IAM

Praktik Terbaik untuk Skenario_Akses Control Policy

Versi 12.0.42

Catatan Perubahan

Tanggal	Deskripsi Perubahan
Juli 26, 2020	Rilis Dokumen versi 12.0.42.
Mei 17, 2021	Dokumen update versi 12.0.42 .

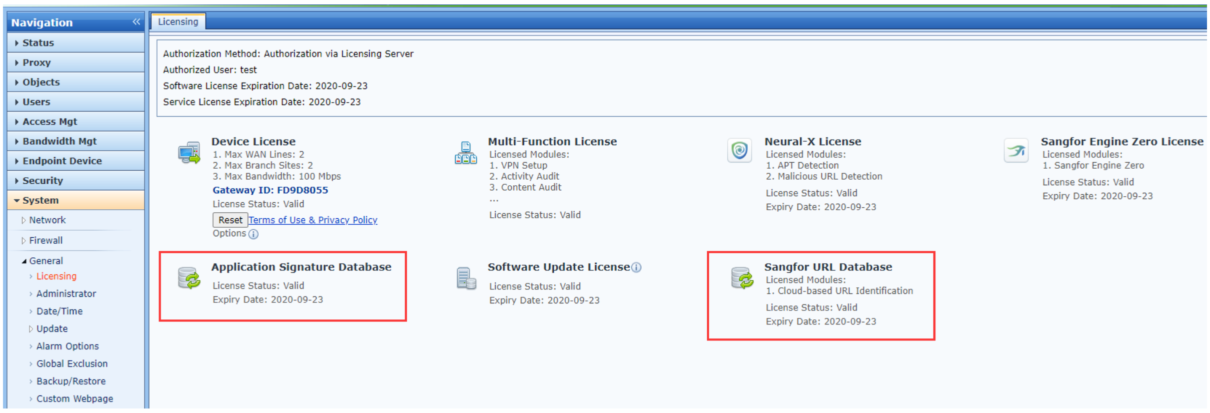
Daftar Isi

Bab 1 Skenario

Departemen R&D dari perusahaan perangkat lunak memiliki kontrol yang ketat terhadap pengguna intranet dan perlu melarang pengguna untuk mengakses Facebook selama jam kerja. Selain itu, untuk memastikan informasi security, pengguna dilarang menggunakan Gmail untuk mengirim file, dan IAM dapat digunakan untuk perilaku kontrol perilaku terkait perilaku.

Bab 2 Konfigurasi

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



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

Device License
1. Max WAN Lines: 2
2. Max Branch Sites: 2
3. Max Bandwidth: 100 Mbps
Gateway ID: FD9D8055
License Status: Valid

Multi-Function License
Licensed Modules:
1. VPN Setup
2. Activity Audit
3. Content Audit
...
License Status: Valid

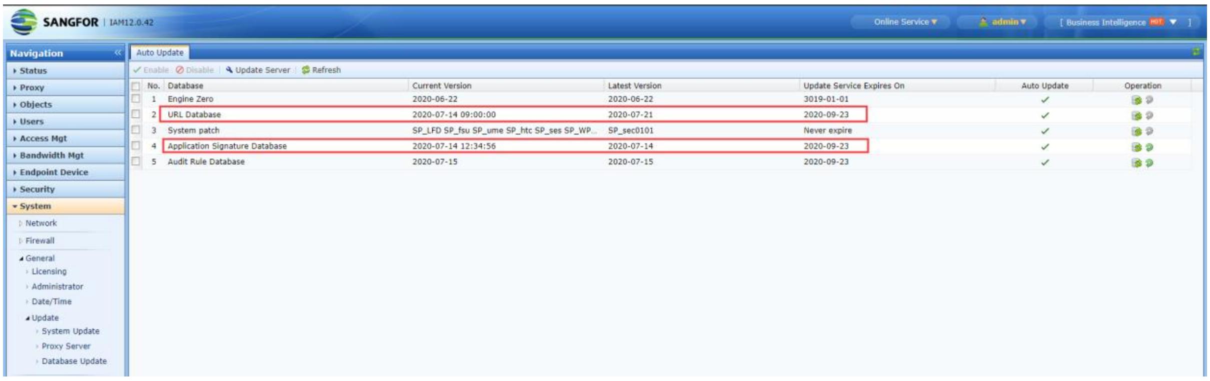
Neural-X License
Licensed Modules:
1. APT Detection
2. Malicious URL Detection
License Status: Valid
Expiry Date: 2020-09-23

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

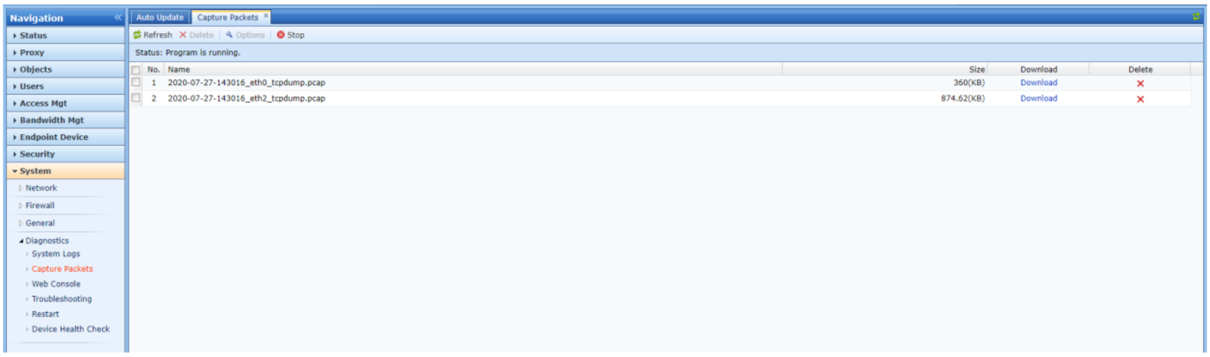
Software Update License
License Status: Valid
Expiry Date: 2020-09-23

Sangfor URL Database
Licensed Modules:
1. Cloud-based URL Identification
License Status: Valid
Expiry Date: 2020-09-23



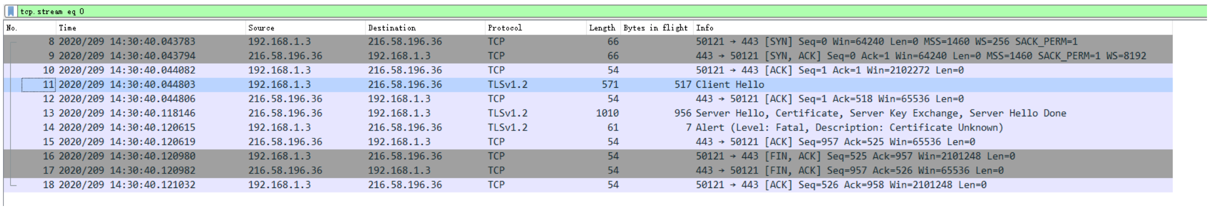
No.	Database	Current Version	Latest Version	Update Service Expires On	Auto Update	Operation
1	Engine Zero	2020-06-22	2020-06-22	3019-01-01	✓	
2	URL Database	2020-07-14 09:00:00	2020-07-21	2020-09-23	✓	
3	System patch	SP_LFD SP_fsu SP_ume SP_htc SP_ses SP_WP...	SP_sec0101	Never expire	✓	
4	Application 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 dua arah. Jika traffic hanya satu arah, maka aplikasi tidak dapat diidentifikasi dan dikontrol.



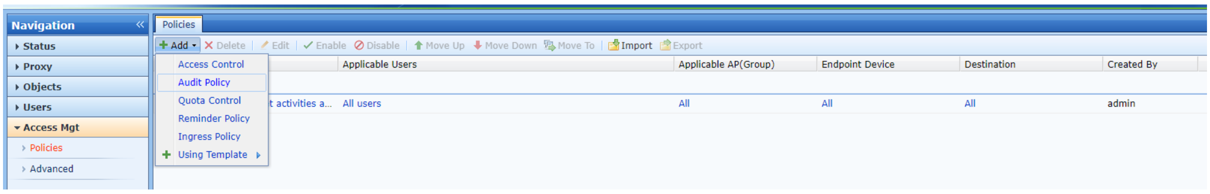
Status: Program is running.

□	No.	Name	Size	Download	Delete
□	1	2020-07-27-143016_eth0_tcpdump.pcap	360(KB)	Download	✕
□	2	2020-07-27-143016_eth2_tcpdump.pcap	874.62(KB)	Download	✕

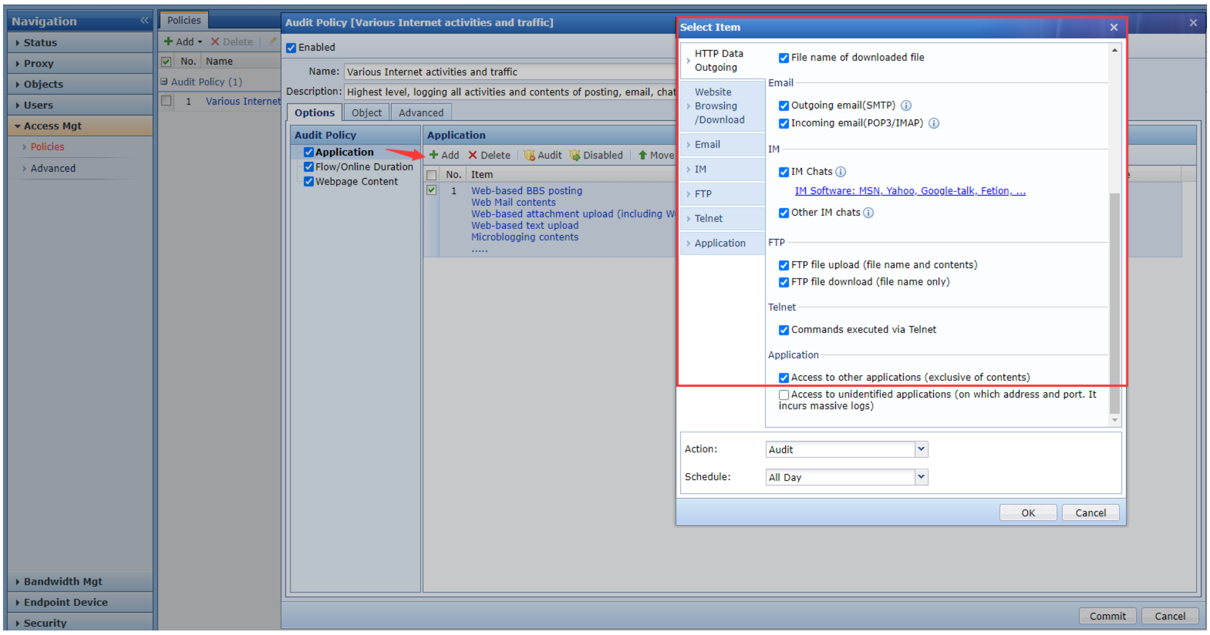


```
tcp.stream eq 0
No.  Time                       Source          Destination     Protocol  Length Bytes in flight Info
   8 2020/209 14:30:40.043783   192.168.1.3     216.58.196.36   TCP       66              50121 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   9 2020/209 14:30:40.043794   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 14:30:40.044803   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
```

3. Konfigurasi audit policies. Aplikasi aktual sering mengandung multiple rule. Perlu untuk memeriksa rule yang mengatur traffic aplikasi dikenali oleh database IAM.



	Applicable Users	Applicable AP(Group)	Endpoint Device	Destination	Created By
t activities a...	All users	All	All	All	admin



☑	No.	Name
Audit Policy (1)		
□	1	Various Internet

Audit Policy [Various Internet activities and traffic]

☑ Enabled

Name: Various Internet activities and traffic

Description: Highest level, logging all activities and contents of posting, email, chat

Audit Policy

- ☑ Application
- ☑ Flow/Online Duration
- ☑ Webpage Content

Application

□	No.	Item
☑	1	Web-based BBS posting Web Mail contents Web-based attachment upload (including W Web-based text upload Microblogging contents .....

Select Item

☑ File name of downloaded file

Email

☑ Outgoing email(SMTP)

☑ Incoming email(POP3/IMAP)

IM

☑ IM Chats

IM Software: MSN, Yahoo, Google-talk, Fetion, ...

☑ Other IM chats

FTP

☑ FTP file upload (file name and contents)

☑ FTP file download (file name only)

Telnet

☑ Commands executed via Telnet

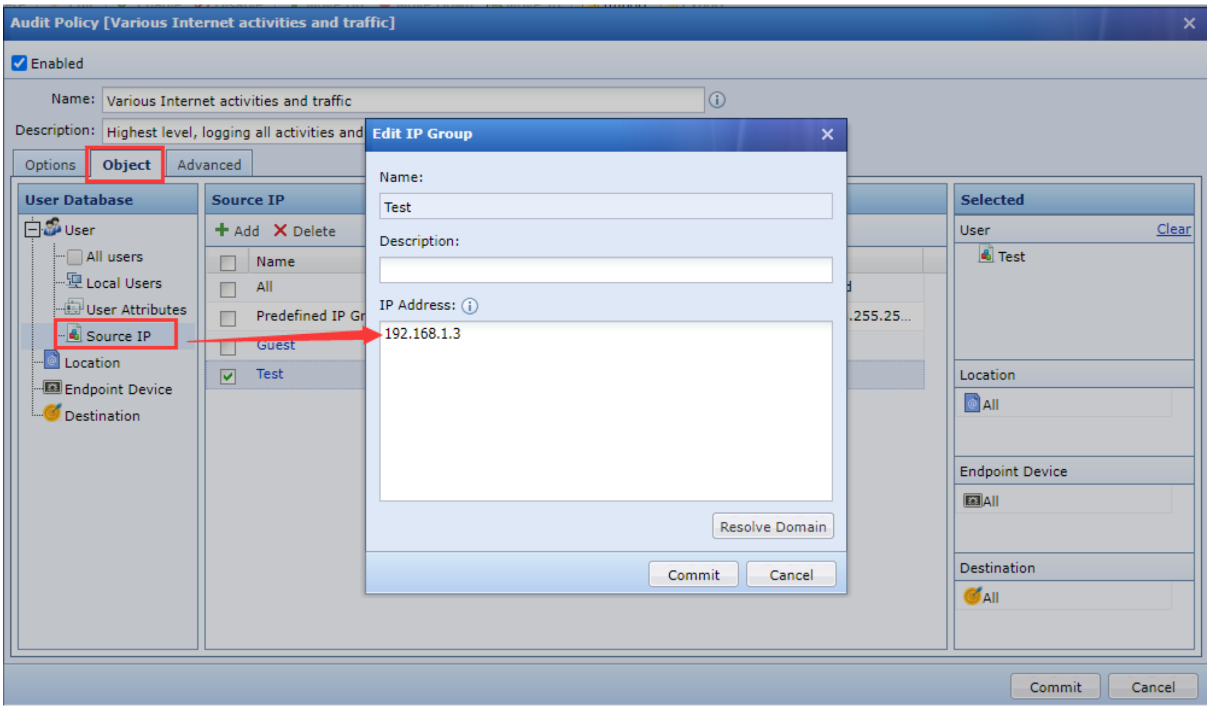
Application

☑ Access to other applications (exclusive of contents)

□ Access to unidentified applications (on which address and port. It incurs massive logs)

Action: Audit

Schedule: All Day



Audit Policy [Various Internet activities and traffic]

☑ Enabled

Name: Various Internet activities and traffic

Description: Highest level, logging all activities and

Options | **Object** | Advanced

User Database: User — All users, Local Users, User Attributes, Source IP; Location; Endpoint Device; Destination

Source IP:

	Name
□	All
□	Predefined IP Gr
□	Guest
☑	Test

Edit IP Group

Name: Test

Description:

IP Address: 192.168.1.3

Resolve Domain | Commit | Cancel

Selected

User Clear
Test

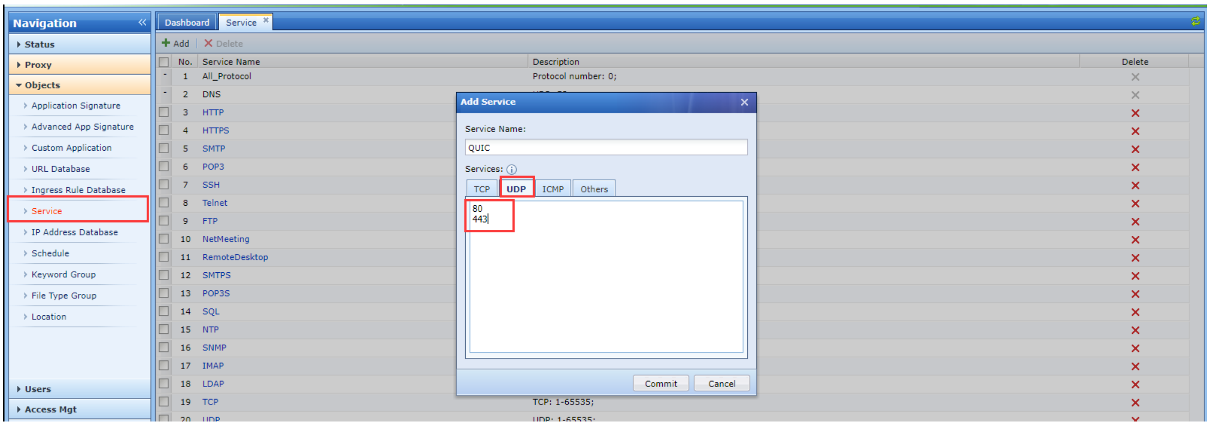
Location
All

Endpoint Device
All

Destination
All

Commit | Cancel

4. Sekarang banyak website dan browser menggunakan protokol QUIC untuk mengirimkan data, dan data terenkripsi oleh protokol QUIC tidak dapat dikontrol, sehingga protokol QUIC perlu dinonaktifkan. Setelah nonaktifkan protokol QUIC, website dan browser secara otomatis akan negosiasi penggunaa dari HTTPS untuk mengirimkan data.



No.	Service Name	Description
1	All_Protocol	Protocol number: 0;
2	DNS	
3	HTTP	
4	HTTPS	
5	SMTP	
6	POP3	
7	SSH	
8	Telnet	
9	FTP	
10	NetMeeting	
11	RemoteDesktop	
12	SMTPS	
13	POP3S	
14	SQL	
15	NTP	
16	SNMP	
17	IMAP	
18	LDAP	
19	TCP	TCP: 1-65535;
20	UDP	UDP: 1-65535;

Add Service

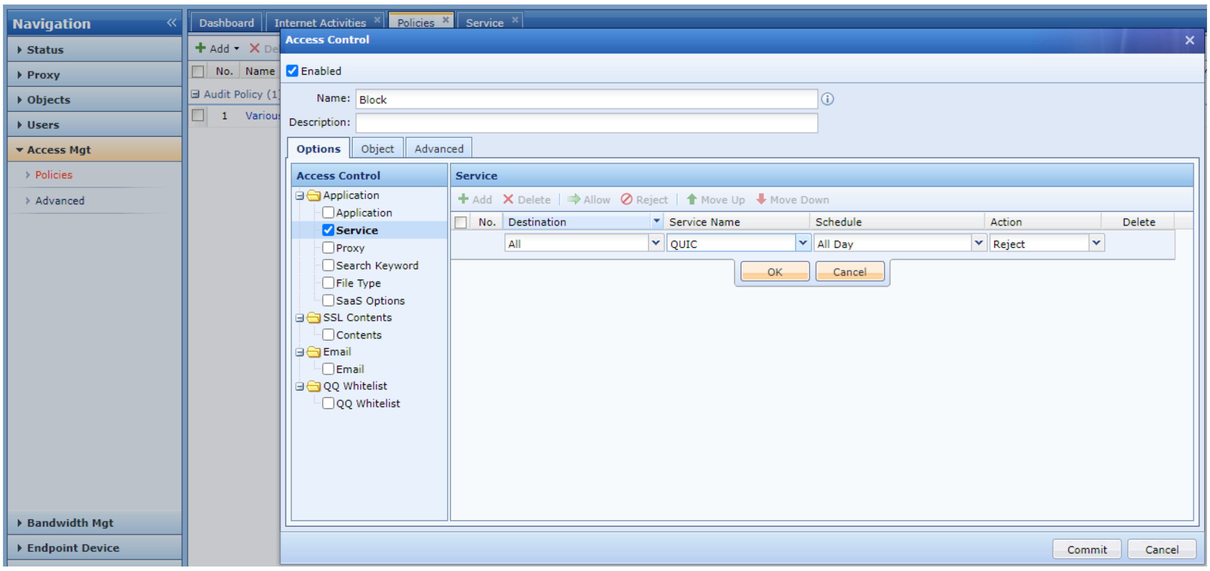
Service Name: QUIC

Services: TCP | **UDP** | ICMP | Others

80
443

Commit | Cancel

Access Control Policy



Access Control

☑ Enabled

Name: Block

Description:

Access Control

- Application
  - □ Application
  - ☑ Service
  - □ Proxy
  - □ Search Keyword
  - □ File Type
  - □ SaaS Options
- SSL Contents
  - □ Contents
- Email
  - □ Email
- QQ Whitelist
  - □ QQ Whitelist

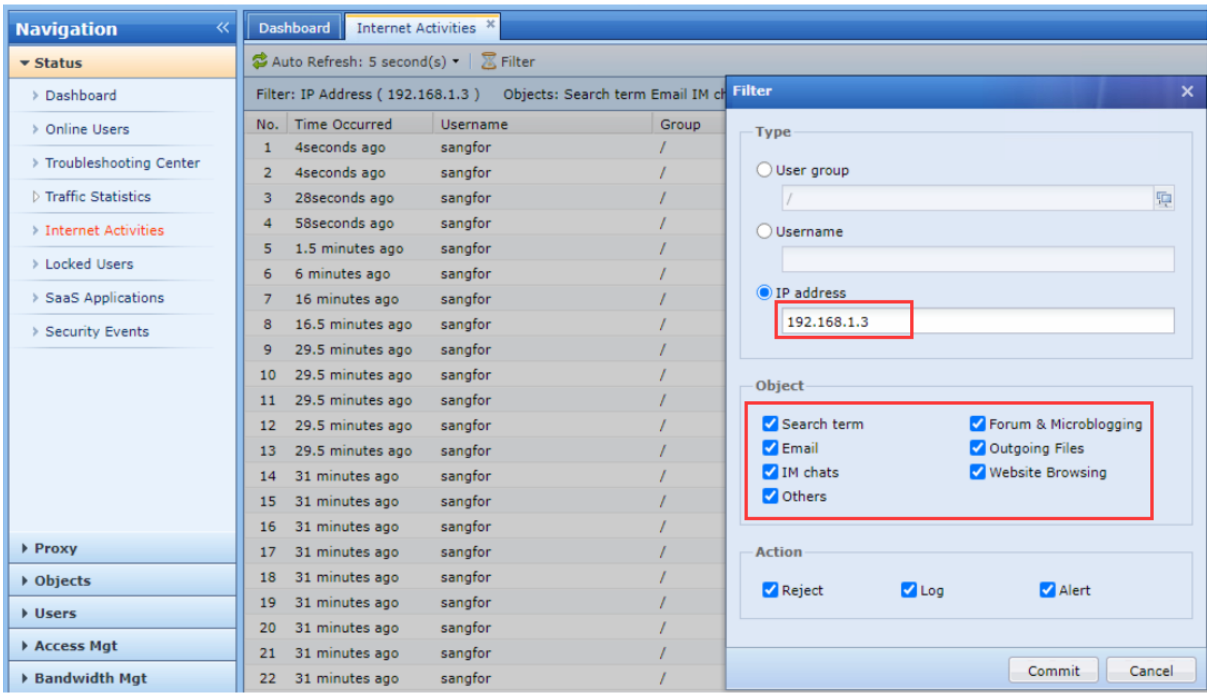
Service

No.	Destination	Service Name	Schedule	Action	Delete
	All	QUIC	All Day	Reject	

Bab 3 Konfigurasi

3.1 Block Facebook

1. Gunakan browser untuk mengakses facebook.com, dan periksa rule traffic Facebook yang telah dikenali dalam aktivitas Internet.



Filter: IP Address (192.168.1.3)   Objects: Search term Email IM ch

No.	Time Occurred	Username	Group
1	4seconds ago	sangfor	/
2	4seconds ago	sangfor	/
3	28seconds ago	sangfor	/
4	58seconds ago	sangfor	/
5	1.5 minutes ago	sangfor	/
6	6 minutes ago	sangfor	/
7	16 minutes ago	sangfor	/
8	16.5 minutes ago	sangfor	/
9	29.5 minutes ago	sangfor	/
10	29.5 minutes ago	sangfor	/
11	29.5 minutes ago	sangfor	/
12	29.5 minutes ago	sangfor	/
13	29.5 minutes ago	sangfor	/
14	31 minutes ago	sangfor	/
15	31 minutes ago	sangfor	/
16	31 minutes ago	sangfor	/
17	31 minutes ago	sangfor	/
18	31 minutes ago	sangfor	/
19	31 minutes ago	sangfor	/
20	31 minutes ago	sangfor	/
21	31 minutes ago	sangfor	/
22	31 minutes ago	sangfor	/

Filter

Type

○ User group

/

○ Username

● IP address

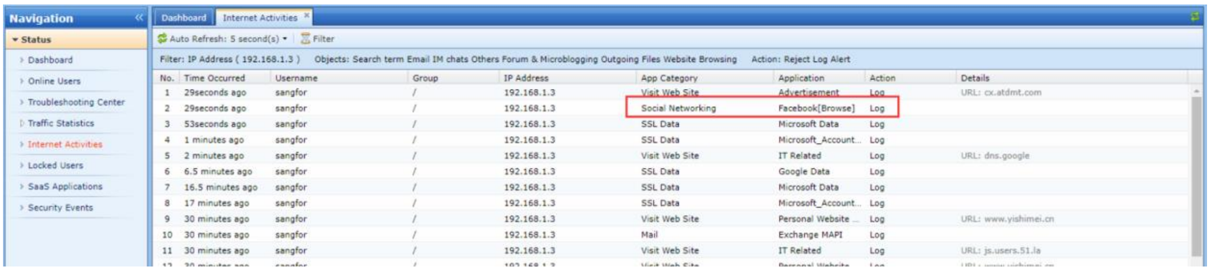
192.168.1.3

Object

☑ Search term ☑ Forum & Microblogging
☑ Email ☑ Outgoing Files
☑ IM chats ☑ Website Browsing
☑ Others

Action

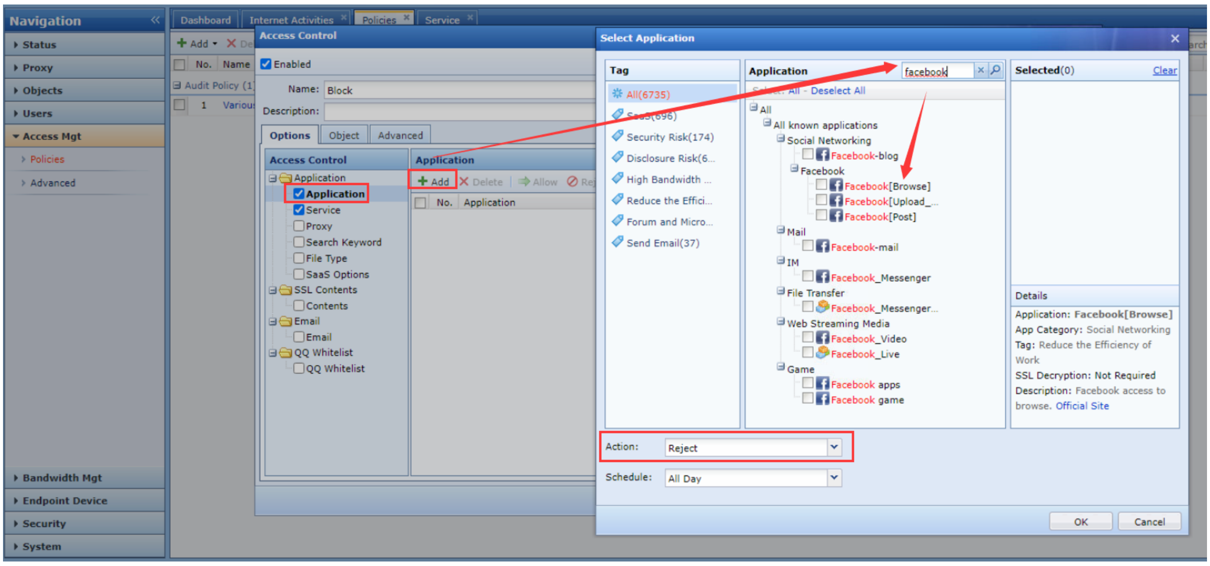
☑ Reject ☑ Log ☑ Alert



Filter: IP Address (192.168.1.3) Objects: Search term Email IM chats Others Forum & Microblogging Outgoing Files Website Browsing Action: Reject Log Alert

No.	Time Occurred	Username	Group	IP Address	App Category	Application	Action	Details
1	29seconds ago	sangfor	/	192.168.1.3	Visit Web Site	Advertisement	Log	URL: cx.atdmt.com
2	29seconds ago	sangfor	/	192.168.1.3	Social Networking	Facebook[Browse]	Log	
3	53seconds ago	sangfor	/	192.168.1.3	SSL Data	Microsoft Data	Log	
4	1 minutes ago	sangfor	/	192.168.1.3	SSL Data	Microsoft_Account...	Log	
5	2 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	IT Related	Log	URL: dns.google
6	6.5 minutes ago	sangfor	/	192.168.1.3	SSL Data	Google Data	Log	
7	16.5 minutes ago	sangfor	/	192.168.1.3	SSL Data	Microsoft Data	Log	
8	17 minutes ago	sangfor	/	192.168.1.3	SSL Data	Microsoft_Account...	Log	
9	30 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Personal Website ...	Log	URL: www.yishimei.cn
10	30 minutes ago	sangfor	/	192.168.1.3	Mail	Exchange MAPI	Log	
11	30 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	IT Related	Log	URL: js.users.51.la

2. Add aturan Facebook [Browse] yang sesuai dalam rule aplikasi control policy, dan pilih action sebagai reject.



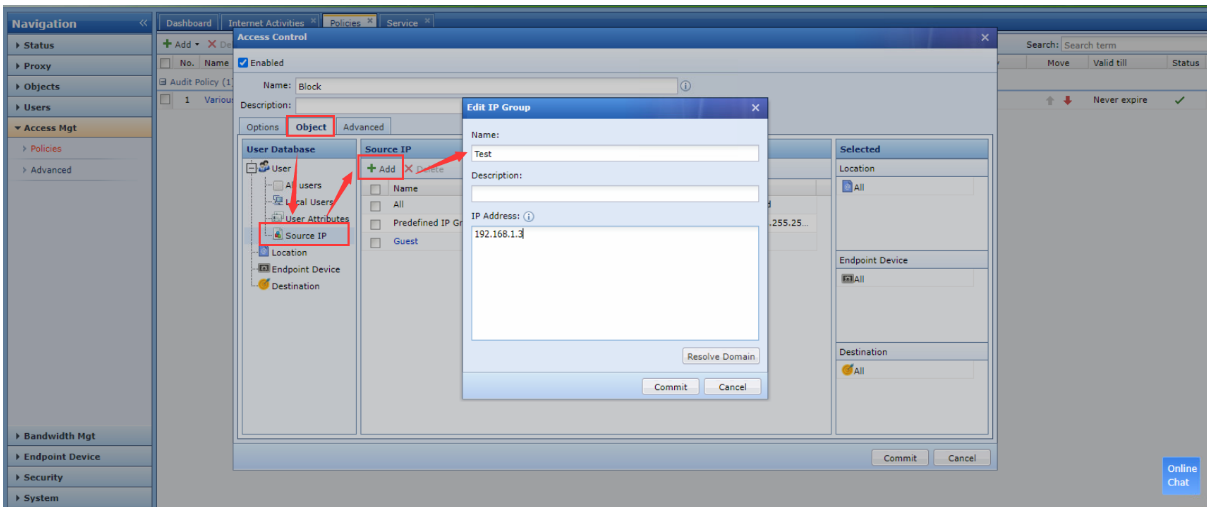
Name: Block

Application: Facebook[Browse]
App Category: Social Networking
Tag: Reduce the Efficiency of Work
SSL Decryption: Not Required
Description: Facebook access to browse. Official Site

Action: Reject

Schedule: All Day

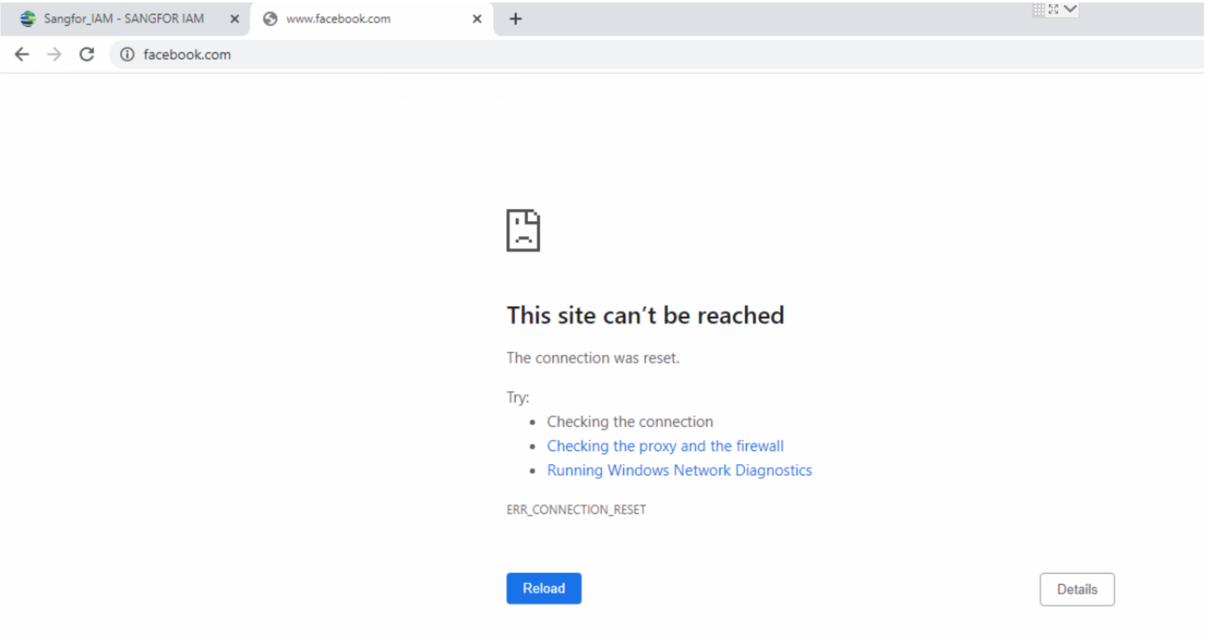
3. Pilih pengguna yang perlu dicocokan oleh policy, Anda dapat memilih berdasarkan username atau source IP, Anda dapat memilih dengan username atau dengan source IP.



Name: Test

IP Address: 192.168.1.3

4. Akses Facebook lagi, Anda dapat melihat bahwa Fecebook tidak lagi dapat diakses.



Sangfor_IAM - SANGFOR IAM | www.facebook.com

facebook.com

This site can't be reached

The connection was reset.

Try:

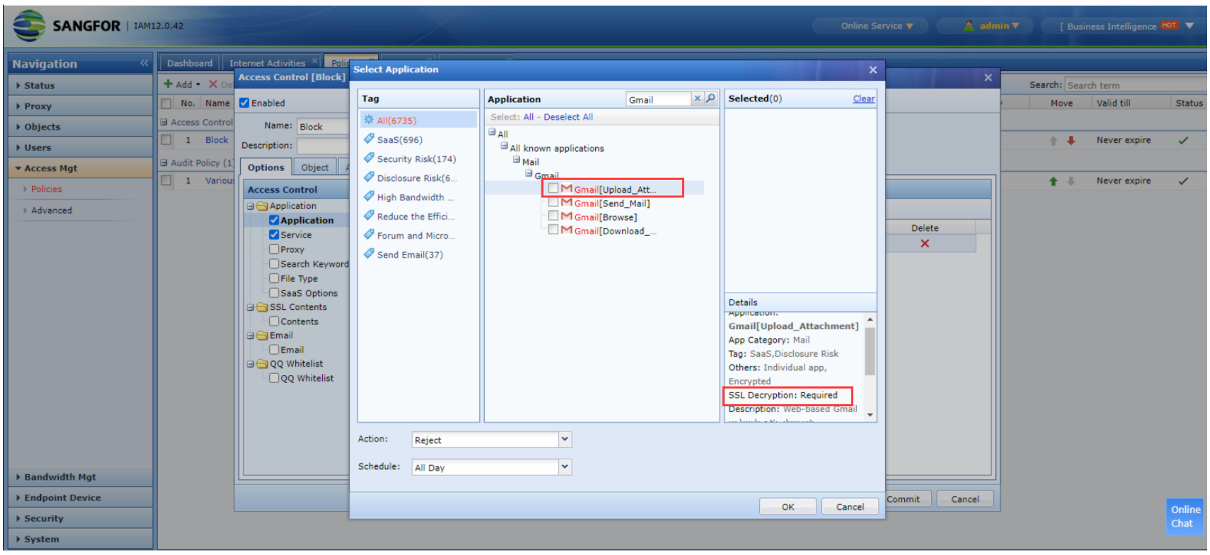
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET

Reload | Details

3.2 Block Gmail Outgoing Attachments

1. Jika Anda ingin melakukan control lebih detail tentang perilaku https website, seperti mengijinkan browsing tetapi tidak upload attachment, maka Anda perlu memeriksa rule deskripsi IAM untuk menentukan apakah Anda perlu decrypt traffic domain name yang relevan. Misalnya, setelah queri deskripsi rule basis, Anda dapat mengetahui bahwa Gmail upload attachment perlu mengaktifkan SSL data decryption.



Select Application

Tag: All(6735), SaaS(696), Security Risk(174), Disclosure Risk(6..., High Bandwidth ..., Reduce the Effici..., Forum and Micro..., Send Email(37)

Application: Gmail

Select: All - Deselect All

All
All known applications
Mail
Gmail
□ Gmail[Upload_Att...
□ Gmail[Send_Mail]
□ Gmail[Browse]
□ Gmail[Download_...

Selected(0) Clear

Details

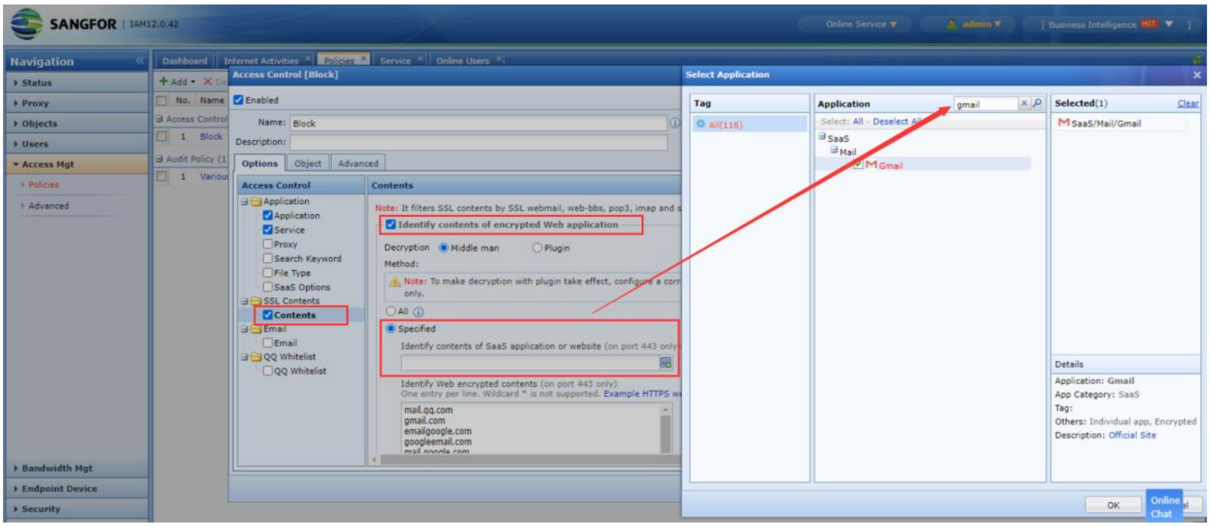
Gmail[Upload_Attachment]
App Category: Mail
Tag: SaaS,Disclosure Risk
Others: Individual app, Encrypted
SSL Decryption: Required
Description: Web-based Gmail

Action: Reject

Schedule: All Day

OK | Cancel

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



Access Control [Block]

☑ Enabled

Name: Block

Description:

Access Control
- Application
  - ☑ Application
  - ☑ Service
  - ☐ Proxy
  - ☐ Search Keyword
  - ☐ File Type
  - ☐ SaaS Options
- SSL Contents
  - ☑ Contents
- Email
  - ☐ Email
- QQ Whitelist
  - ☐ QQ Whitelist

Contents

Note: It filters SSL contents by SSL webmail, web-bbs, pop3, imap and s

☑ Identify contents of encrypted Web application

Decryption Method: ● Middle man ○ Plugin

Note: To make decryption with plugin take effect, configure a corr only.

○ All

● Specified

Identify contents of SaaS application or website (on port 443 only)

Identify Web encrypted contents (on port 443 only)
One entry per line. Wildcard * is not supported. Example HTTPS we

```
mail.qq.com
gmail.com
emailgoogle.com
googleemail.com
mail.google.com
```

Select Application

Tag: All(116)

Application: gmail

Select: All - Deselect All

- SaaS
  - Mail
    - ☑ Gmail

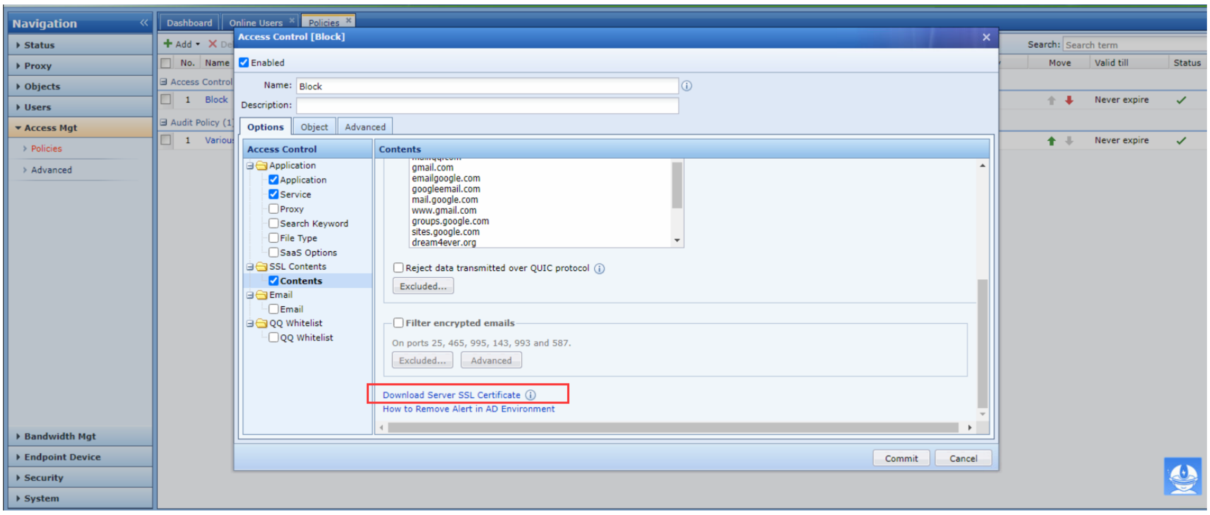
Selected(1) Clear

SaaS/Mail/Gmail

Details

Application: Gmail
App Category: SaaS
Tag:
Others: Individual app, Encrypted
Description: Official Site

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



Access Control [Block]

☑ Enabled

Name: Block

Description:

Access Control
- Application
  - ☑ Application
  - ☑ Service
  - ☐ Proxy
  - ☐ Search Keyword
  - ☐ File Type
  - ☐ SaaS Options
- SSL Contents
  - ☑ Contents
- Email
  - ☐ Email
- QQ Whitelist
  - ☐ QQ Whitelist

Contents

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

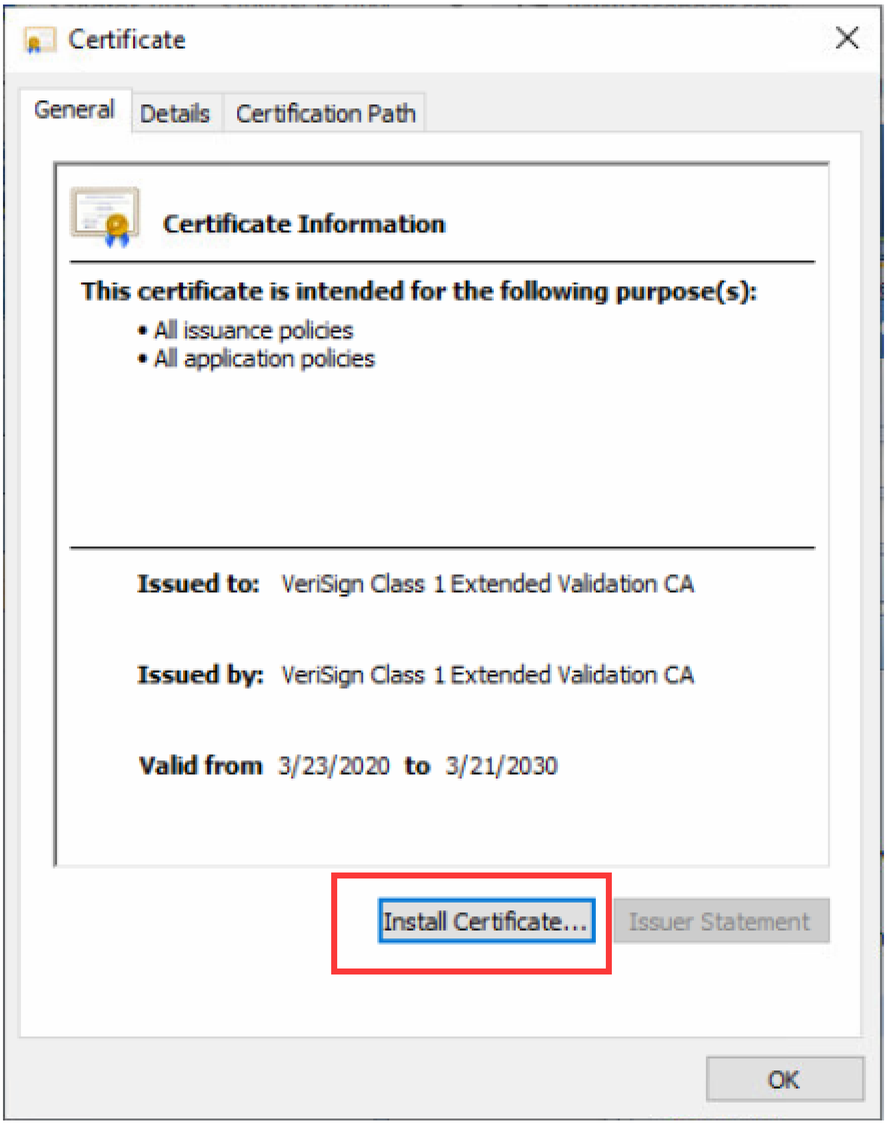
☐ Reject data transmitted over QUIC protocol

☐ Filter encrypted emails

On ports 25, 465, 995, 143, 993 and 587.

Download Server SSL Certificate

How to Remove Alert in AD Environment



Certificate Information

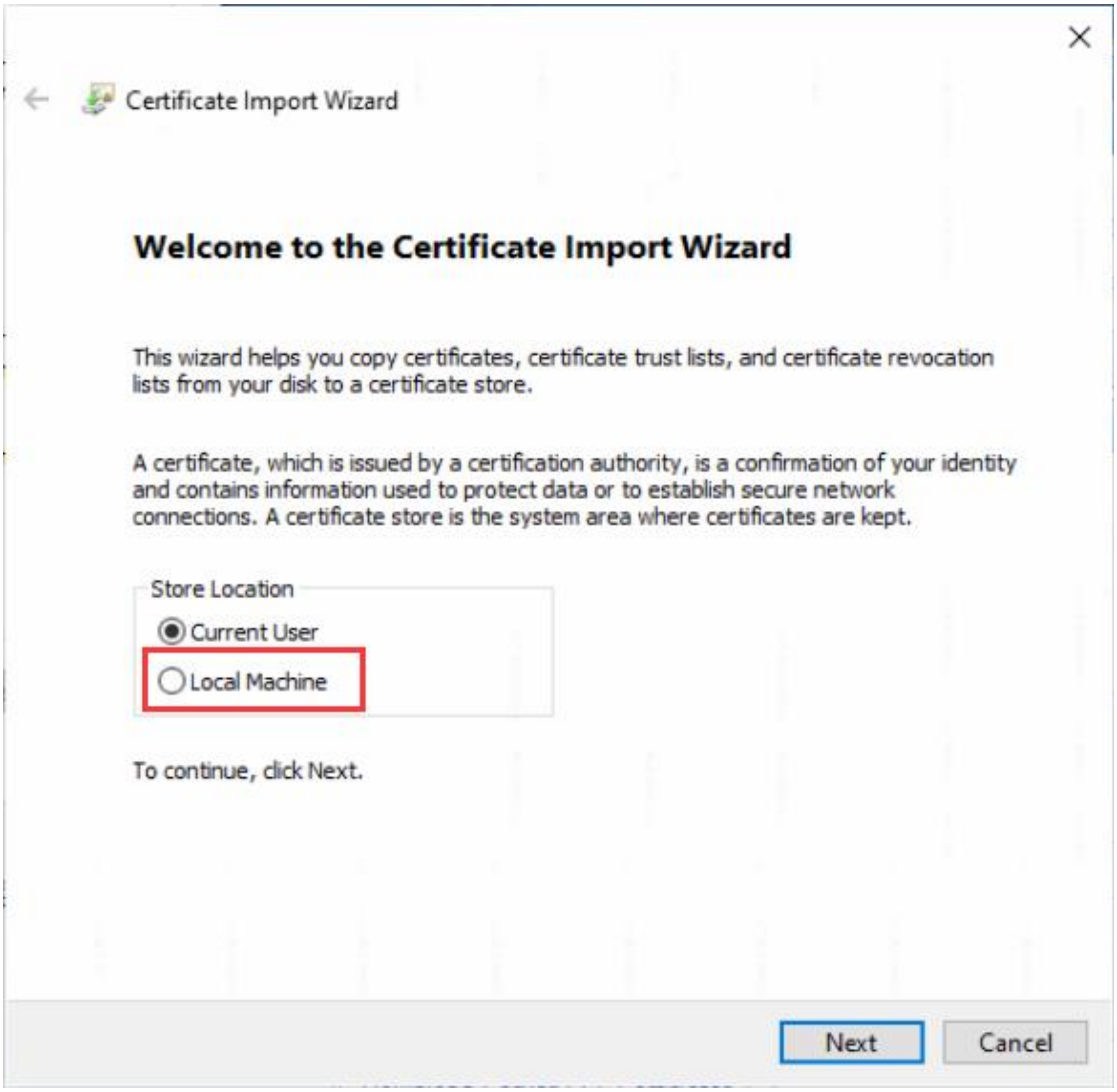
This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: VeriSign Class 1 Extended Validation CA

Issued by: VeriSign Class 1 Extended Validation CA

Valid from 3/23/2020 **to** 3/21/2030



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

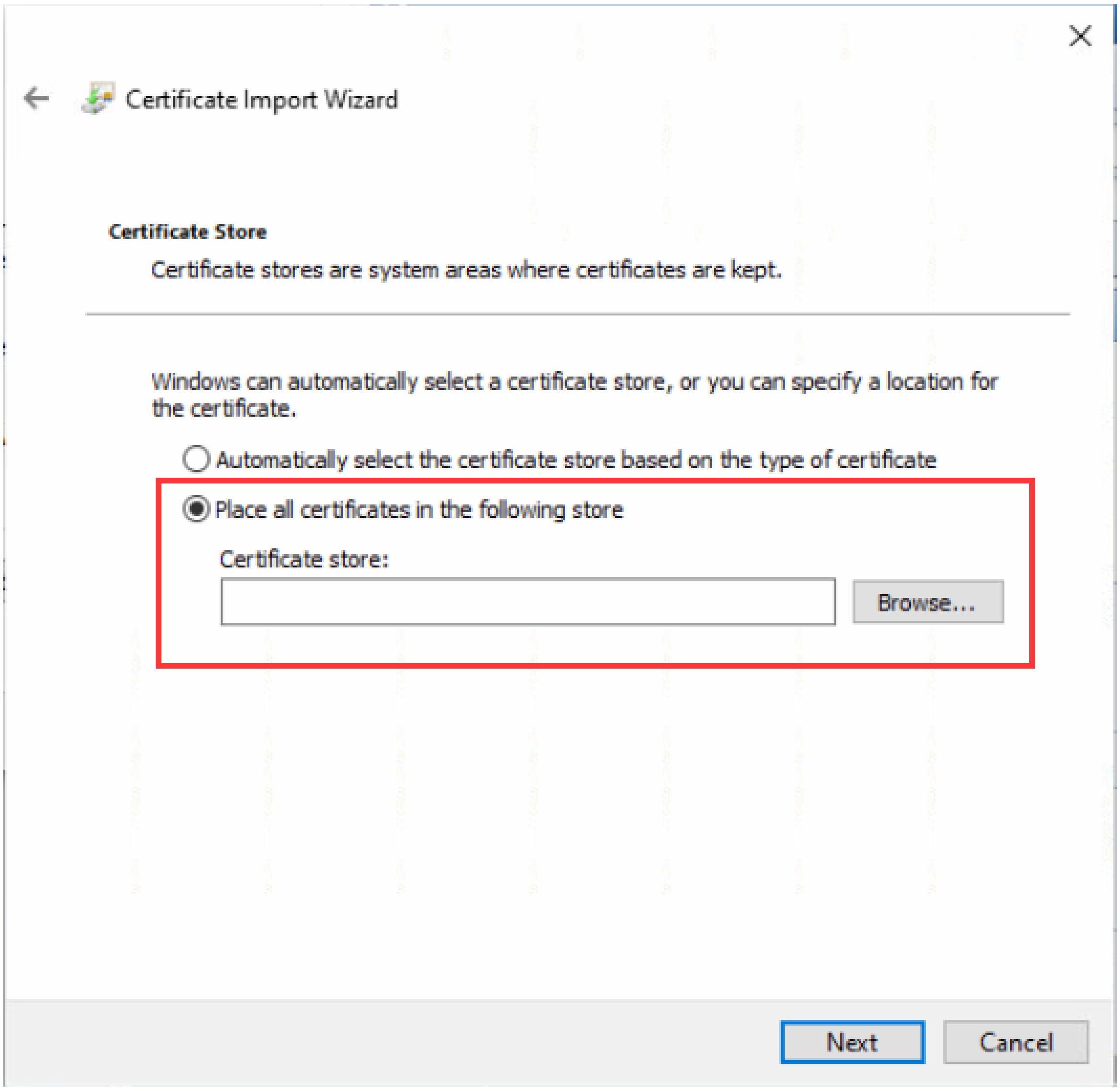
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

● Current User

○ Local Machine

To continue, click Next.



Certificate Import Wizard

Certificate Store

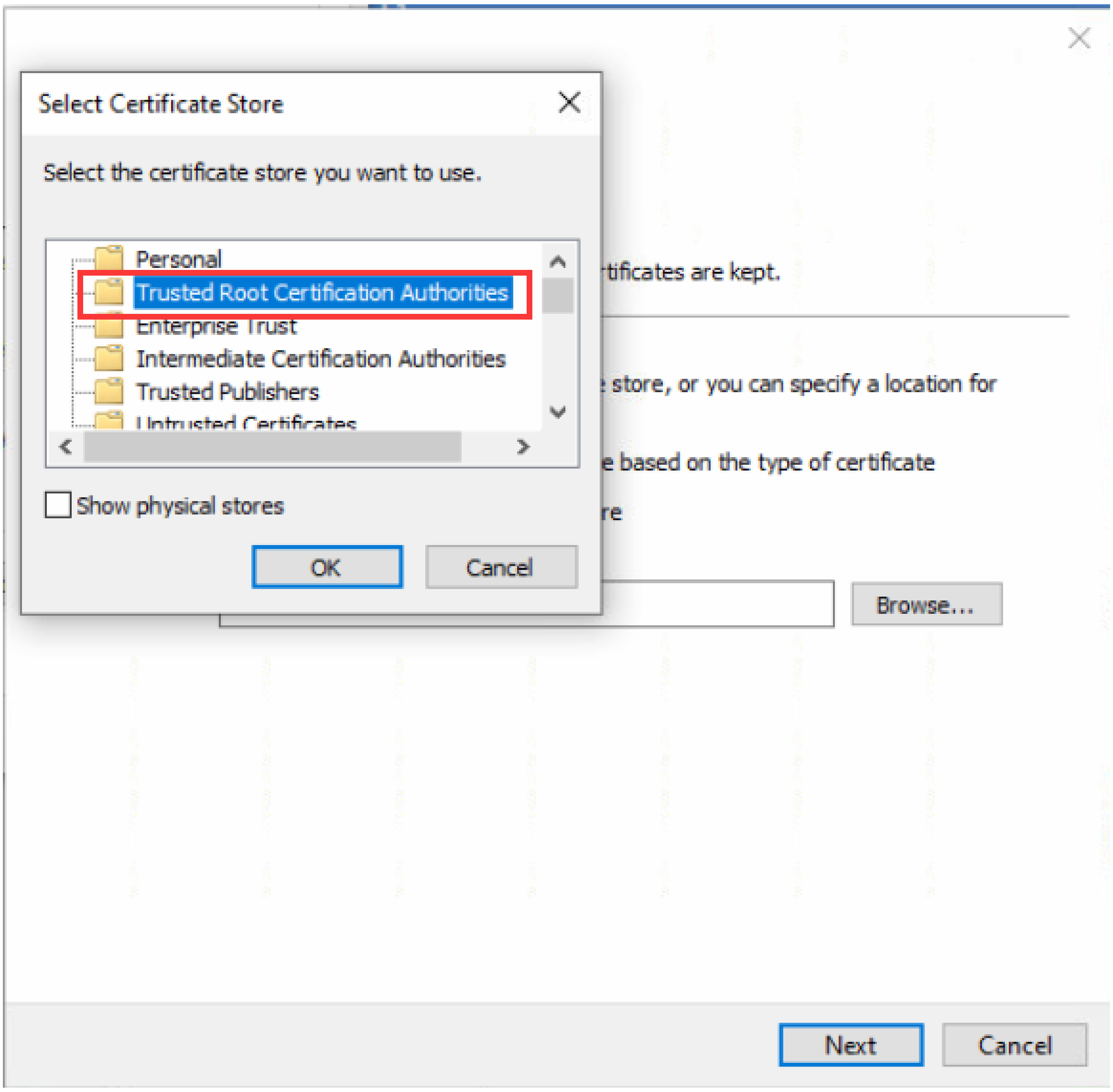
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:



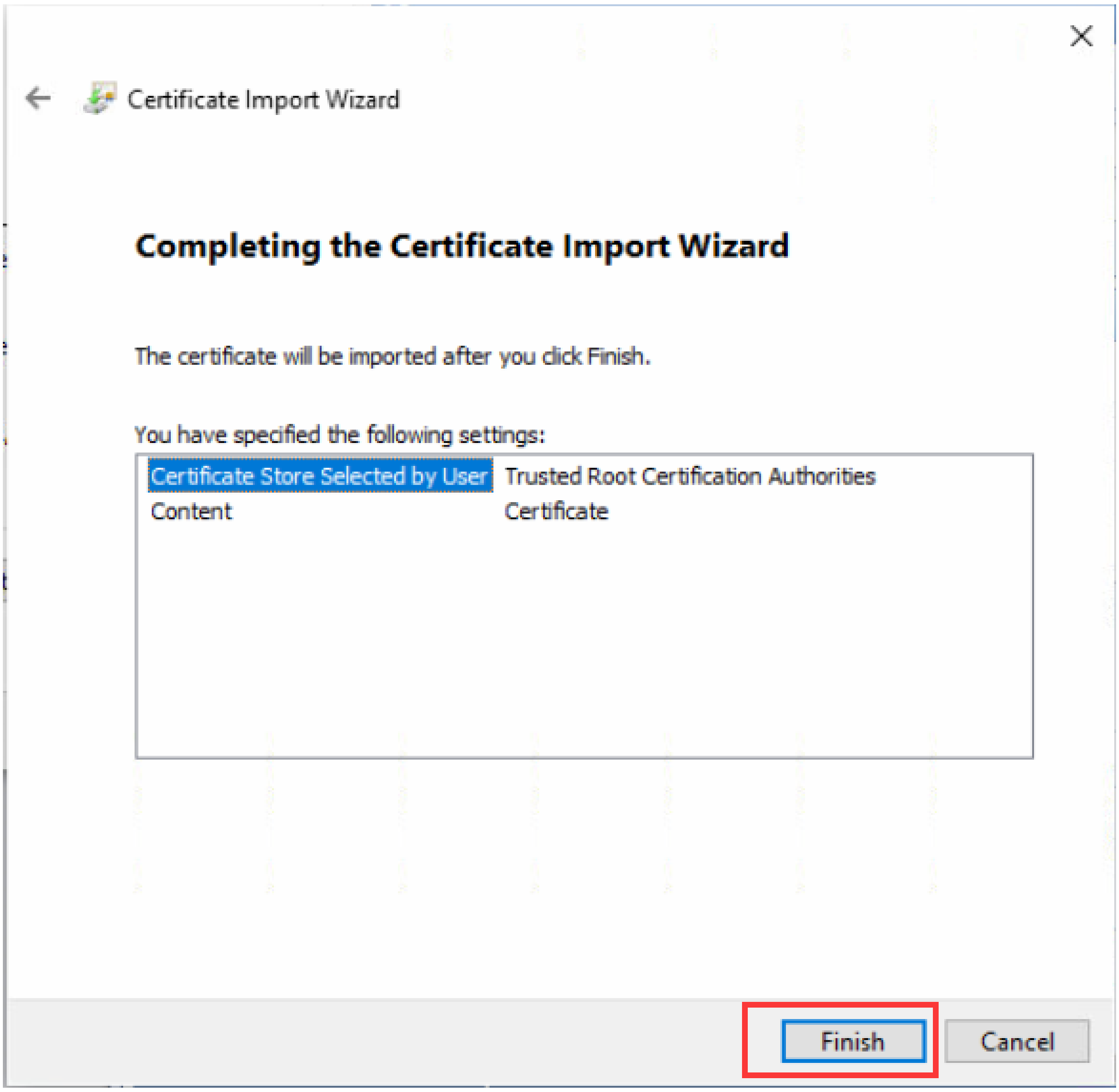
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

OK
Cancel
tificates are kept.
store, or you can specify a location for
e based on the type of certificate
re
Browse...
Next
Cancel



Certificate Import Wizard

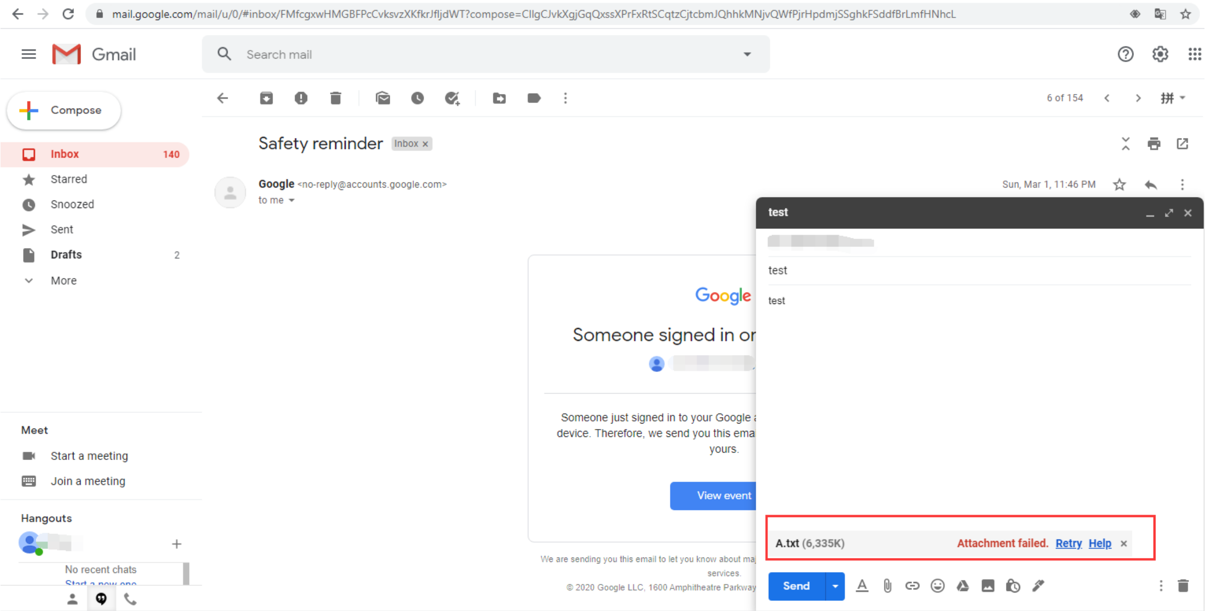
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

3. Ini menampilkan bahwa Gmail tidak dapat upload attachment, dan log dari reject attachment upload dapat ditanyakan dalam Internet Activities.



mail.google.com/mail/u/0/#inbox/FMfcgxwHMGBFPcCvksvzXKfkrJfljdWT?compose=CllgCJvkXgjGqQxssXPrFxRtSCqtzCjtcbmJQhhkMNjvQWfPjrHpdmjSSghkFSddfBrLmfHNhcL

Safety reminder

Google <no-reply@accounts.google.com>

to me

Sun, Mar 1, 11:46 PM

Someone signed in or

Someone just signed in to your Google a
device. Therefore, we send you this ema
yours.

We are sending you this email to let you know about ma
services.

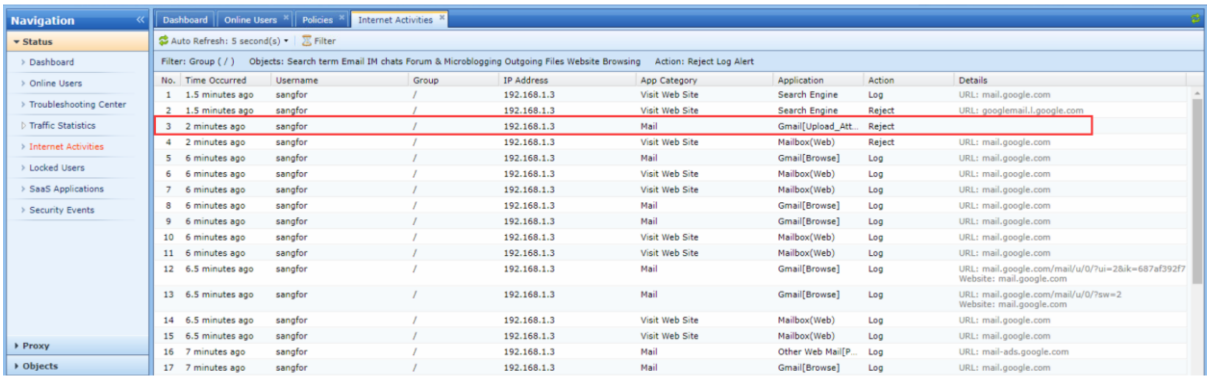
© 2020 Google LLC, 1600 Amphitheatre Parkway

test

test

test

A.txt (6,335K) Attachment failed. Retry Help ×



Filter: Group (/)   Objects: Search term Email IM chats Forum & Microblogging Outgoing Files Website Browsing   Action: Reject Log Alert

No.	Time Occurred	Username	Group	IP Address	App Category	Application	Action	Details
1	1.5 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: mail.google.com
2	1.5 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Reject	URL: googlemail.l.google.com
3	2 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Upload_Att...	Reject	
4	2 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Reject	URL: mail.google.com
5	6 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com
6	6 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
7	6 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
8	6 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com
9	6 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com
10	6 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
11	6 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
12	6.5 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	6.5 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com/mail/u/0/?sw=2 Website: mail.google.com
14	6.5 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
15	6.5 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
16	7 minutes ago	sangfor	/	192.168.1.3	Mail	Other Web Mail[P...	Log	URL: mail-ads.google.com
17	7 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com

Bab 4 Tindakan Pencegahan

1. Disarankan untuk upload file baru yang belum diupload. Jika file ada di Google server, itu tidak akan diupload kembali. Ini akan menampilkan bahwa upload selesai dalam seketika. Dengan cara ini, traffic dari upload attachment tidak benar-benar melewati IAM, jadi IAM tidak Blocked. Untuk membuat brand file baru, Anda dapat melakukan operasi berikut : secara manual buat txt file, kemudian isi fields didalamnya, dan terus copy dan paste untuk membuat ukuran file sekitar 5MB.

2. Sebelum memilih rule dalam aplikasi control policy, disarankan untuk membuka audit policy terlebih dahulu, kemudian gunakan aplikasi dan trigger traffic aplikasi yang relevan, dan kemudian amati rule actual aplikasi traffic yang sebenarnya berisi dalam aktivitas Internet.

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