

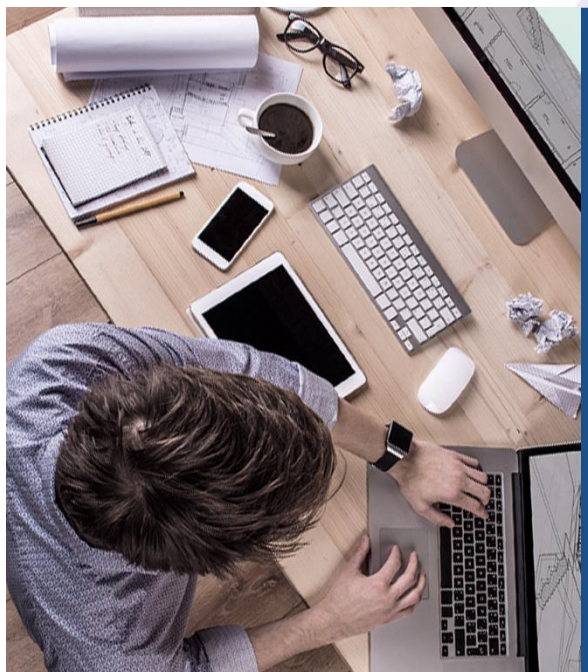


SANGFOR

Sangfor NGAF v8.0.6 Associate

Pengaturan Sistem





1 Lisensi

2 Databases Update

3 Backup/Restore

4 Global Whitelist/Blacklist

5 Troubleshooting

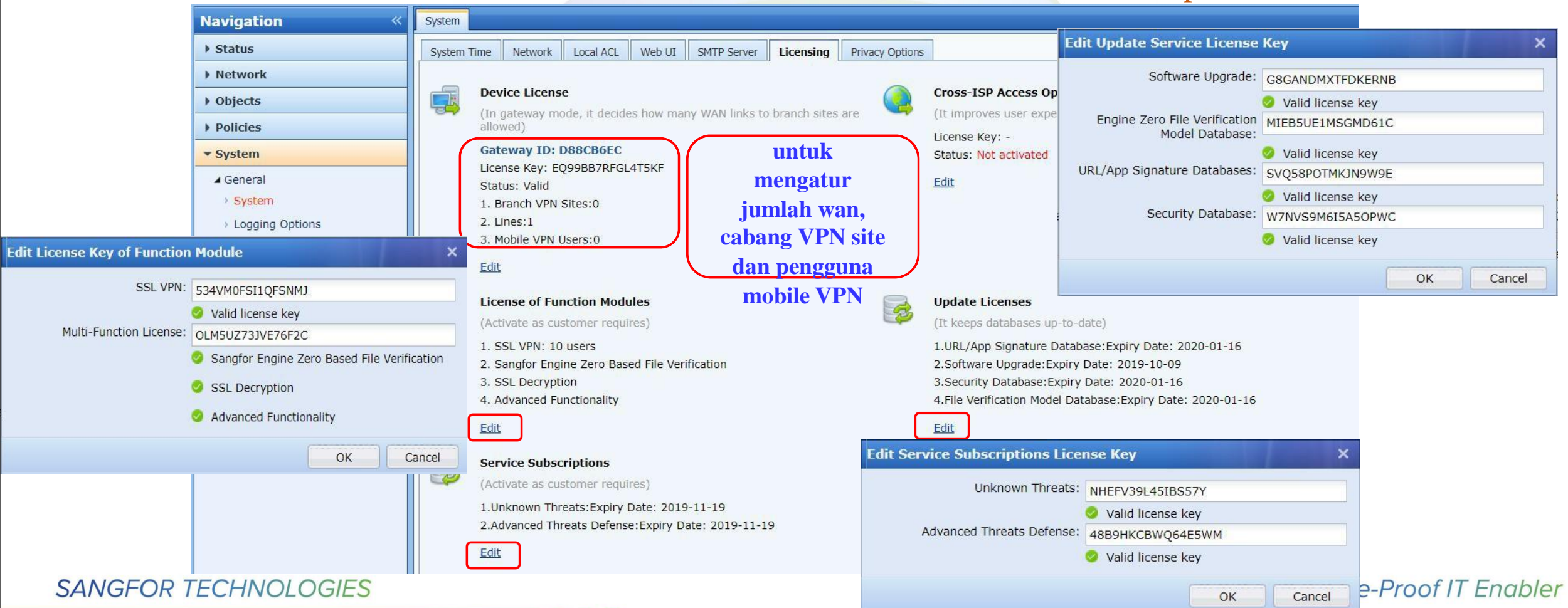
1. Lisensi



SANGFOR
深信服科技

Lisensi

Lisensi pada dasarnya digunakan untuk mengatur kerja sebuah perangkat. Berdasarkan beberapa modul pada perangkat, terdapat beberapa atribut lisensi : **Device License, Update Licenses, Server Access Verification, SSL VPN, Multi-Function License, Service Subscriptions License.**




The screenshot displays the Sangfor management interface with several license-related windows open:

- Navigation Panel:** Shows the 'System' menu expanded.
- System Time Tab:** Contains the 'Device License' section. A red box highlights the 'Gateway ID: D88CB6EC' and 'License Key: EQ99BB7RFGL4T5KF'. A blue text box explains: 'untuk mengatur jumlah wan, cabang VPN site dan pengguna mobile VPN'. Below this, the 'License of Function Modules' section lists: 1. SSL VPN: 10 users, 2. Sangfor Engine Zero Based File Verification, 3. SSL Decryption, 4. Advanced Functionality. A red box highlights the 'Edit' button.
- Service Subscriptions Section:** Lists: 1. Unknown Threats: Expiry Date: 2019-11-19, 2. Advanced Threats Defense: Expiry Date: 2019-11-19. A red box highlights the 'Edit' button.
- Edit Update Service License Key Window:** Shows fields for Software Upgrade (G8GANDMXTFDKERNB), Engine Zero File Verification Model Database (MIEB5UE1MSGMD61C), URL/App Signature Databases (SVQ58POTMKJN9W9E), and Security Database (W7NVS9M6I5A5OPWC). All are marked as 'Valid license key'.
- Edit License Key of Function Module Window:** Shows fields for SSL VPN (534VM0FSI1QFSNMJ) and Multi-Function License (OLM5UZ73JVE76F2C). Both are marked as 'Valid license key'.
- Edit Service Subscriptions License Key Window:** Shows fields for Unknown Threats (NHEFV39L45IBS57Y) and Advanced Threats Defense (48B9HKCBWQ64E5WM). Both are marked as 'Valid license key'.

SANGFOR TECHNOLOGIES e-Proof IT Enabler

Lisensi

**Update Licenses**
(It keeps databases up-to-date)
1.URL/App Signature Database:Expiry Date: 2020-01-16
2.Software Upgrades:Expiry Date: 2019-10-09
3.Security Database:Expiry Date: 2020-01-16
4.File Verification Model Database:Expiry Date: 2020-01-16
[Edit](#)

Setiap database bergantung kepada lisensi yang mengatur kapabilitas database tersebut

Database Update

☒ Enable ☐ Disable ☐ Offline Update ☐ Update Now ☐ Update Server ☐ Proxy Options ☒ Refresh Status: Not updating

| <input type="checkbox"/> | No. | Database | Current Version | Latest Version | Update Svc Expira... | Auto Update | Operation |
|--------------------------|-----|----------------------------------|------------------------------------------|---------------------|----------------------|-------------|-----------|
| <input type="checkbox"/> | 1 | File Verification Model Database | 2018-11-15 Logs | Unavailable Details | 2020-01-16 | ✓ | |
| <input type="checkbox"/> | 2 | URL Database | 2018-12-25 Logs | Unavailable Details | 2020-01-16 | ✗ | |
| <input type="checkbox"/> | 3 | Vulnerability Database | 2019-01-09 Logs | Unavailable Details | 2020-01-16 | ✓ | |
| <input type="checkbox"/> | 4 | Software Update | support-build support KB-AF-20181018-... | Unavailable Details | Never expire | ✓ | |
| <input type="checkbox"/> | 5 | Application Ident Database | 2019-01-07 Logs | Unavailable Details | 2020-01-16 | ✗ | |
| <input type="checkbox"/> | 6 | WAF Signature Database | 2019-01-09 Logs | Unavailable Details | 2020-01-16 | ✓ | |
| <input type="checkbox"/> | 7 | Data Leak Protection | 2018-02-16 Logs | Unavailable Details | 2020-01-16 | ✓ | |
| <input type="checkbox"/> | 8 | Vulnerability Analysis Rule | 2018-12-26 Logs | Unavailable Details | 2020-01-16 | ✓ | |
| <input type="checkbox"/> | 9 | Malicious Connection Database | 2019-01-14 Logs | Unavailable Details | Never expire | ✓ | |
| <input type="checkbox"/> | 10 | Threat Intelligence Database | 2018-12-26 Logs | Unavailable Details | Never expire | ✓ | |
| <input type="checkbox"/> | 11 | Hot Threat Database | 2018-07-27 Logs | Unavailable Details | 2020-01-16 | ✓ | |
| <input type="checkbox"/> | 12 | Security Events | 2018-07-31 Logs | Unavailable Details | 2020-01-16 | ✓ | |

2. Databases Update



SANGFOR
深信服科技

Databases Update

NGAF memiliki banyak libraries, seperti database anti-virus/url/aplikasi, dan lain lain.

Kami telah menunjuk kelompok untuk memelihara database sehingga bisa beradaptasi dengan perubahan lingkungan, **Pilihan rekomendasi untuk Auto update.**

(1) Offline update

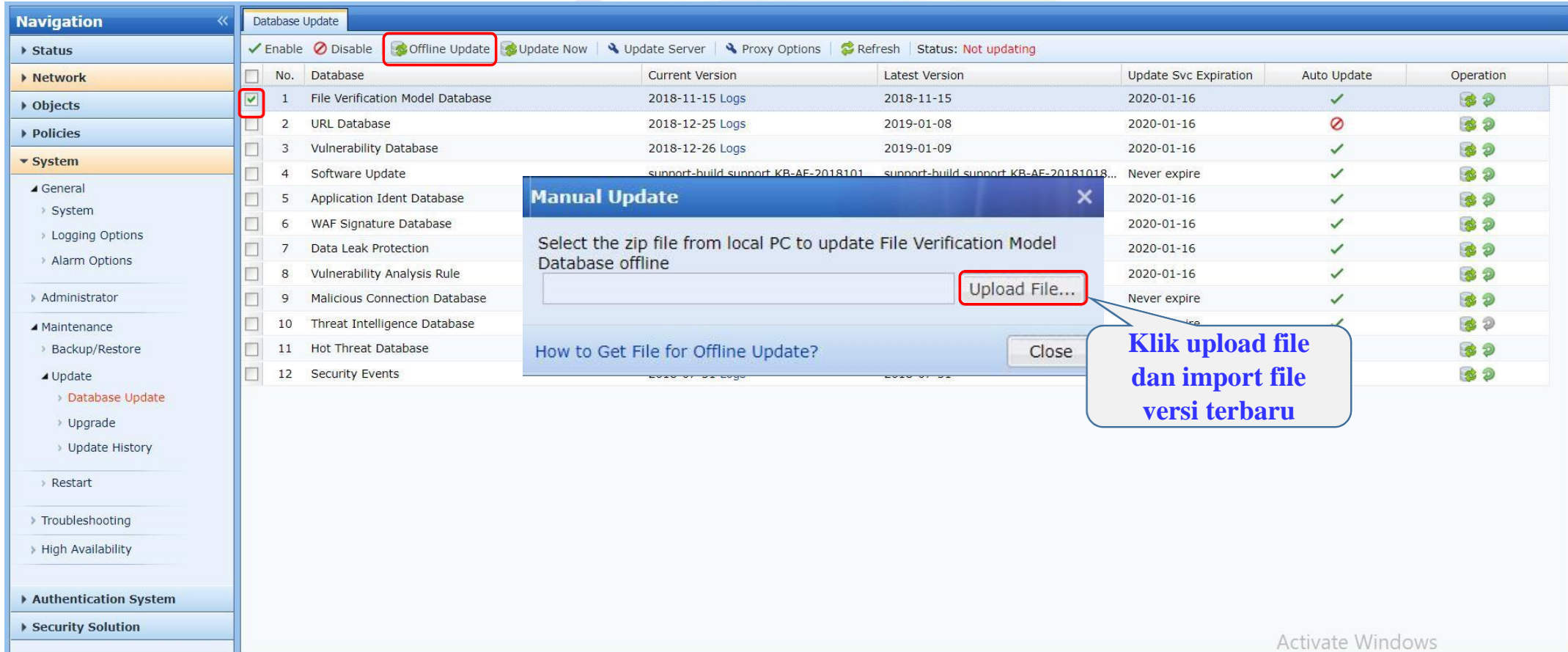
Kita bisa mendapatkan library dan meng-import kedalam perangkat secara manual sebelum layanan update sudah tidak valid(expired)

(2) Auto update

Pastikan bahwa NGAF terkoneksi dengan server Sangfor update. Jika ada update terbaru, NGAF akan mendapatkan library dari server secara otomatis, dengan syarat layanan update masih valid.

Databases Update

Secara Offline



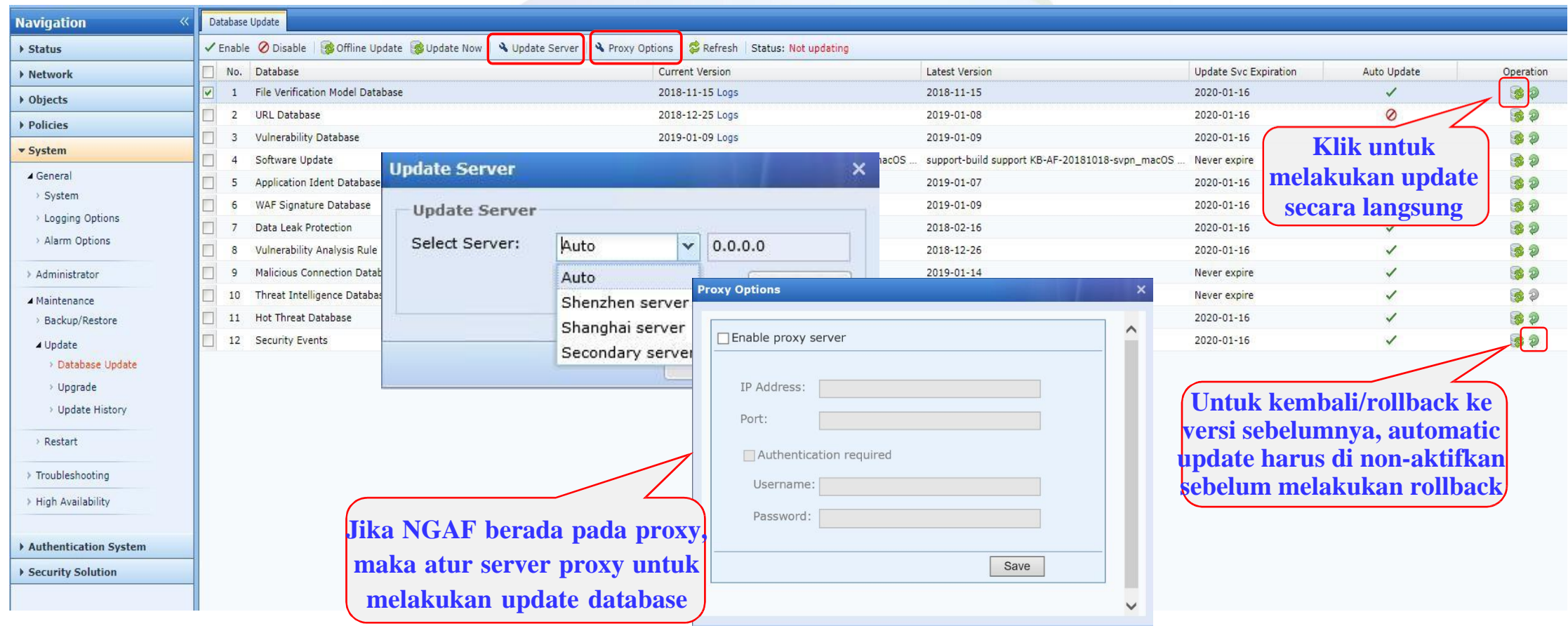
The screenshot displays the Sangfor security management interface. On the left is a navigation menu with categories like Status, Network, Objects, Policies, System, Administrator, Maintenance, Update, Authentication System, and Security Solution. The 'Database Update' tab is active in the main panel. It shows a table of databases with columns for No., Database, Current Version, Latest Version, Update Svc Expiration, Auto Update, and Operation. The 'Offline Update' button is highlighted with a red box. A 'Manual Update' dialog box is open, prompting the user to 'Select the zip file from local PC to update File Verification Model Database offline'. The 'Upload File...' button in the dialog is also highlighted with a red box. A callout bubble points to this button with the text 'Klik upload file dan import file versi terbaru'. The status bar at the top indicates 'Status: Not updating'.

| No. | Database | Current Version | Latest Version | Update Svc Expiration | Auto Update | Operation |
|-----|----------------------------------|----------------------------------------|-----------------------------------------|-----------------------|-------------|-----------|
| 1 | File Verification Model Database | 2018-11-15 Logs | 2018-11-15 | 2020-01-16 | ✓ | |
| 2 | URL Database | 2018-12-25 Logs | 2019-01-08 | 2020-01-16 | ✗ | |
| 3 | Vulnerability Database | 2018-12-26 Logs | 2019-01-09 | 2020-01-16 | ✓ | |
| 4 | Software Update | support-build support_KB-AF-2018101... | support-build support_KB-AF-20181018... | Never expire | ✓ | |
| 5 | Application Ident Database | | | 2020-01-16 | ✓ | |
| 6 | WAF Signature Database | | | 2020-01-16 | ✓ | |
| 7 | Data Leak Protection | | | 2020-01-16 | ✓ | |
| 8 | Vulnerability Analysis Rule | | | 2020-01-16 | ✓ | |
| 9 | Malicious Connection Database | | | Never expire | ✓ | |
| 10 | Threat Intelligence Database | | | | ✓ | |
| 11 | Hot Threat Database | | | | | |
| 12 | Security Events | | | | | |

Databases update

Auto update

NGAF akan melakukan update database setiap pagi.



The screenshot shows the 'Database Update' section of the Sangfor NGAF management console. The interface includes a navigation sidebar on the left, a main table of databases, and two modal windows for configuration.

Database Update Table:

| No. | Database | Current Version | Latest Version | Update Svc Expiration | Auto Update | Operation |
|-----|----------------------------------|-----------------|------------------------------------------------------|-----------------------|-------------|-----------|
| 1 | File Verification Model Database | 2018-11-15 Logs | 2018-11-15 | 2020-01-16 | ✓ | [Update] |
| 2 | URL Database | 2018-12-25 Logs | 2019-01-08 | 2020-01-16 | ✗ | [Update] |
| 3 | Vulnerability Database | 2019-01-09 Logs | 2019-01-09 | 2020-01-16 | ✓ | [Update] |
| 4 | Software Update | | support-build support KB-AF-20181018-svnpn_macOS ... | Never expire | ✓ | [Update] |
| 5 | Application Ident Database | | 2019-01-07 | 2020-01-16 | ✓ | [Update] |
| 6 | WAF Signature Database | | 2019-01-09 | 2020-01-16 | ✓ | [Update] |
| 7 | Data Leak Protection | | 2018-02-16 | 2020-01-16 | ✓ | [Update] |
| 8 | Vulnerability Analysis Rule | | 2018-12-26 | 2020-01-16 | ✓ | [Update] |
| 9 | Malicious Connection Data | | 2019-01-14 | Never expire | ✓ | [Update] |
| 10 | Threat Intelligence Database | | | Never expire | ✓ | [Update] |
| 11 | Hot Threat Database | | | 2020-01-16 | ✓ | [Update] |
| 12 | Security Events | | | 2020-01-16 | ✓ | [Update] |

Update Server Modal:

Select Server:

Options: Auto, Shenzhen server, Shanghai server, Secondary server

Proxy Options Modal:

☐ Enable proxy server

IP Address:

Port:

☐ Authentication required

Username:

Password:


Save

Annotations:

- Update Server:** Klik untuk melakukan update secara langsung
- Proxy Options:** Untuk kembali/rollback ke versi sebelumnya, automatic update harus di non-aktifkan sebelum melakukan rollback
- Database Update Table:** Jika NGAF berada pada proxy, maka atur server proxy untuk melakukan update database

Databases update

Database update mengharuskan NGAF untuk mengakses internet, oleh karena itu penting untuk melakukan pengaturan DNS server yang benar.



The screenshot displays the SANGFOR NGAF web interface. On the left is a 'Navigation' sidebar with options like Status, Network, and Objects. The main area shows 'System' > 'Advanced Options' > 'DNS'. The 'DNS Server' section is highlighted with a red box and contains the text: 'Both automatic update and DNS proxy require valid DNS server be specified.' Below this, 'Preferred DNS' is set to '8.8.8.8' and 'Alternate DNS' is set to '8.8.4.4'. The 'DNS Proxy' section below it has 'DNS Proxy' set to 'Enable' (radio button selected). An 'OK' button is at the bottom right.

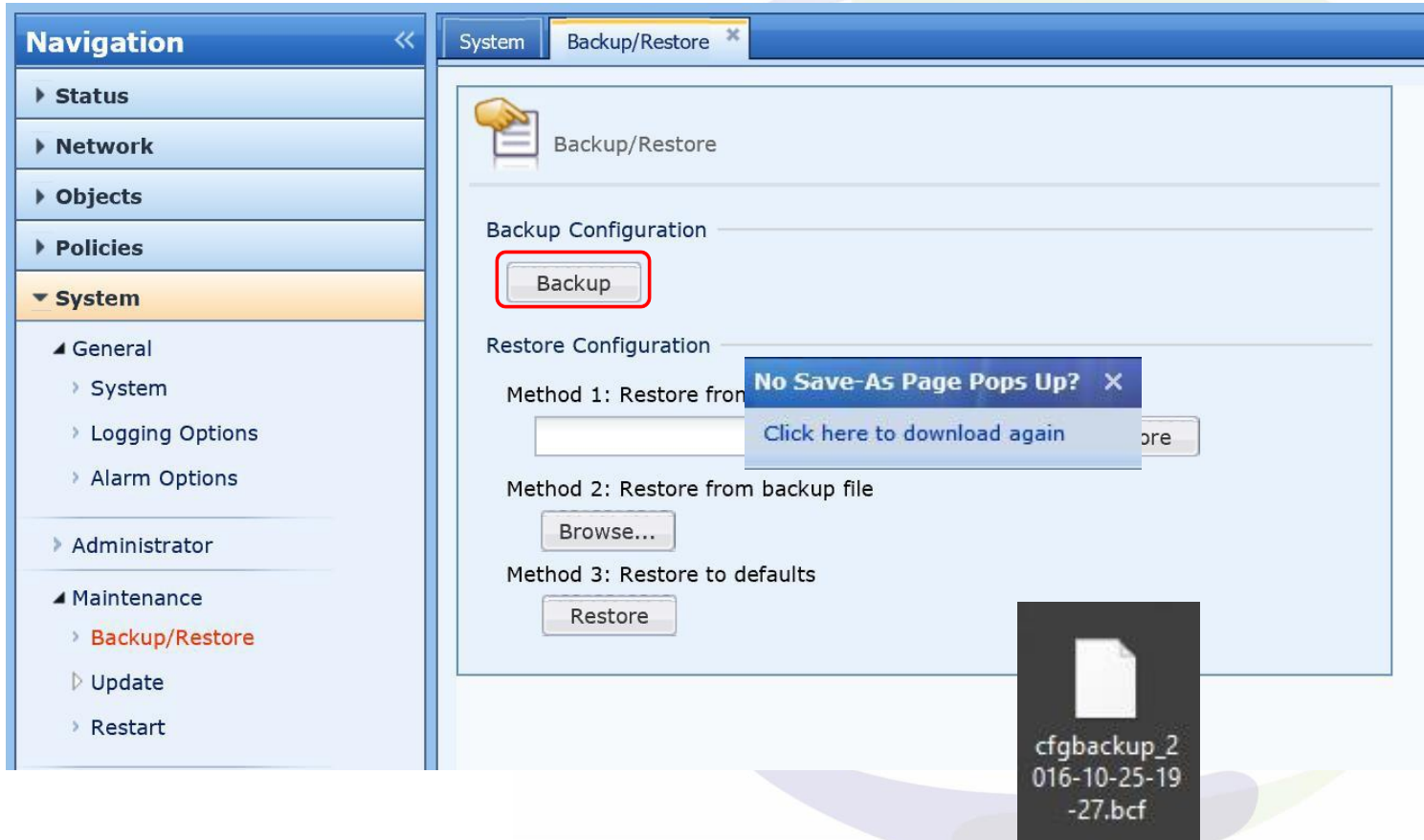
3. Backup/Restore



SANGFOR
深信服科技

Backup/Restore

Konfigurasi Backup



Navigation

- Status
- Network
- Objects
- Policies
- ▼ **System**
 - ▲ General
 - System
 - Logging Options
 - Alarm Options
 - Administrator
 - ▲ Maintenance
 - **Backup/Restore**
 - Update
 - Restart

System Backup/Restore

Backup/Restore

Backup Configuration

Backup

Restore Configuration

Method 1: Restore from [Click here to download again](#)

Method 2: Restore from backup file [Browse...](#)

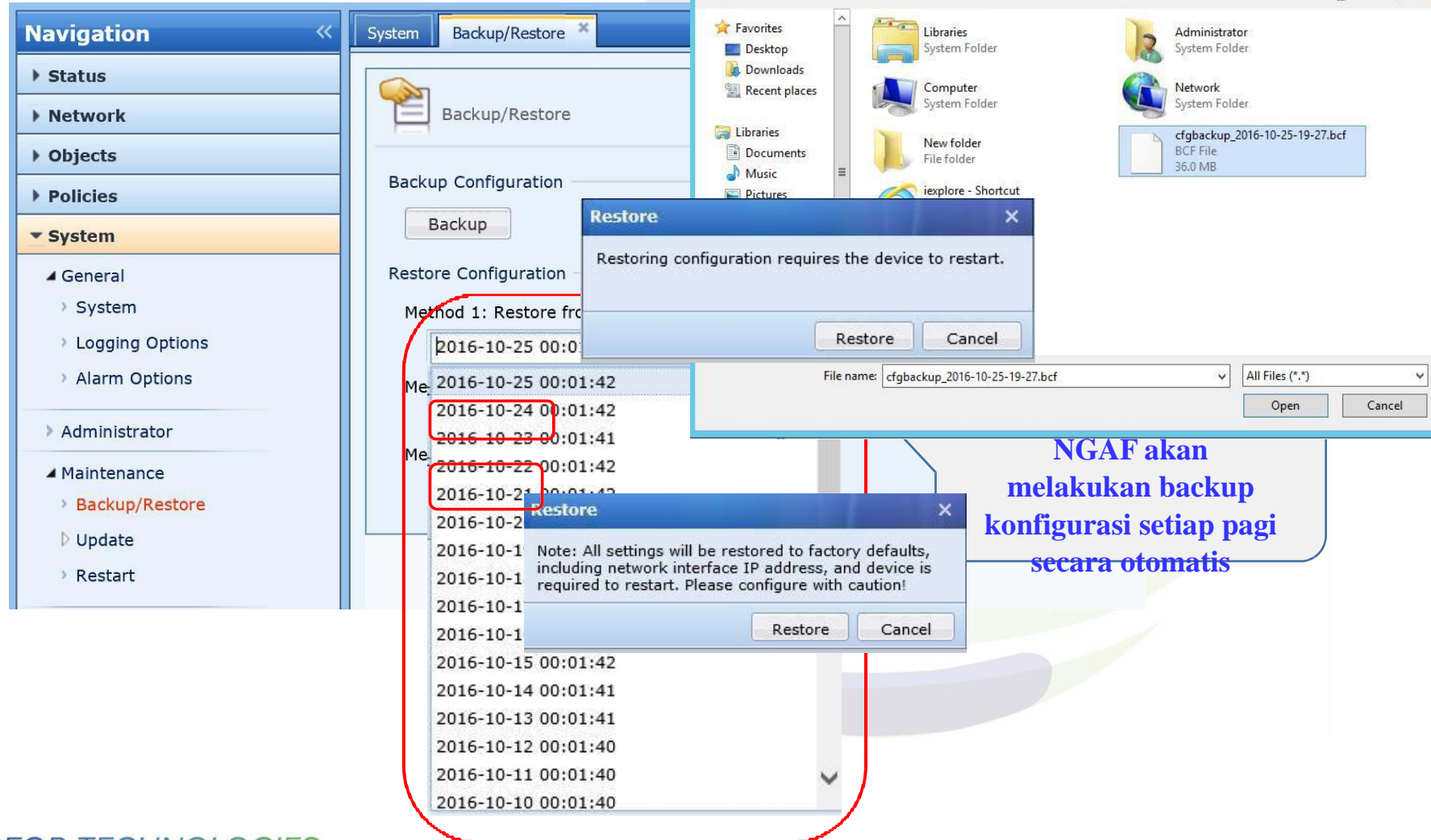
Method 3: Restore to defaults [Restore](#)

No Save-As Page Pops Up? [Click here to download again](#)

cfgbackup_2
016-10-25-19
-27.bcf

Backup/Restore

Konfigurasi Restore



The screenshot displays the Sangfor NGAF Backup/Restore configuration interface. The left sidebar shows the 'System' menu with 'Backup/Restore' highlighted. The main panel shows the 'Backup/Restore' configuration page, including 'Backup Configuration' and 'Restore Configuration' sections. A list of backup files is shown, with the file 'cfbackup_2016-10-25-19-27.bcf' selected. A 'Choose File to Upload' dialog box is open, showing the selected file. A 'Restore' dialog box is also open, displaying a warning message: 'Restoring configuration requires the device to restart.' A red line highlights the 'Restore' button in the 'Restore' dialog box. A blue callout box with the text 'NGAF akan melakukan backup konfigurasi setiap pagi secara otomatis' (NGAF will automatically backup configuration every morning) points to the 'Backup' button in the 'Backup Configuration' section.

Navigation

- Status
- Network
- Objects
- Policies
- ▼ System
 - ▲ General
 - System
 - Logging Options
 - Alarm Options
 - Administrator
 - ▲ Maintenance
 - Backup/Restore
 - Update
 - Restart

Backup/Restore

Backup Configuration

Backup

Restore Configuration

Method 1: Restore from

2016-10-25 00:01:42

Me 2016-10-24 00:01:42

2016-10-23 00:01:41

Me 2016-10-22 00:01:42

2016-10-21 00:01:42

2016-10-20 00:01:42

2016-10-19 00:01:42

2016-10-18 00:01:42

2016-10-17 00:01:42

2016-10-16 00:01:42

2016-10-15 00:01:42

2016-10-14 00:01:41

2016-10-13 00:01:41

2016-10-12 00:01:40

2016-10-11 00:01:40

2016-10-10 00:01:40

Choose File to Upload

File name: cfbackup_2016-10-25-19-27.bcf

All Files (*.*)

Open Cancel

Restore

Restoring configuration requires the device to restart.

Restore Cancel

Restore

Note: All settings will be restored to factory defaults, including network interface IP address, and device is required to restart. Please configure with caution!

Restore Cancel

NGAF akan melakukan backup konfigurasi setiap pagi secara otomatis

4. Global Whitelist/Blacklist



SANGFOR
深信服科技

Global Whitelist/Blacklist

IP/domain yang ditambahkan pada whitelist dikecualikan pada NGAF policy.

Navigation

Status

Network

Objects

Policies

NAT

Access Control

Application Control

Country Blocking

Connection Control

Network Security

Policies

Anti-DoS/DDoS

ARP Spoofing Prevention

Decryption

Bandwidth Management

Configuration Wizard

Blacklist/Whitelist

Custom Webpage

System

Authentication System

Security Solution

Blacklist/Whitelist

Global Whitelist Global Blacklist

Refresh

Add

Delete

Enable

Disable

Import

Export

Search term

| No. | Address | Description | Type | Time Created | Status |
|-----|-------------------------------------|-------------------------------------|-----------|------------------|--------|
| 1 | 192.168.19.238 | Test PC | Specified | 2018-12-21 17:24 | ✓ |
| 2 | sangfor.net | sangfor.net | Internal | 2011-07-01 08:30 | ✓ |
| 3 | update1.sangfor.net | update1.sangfor.net | Internal | 2011-07-01 08:30 | ✓ |
| 4 | sangfor.com | sangfor.com | Internal | 2011-07-01 08:30 | ✓ |
| 5 | sangfor.com.cn | sangfor.com.cn | Internal | 2011-07-01 08:30 | ✓ |
| 6 | sinfors.com | sinfors.com | Internal | 2011-07-01 08:30 | ✓ |
| 7 | sinfors.com.cn | sinfors.com.cn | Internal | 2011-07-01 08:30 | ✓ |
| 8 | duba.net | duba.net | Internal | 2011-07-01 08:30 | ✓ |
| 9 | urs.microsoft.com | urs.microsoft.com | Internal | 2011-07-01 08:30 | ✓ |
| 10 | smartscreen.microsoft.com.nsatc.net | smartscreen.microsoft.com.nsatc.net | Internal | 2011-07-01 08:30 | ✓ |
| 11 | smartscreen.microsoft.com | smartscreen.microsoft.com | Internal | 2011-07-01 08:30 | ✓ |
| 12 | acs.pandasoftware.com | acs.pandasoftware.com | Internal | 2011-07-01 08:30 | ✓ |
| 13 | upgrades.pandasoftware.com | upgrades.pandasoftware.com | Internal | 2011-07-01 08:30 | ✓ |
| 14 | db.kingsoft.com | db.kingsoft.com | Internal | 2011-07-01 08:30 | ✓ |
| 15 | liveupdate.symantecliveupdate.com | liveupdate.symantecliveupdate.com | Internal | 2011-07-01 08:30 | ✓ |
| 16 | jiangmin.com | jiangmin.com | Internal | 2011-07-01 08:30 | ✓ |
| 17 | kaspersky-labs.com | kaspersky-labs.com | Internal | 2011-07-01 08:30 | ✓ |
| 18 | activeupdate.trendmicro.com | activeupdate.trendmicro.com | Internal | 2011-07-01 08:30 | ✓ |
| 19 | pccchk.trendmicro.com | pccchk.trendmicro.com | Internal | 2011-07-01 08:30 | ✓ |
| 20 | windowsupdate.microsoft.com | windowsupdate.microsoft.com | Internal | 2011-07-01 08:30 | ✓ |
| 21 | download.windowsupdate.com | download.windowsupdate.com | Internal | 2011-07-01 08:30 | ✓ |

1 / 1

50

bisa aktif/non-aktifkan setiap pengaturan bawaan ataupun khusus.

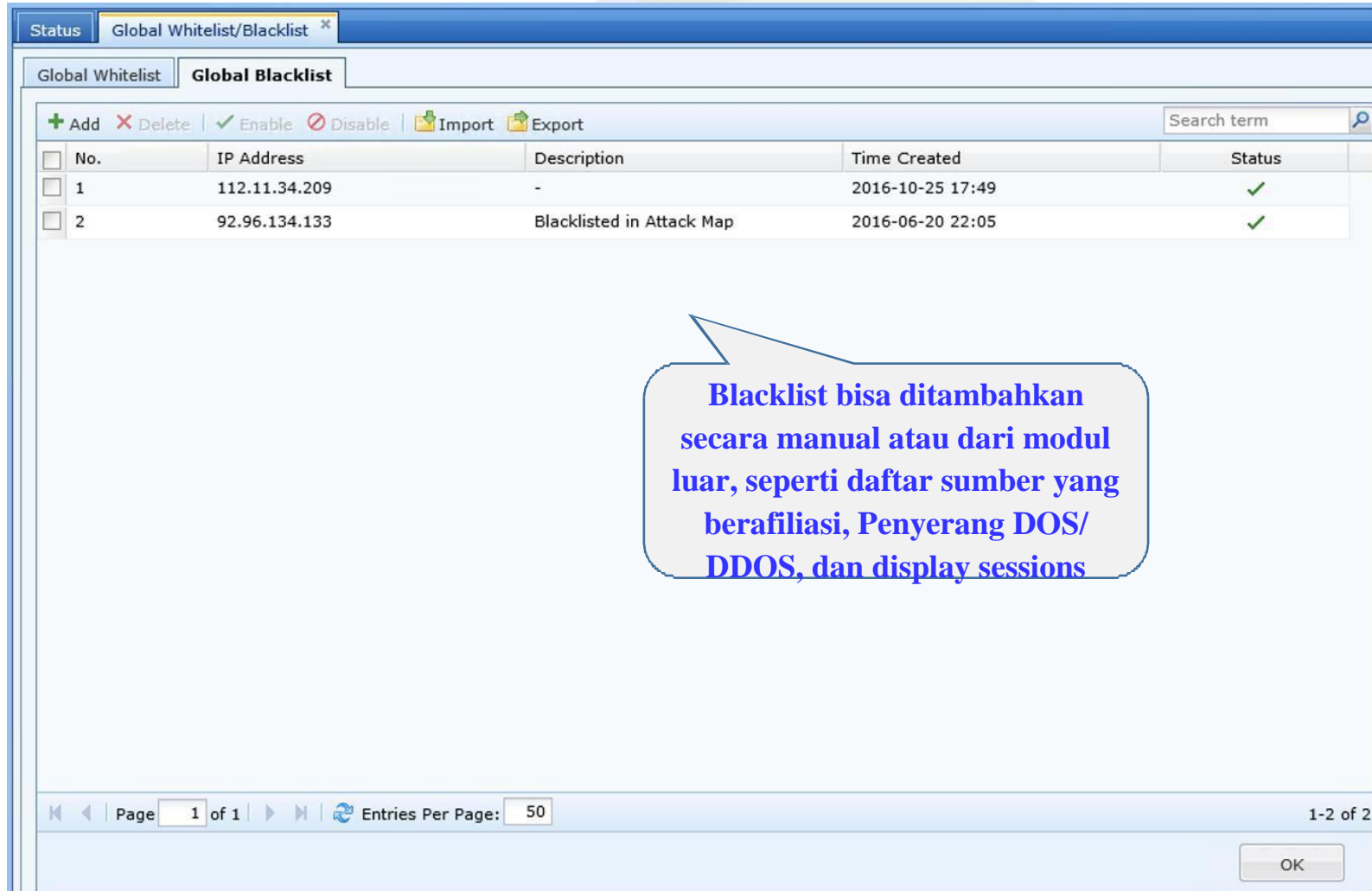
Tambah manual

Berbagai macam domain bawaan untuk antivirus dan NGAF database update, dan peraturan bawaan ini tidak bisa dihapus

tambah waktu

Global Whitelist/Blacklist

IP ditambahkan ke Global Blacklist akan di-blok oleh NGAF pada jaringan.



Global Whitelist/Blacklist

Global Whitelist Global Blacklist

+ Add - Delete Enable Disable Import Export Search term

| No. | IP Address | Description | Time Created | Status |
|-----|---------------|---------------------------|------------------|--------|
| 1 | 112.11.34.209 | - | 2016-10-25 17:49 | ✓ |
| 2 | 92.96.134.133 | Blacklisted in Attack Map | 2016-06-20 22:05 | ✓ |

Blacklist bisa ditambahkan secara manual atau dari modul luar, seperti daftar sumber yang berafiliasi, Penyerang DOS/DDOS, dan display sessions

Page 1 of 1 Entries Per Page: 50 1-2 of 2 OK

Global Whitelist/Blacklist

After menambahkan IP atau nama domain ke **Global whitelist**, modul-modul berikut yang akan tetap aktif, yaitu:

Packet-based attack dan abnormal message probe pada DOS/DDOS protection.

Setelah mengaktifkan bypass pada **Troubleshooting(software bypass)**, modul-modul berikut yang akan tetap aktif, yaitu:

Packet-based attack dan abnormal message probe pada DOS/DDOS protection, HTTP dan FTP application hiding.

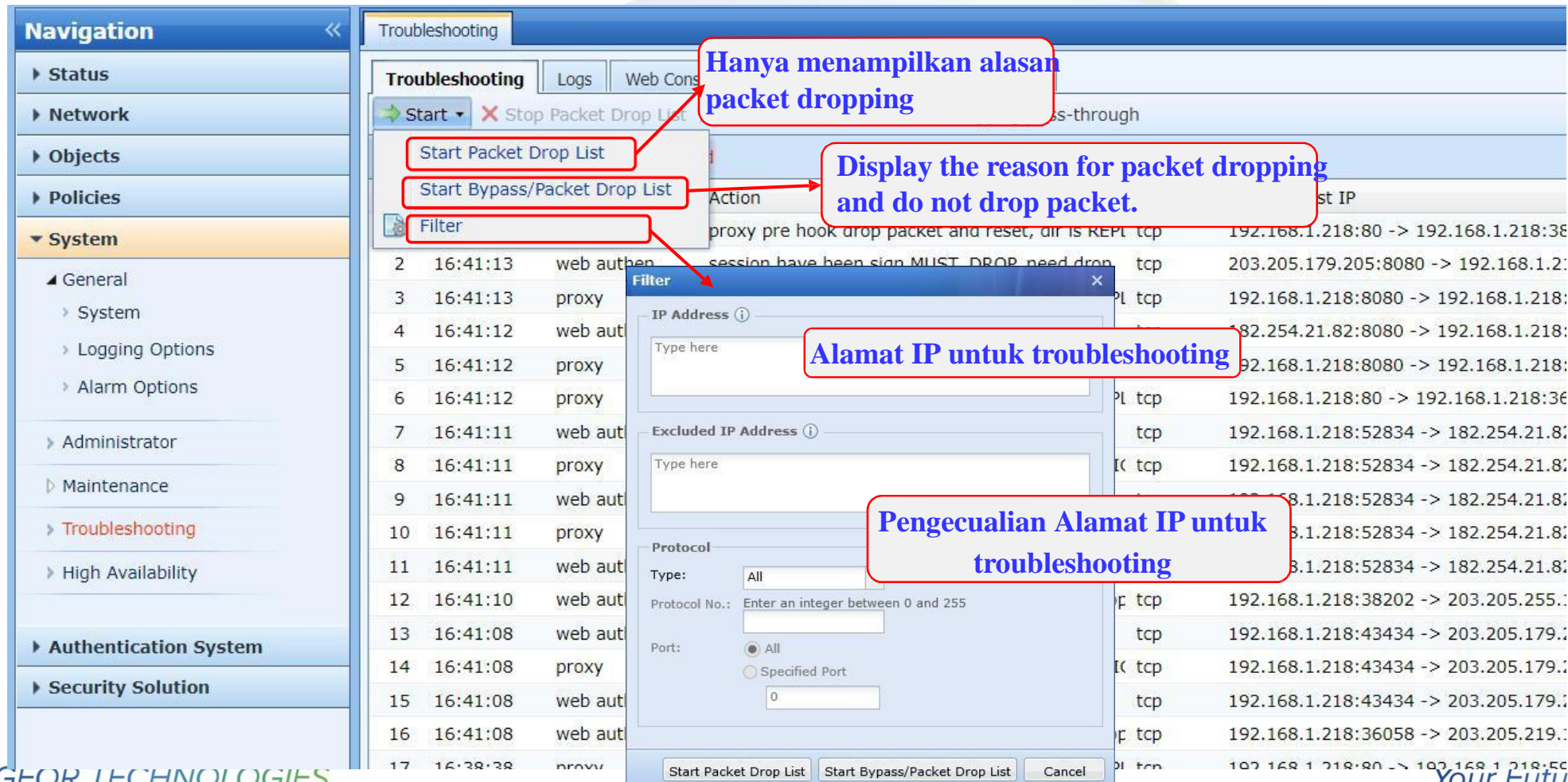
5. Troubleshooting



SANGFOR
深信服科技

Troubleshooting(software bypass)

Ketika kita menghadapi masalah tetapi kita tidak mengetahui penyebab masalahnya, kita bisa mulai dengan bypass/packet drop list. Melalui packet yang sudah difilter, bisa kita lihat policy mana yang beermasalah.



The screenshot shows the Sangfor Troubleshooting interface. On the left is a navigation menu with categories: Status, Network, Objects, Policies, and System (expanded). Under System, there are sub-items: General, System, Logging Options, Alarm Options, Administrator, Maintenance, Troubleshooting (highlighted), and High Availability. Below these are Authentication System and Security Solution.

The main area is titled 'Troubleshooting' and contains a table of logs. The table has columns for time, action, and details. The logs show various actions like 'web authentication', 'proxy', and 'web authentication'.

Annotations with red boxes and blue text are present:

- Hanya menampilkan alasan packet dropping** (Only display the reason for packet dropping) - points to the 'Start Packet Drop List' button.
- Display the reason for packet dropping and do not drop packet.** - points to the 'Start Bypass/Package Drop List' button.
- Alamat IP untuk troubleshooting** (IP address for troubleshooting) - points to the 'Filter' button.
- Pengecualian Alamat IP untuk troubleshooting** (IP address exception for troubleshooting) - points to the 'Filter' dialog box.

The 'Filter' dialog box is open, showing fields for 'IP Address' and 'Excluded IP Address', both with 'Type here' placeholders. It also has a 'Protocol' section with 'Type' set to 'All', 'Protocol No.' set to 'Enter an integer between 0 and 255', and 'Port' set to 'All'.

At the bottom of the dialog are buttons: 'Start Packet Drop List', 'Start Bypass/Package Drop List', and 'Cancel'.

Troubleshooting(software bypass)

Bagaimana cara melakukan troubleshooting(software bypass)?

| Troubleshooting | | | | | | | | | | |
|-------------------------------------------------------------------------------------------------------------------------|----------|-------------|--------------------------------------------------|----------|----------------------------------------|--------------|--------|-------|------------------|---------------|
| Start Stop Packet Drop List Refresh Start L2 debugging pass-through | | | | | | | | | | |
| Current Status: Packet drop list and bypass start | | | | | | | | | | |
| No. | Time | Source | Action | Protocol | Src IP > Dst IP | Device | Size | Line | Packet Drop T... | Application |
| 1 | 11:42:43 | app control | previs haved matched policy, app control drop t | cmp | 192.168.1.3:8 -> 192.200.19.200:0 | eth3 -> eth1 | 74(B) | Line1 | appcontrol | ICMP Protocol |
| 2 | 11:42:43 | app control | previs haved matched policy, app control drop t | cmp | 192.200.19.200:0 -> 192.168.1.3:0 | eth1 -> eth3 | 74(B) | Line1 | appcontrol | ICMP Protocol |
| 3 | 11:42:42 | app control | previs haved matched policy, app control drop t | cmp | 192.168.1.3:8 -> 192.200.19.200:0 | eth3 -> eth1 | 74(B) | Line1 | appcontrol | ICMP Protocol |
| 4 | 11:42:42 | app control | previs haved matched policy, app control drop t | cmp | 192.200.19.200:0 -> 192.168.1.3:0 | eth1 -> eth3 | 74(B) | Line1 | appcontrol | ICMP Protocol |
| 5 | 11:42:41 | app control | previs haved matched policy, app control drop t | cmp | 192.168.1.3:8 -> 192.200.19.200:0 | eth3 -> eth1 | 74(B) | Line1 | appcontrol | ICMP Protocol |
| 6 | 11:42:41 | app control | previs haved matched policy, app control drop t | cmp | 192.200.19.200:0 -> 192.168.1.3:0 | eth1 -> eth3 | 74(B) | Line1 | appcontrol | ICMP Protocol |
| 7 | 11:42:40 | app control | previs haved matched policy, app control drop t | cmp | 192.168.1.3:8 -> 192.200.19.200:0 | eth3 -> eth1 | 74(B) | Line1 | appcontrol | ICMP Protocol |
| 8 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 54(B) | Line1 | appcontrol | SSL |
| 9 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 192.168.1.3:58715 -> 200.200.5.100:443 | eth3 -> eth1 | 54(B) | Line1 | appcontrol | SSL |
| 10 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 192.168.1.3:58715 -> 200.200.5.100:443 | eth3 -> eth1 | 54(B) | Line1 | appcontrol | SSL |
| 11 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 192.168.1.3:58715 -> 200.200.5.100:443 | eth3 -> eth1 | 54(B) | Line1 | appcontrol | SSL |
| 12 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 54(B) | Line1 | appcontrol | SSL |
| 13 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 86(B) | Line1 | appcontrol | SSL |
| 14 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 59(B) | Line1 | appcontrol | SSL |
| 15 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 502(B) | Line1 | appcontrol | SSL |
| 16 | 11:42:40 | app control | app control drop the packet default policy. mast | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 59(B) | Line1 | appcontrol | SSL |
| 17 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 54(B) | Line1 | appcontrol | SSL |
| 18 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 192.168.1.3:58715 -> 200.200.5.100:443 | eth3 -> eth1 | 176(B) | Line1 | appcontrol | SSL |
| 19 | 11:42:40 | app control | app control drop the packet default policy. mast | tcp | 192.168.1.3:58715 -> 200.200.5.100:443 | eth3 -> eth1 | 736(B) | Line1 | appcontrol | SSL |
| 20 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 192.168.1.3:58715 -> 200.200.5.100:443 | eth3 -> eth1 | 54(B) | Line1 | appcontrol | SSL_HELLO |
| 21 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 102(B) | Line1 | appcontrol | SSL_HELLO |
| 22 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 59(B) | Line1 | appcontrol | SSL_HELLO |
| 23 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 55(B) | Line1 | appcontrol | SSL_HELLO |
| 24 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 59(B) | Line1 | appcontrol | SSL_HELLO |
| 25 | 11:42:40 | app control | previs haved matched policy, app control drop t | tcp | 200.200.5.100:443 -> 192.168.1.3:58715 | eth1 -> eth3 | 54(B) | Line1 | appcontrol | SSL_HELLO |

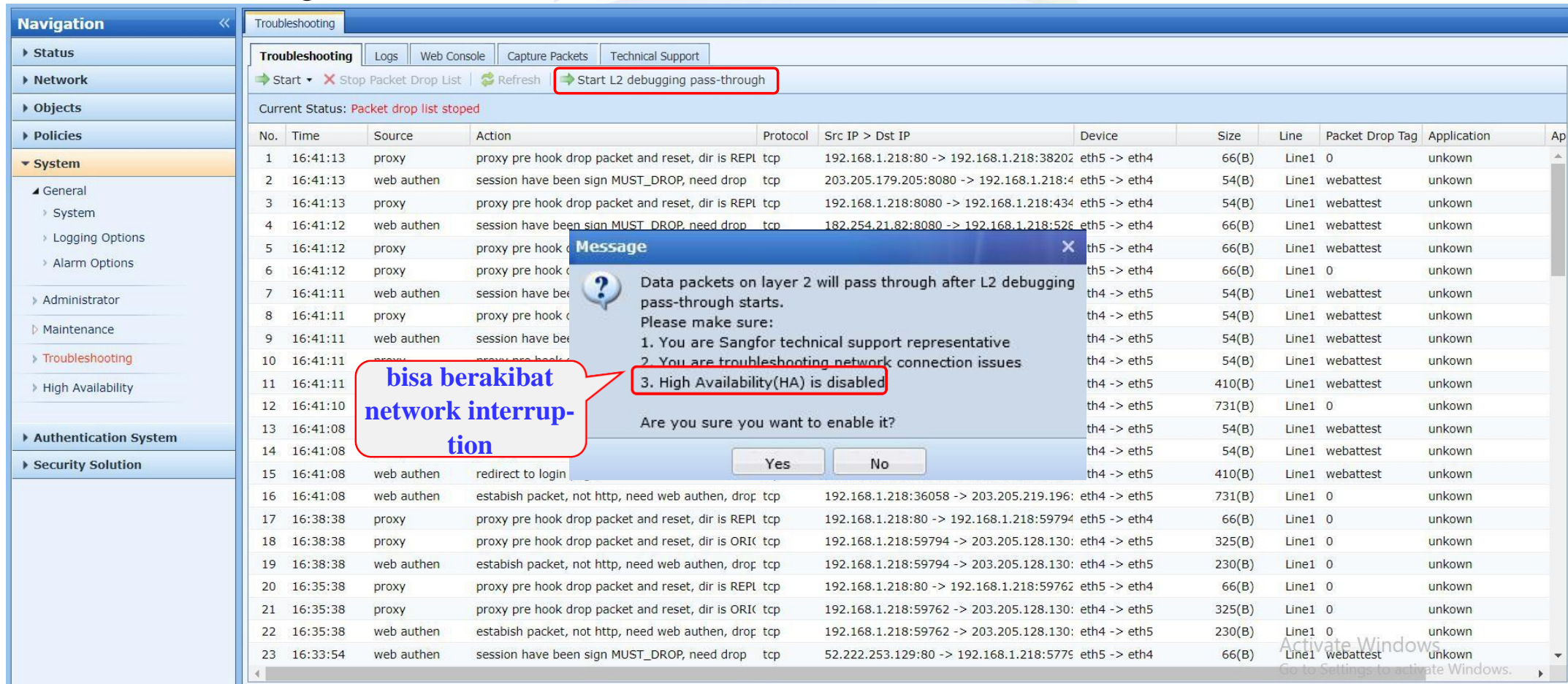
ini di-blok oleh
app control policy

Traffic flow

Aplikasi yang
di-blok

Troubleshooting(software bypass)

Layer 2 pass-through hanya efektif untuk mode bridge. Virtual wire hanya akan efektif jika Packet melalui forwarding network interface.



The screenshot shows the Sangfor Troubleshooting interface. On the left is a navigation menu with sections: Status, Network, Objects, Policies, System (expanded), Administrator, Maintenance, Troubleshooting (selected), High Availability, Authentication System, and Security Solution. The main area is titled 'Troubleshooting' and has tabs for Logs, Web Console, Capture Packets, and Technical Support. Below these tabs are buttons: Start (green), Stop Packet Drop List (red X), Refresh (green), and Start L2 debugging pass-through (green, highlighted with a red box). The current status is 'Packet drop list stopped'.

A table displays a list of packet drops with columns: No., Time, Source, Action, Protocol, Src IP > Dst IP, Device, Size, Line, Packet Drop Tag, Application, and Ap. The table contains 23 rows of data.

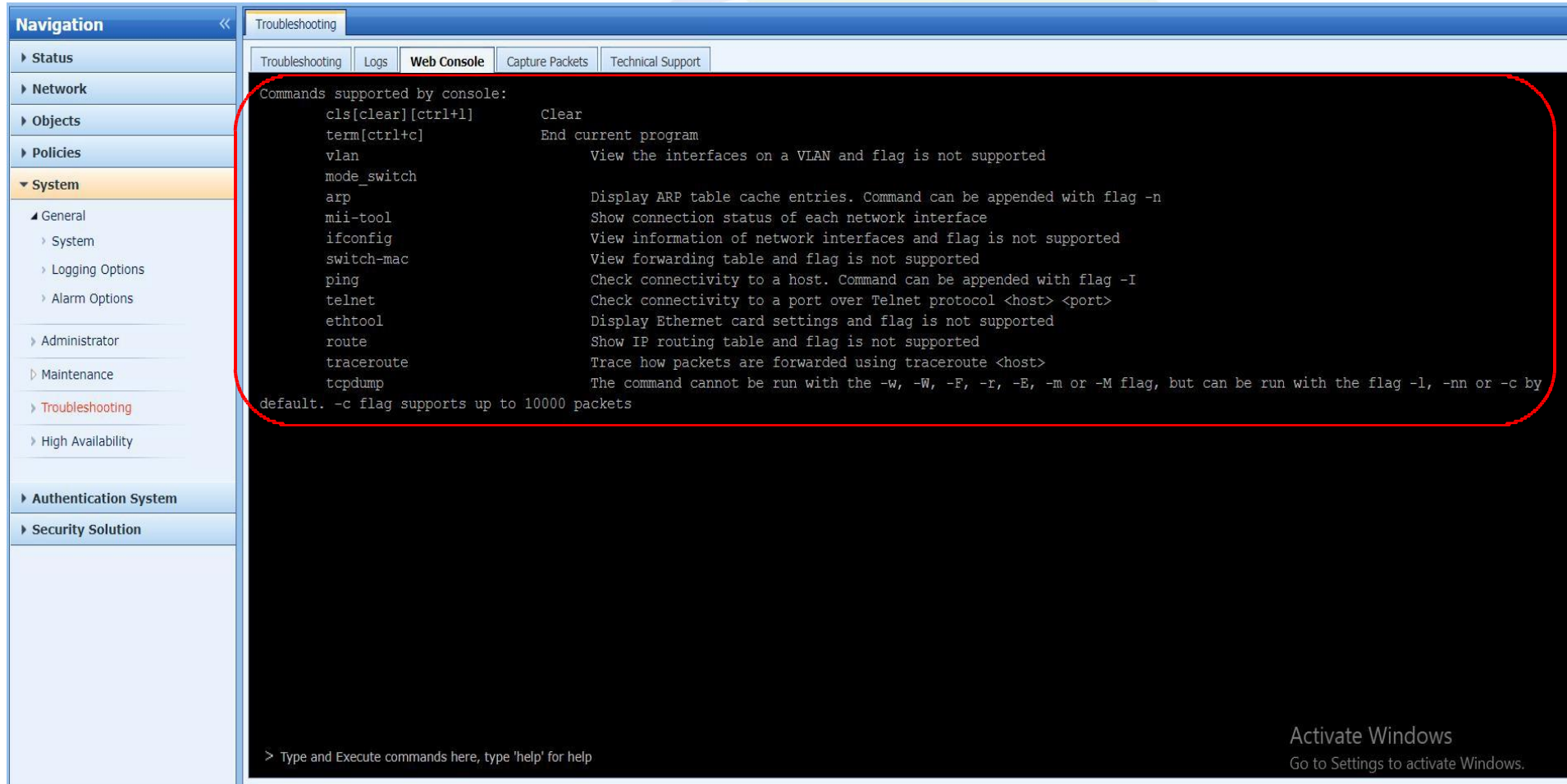
A 'Message' dialog box is overlaid on the table. It contains the following text:

- Data packets on layer 2 will pass through after L2 debugging pass-through starts.
- Please make sure:
- 1. You are Sangfor technical support representative
- 2. You are troubleshooting network connection issues
- 3. High Availability(HA) is disabled

 At the bottom of the dialog is the question 'Are you sure you want to enable it?' with 'Yes' and 'No' buttons. A red speech bubble points to the dialog with the text 'bisa berakibat network interruption'.

Web Console

Web console juga menyediakan beberapa command untuk maintenance



The screenshot displays the SANGFOR Web Console interface. On the left is a navigation menu with categories like Status, Network, Objects, Policies, System (expanded), Authentication System, and Security Solution. The 'System' category is expanded, showing sub-items: General, System, Logging Options, Alarm Options, Administrator, Maintenance, Troubleshooting (highlighted), and High Availability. The main content area is titled 'Troubleshooting' and contains a 'Web Console' tab. Below the tab, a list of commands supported by the console is shown, each with a brief description. A red rounded rectangle highlights this list. At the bottom of the console area, there is a prompt '> Type and Execute commands here, type 'help' for help' and a Windows activation notice.

Commands supported by console:

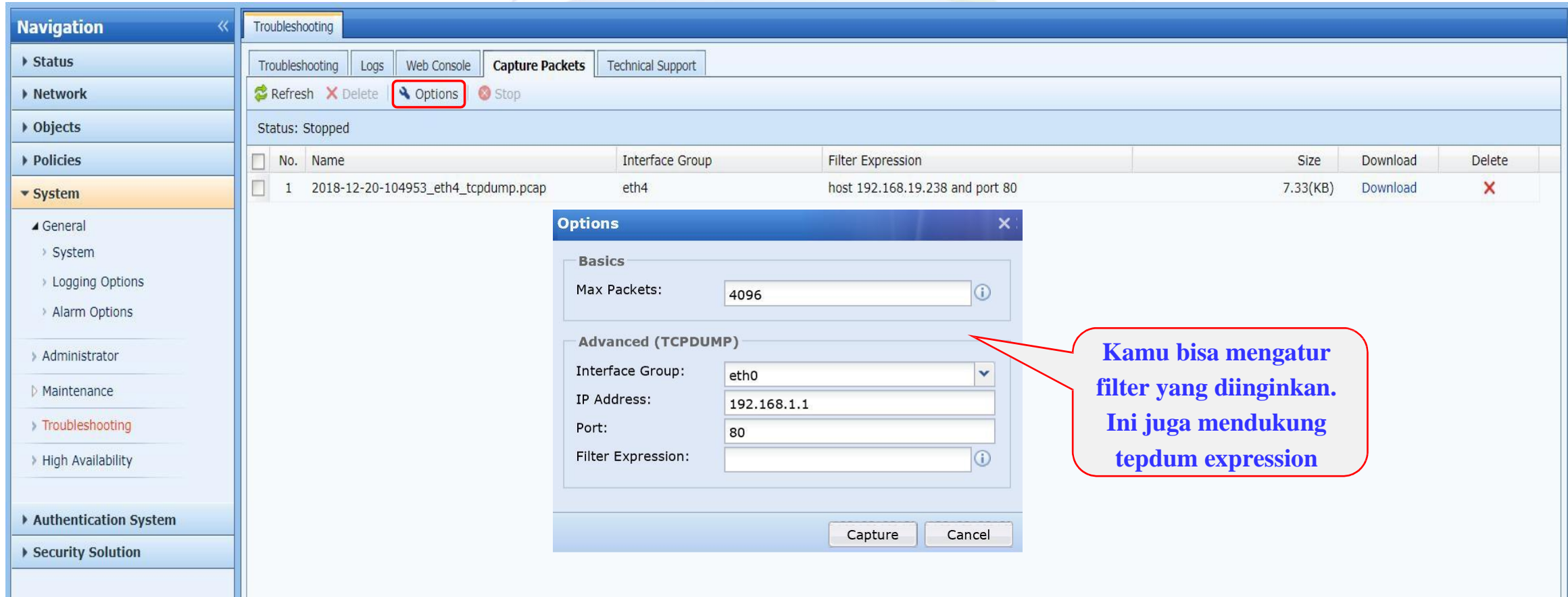
| Command | Description |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cls[clear][ctrl+l] | Clear |
| term[ctrl+c] | End current program |
| vlan | View the interfaces on a VLAN and flag is not supported |
| mode_switch | |
| arp | Display ARP table cache entries. Command can be appended with flag -n |
| mii-tool | Show connection status of each network interface |
| ifconfig | View information of network interfaces and flag is not supported |
| switch-mac | View forwarding table and flag is not supported |
| ping | Check connectivity to a host. Command can be appended with flag -I |
| telnet | Check connectivity to a port over Telnet protocol <host> <port> |
| ethtool | Display Ethernet card settings and flag is not supported |
| route | Show IP routing table and flag is not supported |
| tracert | Trace how packets are forwarded using traceroute <host> |
| tcpdump | The command cannot be run with the -w, -W, -F, -r, -E, -m or -M flag, but can be run with the flag -l, -nn or -c by default. -c flag supports up to 10000 packets |

> Type and Execute commands here, type 'help' for help

Activate Windows
Go to Settings to activate Windows.

Capture Packets

tcpdump pada Web Console digunakan untuk menganalisa beberapa packet yang gampang, untuk beberapa packets yang kompleks kamu bisa menyimpan di local dan menganalisa dengan Wireshark.



The screenshot displays the Sangfor Web Console interface for packet capture. The left sidebar shows the navigation menu with 'System' expanded. The main area shows the 'Capture Packets' tab with a table of active captures. One capture is listed with ID 1, name '2018-12-20-104953_eth4_tcpdump.pcap', interface 'eth4', and filter 'host 192.168.19.238 and port 80'. The 'Options' dialog box is open, showing the 'Advanced (TCPDUMP)' section with fields for Interface Group (eth0), IP Address (192.168.1.1), Port (80), and Filter Expression. A red callout bubble points to the Filter Expression field with the text: "Kamu bisa mengatur filter yang diinginkan. Ini juga mendukung tcpdump expression".

| No. | Name | Interface Group | Filter Expression | Size | Download | Delete |
|-----|-------------------------------------|-----------------|---------------------------------|----------|----------|--------|
| 1 | 2018-12-20-104953_eth4_tcpdump.pcap | eth4 | host 192.168.19.238 and port 80 | 7.33(KB) | Download | X |

Options

Basics

Max Packets: 4096

Advanced (TCPDUMP)

Interface Group: eth0

IP Address: 192.168.1.1

Port: 80

Filter Expression:

Capture Cancel

System logs



Log sistem digunakan untuk menganalisa beberapa NGAF yang error ataupun untuk mendapatkan beberapa informasi dari log yang sedang berjalan.

Navigation

► Status

► Network

► Objects

► Policies

▼ System

▲ General

► System

► Logging Options

► Alarm Options

► Administrator

► Maintenance

► Troubleshooting

► High Availability

► Authentication System

► Security Solution

Troubleshooting

TroubleshootingLogsWeb ConsoleCapture PacketsTechnical Support

Options

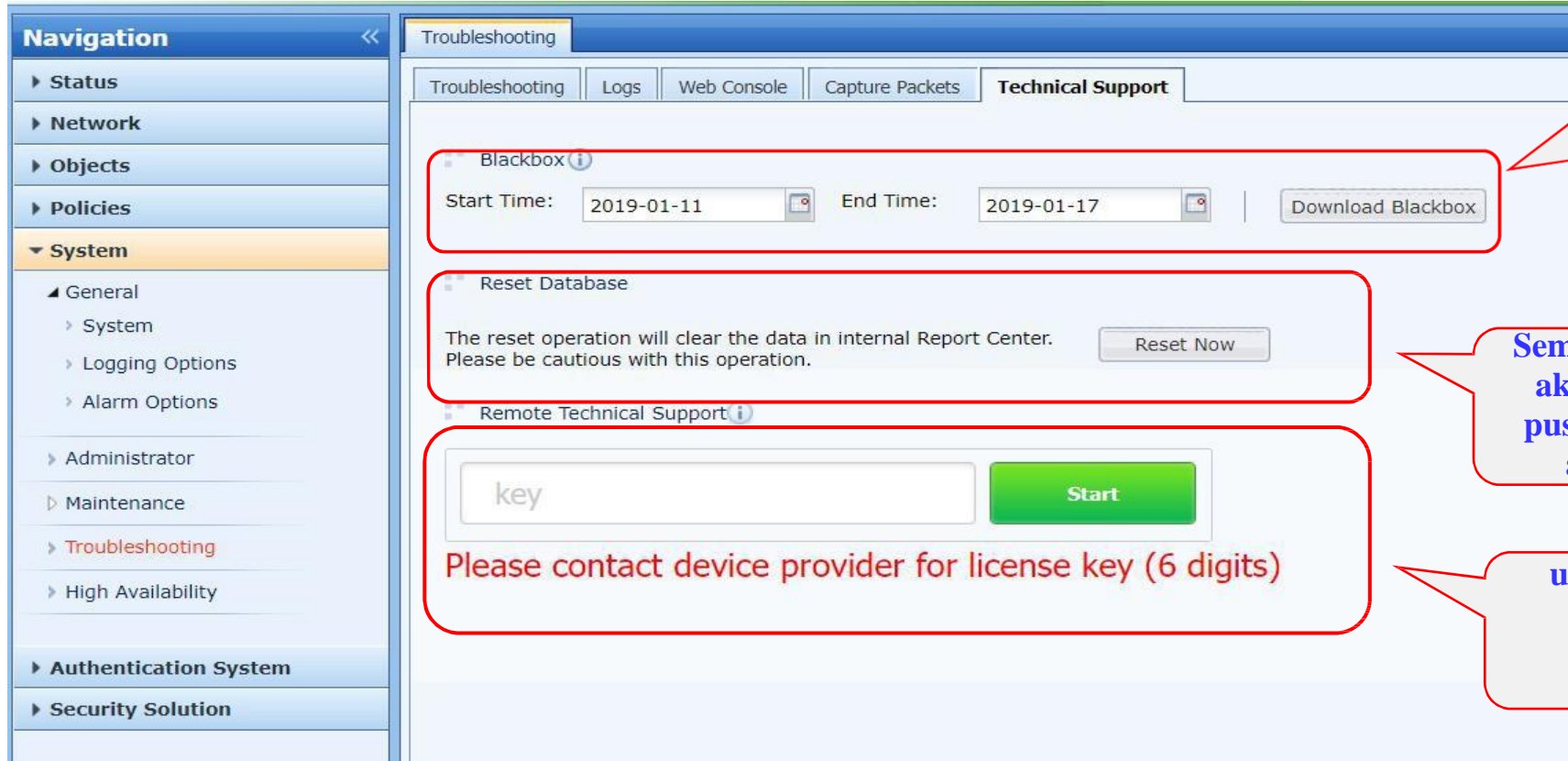
Date: 2019-01-17

| No. | Module | Type | Time | Details |
|-----|---------------------------|---------|----------|-----------------------------------------------------------------------------------------------------------|
| 1 | VPN Service | Info | 09:36:58 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 2 | VPN Service | Warning | 09:36:57 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 3 | VPN Service | Info | 09:35:57 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 4 | VPN Service | Warning | 09:35:55 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 5 | VPN Service | Info | 09:34:56 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 6 | VPN Service | Warning | 09:34:51 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 7 | VPN Service | Info | 09:33:54 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 8 | VPN Service | Warning | 09:33:53 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 9 | Intermediate Report Ge... | Info | 09:33:32 | i0:Midtable.cpp:987 CheckAllDate for /fwlog/log_data/fwlog |
| 10 | VPN Service | Info | 09:32:53 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 11 | VPN Service | Warning | 09:32:51 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 12 | VPN Service | Info | 09:31:52 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 13 | VPN Service | Warning | 09:31:52 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 14 | VPN Service | Info | 09:30:51 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 15 | VPN Service | Warning | 09:30:49 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 16 | VPN Service | Info | 09:29:50 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 17 | VPN Service | Warning | 09:29:48 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 18 | VPN Service | Info | 09:28:49 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 19 | VPN Service | Warning | 09:28:48 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 20 | VPN Service | Info | 09:27:48 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 21 | VPN Service | Warning | 09:27:45 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 22 | VPN Service | Info | 09:26:46 | [Isakmp_Server]Start to initiate negotiation with [test](IP:192.168.19.215) using main mode! |
| 23 | VPN Service | Warning | 09:26:46 | [Isakmp_Server]Negotiating with [test]'s Phase 1 security association failed. Failed to build connection! |
| 24 | Access Log System | Info | 09:26:46 | i0:CfqTableUpdate.cpp:2577 update table CfqServAppCrc, CfqCrcName ok. |

Page 1 of 27Entries Per Page: 50

Activate WindowsGo to Settings to activate Wind150 of 1307

Perangkat Technical Support Lainnya



The screenshot shows the Sangfor Technical Support interface. On the left is a navigation menu with categories: Status, Network, Objects, Policies, System (expanded), Authentication System, and Security Solution. The 'System' category is expanded, showing sub-items: General, System, Logging Options, Alarm Options, Administrator, Maintenance, Troubleshooting (highlighted), and High Availability. The main content area has tabs for Troubleshooting, Logs, Web Console, Capture Packets, and Technical Support (selected). Under the 'Technical Support' tab, there are three sections: 1. 'Blackbox' with a date range from 2019-01-11 to 2019-01-17 and a 'Download Blackbox' button. 2. 'Reset Database' with a warning message and a 'Reset Now' button. 3. 'Remote Technical Support' with a text input field containing 'key', a green 'Start' button, and a red instruction: 'Please contact device provider for license key (6 digits)'.

Blackbox logs digunakan pada Sangfor Technical Support untuk menganalisa beberapa masalah historis

Semua logs pada pusat data akan dihapus, umumnya pusat data akan di-restore apabila terjadi error

untuk sementara, remote support belum bisa digunakan

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)

