



IAM

Praktik Terbaik untuk Skenario_Audit Policy

Versi 12.0.42



Catatan Perubahan

| Tanggal | Deskripsi Perubahan |
|---------------|------------------------------|
| Juli 27, 2020 | Rilis Dokumen Versi 12.0.42. |
| Mei 17, 2021 | Dokumen updateVersi 12.0.42. |

Daftar Isi

| | |
|--|---|
| Bab 1 Skenario | 1 |
| Bab 2 Pemeriksaan Lingkungan Network | 1 |
| Bab 3 Konfigurasi | 2 |

Bab 1 Skenario

Sebuah Universitas berharap untuk audit perilaku online siswa, termasuk website yang mereka kunjungi dan aplikasi yang mereka gunakan. Selain itu, mereka perlu menganalisis peringkat total traffic dan durasi akses siswa ke berbagai aplikasi.

Bab 2 Pemeriksaan Lingkungan Network

1. Periksa authorization dan versi database untuk memastikan bahwa rule basis telah update ke tanggal terbaru. Aplikasi control policy untuk memproses paket data yang bergantung pada database. Jika database tidak update ke versi terbaru, identifikasi beberapa traffic mungkin salah.

The screenshot displays the Sangfor FWMS interface. The top section shows the 'Licensing' page with various license details:

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

Below this, several license modules are listed:

- Device License:** 1. Max WAN Lines: 2, 2. Max Branch Sites: 2, 3. Max Bandwidth: 100 Mbps. Gateway ID: FD9D8055. License Status: Valid. Expiry Date: 2020-09-23.
- 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.

The bottom section shows the 'Auto Update' page with a table of database updates:

| No. | Database | Current Version | Latest Version | Update Service Expires On | Auto Update | Operation |
|-----|--------------------------------|---|----------------|---------------------------|-------------|-----------|
| 1 | Engine Zero | 2020-06-22 | 2020-07-21 | 2019-01-01 | ✓ | 🔄 |
| 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_hic SP_res 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. Pastikan network traffic melewati perangkat IAM di kedua arah. Jika traffic hanya satu arah, maka aplikasi tidak dapat diidentifikasi dan dikontrol.

The screenshot shows the 'Capture Packets' status window. The status is 'Program is running.' Below it, there is a table with columns: No., Name, Size, Download, and Delete. Two packets are listed:

| No. | Name | Size | Download | Delete |
|-----|-------------------------------------|------------|----------|--------|
| 1 | 2020-07-27-143016_ath0_tcpdump.pcap | 360(KB) | Download | X |
| 2 | 2020-07-27-143016_ath2_tcpdump.pcap | 874.62(KB) | Download | X |

Below the status window, there is a packet capture log table with columns: No., Time, Source, Destination, Protocol, Length, Bytes in Flight, and Info. The log shows various network events including TCP connections, TLSv1.2 sessions, and alerts.

| 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 14:30:40.044802 | 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 |

Bab 3 Konfigurasi

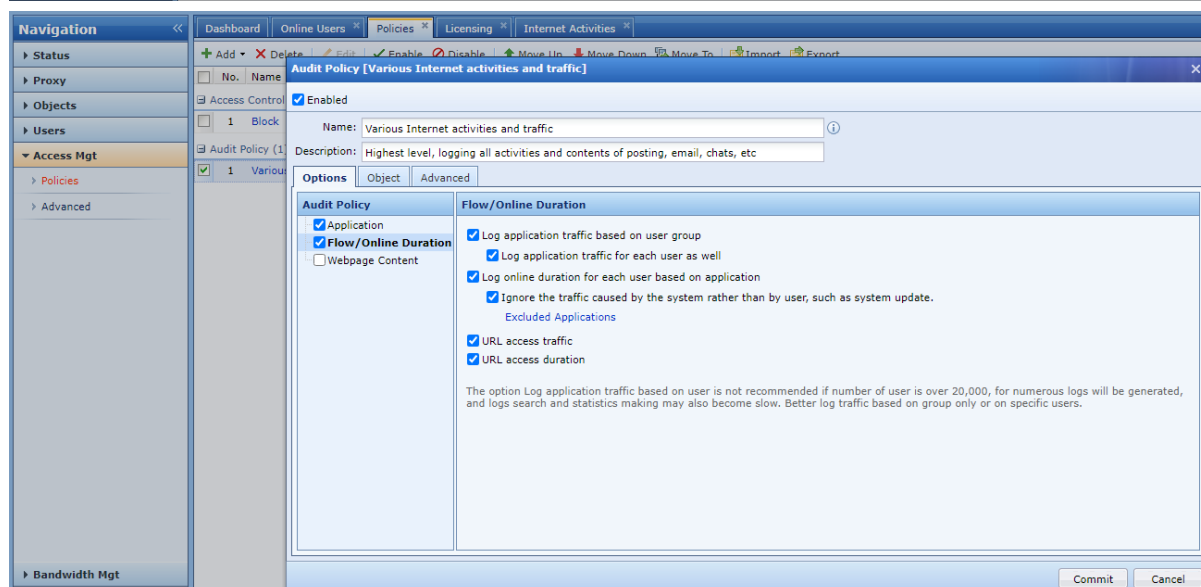
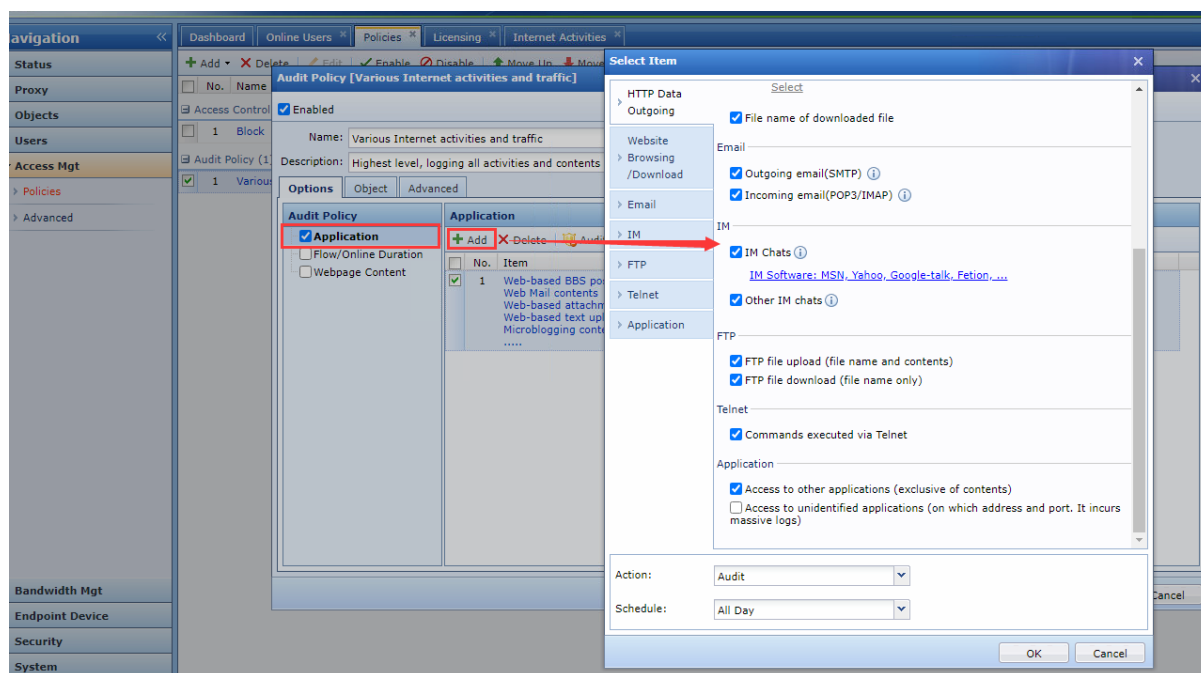
1. Konfigurasi policy dan periksa content yang perlu diaudit, seperti perilaku aplikasi, traffic, dan web content.

The screenshot shows the 'Policies' tab in the Sangfor Firewall Management Console. The 'Add' button is highlighted, and a dropdown menu is open showing various policy types. The 'Audit Policy' option is selected and highlighted with a red box.

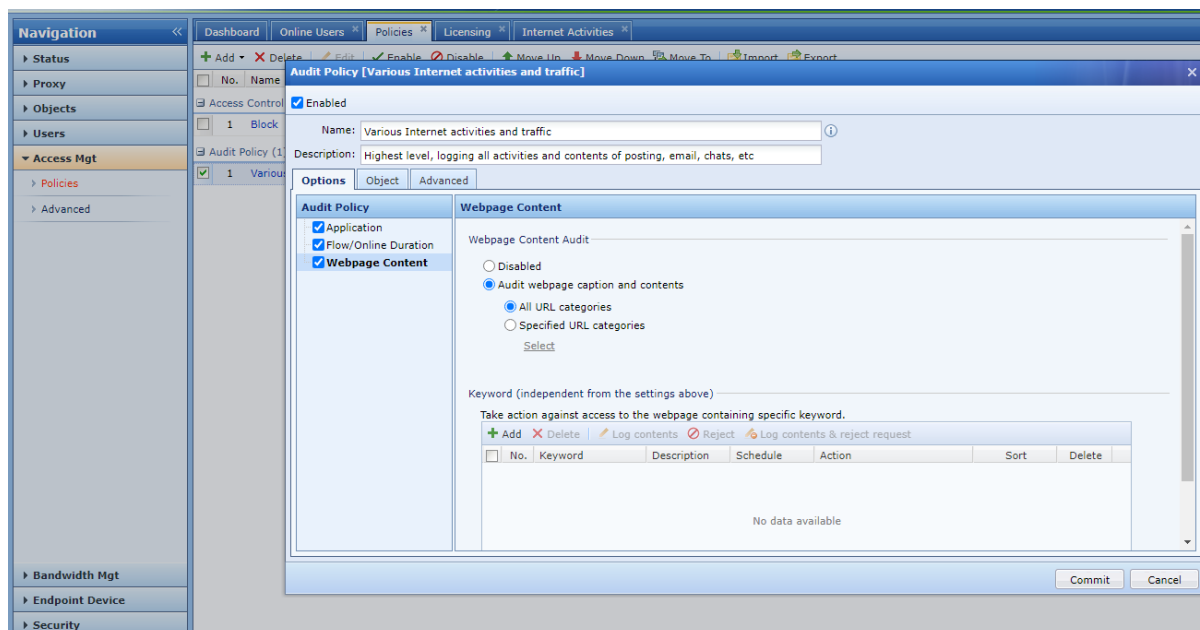
| Policy Name | Applicable Users | Applicable AP(Group) |
|---------------------|------------------|----------------------|
| Test | All | All |
| Internet Activities | All users | All |

Ketika Audit perilaku aplikasi, perlu dicatat bahwa Anda biasanya perlu periksa "Access to other applications (exclusive of contents)", karena ada banyak kategori aplikasi, dan option di atas option ini hanyalah beberapa kategori yang umum digunakan, dan sebagian besar rule basis aplikasi termasuk dalam option ini. Biasanya, "Access to unidentified applications (on which address and port. It incurs massive logs)" tidak diperiksa, karena akan menyebabkan sejumlah besar log.

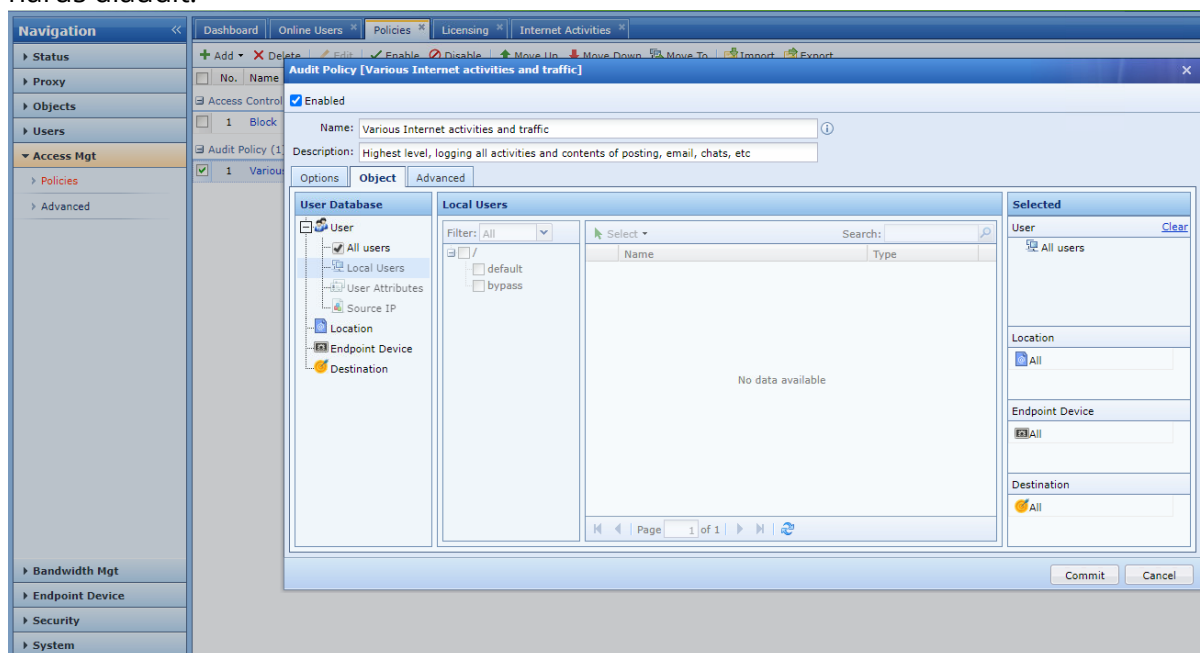
Audit Policy



Audit Policy



2. Pilih target untuk policy dan menentukan perilaku pengguna mana dan traffic yang harus diaudit.



3. Lihat perilaku pengguna di "Internet Activities". Jika Anda ingin filter perilaku pengguna sebanyak mungkin, Anda perlu memeriksa "Others" di filter, karena selain kategori aplikasi umum lainnya seperti Mail, adalah rules milik "Others".

Audit Policy

Filter Dialog:

- Type: ☒ User group
- Object: ☒ Search term, ☒ Email, ☒ IM chats, ☒ Others, ☒ Forum & Microblogging, ☒ Outgoing Files, ☒ Website Browsing
- Action: ☒ Reject, ☒ Log, ☒ Alert

Main Table:

| 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 | / | Search Engine | Log | URL: www.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: www.google.com |
| 14 | 10seconds ago | sangfor | / | Search Engine | Log | URL: www.google.com |
| 15 | 1 minutes ago | sangfor | / | Search Engine | Log | URL: www.google.com |
| 16 | 1.5 minutes ago | sangfor | / | Search Engine | Log | URL: www.google.com |
| 17 | 1.5 minutes ago | sangfor | / | Search Engine | Log | URL: www.google.com |
| 18 | 1.5 minutes ago | sangfor | / | Search Engine | Log | URL: www.google.com |
| 19 | 1.5 minutes ago | sangfor | / | Search Engine | Log | URL: www.google.com |
| 20 | 1.5 minutes ago | sangfor | / | Search Engine | Log | URL: www.google.com |
| 21 | 1.5 minutes ago | sangfor | / | Search Engine | Log | URL: www.google.com |
| 22 | 1.5 minutes ago | sangfor | / | Search Engine | Log | URL: www.google.com |
| 23 | 1.5 minutes ago | sangfor | / | Search Engine | Log | URL: www.google.com |

4. Anda dapat queri pengguna traffic ranking data.

Filter Dialog:

- Type: ☒ Top 60, user group (/)

Main Table:

| 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 |

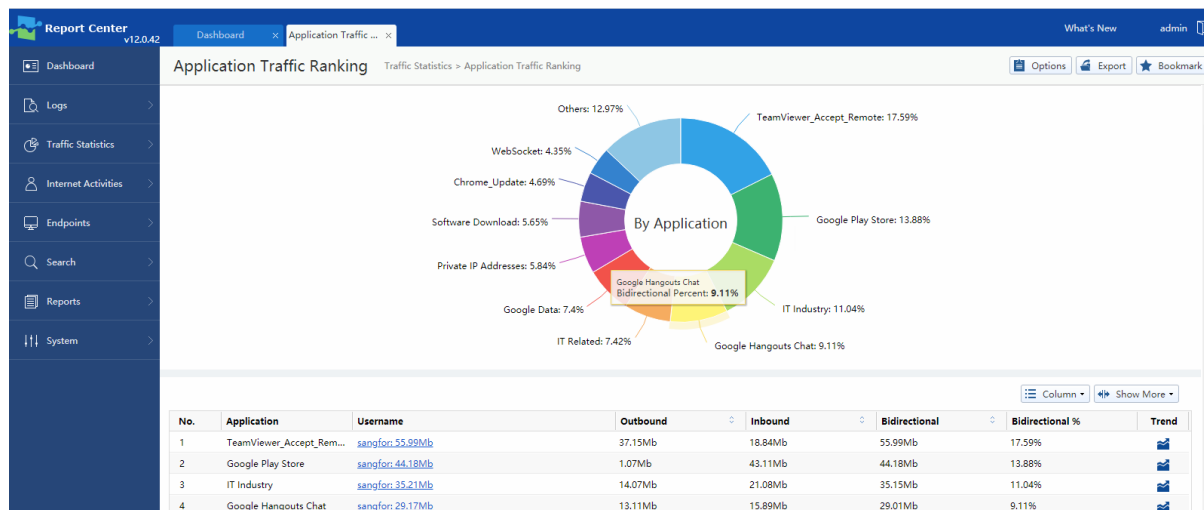
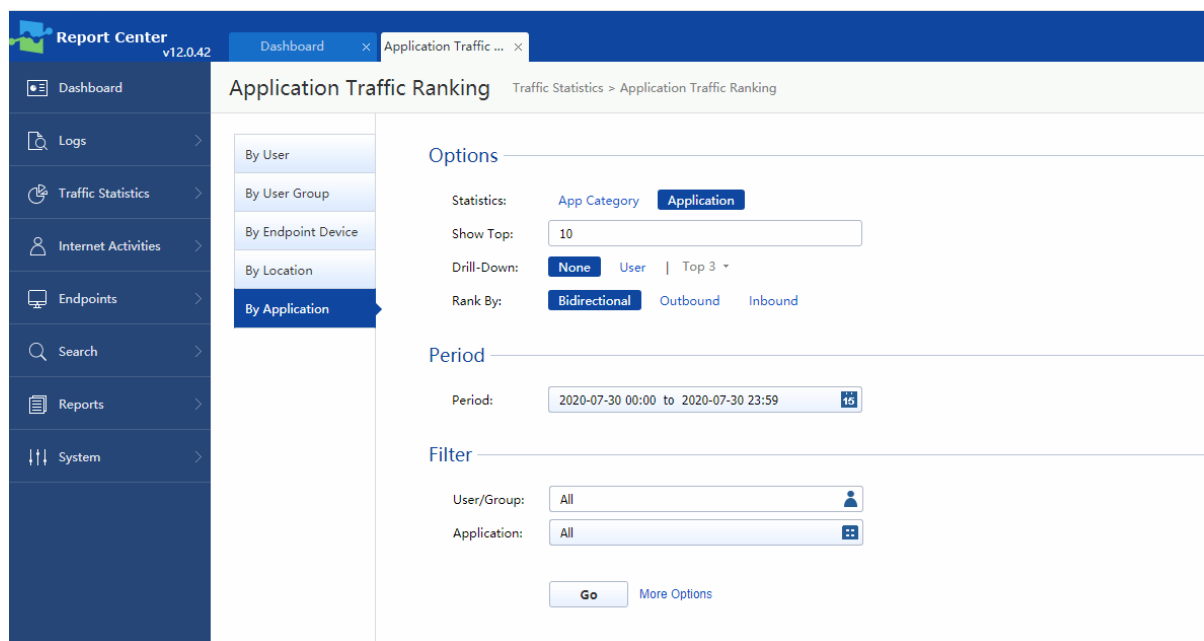
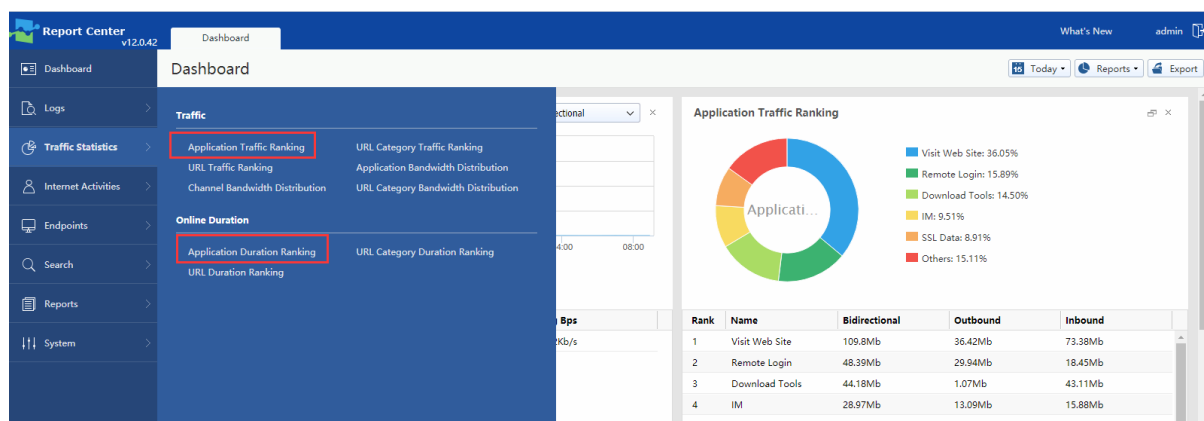
5. Anda dapat log in ke log center untuk melihat perilaku network pengguna dan informasi peringkat traffic. Umumnya, hanya informasi historis log yang dapat di queri. Log yang baru-baru ini diakses dapat diqueri di data center setelah beberapa saat.

Filter Dialog:

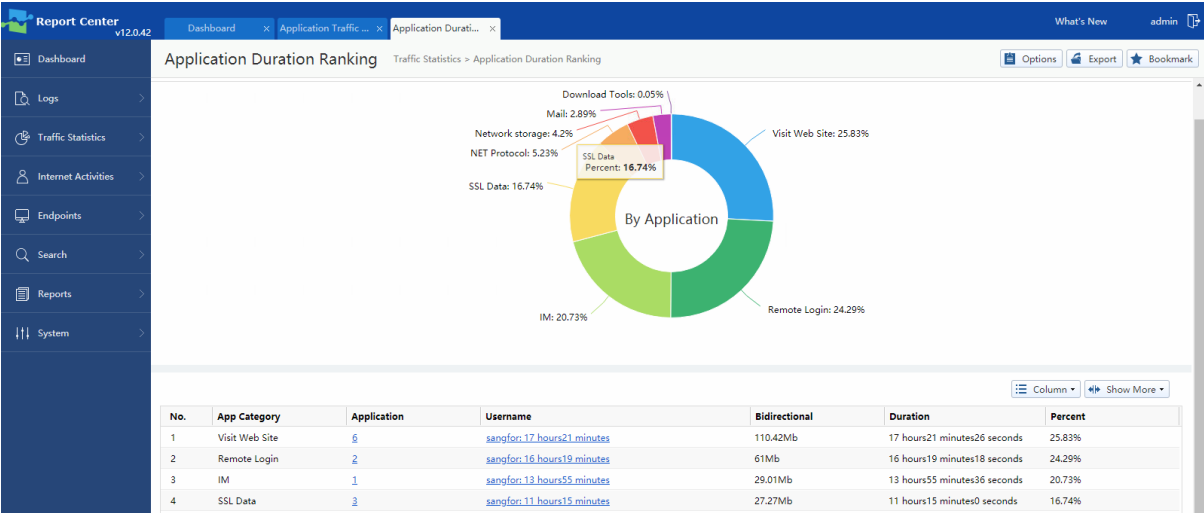
- Type: ☒ Top 60, user group (/)

Main Table:

| 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 |



Audit Policy





SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

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