SANGFOR

IAG

Panduan Konfigurasi Ingress Client SSL Decryption

Versi 13.0.15

Catatan Perubahan

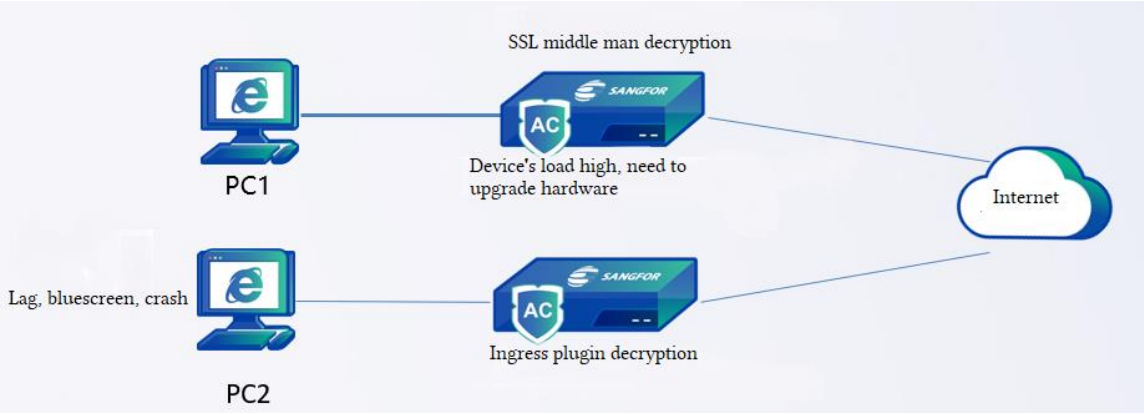
Tanggal	Deskripsi Perubahan
September 9, 2020	Rilis Dokumen Versi 13.0.15.

Daftar Isi

Bab 1 Latar Belakang Permintaan

1. Tradisional middleman decryption memiliki dampak besar pada kinerja perangkat, mengharuskan perusahaan untuk upgrade dan mengganti perangkat IAG, yang sangat meningkatkan biaya tata kelola SSL perusahaan, tetapi ada banyak risiko kebocoran data tanpa decryption.

2. Plugin IAG tradisional metode decryption terutama menggunakan global proxy untuk audit https. Solusi ini terbatas pada versi dan tipe browser, yang dapat menyebabkan masalah kompatibilitas seperti blue screen dan ketidakstabilan sistem, dan tidak mendukung http2.0.



Bab 2 Penjelasan Fitur

2.1 Pengantar

- Ingress client decryption menggantikan metode ingress plug-in decrypt untuk mencapai high-through decryption, install ingress client tanpa persepsi, dan decrypt dengan kompatibilitas yang lebih tinggi.

- Prinsip: Proxy traffic PC yang menjelajahi Internet berinteraksi dengan server melalui plugin, dan secara langsung mengekstrak master session key dari level sistem decryption. Saat ini, terminal proxy didadaptasi ke windows, dan ingress client proxy digunakan untuk memodifikasi paket data untuk mensimulasikan fungsi NAT, sehingga untuk mencapai fungsi dasar dari proxy semua koneksi TCP/UDP pada windows, dan menerapkan SSL middleman proxy, SOCKS proxy dan fungsi lainnya atas dasar ini.

- Catatan: Program proxy adalah bagian dari ingress program dan tidak mendukung uninstallasi terpisah. Itu juga akan diuninstal saat uninstal ingress.

2.2 Penjelasan

- Jika proxy semua SSL traffic dapat menyebabkan masalah kompatibilitas, dalam versi ini, client decryption hanya berfokus pada proses tertentu untuk proxy traffic.

- Proxy client hanya melakukan decryption pada web browser tertentu dan aplikasi lain yang

mendukung audit.

- Saat ini hanya mendukung 34 aplikasi yang ditambahkan ke daftar decryption (21 web browsers, 11 aplikasi kebocoran Data, 2 aplikasi proxy):

Application Type	Application name
Web Browser	Chrome
Web Browser	Firefox
Web Browser	IE 8
Web Browser	IE 9
Web Browser	IE 10
Web Browser	IE 11
Web Browser	Edge
Web Browser	Sogou web browser
Web Browser	360 Web Browser
Web Browser	QQ Web Browser
Web Browser	Maxthon **Web browser**
Web Browser	CM Browser
Web Browser	Opera Web browser
Web Browser	UC web browser

Application Type	Application Name
Web Browser	Chromium
Web Browser	Brave
Web Browser	Maxthon Cloud Browser
Web Browser	Torch
Web Browser	Vivaldi
Web Browser	Tor Browser
Web Browser	Epic Privacy Browser

Application Type	Application Name
Data Leak risk	Baidu Wangpan
Data Leak risk	Evernote
Data Leak risk	Youdao Note
Data Leak risk	YunZhiJia
Data Leak risk	NetEase Tunder mail
Data Leak risk	QQ – WeiYun
Data Leak risk	115
Data Leak risk	DingPan
Data Leak risk	DingDing Mail
Data Leak risk	Microsoft-onedrive
Data Leak risk	Itunes

Application Type	Application Name
Proxy Software	CC proxy
Antivirus	Rising Antivirus

- **Menambah dukungan bagi protokol HTTP 2.0 (tradisional ingress client decryption hanya mendukung HTTP 1.0 dan protokol HTTP 1.1).**

1. Program proxy downgrade protokol HTTP 2.0 ke data protokol HTTP 1.1 .

2. Berdasarkan protokol TLS 1.3 saat ini, akan digunakan sebagai konjungsi dengan HTTP 2.0, jadi TLS 1.3 juga akan downgrade.

3. Jika downgrade gagal, server akan terhubung kembali. Setelah koneksi ulang berhasil, itu akan melakukan SSL handshake dengan server lagi dan mengatur hal yang sama seperti paket original client hello untuk mencapai transparent proxy yang sebenarnya , yaitu, program proxy tidak memodifikasi paket data, memastikan bahwa network PC tidak terganggu.

- **Ditambahkan proses fungsi daftar decryption.**

1. Tambah proses daftar decryption untuk memfasilitasi pengguna untuk menentukan aplikasi untuk decryption.

2. Kustom proses exclusion saat ini hanya berlaku untuk aplikasi yang memerlukan proxy decryption. (Misalnya, menambahkan browser chrome ke daftar proses kustom exclude tidak akan decrypt data chrome).

3. Daftar proses decryption perlu disesuaikan di backend (artinya, tambah proses/aplikasi yang memerlukan proxy decryption, jika tidak, hanya 34 aplikasi default yang akan di decrypt).

2.3 Perbandingan Tiga Metode Decryption

	Ingress Client	Decryption Method	Pros and cons	Application Scenarios
Ingress client decryption	Needed	Ingress client Transparent proxy Replace certificate	Good compatibility. The decryption throughput rate is high. Richer audit content. Low consumption of IAM performance, support http2.0. Can do decryption for specified software applications. Currently only supports WINDOWS system.	Applied to routing/bridge/by pass mode, IAM audits SSL protocol data through the client.
Ingress plugin decryption	Needed	Ingress client Intercept certificate	Low consumption of IAM performance. Poor compatibility, http2.0 is not supported. Only supports WINDOWS system. Does not support the specified process for decryption.	Mainly used in bypass mode, IAM audits SSL protocol data through the client.
SSL middleman decryption	Not needed	Proxy access Replace certificate	No restrictions on the operating system. No compatibility issues. Low decryption throughput rate. High consumption of IAM performance. Does not support the specified process for decryption.	Mainly used in bridge/routing mode, the middleman audits the SSL protocol data between the endpoint and the server.

Bab 3 Skenario Aplikasi

Ingress client adalah terutama digunakan di perusahaan yang memiliki banyak website dan persyaratan aplikasi decryption dan dapat menerima instalasi software ingress, yang dapat mencapai high-throughput decryption dan sangat mengurangi beban pada perangkat IAG .

Bab 4 Konfigurasi

4.1 Langkah Konfigurasi:

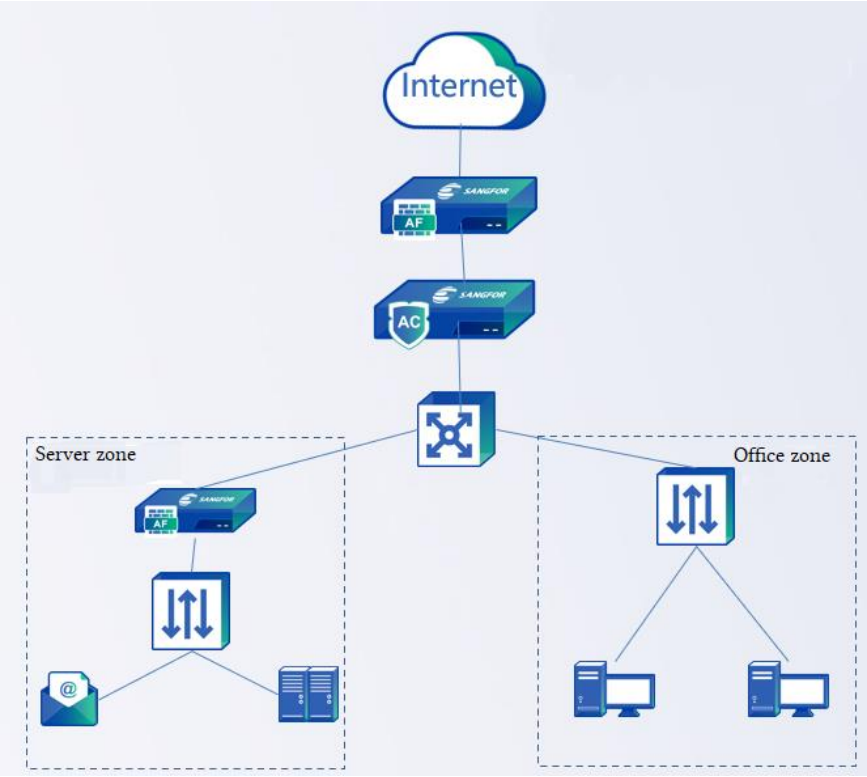
1. Fungsi pengingat installasi ingress diaktifkan pada IAG (diaktifkan secara default).

2. Endpoint PC instal ingress client, online pada IAG, dan memelihara konektivitas network dengan IAG.

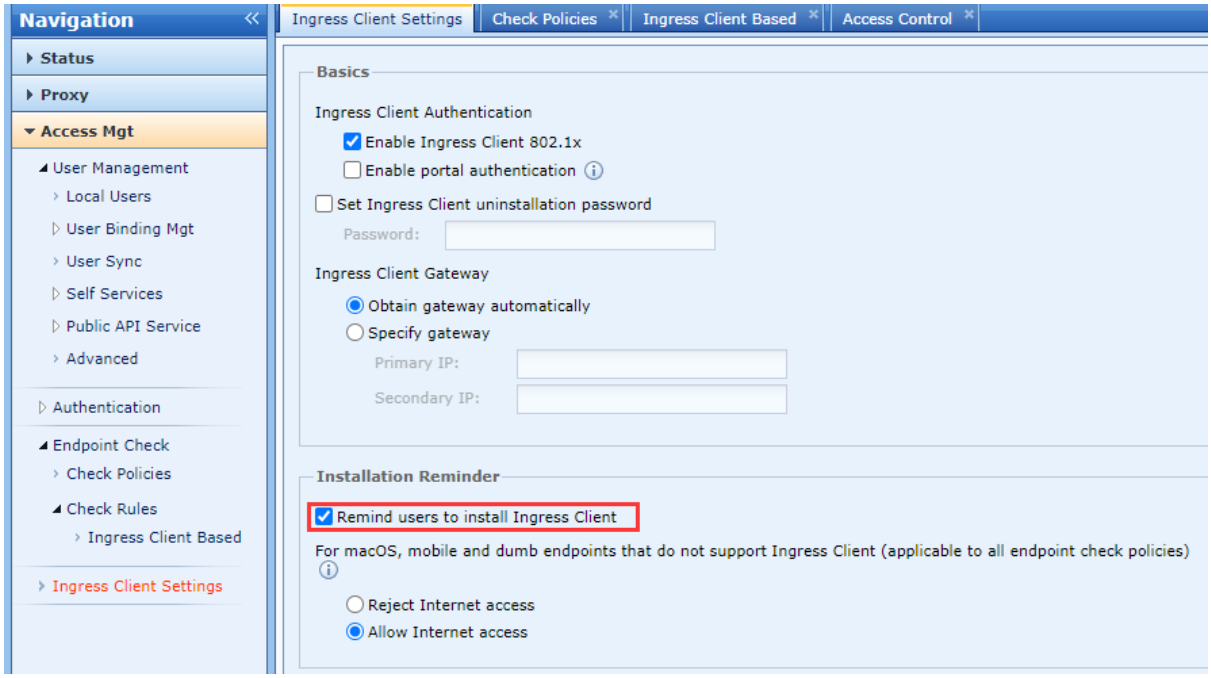
3. Aktifkan fungsi ingress client decryption di IAG **[Access Control] - [SSL Decryption] - [Ingress Client Decryption]**.

4.2 Kasus Konfigurasi:

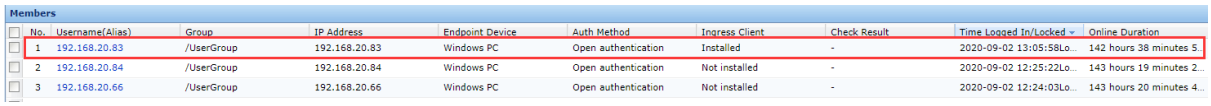
Baru-baru ini, telah terjadi insiden kebocoran data di perusahaan B. Untuk keamanan informasi perusahaan, perusahaan B mengharuskan mereka untuk audit traffic internet (termasuk data https) dari internal endpoints untuk mengurangi risiko karyawan internal membocorkan informasi melalui internet. Hardware IAG sudah tua tetapi saat ini perusahaan B tidak ingin mengganti perangkat.



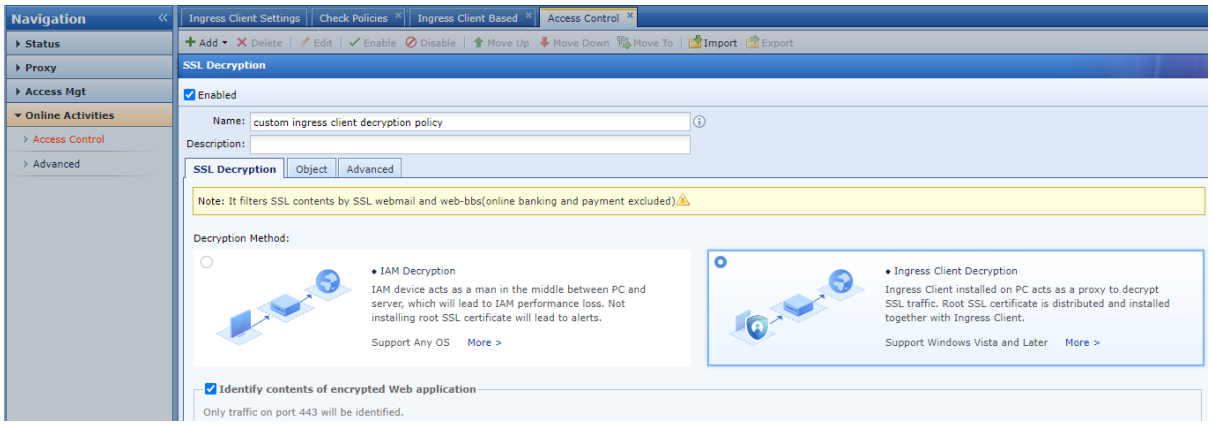
1. Aktifkan fungsi pengingat instalasi ingress pada IAG (diaktifkan secara default).

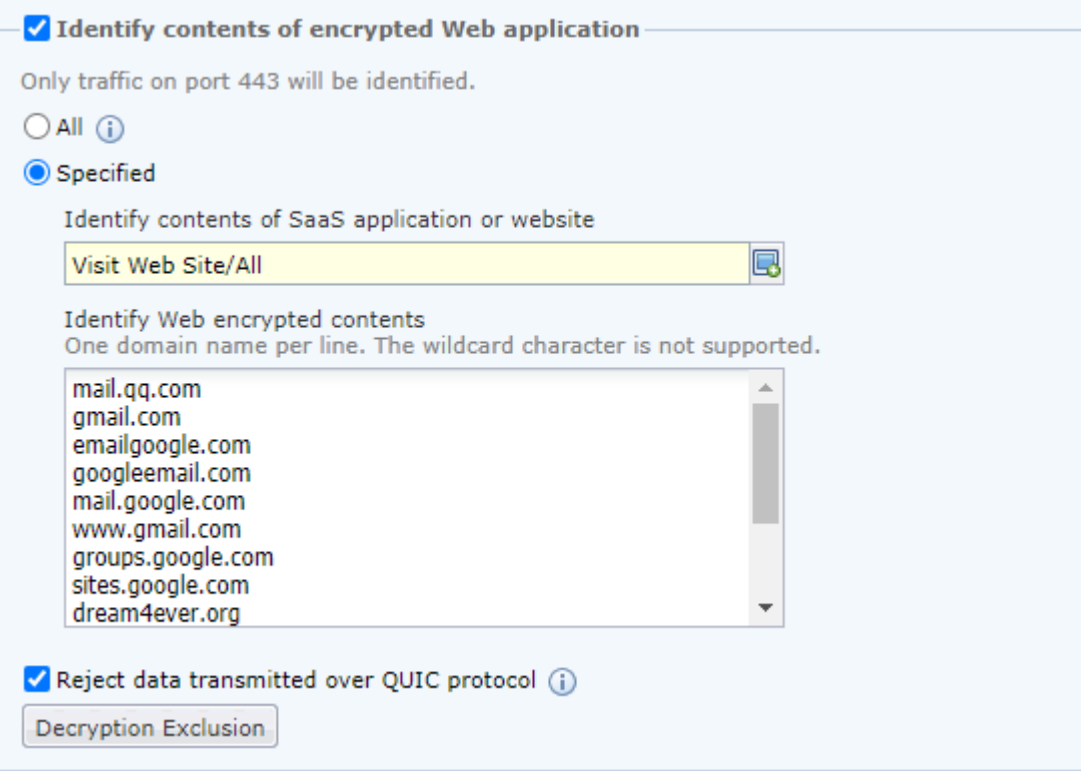


2. Pastikan bahwa pengguna online di IAG dan instal ingress client:

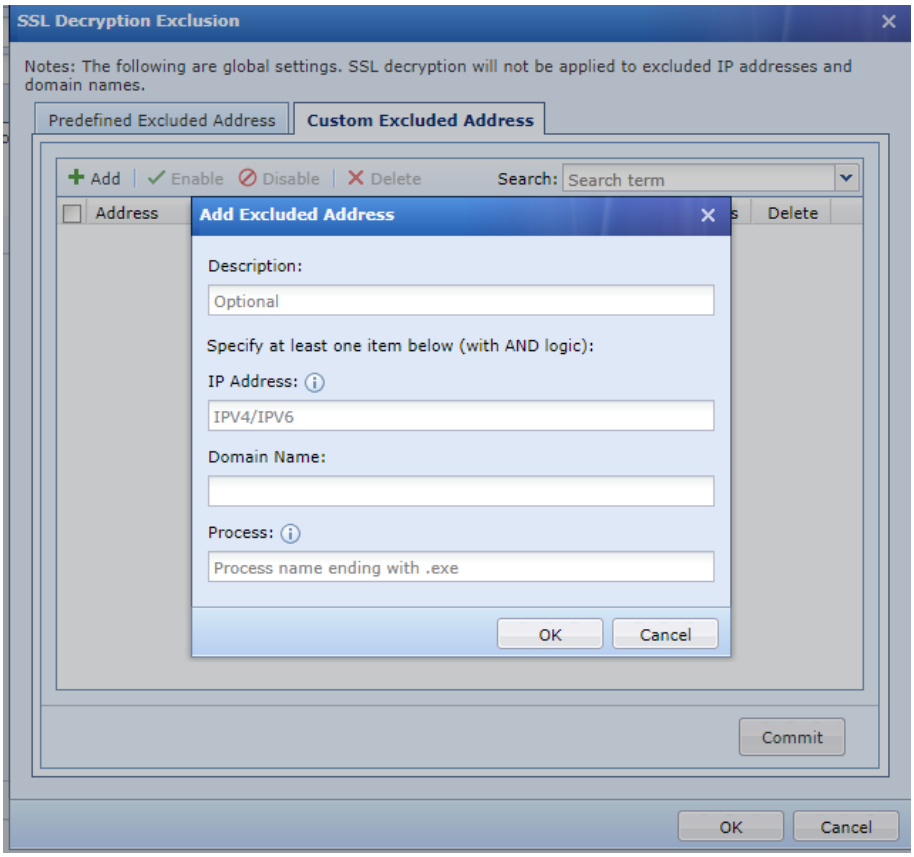


3. Pada IAG, pilih **[Access Control] - [SSL Decryption] - [Ingress Client Decryption]** dan pilih ingress client decryption:

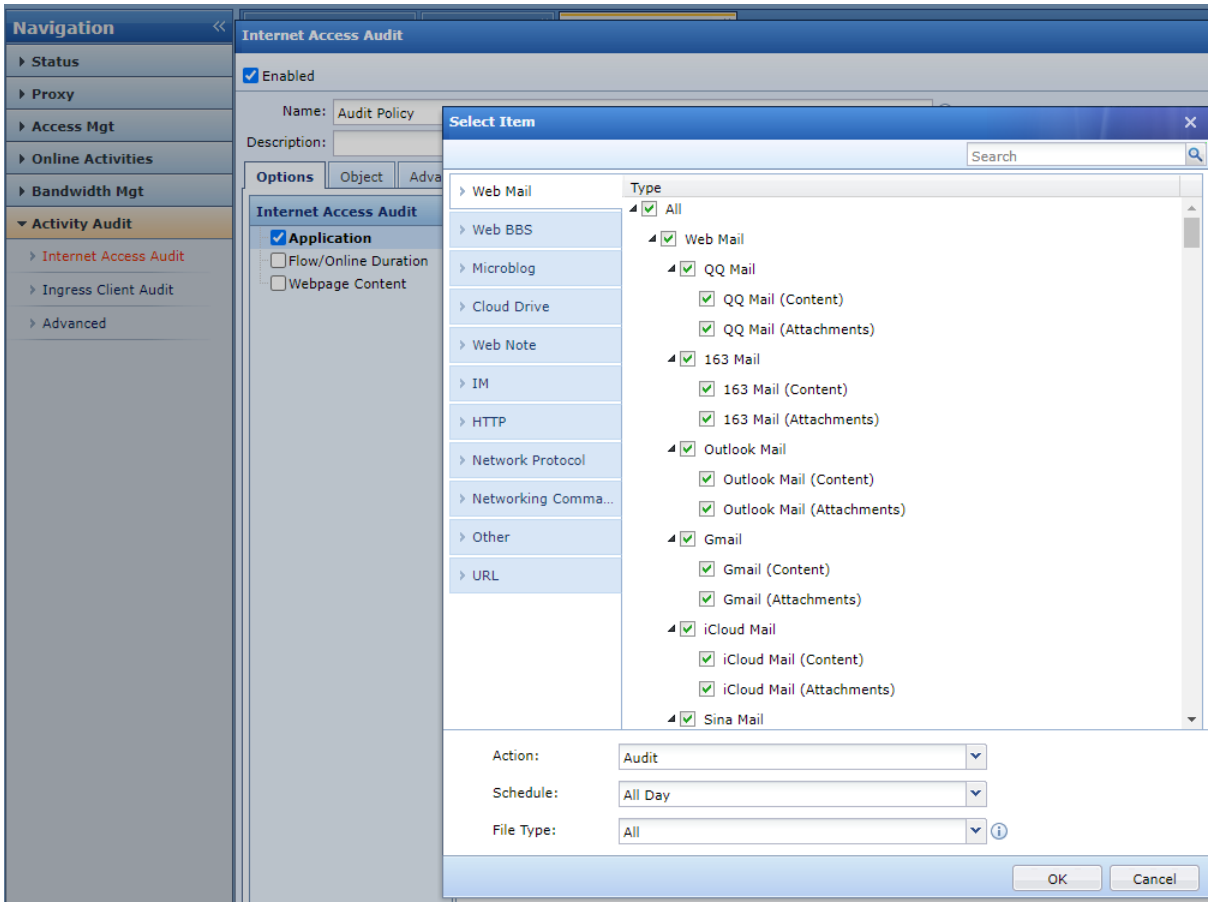




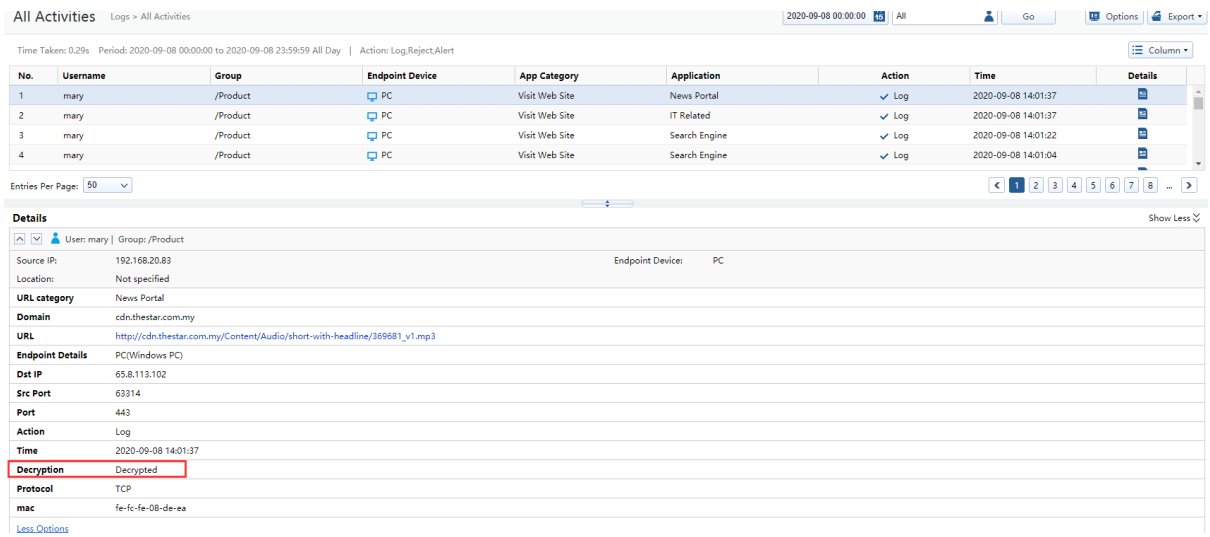
4. Sesuaikan address atau domain name dan proses yang perlu excluded di IAG (artinya, daftar yang tidak perlu di decrypt):



5. Konfigurasi internet access audit policy di IAG:



6. Verifikasi: Masuk ke report center dan kueri audited logs:



Bab 5 Tindakan Pencegahan

1. Fungsi ini membutuhkan PC untuk instal ingress client. Saat ini, hanya mendukung sistem Windows (sistem XP tidak mendukung). Sistem MAC dan sistem Linux dapat menggunakan SSL middleman untuk decryption.

2. Fungsi ini perlu diaktifkan [Multi-function license] - [SSL content ident].

3. Ketika SSL middleman decryption dan ingress client decryption dikonfigurasi pada saat yang sama, daftar policy dicocokkan dari atas ke bawah, dan hanya yang pertama yang cocok yang akan efek.

4. Fungsi ingress plug-in decryption telah dibatalkan dalam versi ini, dan digantikan oleh ingress client decryption.

5. Ingress client hanya decrypts port 443 secara default.

6. Ingress client memiliki finansial bypass bawaan domain name, dan tipe bypass konsisten dengan decryption dari middleman [bank website, online banking, foreign exchange, futures market (Web), futures trading (Web)].

7. Jika endpoint adalah virtual machine, tidak direkomendasikan untuk menggunakan ingress client untuk decryption. Anda dapat menggunakan SSL middleman untuk decrypt.

8. IAG tidak mendukung fungsi proxy decryption dari ingress client ketika fungsi proxy diaktifkan.

SANGFOR