SANGFOR

IAM

Best Practices for Scenarios_Audit Policy

Version 12.0.42

Change Log

Date	Change Description
July 27, 2020	Version 12.0.42 document release.
May 17, 2021	Version 12.0.42 document update.

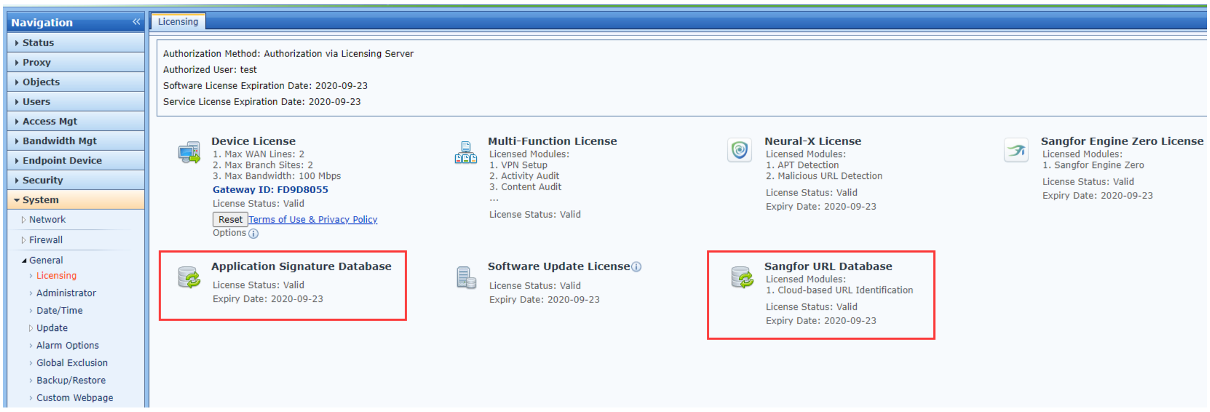
CONTENT

Chapter 1 Scenario

A university hopes to audit students' online behavior, including the websites they visit and the applications they use. In addition, they need to analyze the ranking of the total traffic and duration of the students' access to various applications.

Chapter 2 Network Environment Checking

1. Check the authorization and database version to ensure that the rule base has been updated to the latest date. The application control policy for processing data packets relies on the dataabse. If the database is not updated to the latest version, the identification of some traffic may be wrong.



Authorization Method: Authorization via Licensing Server
Authorized User: test
Software License Expiration Date: 2020-09-23
Service License Expiration Date: 2020-09-23

Device License
1. Max WAN Lines: 2
2. Max Branch Sites: 2
3. Max Bandwidth: 100 Mbps
Gateway ID: FD9D8055
License Status: Valid
Reset Terms of Use & Privacy Policy
Options

Multi-Function License
Licensed Modules:
1. VPN Setup
2. Activity Audit
3. Content Audit
...
License Status: Valid

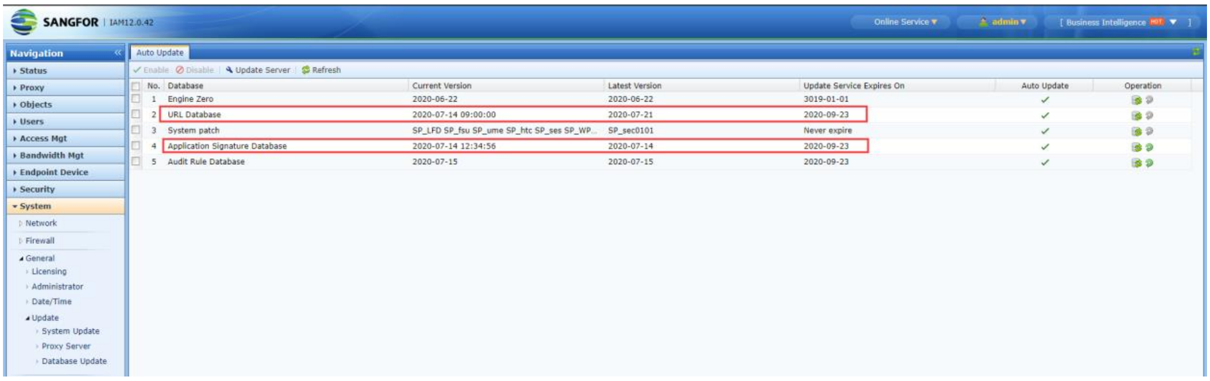
Neural-X License
Licensed Modules:
1. APT Detection
2. Malicious URL Detection
License Status: Valid
Expiry Date: 2020-09-23

Sangfor Engine Zero License
Licensed Modules:
1. Sangfor Engine Zero
License Status: Valid
Expiry Date: 2020-09-23

Application Signature Database
License Status: Valid
Expiry Date: 2020-09-23

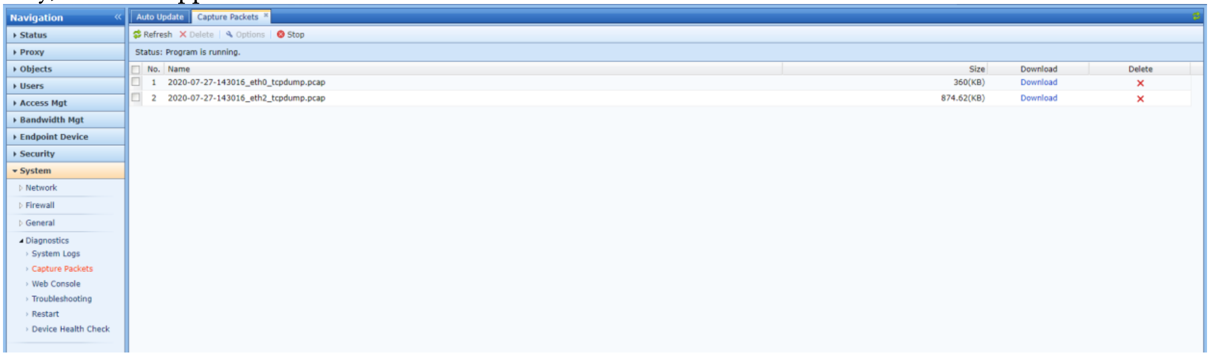
Software Update License
License Status: Valid
Expiry Date: 2020-09-23

Sangfor URL Database
Licensed Modules:
1. Cloud-based URL Identification
License Status: Valid
Expiry Date: 2020-09-23



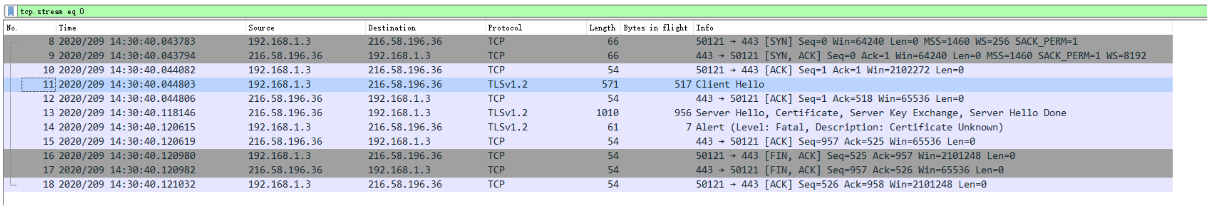
□	No.	Database	Current Version	Latest Version	Update Service Expires On	Auto Update	Operation
□	1	Engine Zero	2020-06-22	2020-06-22	3019-01-01	✓	
□	2	URL Database	2020-07-14 09:00:00	2020-07-21	2020-09-23	✓	
□	3	System patch	SP_LFD SP_fsu SP_ume SP_htc SP_ses SP_WP...	SP_sec0101	Never expire	✓	
□	4	Application Signature Database	2020-07-14 12:34:56	2020-07-14	2020-09-23	✓	
□	5	Audit Rule Database	2020-07-15	2020-07-15	2020-09-23	✓	

2. Ensure that network traffic passes through the IAM device in both directions. If the traffic is only one-way, then the application cannot be identified and controlled.



Status: Program is running.

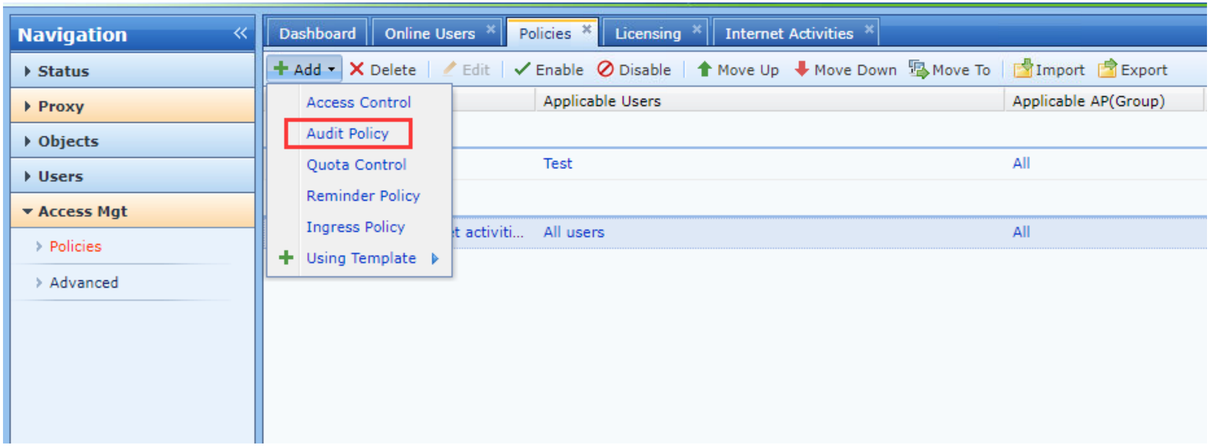
□	No.	Name	Size	Download	Delete
□	1	2020-07-27-143016_eth0_tcpdump.pcap	360(KB)	Download	✕
□	2	2020-07-27-143016_eth2_tcpdump.pcap	874.62(KB)	Download	✕



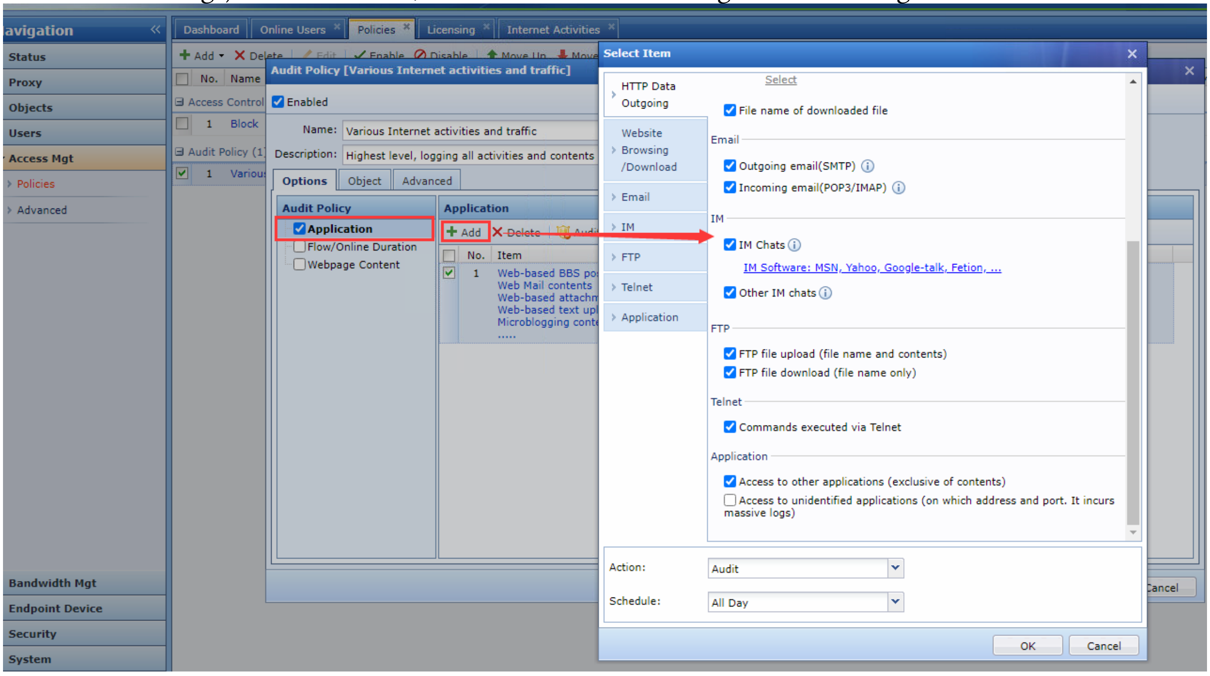
```
tcp.stream eq 0
No.    Time                        Source          Destination     Protocol  Length  Bytes in flight  Info
     8 2020/209 14:30:40.043783    192.168.1.3     216.58.196.36   TCP           66                   50121 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
     9 2020/209 14:30:40.043794    216.58.196.36   192.168.1.3     TCP           66                   443 → 50121 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
    10 2020/209 14:30:40.044082    192.168.1.3     216.58.196.36   TCP           54                   50121 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
    11 2020/209 14:30:40.044803    192.168.1.3     216.58.196.36   TLSv1.2      571              517 Client Hello
    12 2020/209 14:30:40.044806    216.58.196.36   192.168.1.3     TCP           54                   443 → 50121 [ACK] Seq=1 Ack=518 Win=65536 Len=0
    13 2020/209 14:30:40.118146    216.58.196.36   192.168.1.3     TLSv1.2     1010              956 Server Hello, Certificate, Server Key Exchange, Server Hello Done
    14 2020/209 14:30:40.120615    192.168.1.3     216.58.196.36   TLSv1.2       61                7 Alert (Level: Fatal, Description: Certificate Unknown)
    15 2020/209 14:30:40.120619    216.58.196.36   192.168.1.3     TCP           54                   443 → 50121 [ACK] Seq=957 Ack=525 Win=65536 Len=0
    16 2020/209 14:30:40.120980    192.168.1.3     216.58.196.36   TCP           54                   50121 → 443 [FIN, ACK] Seq=525 Ack=957 Win=2101248 Len=0
    17 2020/209 14:30:40.120982    216.58.196.36   192.168.1.3     TCP           54                   443 → 50121 [FIN, ACK] Seq=957 Ack=526 Win=65536 Len=0
    18 2020/209 14:30:40.121032    192.168.1.3     216.58.196.36   TCP           54                   50121 → 443 [ACK] Seq=526 Ack=958 Win=2101248 Len=0
```

Chapter 3 Configuration

1. Configure the policy and check the content that needs to be audited, such as application behavior, traffic, and web content.



When auditing application behavior, it should be noted that you usually need to check "Access to other applications (exclusive of contents)", because there are many categories of applications, and the options above this option are just a few commonly used categories, and most of the rule bases Applications are included in this option. Usually, "Access to unidentified applications (on which address and port. It incurs massive logs)" is not checked, because it will cause a huge amount of logs.



Audit Policy [Various Internet activities and traffic]

☑ Enabled

Name: Various Internet activities and traffic

Description: Highest level, logging all activities and contents

Audit Policy

☑ Application

□ Flow/Online Duration

□ Webpage Content

Application

☑	No.	Item
☑	1	Web-based BBS po Web Mail contents Web-based attachm Web-based text up Microblogging conte .....

☑ File name of downloaded file

Email

☑ Outgoing email(SMTP)

☑ Incoming email(POP3/IMAP)

IM

☑ IM Chats

IM Software: MSN, Yahoo, Google-talk, Fetion, ...

☑ Other IM chats

FTP

☑ FTP file upload (file name and contents)

☑ FTP file download (file name only)

Telnet

☑ Commands executed via Telnet

Application

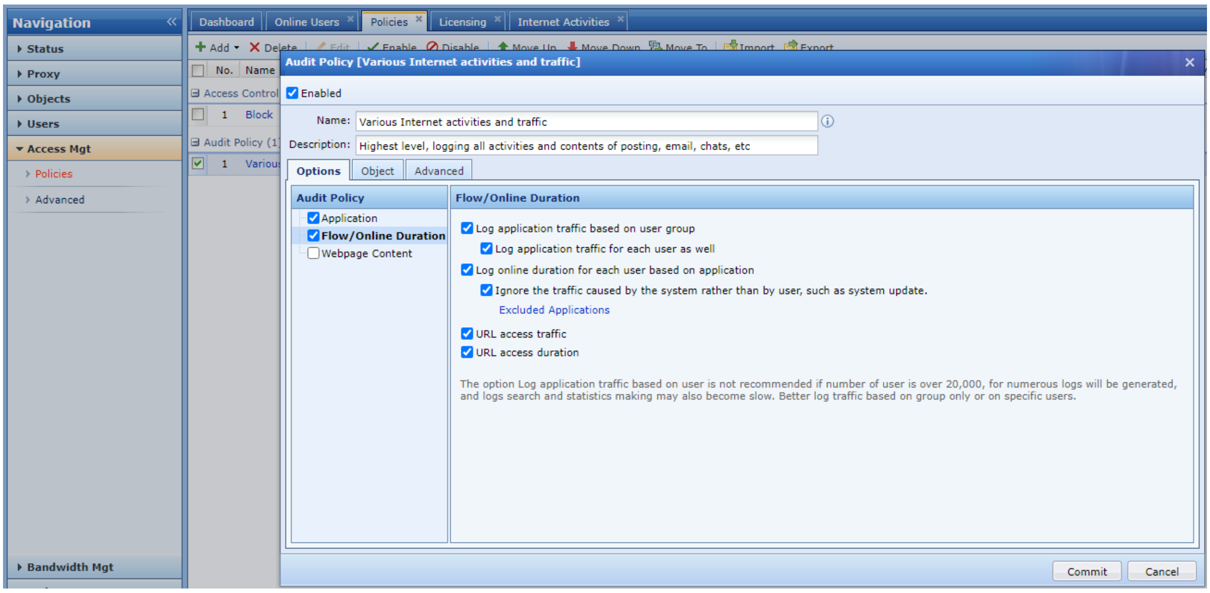
☑ Access to other applications (exclusive of contents)

□ Access to unidentified applications (on which address and port. It incurs massive logs)

Action: Audit

Schedule: All Day

Audit Policy



Audit Policy [Various Internet activities and traffic]

☑ Enabled

Name: Various Internet activities and traffic

Description: Highest level, logging all activities and contents of posting, email, chats, etc

Options | Object | Advanced

Audit Policy
- ☑ Application
- ☑ Flow/Online Duration
- □ Webpage Content

Flow/Online Duration

☑ Log application traffic based on user group

☑ Log application traffic for each user as well

☑ Log online duration for each user based on application

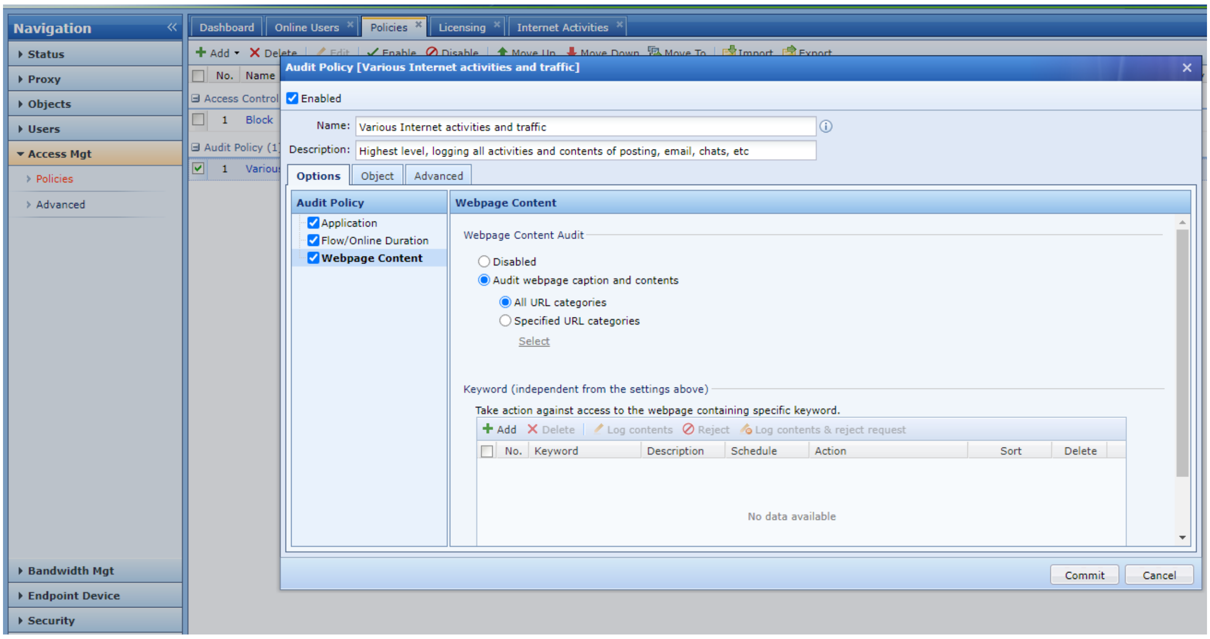
☑ Ignore the traffic caused by the system rather than by user, such as system update.

Excluded Applications

☑ URL access traffic

☑ URL access duration

The option Log application traffic based on user is not recommended if number of user is over 20,000, for numerous logs will be generated, and logs search and statistics making may also become slow. Better log traffic based on group only or on specific users.



Audit Policy [Various Internet activities and traffic]

☑ Enabled

Name: Various Internet activities and traffic

Description: Highest level, logging all activities and contents of posting, email, chats, etc

Options | Object | Advanced

Audit Policy
- ☑ Application
- ☑ Flow/Online Duration
- ☑ Webpage Content

Webpage Content

Webpage Content Audit

○ Disabled

● Audit webpage caption and contents

● All URL categories

○ Specified URL categories

Select

Keyword (independent from the settings above)

Take action against access to the webpage containing specific keyword.

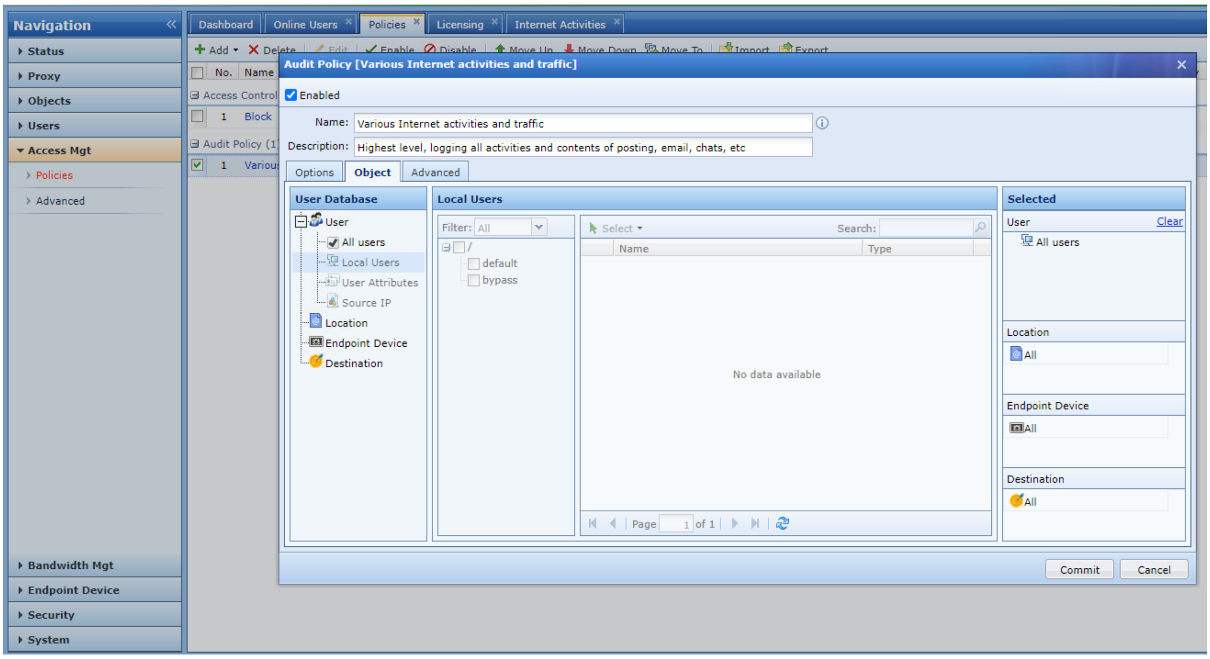
Add | Delete | Log contents | Reject | Log contents & reject request

□	No.	Keyword	Description	Schedule	Action	Sort	Delete

No data available

2. Select the target for the policy and determine which users' behavior and traffic should be audited.

Audit Policy



Audit Policy [Various Internet activities and traffic]

☑ Enabled

Name: Various Internet activities and traffic

Description: Highest level, logging all activities and contents of posting, email, chats, etc

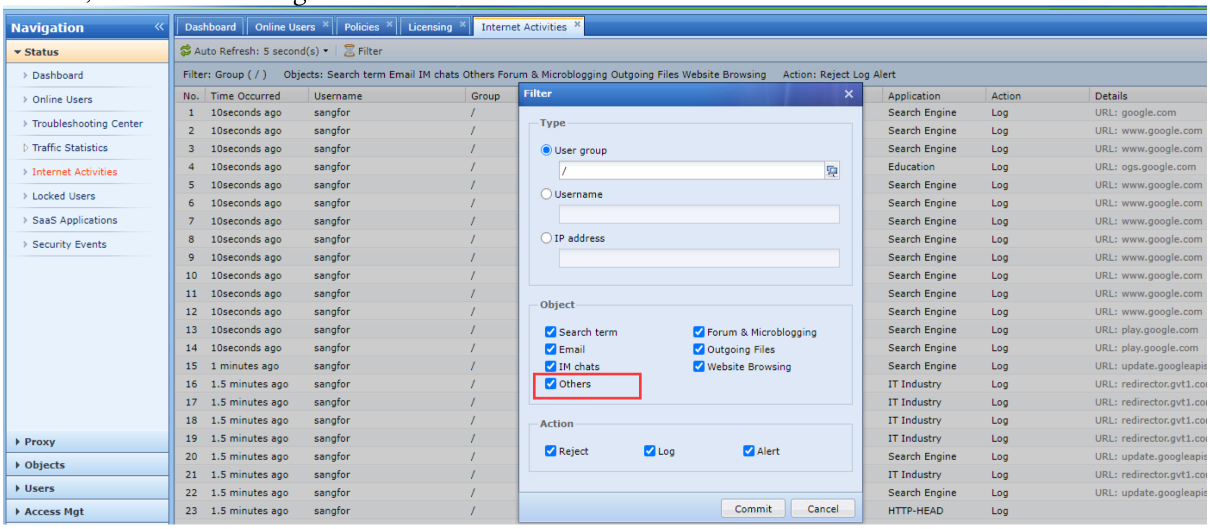
Options | **Object** | Advanced

User Database:
- User
  - ☑ All users
  - Local Users
  - User Attributes
  - Source IP
- Location
- Endpoint Device
- Destination

Local Users: Filter: All; / ☐ default ☐ bypass; Select; Search:; Name | Type; No data available; Page 1 of 1

Selected:
- User Clear: All users
- Location: All
- Endpoint Device: All
- Destination: All

3. View user behavior in "Internet Activities". If you want to filter out user behavior as much as possible, you need to check "Others" in the filter, because in addition to other common application categories such as Mail, other rules belong to "Others".



Filter: Group (/) Objects: Search term Email IM chats Others Forum & Microblogging Outgoing Files Website Browsing Action: Reject Log Alert

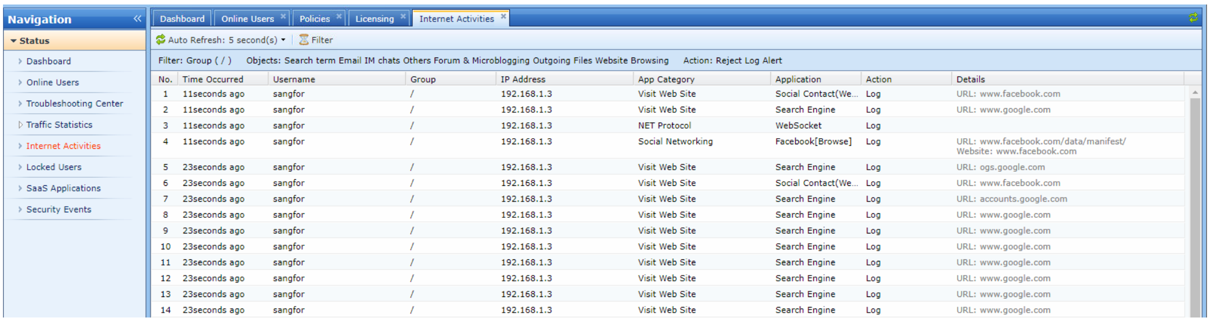
No.	Time Occurred	Username	Group	Application	Action	Details
1	10seconds ago	sangfor	/	Search Engine	Log	URL: google.com
2	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
3	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
4	10seconds ago	sangfor	/	Education	Log	URL: ogs.google.com
5	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
6	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
7	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
8	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
9	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
10	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
11	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
12	10seconds ago	sangfor	/	Search Engine	Log	URL: www.google.com
13	10seconds ago	sangfor	/	Search Engine	Log	URL: play.google.com
14	10seconds ago	sangfor	/	Search Engine	Log	URL: play.google.com
15	1 minutes ago	sangfor	/	Search Engine	Log	URL: update.googleapis
16	1.5 minutes ago	sangfor	/	IT Industry	Log	URL: redirector.gvt1.co
17	1.5 minutes ago	sangfor	/	IT Industry	Log	URL: redirector.gvt1.co
18	1.5 minutes ago	sangfor	/	IT Industry	Log	URL: redirector.gvt1.co
19	1.5 minutes ago	sangfor	/	IT Industry	Log	URL: redirector.gvt1.co
20	1.5 minutes ago	sangfor	/	Search Engine	Log	URL: update.googleapis
21	1.5 minutes ago	sangfor	/	IT Industry	Log	URL: redirector.gvt1.co
22	1.5 minutes ago	sangfor	/	Search Engine	Log	URL: update.googleapis
23	1.5 minutes ago	sangfor	/	HTTP-HEAD	Log	

Filter

Type
- ● User group: /
- ○ Username
- ○ IP address

Object
- ☑ Search term
- ☑ Email
- ☑ IM chats
- ☑ Others
- ☑ Forum & Microblogging
- ☑ Outgoing Files
- ☑ Website Browsing

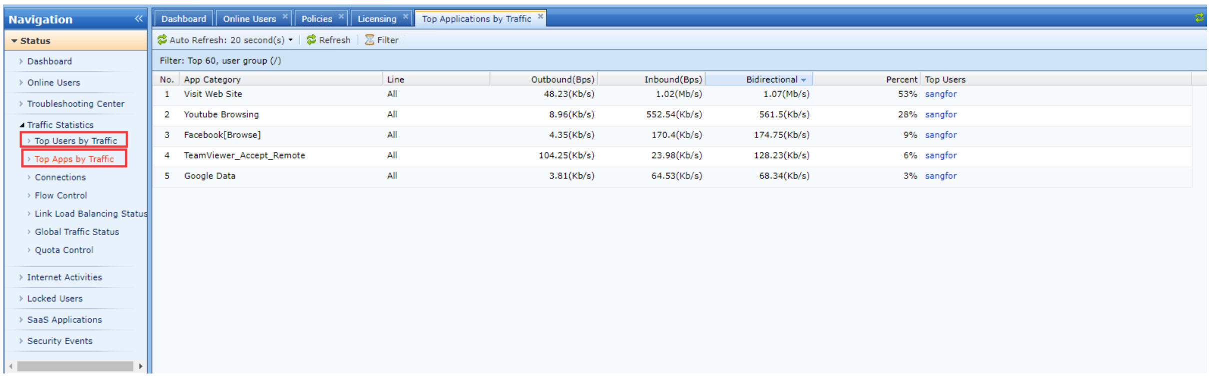
Action
- ☑ Reject ☑ Log ☑ Alert



Filter: Group (/) Objects: Search term Email IM chats Others Forum & Microblogging Outgoing Files Website Browsing Action: Reject Log Alert

No.	Time Occurred	Username	Group	IP Address	App Category	Application	Action	Details
1	11seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Social Contact(We...	Log	URL: www.facebook.com
2	11seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: www.google.com
3	11seconds ago	sangfor	/	192.168.1.3	NET Protocol	WebSocket	Log	
4	11seconds ago	sangfor	/	192.168.1.3	Social Networking	Facebook[Browse]	Log	URL: www.facebook.com/data/manifest/ Website: www.facebook.com
5	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: ogs.google.com
6	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Social Contact(We...	Log	URL: www.facebook.com
7	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: accounts.google.com
8	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: www.google.com
9	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: www.google.com
10	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: www.google.com
11	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: www.google.com
12	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: www.google.com
13	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: www.google.com
14	23seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: www.google.com

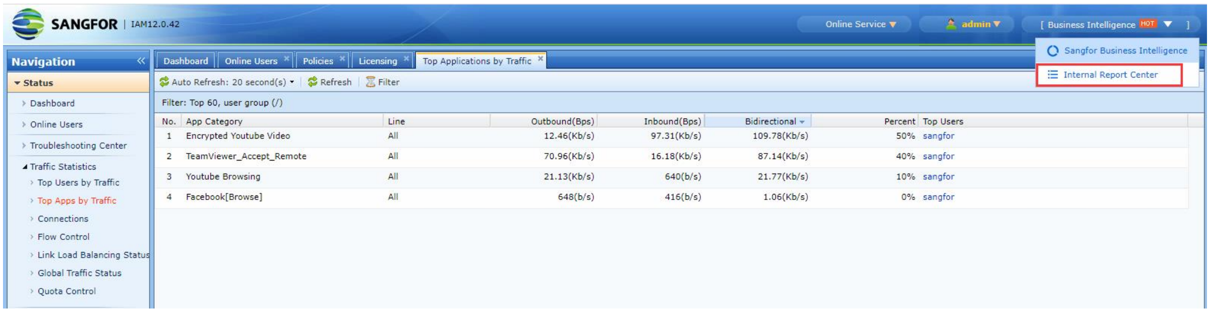
4. You can query the user's traffic ranking data.



Filter: Top 60, user group (/)

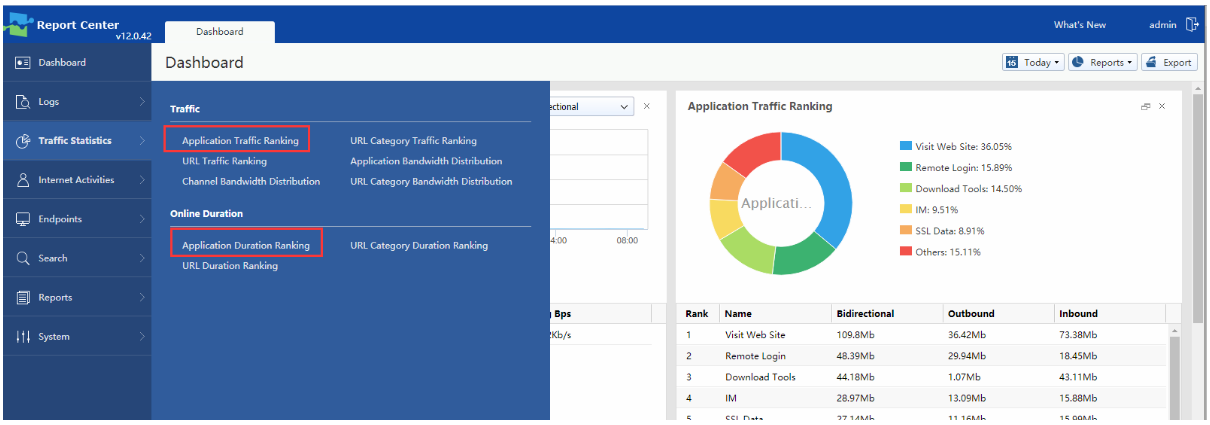
No.	App Category	Line	Outbound(Bps)	Inbound(Bps)	Bidirectional	Percent	Top Users
1	Visit Web Site	All	48.23(Kb/s)	1.02(Mb/s)	1.07(Mb/s)	53%	sangfor
2	Youtube Browsing	All	8.96(Kb/s)	552.54(Kb/s)	561.5(Kb/s)	28%	sangfor
3	Facebook[Browse]	All	4.35(Kb/s)	170.4(Kb/s)	174.75(Kb/s)	9%	sangfor
4	TeamViewer_Accept_Remote	All	104.25(Kb/s)	23.98(Kb/s)	128.23(Kb/s)	6%	sangfor
5	Google Data	All	3.81(Kb/s)	64.53(Kb/s)	68.34(Kb/s)	3%	sangfor

5. You can log in to the log center to view user network behavior and traffic ranking information. Generally, only historical log information can be queried. The recently accessed log can be queried in the data center after a while.

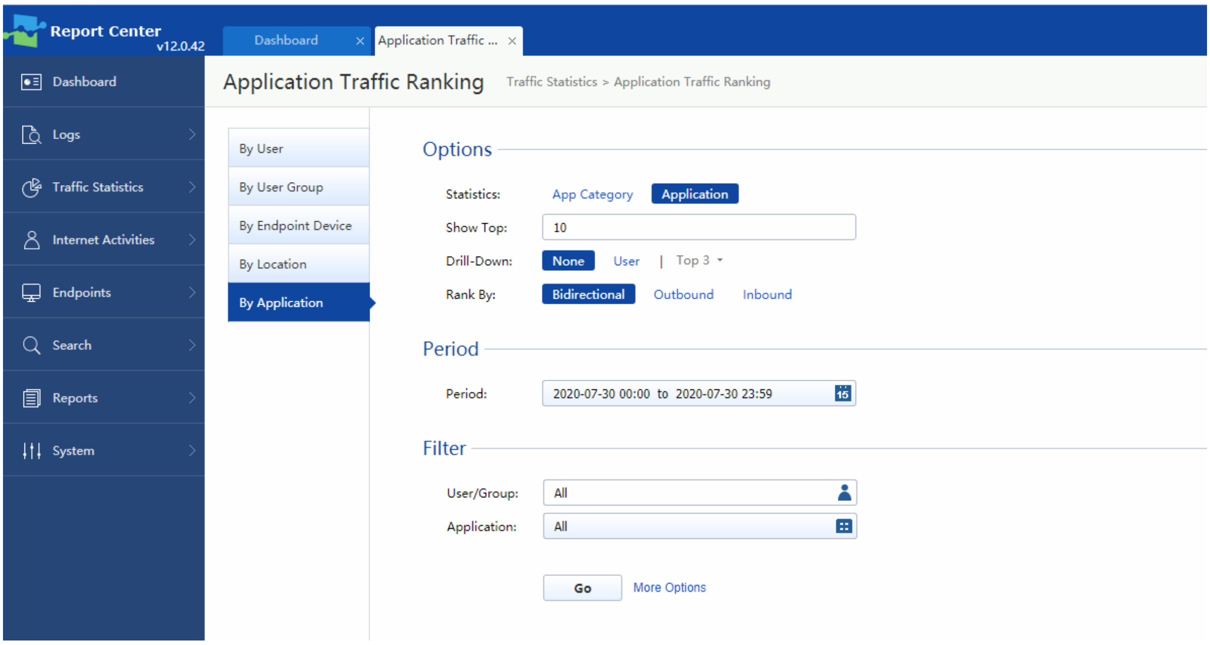


Filter: Top 60, user group (/)

No.	App Category	Line	Outbound(Bps)	Inbound(Bps)	Bidirectional	Percent	Top Users
1	Encrypted Youtube Video	All	12.46(Kb/s)	97.31(Kb/s)	109.78(Kb/s)	50%	sangfor
2	TeamViewer_Accept_Remote	All	70.96(Kb/s)	16.18(Kb/s)	87.14(Kb/s)	40%	sangfor
3	Youtube Browsing	All	21.13(Kb/s)	640(b/s)	21.77(Kb/s)	10%	sangfor
4	Facebook[Browse]	All	648(b/s)	416(b/s)	1.06(Kb/s)	0%	sangfor



Rank	Name	Bidirectional	Outbound	Inbound
1	Visit Web Site	109.8Mb	36.42Mb	73.38Mb
2	Remote Login	48.39Mb	29.94Mb	18.45Mb
3	Download Tools	44.18Mb	1.07Mb	43.11Mb
4	IM	28.97Mb	13.09Mb	15.88Mb
5	SSL Data	27.14Mb	11.16Mb	15.99Mb



Application Traffic Ranking Traffic Statistics > Application Traffic Ranking

Options

Statistics: App Category [✓ Application]

Show Top: 10

Drill-Down: [✓ None] User | Top 3

Rank By: [✓ Bidirectional] Outbound Inbound

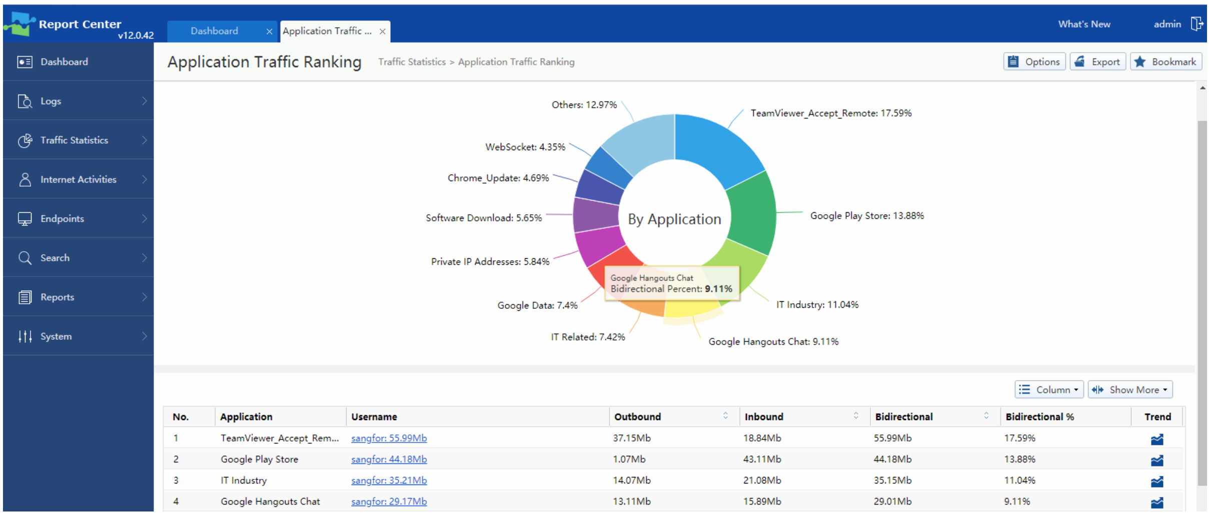
Period

Period: 2020-07-30 00:00 to 2020-07-30 23:59

Filter

User/Group: All

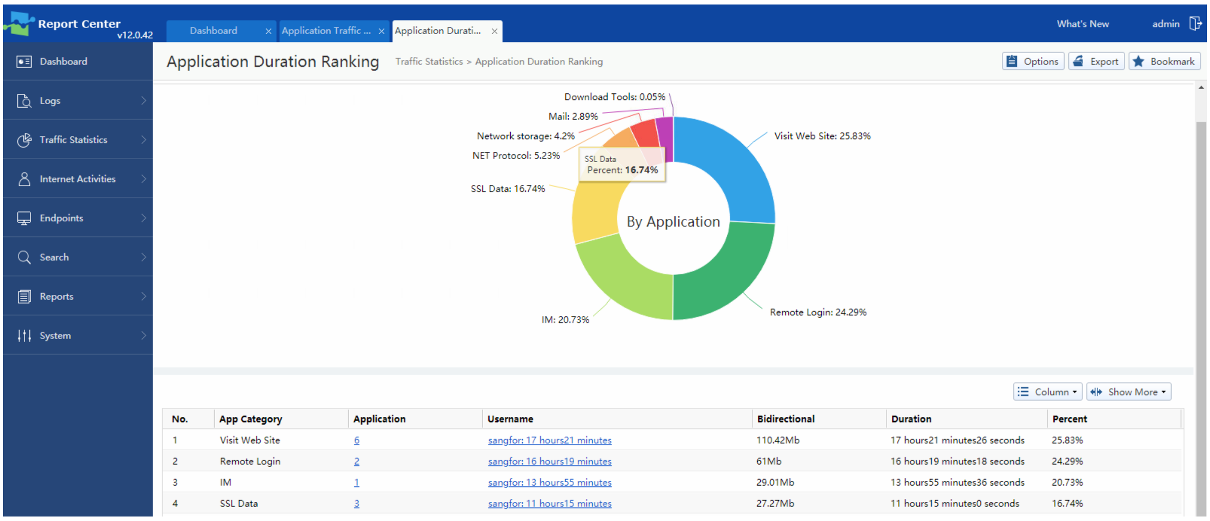
Application: All



Application Traffic Ranking

Traffic Statistics > Application Traffic Ranking

No.	Application	Username	Outbound	Inbound	Bidirectional	Bidirectional %	Trend
1	TeamViewer_Accept_Rem...	sangfor: 55.99Mb	37.15Mb	18.84Mb	55.99Mb	17.59%	
2	Google Play Store	sangfor: 44.18Mb	1.07Mb	43.11Mb	44.18Mb	13.88%	
3	IT Industry	sangfor: 35.21Mb	14.07Mb	21.08Mb	35.15Mb	11.04%	
4	Google Hangouts Chat	sangfor: 29.17Mb	13.11Mb	15.89Mb	29.01Mb	9.11%	



Application Duration Ranking

Traffic Statistics > Application Duration Ranking

No.	App Category	Application	Username	Bidirectional	Duration	Percent
1	Visit Web Site	6	sangfor: 17 hours21 minutes	110.42Mb	17 hours21 minutes26 seconds	25.83%
2	Remote Login	2	sangfor: 16 hours19 minutes	61Mb	16 hours19 minutes18 seconds	24.29%
3	IM	1	sangfor: 13 hours55 minutes	29.01Mb	13 hours55 minutes36 seconds	20.73%
4	SSL Data	3	sangfor: 11 hours15 minutes	27.27Mb	11 hours15 minutes0 seconds	16.74%

SANGFOR

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc