



IAM

Implementasi yang Direkomendasikan untuk Skenario_ SSL Content Decryption

Versi 12.0.42



Catatan Perubahan

Tanggal	Deskripsi Perubahan
Juli 27, 2020	Rilis Dokumen Versi 12.0.42.
Mei 17, 2021	Dokumen update Versi 12.0.42.

Daftar Isi

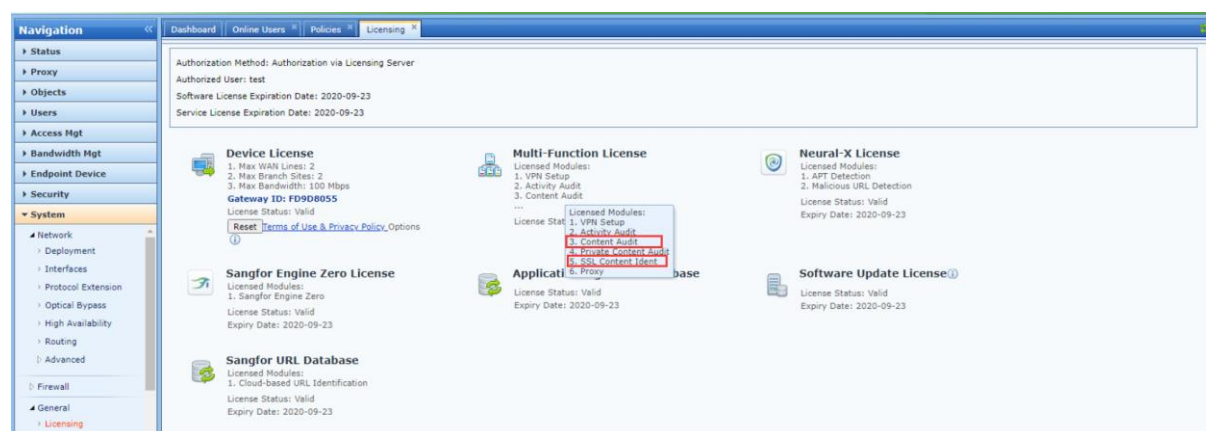
Bab 1 Skenario	1
Bab 2 Konfigurasi	1

Bab 1 Skenario

Departemen R&D dari perusahaan perangkat lunak perlu audit content email yang dikirim oleh developer untuk menghindari kebocoran informasi kode, jadi hendak menggunakan IAM untuk audit content terenkripsi pengguna.

Bab 2 Konfigurasi

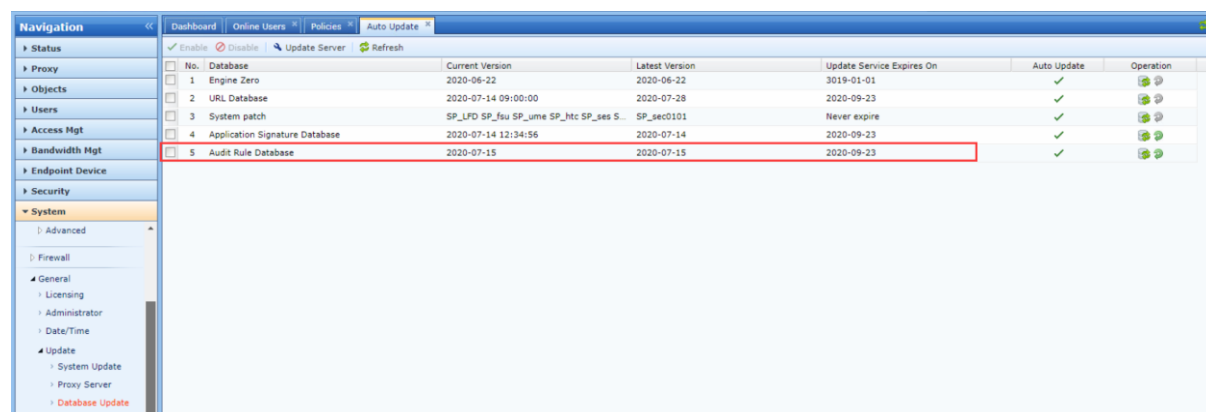
1. Periksa authorization dan rule basis versi untuk memastikan bahwa Multi-Function License berisi Content dan SSL Content Ident



The screenshot shows the 'Licensing' page in the Sangfor IAM interface. It displays several licenses and their associated modules:

- 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, 4. Private Certificate Audit, 5. SSL Content Ident, 6. Proxy. License Status: Valid. Expiry Date: 2020-09-23.
- 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.
- Sangfor URL Database:** Licensed Modules: 1. Cloud-based URL Identification. License Status: Valid. Expiry Date: 2020-09-23.
- Software Update License:** License Status: Valid. Expiry Date: 2020-09-23.

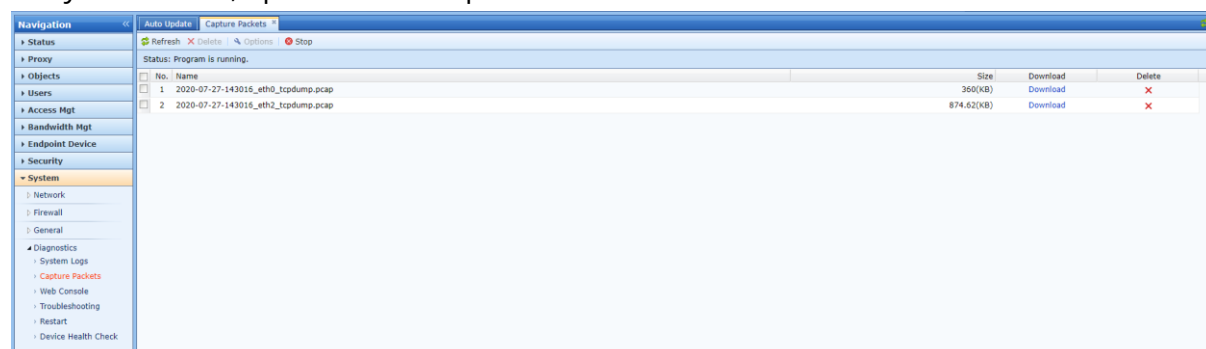
The 'Multi-Function License' is highlighted, and its modules are listed. A red box highlights the 'Content Audit' and 'SSL Content Ident' modules.



The screenshot shows the 'Auto Update' page in the Sangfor IAM interface. It displays a table of updates:

No.	Database	Current Version	Latest Version	Update Service Expires On	Auto Update	Operation
1	Engine Zero	2020-06-22	2020-06-22	2019-01-01	✓	
2	URL Database	2020-07-14 09:00:00	2020-07-28	2020-09-23	✓	
3	System patch	SP_LFD SP_fsu SP_ume SP_hic SP_ses S...	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 bahwa traffic network melewati perangkat IAM di kedua arah. Jika traffic hanya satu arah, aplikasi tidak dapat diidentifikasi dan dikontrol.



The screenshot shows the 'Capture Packets' page in the Sangfor IAM interface. It displays a table of captured packets:

No.	Name	Size	Download	Delete
1	2020-07-27-143016_eth0_tcpdump.pcap	260(KB)	Download	✗
2	2020-07-27-143016_eth2_tcpdump.pcap	874.62(KB)	Download	✗

SSL Content Decryption

Top stream seq 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 14:30:40.044883	192.168.1.3	216.58.196.36	TLSv1.2	571		517 Client Hello
12	2020/209 14:30:40.044896	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 14:30:40.121832	192.168.1.3	216.58.196.36	TCP	54		50121 → 443 [ACK] Seq=526 Ack=958 Win=2101248 Len=0

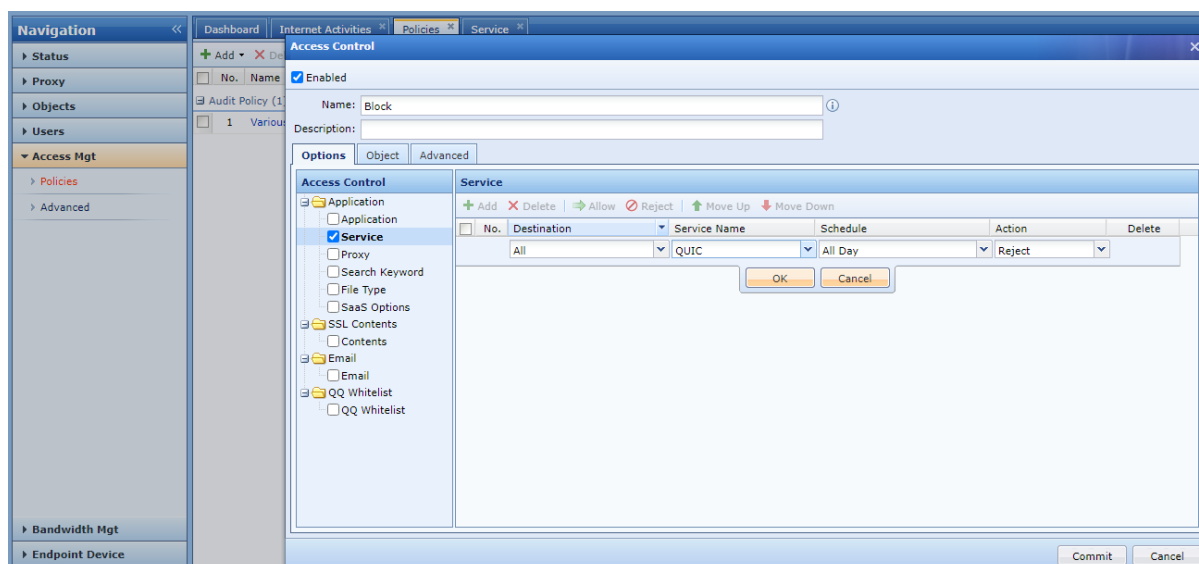
3. Konfigurasi audit policy, karena aplikasi sering berisi multiple rules, perlu untuk memeriksa rule aplikasi mana yang dikenali oleh IAM database.

The screenshot shows the Sangfor Firewall configuration interface. The 'Policies' section is active, and the 'Audit Policy' is selected. The 'Select Item' dialog box is open, showing various application categories. The 'Application' category is selected, and the 'Audit' action is chosen. The 'Schedule' is set to 'All Day'.

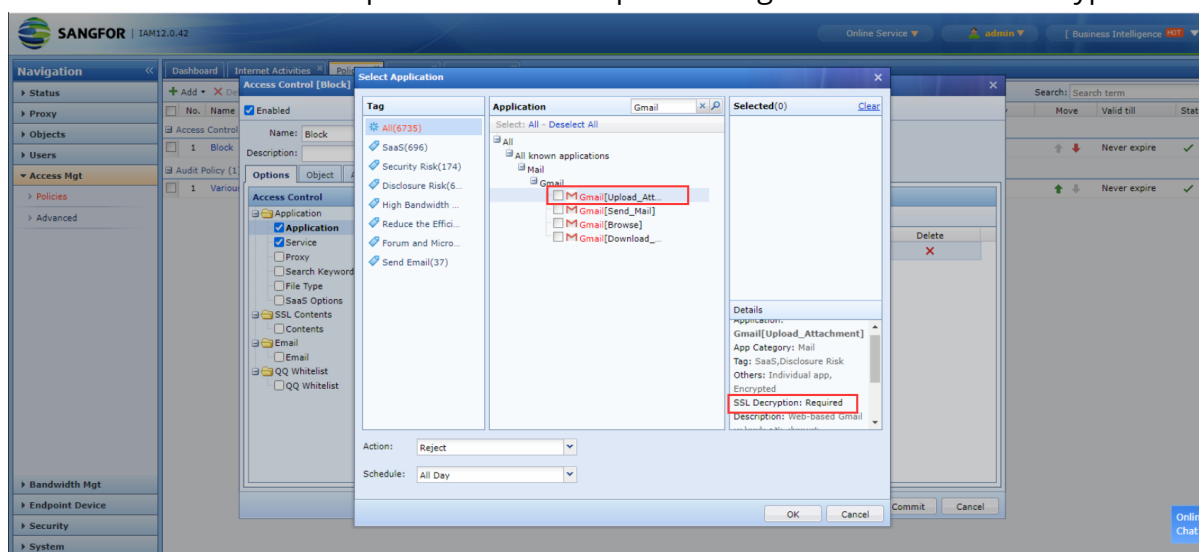
4. Sekarang banyak website dan browser menggunakan protokol QUIC untuk mengirimkan data, dan data yang dienkrpsi oleh protokol QUIC tidak dapat dikontrol, jadi protokol QUIC perlu dinonaktifkan. Setelah nonaktifkan protokol QUIC, website dan browser akan secara otomatis negosiasi penggunaan HTTPS untuk mengirimkan data.

The screenshot shows the Sangfor Firewall configuration interface. The 'Service' section is active, and the 'Add Service' dialog box is open. The 'Service Name' is set to 'QUIC', and the 'Protocol' is set to 'QUIC'. The 'Add Service' button is highlighted.

SSL Content Decryption

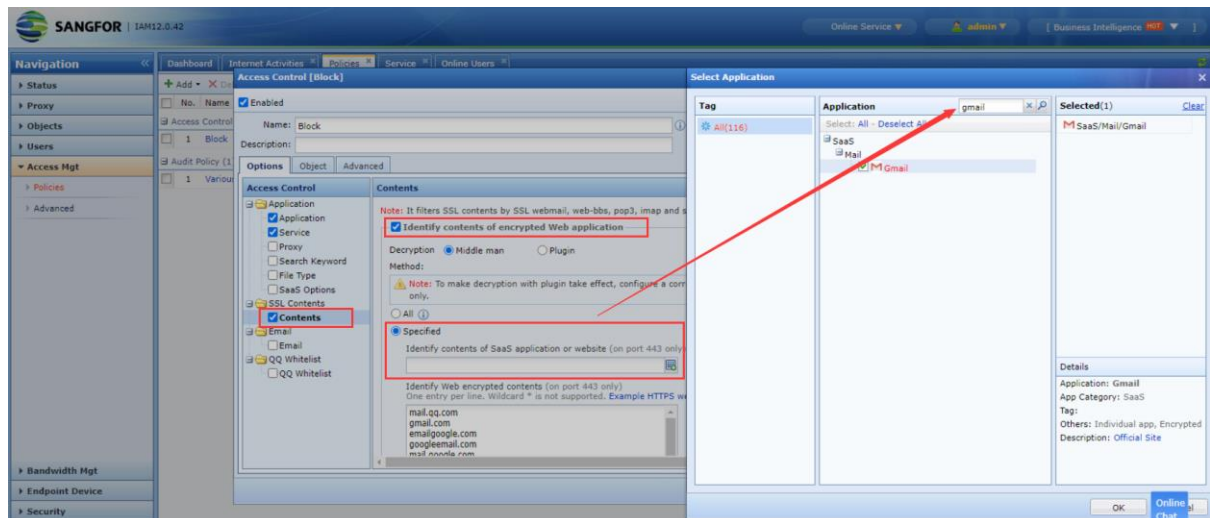


1. Jika Anda ingin melakukan kontrol yang lebih detail atas tindakan dari website https, seperti mengizinkan browsing tetapi tidak upload attachment, kemudian Anda perlu memeriksa deskripsi database apps untuk menentukan apakah Anda perlu decrypt domain name yang relevan. Misalnya, setelah query deskripsi database, Anda dapat konfirmasi bahwa Gmail upload attachment perlu mengaktifkan SSL data decryption.

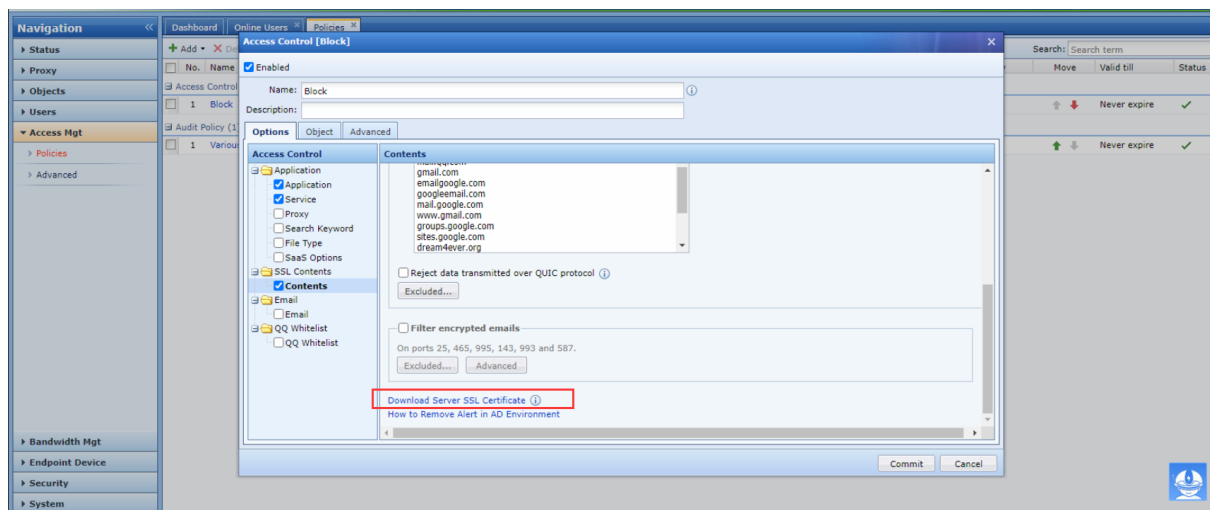


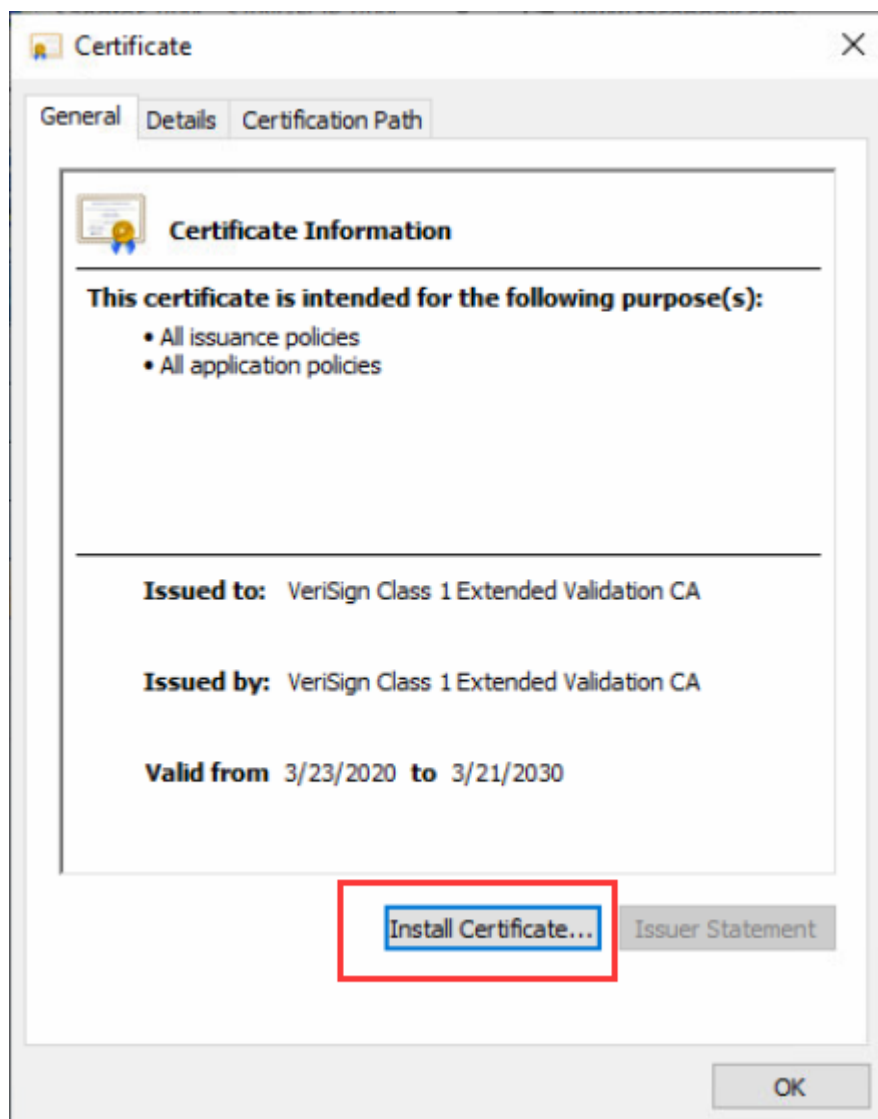
2. Aktifkan SSL recognition dan pilih website yang memerlukan SSL decryption sebagai Gmail.

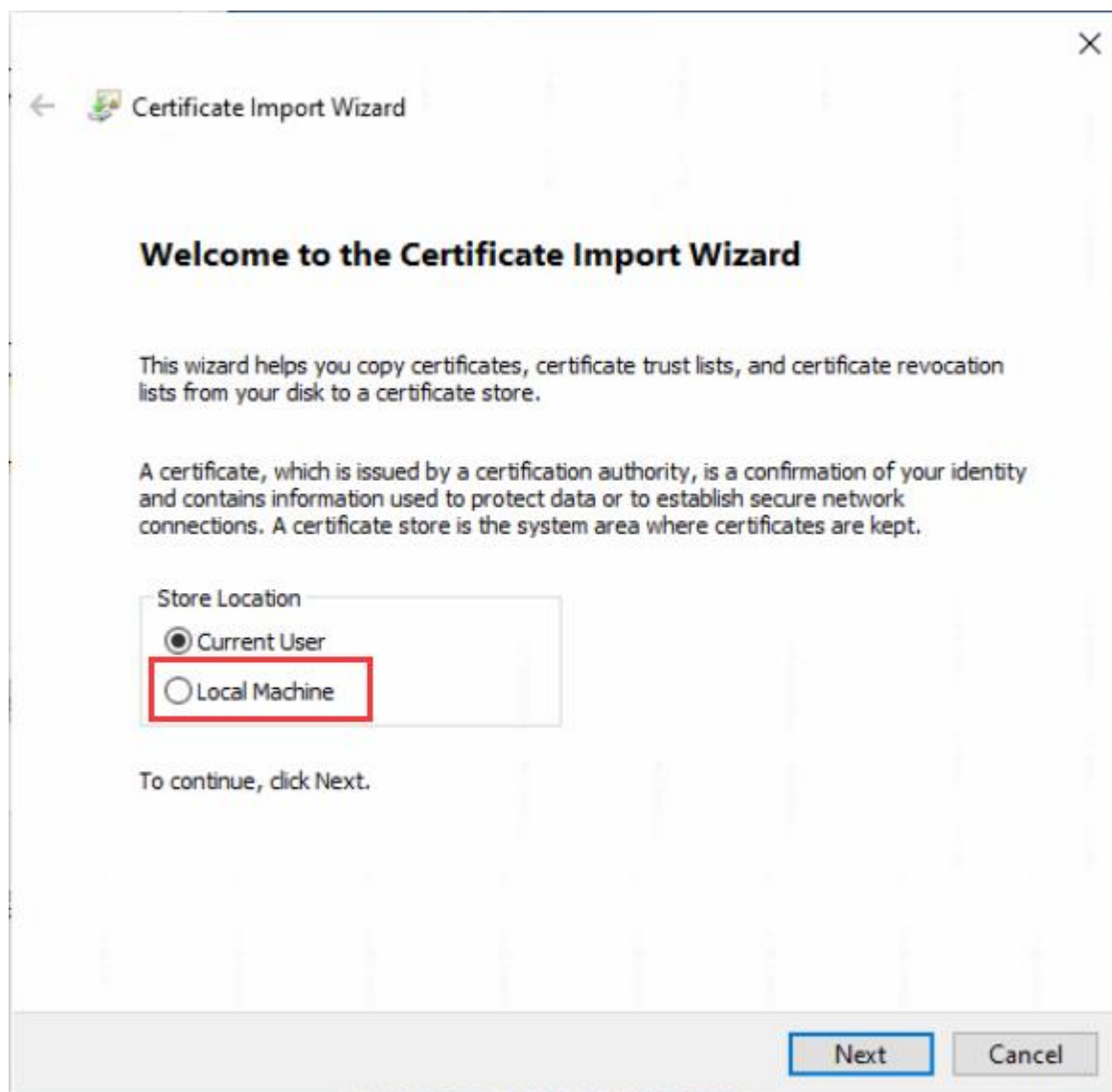
SSL Content Decryption

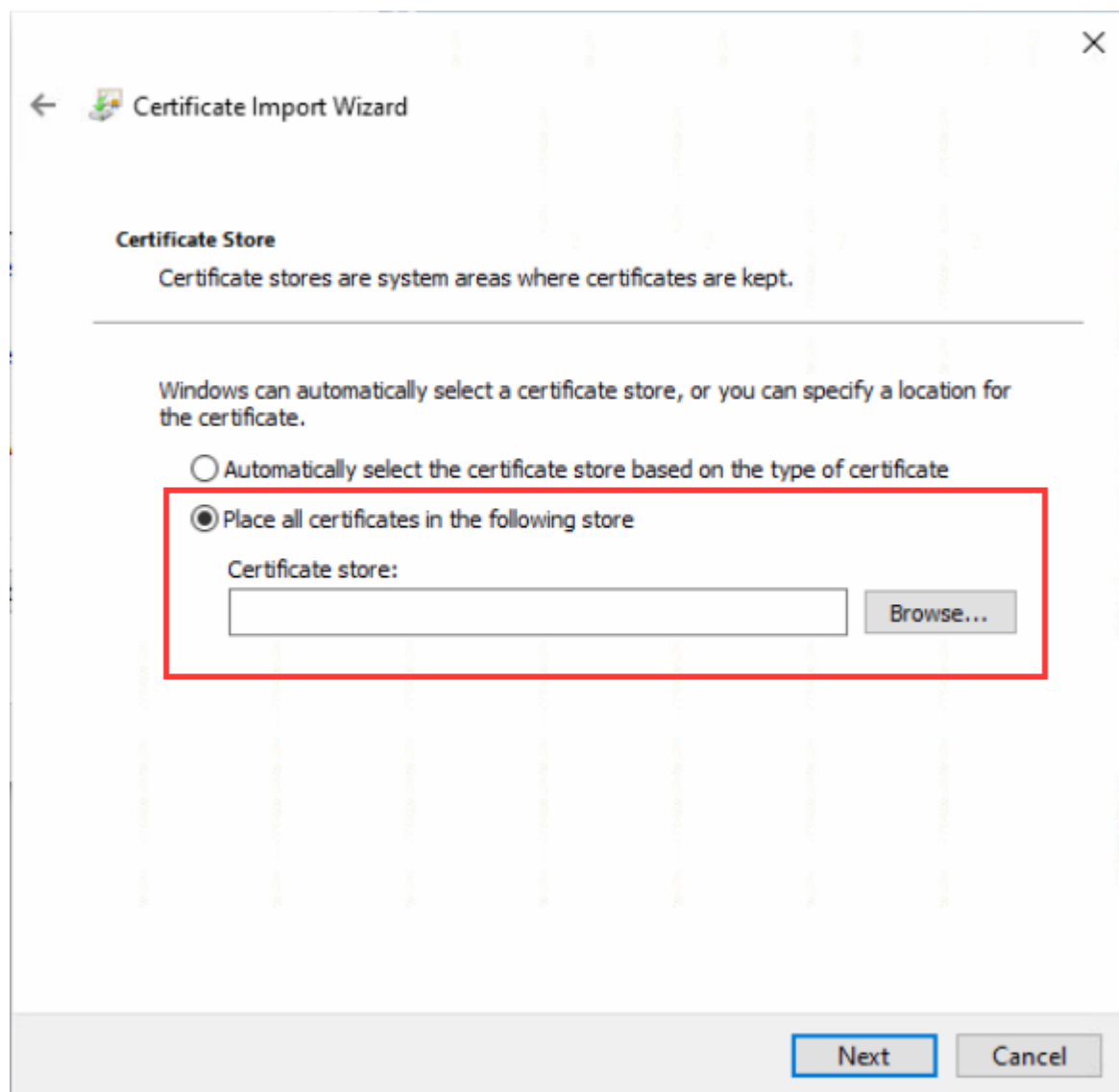


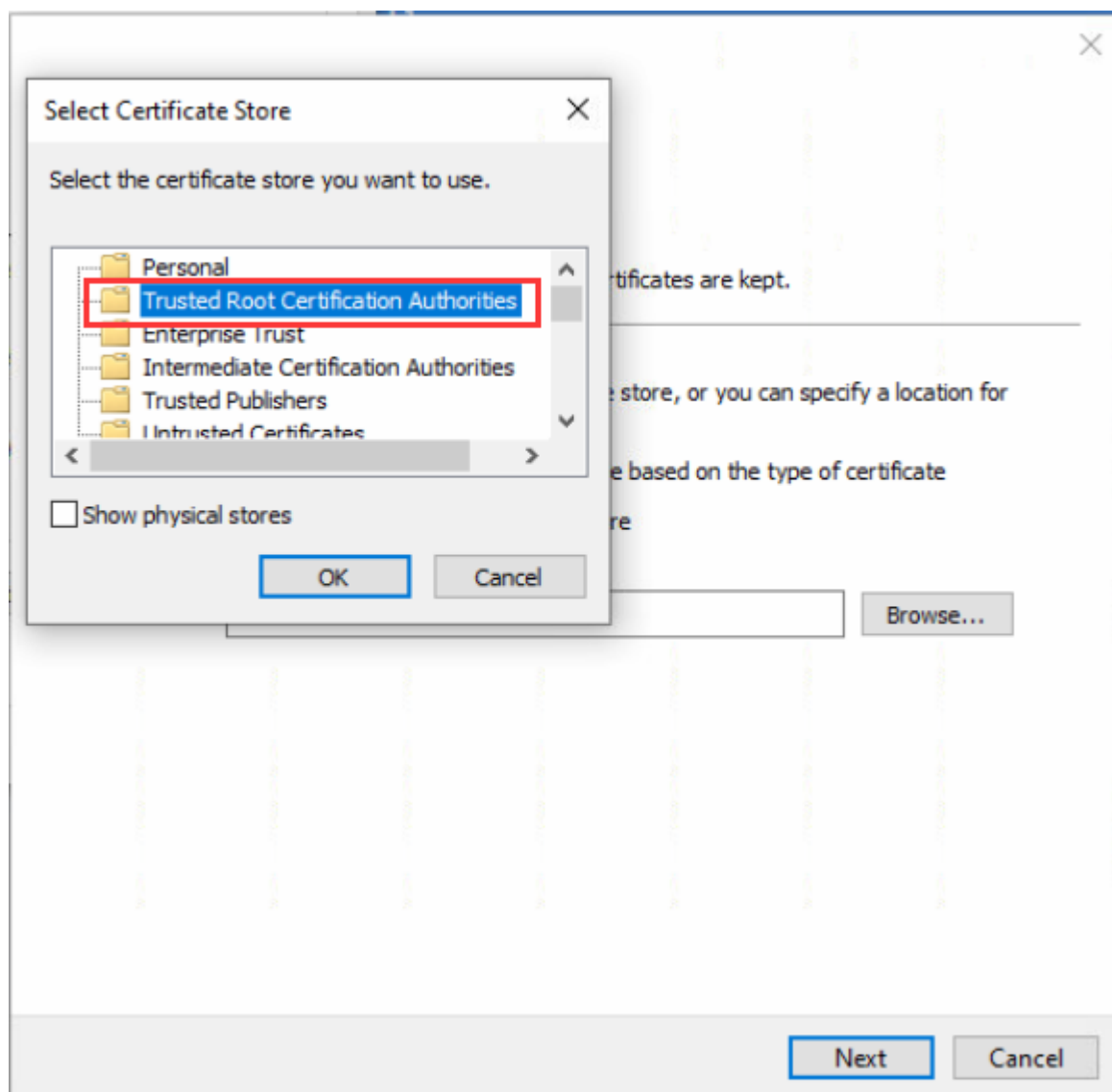
3. Download root certificate yang dikenali oleh SSL dari perangkat IAM dan import ke dalam sistem.

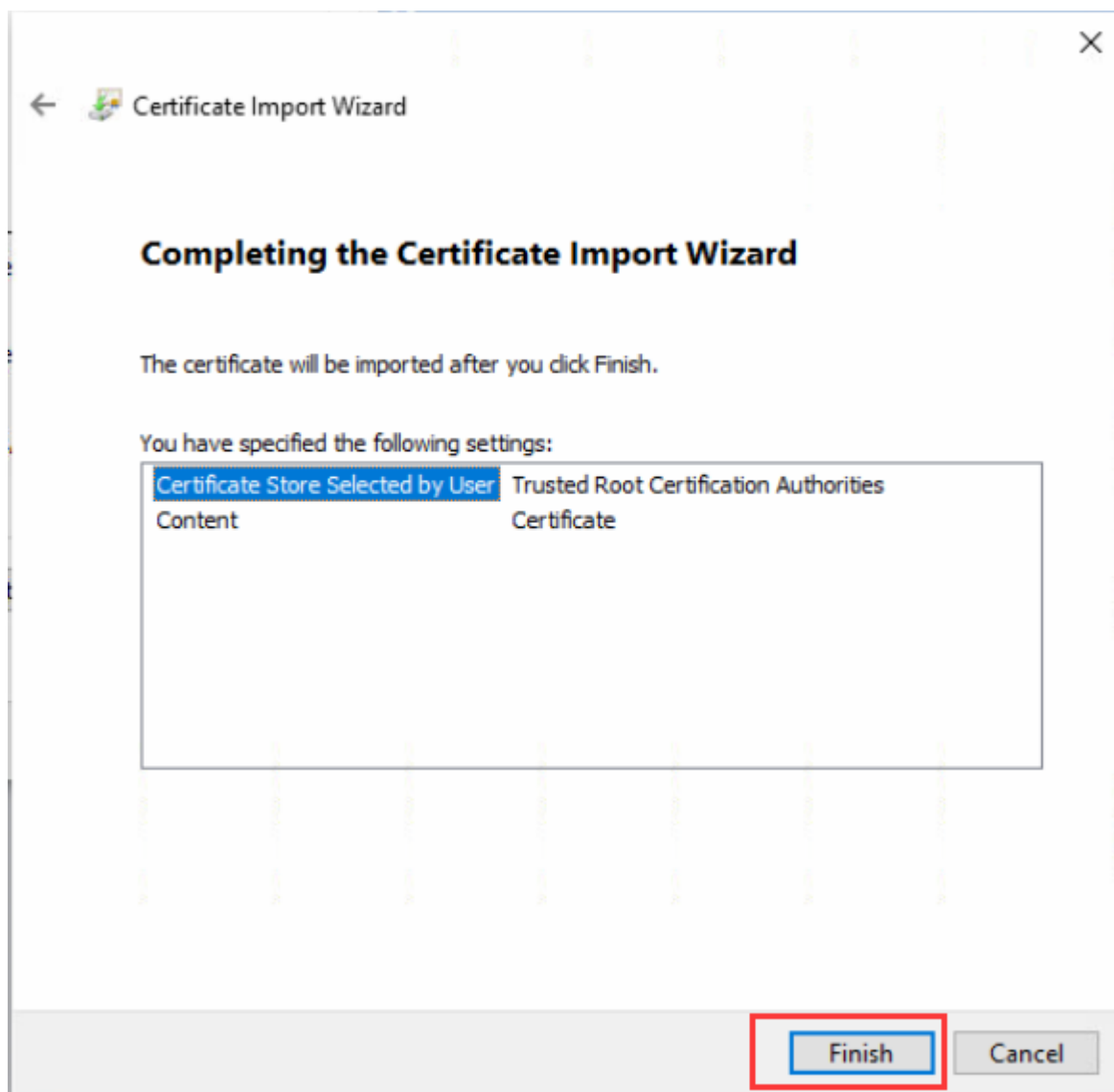






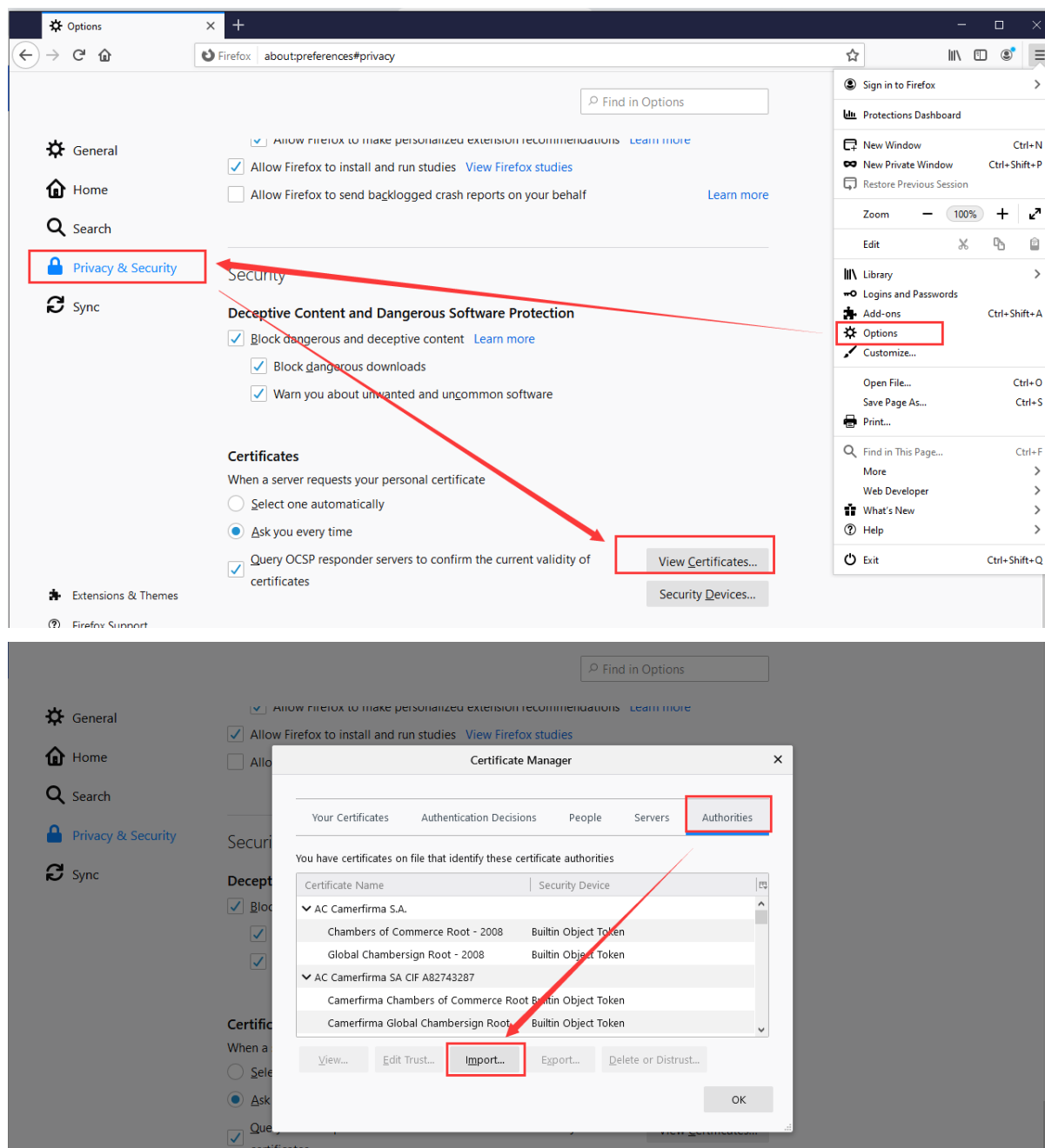




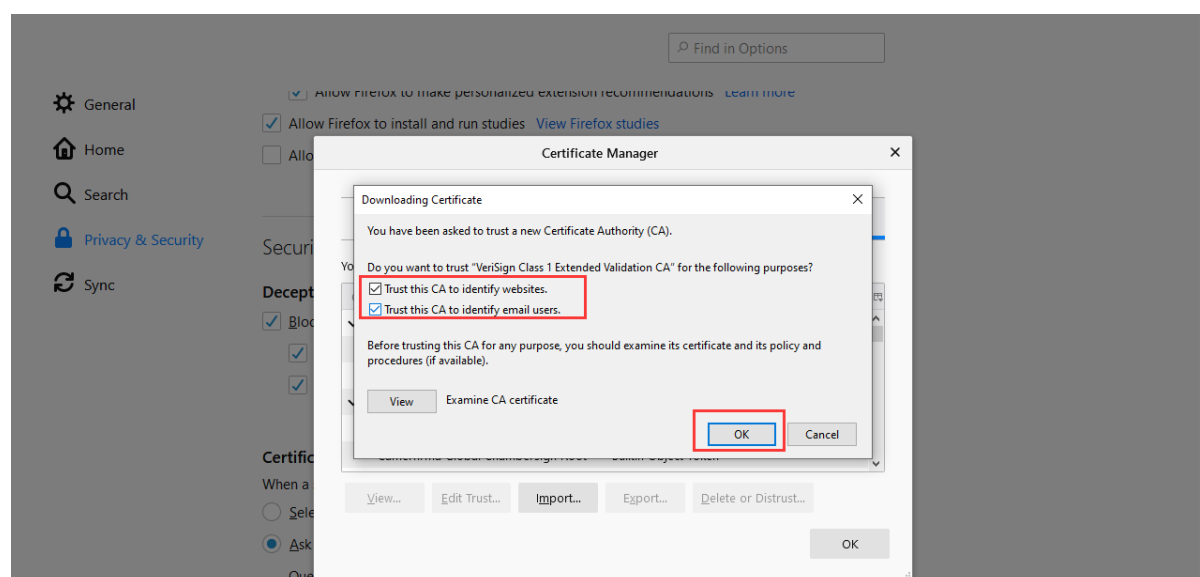
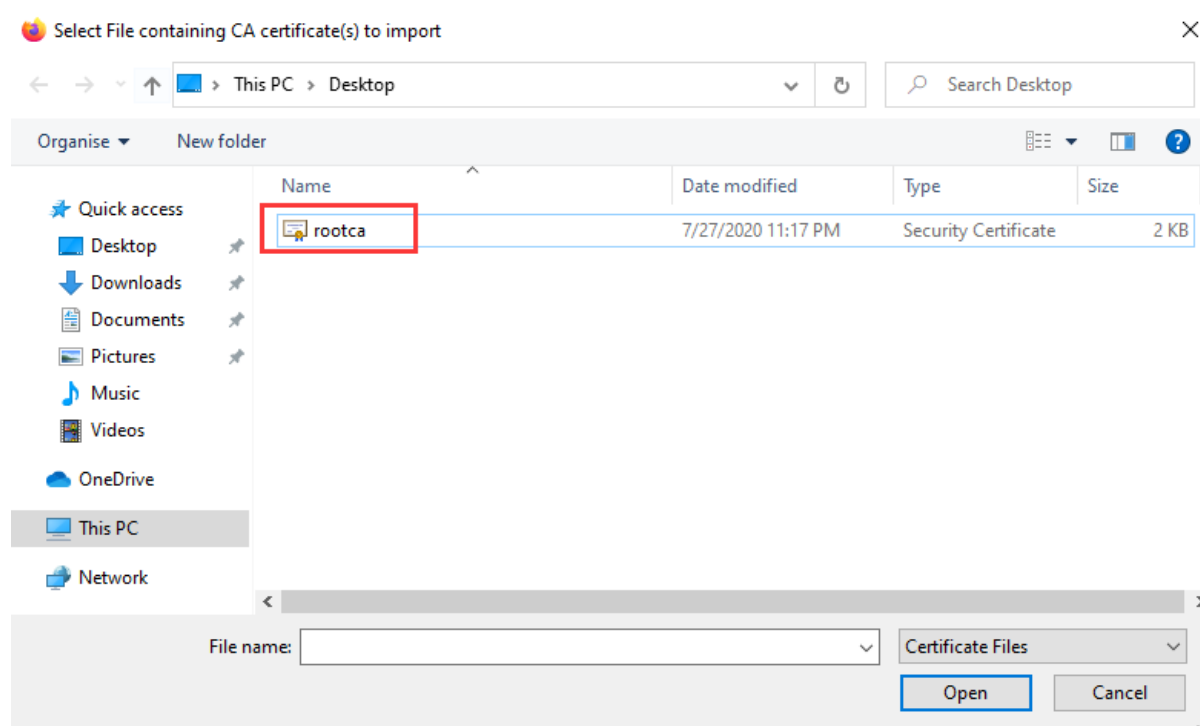


4. IE dan Chrome call certificate bawaan dari sistem Windows, dan Firefox browser tidak call certificate bawaan dari sistem Windows dan perlu diimport secara terpisah.

SSL Content Decryption



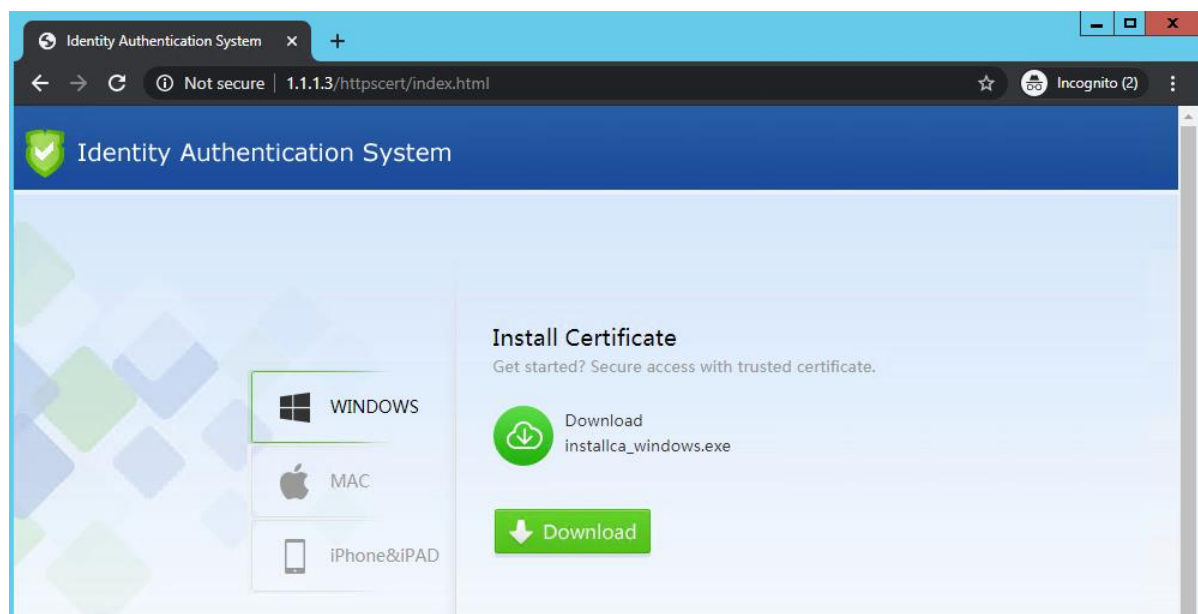
SSL Content Decryption



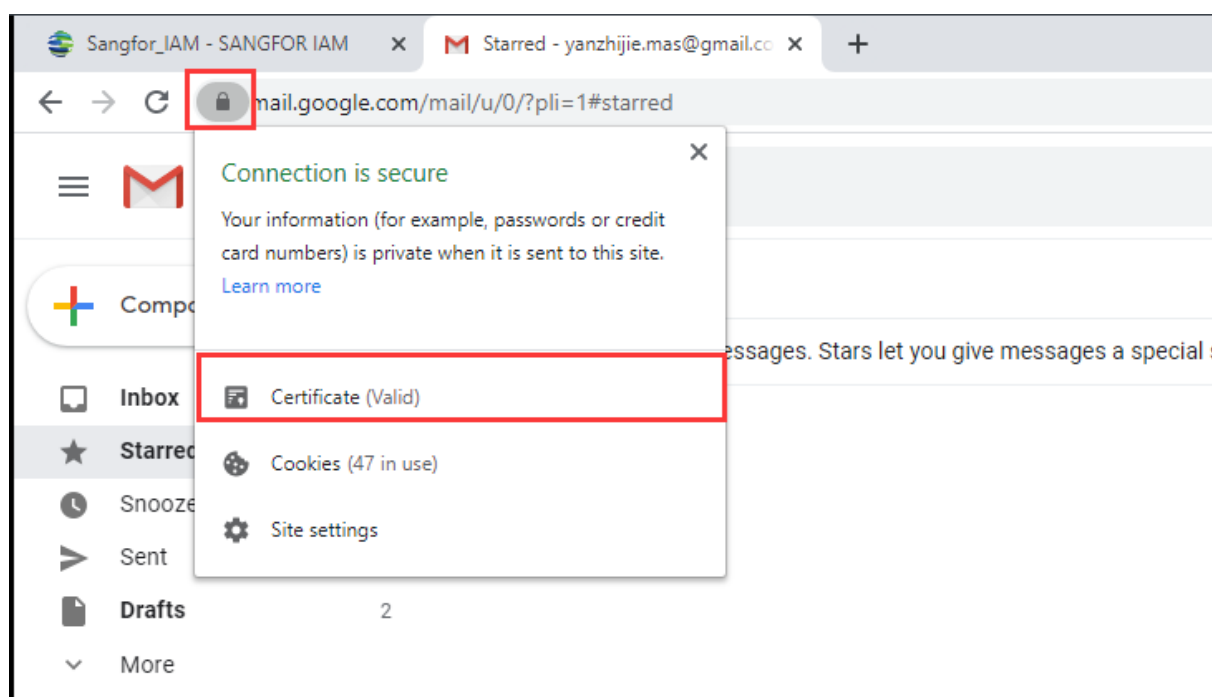
4. Anda juga dapat menggunakan cert installer download dari IAM link.

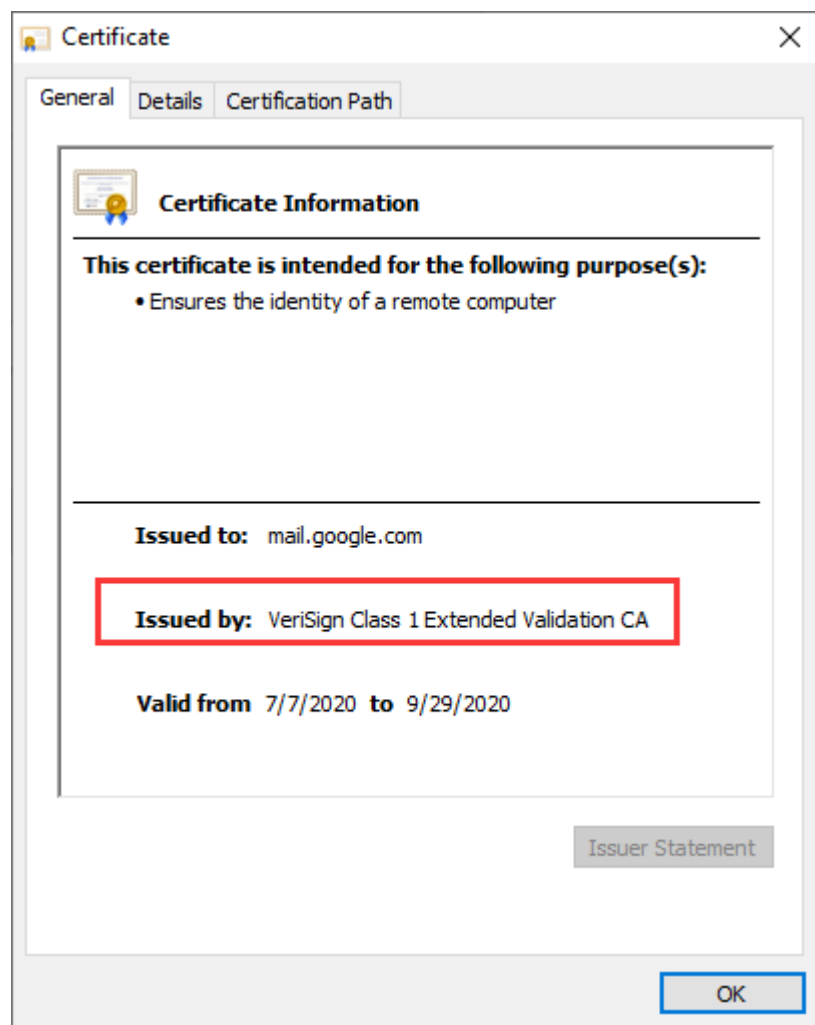
<http://IAMip/httpsert/index.html> IP IAM adalah IP IAM apapun yang dapat terkoneksi dari PC ke IAM.

misalnya: <http://1.1.1.3/httpsert/index.html>

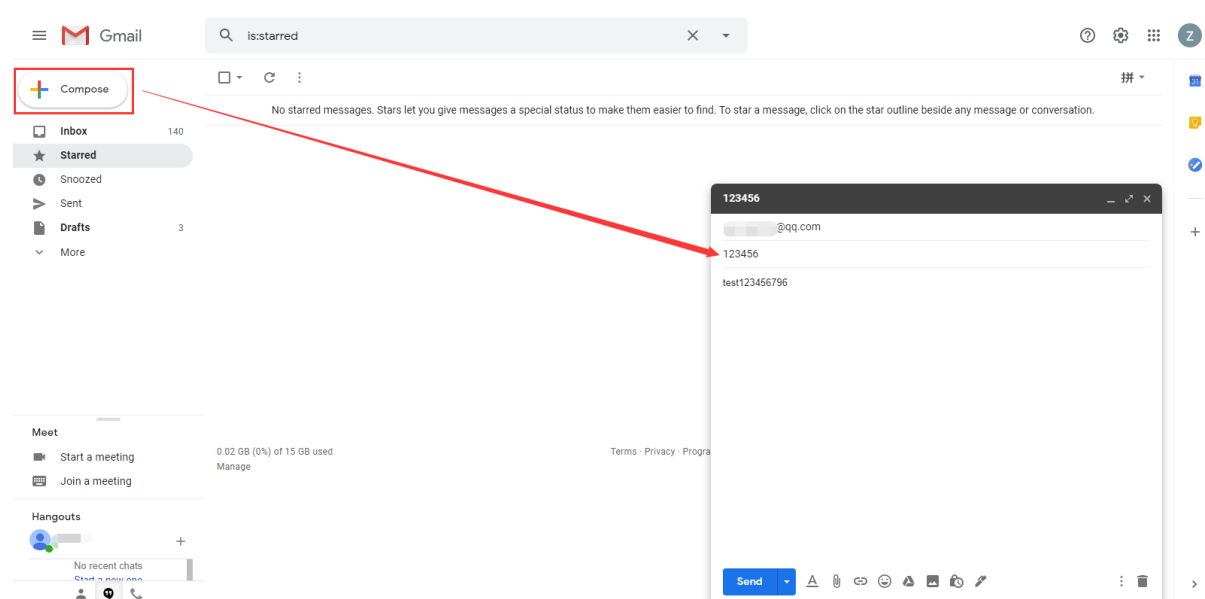


5. Periksa apakah certificate yang digunakan untuk mengakses website "VeriSign Class 1 Extended Validation CA", jika benar, berarti SSL decryption berhasil.





5. Gunakan Gmail untuk mengirim mail, Anda bisa mendapatkan judul dan body content dari mail.



SSL Content Decryption

Navigation		Dashboard	Online Users	Policies	Licensing	Internet Activities				
▼ Status		Auto Refresh: 5 second(s) Filter								
▼ Dashboard		Filter: Group (/) Objects: Search term Email IM chats Others Forum & Microblogging Outgoing Files Website Browsing Action: Reject Log Alert								
▼ Online Users		No.	Time Occurred	Username	Group	IP Address	App Category	Application	Action	Details
▼ Troubleshooting Center		1	7seconds ago	sangfor	/	192.168.1.3	Mail	Gmail[Send_Mail]	Log	URL: mail.google.com Contents: <div dir="ltr">test123456796</div> Sender: max@gmail.com Receiver: 123456 Receiver: @qq.com
▼ Traffic Statistics										
▼ Internet Activities		2	7seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: taskassist-pa.clients6.google.com
▼ Locked Users		3	7seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: translate.googleapis.com
▼ SaaS Applications		4	7seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
▼ Security Events		5	46seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: translate.googleapis.com
		6	1 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com
		7	1 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Send_Mail]	Log	URL: mail.google.com/mail/u/0/?ui=1&sw=2 Website: mail.google.com
		8	1 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
		9	1 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
		10	1 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: taskassist-pa.clients6.google.com
		11	1 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
		12	1 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com/mail/u/0/?ui=2&ik=687af392f7 Website: mail.google.com
		13	1 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com
		14	1 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com
		15	1 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: translate.googleapis.com
		16	1 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: translate.googleapis.com
▼ Proxy										



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