

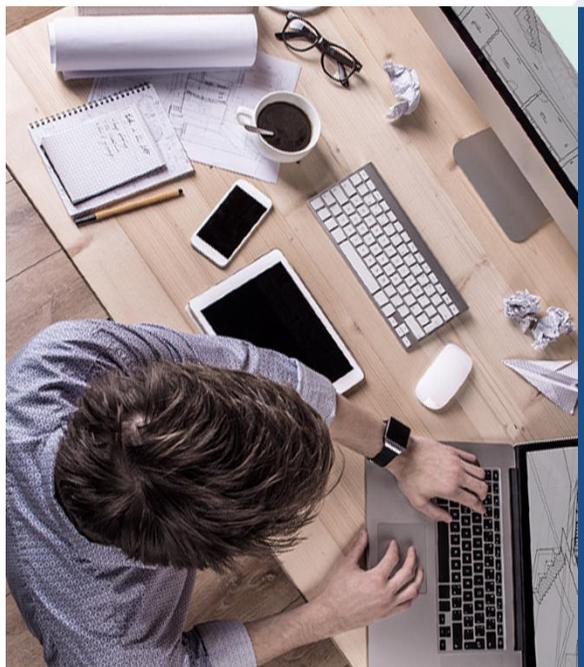


SANGFOR

Sangfor NGAF v8.0.6 Associate

Pengaturan Sistem





1 Lisensi

2 Databases Update

3 Backup/Restore

4 Global Whitelist/Blacklist

5 Troubleshooting

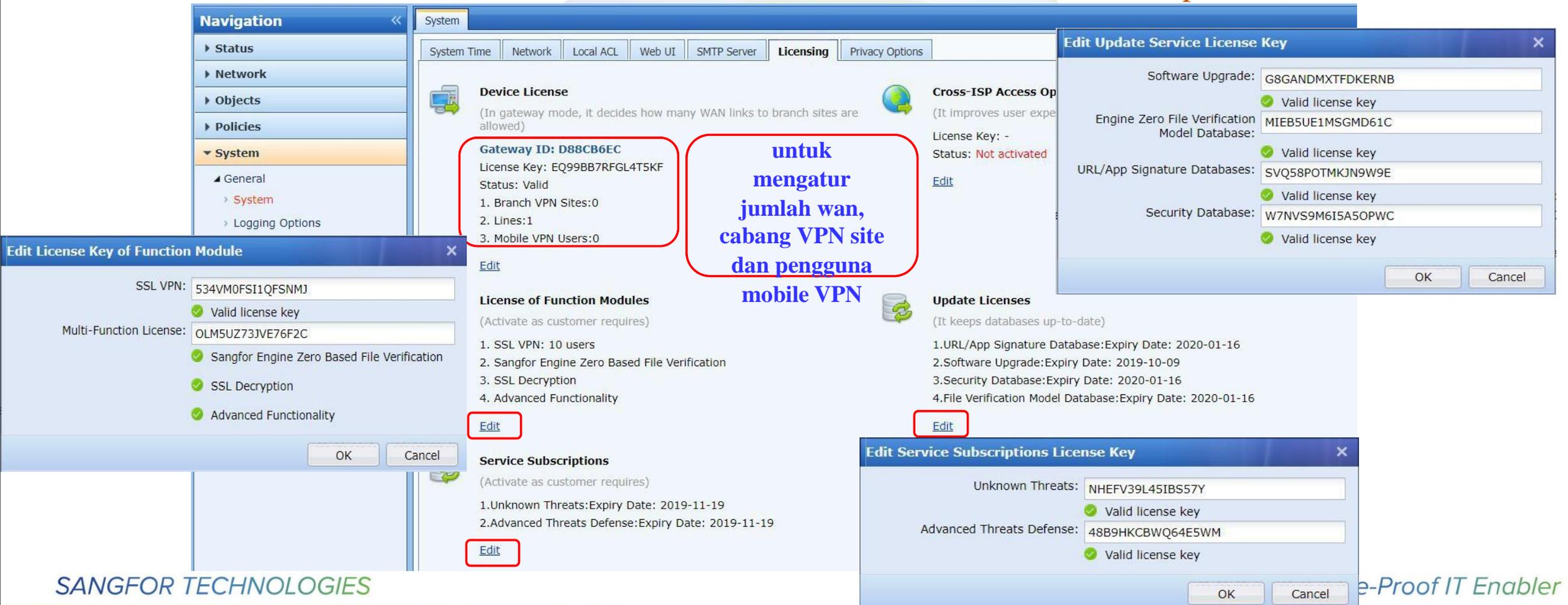
1. Lisensi



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 configuration windows open:

- Navigation Panel:** Shows system configuration options like Status, Network, Objects, Policies, and System (General, System, Logging Options).
- System Time Tab:** Contains sections for Device License, Cross-ISP Access Op, License of Function Modules, Service Subscriptions, and Update Licenses.
- Device License:** Shows Gateway ID: D88CB6EC, License Key: EQ99BB7RFGL4T5KF, Status: Valid, and lists 0 Branch VPN Sites, 1 Line, and 0 Mobile VPN Users. A red box highlights this section.
- License of Function Modules:** Lists SSL VPN (10 users), Sangfor Engine Zero Based File Verification, SSL Decryption, and Advanced Functionality. A red box highlights the Edit button.
- Service Subscriptions:** Lists Unknown Threats (Expiry Date: 2019-11-19) and Advanced Threats Defense (Expiry Date: 2019-11-19). A red box highlights the Edit button.
- Update Licenses:** Lists various databases with expiry dates: URL/App Signature Database (2020-01-16), Software Upgrade (2019-10-09), Security Database (2020-01-16), and File Verification Model Database (2020-01-16). A red box highlights the Edit button.
- Edit Update Service License Key:** Shows fields for Software Upgrade, Engine Zero File Verification, Model Database, URL/App Signature Databases, and Security Database, all with valid license keys.
- Edit License Key of Function Module:** Shows fields for SSL VPN and Multi-Function License, both with valid license keys.
- Edit Service Subscriptions License Key:** Shows fields for Unknown Threats and Advanced Threats Defense, both with valid license keys.

Central Text Box: **untuk mengatur jumlah wan, cabang VPN site dan pengguna mobile VPN**

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](#)

Database Update

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

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

Setiap database bergantung kepada lisensi yang mengatur kapabilitas database tersebut

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

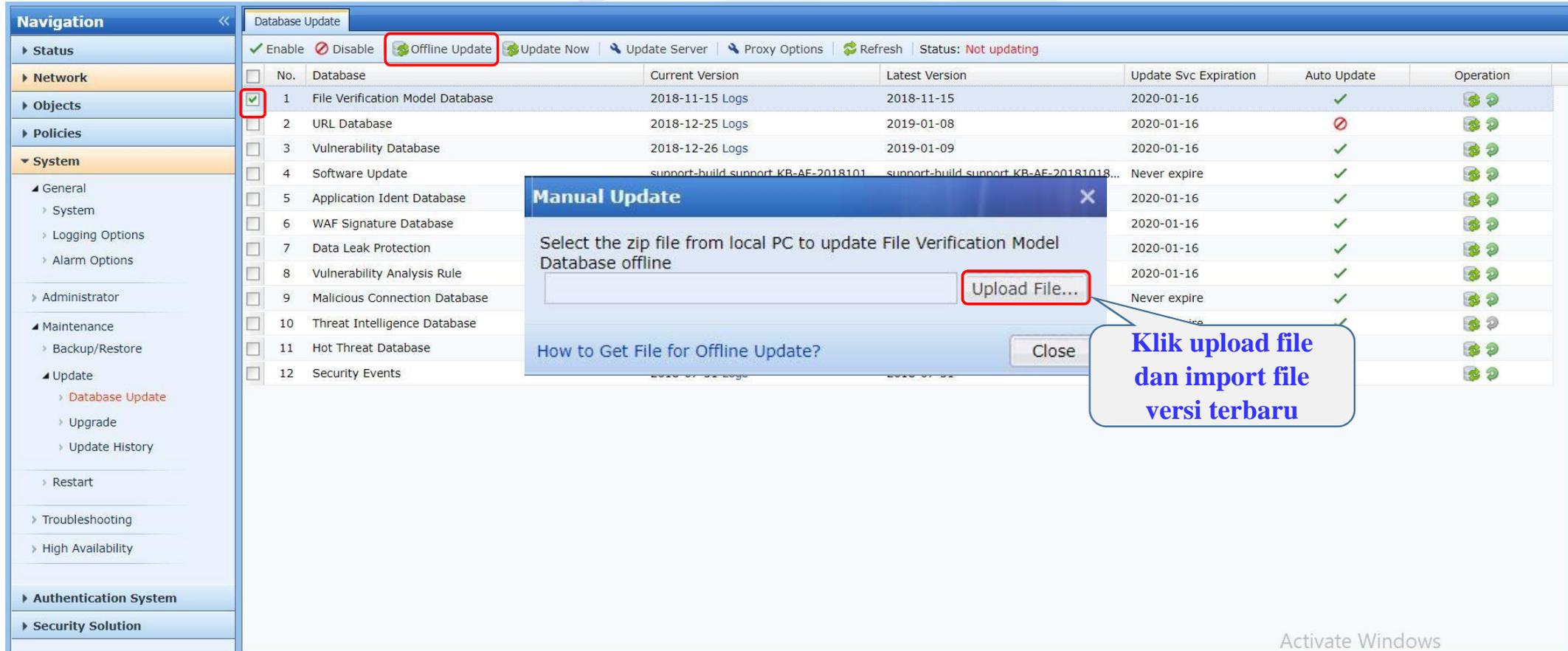
Kita bisa mendapatkan library dan meng-import kedalam perangkat secara manual sebelum layanan update sudah tidak valid(expired)

(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



Navigation

Database Update

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

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

Manual Update

Select the zip file from local PC to update File Verification Model Database offline

Upload File...

Close

How to Get File for Offline Update?

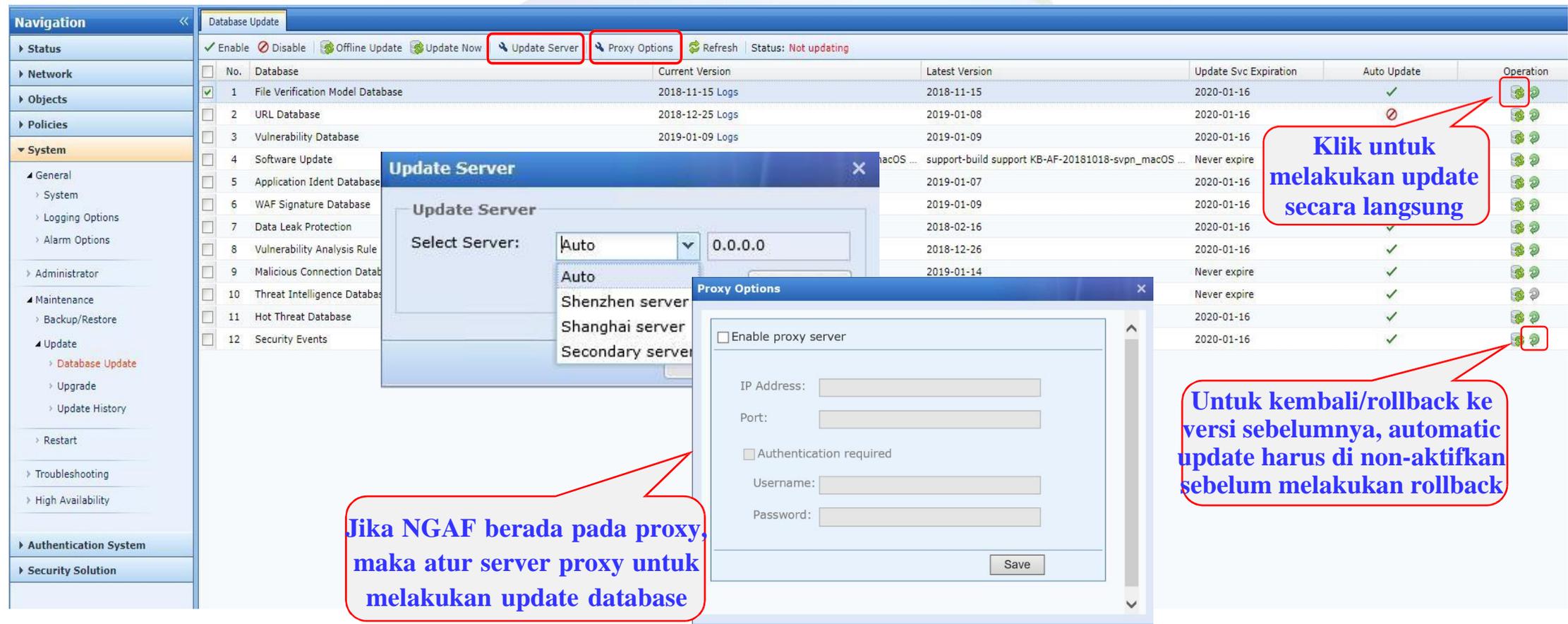
Klik upload file dan import file versi terbaru

Activate Windows

Databases update

Auto update

NGAF akan melakukan update database setiap pagi.



The screenshot shows the 'Database Update' configuration page in the NGAF management console. The page includes a navigation sidebar on the left and a main content area with a table of databases and their update settings. Two modal windows are open: 'Update Server' and 'Proxy Options'.

Annotations:

- Update Server:** A red box highlights the 'Update Server' button in the top toolbar.
- Proxy Options:** A red box highlights the 'Proxy Options' button in the top toolbar.
- Update Server Modal:** A red box highlights the 'Auto' dropdown menu in the 'Select Server' field.
- Proxy Options Modal:** A red box highlights the 'Enable proxy server' checkbox.
- Operation Column:** A red box highlights the 'Operation' column header in the table.
- Refresh Button:** A red box highlights the 'Refresh' button in the top toolbar.

Table Data:

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	2019-01-09 Logs	2019-01-09	2020-01-16	✓	⊕ ⊖
4	Software Update	macOS ... support-build support KB-AF-20181018-svprn_macOS ...	Never expire	2020-01-16	✓	⊕ ⊖
5	Application Ident Database	2019-01-07	2020-01-16	2020-01-16	✓	⊕ ⊖
6	WAF Signature Database	2019-01-09	2020-01-16	2020-01-16	✓	⊕ ⊖
7	Data Leak Protection	2018-02-16	2020-01-16	2020-01-16	✓	⊕ ⊖
8	Vulnerability Analysis Rule	2018-12-26	2020-01-16	2020-01-16	✓	⊕ ⊖
9	Malicious Connection Databa	2019-01-14	Never expire	Never expire	✓	⊕ ⊖
10	Threat Intelligence Databas		Never expire	Never expire	✓	⊕ ⊖
11	Hot Threat Database		2020-01-16	2020-01-16	✓	⊕ ⊖
12	Security Events		2020-01-16	2020-01-16	✓	⊕ ⊖

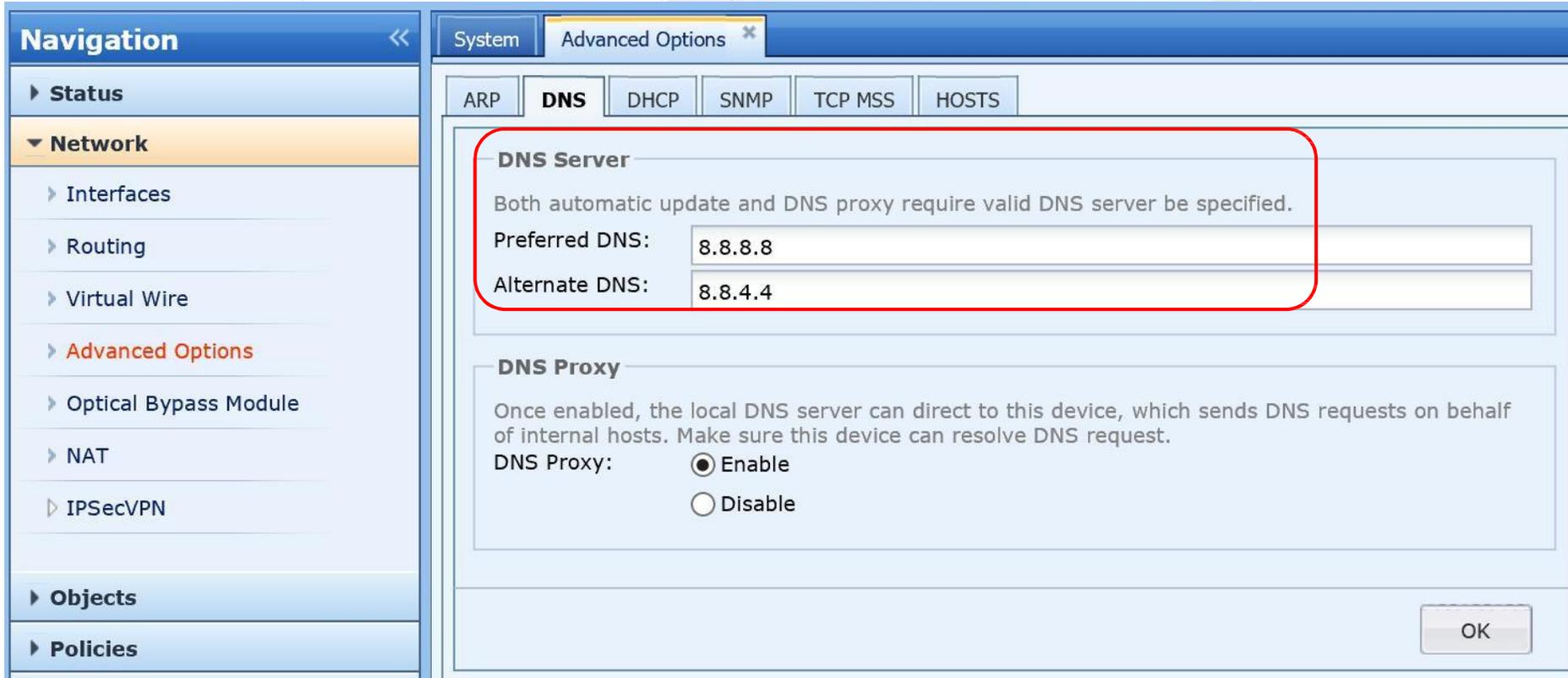
Jika NGAF berada pada proxy, maka atur server proxy untuk melakukan update database

Klik untuk melakukan update secara langsung

Untuk kembali/rollback ke versi sebelumnya, automatic update harus di non-aktifkan sebelum melakukan rollback

Databases update

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



The screenshot displays the 'Advanced Options' configuration page for the 'System' tab. The 'DNS' sub-tab is selected, showing the 'DNS Server' and 'DNS Proxy' sections. The 'DNS Server' section is highlighted with a red box and contains the following text: 'Both automatic update and DNS proxy require valid DNS server be specified.' Below this text are two input fields: 'Preferred DNS' with the value '8.8.8.8' and 'Alternate DNS' with the value '8.8.4.4'. The 'DNS Proxy' section is below and includes a radio button for 'Enable' (which is selected) and a radio button for 'Disable'. An 'OK' button is located at the bottom right of the configuration area.

Navigation

- ▶ Status
- ▼ Network
 - ▶ Interfaces
 - ▶ Routing
 - ▶ Virtual Wire
 - ▶ **Advanced Options**
 - ▶ Optical Bypass Module
 - ▶ NAT
 - ▶ IPSecVPN
- ▶ Objects
- ▶ Policies

System | **Advanced Options**

ARP | **DNS** | DHCP | SNMP | TCP MSS | HOSTS

DNS Server

Both automatic update and DNS proxy require valid DNS server be specified.

Preferred DNS: 8.8.8.8

Alternate DNS: 8.8.4.4

DNS Proxy

Once enabled, the local DNS server can direct to this device, which sends DNS requests on behalf of internal hosts. Make sure this device can resolve DNS request.

DNS Proxy: Enable Disable

OK

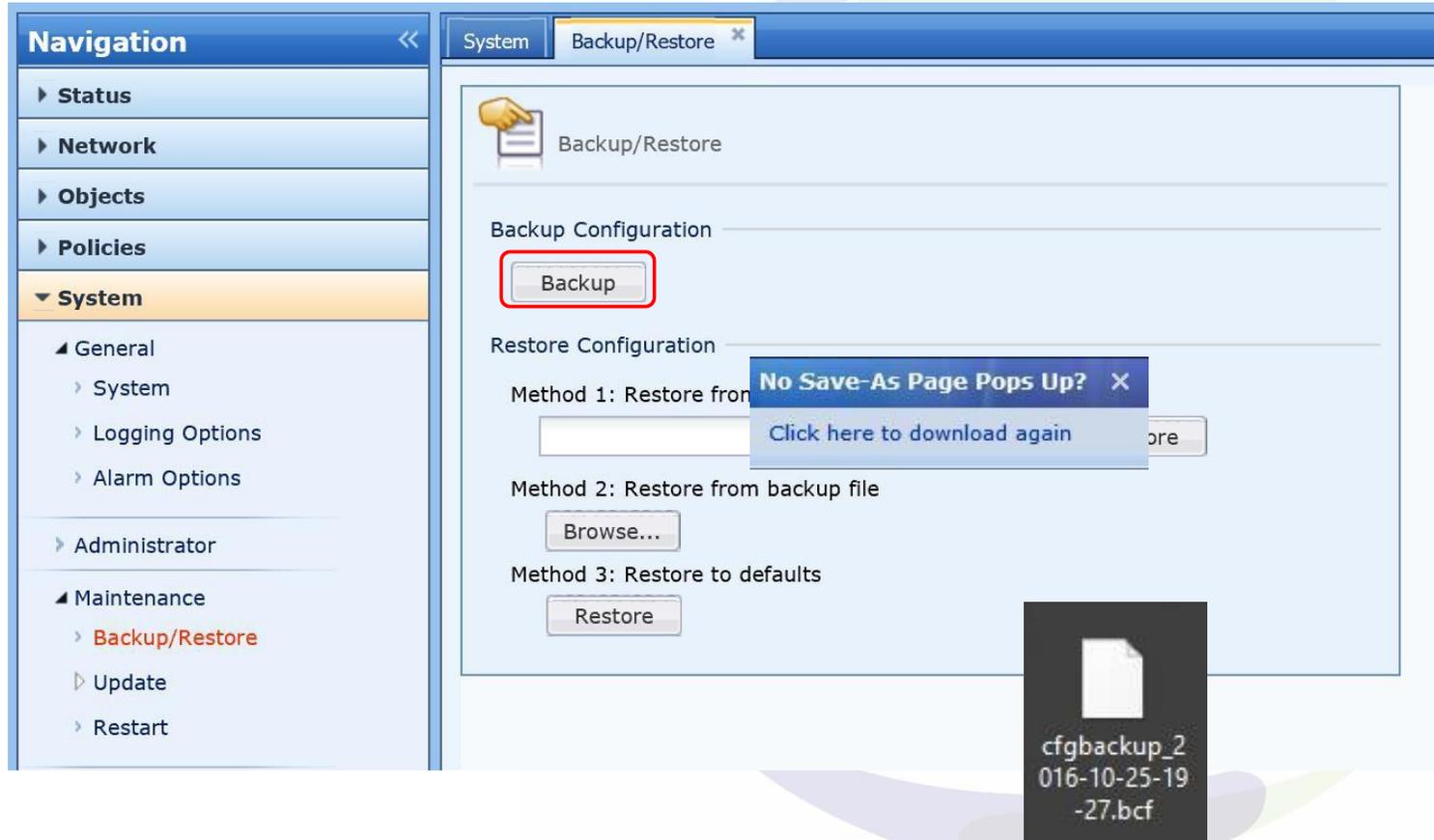
3. Backup/Restore



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 x

Backup/Restore

Backup Configuration

Backup

Restore Configuration

Method 1: Restore from [input field] Restore

Method 2: Restore from backup file

Browse...

Method 3: Restore to defaults

Restore

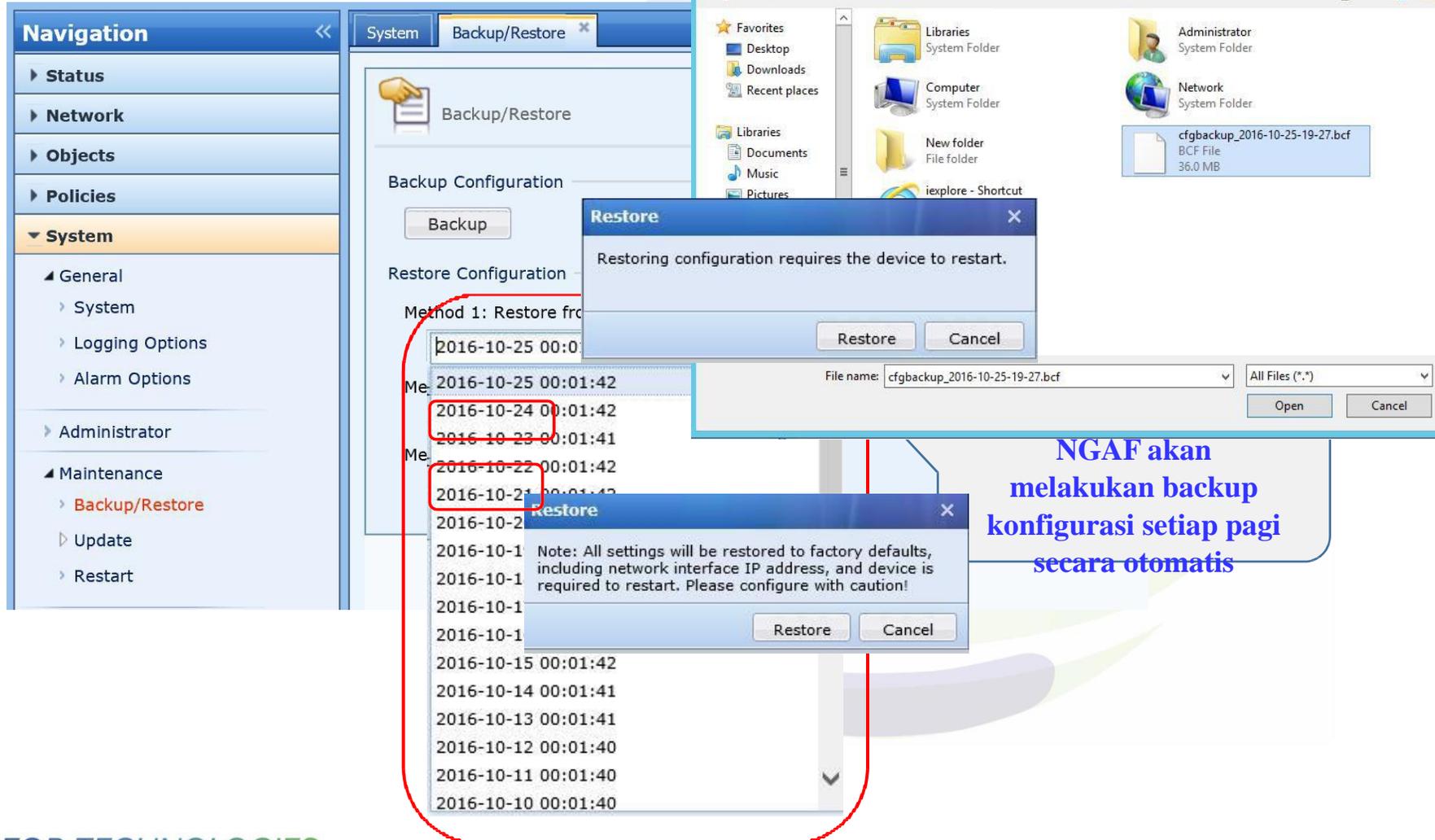
No Save-As Page Pops Up? X

Click here to download again

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

Backup/Restore

Konfigurasi Restore



The screenshot displays the NGAF Backup/Restore configuration interface. The left sidebar shows the 'System' menu with 'Backup/Restore' selected. The main area shows the 'Backup/Restore' configuration page with a list of backup files. A 'Restore' dialog box is open, displaying the message: "Restoring configuration requires the device to restart." Below the dialog, a list of backup files is shown, with the file name "cfgbackup_2016-10-25-19-27.bcf" highlighted. A red circle highlights the file name in the list. A blue callout box with a white background and a blue border contains the text: "NGAF akan melakukan backup konfigurasi setiap pagi secara otomatis".

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

2016-10-25 00:01:42

Me 2016-10-25 00:01:42

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

Restore

Restoring configuration requires the device to restart.

Restore Cancel

File name: cfgbackup_2016-10-25-19-27.bcf All Files (*.*)

Open Cancel

NGAF akan melakukan backup konfigurasi setiap pagi secara otomatis

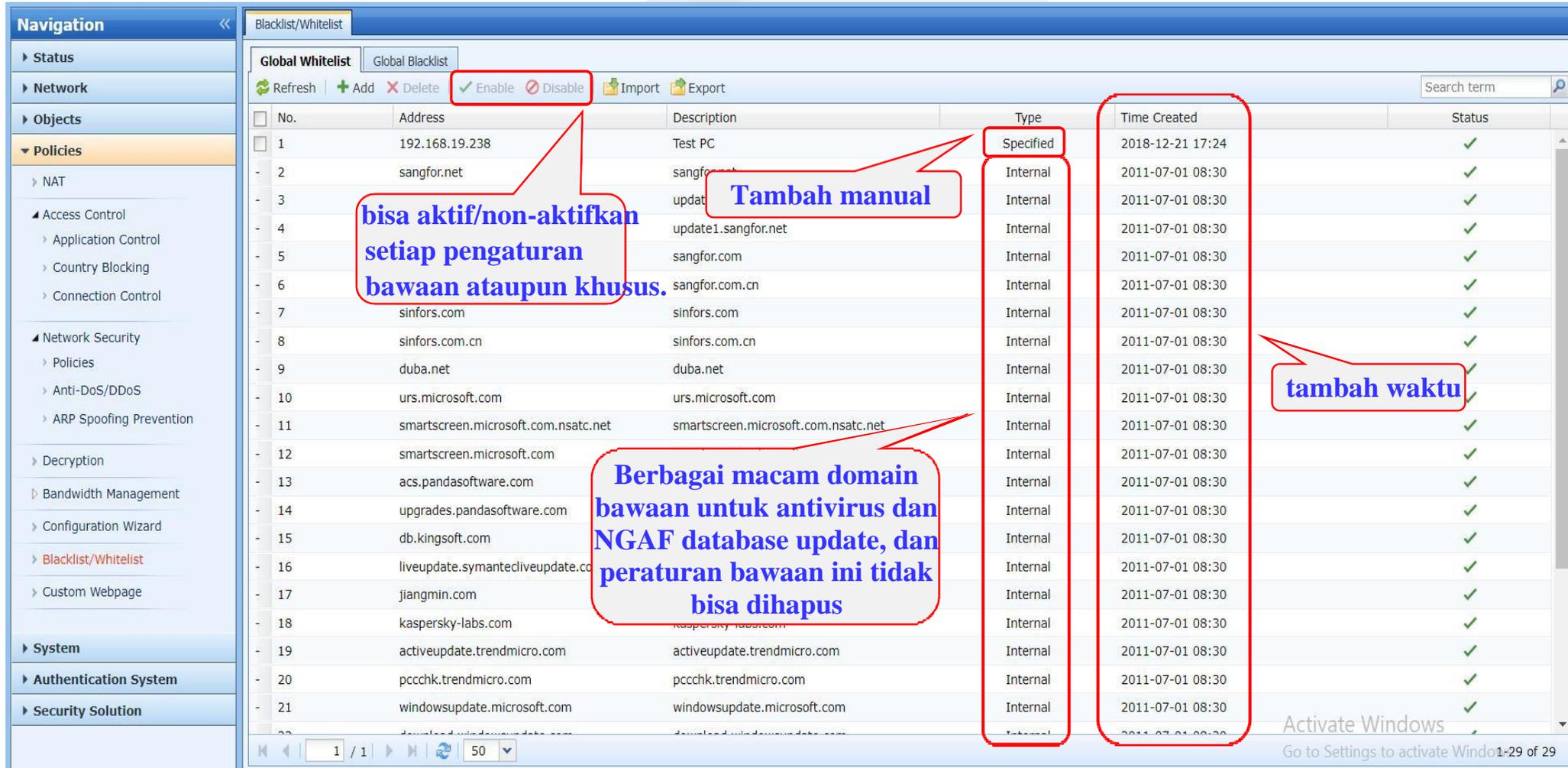
4. Global Whitelist/Blacklist



SANGFOR
深信服科技

Global Whitelist/Blacklist

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

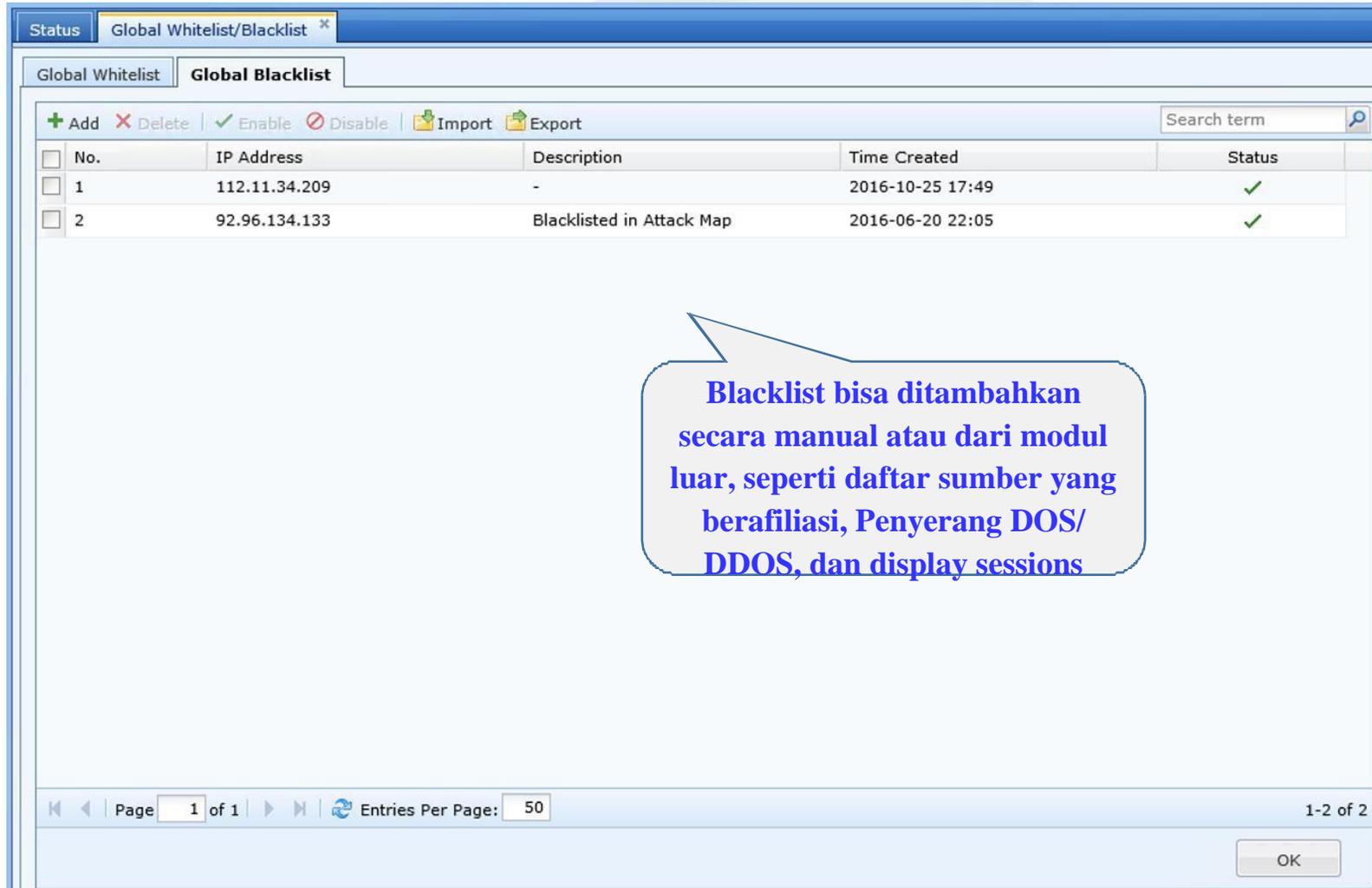


The screenshot shows the 'Global Whitelist' configuration page in the Sangfor NGAF management console. The interface includes a navigation sidebar on the left, a top toolbar with actions like 'Refresh', 'Add', 'Delete', 'Enable', 'Disable', 'Import', and 'Export', and a main table listing whitelisted items. The table columns are: No., Address, Description, Type, Time Created, and Status. Annotations in blue text boxes highlight specific features: 'bisa aktif/non-aktifkan setiap pengaturan bawaan ataupun khusus.' points to the 'Enable' and 'Disable' buttons; 'Tambah manual' points to the 'Add' button; 'Berbagai macam domain bawaan untuk antivirus dan NGAF database update, dan peraturan bawaan ini tidak bisa dihapus' points to the list of domains; and 'tambah waktu' points to the 'Time Created' column.

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	✓

Global Whitelist/Blacklist

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



Global Whitelist/Blacklist

Global Whitelist Global Blacklist

+ Add X 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.

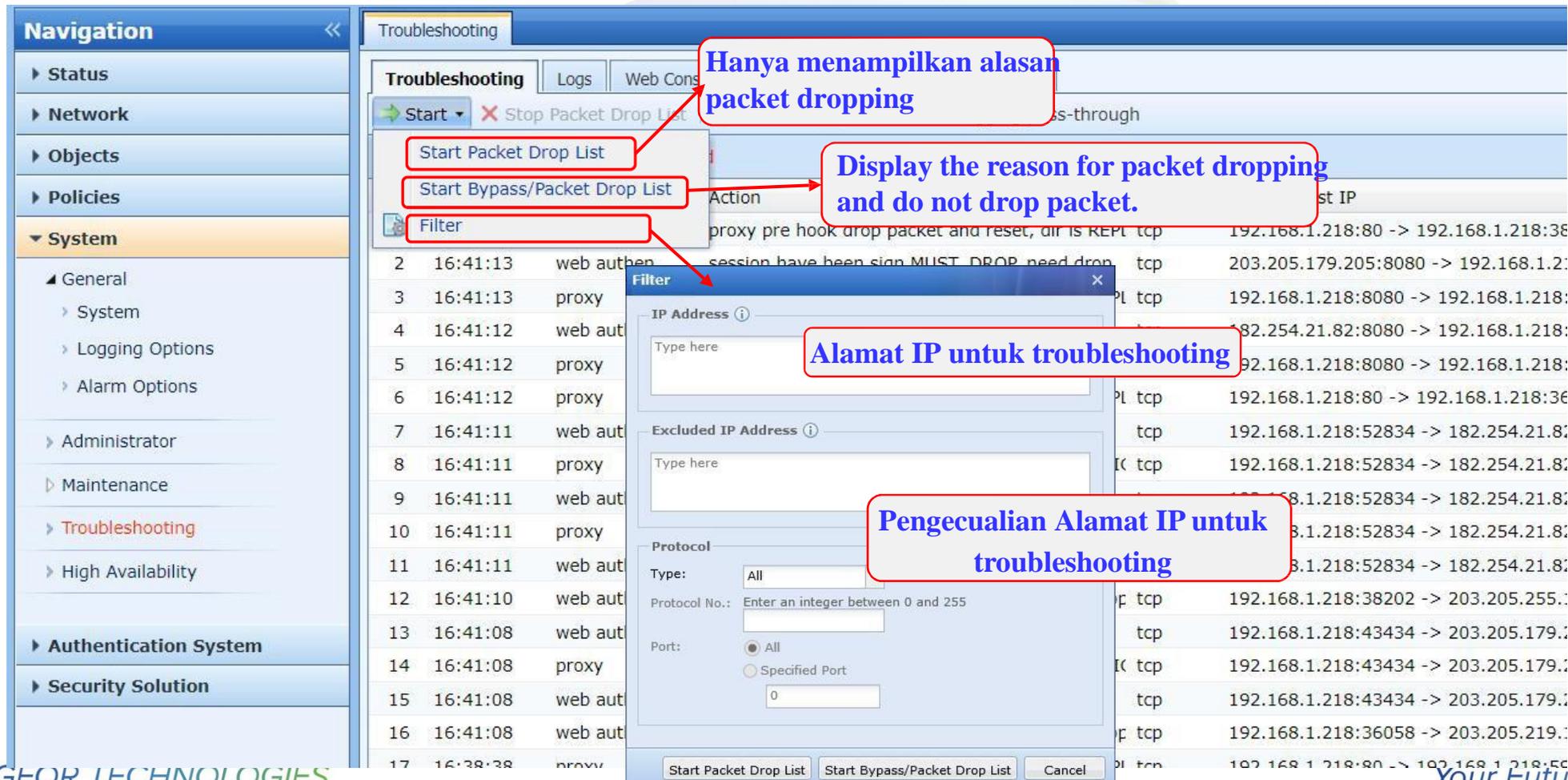
5. Troubleshooting



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 displays the Sangfor firewall management interface. On the left is a navigation menu with categories like Status, Network, Objects, Policies, and System. The main area is titled 'Troubleshooting' and contains a table of logs. A 'Filter' dialog box is open, allowing configuration of IP addresses and protocols for troubleshooting. Red callout boxes with blue text provide instructions on how to use the interface.

Hanya menampilkan alasan packet dropping

Display the reason for packet dropping and do not drop packet.

Alamat IP untuk troubleshooting

Pengecualian Alamat IP untuk troubleshooting

No.	Time	Action	Source IP	Destination IP	Protocol
2	16:41:13	web authentication	192.168.1.218:80	192.168.1.218:36058	tcp
3	16:41:13	proxy	203.205.179.205:8080	192.168.1.218:8080	tcp
4	16:41:12	web authentication	182.254.21.82:8080	192.168.1.218:8080	tcp
5	16:41:12	proxy	192.168.1.218:8080	192.168.1.218:8080	tcp
6	16:41:12	proxy	192.168.1.218:80	192.168.1.218:36058	tcp
7	16:41:11	web authentication	192.168.1.218:52834	182.254.21.82:8080	tcp
8	16:41:11	proxy	192.168.1.218:52834	182.254.21.82:8080	tcp
9	16:41:11	web authentication	182.254.21.82:8080	192.168.1.218:52834	tcp
10	16:41:11	proxy	182.254.21.82:8080	192.168.1.218:52834	tcp
11	16:41:11	web authentication	192.168.1.218:52834	182.254.21.82:8080	tcp
12	16:41:10	web authentication	192.168.1.218:38202	203.205.255.100:8080	tcp
13	16:41:08	web authentication	192.168.1.218:43434	203.205.179.100:8080	tcp
14	16:41:08	proxy	192.168.1.218:43434	203.205.179.100:8080	tcp
15	16:41:08	web authentication	192.168.1.218:43434	203.205.179.100:8080	tcp
16	16:41:08	web authentication	192.168.1.218:36058	203.205.219.100:8080	tcp
17	16:38:38	proxy	192.168.1.218:80	192.168.1.218:36058	tcp

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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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 have 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

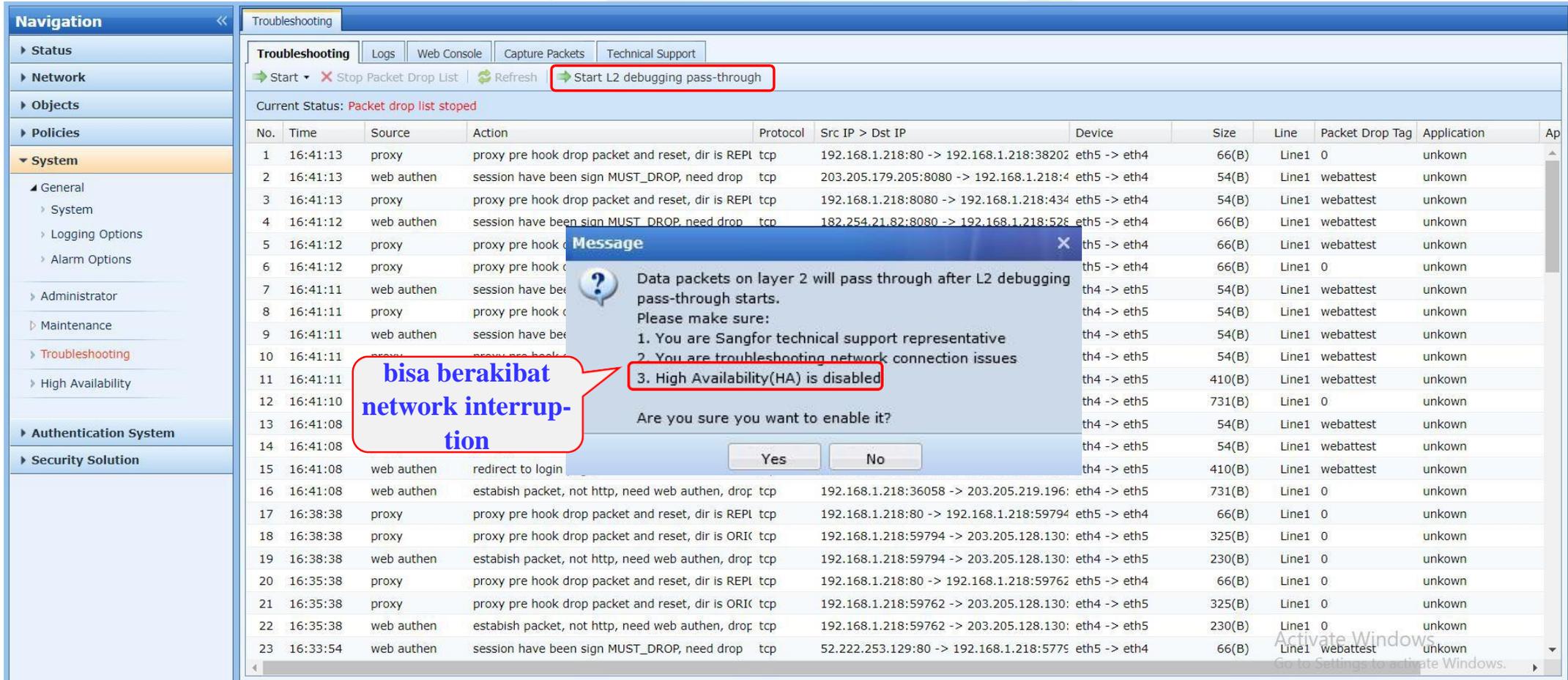
ini di-blok oleh app control policy

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 'Troubleshooting' interface in the Sangfor management console. The 'Start L2 debugging pass-through' button is highlighted with a red box. A message dialog box is displayed in the foreground, containing the following text:

Message

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

Are you sure you want to enable it?

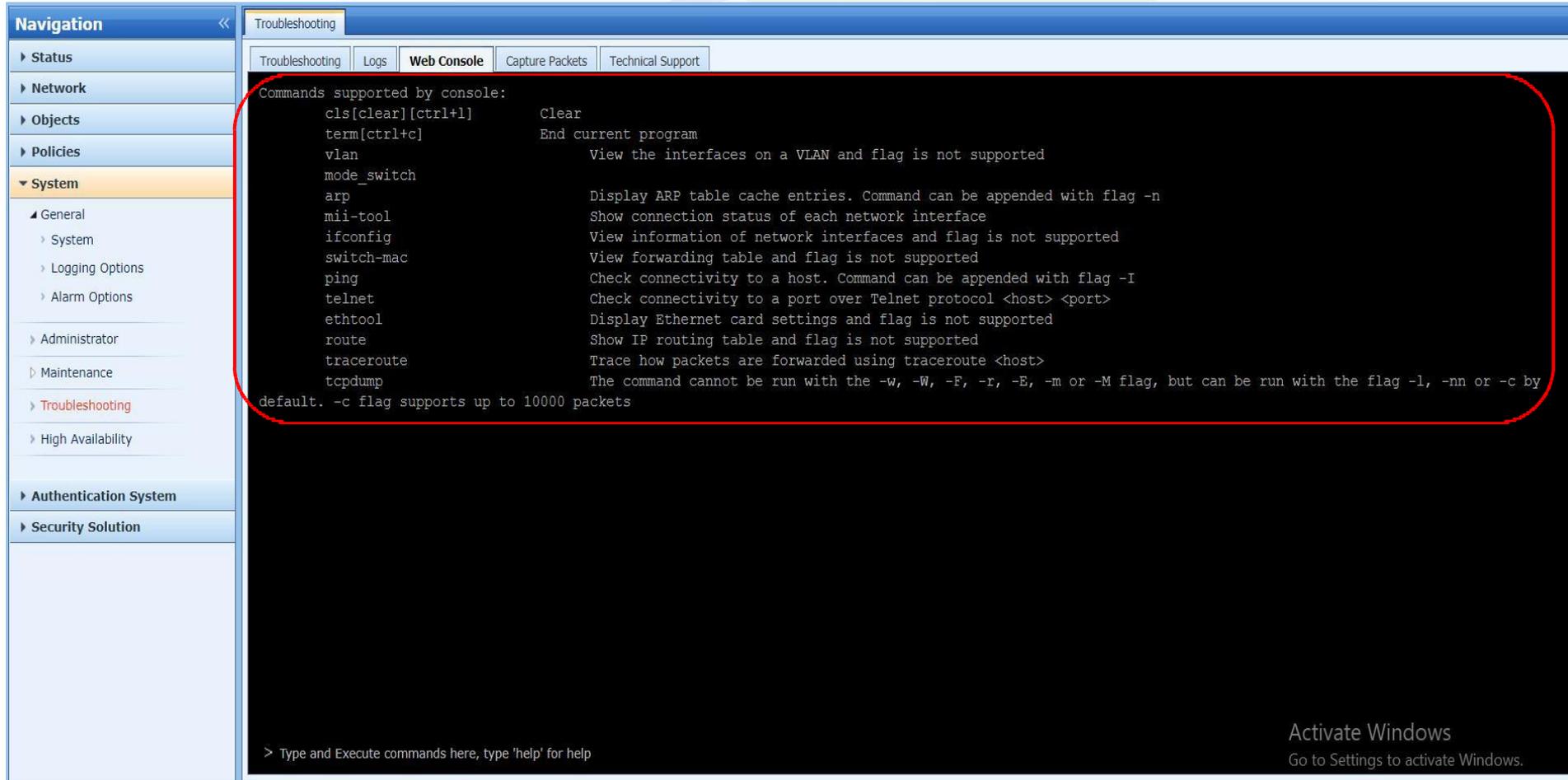
Yes No

A red callout bubble points to item 3 in the list, containing the text: **bisa berakibat network interruption**.

No.	Time	Source	Action	Protocol	Src IP > Dst IP	Device	Size	Line	Packet Drop Tag	Application	Ap
1	16:41:13	proxy	proxy pre hook drop packet and reset, dir is REPL	tcp	192.168.1.218:80 -> 192.168.1.218:38202	eth5 -> eth4	66(B)	Line1	0	unkown	
2	16:41:13	web authen	session have been sign MUST_DROP, need drop	tcp	203.205.179.205:8080 -> 192.168.1.218:4	eth5 -> eth4	54(B)	Line1	webatatest	unkown	
3	16:41:13	proxy	proxy pre hook drop packet and reset, dir is REPL	tcp	192.168.1.218:8080 -> 192.168.1.218:434	eth5 -> eth4	54(B)	Line1	webatatest	unkown	
4	16:41:12	web authen	session have been sign MUST_DROP, need drop	tcp	182.254.21.82:8080 -> 192.168.1.218:526	eth5 -> eth4	66(B)	Line1	webatatest	unkown	
5	16:41:12	proxy	proxy pre hook			eth5 -> eth4	66(B)	Line1	webatatest	unkown	
6	16:41:12	proxy	proxy pre hook			eth5 -> eth4	66(B)	Line1	0	unkown	
7	16:41:11	web authen	session have been			th4 -> eth5	54(B)	Line1	webatatest	unkown	
8	16:41:11	proxy	proxy pre hook			th4 -> eth5	54(B)	Line1	webatatest	unkown	
9	16:41:11	web authen	session have been			th4 -> eth5	54(B)	Line1	webatatest	unkown	
10	16:41:11	proxy	proxy pre hook			th4 -> eth5	54(B)	Line1	webatatest	unkown	
11	16:41:11	proxy	proxy pre hook			th4 -> eth5	54(B)	Line1	webatatest	unkown	
12	16:41:10	proxy	proxy pre hook			th4 -> eth5	410(B)	Line1	webatatest	unkown	
13	16:41:08	proxy	proxy pre hook			th4 -> eth5	731(B)	Line1	0	unkown	
14	16:41:08	proxy	proxy pre hook			th4 -> eth5	54(B)	Line1	webatatest	unkown	
15	16:41:08	web authen	redirect to login			th4 -> eth5	54(B)	Line1	webatatest	unkown	
16	16:41:08	web authen	establish packet, not http, need web authen, drop	tcp	192.168.1.218:36058 -> 203.205.219.196:	eth4 -> eth5	410(B)	Line1	webatatest	unkown	
17	16:38:38	proxy	proxy pre hook drop packet and reset, dir is REPL	tcp	192.168.1.218:80 -> 192.168.1.218:59794	eth5 -> eth4	731(B)	Line1	0	unkown	
18	16:38:38	proxy	proxy pre hook drop packet and reset, dir is ORIK	tcp	192.168.1.218:59794 -> 203.205.128.130:	eth4 -> eth5	66(B)	Line1	0	unkown	
19	16:38:38	web authen	establish packet, not http, need web authen, drop	tcp	192.168.1.218:59794 -> 203.205.128.130:	eth4 -> eth5	325(B)	Line1	0	unkown	
20	16:35:38	proxy	proxy pre hook drop packet and reset, dir is REPL	tcp	192.168.1.218:80 -> 192.168.1.218:59762	eth5 -> eth4	230(B)	Line1	0	unkown	
21	16:35:38	proxy	proxy pre hook drop packet and reset, dir is ORIK	tcp	192.168.1.218:59762 -> 203.205.128.130:	eth4 -> eth5	66(B)	Line1	0	unkown	
22	16:35:38	web authen	establish packet, not http, need web authen, drop	tcp	192.168.1.218:59762 -> 203.205.128.130:	eth4 -> eth5	325(B)	Line1	0	unkown	
23	16:33:54	web authen	session have been sign MUST_DROP, need drop	tcp	52.222.253.129:80 -> 192.168.1.218:5775	eth5 -> eth4	230(B)	Line1	0	unkown	

Web Console

Web console juga menyediakan beberapa command untuk maintenance

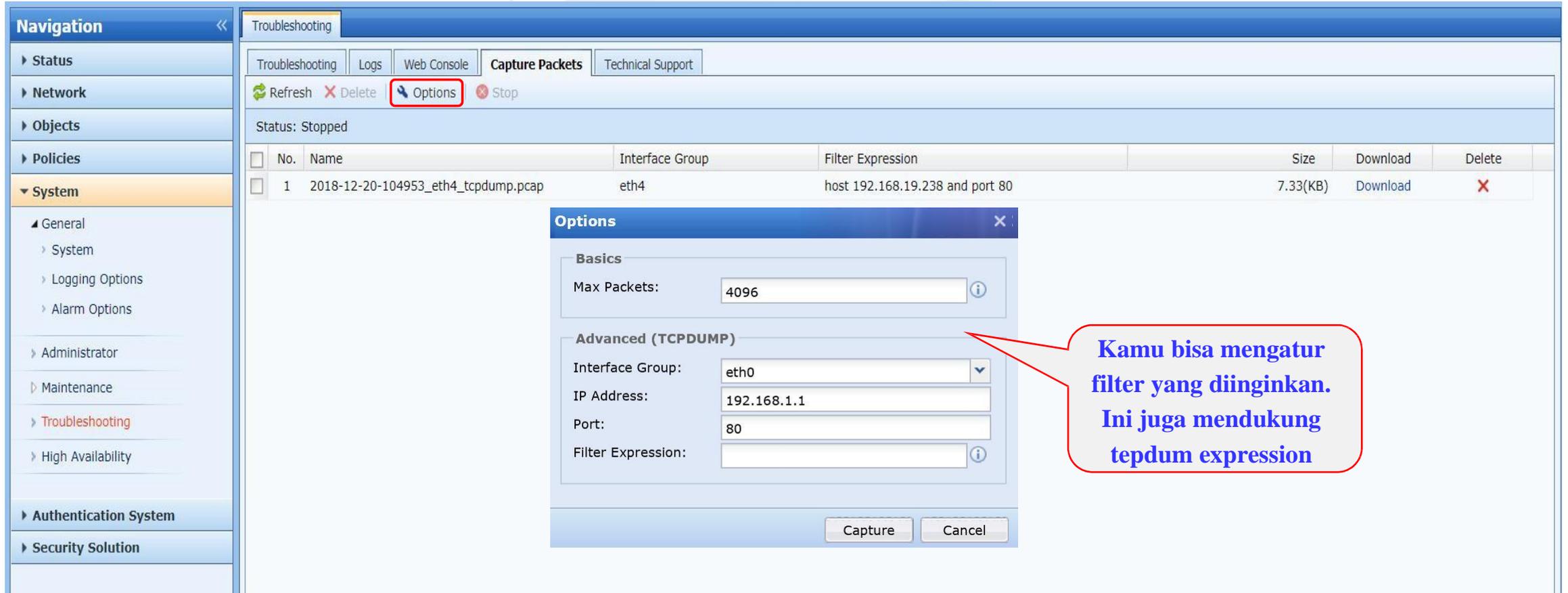


The screenshot displays the SANGFOR Web Console interface. On the left is a navigation menu with categories like Status, Network, Objects, Policies, System, Authentication System, and Security Solution. The 'System' category is expanded, showing sub-items like General, System, Logging Options, Alarm Options, Administrator, Maintenance, Troubleshooting, and High Availability. The 'Troubleshooting' sub-item is selected, leading to a 'Web Console' window. This window lists various commands supported by the console, such as 'cls', 'term', 'vlan', 'mode_switch', 'arp', 'mii-tool', 'ifconfig', 'switch-mac', 'ping', 'telnet', 'ethtool', 'route', 'tracert', and 'tcpdump', each with a brief description of its function. A red rounded rectangle highlights this list of commands. At the bottom of the console window, there is a prompt '>' and a note to 'Type and Execute commands here, type 'help' for help'. An 'Activate Windows' watermark is also visible in the bottom right corner of the console area.

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

Capture Packets

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



The screenshot displays the Sangfor Web Console interface. On the left is a navigation menu with categories like Status, Network, Objects, Policies, System, Administrator, Maintenance, Troubleshooting, High Availability, Authentication System, and Security Solution. The main area shows the 'Capture Packets' tab, which is currently 'Stopped'. A table lists a single capture rule with the following details:

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

An 'Options' dialog box is open, showing configuration for the selected rule. It has two sections: 'Basics' and 'Advanced (TCPDUMP)'. The 'Basics' section includes 'Max Packets' set to 4096. The 'Advanced (TCPDUMP)' section includes 'Interface Group' (eth0), 'IP Address' (192.168.1.1), 'Port' (80), and an empty 'Filter Expression' field. A red callout bubble points to the 'Filter Expression' field with the text: 'Kamu bisa mengatur filter yang diinginkan. Ini juga mendukung tepdum expression'. The dialog has 'Capture' and 'Cancel' buttons at the bottom.

System logs

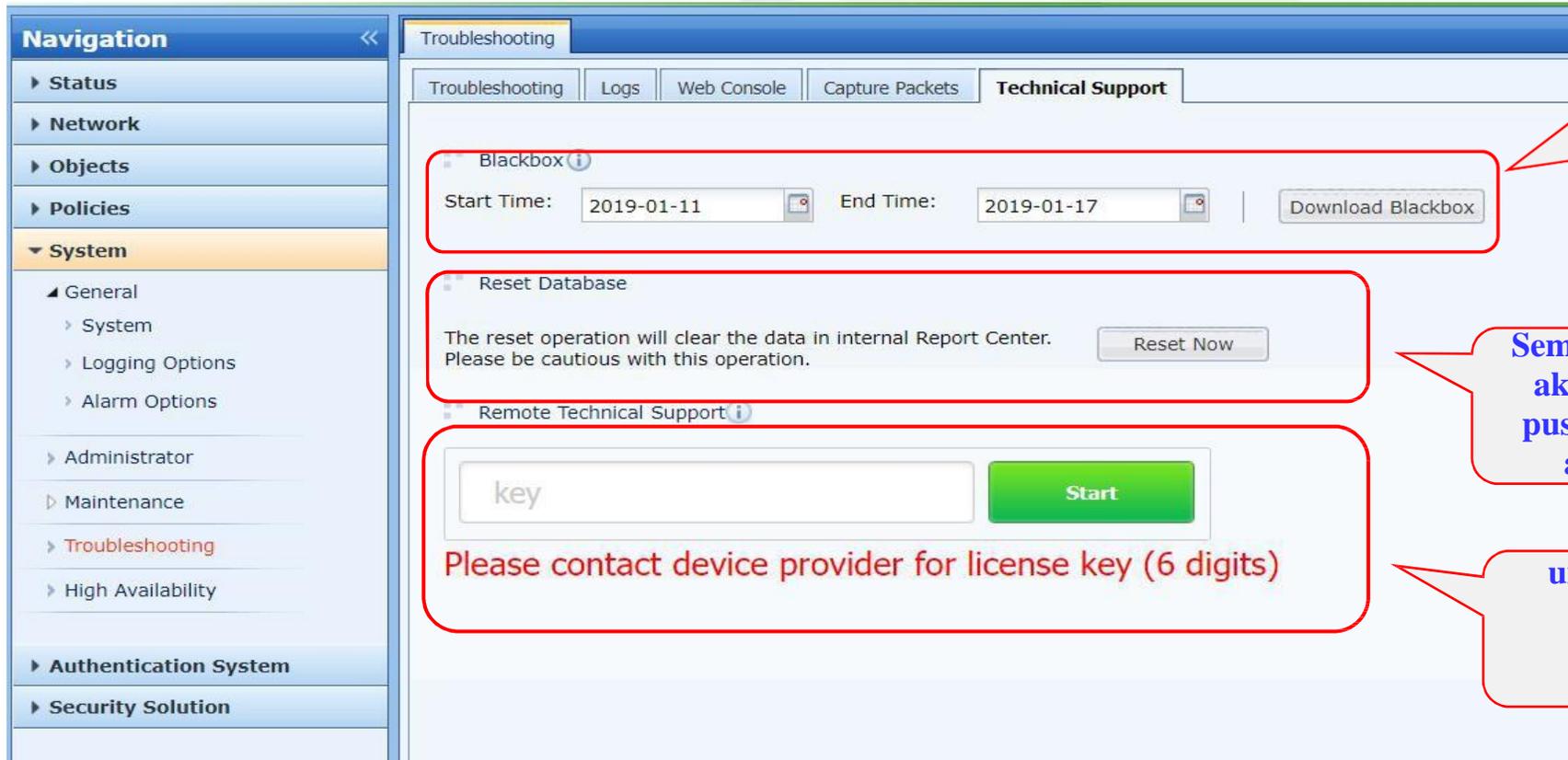


Log sistem digunakan untuk menganalisa beberapa NGAF yang error ataupun untuk mendapatkan beberapa informasi dari log yang sedang berjalan.

The screenshot displays the 'System Logs' interface in a Sangfor management console. The left sidebar shows a navigation menu with categories like Status, Network, Objects, Policies, System, Authentication System, and Security Solution. The main area is titled 'Troubleshooting' and contains a 'Logs' tab. A table lists 24 log entries, alternating between 'Info' and 'Warning' types, primarily related to VPN Service negotiations. The details for the warning entries indicate that Phase 1 security association failed, leading to a failed connection build. The interface also includes a date filter set to '2019-01-17', a page number of '1 of 27', and an 'Entries Per Page' of '50'.

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:CfgTableUpdate.cpp:2577 update table CfgServAppCrc, CfgCrcName ok.

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 menu includes General, System, Logging Options, Alarm Options, Administrator, Maintenance, Troubleshooting (highlighted), and High Availability. The main content area is titled 'Technical Support' and contains 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)

