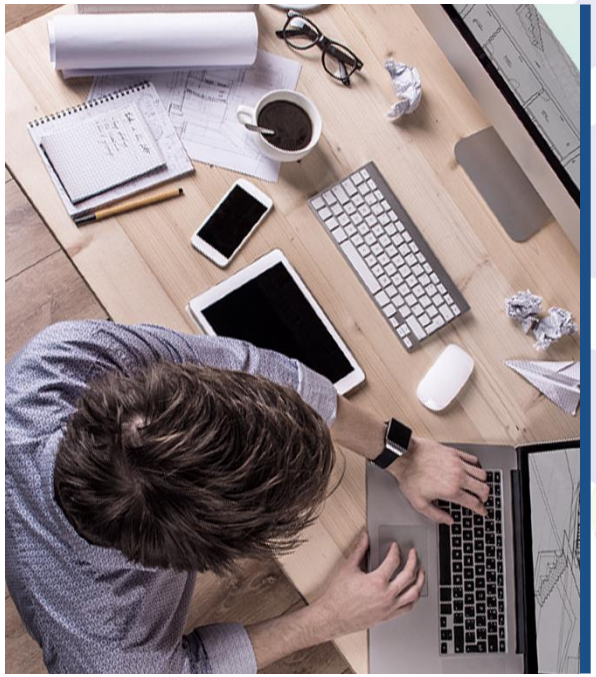
Sangfor NGAF V8.0.6 Associate

Konten Keamanan



1. Visibilitas Trafik Data
2. Pemfilteran URL
3. Pemfilteran File
4. Sangfor Engine Zero
5. Neural X

1. Visibilitas Trafik Data

SANGFOR
深信服科技

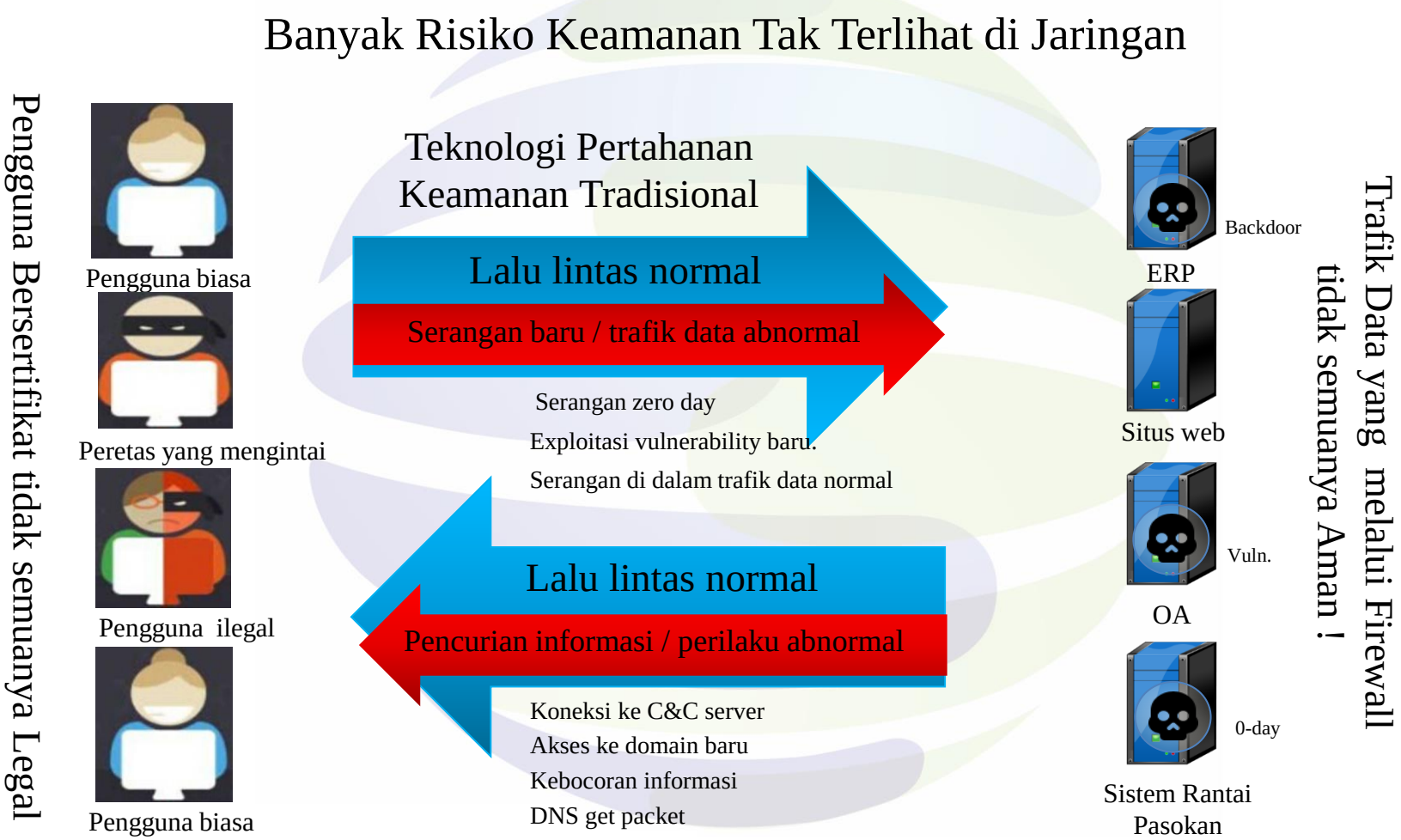
Visibilitas Trafik Data

Firewall tradisional melakukan penyaringan paket menggunakan ACL untuk menjaga keamanan jaringan.

ACL mengontrol lalu lintas berdasarkan IP sumber/tujuan, Port sumber/tujuan, dan protokol.

Apakah sudah aman
dengan ACL saja?

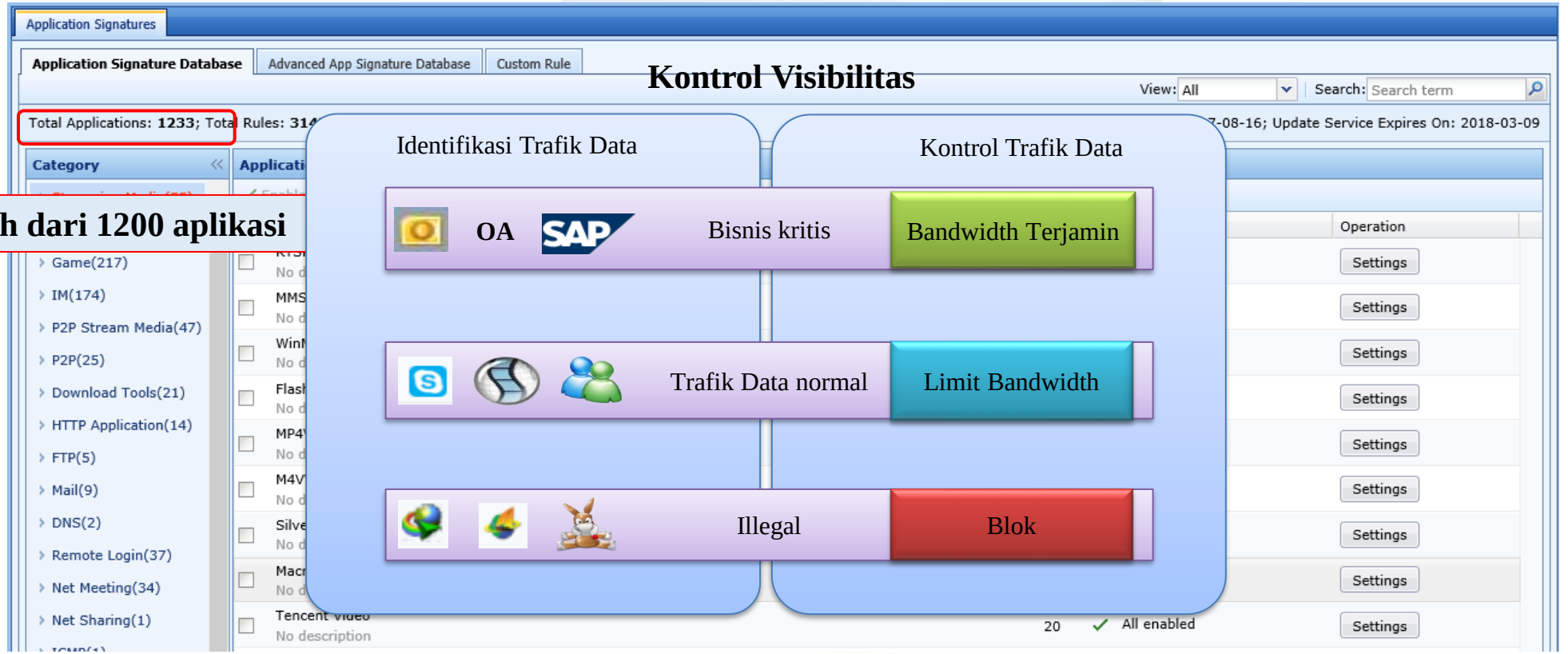
Visibilitas Trafik Data



Visibilitas Trafik Data

Dengan tingkat identifikasi database aplikasi yang tinggi, kita bisa mendapatkan semua komposisi trafik data di jaringan tepat pada waktunya, membuat trafik data berada dalam kendali dan lebih aman.

Lebih dari 1200 aplikasi



2. Pemfilteran URL

SANGFOR
深信服科技

Pemfilteran URL

Apa itu pemfilteran URL?

NGAF mengidentifikasi suatu URL apakah diizinkan atau ditolak dengan mendeteksi paket HTTP request, kemudian mengambil tindakan yang sesuai.

Mengapa kita membutuhkan pemfilteran URL?

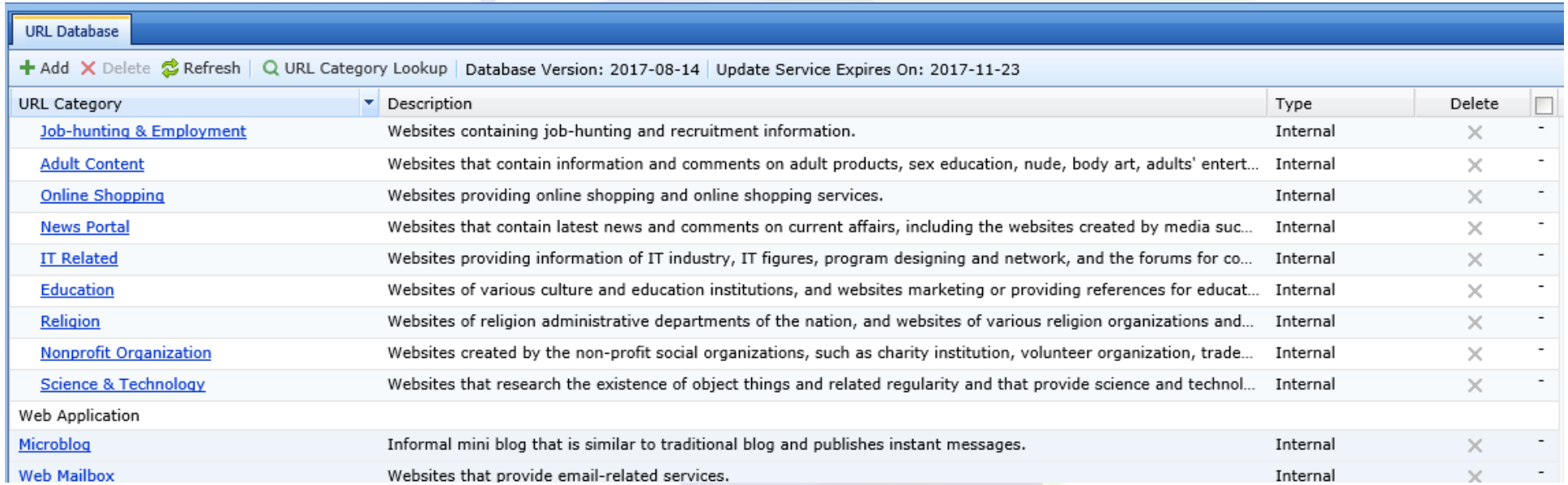
- Konten yang tidak pantas: Porno, konten dewasa, obat-obatan, dll.
- Phishing dan Tautan berbahaya, situs web dengan trojan, virus.
- Web yang tidak terkait dengan pekerjaan : video online, game.

Pemfilteran URL

Database URL:

- Lebih dari 60 jenis;
- Jutaan situs web;
- Update setiap dua minggu

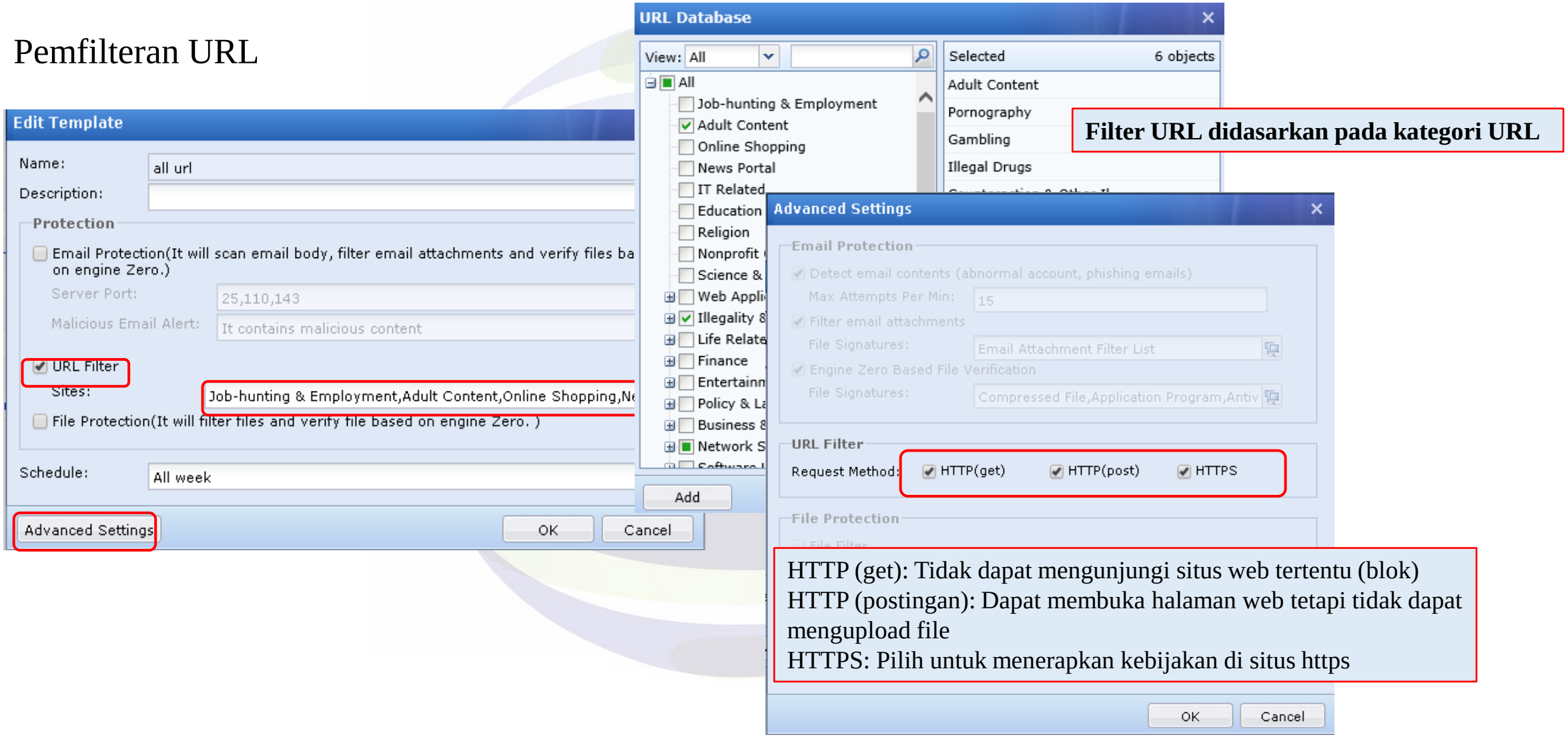
- Pencarian kategori URL
- Kustomisasi URL



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

Keamanan Konten

Pemfilteran URL

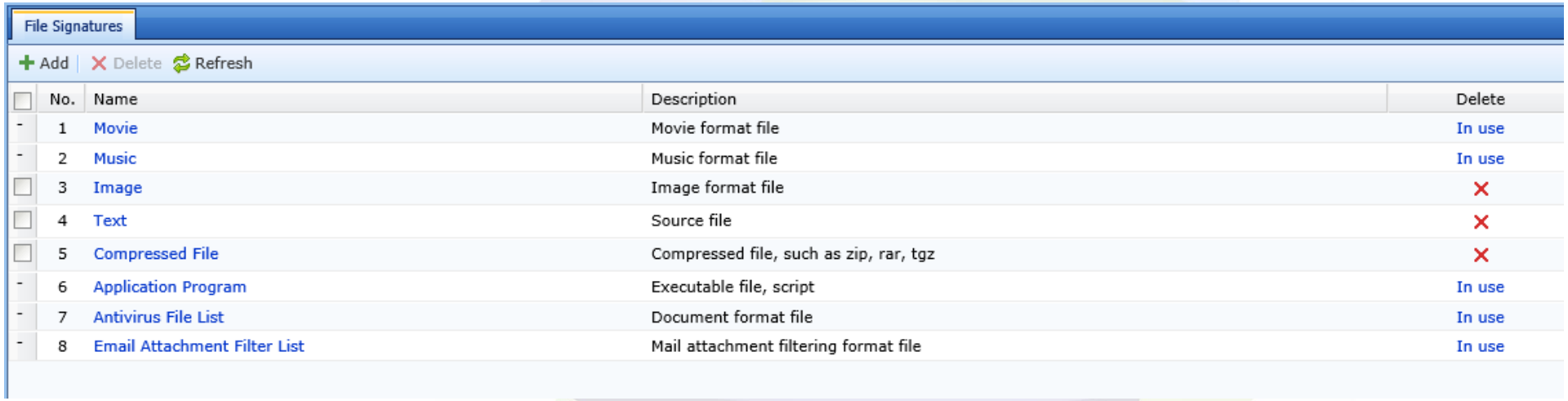


3. Pemfilteran File

SANGFOR
深信服科技

Pemfilteran File

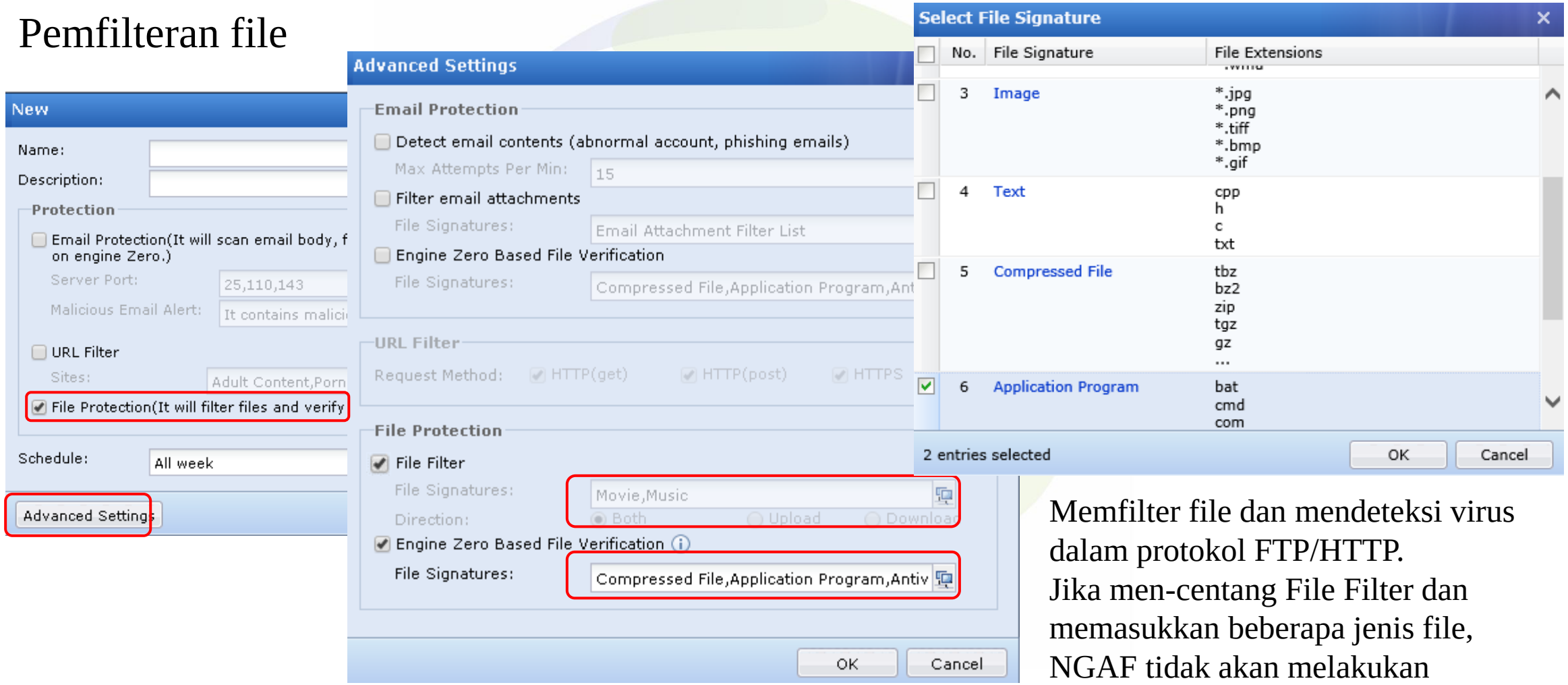
Siganture file umum yang telah ditentukan sebelumnya (predefined) dan dapat dikustomisasi untuk pemfilteran file dan pemindaian file virus.



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

Keamanan Konten

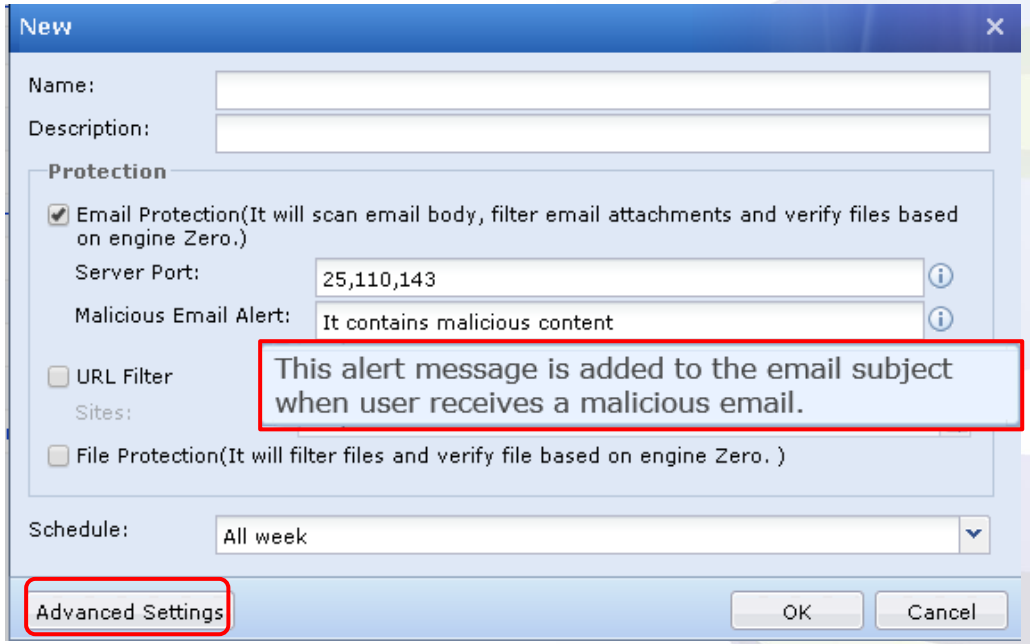
Pemfilteran file

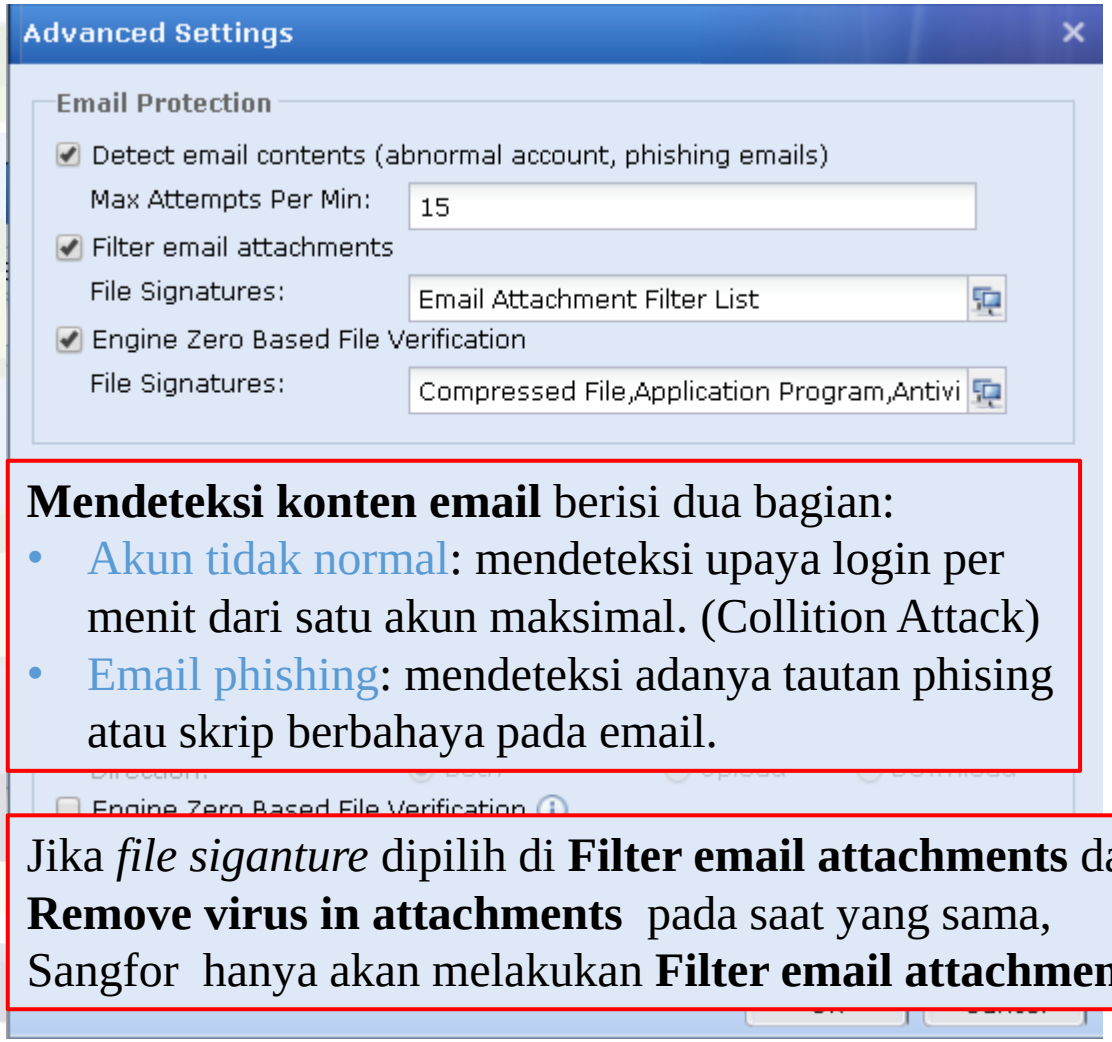


Memfilter file dan mendeteksi virus dalam protokol FTP/HTTP.
Jika men-centang File Filter dan memasukkan beberapa jenis file, NGAF tidak akan melakukan scanning terhadap jenis tersebut.

Keamanan Konten

Keamanan Email





Mendeteksi konten email berisi dua bagian:

- Akun tidak normal: mendeteksi upaya login per menit dari satu akun maksimal. (Collition Attack)
- Email phishing: mendeteksi adanya tautan phising atau skrip berbahaya pada email.

Jika *file siganture* dipilih di **Filter email attachments** dan **Remove virus in attachments** pada saat yang sama, Sangfor hanya akan melakukan **Filter email attachments .**

Catatan

a. Jika kebijakan keamanan konten mendukung dekripsi, Anda harus mengaktifkan kebijakan dekripsi.
b. Perlindungan eMail mendukung proteksi attachment yang berisi virus, link mencurigakan, serangan XSS, file filter, dan Collision Attack.
c. Proteksi eMail secara default mendeteksi port 25,110,143, dan dapat dikustomisasi untuk port lain.
d. Ketika klien menerima email berbahaya, NGAF tidak akan melakukan deny action meskipun kebijakannya adalah deny, tetapi NGAF akan merusak subjek surat jika kebijakannya adalah deny.
e. Log unduhan/unggahan HTTP/HTTPS, dan FTP disimpan di Application Control, bukan di Content Security Policy.

4. Sangfor Engine Zero

SANGFOR
深信服科技

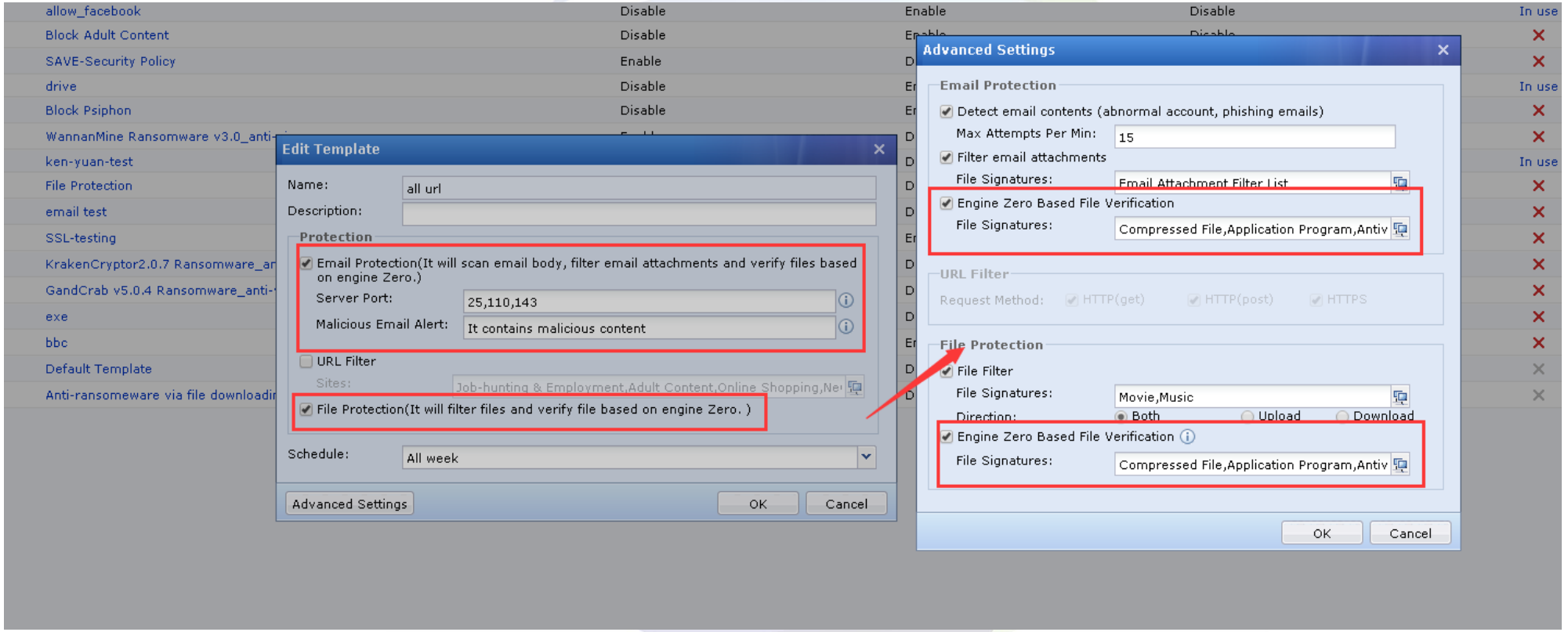
SAVE Engine

SAVE (Sangfor AI-based Vanguard Engine) adalah program pendeteksi file berbahaya berbasiskan kecerdasan buatan (AI) yang menggunakan teknologi pembelajaran mendalam (deep learning) untuk menganalisis dan mensintesis ratusan juta fitur asli, dikombinasikan dengan pengetahuan pakar keamanan, dan akhirnya memilih ribuan fitur dimensi tinggi yang paling efisien untuk mengidentifikasi file berbahaya.

- Menggunakan kecerdasan buatan, SAVE **memiliki kemampuan generalisasi yang kuat** untuk mengidentifikasi virus yang tidak dikenal atau adanya varian baru dari virus lama;
- **Kemampuan deteksi** dari **virus ransom telah mencapai level terdepan**, termasuk WannaCry, BadRabbit dan virus lainnya, dan memiliki efek deteksi yang lebih baik pada non-lesoviruses;
- **Cloud + device + end linkage**, mengandalkan data keamanan dari otak keamanan di cloud yang sangat meyakinkan, SAVE dapat terus berkembang, terus memperbarui model dan meningkatkan kemampuan deteksi, sehingga membentuk kombinasi sempurna dari mesin lokal tradisional, mesin pendeteksi berbasis kecerdasan buatan, dan mesin pembunuh virus di cloud.

Konfigurasi SAVE Engine

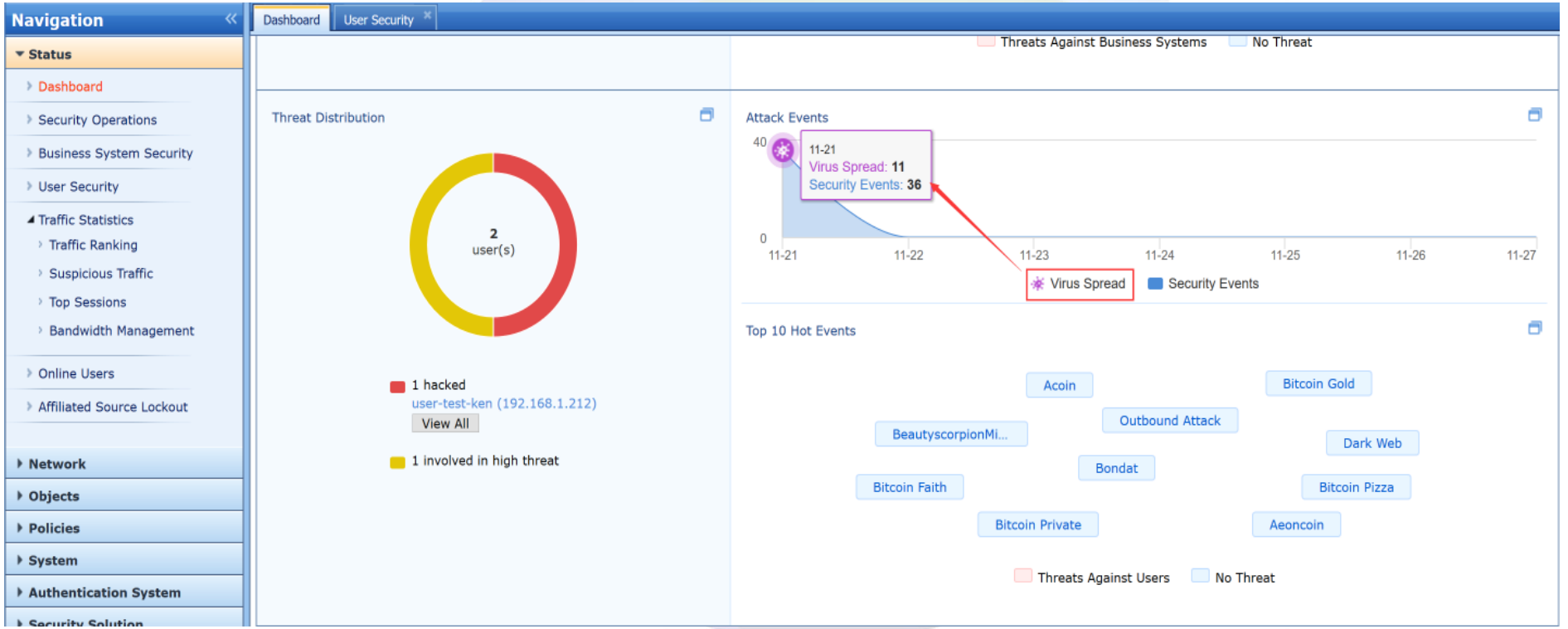
Jalur Konfigurasi: Object > Security Policy Template > Content Security > Add



Catatan: Save Engine saat ini hanya mendukung deteksi file jenis PE seperti exe, object code, DLL, FON Font file dan lain-lain

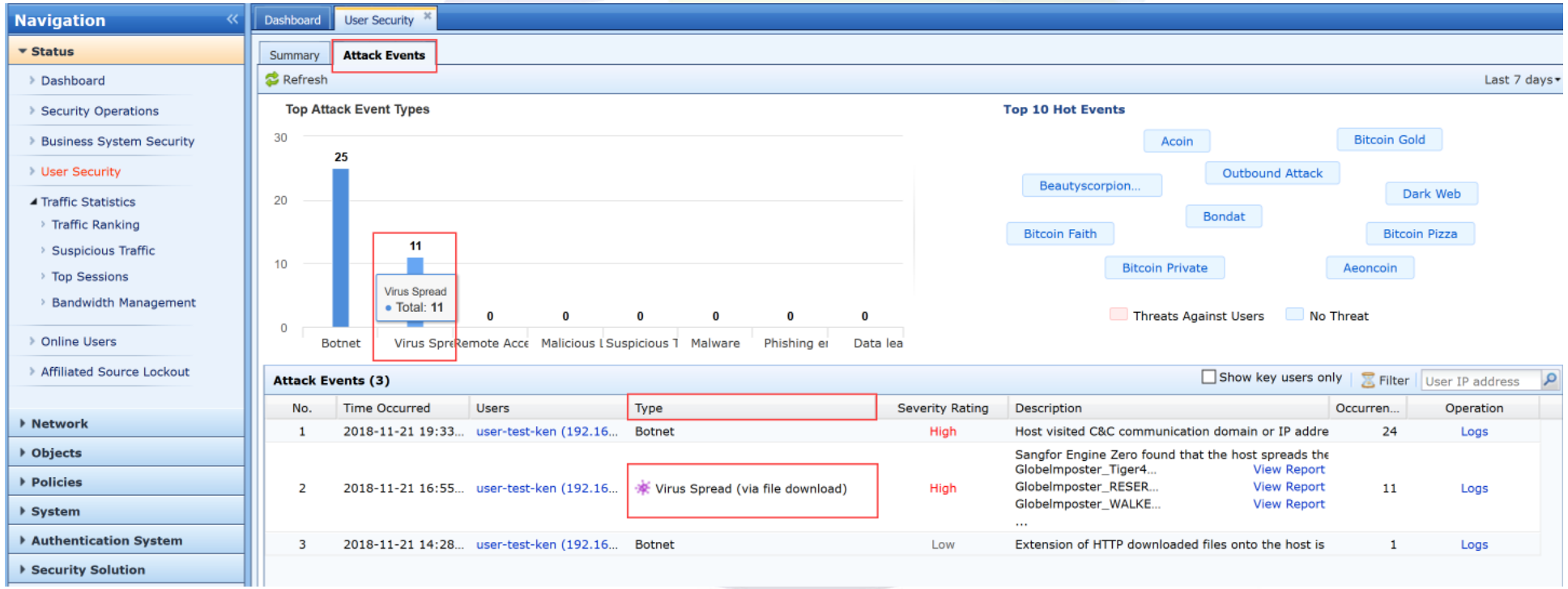
Penempatan dan deskripsi kinerja

Status keamanan pengguna di Dashboard menampilkan ikon penyebaran virus



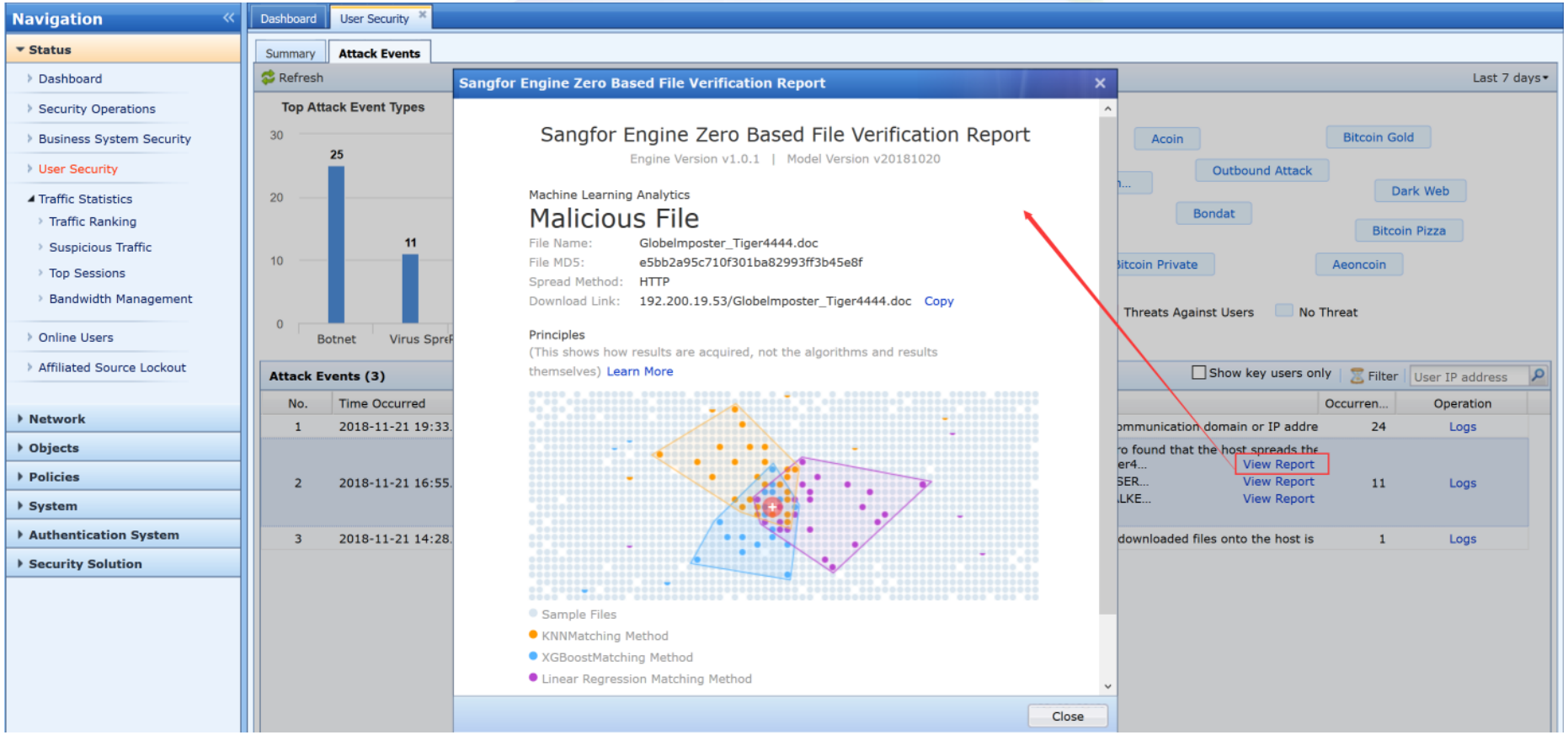
Penempatan dan deskripsi kinerja

Keamanan Pengguna - Event Serangan, menambahkan Histogram Propagasi Virus, tipe Event menambahkan tipe propagasi virus.



Penempatan dan deskripsi kinerja

Klik View Report untuk melihat Deskripsi Virus dan Identifikasi Virus



5. Neural X

SANGFOR
深信服科技

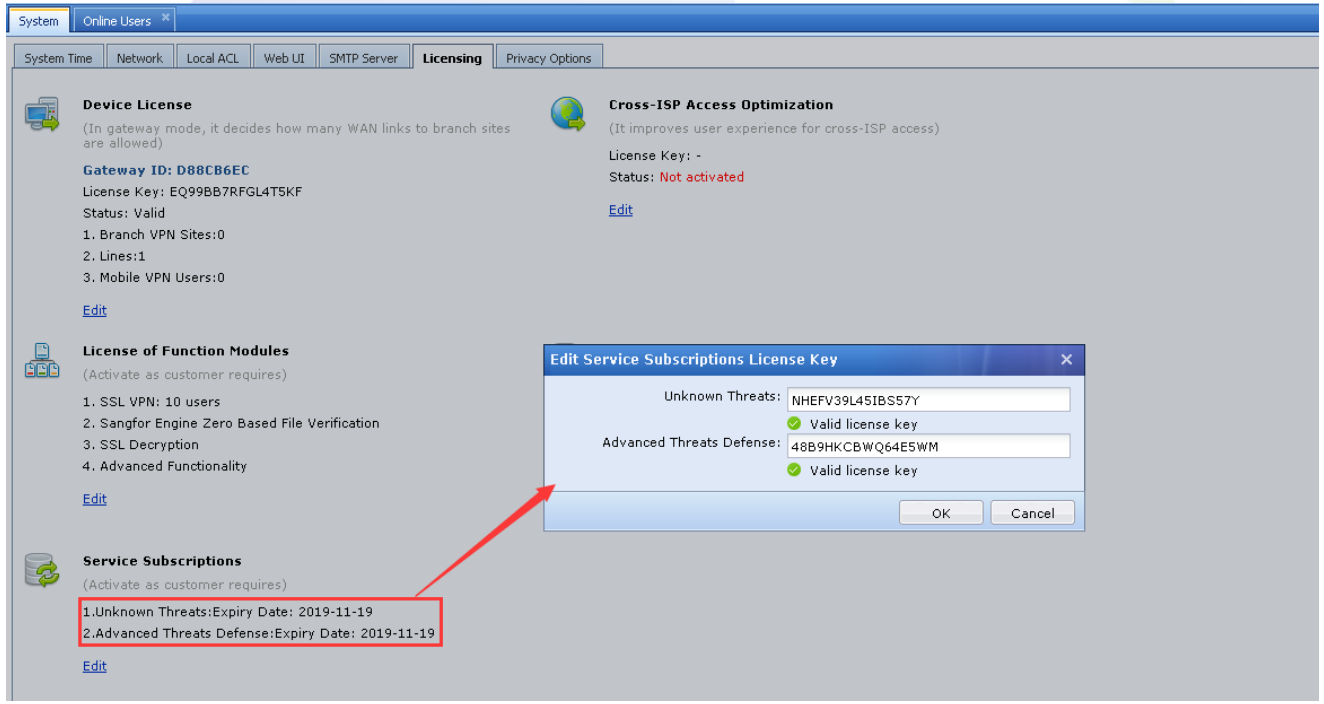
Neural X

- NGAF memeriksa data yang lewat. Saat menemukan adanya local rule database yang tidak cocok, NGAF menguploadnya ke Neural X untuk memeriksa apakah itu adalah data yang berisiko.
- Rule Database Neural X memiliki lebih banyak sumber untuk terus memperkaya kemampuan pendeteksian
- Local rule database NGAF terbatas ukurannya, dan ada ratusan juta rule database di cloud, sehingga tidak dapat dikirim ke local rule database . Selain memiliki rule database yang jumlahnya besar, Neural X juga mengintegrasikan banyak mesin pendeteksi berbasis cloud. Jika beberapa data tidak dapat dicocokkan dengan rule database, Neural X akan mendeteksi status risiko menggunakan mesin pendeteksi. Mesin pendeteksi berbasis cloud ini belum tersedia di NGAF dalam waktu dekat.

Konfigurasi Neural X

Neural X tidak perlu dikonfigurasi secara terpisah, dan memiliki tiga persyaratan berikut:

1. Versi perangkat adalah AF8.0.5 atau yang lebih baru;
2. Perangkat dapat terhubung ke Internet secara normal, dan data pengguna intranet yang mengakses internet mengalir melalui AF;
3. Fungsi perangkat Neural X biasanya sudah dihidupkan, untuk mencek Serial Numbernya. Navigasi ke System > General > Licensing, seperti yang ditunjukkan di bawah ini:

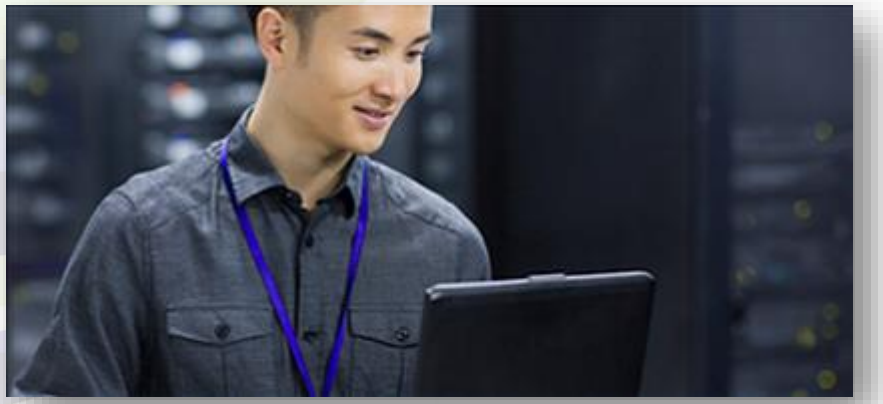


CatatanNeural X

1. Log deteksi Neural X membutuhkan waktu sekitar **6 sampai 15 menit untuk dihasilkan**, jadi Anda perlu menjadwalkan waktu tes.
2. Jika menemukan bahwa peristiwa DGA tidak ter-generate, Anda dapat menjalankan skrip beberapa kali, dan setiap kali menjalankan skrip, peristiwa DGA akan di-generate.
3. AF melaporkan **200.000 domain mencurigakan setiap hari,** jadi jika perangkat dengan jumlah pengguna yang relatif besar, penyimpanan laporan dapat dengan mudah penuh. Jika Anda ingin melakukan pengujian lagi, Anda hanya dapat mengujinya setelah AF di-restart.
4. Hasil investigasi Neural X terhadap nama domain DGA adalah **hanya dianalisis dan ditelusuri, dan tidak akan dicegat** , jadi pengguna perlu memeriksa terminal dan secara manual menggunakan tool penghenti aplikasi (killing tools).

Terima kasih !

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)