Project Summary

1) Assist in Setting up Python on a Windows 7 Workstation. python-3.7.4-amd64.exe is installed on the machine but will require assistance with any additional configurations needed for this project.
2) Assist in setting up Authentication, on the Windows 7 Workstation, to allow the Scripts to execute successfully.
3) Create Python Scripts based on the 2 scenarios detailed below in the “Project Details” section.
4) Provide the matching configurations of the Python scripts that were create that can be used to verify the functionality using POSTMAN.

Resource

- AsyncOS API 12.0 for Cisco Security Management Appliances - Getting Started Guide - GD (General Deployment)

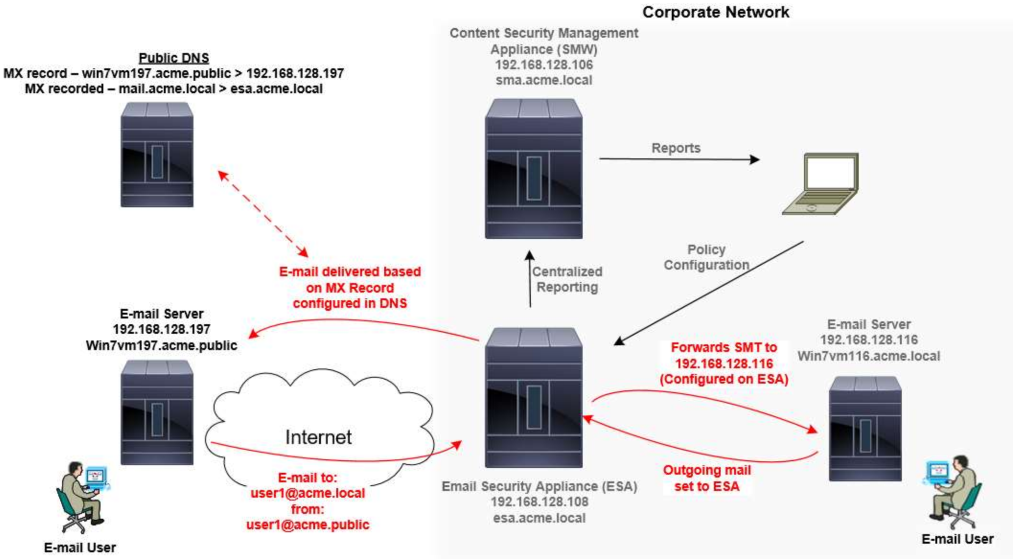
https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12.html

Test Environment Details

- Workstation running Windows 7 with python-3.7.4-amd64.exe & Postman-win64-7.7.3-Setup.exe for testing if needed.
- Cisco Content Security Management Appliance and Email Security Appliance installed and configured.
- The systems will be configured with TCTP/IP and all necessary initialization.

Project Details

A policy will be created to block incoming e-mail from the domain acme.public.



Access Information

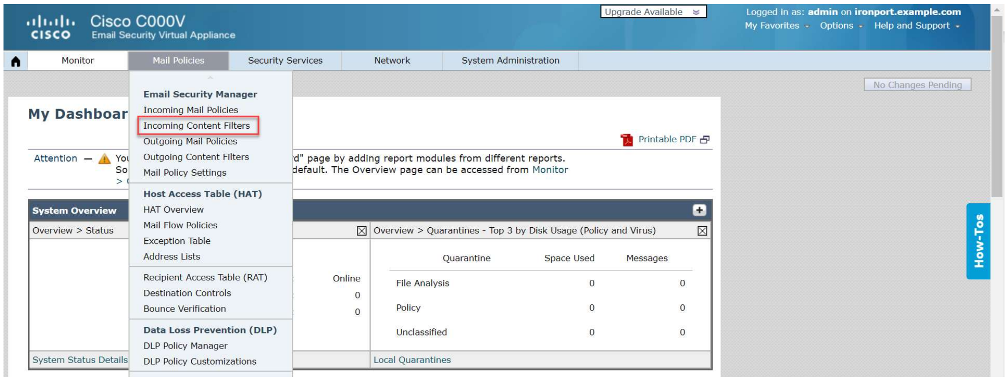
ESA GUI – username: admin / Password: WWTwwt1!
SMA GUI – username: admin / Password: WWTwwt1!
Workstations with Mail server and Client used to send/receive e-mail. RDP to IP address in diagram.
username: Admin / Password: WWTwwt1!

Configuration Example

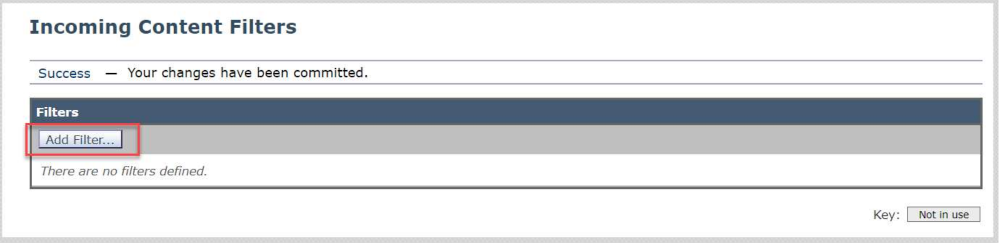
This scenario will use the Web Interface to show the configuration to block email incoming to the ESA from “acme.local”.

The configuration is performed on the ESA.

Create a Content Filter.



Quarantine	Space Used	Messages
File Analysis	0	0
Policy	0	0
Unclassified	0	0



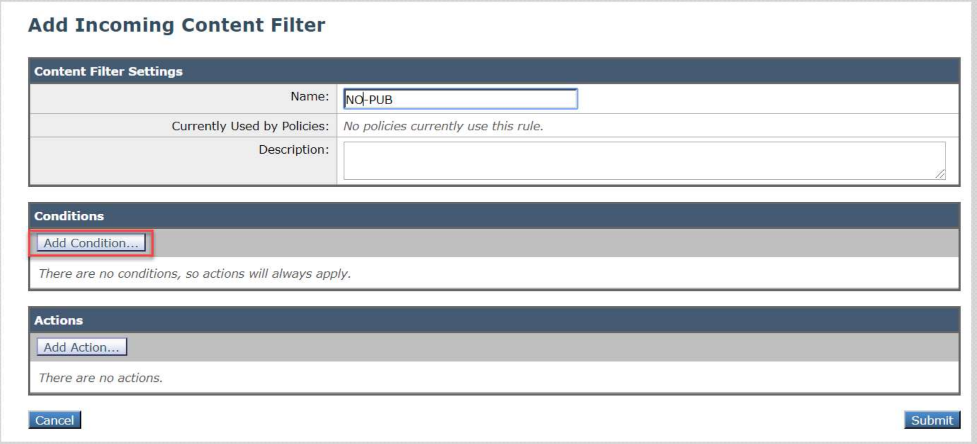
Incoming Content Filters

Success — Your changes have been committed.

Filters

There are no filters defined.

Key: Not in use



Add Incoming Content Filter

Content Filter Settings

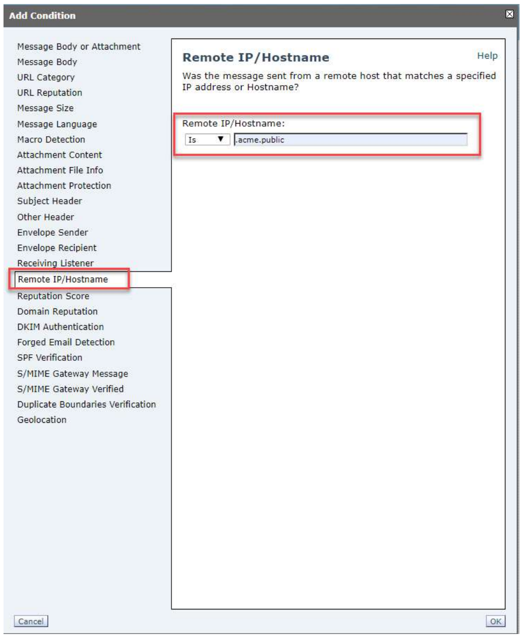
Name:	NO-PUB
Currently Used by Policies:	No policies currently use this rule.
Description:	

Conditions

There are no conditions, so actions will always apply.

Actions

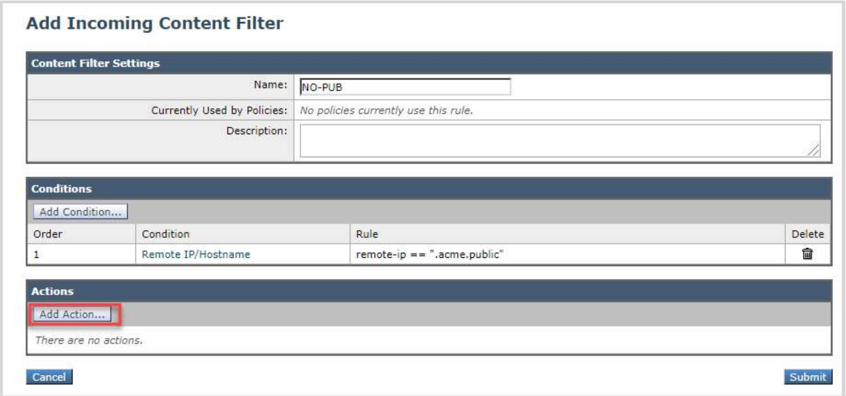
There are no actions.



Remote IP/Hostname

Was the message sent from a remote host that matches a specified IP address or Hostname?

Remote IP/Hostname: Is .acme.public



Add Incoming Content Filter

Content Filter Settings

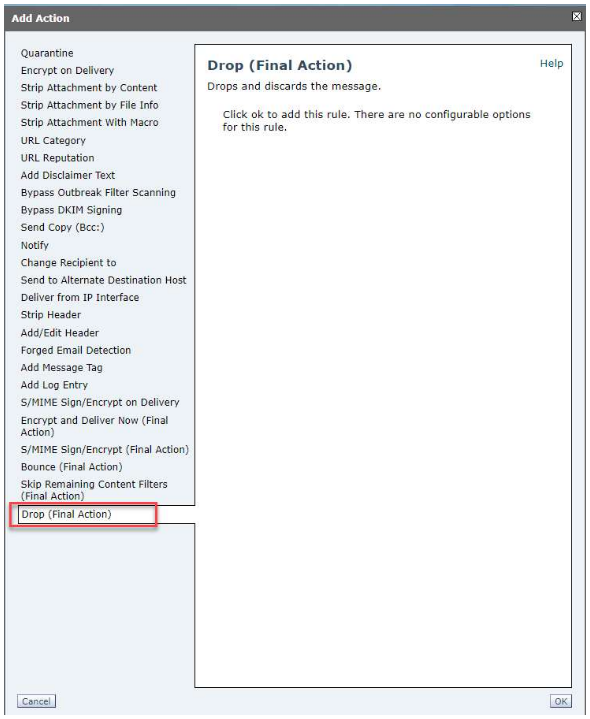
Name:	NO-PUB
Currently Used by Policies:	*No policies currently use this rule.*
Description:	

Conditions

Order	Condition	Rule	Delete
1	Remote IP/Hostname	remote-ip == ".acme.public"	🗑

Actions

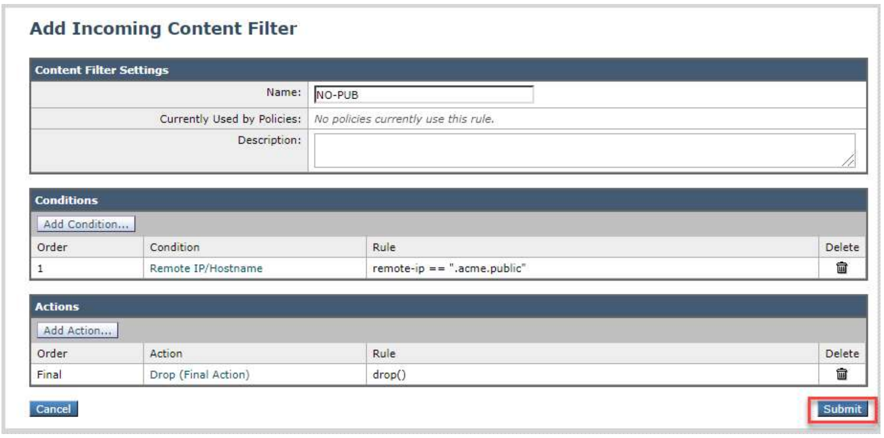
There are no actions.


Add Action
Quarantine
Encrypt on Delivery
Strip Attachment by Content
Strip Attachment by File Info
Strip Attachment With Macro
URL Category
URL Reputation
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Bypass DKIM Signing
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add/Edit Header
Forged Email Detection
Add Message Tag
Add Log Entry
S/MIME Sign/Encrypt on Delivery
Encrypt and Deliver Now (Final Action)
S/MIME Sign/Encrypt (Final Action)
Bounce (Final Action)
Skip Remaining Content Filters (Final Action)
Drop (Final Action)
Help
Cancel
OK

Drop (Final Action)

Drops and discards the message.

Click ok to add this rule. There are no configurable options for this rule.



Add Incoming Content Filter

Content Filter Settings

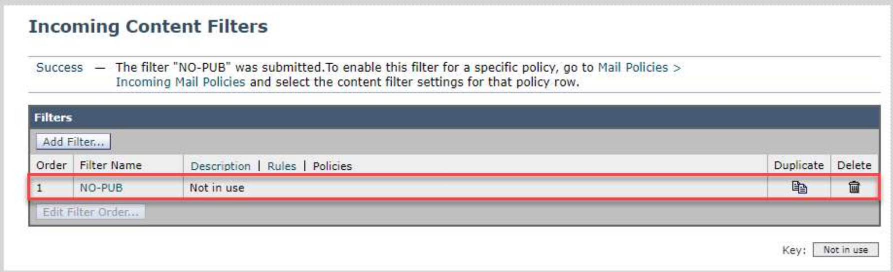
Name:	NO-PUB
Currently Used by Policies:	*No policies currently use this rule.*
Description:	

Conditions

Order	Condition	Rule	Delete
1	Remote IP/Hostname	remote-ip == ".acme.public"	🗑

Actions

Order	Action	Rule	Delete
Final	Drop (Final Action)	drop()	🗑



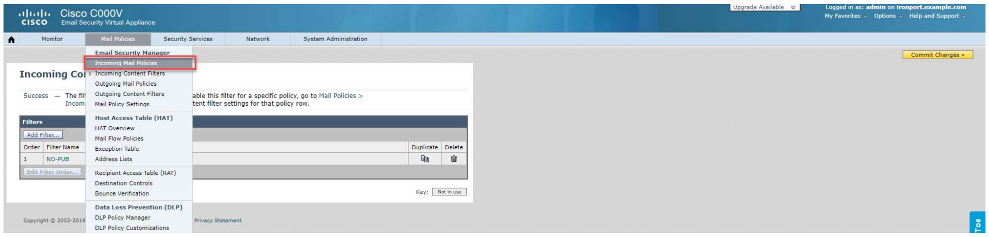
Incoming Content Filters

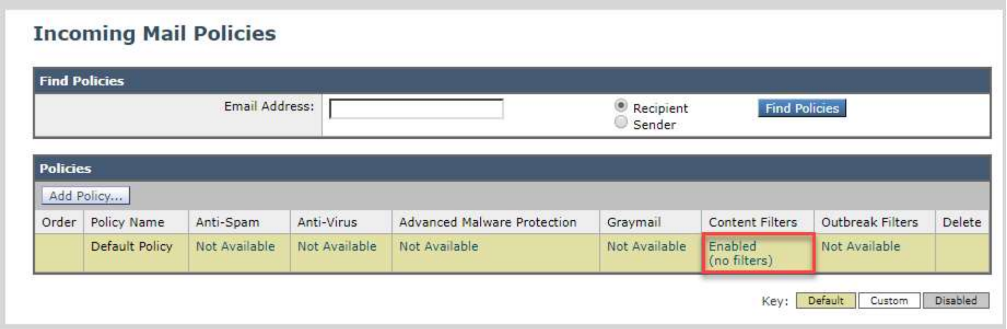
Success — The filter "NO-PUB" was submitted.To enable this filter for a specific policy, go to Mail Policies > Incoming Mail Policies and select the content filter settings for that policy row.

Filters

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	NO-PUB	Not in use	⧉	🗑

Apply the Content Filter to the default Incoming Mail Policy.





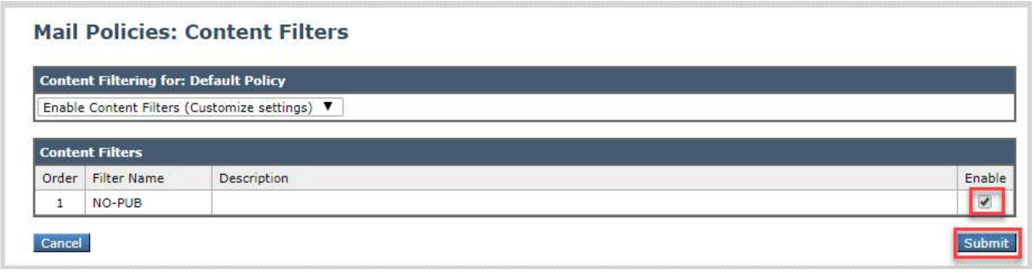
Incoming Mail Policies

Find Policies

Email Address: ______ ● Recipient ○ Sender

Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	Not Available	Not Available	Not Available	Not Available	Enabled (no filters)	Not Available	



Mail Policies: Content Filters

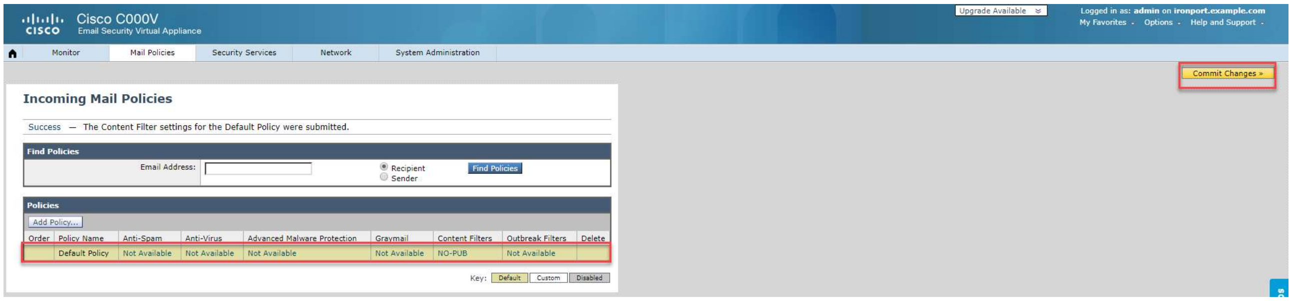
Content Filtering for: Default Policy

Enable Content Filters (Customize settings) ▼

Content Filters

Order	Filter Name	Description	Enable
1	NO-PUB		☑

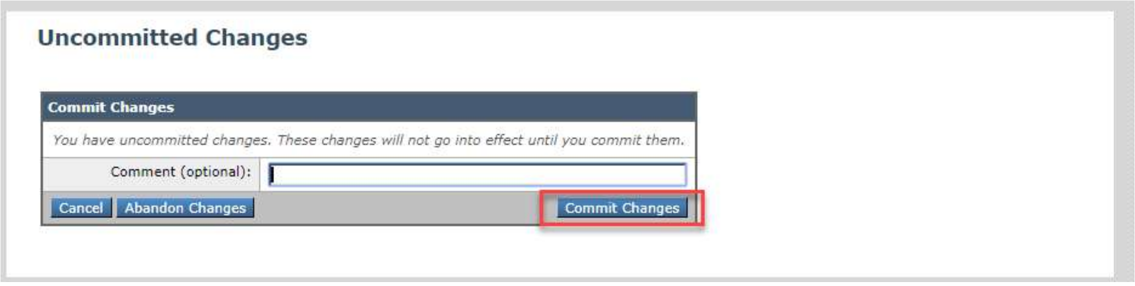
Must commit changes for the policy to become active.



Incoming Mail Policies

Success — The Content Filter settings for the Default Policy were submitted.

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	Not Available	Not Available	Not Available	Not Available	NO-PUB	Not Available	

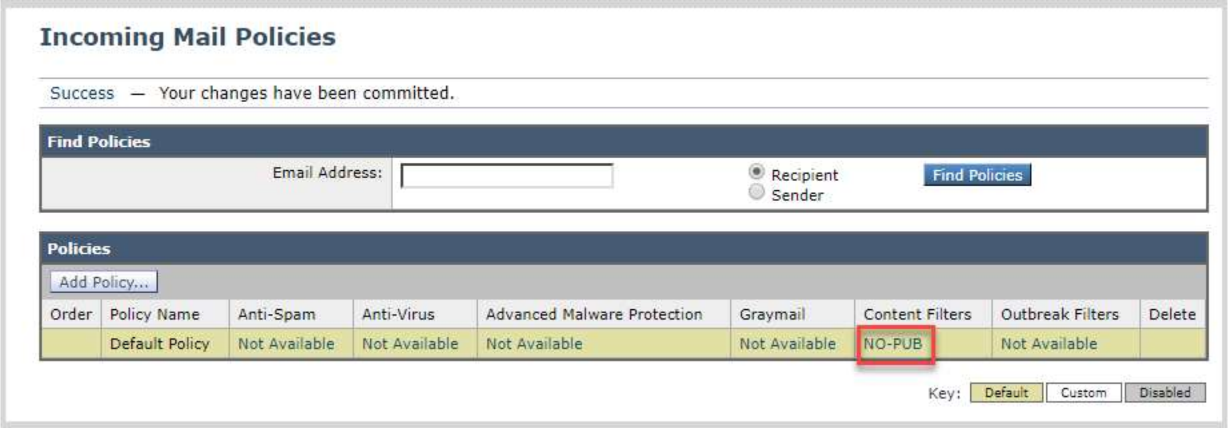


Uncommitted Changes

Commit Changes

You have uncommitted changes. These changes will not go into effect until you commit them.

Result.



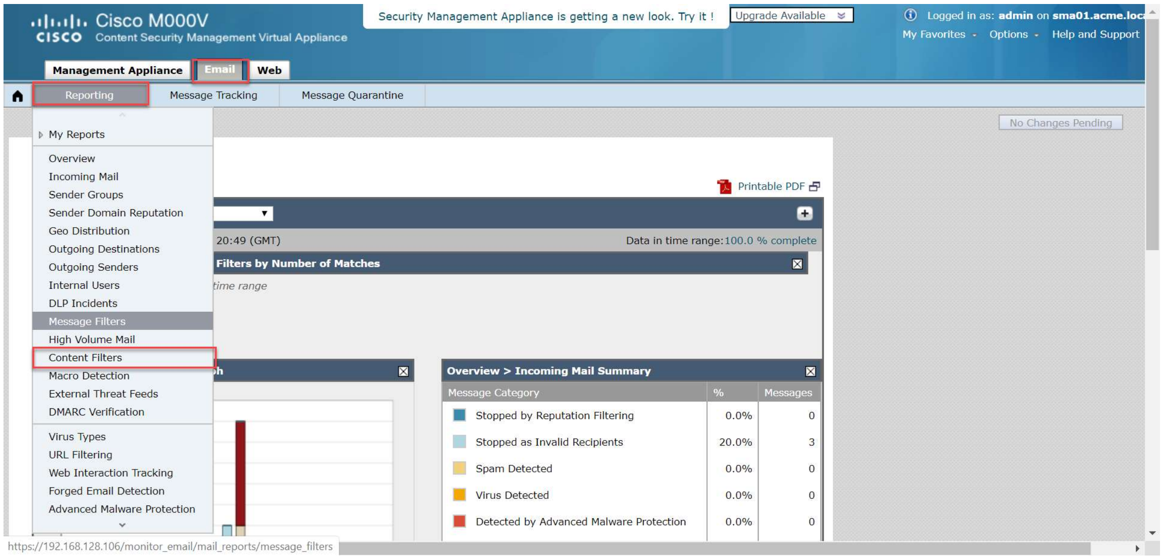
Incoming Mail Policies

Success — Your changes have been committed.

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	Not Available	Not Available	Not Available	Not Available	NO-PUB	Not Available	

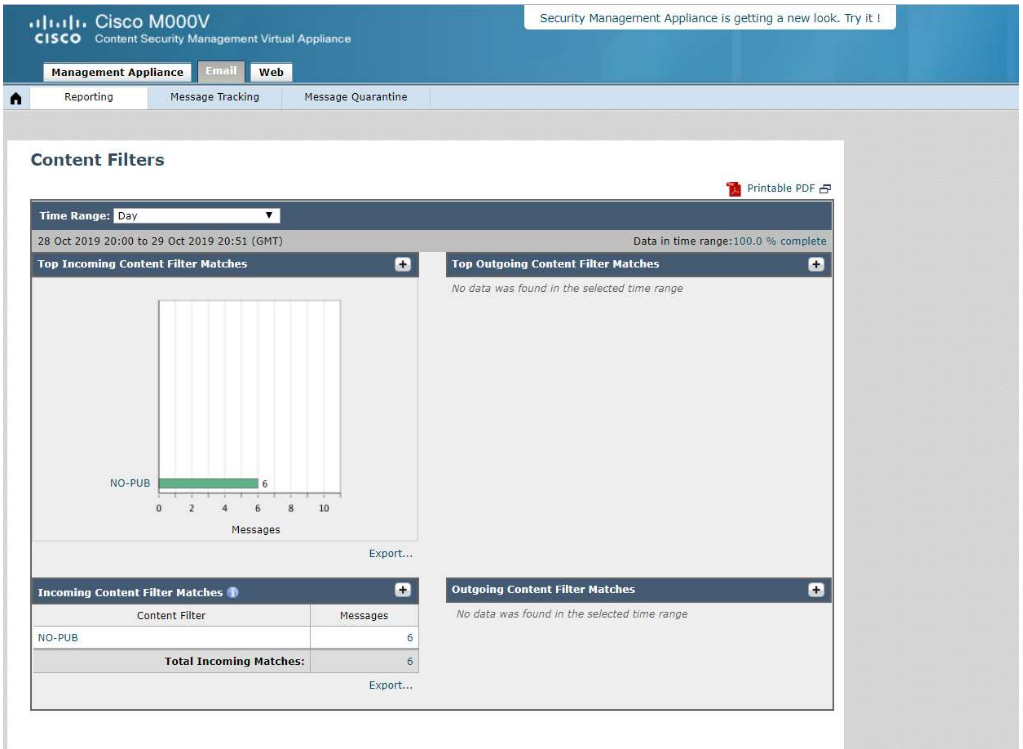
Reports are gathered from the SMA. This is done on the SMA.

Pull reports of the e-mails that were blocked by the content filter.



Overview > Incoming Mail Summary

Message Category	%	Messages
Stopped by Reputation Filtering	0.0%	0
Stopped as Invalid Recipients	20.0%	3
Spam Detected	0.0%	0
Virus Detected	0.0%	0
Detected by Advanced Malware Protection	0.0%	0



Content Filters

Time Range: Day

28 Oct 2019 20:00 to 29 Oct 2019 20:51 (GMT)

Data in time range: 100.0 % complete

Top Incoming Content Filter Matches

Top Outgoing Content Filter Matches

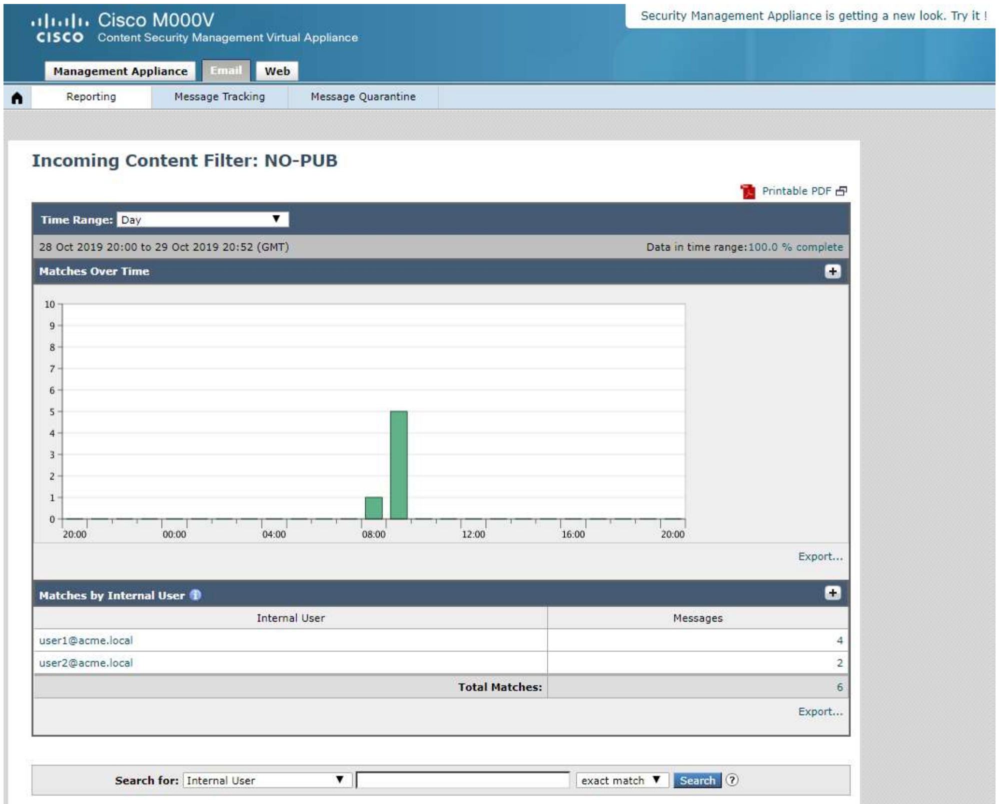
No data was found in the selected time range

Incoming Content Filter Matches

Content Filter	Messages
NO-PUB	6
Total Incoming Matches:	6

Outgoing Content Filter Matches

No data was found in the selected time range



Incoming Content Filter: NO-PUB

Time Range: Day

28 Oct 2019 20:00 to 29 Oct 2019 20:52 (GMT)

Data in time range: 100.0 % complete

Matches Over Time

Matches by Internal User

Internal User	Messages
user1@acme.local	4
user2@acme.local	2
Total Matches:	6

Search for: Internal User ▼ exact match ▼