



# IAG

## Panduan Konfigurasi Ingress Client SSL Decryption

**Versi 13.0.15**



## Catatan Perubahan

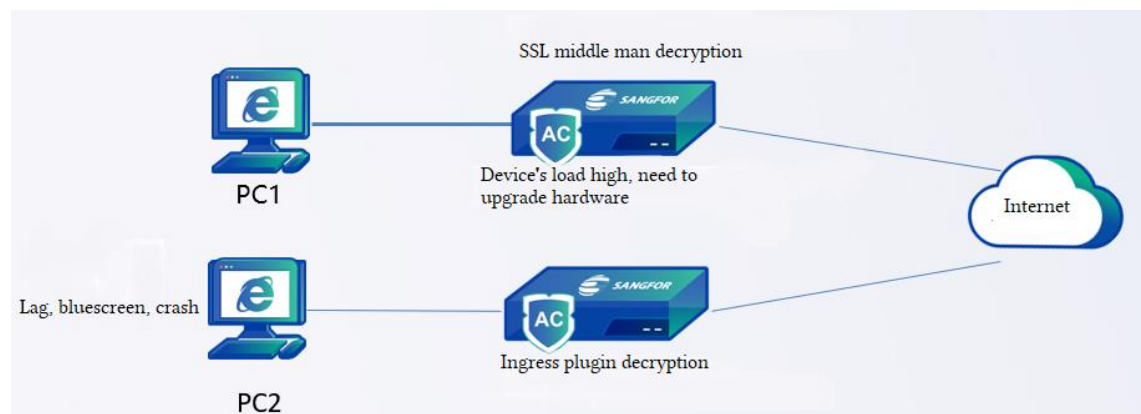
Tanggal	Deskripsi Perubahan
September 9, 2020	Rilis Dokumen Versi 13.0.15.

# Daftar Isi

Bab 1 Latar Belakang Permintaan.....	1
Bab 2 Penjelasan Fitur .....	1
2.1 Pengantar .....	1
2.2 Penjelasan .....	1
2.3 Perbandingan Tiga Metode Decryption.....	3
Bab 3 Skenario Aplikasi.....	3
Bab 4 Konfigurasi.....	3
4.1 Langkah Konfigurasi: .....	4
4.2 Kasus Konfigurasi:.....	4
Bab 5 Tindakan Pencegahan.....	7


## 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	Application Type	Application Name
Web Browser	Chrome	Web Browser	Chromium
Web Browser	Firefox	Web Browser	Brave
Web Browser	IE 8	Web Browser	Maxthon Cloud Browser
Web Browser	IE 9	Web Browser	Torch
Web Browser	IE 10	Web Browser	Vivaldi
Web Browser	IE 11	Web Browser	Tor Browser
Web Browser	Edge	Web Browser	Epic Privacy Browser
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	Application Type	Application Name
Data Leak risk	Baidu Wangpan	Proxy Software	CC proxy
Data Leak risk	Evernote	Antivirus	Rising Antivirus
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		

- Menambah dukungan bagi protokol HTTP 2.0 (tradisional ingress client decryption hanya mendukung HTTP 1.0 dan protokol HTTP 1.1).**
  - Program proxy downgrade protokol HTTP 2.0 ke data protokol HTTP 1.1 .
  - 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/bypass 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.

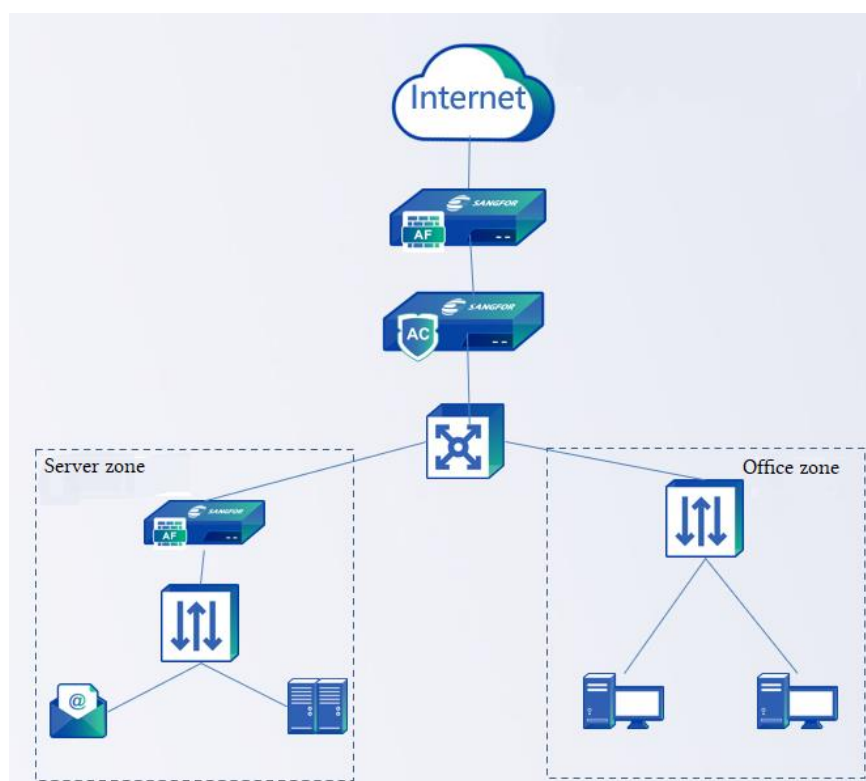
## Bab 4 Konfigurasi

## 4.1 Langkah Konfigurasi:

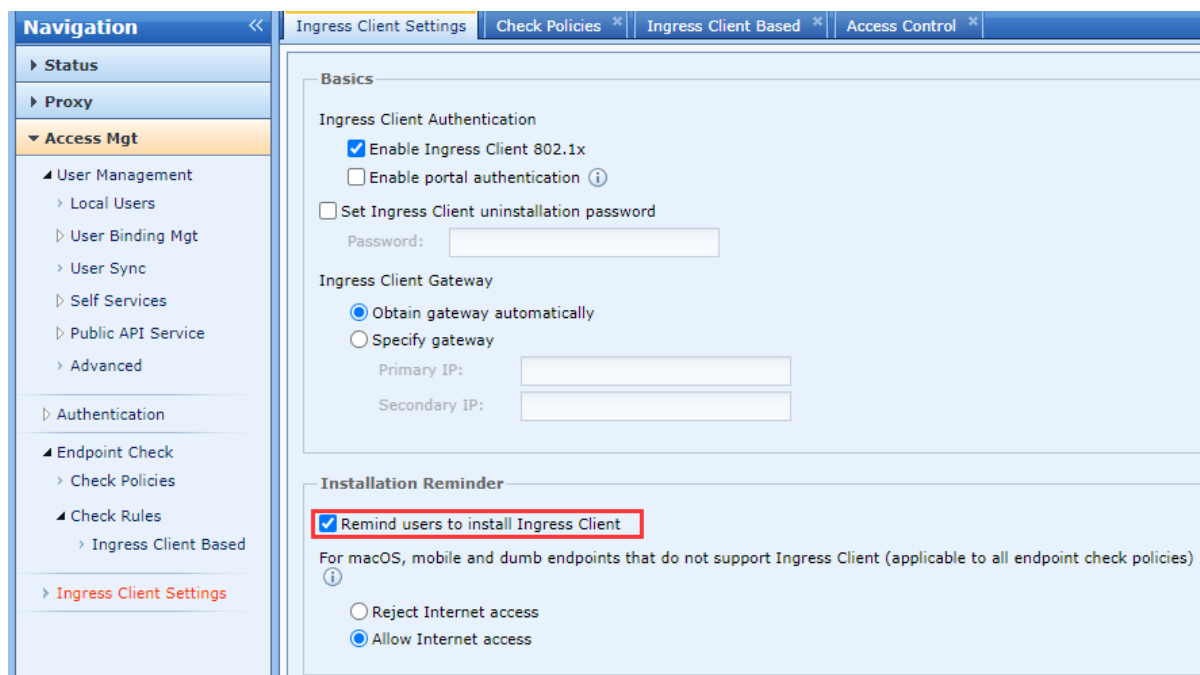
1. Fungsi pengingat instalasi ingress diaktifkan pada IAG (diaktifkan secara default).
2. Endpoint PC instal ingress client, online pada IAG, dan memelihara konektivitas network dengan IAG.
3. Aktifkan fungsi ingress client decryption di IAG **[Access Control]** - **[SSL Decryption]** - **[Ingress Client 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.



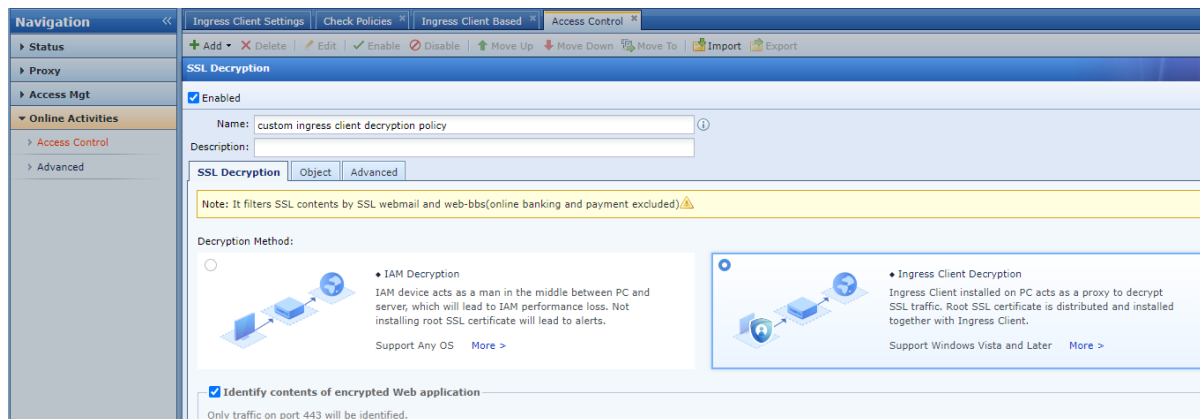
1. Aktifkan fungsi pengingat instalasi ingress pada IAG (diaktifkan secara default).



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

Members									
No.	Username(Alias)	Group	IP Address	Endpoint Device	Auth Method	Ingress Client	Check Result	Time Logged In/Locked	Online Duration
1	192.168.20.83	/UserGroup	192.168.20.83	Windows PC	Open authentication	Installed	-	2020-09-02 13:05:58Lo...	142 hours 38 minutes 5...
2	192.168.20.84	/UserGroup	192.168.20.84	Windows PC	Open authentication	Not installed	-	2020-09-02 12:25:22Lo...	143 hours 19 minutes 2...
3	192.168.20.66	/UserGroup	192.168.20.66	Windows PC	Open authentication	Not installed	-	2020-09-02 12:24:03Lo...	143 hours 20 minutes 4...

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





☒ **Identify contents of encrypted Web application**

Only traffic on port 443 will be identified.

☐ All ?

☒ Specified

Identify contents of SaaS application or website

Visit Web Site/All +

Identify Web encrypted contents  
One domain name per line. The wildcard character is not supported.

mail.qq.com  
gmail.com  
emailgoogle.com  
googleemail.com  
mail.google.com  
www.gmail.com  
groups.google.com  
sites.google.com  
dream4ever.org

☒ Reject data transmitted over QUIC protocol ?

Decryption Exclusion

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

**SSL Decryption Exclusion**

Notes: The following are global settings. SSL decryption will not be applied to excluded IP addresses and domain names.

Predefined Excluded Address | **Custom Excluded Address**

+ Add | ✓ Enable | ✗ Disable | ✗ Delete | Search: Search term

**Add Excluded Address**

Description: Optional

Specify at least one item below (with AND logic):

IP Address: ? IPV4/IPV6

Domain Name:

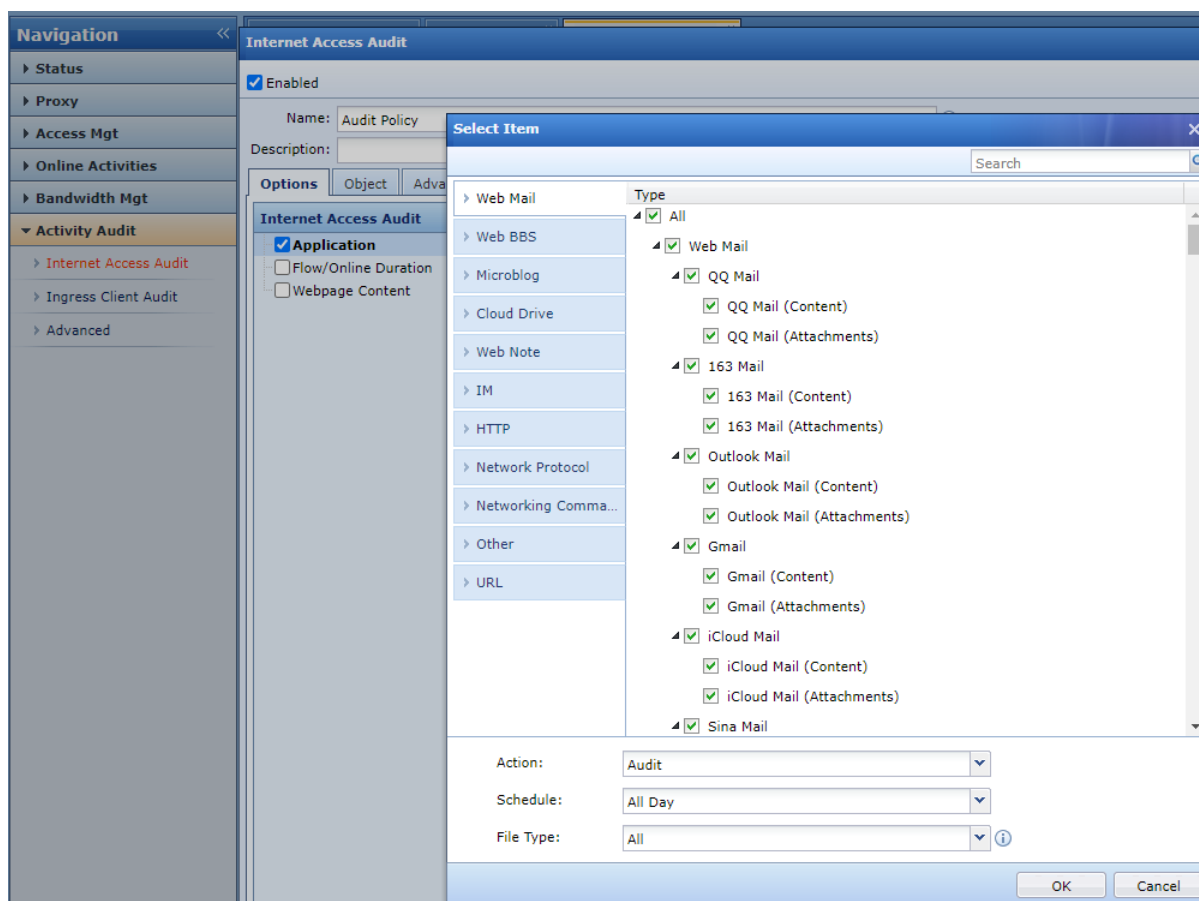
Process: ? Process name ending with .exe

OK Cancel

Commit

OK Cancel

5. Konfigurasi internet access audit policy di IAG:



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

All Activities [Logs > All Activities](#) 2020-09-08 00:00:00 [Go](#) [Options](#) [Export](#)

Time Taken: 0.29s Period: 2020-09-08 00:00:00 to 2020-09-08 23:59:59 All Day Action: LogRejectAlert

No.	Username	Group	Endpoint Device	App Category	Application	Action	Time	Details
1	mary	/Product	PC	Visit Web Site	News Portal	✓ Log	2020-09-08 14:01:37	<a href="#">Details</a>
2	mary	/Product	PC	Visit Web Site	IT Related	✓ Log	2020-09-08 14:01:37	<a href="#">Details</a>
3	mary	/Product	PC	Visit Web Site	Search Engine	✓ Log	2020-09-08 14:01:22	<a href="#">Details</a>
4	mary	/Product	PC	Visit Web Site	Search Engine	✓ Log	2020-09-08 14:01:04	<a href="#">Details</a>

Entries Per Page: 50

**Details** [Show Less](#)

User: mary | Group: /Product

Source IP: 192.168.20.83 Endpoint Device: PC

Location: Not specified

URL category: News Portal

Domain: cdn.thestar.com.my

URL: http://cdn.thestar.com.my/Content/Audio/short-with-headline/369681\_v1.mp3

**Endpoint Details** PC(Windows PC)

Dst IP: 65.8.113.102

Src Port: 63314

Port: 443

Action: Log

Time: 2020-09-08 14:01:37

**Decryption** Decrypted

Protocol: TCP

mac: fe-fc-fe-08-de-ea

[Less Options](#)

# 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**

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