SANGFOR

IAM

Email Filter Configuration Guide

Version 12.0.18

Change Log

Date	Change Description
Dec 24, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Content requirements

1 Product Introduction

Email that send from client internal network need to be control, reject the email with sensitive content, need to take control on the source and destination of the email as well as limit the content size and number of attachments of each email.

2 Application Scenario

Email filtering application scenario:

1. Focus on email that send by the internal user, take control of user behavior to avoid sensitive content from leaking.
2. Control the behavior of internal users.

3 Requirement Condition

1. IAM device with version 12.0.18 or above
2. Prepare a PC that able to communicate with public network.
3. Install any email client on the PC.

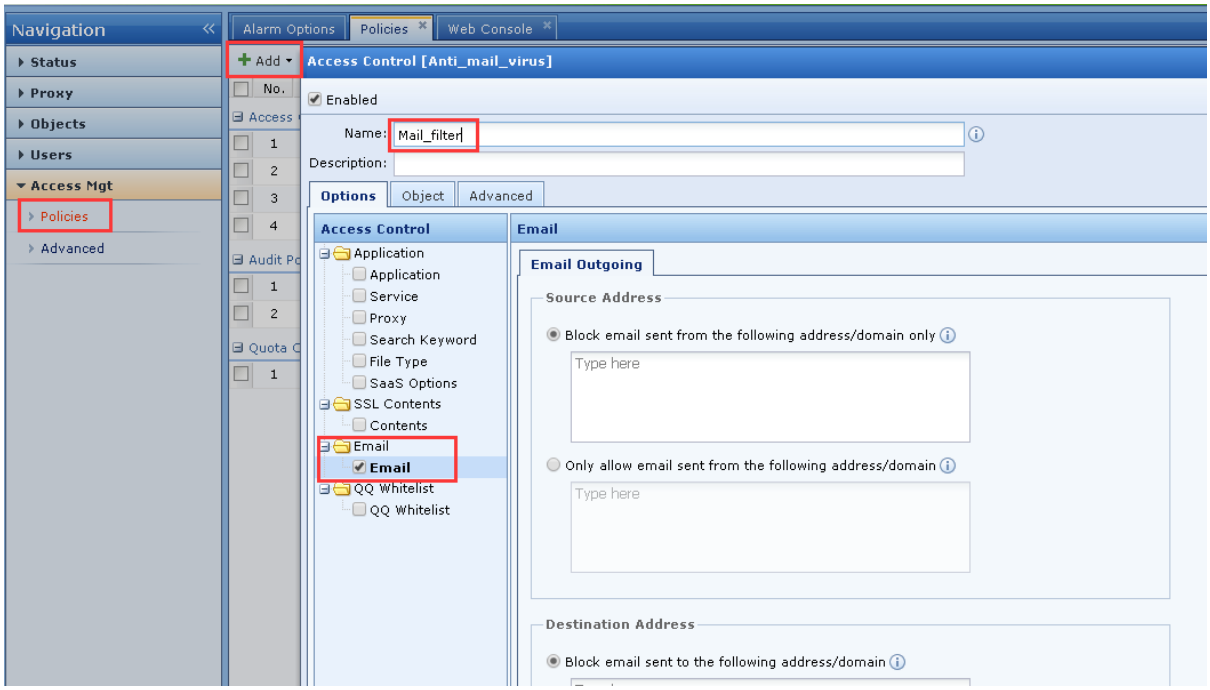
4 Configuration Idea

1. Well configure the email filtering policy on IAM
2. Setup a email client
3. Test send an email through client PC.
4. Test on encrypted email client whether it can send mail.

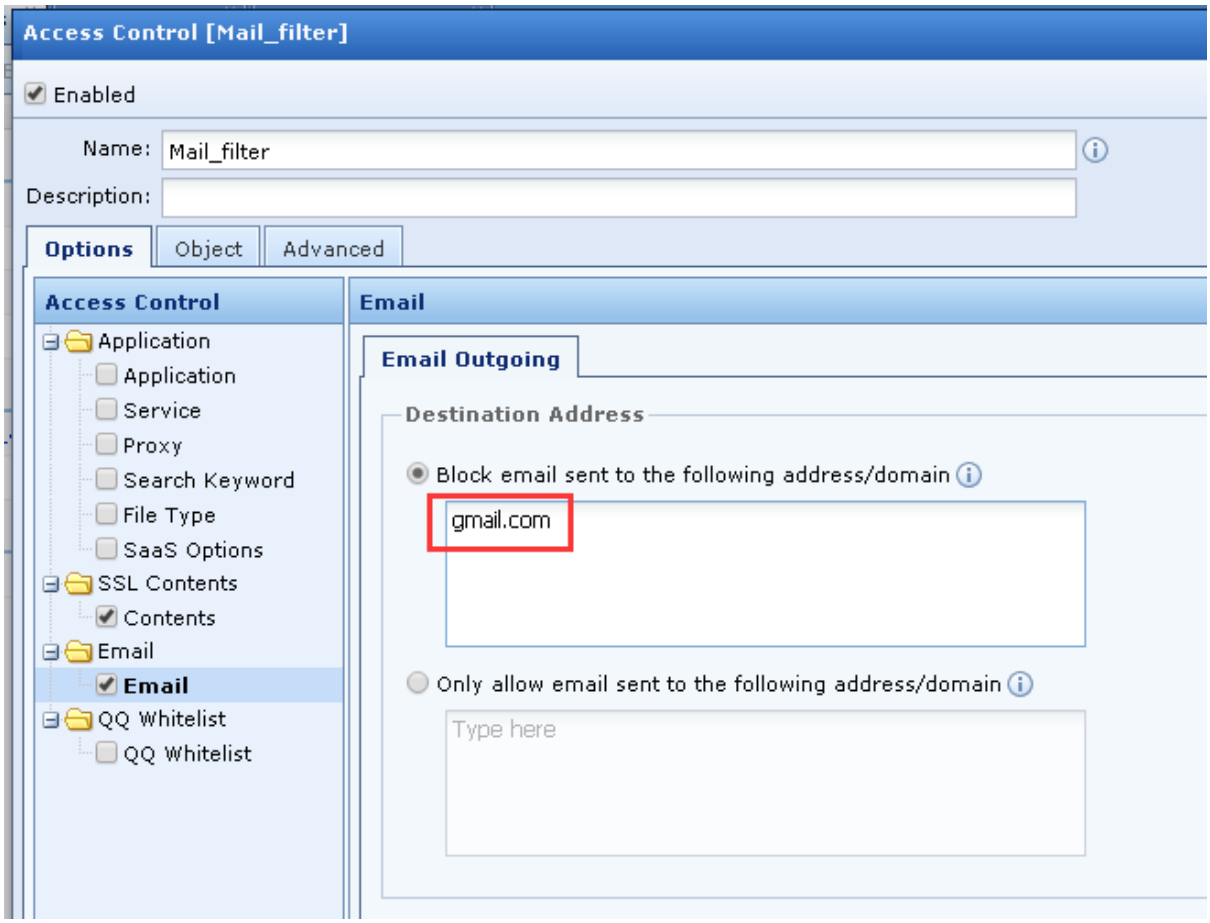
5 Configuration Guide with Screenshot

5.1 Configure Email filtering on IAM

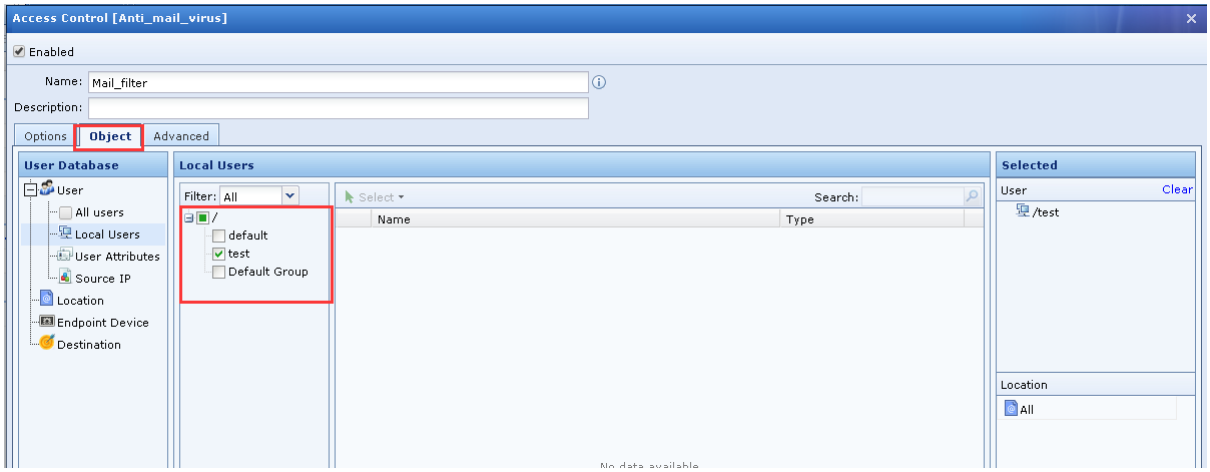
1. Configure the email filtering at [**Access Mgt**] – [**Policies**] – [**Access Control**] – [**Email**], the configuration must based on the requirement. In this document, we mainly focus on [**Destination Address**].



2. Insert the domain address that not allowed to send email at [**Destination Address**].

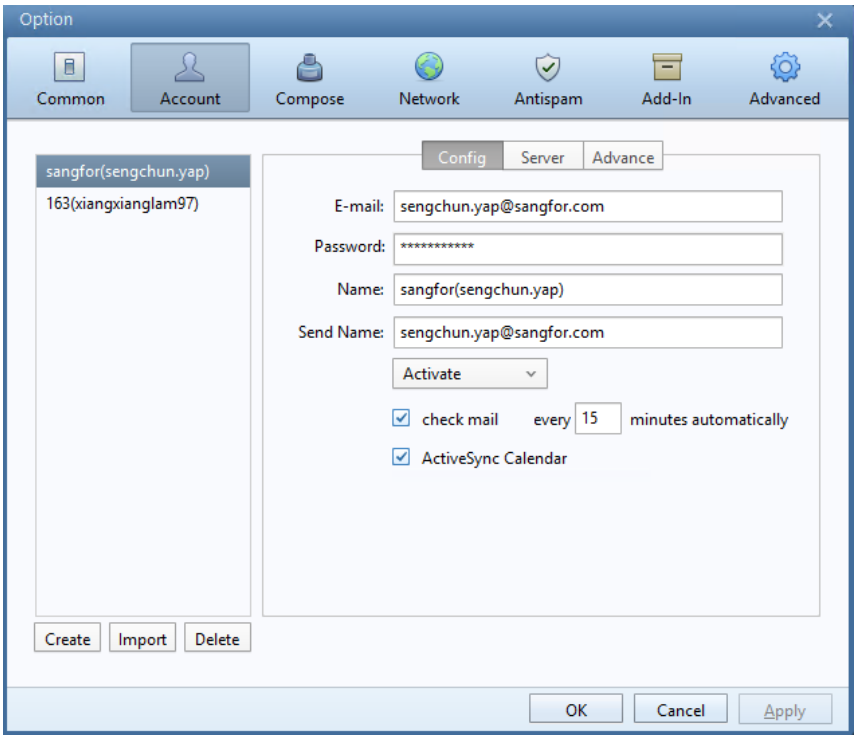


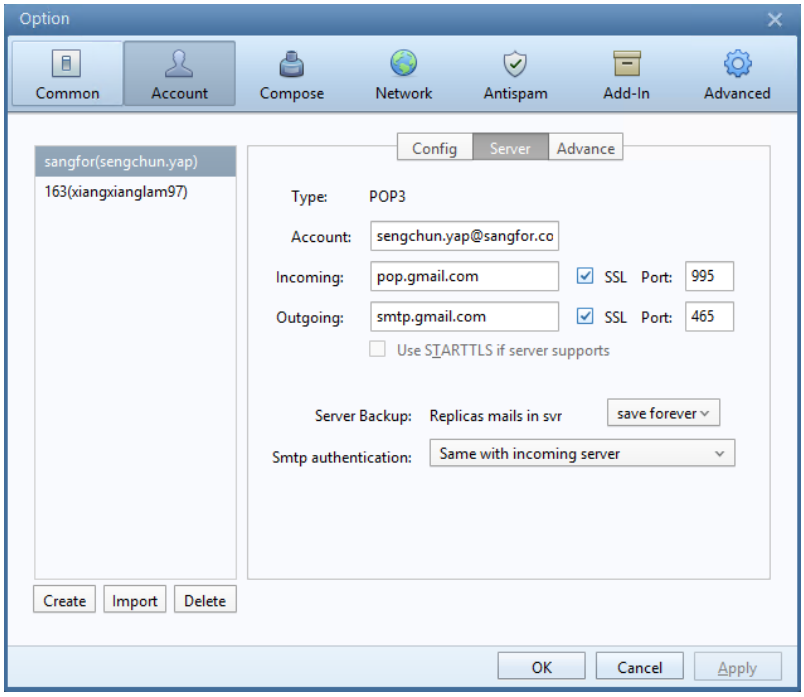
3. Assign the policy to specific test user.



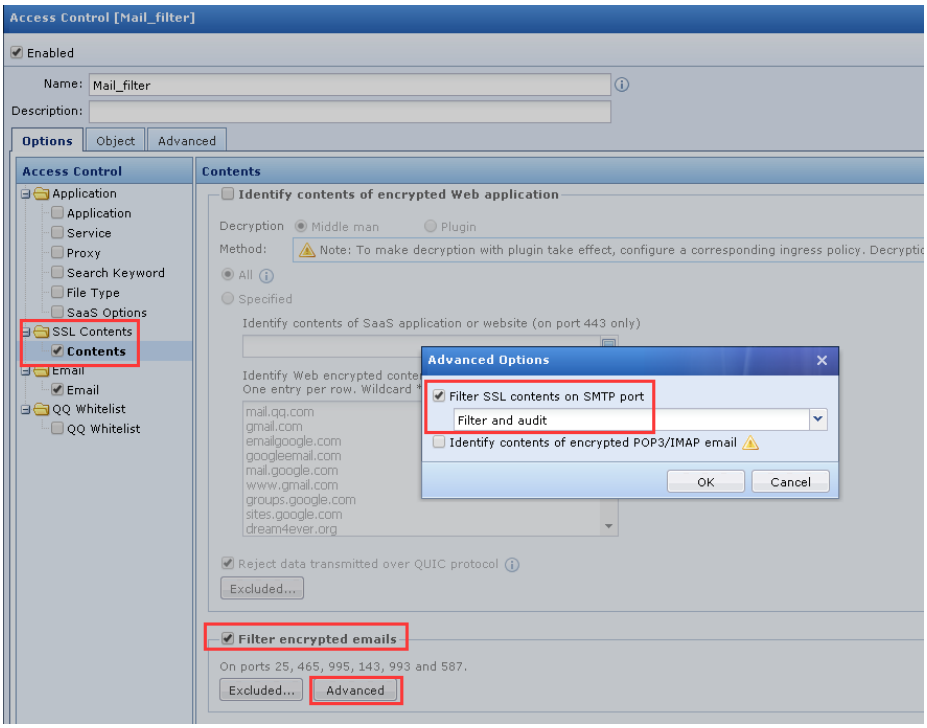
5.2 Email client configuration

1. Download Foxmail client, in this case we will used the gmail to send email. The configuration on "Server" will use secure SMTP with 465 port number.



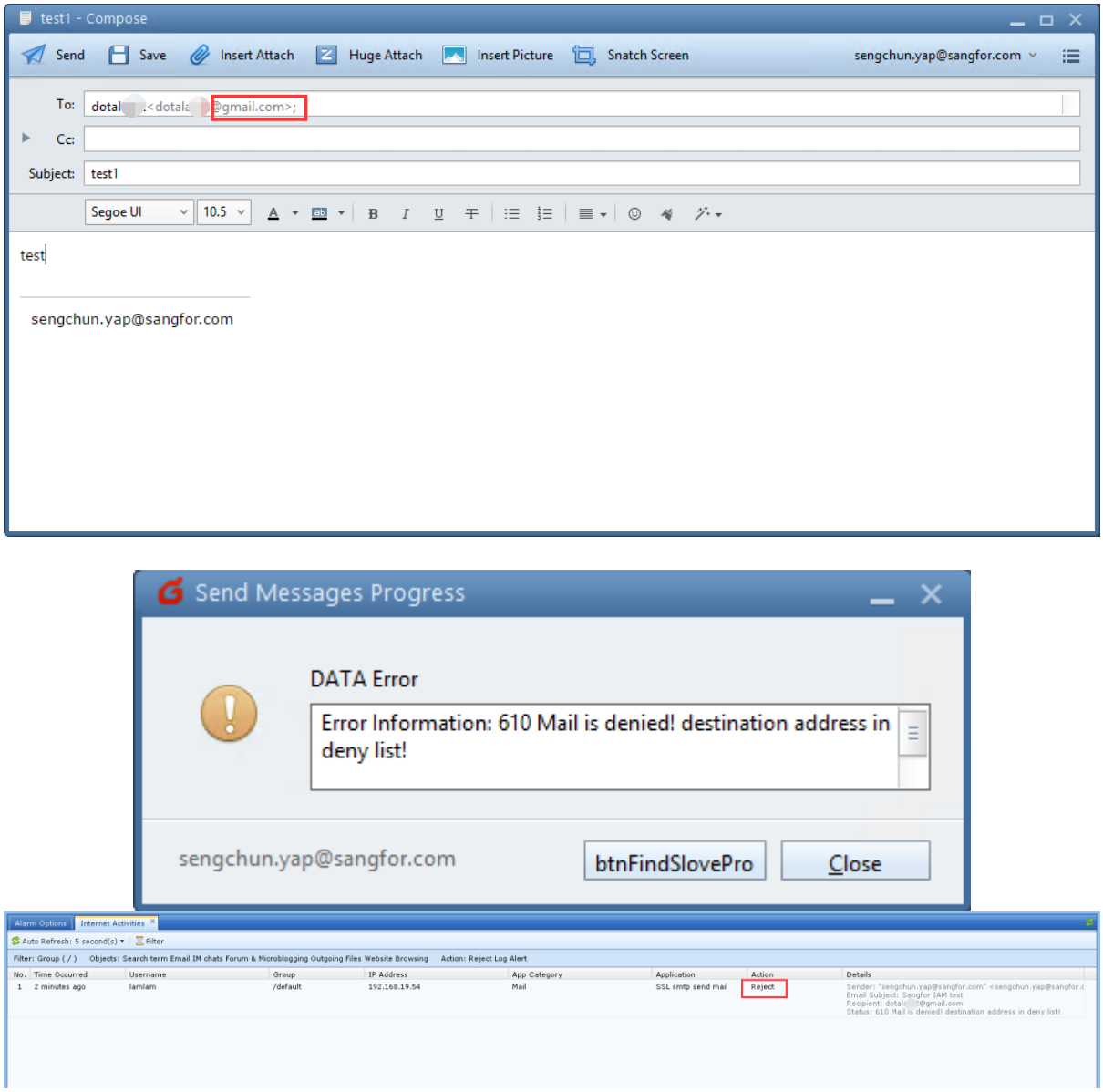


2. If the email client has configure with a secure protocol, we need to enable the [SSL content] function on the Mail_filter policy. Enable the [SSL content] function is able to encrypt the email and identify the source mail domain.



5.3 PC mail client testing result

Test send an email to gmail.com



As the diagram above show the testing result that email is being filter out and block by IAM device.

6 Precaution

1. Email filter only works on email client, do not include webmail.
2. The email address that insert in [Email] filter is able to insert a complete email address, for example xxx@abc.com. You also can insert with more than one email address, for example, @abc.com, cde.com. Important: If two email address write in a single line, it will match both abc.com and cde.com at the same time. Fill in the email address per line.
3. At the "Block outgoing email containing keyword" in [Email] filter, it support regular expressions, for example insert with "key.*d" , it will identify as "keyd","keyword" and etc. Recommended to fill in one keyword per line. If fill with many keyword in single line, please separate with commas.
4. IAM device mainly focus on SMTP/SMTPS protocol mail filtering, does not work for webmail, and make sure the traffic must pass through IAM device. The standard port number for mail sending SMTP/SMTPS is 25/465, if sending email by using other port number, then the email filter will not f functionable.
5. Make sure the device is able to communicate with the email server, else the email unable to send and email filter will not functionable.

SANGFOR