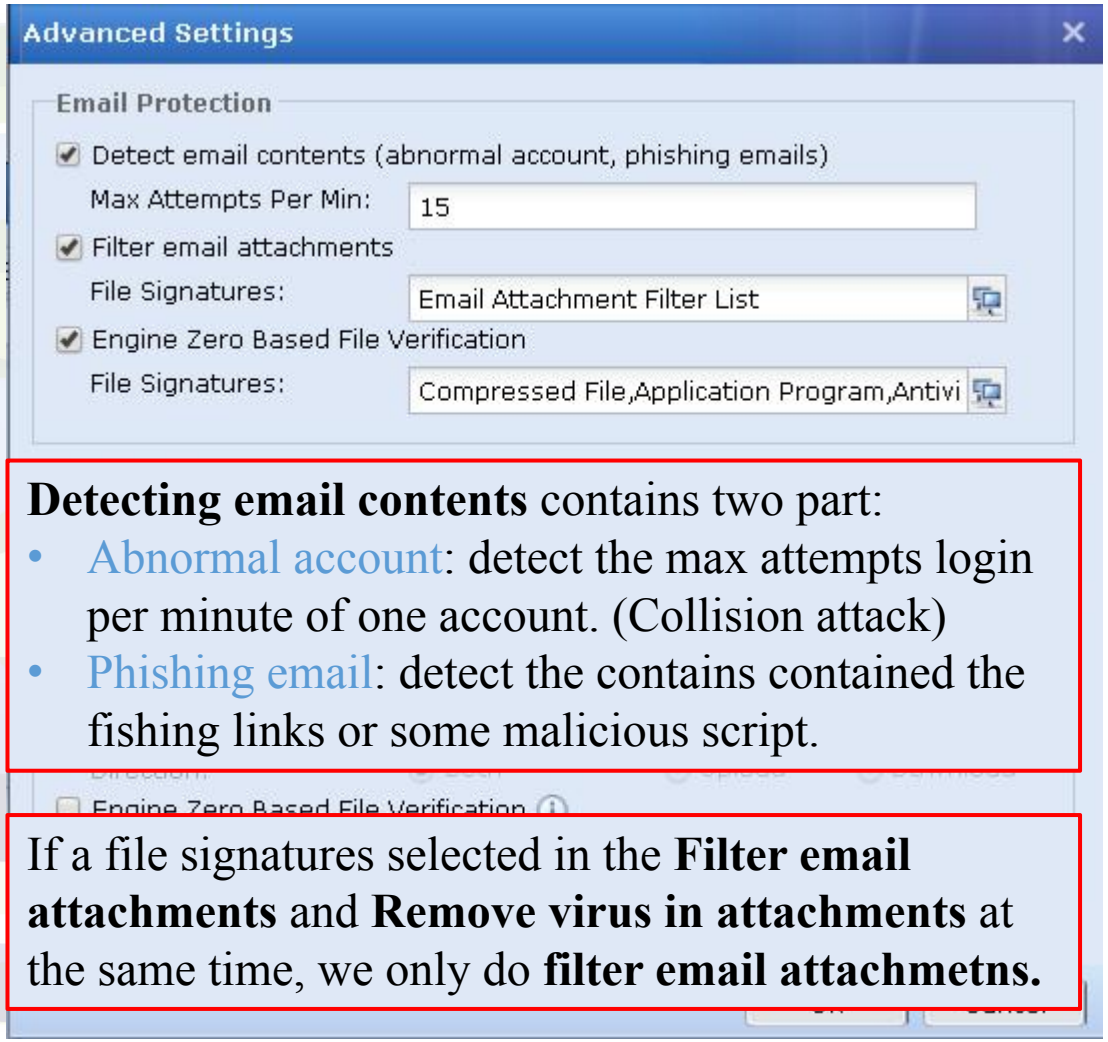


Filtering file and detecting the virus file in FTP/HTTP protocol. If filter some file type, NGAF don't detect the file contained virus or not.

Content Security

Email Security





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

SANGFOR
深信服科技

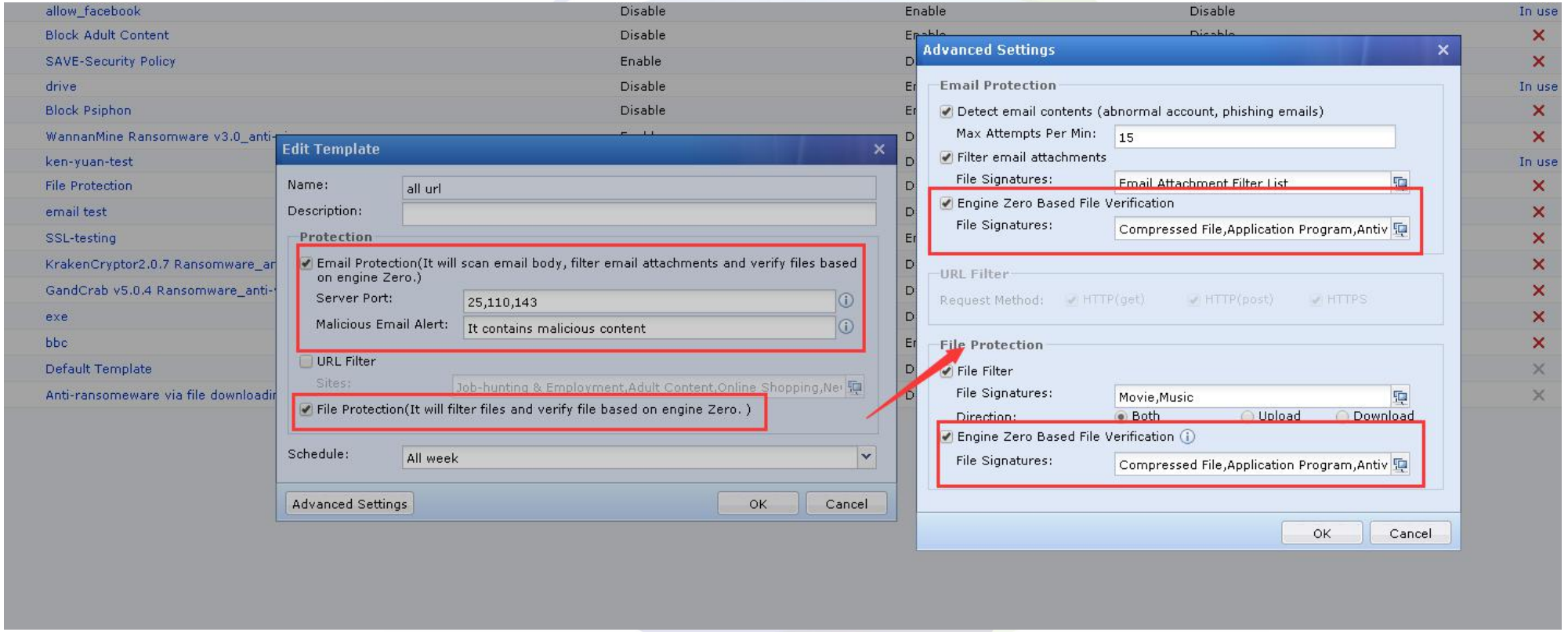
SAVE Engine

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

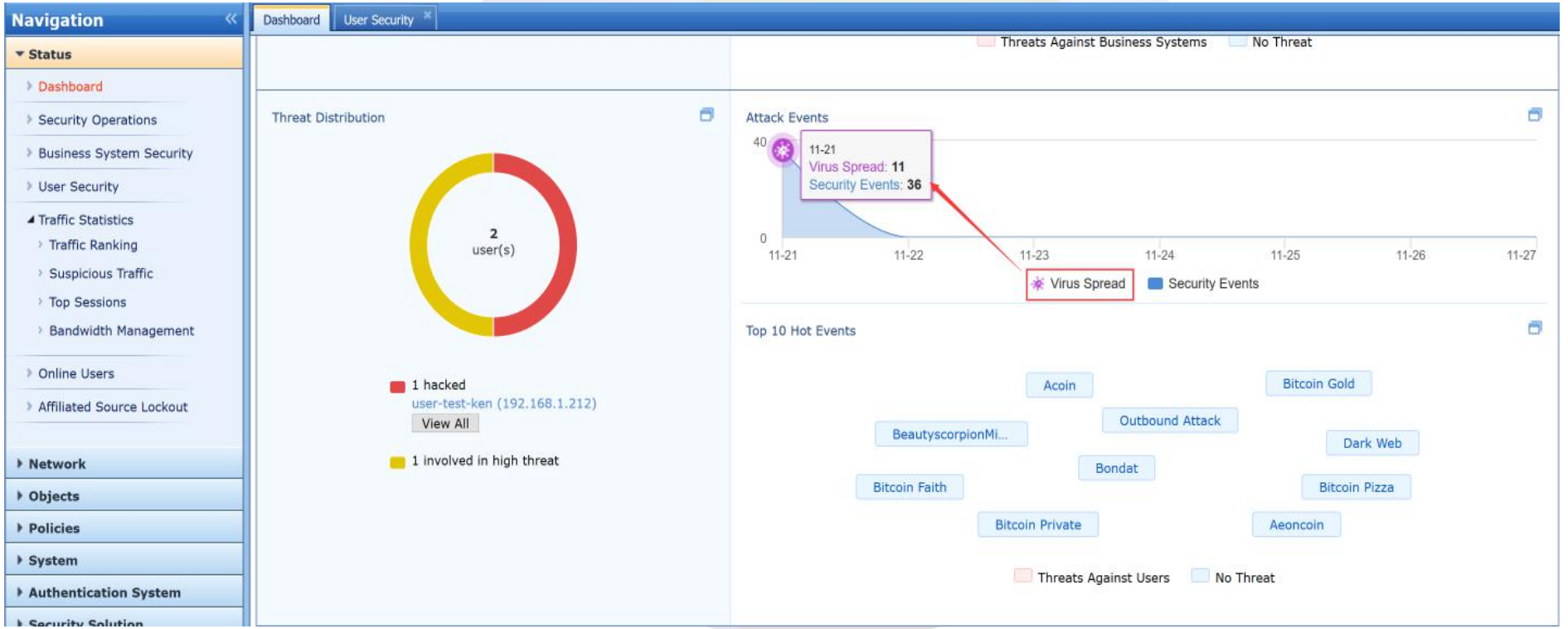
Configuration Path: Object > Security Policy Template > Content Security > Add



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

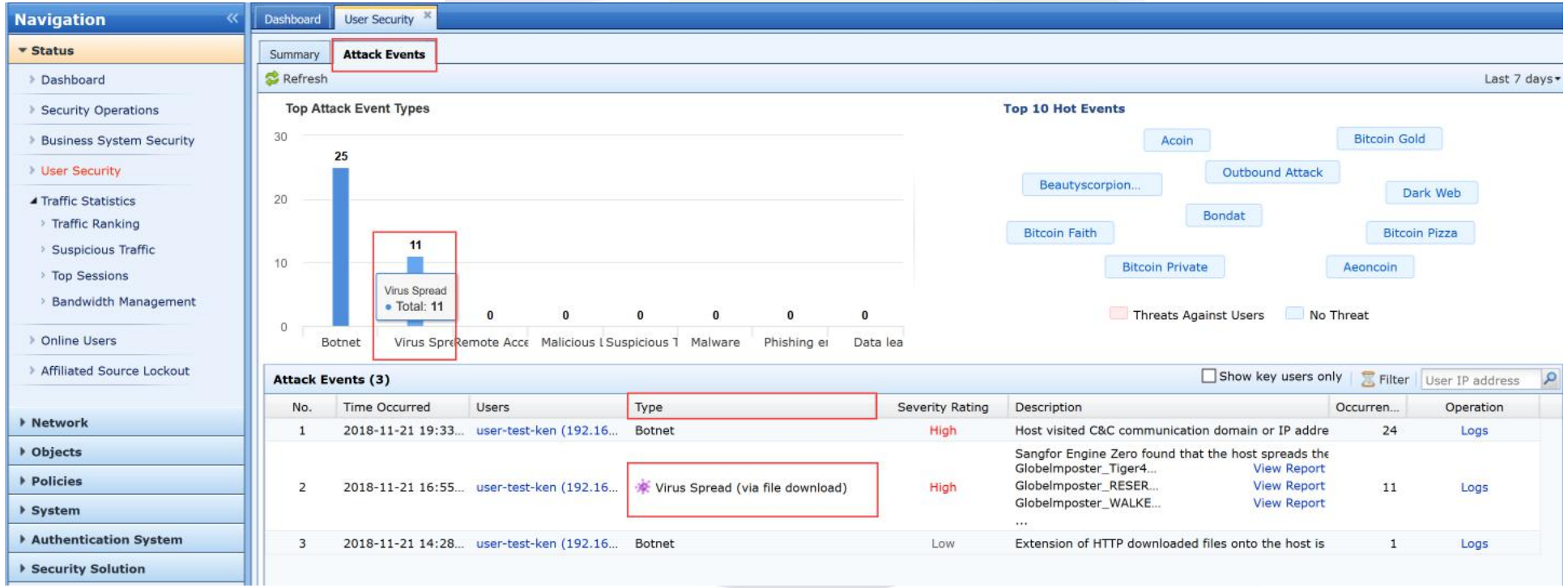
Placement and performance description

User security status of the Dashboard increases the virus spread icon



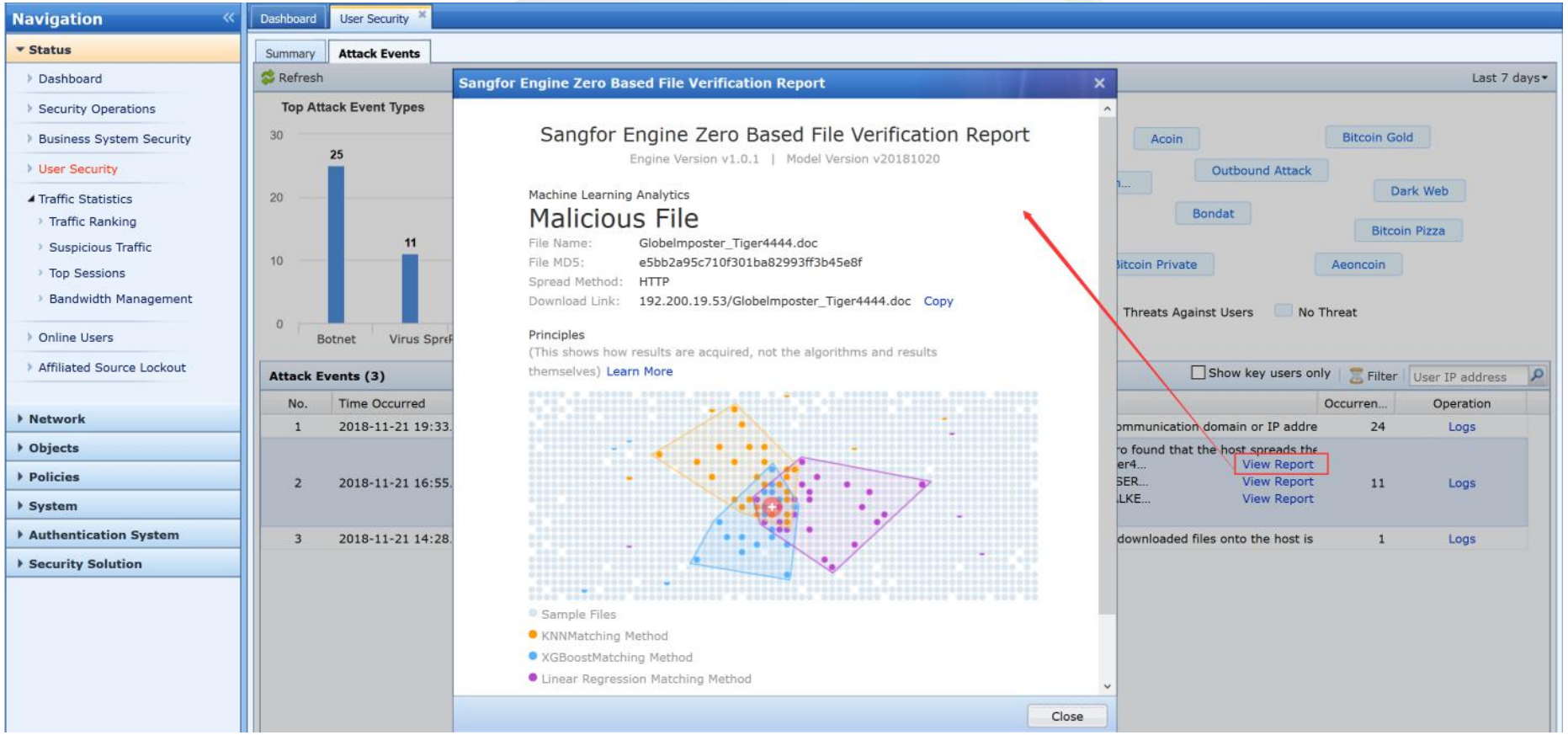
Placement and performance description

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



5. Neural X

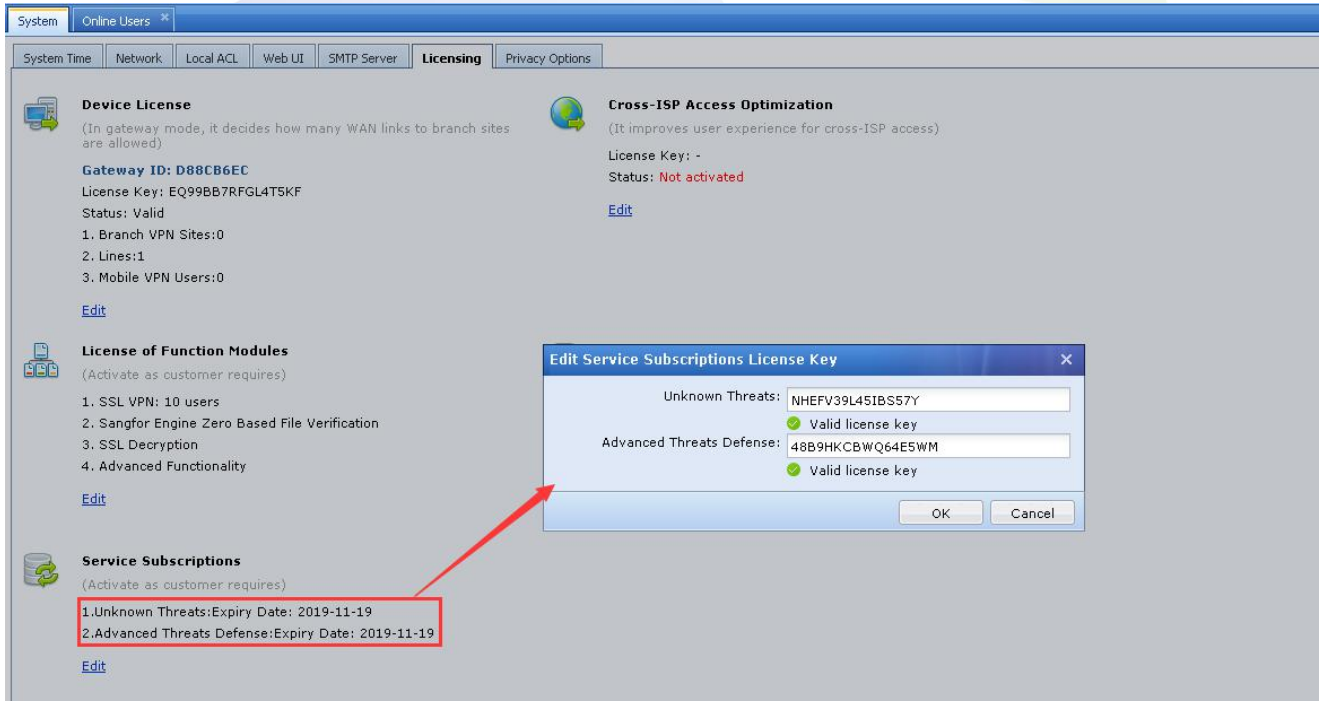
SANGFOR
深信服科技

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)