

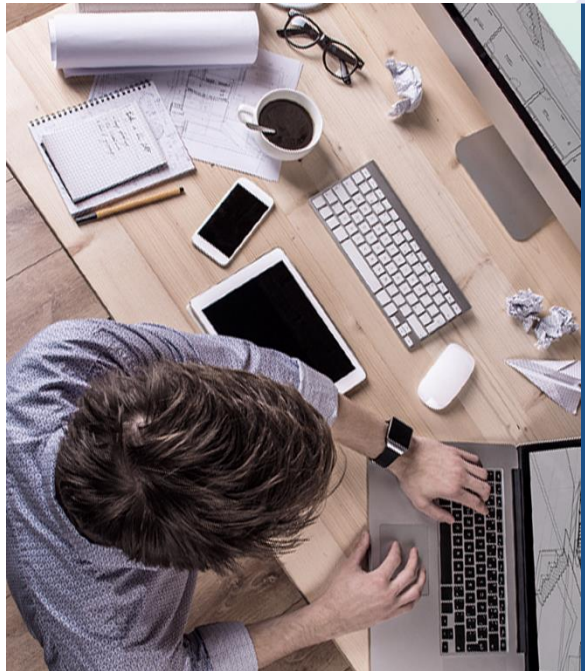


SANGFOR

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



Visibilitas Trafik Data

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

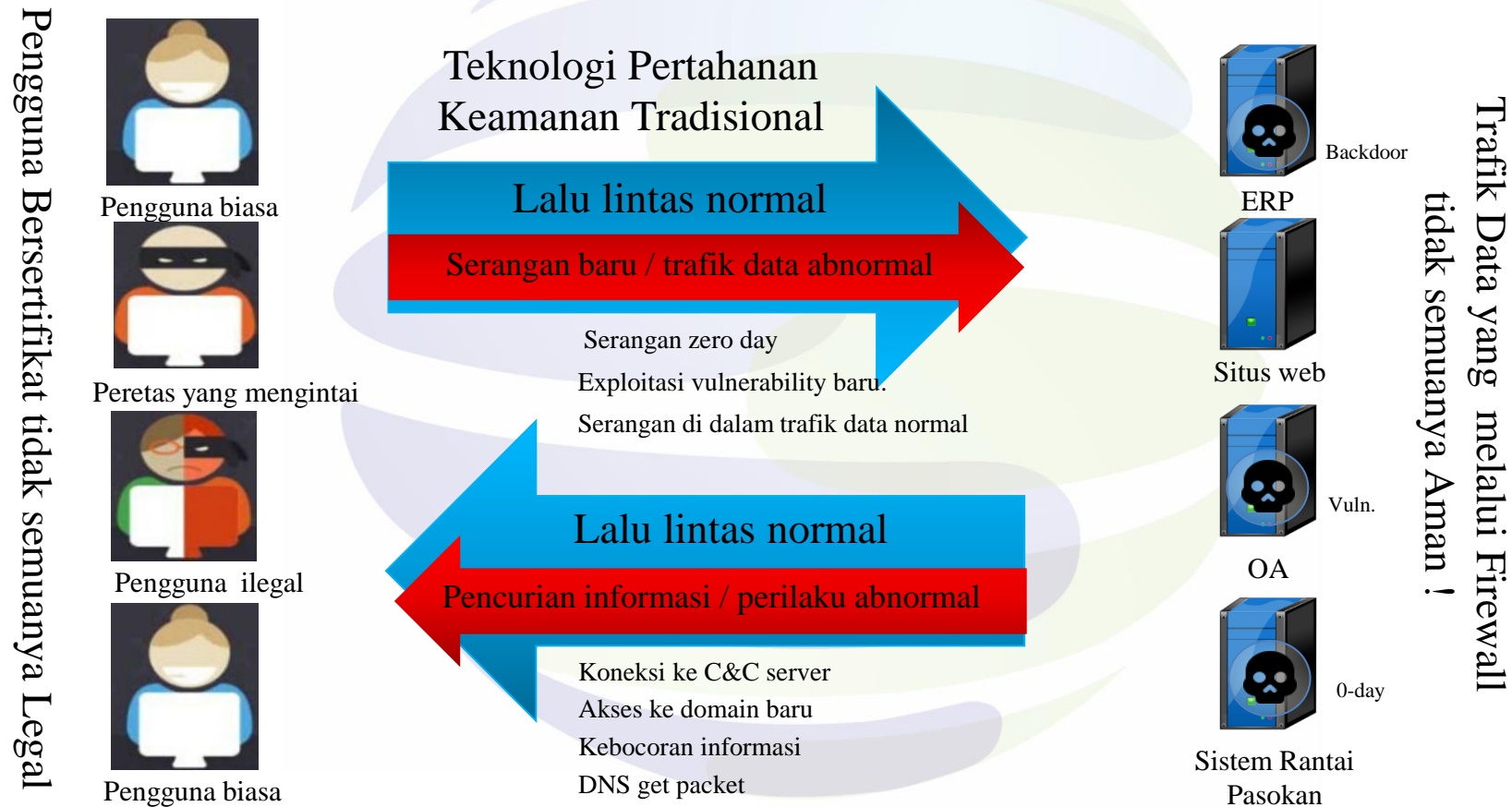
ACL mengontrol lalu lintas berdasarkan IP sumber/tujuan, Port sumber/tujuan, dan protokol.



Apakah sudah aman
dengan ACL saja?

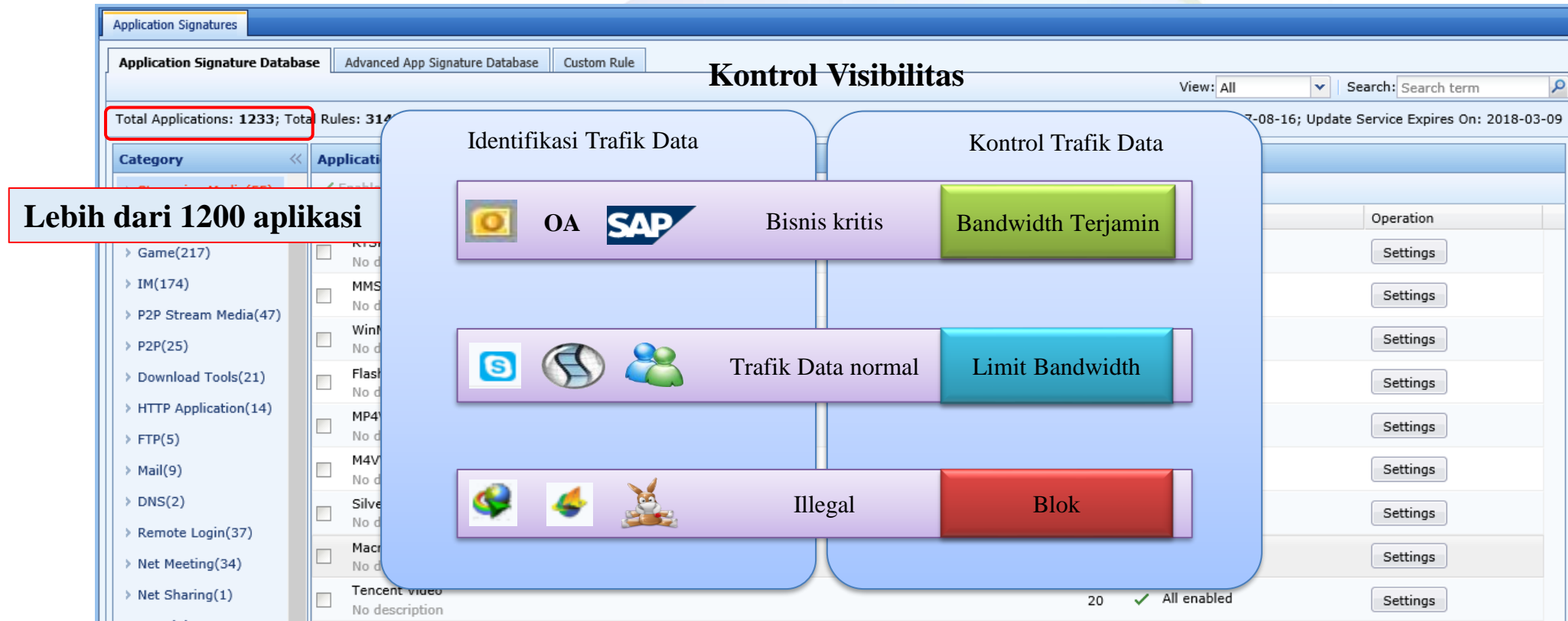
Visibilitas Trafik Data

Banyak Risiko Keamanan Tak Terlihat di Jaringan



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.



The screenshot displays the 'Kontrol Visibilitas' (Visibility Control) interface. On the left, a sidebar lists application categories with counts: Game(217), IM(174), P2P Stream Media(47), P2P(25), Download Tools(21), HTTP Application(14), FTP(5), Mail(9), DNS(2), Remote Login(37), Net Meeting(34), and Net Sharing(1). A red box highlights the text 'Lebih dari 1200 aplikasi' (More than 1200 applications). The main panel is titled 'Kontrol Visibilitas' and features a 'Total Applications: 1233; Total Rules: 314' status bar. It is divided into two columns: 'Identifikasi Trafik Data' (Traffic Data Identification) and 'Kontrol Trafik Data' (Traffic Data Control). The 'Identifikasi' column lists three categories: 'Bisnis kritis' (Critical Business) with icons for OA and SAP, 'Trafik Data normal' (Normal Traffic Data) with icons for a chat app, a globe, and a group of people, and 'Illegal' with icons for a globe, a folder, and a rabbit. The 'Kontrol' column shows corresponding actions: 'Bandwidth Terjamin' (Guaranteed Bandwidth) for critical business, 'Limit Bandwidth' for normal traffic, and 'Blok' (Block) for illegal traffic. Each action button has a 'Settings' link next to it. At the bottom right, it shows '20' items and a status 'All enabled'.

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

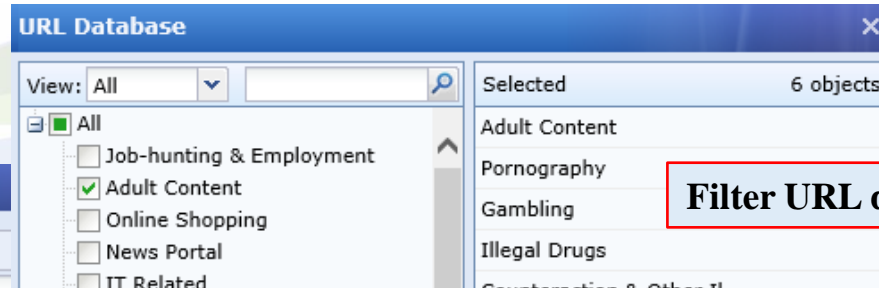
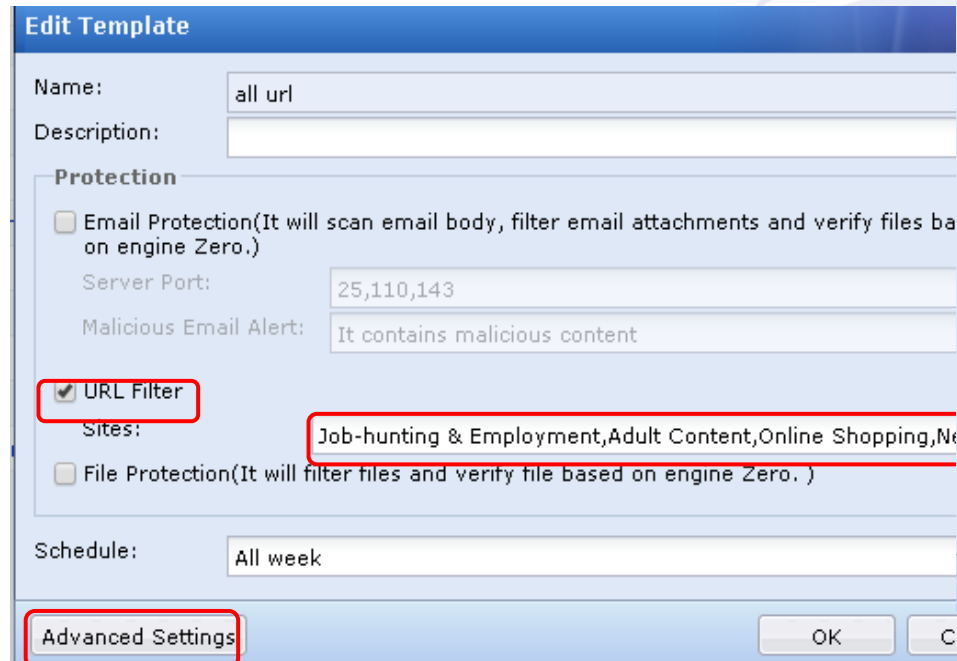
Database URL:

- Lebih dari 60 jenis;
- Jutaan situs web;
- Update setiap dua minggu
- Pencarian kategori URL
- Kustomisasi URL

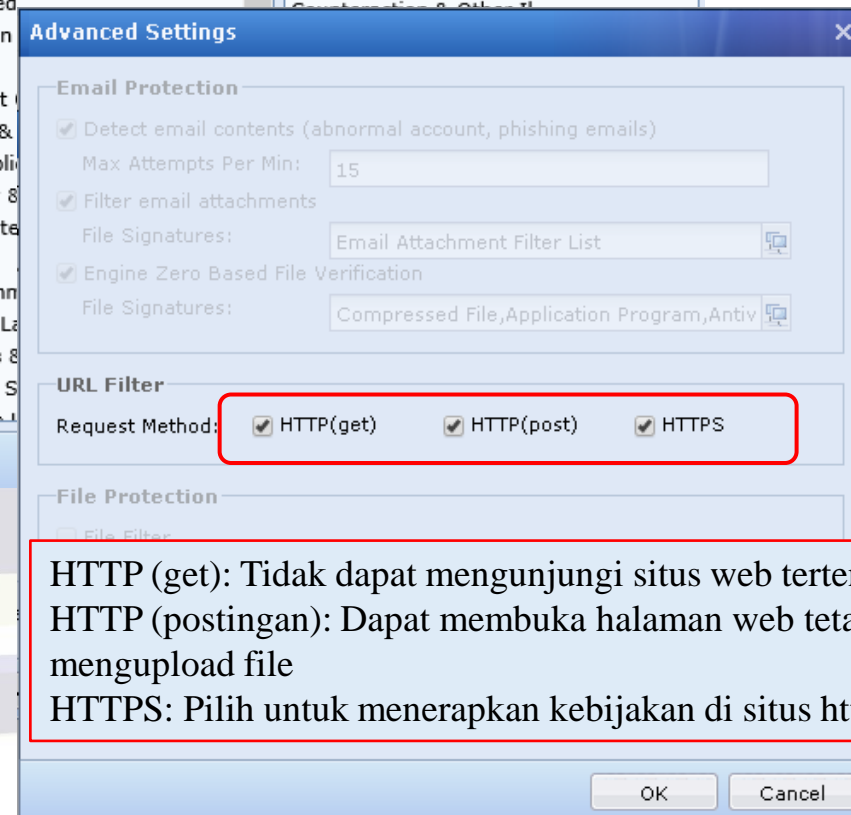
| URL Database | | | | |
|---|--|----------|--------|---|
| + Add X Delete Refresh URL Category Lookup Database Version: 2017-08-14 Update Service Expires On: 2017-11-23 | | | | |
| URL Category | Description | Type | Delete | |
| Job-hunting & Employment | Websites containing job-hunting and recruitment 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 | - |

Keamanan Konten

Pemfilteran URL



Filter URL didasarkan pada kategori URL



HTTP (get): Tidak dapat mengunjungi situs web tertentu (blok)
HTTP (postingan): Dapat membuka halaman web tetapi tidak dapat mengupload file
HTTPS: Pilih untuk menerapkan kebijakan di situs https

3. Pemfilteran File



SANGFOR
深信服科技

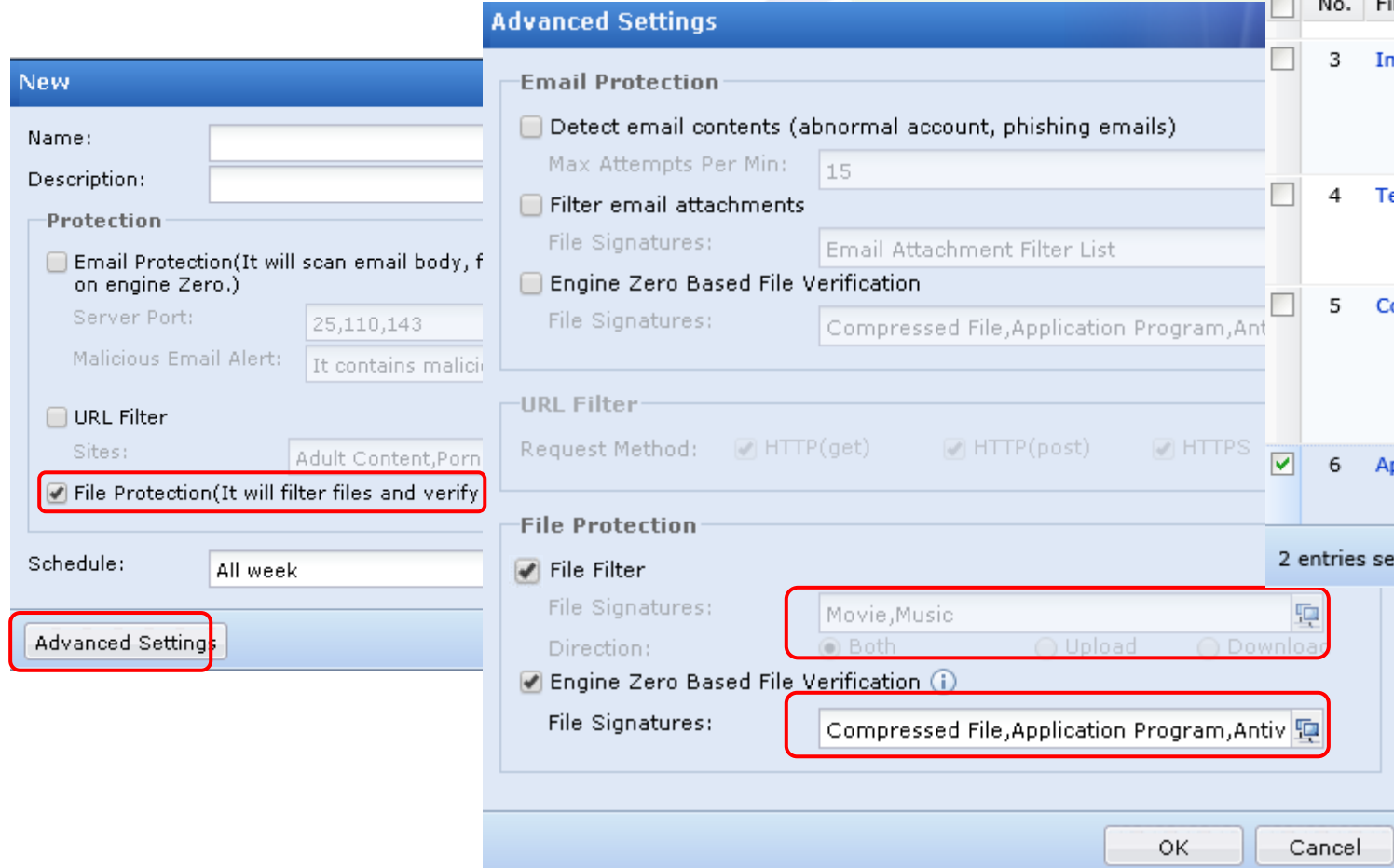
Pemfilteran File

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

| File Signatures | | | | |
|----------------------------|-----|------------------------------|--|--------|
| + Add X Delete Refresh | | | | |
| <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 |

Keamanan Konten

Pemfilteran file



The screenshot displays the Sangfor NGAF configuration interface. On the left, the 'New' tab is active, showing fields for 'Name' and 'Description'. Under the 'Protection' section, 'File Protection (It will filter files and verify)' is checked and highlighted with a red box. Below it, 'Advanced Settings' is also highlighted with a red box. The 'Advanced Settings' window is open, showing several sections: 'Email Protection' with checkboxes for detecting email contents, filtering attachments, and engine zero-based file verification; 'URL Filter' with checkboxes for HTTP (get), HTTP (post), and HTTPS; and 'File Protection' with checkboxes for 'File Filter' and 'Engine Zero Based File Verification'. In the 'File Filter' section, the 'File Signatures' field contains 'Movie,Music' and the 'Direction' is set to 'Both', both highlighted with red boxes. In the 'Engine Zero Based File Verification' section, the 'File Signatures' field contains 'Compressed File,Application Program,Antiv', also highlighted with a red box. On the right, the 'Select File Signature' dialog box is open, showing a table of file signatures and extensions. The table has columns for 'No.', 'File Signature', and 'File Extensions'. The following table represents the data in this dialog:

| No. | File Signature | File Extensions |
|-----|---------------------|--|
| 3 | Image | *.jpg *.png *.tiff *.bmp *.gif |
| 4 | Text | cpp h c txt |
| 5 | Compressed File | tbz bz2 zip tgz gz ... |
| 6 | Application Program | bat cmd com |

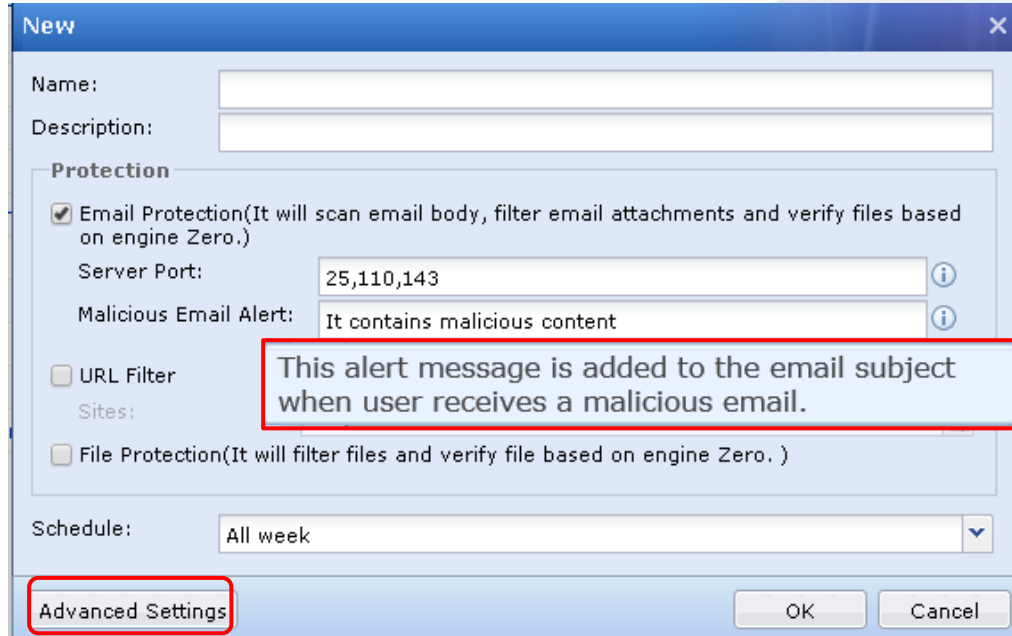
At the bottom of the dialog, it says '2 entries selected' and has 'OK' and 'Cancel' buttons.

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



New

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

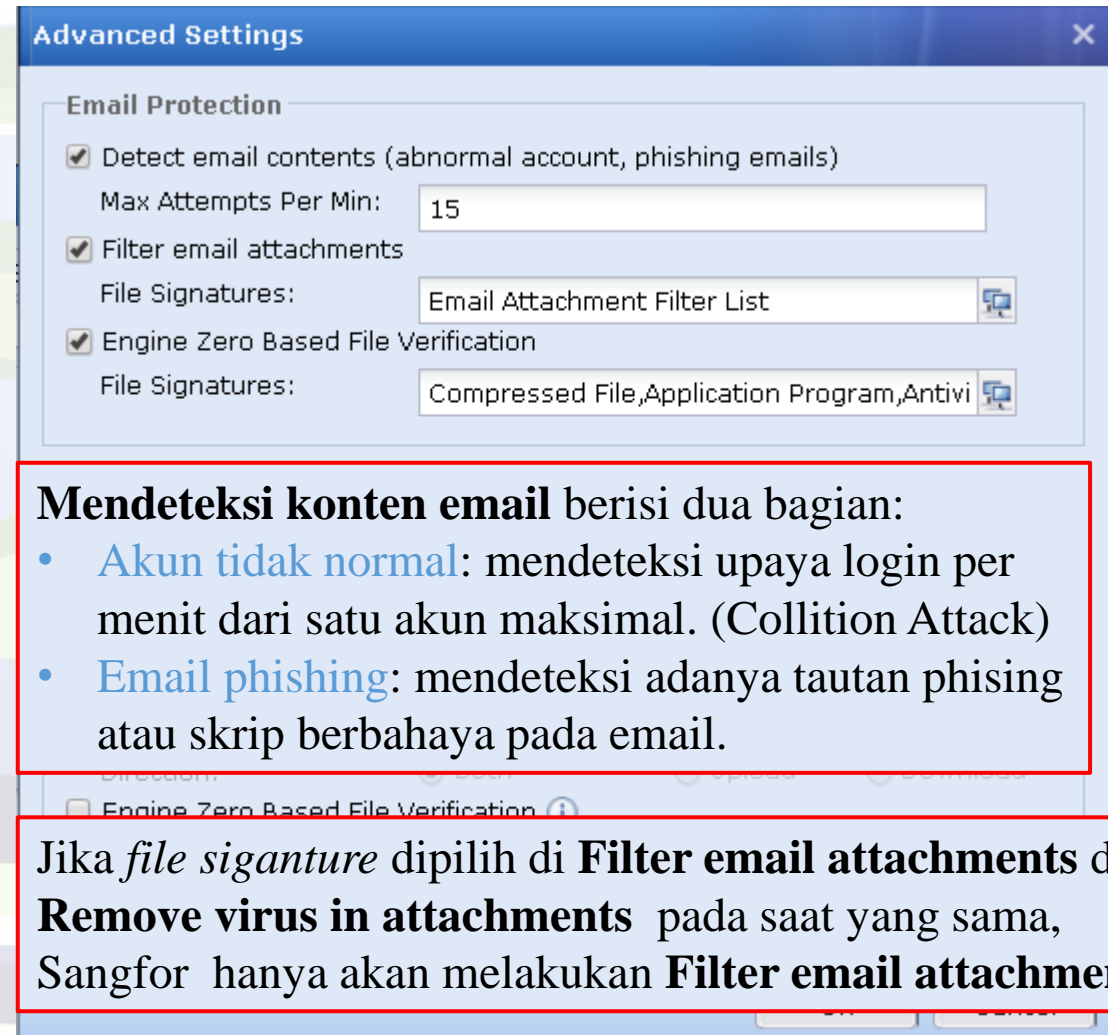
Sites:

☐ 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:

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

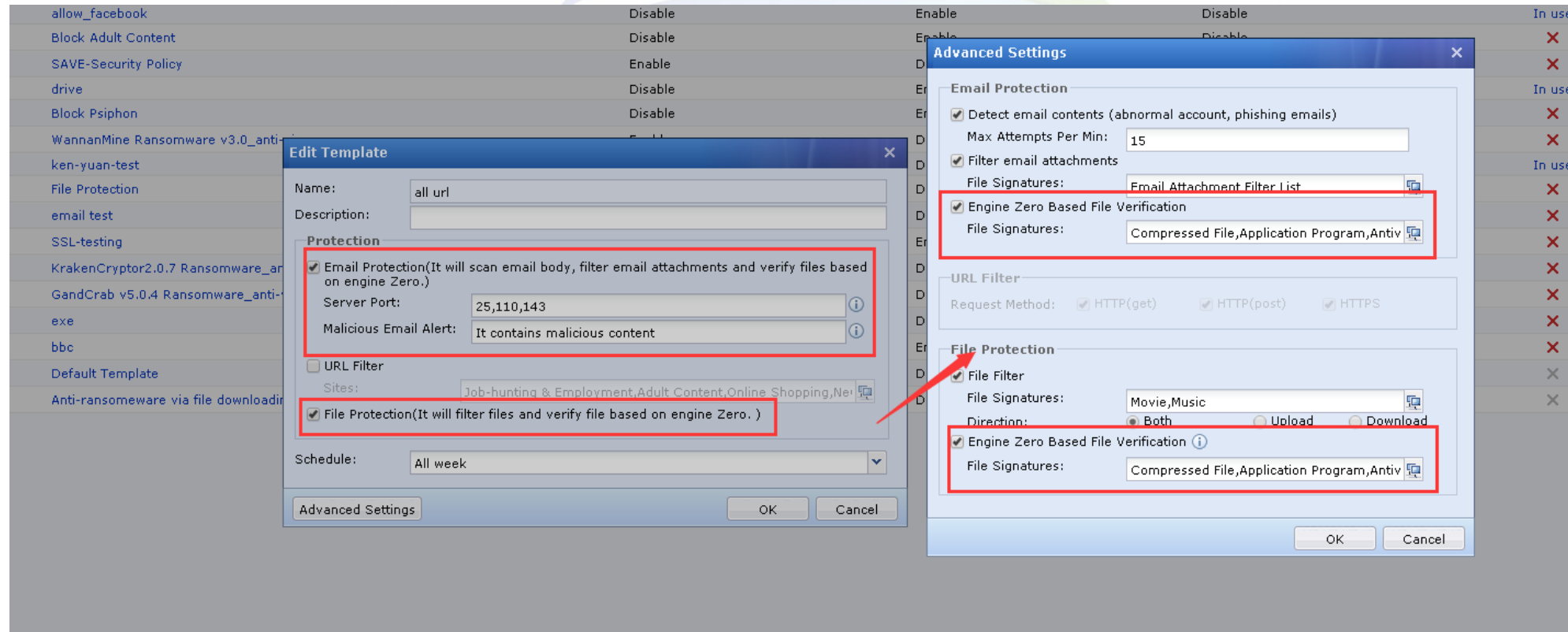
SAVE Engine

SAVE (Sangfor AI-based Vanguard Engine) adalah program pendeteksi file berbahaya berbasis 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

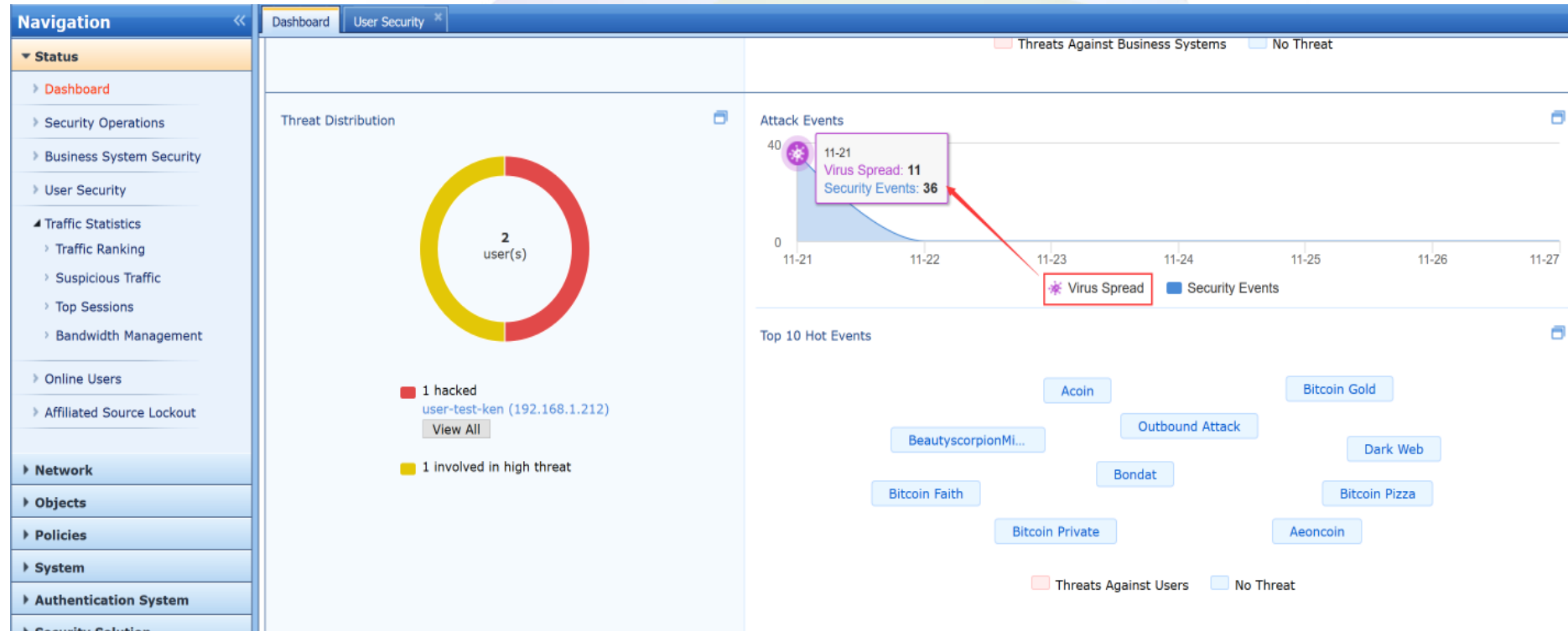
Jalur Konfigurasi: Object > Security Policy Template > Content Security > Add



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

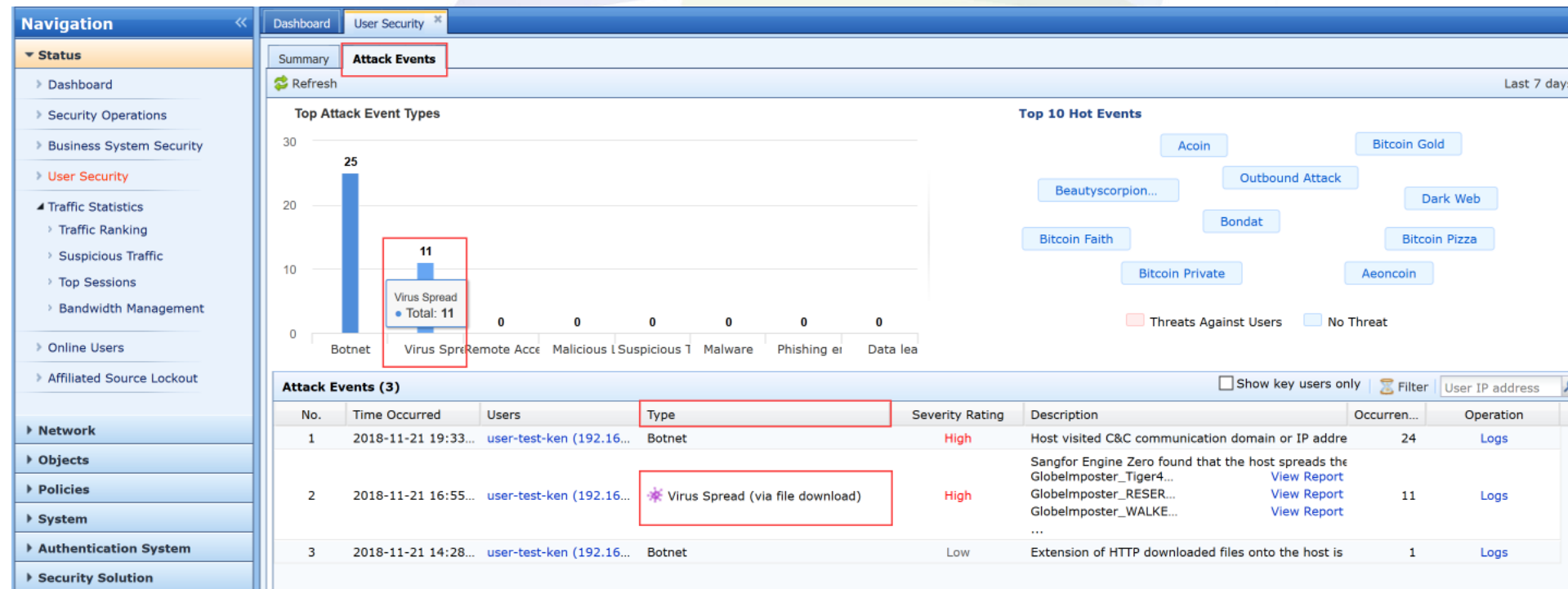
Penempatan dan deskripsi kinerja

Status keamanan pengguna di Dashboard menampilkan ikon penyebaran virus



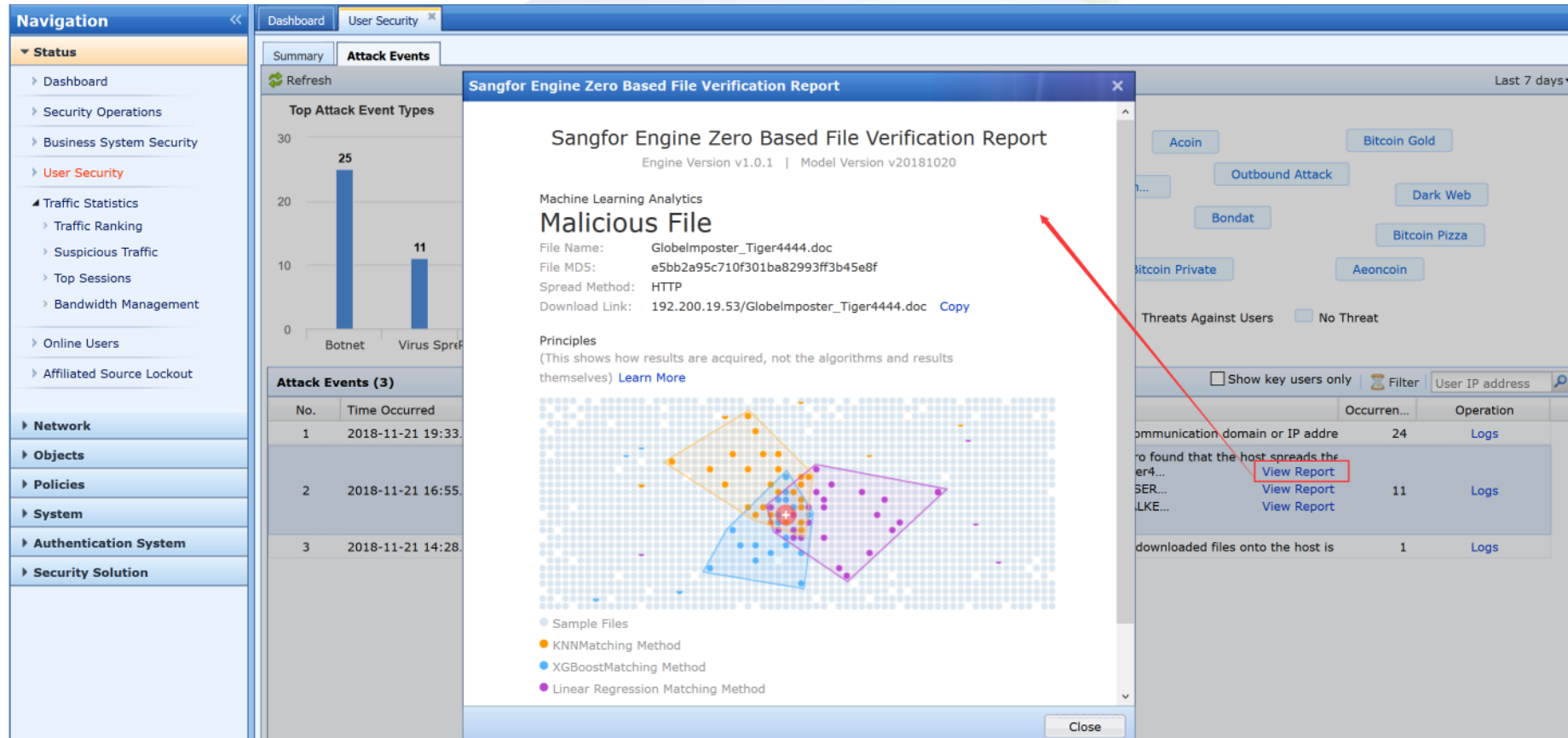
Penempatan dan deskripsi kinerja

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

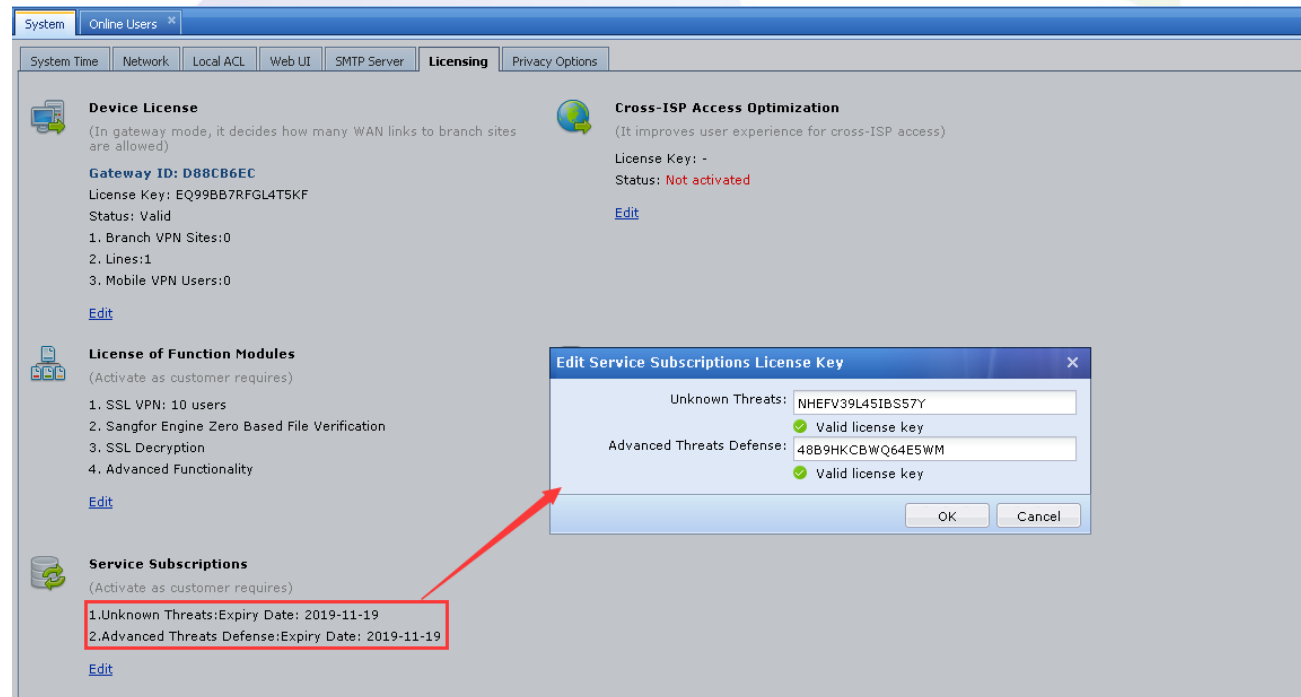
- NGAF memeriksa data yang lewat. Saat menemukan adanya local rule database yang tidak cocok, NGAF menguploadnya ke Neural X untuk memeriksa apakah itu adalah data yang berisiko.
- Rule Database Neural X memiliki lebih banyak sumber untuk terus memperkaya kemampuan pendeteksian
- Local rule database 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 mengecek Serial Numbernya.
- Navigasi ke System > General > Licensing, seperti yang ditunjukkan di bawah ini:



Catatan Neural 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)

