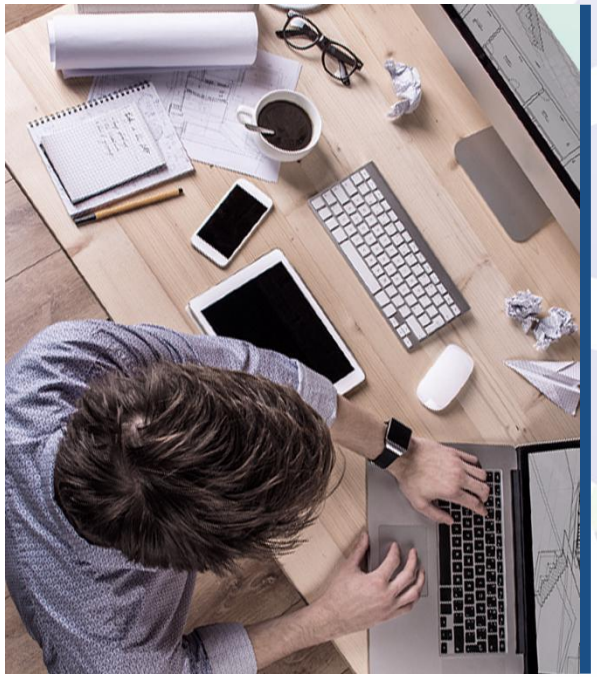
Sangfor NGAF v8.0.6 Associate

Pengaturan Sistem



1. Lisensi
2. Databases Update
3. Backup/Restore
4. Global Whitelist/Blacklist
5. Troubleshooting

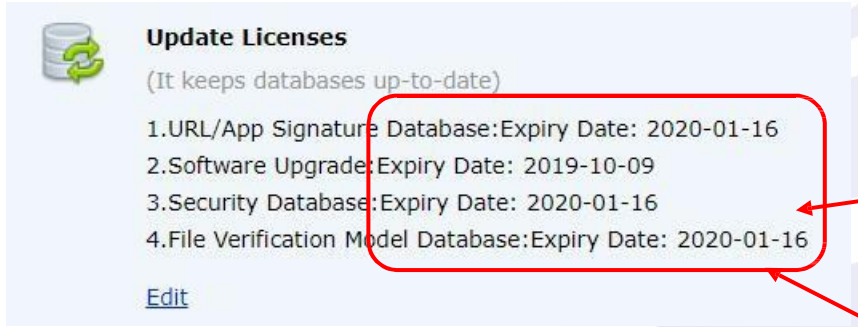
1. Lisensi

SANGFOR
深信服科技

Lisensi

Lisensi pada dasarnya digunaan 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.

Lisensi



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

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	✓	

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

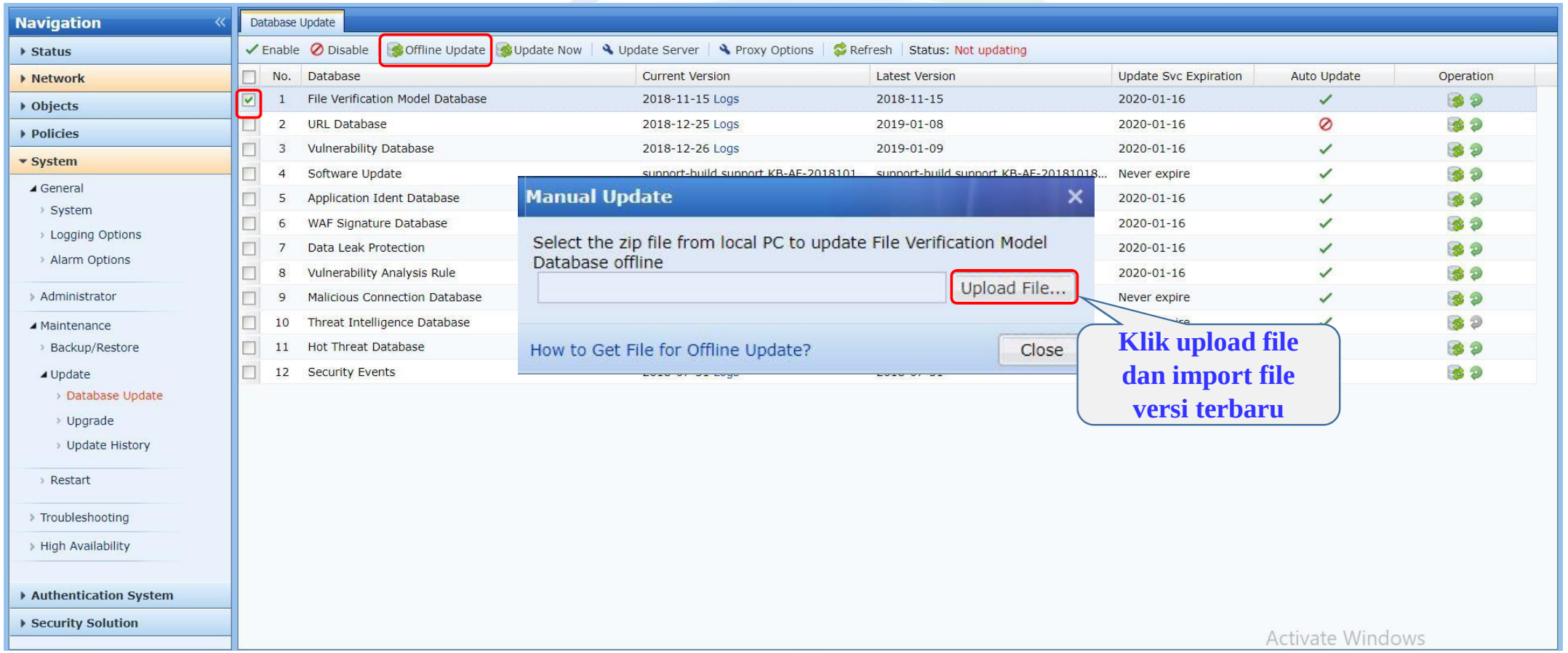
Pastikan bahwa NGAF terkoneksi dengan server Sangfor update. Jika ada update terbaru,

NGAF akan mendapatkan library dari server secara otomatis, dengan syarat layanan

update masih valid.

Databases Update

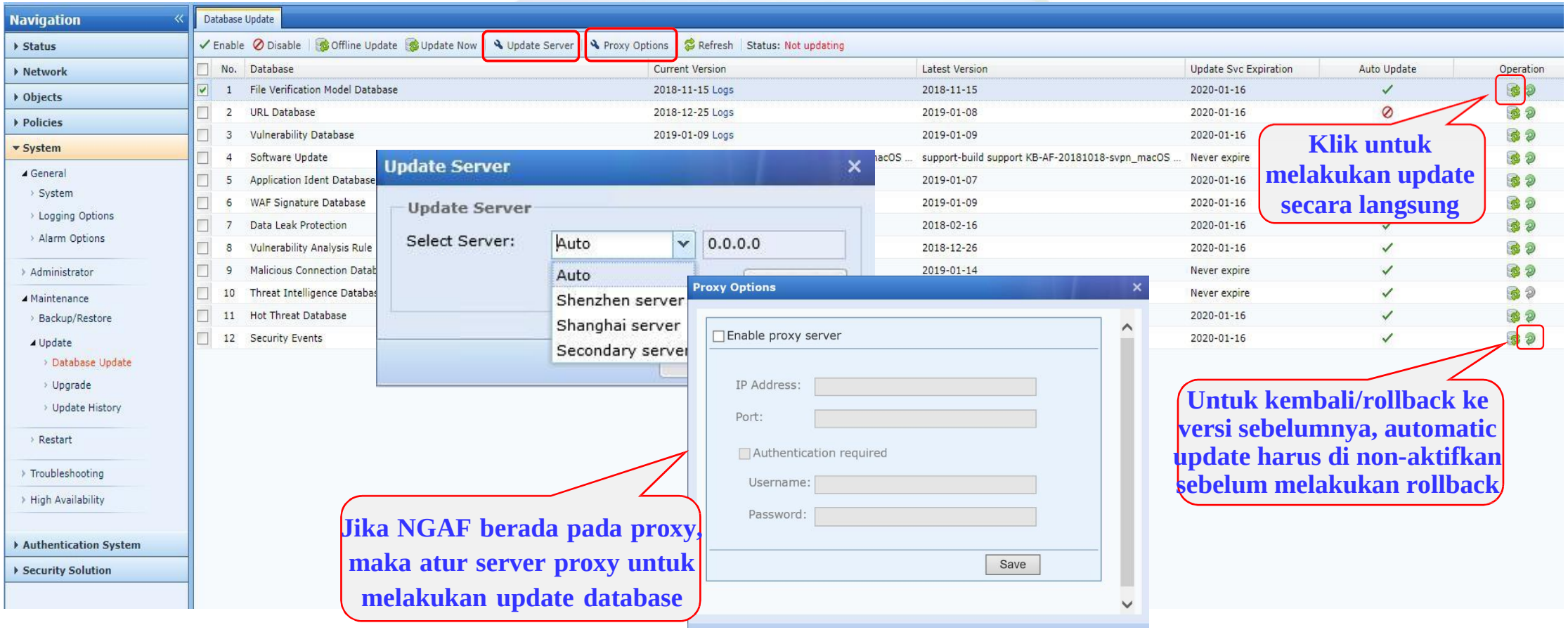
Secara Offline



Databases update

Auto update

NGAF akan melakukan update database setiap pagi.



Databases update

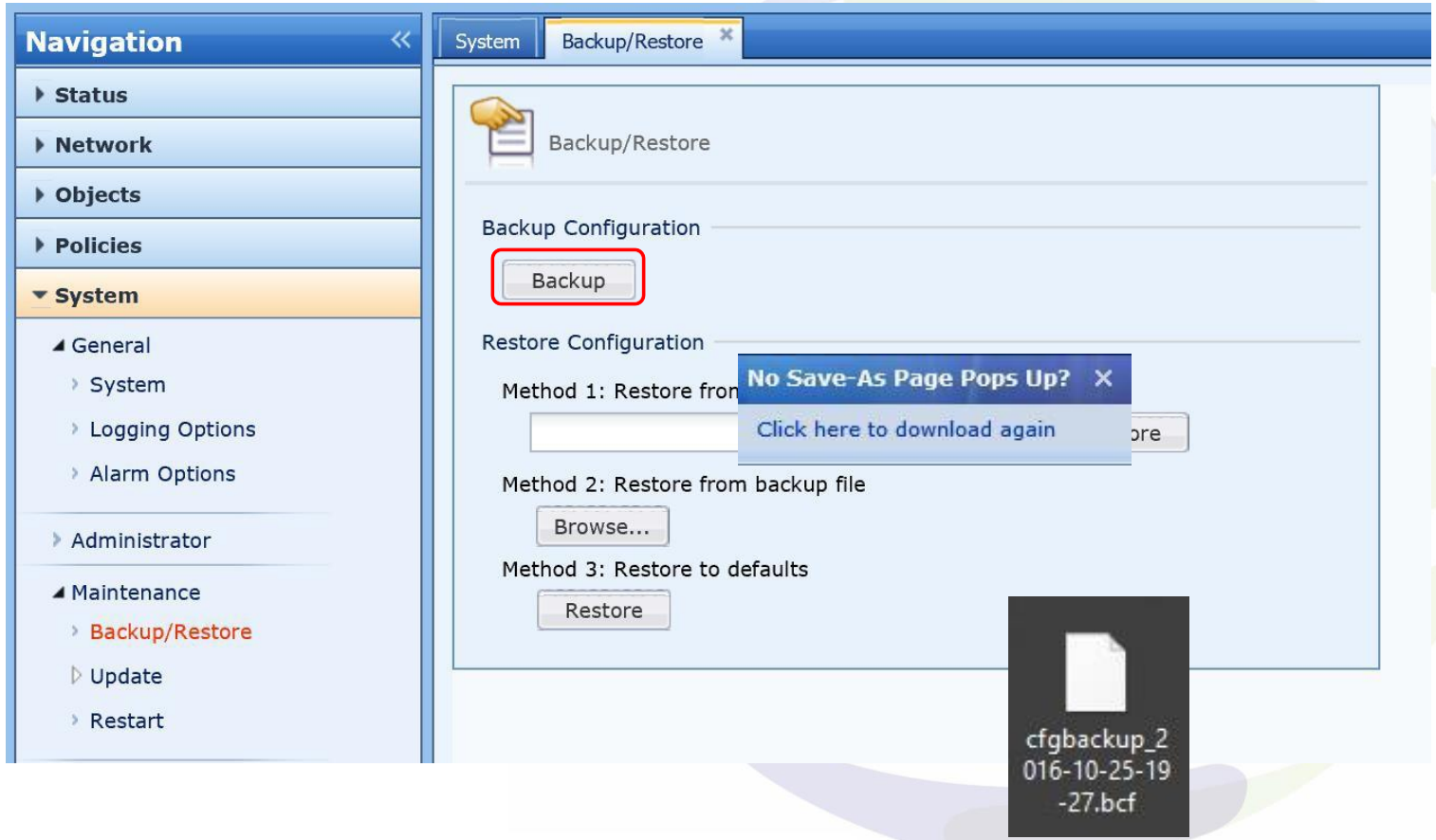
Database update mengharuskan NGAF untuk mengakses internet, oleh karena itu penting untuk melakukan pengaturan DNS server yang benar.

3. Backup/Restore

SANGFOR
深信服科技

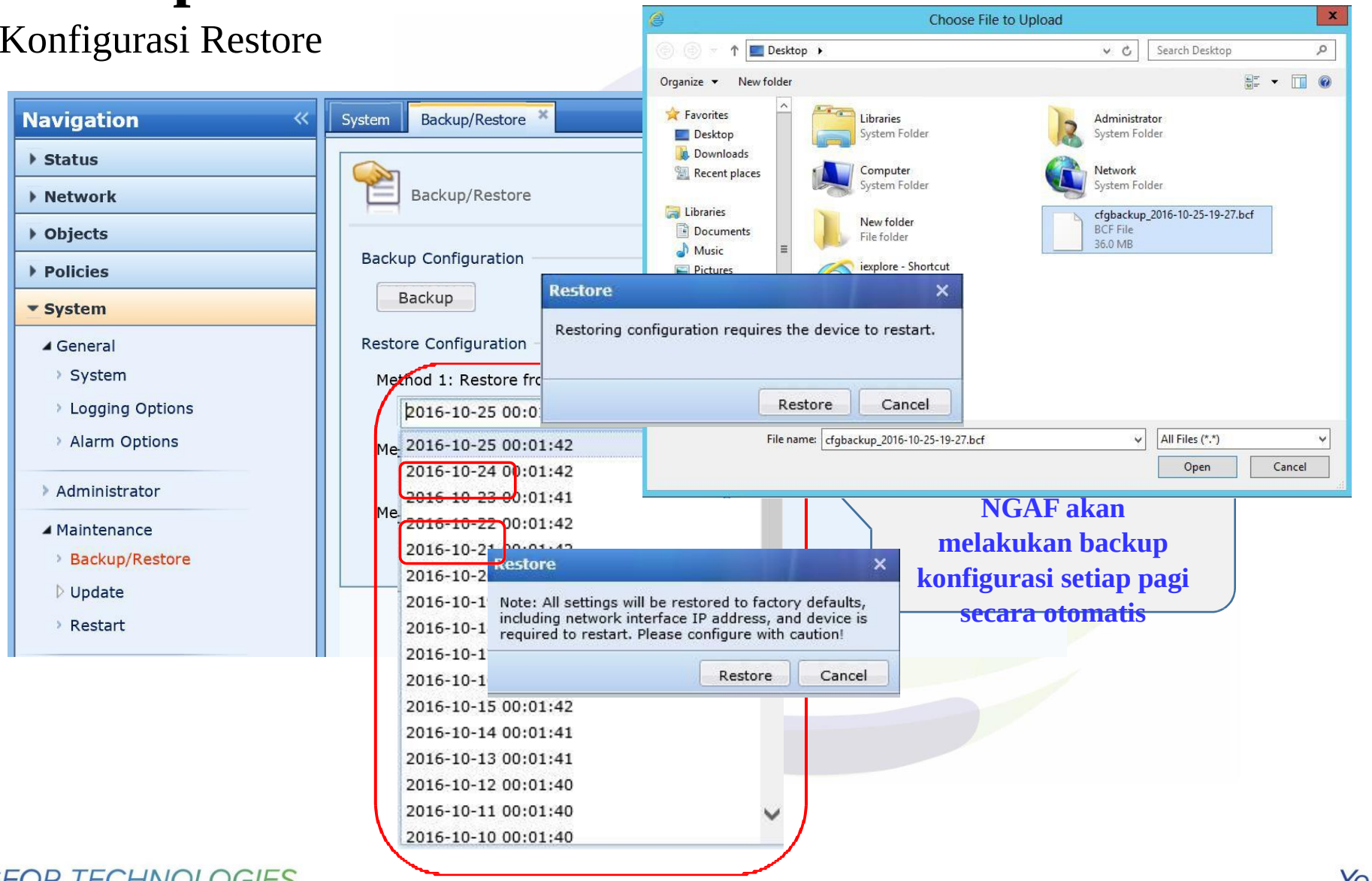
Backup/Restore

Konfigurasi Backup



Backup/Restore

Konfigurasi Restore

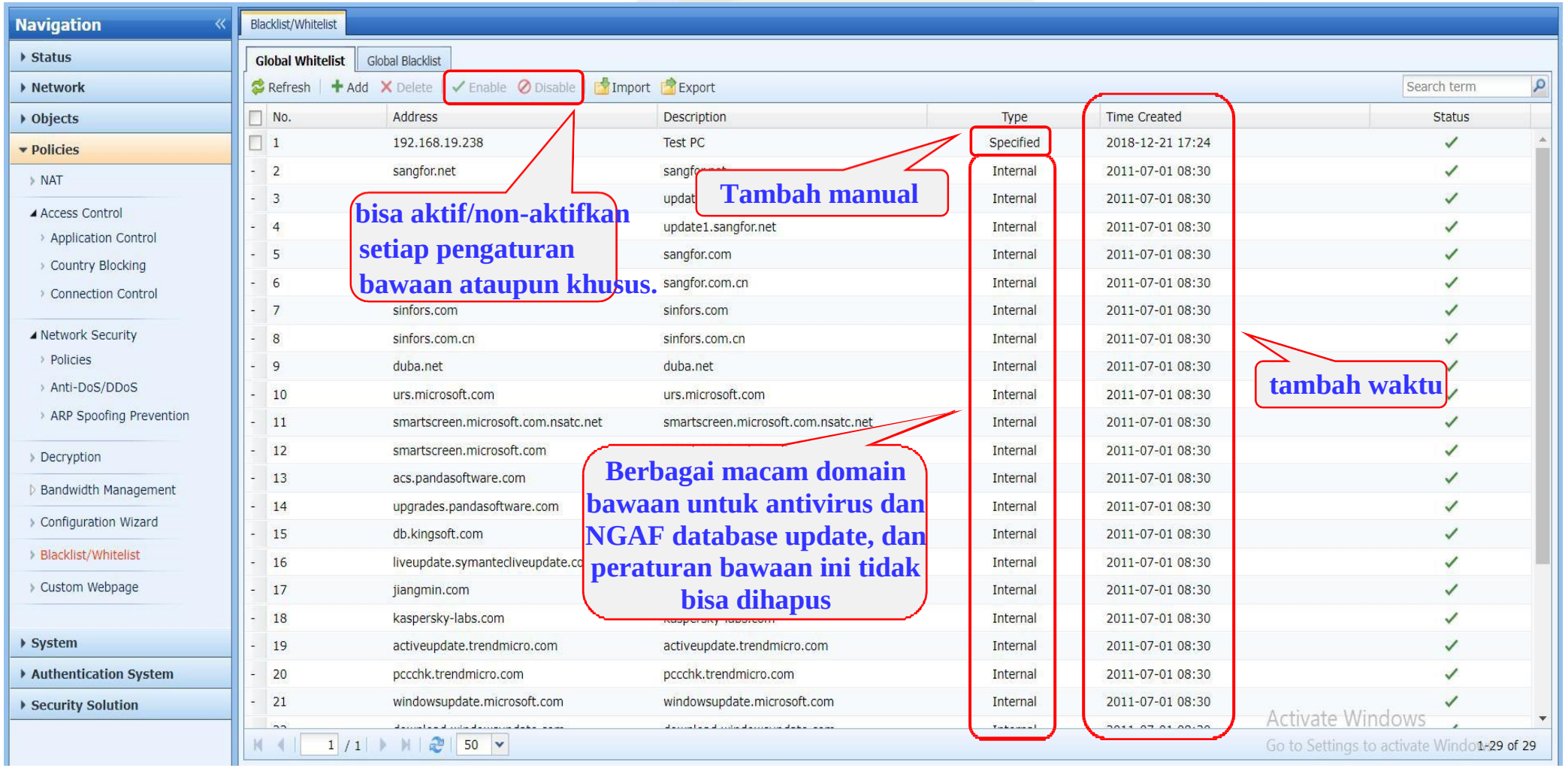


4. Global Whitelist/Blacklist

SANGFOR
深信服科技

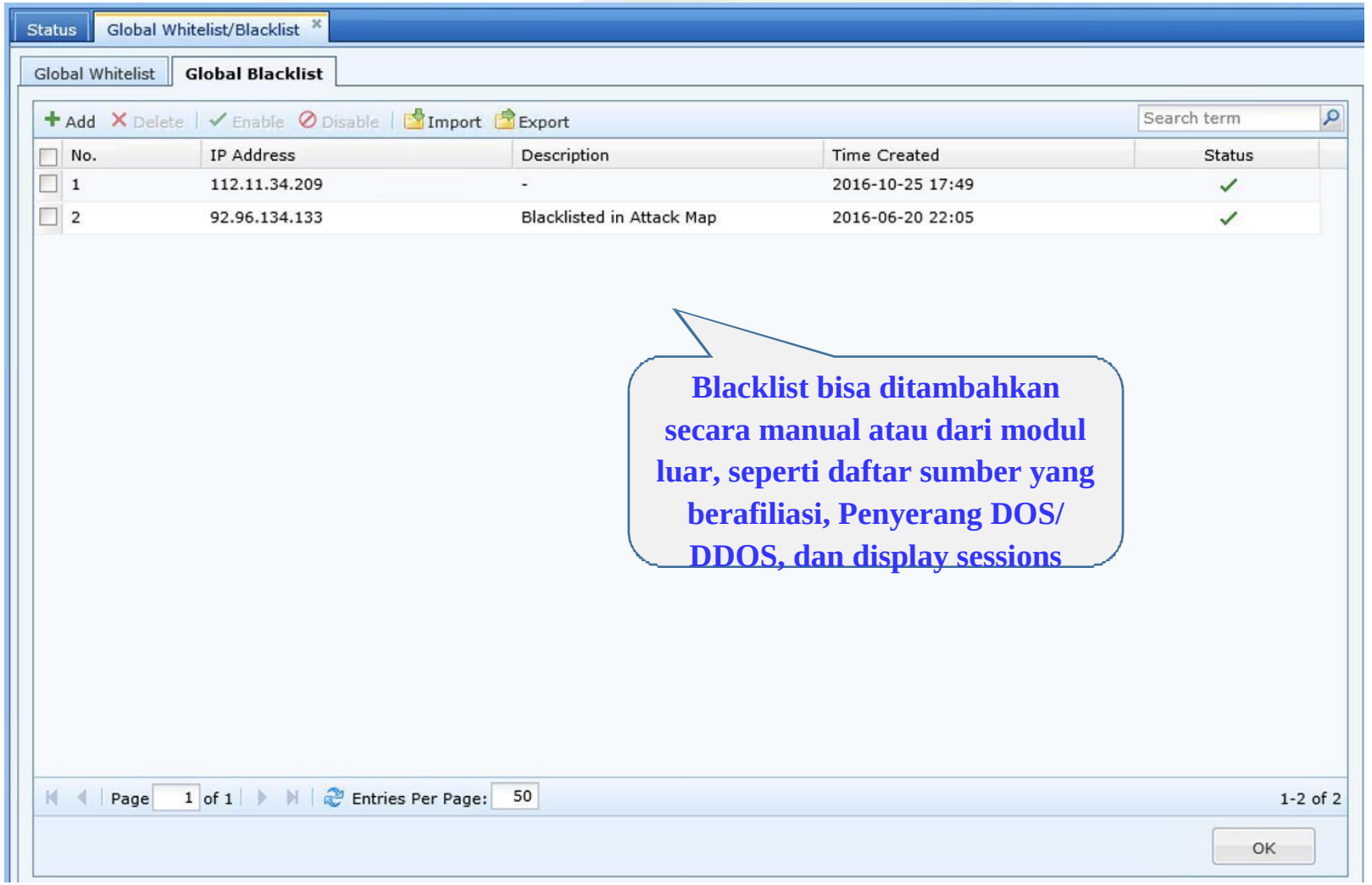
Global Whitelist/Blacklist

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



Global Whitelist/Blacklist

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



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:

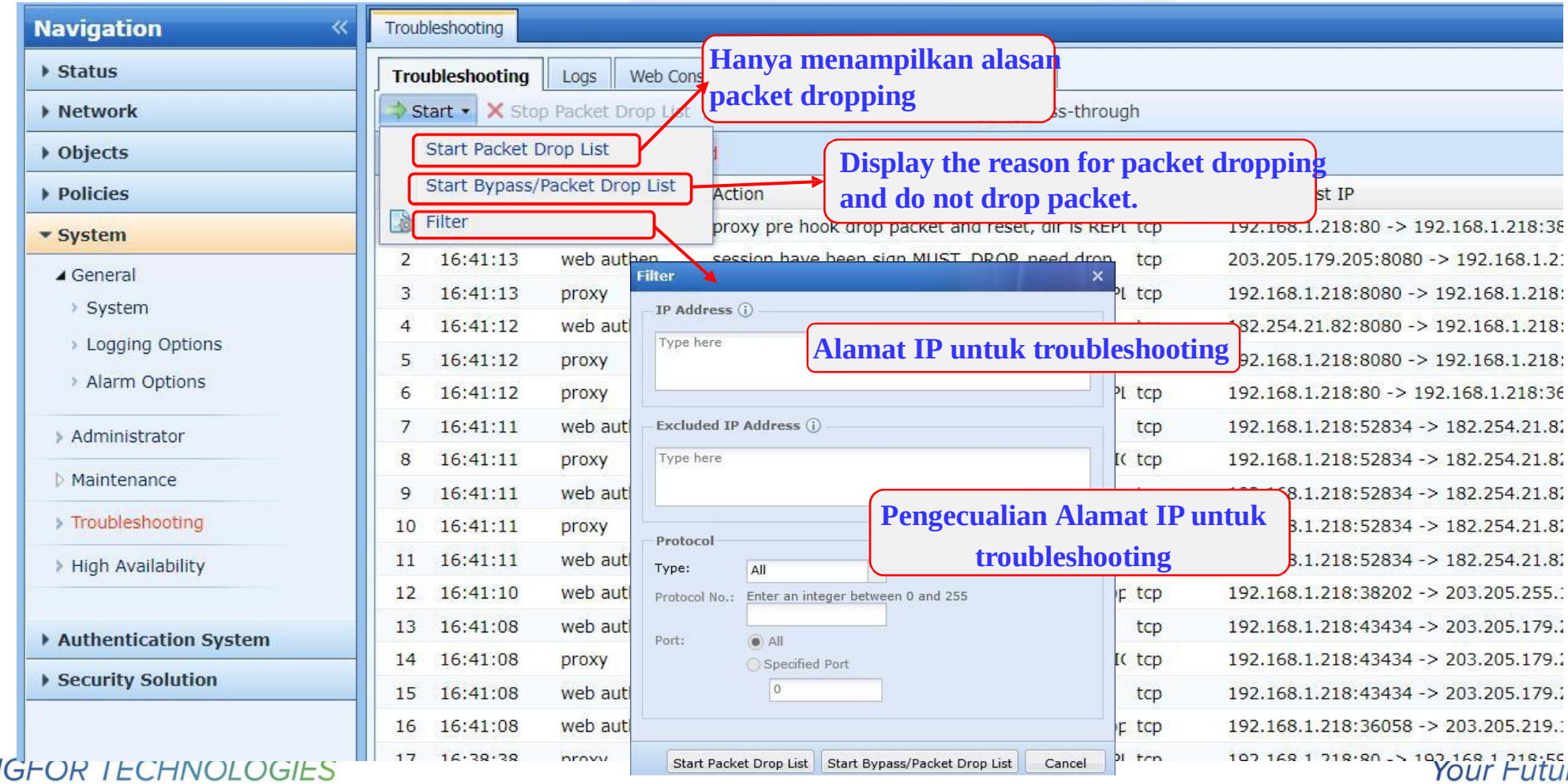
Packet-based attack dan abnormal message probe pada DOS/DDOS protection, HTTP dan FTP application hiding.

5. Troubleshooting

SANGFOR
深信服科技

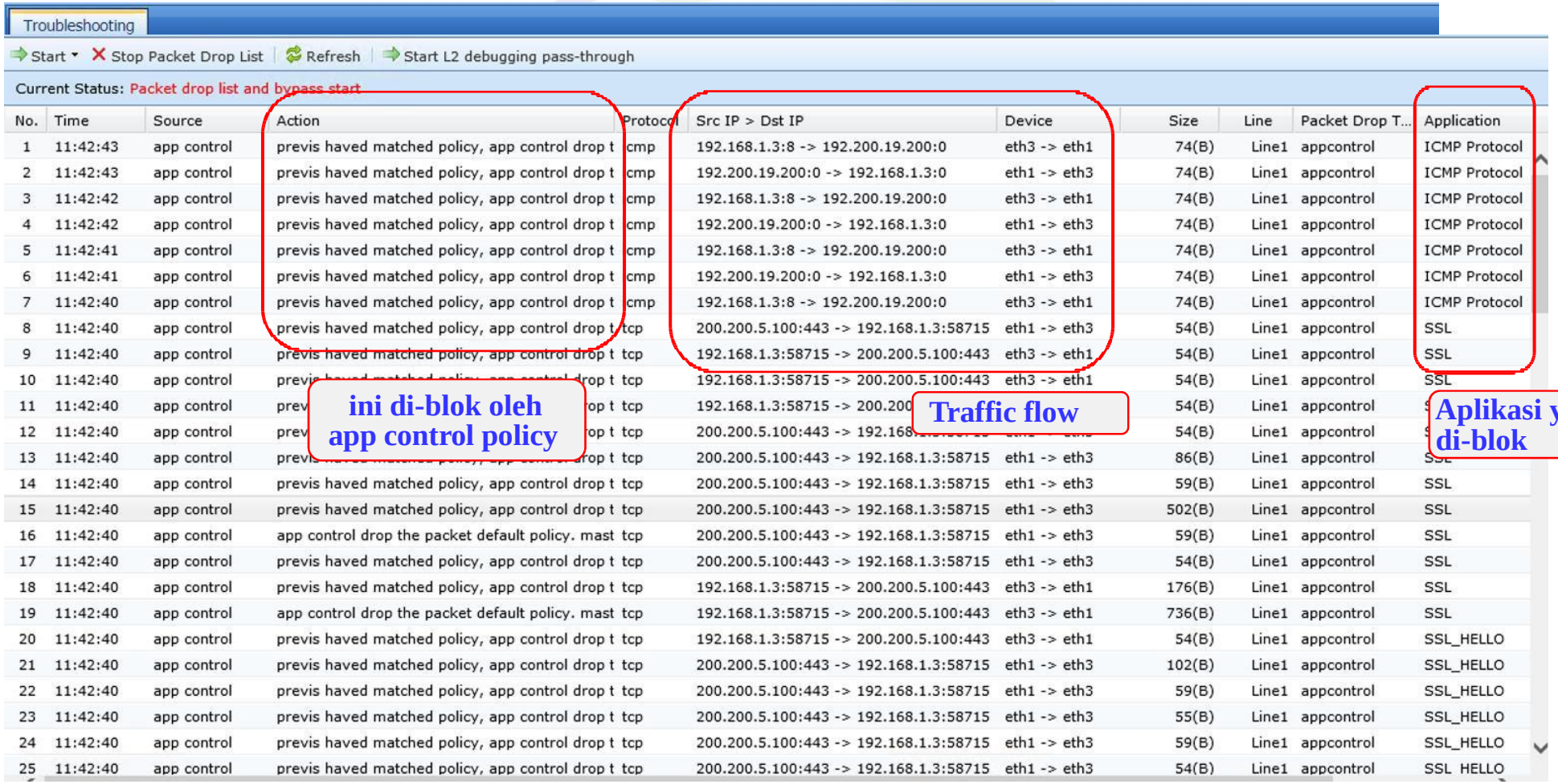
Troubleshooting(software bypass)

Ketika kita menhadapi 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.



Troubleshooting(software bypass)

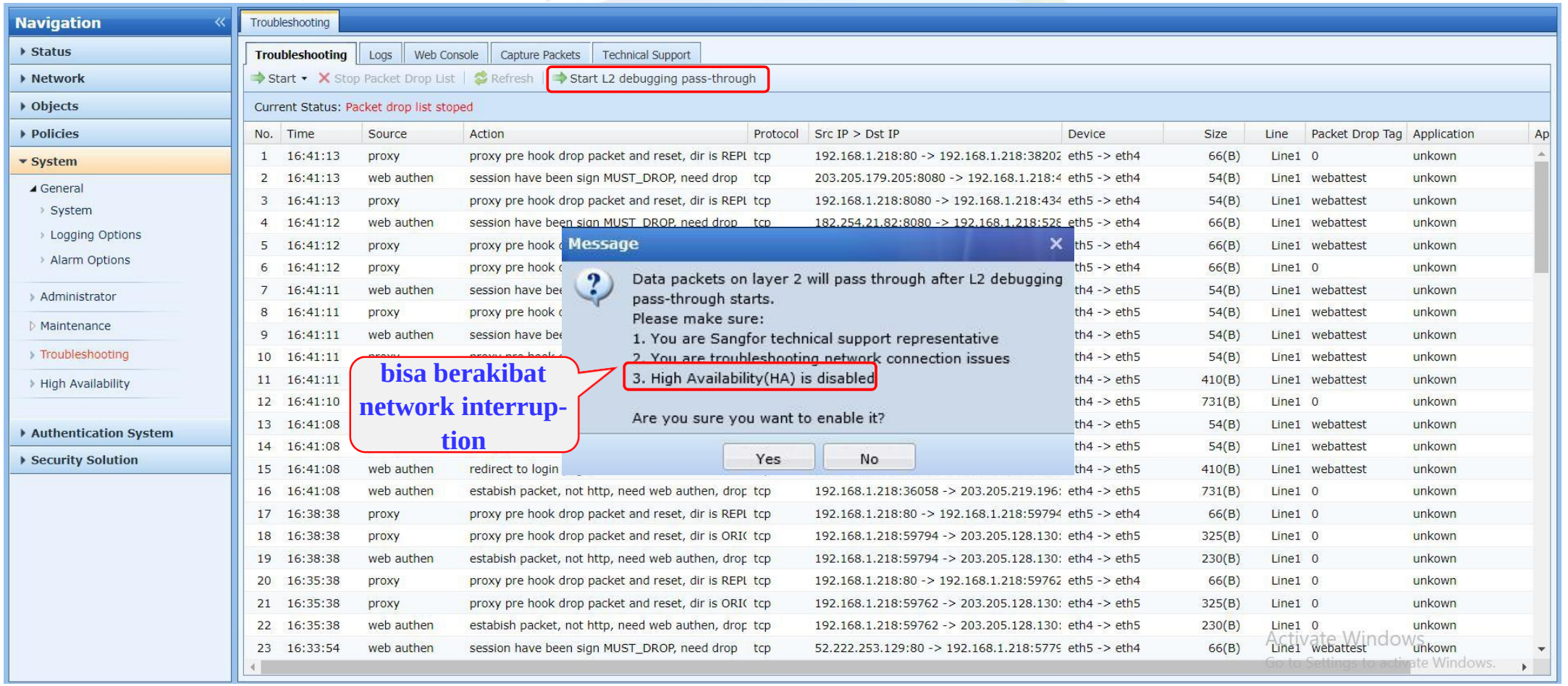
Bagaimana cara melakukan troubleshooting(software bypass)?



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	prev	tcp	192.168.1.3:58715 -> 200.200		54(B)	Line1	appcontrol	S
12	11:42:40	app control	prev	tcp	200.200.5.100:443 -> 192.168		54(B)	Line1	appcontrol	S
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

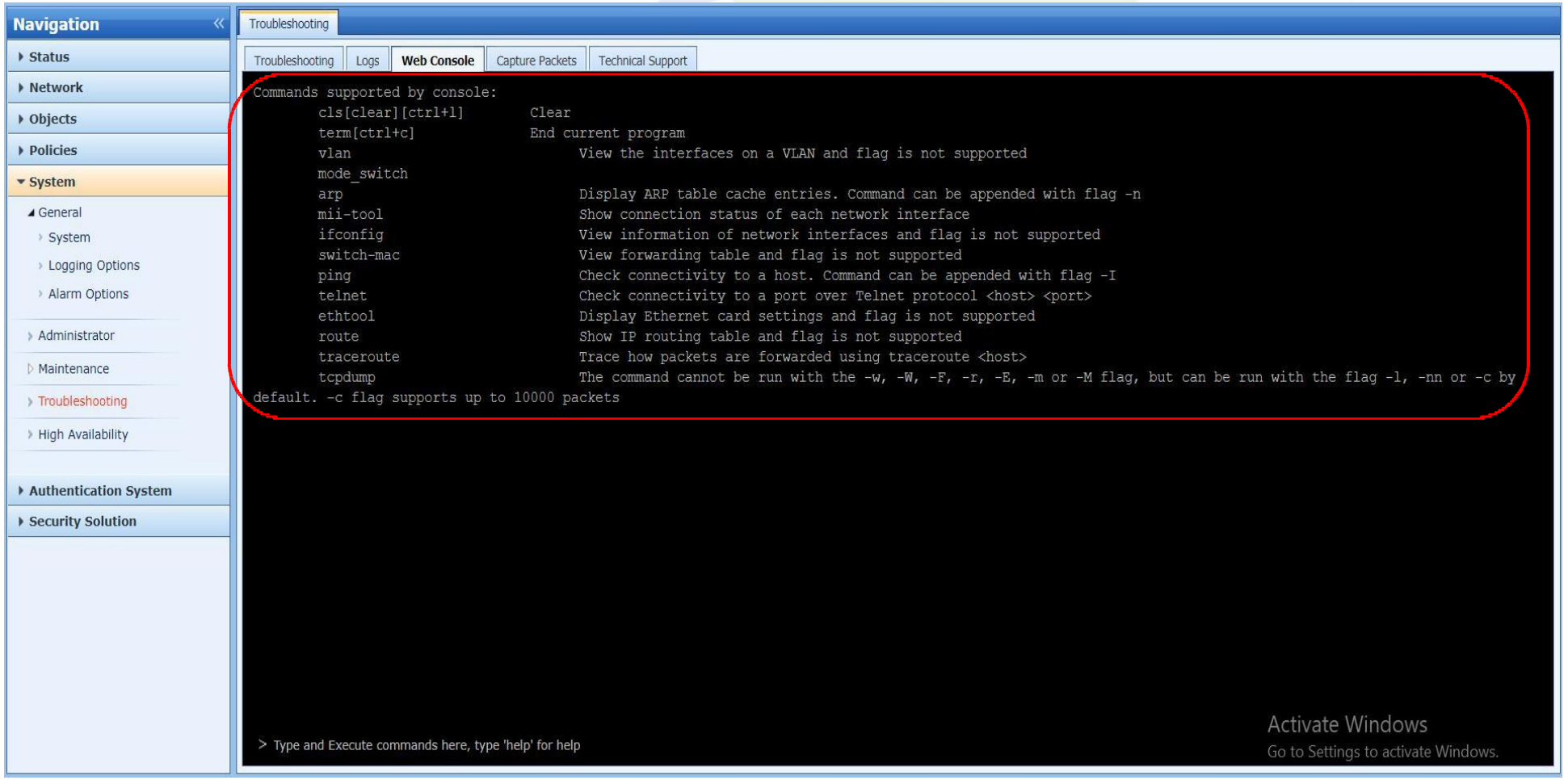
Troubleshooting(software bypass)

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



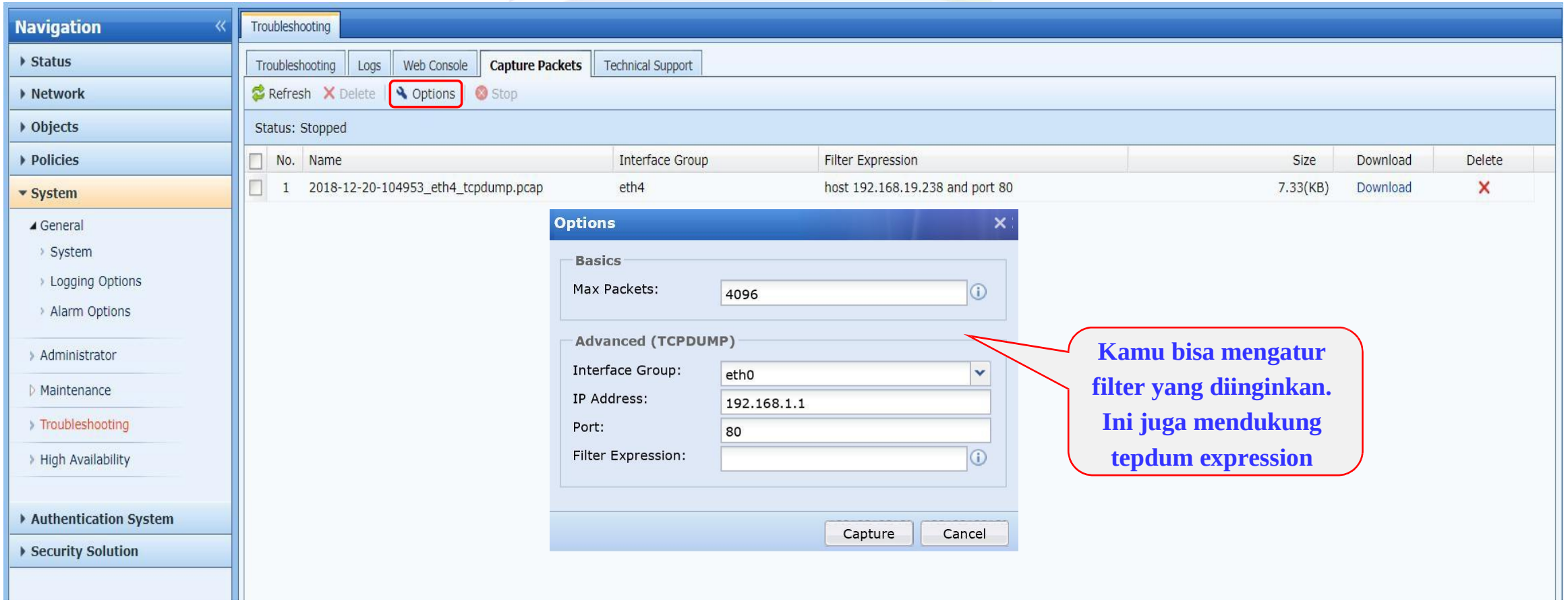
Web Console

Web console juga menyediakan beberapa command untuk maintenance



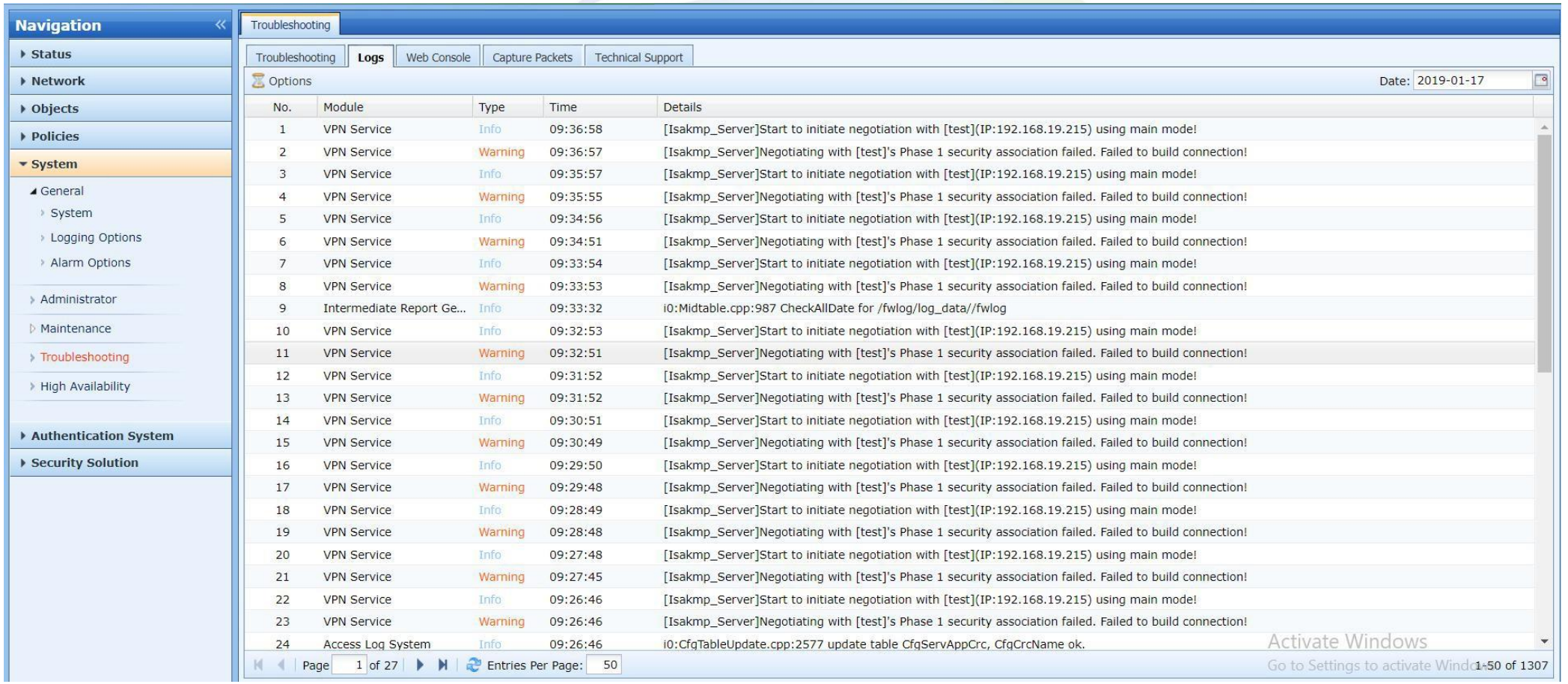
Capture Packets

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

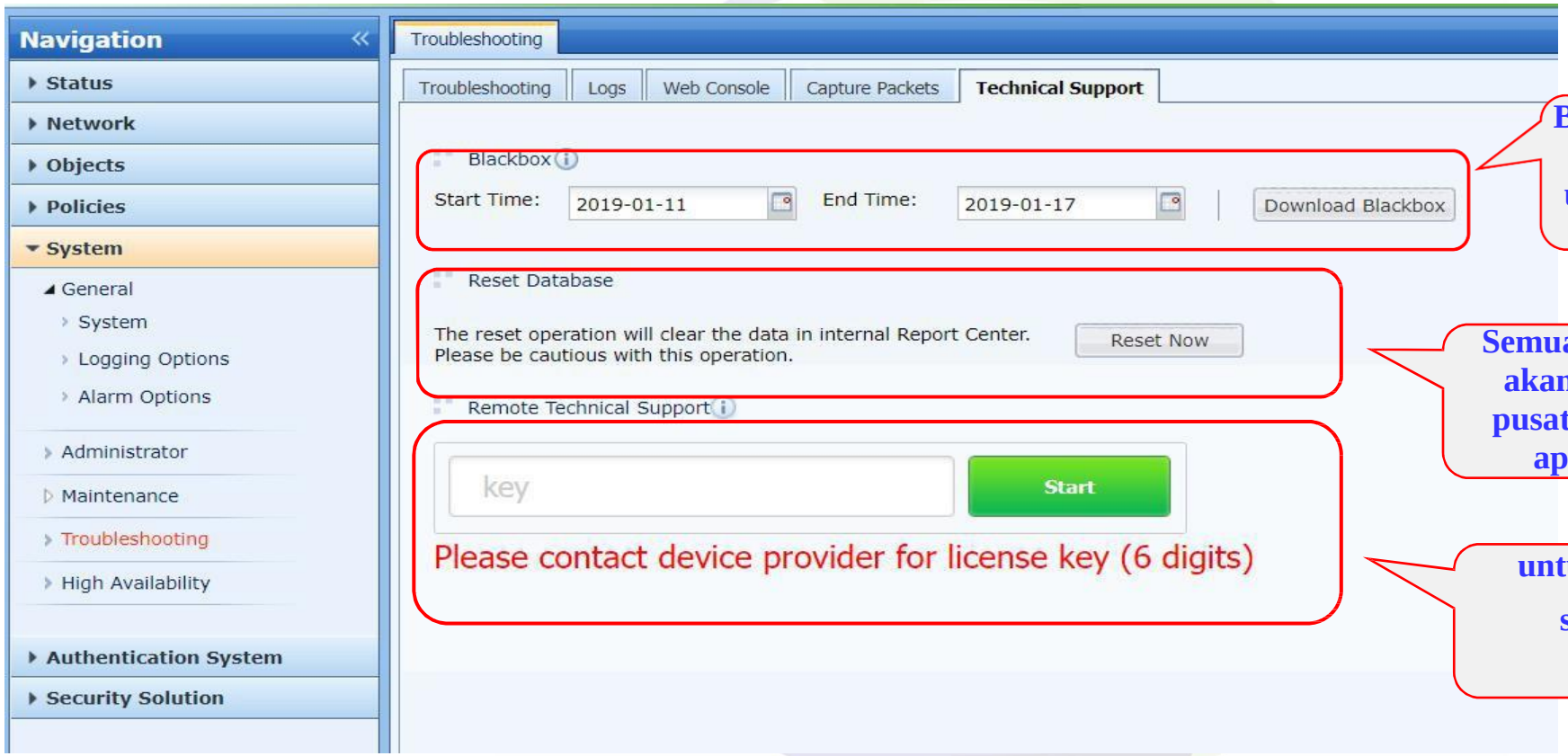


System logs

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



Perangkat Technical Support Lainnya



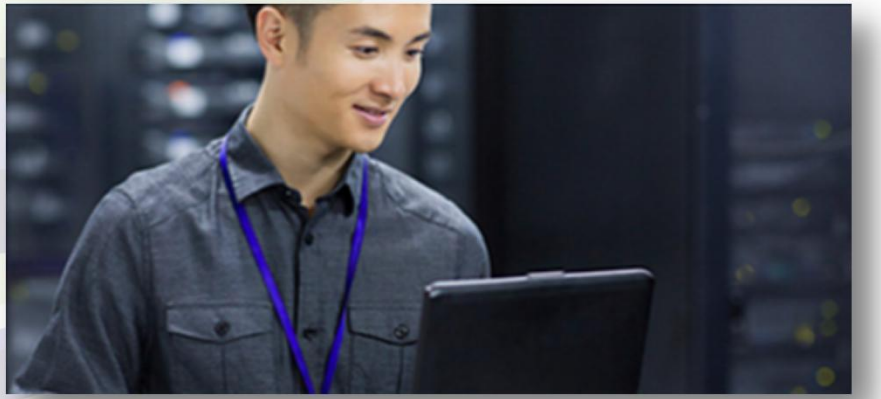
Blackbox logs digunakan pada Sangfor Technical Support untuk menganalisa beberapa masalah historis

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)