

## 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)

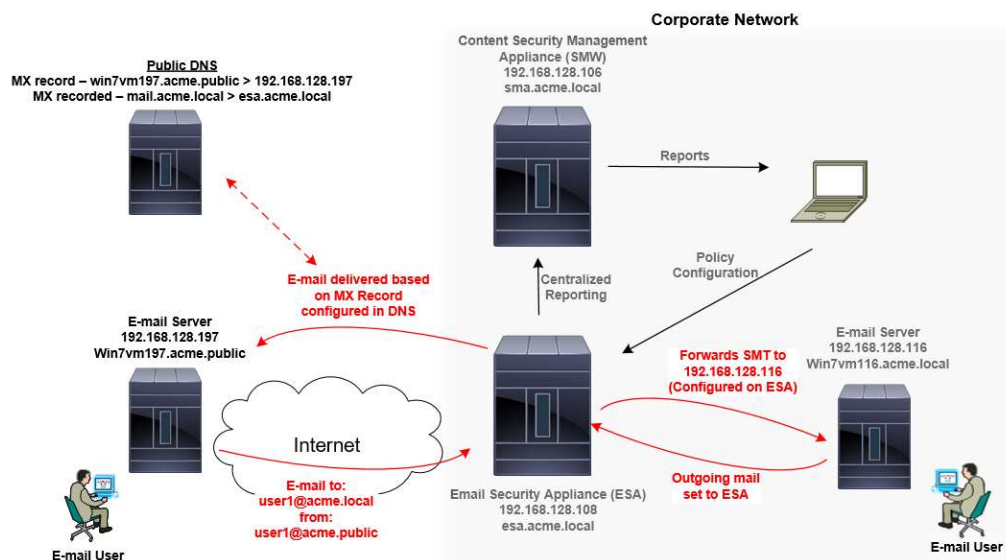
[https://www.cisco.com/c/en/us/td/docs/security/security\\_management/sma/sma12-0/api/b\\_SMA\\_API\\_12.html](https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12.html)

## 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 TFTP/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.

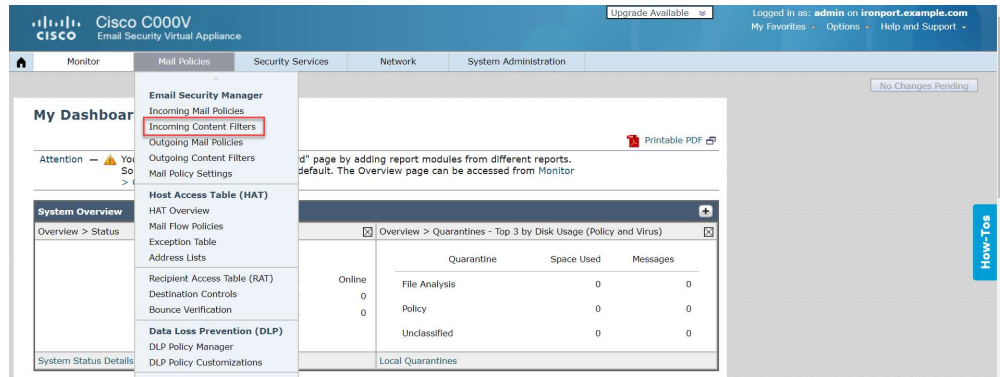
username: Admin / Password: WWTwwt1!

## 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.



### Incoming Content Filters

Success — Your changes have been committed.

**Filters**

[Add Filter...](#)

There are no filters defined.

Key: ☐ Not in use

### Add Incoming Content Filter

**Content Filter Settings**

Name:

Currently Used by Policies: No policies currently use this rule.

Description:

**Conditions**

[Add Condition...](#)

There are no conditions, so actions will always apply.

**Actions**

[Add Action...](#)

There are no actions.

Add Condition

Message Body or Attachment

Message Body

URL Category

URL Reputation

Message Size

Message Language

Macro Detection

Attachment Content

Attachment File Info

Attachment Protection

Subject Header

Other Header

Envelope Sender

Envelope Recipient

Receiving Listener

Remote IP/Hostname

Reputation Score

Domain Reputation

DKIM Authentication

Forged Email Detection

S/PF Verification

S/MIME Gateway Message

S/MIME Gateway Verified

Duplicate Boundaries Verification

Geolocation

Remote IP/Hostname

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

Remote IP/Hostname:

Is

Cancel

OK

Add Incoming Content Filter

Content Filter Settings

Name:

NO-PUB

Currently Used by Policies:

No policies currently use this rule.

Description:

Conditions

Add Condition...

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

Actions

Add Action...

There are no actions.

Cancel

Submit

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)

Drop (Final Action)

Help

Drops and discards the message.

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

Cancel

OK

### 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()	

Cancel
Submit

### 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.

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

Key: Not in use

Apply the Content Filter to the default Incoming Mail Policy.

The screenshot shows the Cisco ESM web interface. The 'Incoming Mail Policies' page is active, displaying a list of filters and policies. The 'NO-PUB' filter is listed in the 'Filters' table, and the 'Default Policy' is highlighted in the 'Policies' table.

### Incoming Mail Policies

**Find Policies**

Email Address:		<input checked="" type="radio"/> Recipient <input type="radio"/> Sender	Find Policies
----------------	--	--	---------------

**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	

Key: Default Custom Disabled

### Mail Policies: Content Filters

Content Filtering for: Default Policy

Enable Content Filters (Customize settings) ▼

Order	Filter Name	Description	Enable
1	NO-PUB		<input checked="" type="checkbox"/>

Cancel
Submit

Must commit changes for the policy to become active.

Cisco C000V  
Email Security Virtual Appliance

Upgrade Available

Logged in as: admin on transport.example.com  
My Favorites Options Help and Support

Monitor Mail Policies Security Services Network System Administration

**Incoming Mail Policies**

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

**Find Policies**

Email Address:  ☐ Recipient ☐ Sender **Find Policies**

**Policies**

**Add Policy...**

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	

Key: **Default** Custom Disabled

**Commit Changes**

**Uncommitted Changes**

**Commit Changes**

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

Comment (optional):

**Cancel** **Abandon Changes** **Commit Changes**

Result.

**Incoming Mail Policies**

Success — Your changes have been committed.

**Find Policies**

Email Address:  ☐ Recipient ☐ Sender **Find Policies**

**Policies**

**Add Policy...**

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	

Key: **Default** Custom Disabled

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.

The screenshot shows the Cisco M000V Content Security Management Virtual Appliance interface. The 'Reporting' tab is selected, and the 'Content Filters' menu item is highlighted in the left sidebar. The main area displays a bar chart titled 'Filters by Number of Matches' and an 'Overview > Incoming Mail Summary' table.

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

The screenshot shows the 'Content Filters' report in the Cisco M000V Content Security Management Virtual Appliance interface. The 'Time Range' is set to 'Day' (28 Oct 2019 20:00 to 29 Oct 2019 20:51 GMT). The 'Top Incoming Content Filter Matches' section displays a bar chart for 'NO-PUB' with 6 matches. The 'Incoming Content Filter Matches' table lists 'NO-PUB' with 6 messages.

Content Filter	Messages
NO-PUB	6
<b>Total Incoming Matches:</b>	<b>6</b>

## Incoming Content Filter: NO-PUB

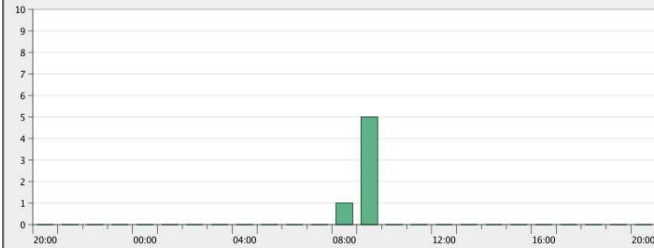
Printable PDF

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



Export...

### Matches by Internal User

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

Export...

Search for: Internal User

exact match

Search ?