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.

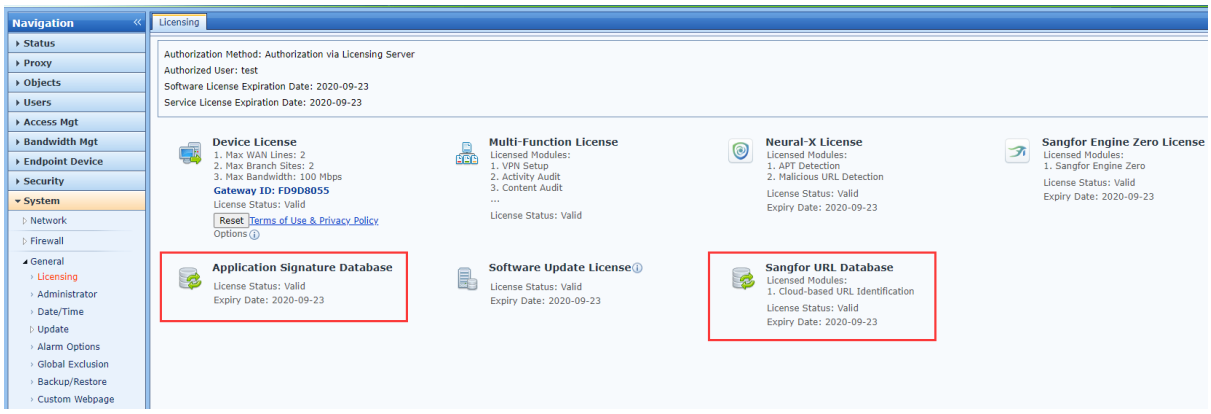
Daftar Isi

Bab 1 Skenario

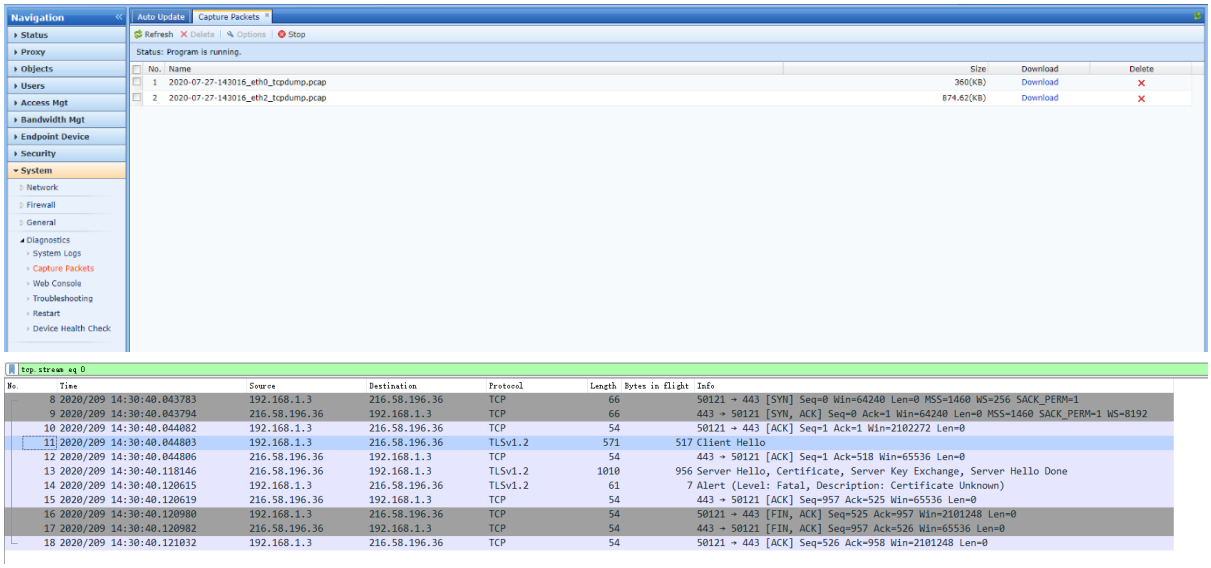
Sebuah Universitas berharap untuk audit perilaku online siswa, termasuk website yang mereka kunjungi dan aplikasi yang mereka gunakan. Selain itu, mereka perlu menganalisis peringkat total traffic dan durasi akses siswa ke berbagai aplikasi.

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.

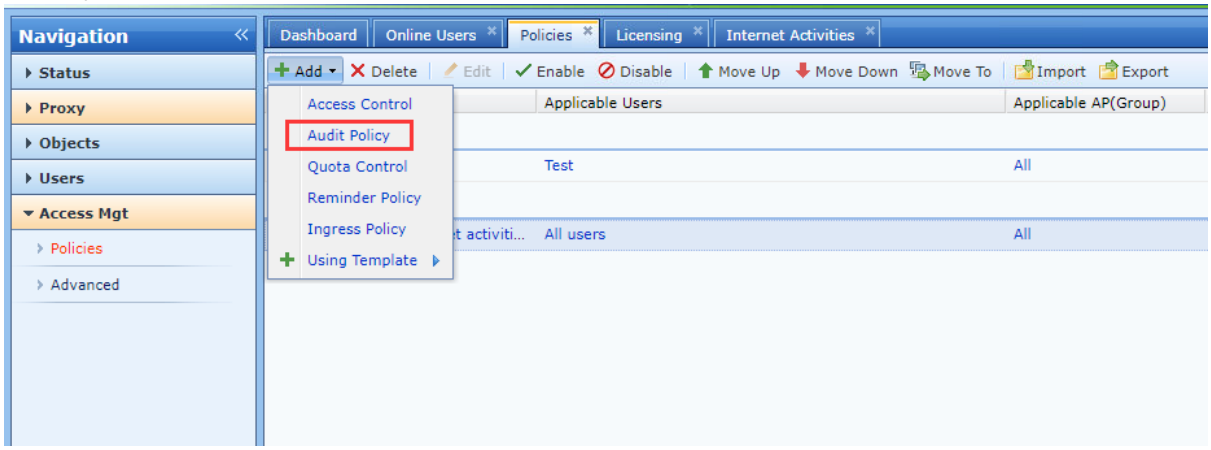


2. Pastikan network traffic melewati perangkat IAM di kedua arah. Jika traffic hanya satu arah, maka aplikasi tidak dapat diidentifikasi dan dikontrol.



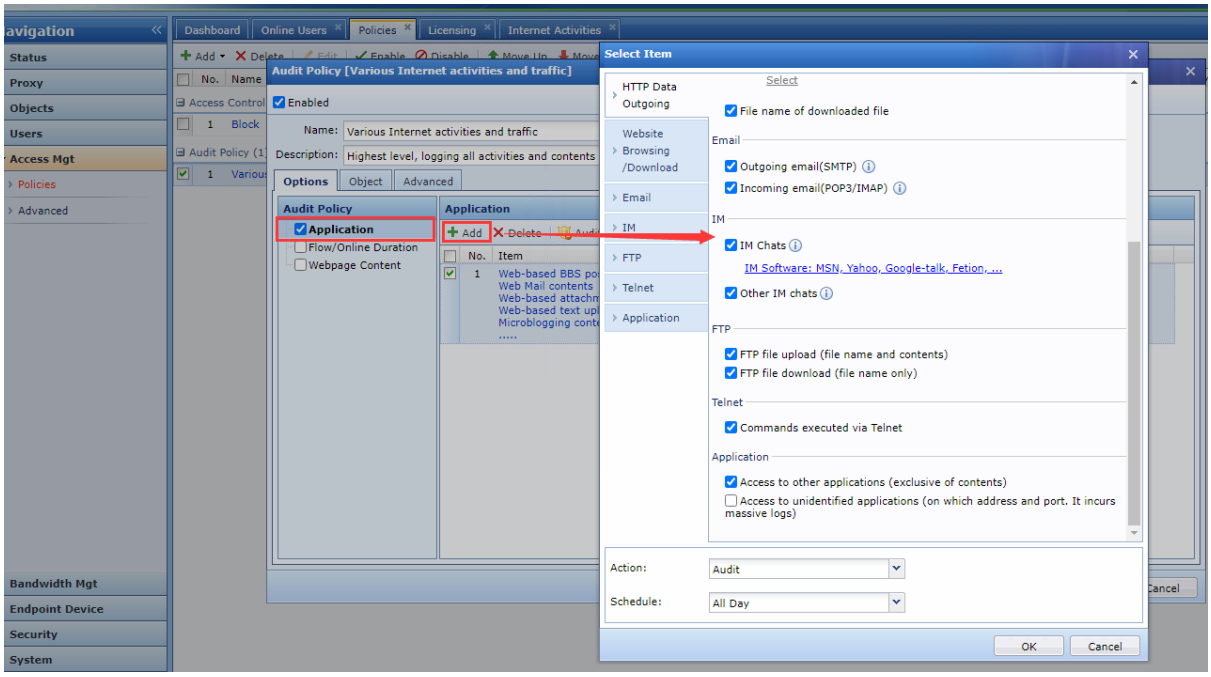
Bab 3 Konfigurasi

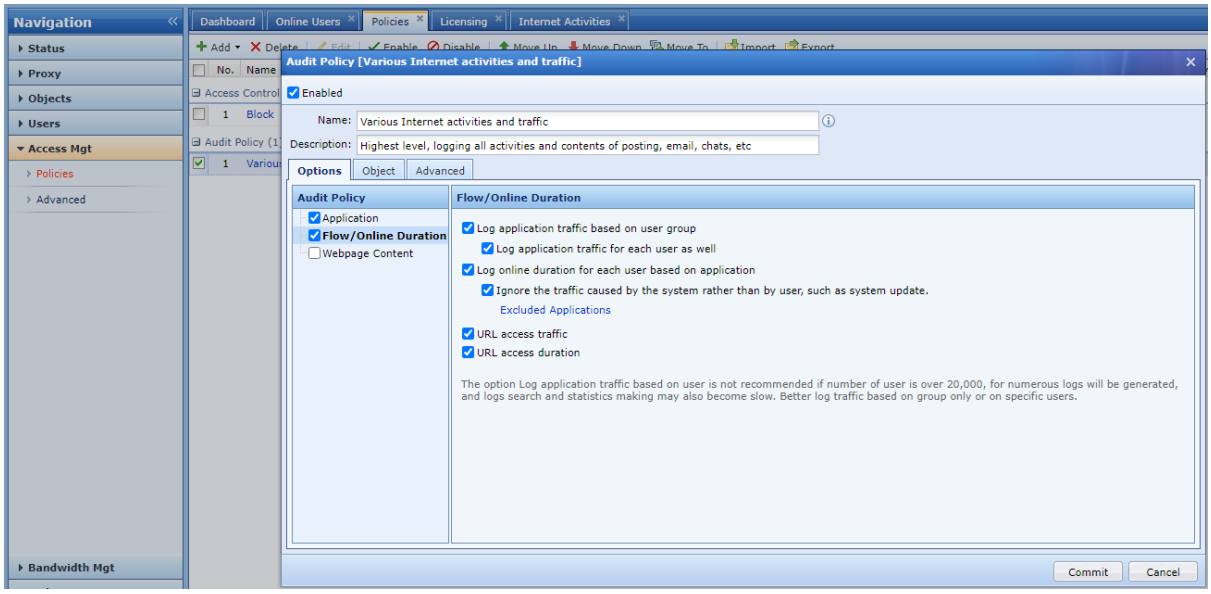
1. Konfigurasi policy dan periksa content yang perlu diaudit, seperti perilaku aplikasi, traffic, dan web content.

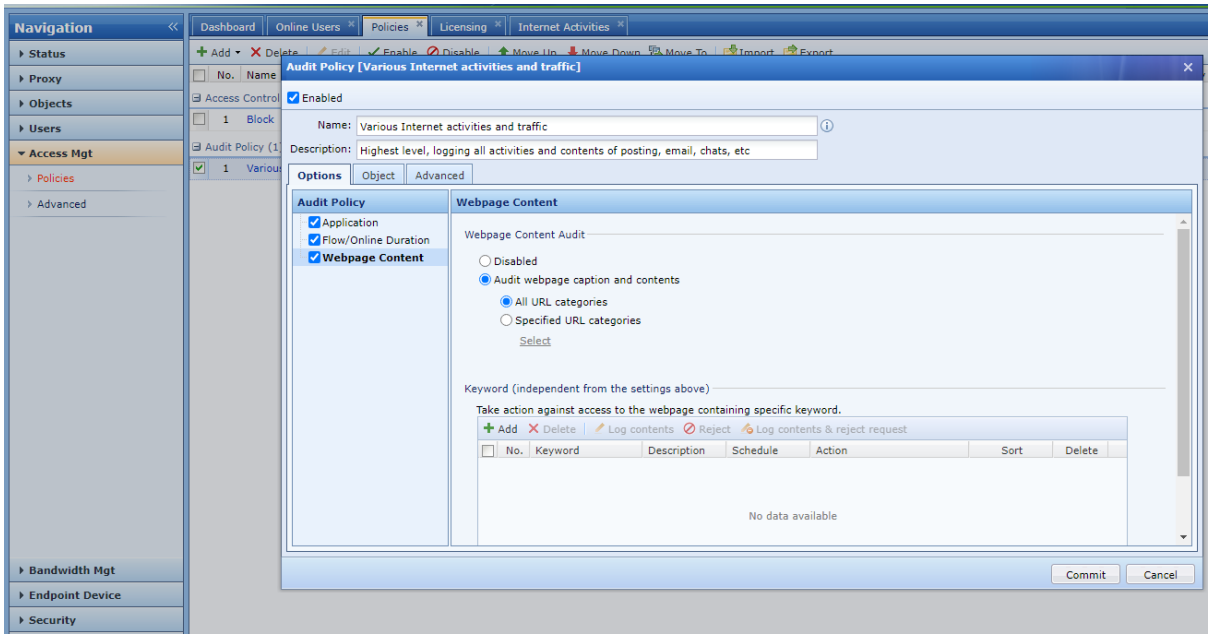


Ketika Audit perilaku aplikasi, perlu dicatat bahwa Anda biasanya perlu periksa "Access to other applications (exclusive of contents)", karena ada banyak kategori aplikasi, dan option di atas option ini hanyalah beberapa kategori yang umum digunakan, dan sebagian besar rule basis aplikasi termasuk dalam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

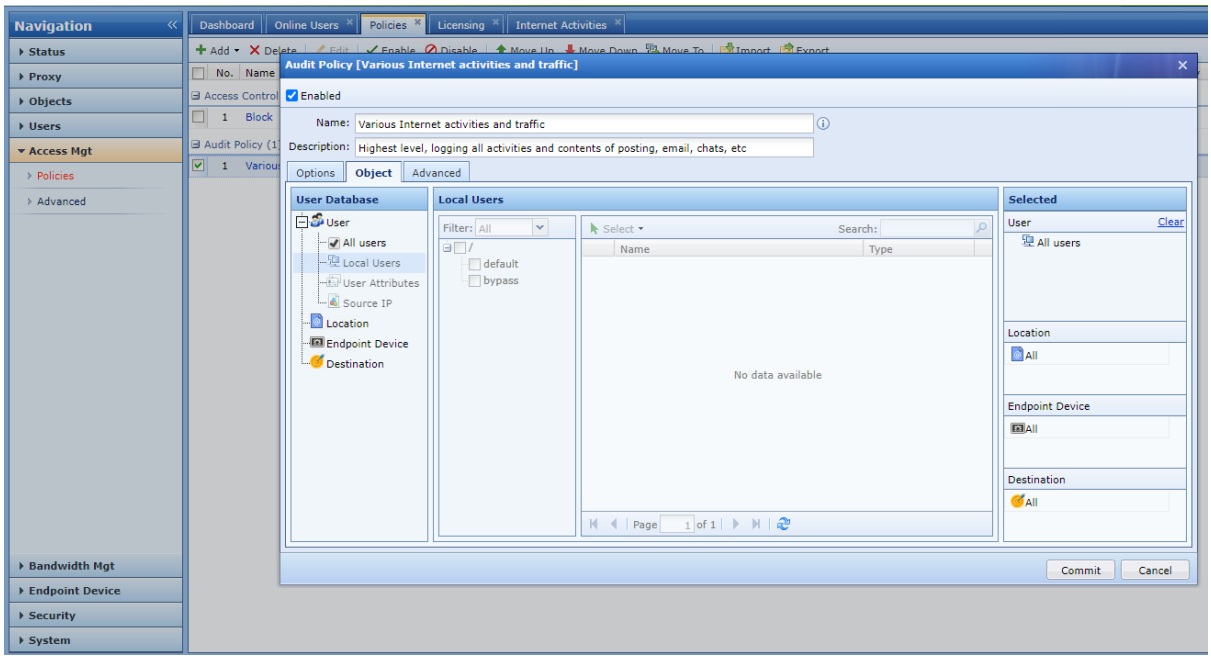
Audit Policy



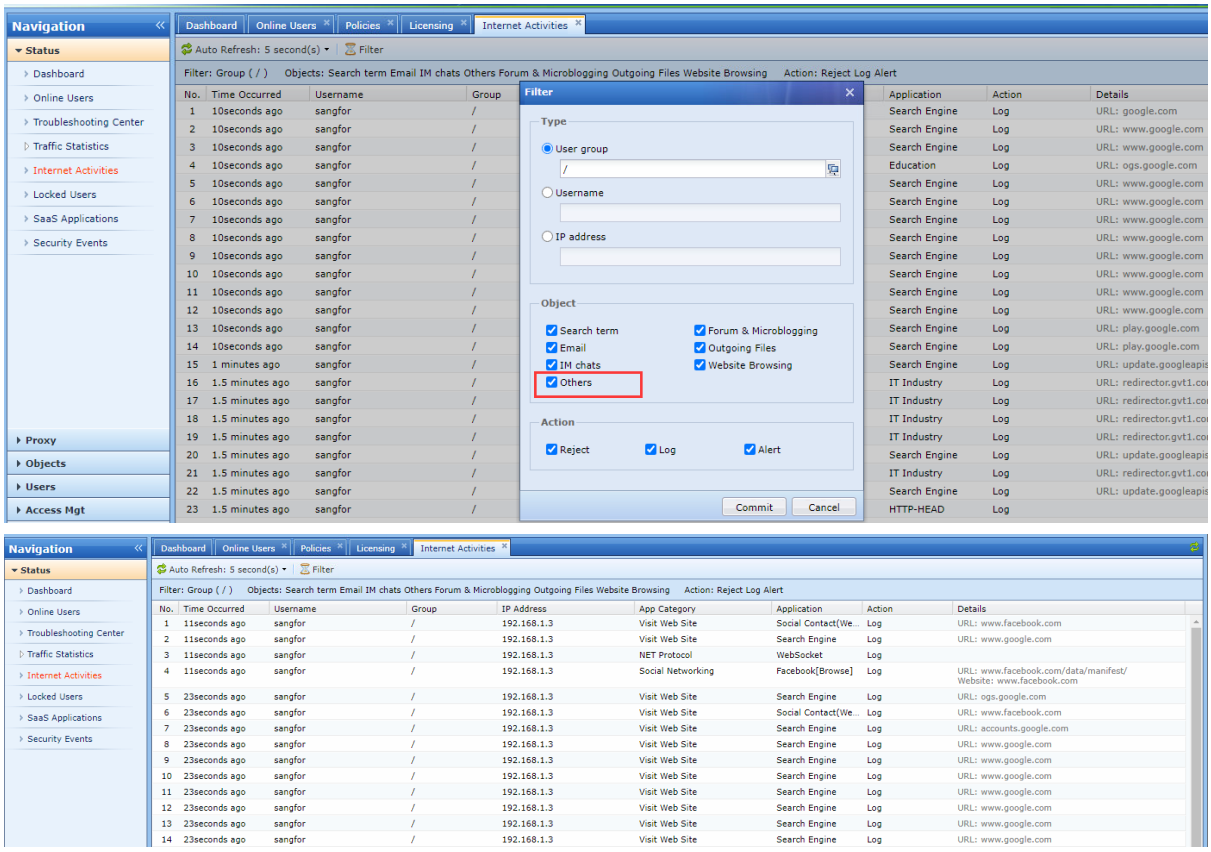




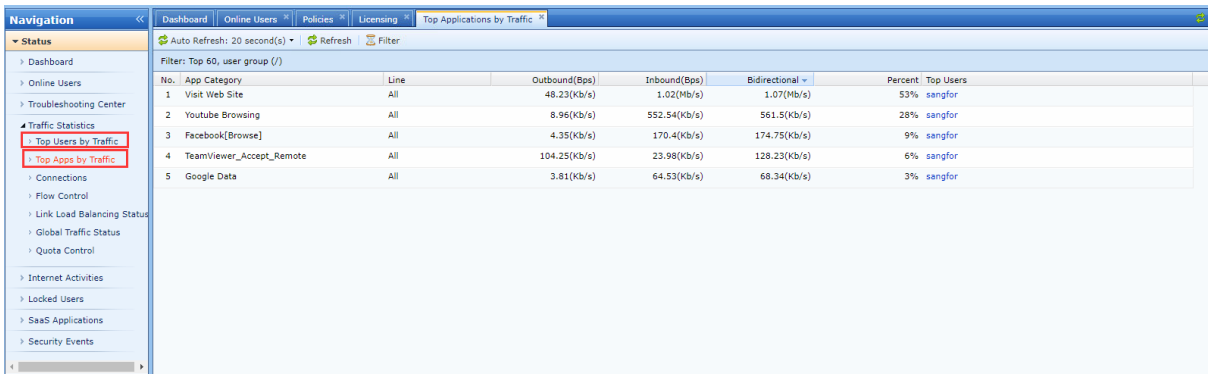
2. Pilih target untuk policy dan menentukan perilaku pengguna mana dan traffic yang harus diaudit.



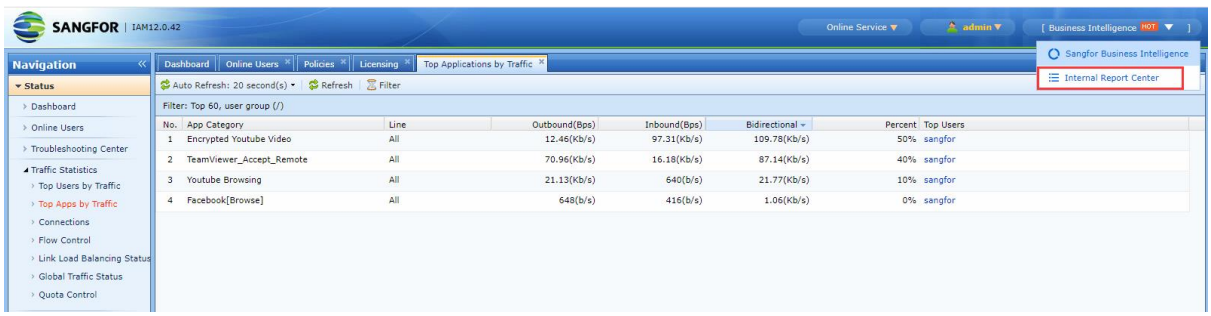
3. Lihat perilaku pengguna di "Internet Activities". Jika Anda ingin filter perilaku pengguna sebanyak mungkin, Anda perlu periksa "Others" di filter, karena selain kategori aplikasi umum lainnya seperti Mail, adalah rules milik "Others".



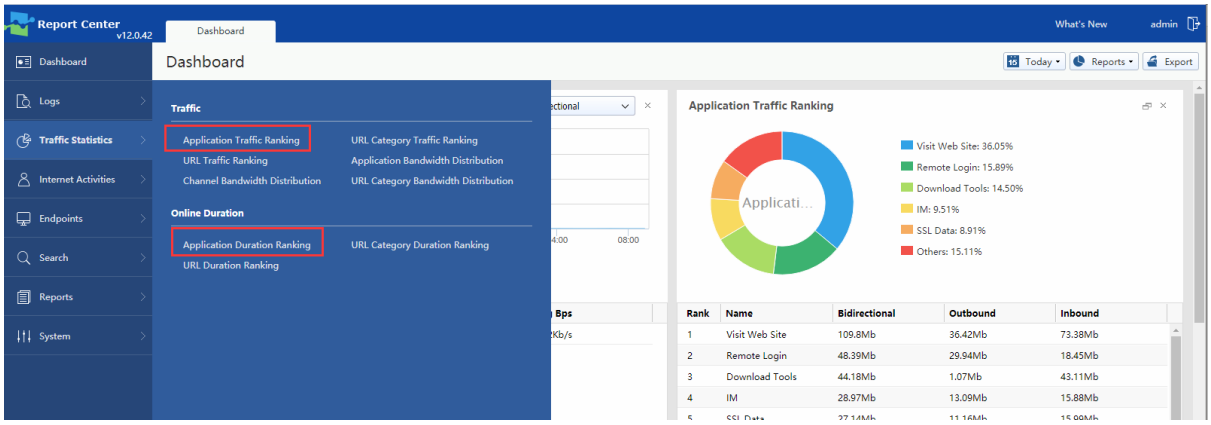
4. Anda dapat queri pengguna traffic ranking data.

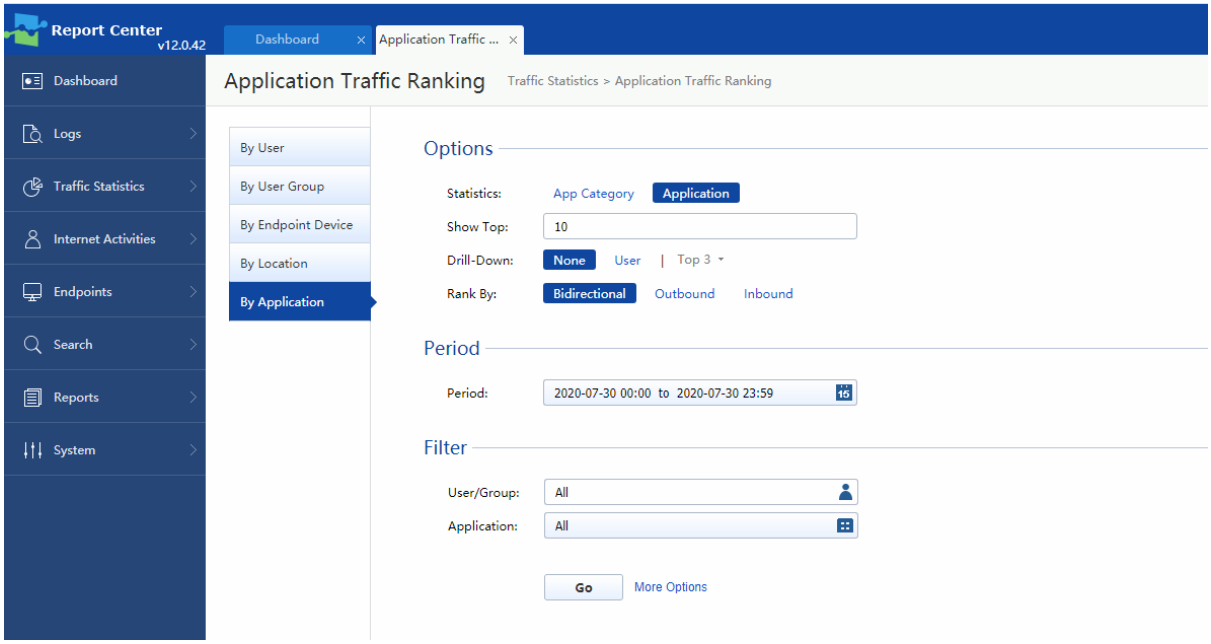


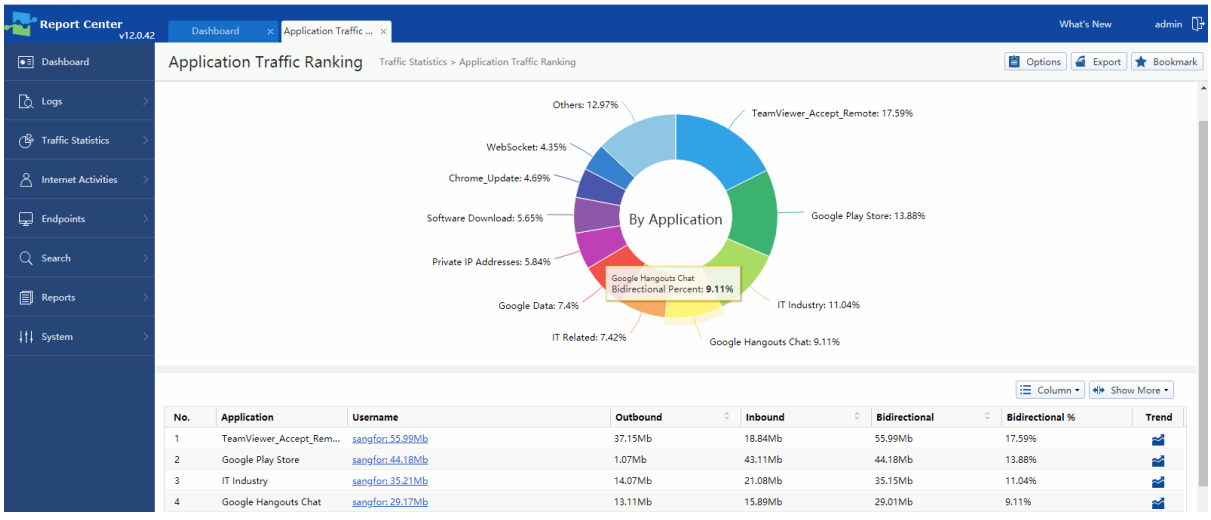
5. Anda dapat log in ke log center untuk melihat perilaku network pengguna dan informasi peringkat traffic. Umumnya, hanya informasi historis log yang dapat di queri. Log yang baru-baru ini diakses dapat diqueri di data center setelah beberapa saat.



Audit Policy







Audit Policy