



# 300-207<sup>Q&As</sup>

Implementing Cisco Threat Control Solutions

**Pass Cisco 300-207 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/300-207.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

**Scenario**

In this simulation, you have access to the mail flow policies and sender groups configured on a Cisco Email Security Appliance. You are also provided the following list of fictional domains. SenderBase has records for one sender from each of these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.

Vt120 red.public, -6  
orange.public, -4  
yellow.public, -2  
green.public, 2  
blue.public, 6  
violet.public, 8

Your task is to review the configuration on the Cisco Email Security Appliance, and then answer 5 multiple choice questions about the behavior of the Cisco Email Security Appliance given the configuration and the domain SenderBase Reputation Scores.

**Instructions**

Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the HAT Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.

- red.public, -6
- orange.public, -4
- yellow.public, -2
- green.public, 2
- blue.public, 6
- violet.public, 8

**THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**  
Click on the MailFlowPolicies tab to access the device configuration.  
To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.  
There are four multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.

Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local  
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policies

Policies (Listener: IncomingMail 172.16.16.25:25)

Add Policy ...

Policy Name	Behavior	Delete
ACCEPTED	Accept	?
BLOCKED	Reject	🗑️
RELAYED	Relay	🗑️
THROTTLED	Accept	🗑️
TRUSTED	Accept	🗑️
Default Policy Parameters		

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement





Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local

Monitor | Mail Policies | Security Services | Network | System Administration

**HAT Overview**

Find Senders

Sender Groups (Listeners)

Host Access Table (HAT)

Order	Sender	SenderBase™ Reputation Score (?)	Mail Flow Policy	Delete
1	RELAYLIST	-4	RELAYED	
2	WHITELIST	0	TRUSTED	
3	BLACKLIST	2	BLOCKED	
4	SUSPECTLIST	4	THROTTLED	
5	UNKNOWNLIST	6	ACCEPTED	
	ALL	8	ACCEPTED	

Key: Custom Default

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local

Monitor | Mail Policies | Security Services | Network | System Administration

**HAT Overview**

Find Senders

Sender Groups (Listener: IncomingMail 172.16.16.25:25)

Order	Sender Group	SenderBase™ Reputation Score (?)	Mail Flow Policy	Delete
1	RELAYLIST	-10	RELAYED	
2	WHITELIST	-8	TRUSTED	
3	BLACKLIST	-6	BLOCKED	
4	SUSPECTLIST	-4	THROTTLED	
5	UNKNOWNLIST	-2	ACCEPTED	
	ALL	0	ACCEPTED	

Key: Custom Default

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local


Monitor | Mail Policies | Security Services | Network | System Administration

**Mail Flow Policy**

Policies (Listeners)

Policy Name	Behavior	Delete
ACCEPTED	Accept	
BLOCKED	Reject	
RELAYED	Relay	
THROTTLED	Accept	
TRUSTED	Accept	
Default Policy Parameters		

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement





Cisco C100V Email Security Virtual Appliance  
Logged in as: admin on esm.secure-x.local  
My Favorites - Options - Help and Support

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:

Connection Behavior:

**Connections:**

- Max. Messages Per Connection:  Use Default (10)
- Max. Recipients Per Message:  Use Default (50)
- Max. Message Size:  Use Default (10M)   
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP:  Use Default (10)

**SMTP:**

- Custom SMTP Banner Code:  Use Default (220)
- Custom SMTP Banner Text:  Use Default ()
- Override SMTP Banner Hostname:  Use Default (Use Hostname from Interface)  Use Hostname from Interface

**Mail Flow Limits**

- Rate Limit for Hosts: Max. Recipients Per Hour:  Use Default (Unlimited)  Unlimited
- Max. Recipients Per Hour Code:  Use Default (452)
- Max. Recipients Per Hour Text:  Use Default (Too many recipients received this hour)

Cisco C100V Email Security Virtual Appliance  
Logged in as: admin on esm.secure-x.local  
My Favorites - Options - Help and Support

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:

Connection Behavior:

**Connections:**

- Max. Messages Per Connection:  Use Default (10)
- Max. Recipients Per Message:  Use Default (50)
- Max. Message Size:  Use Default (10M)   
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP:  Use Default (10)

**SMTP:**

- Custom SMTP Banner Code:  Use Default (220)
- Custom SMTP Banner Text:  Use Default ()
- Override SMTP Banner Hostname:  Use Default (Use Hostname from Interface)  Use Hostname from Interface

**Mail Flow Limits**

- Rate Limit for Hosts: Max. Recipients Per Hour:  Use Default (Unlimited)  Unlimited
- Max. Recipients Per Hour Code:  Use Default (452)
- Max. Recipients Per Hour Text:  Use Default (Too many recipients received this hour)





Cisco C100V Email Security Virtual Appliance  
Logged in as: admin on esa.secure-x.local  
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	BLACKLIST
Order:	3
Comment:	Spammers are rejected
Policy:	BLOCKED
SBRs (Optional):	-10.0 to -3.0
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Add Sender...  
There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Cisco C100V Email Security Virtual Appliance  
Logged in as: admin on esa.secure-x.local  
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	BLACKLIST
Order:	3
Comment:	Spammers are rejected
Policy:	BLOCKED
SBRs (Optional):	-10.0 to -3.0
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Add Sender...  
There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement





Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local  
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:

Connection Behavior:

Connections:

- Max. Messages Per Connection:  Use Default (10)
- Max. Recipients Per Message:  Use Default (50)
- Max. Message Size:  Use Default (10M)   
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP:  Use Default (10)

SMTP:

- Custom SMTP Banner Code:  Use Default (554)
- Custom SMTP Banner Text:  Use Default ()  
 Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure
- Override SMTP Banner Hostname:  Use Default (Use Hostname from Interface)  
 Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

- Max. Recipients Per Hour:  Use Default (Unlimited)  
 Unlimited
- Max. Recipients Per Hour Code:  Use Default (452)
- Max. Recipients Per Hour Text:  Use Default (Too many recipients received this hour)

Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local  
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:

Connection Behavior:

Connections:

- Max. Messages Per Connection:  Use Default (10)
- Max. Recipients Per Message:  Use Default (50)
- Max. Message Size:  Use Default (10M)   
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP:  Use Default (10)

SMTP:

- Custom SMTP Banner Code:  Use Default (554)
- Custom SMTP Banner Text:  Use Default ()  
 Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure
- Override SMTP Banner Hostname:  Use Default (Use Hostname from Interface)  
 Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

- Max. Recipients Per Hour:  Use Default (Unlimited)  
 Unlimited
- Max. Recipients Per Hour Code:  Use Default (452)
- Max. Recipients Per Hour Text:  Use Default (Too many recipients received this hour)





Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name: RELAYED

Connection Behavior: Relay

Connections:

- Max. Messages Per Connection:  Use Default (10)
- Max. Recipients Per Message:  Use Default (50)
- Max. Message Size:  Use Default (10M)   
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP:  Use Default (10)

SMTP:

- Custom SMTP Banner Code:  Use Default (220)
- Custom SMTP Banner Text:  Use Default ()
- Override SMTP Banner Hostname:  Use Default (Use Hostname from Interface)  Use Hostname from Interface

**Mail Flow Limits**

- Rate Limit for Hosts:  Use Default (Unlimited)  Unlimited
- Max. Recipients Per Hour Code:  Use Default (452)
- Max. Recipients Per Hour Text:  Use Default (Too many recipients received this hour)

Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name: RELAYED

Connection Behavior: Relay

Connections:

- Max. Messages Per Connection:  Use Default (10)
- Max. Recipients Per Message:  Use Default (50)
- Max. Message Size:  Use Default (10M)   
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP:  Use Default (10)

SMTP:

- Custom SMTP Banner Code:  Use Default (220)
- Custom SMTP Banner Text:  Use Default ()
- Override SMTP Banner Hostname:  Use Default (Use Hostname from Interface)  Use Hostname from Interface

**Mail Flow Limits**

- Rate Limit for Hosts:  Use Default (Unlimited)  Unlimited
- Max. Recipients Per Hour Code:  Use Default (452)
- Max. Recipients Per Hour Text:  Use Default (Too many recipients received this hour)

**Host Access Table (HAT)**

- HAT Overview
- Mail Flow Policies
- Exception Table
- Address Lists

**Recipient Access Table (RAT)**

- Destination Controls
- Bounce Verification

**Data Loss Prevention (DLP)**

- DLP Policy Manager
- DLP Message Actions

**Domain Keys**

- Verification Profiles
- Signing Profiles
- Signing Keys

**Text Resources**

- Dictionaries





Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	RELAYLIST
Order:	1
Comment:	Only select hosts can relay from this box
Policy:	RELAYED
SBRs (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Sender	Comment	All Delete
hq-mail.maroon.public	None	<input type="checkbox"/>

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	RELAYLIST
Order:	1
Comment:	Only select hosts can relay from this box
Policy:	RELAYED
SBRs (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Sender	Comment	All Delete
hq-mail.maroon.public	None	<input type="checkbox"/>

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement







Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local  
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Sender Group: SUSPECTLIST - IncomingMail 172.16.16.25:25

Sender Group Settings	
Name:	SUSPECTLIST
Order:	4
Comment:	Suspicious senders are throttled
Policy:	THROTTLED
SBRS (Optional):	-3.0 to 3.0
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview Edit Settings...

**Find Senders**

Find Senders that Contain this Text:  Find

**Sender List: Display All Items in List**

Add Sender...

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local  
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Sender Group: IncomingMail 172.16.16.25:25

Sender Group Settings	
Name:	SUSPECTLIST
Order:	4
Comment:	Suspicious senders are throttled
Policy:	THROTTLED
SBRS (Optional):	-3.0 to 3.0
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview Edit Settings...

**Find Senders**

Find Senders that Contain this Text:  Find


**Sender List: Display All Items in List**

Add Sender...

There are no senders.

- Email Security Manager
  - Incoming Mail Policies
  - Incoming Content Filters
  - Outgoing Mail Policies
  - Outgoing Content Filters
- Host Access Table (HAT)
  - HAT Overview
  - Mail Flow Policies
  - Exception Table
  - Address Lists
- Recipient Access Table (RAT)
  - Destination Controls
  - Bounce Verification
- Data Loss Prevention (DLP)
  - DLP Policy Manager
  - DLP Message Actions
- Domain Keys
  - Verification Profiles
  - Signing Profiles
  - Signing Keys
- Text Resources
- Dictionaries

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement





Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name: THROTTLED

Connection Behavior: Accept

Connections:

- Max. Messages Per Connection: Use Default (10)  1
- Max. Recipients Per Message: Use Default (50)  25
- Max. Message Size: Use Default (10M)  10485760  
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP: Use Default (10)  1

SMTP:

- Custom SMTP Banner Code: Use Default (220)  220
- Custom SMTP Banner Text: Use Default ()
- Override SMTP Banner Hostname: Use Default (Use Hostname from Interface)

**Mail Flow Limits**

- Rate Limit for Hosts: Max. Recipients Per Hour: Use Default (Unlimited)  Unlimited  20
- Max. Recipients Per Hour Code: Use Default (452)
- Max. Recipients Per Hour Text: Use Default (Too many recipients received this hour)

Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name: THROTTLED

Connection Behavior: Accept

Connections:

- Max. Messages Per Connection: Use Default (10)  1
- Max. Recipients Per Message: Use Default (50)  25
- Max. Message Size: Use Default (10M)  10485760  
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP: Use Default (10)  1

SMTP:

- Custom SMTP Banner Code: Use Default (220)  220
- Custom SMTP Banner Text: Use Default ()
- Override SMTP Banner Hostname: Use Default (Use Hostname from Interface)

**Mail Flow Limits**

- Rate Limit for Hosts: Max. Recipients Per Hour: Use Default (Unlimited)  Unlimited  20
- Max. Recipients Per Hour Code: Use Default (452)
- Max. Recipients Per Hour Text: Use Default (Too many recipients received this hour)

Host Access Table (HAT)

- HAT Overview
- Mail Flow Policies
- Exception Table
- Address Lists
- Recipient Access Table (RAT)
- Destination Controls
- Bounce Verification
- Data Loss Prevention (DLP)
- DLP Policy Manager
- DLP Message Actions
- Domain Keys
- Verification Profiles
- Signing Profiles
- Signing Keys
- Text Resources
- Dictionaries



Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name: TRUSTED

Connection Behavior: Accept

Connections:

- Max. Messages Per Connection:  Use Default (10)  5000
- Max. Recipients Per Message:  Use Default (50)  5000
- Max. Message Size:  Use Default (10M)  104857600  
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP:  Use Default (10)  300

SMTP:

- Custom SMTP Banner Code:  Use Default (220)  220
- Custom SMTP Banner Text:  Use Default ()  
 [Text Box]
- Override SMTP Banner Hostname:  Use Default (Use Hostname from Interface)  
 Use Hostname from Interface  
 [Text Box]

**Mail Flow Limits**

- Rate Limit for Hosts:  Use Default (Unlimited)  Unlimited  [Text Box]
- Max. Recipients Per Hour Code:  Use Default (452)  [Text Box]
- Max. Recipients Per Hour Text:  Use Default (Too many recipients received this hour)  [Text Box]

Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name: TRUSTED

Connection Behavior: Accept

Connections:

- Max. Messages Per Connection:  Use Default (10)  5000
- Max. Recipients Per Message:  Use Default (50)  5000
- Max. Message Size:  Use Default (10M)  104857600  
(add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP:  Use Default (10)  300

SMTP:

- Custom SMTP Banner Code:  Use Default (220)  220
- Custom SMTP Banner Text:  Use Default ()  
 [Text Box]
- Override SMTP Banner Hostname:  Use Default (Use Hostname from Interface)  
 Use Hostname from Interface  
 [Text Box]

**Mail Flow Limits**

- Rate Limit for Hosts:  Use Default (Unlimited)  Unlimited  [Text Box]
- Max. Recipients Per Hour Code:  Use Default (452)  [Text Box]
- Max. Recipients Per Hour Text:  Use Default (Too many recipients received this hour)  [Text Box]

**Navigation Menu:**

- Email Security Manager
  - Incoming Mail Policies
  - Incoming Content Filters
  - Outgoing Mail Policies
  - Outgoing Content Filters
- Host Access Table (HAT)
  - HAT Overview
  - Mail Flow Policies
  - Exception Table
  - Address Lists
- Recipient Access Table (RAT)
  - Destination Controls
  - Bounce Verification
- Data Loss Prevention (DLP)
  - DLP Policy Manager
  - DLP Message Actions
- Domain Keys
  - Verification Profiles
  - Signing Profiles
  - Signing Keys
- Text Resources
  - Dictionaries





Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Sender Group: UNKNOWNLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	UNKNOWNLIST
Order:	5
Comment:	Reviewed but undecided, continue normal acceptance
Policy:	ACCEPTED
SBRS (Optional):	3.0 to 10.0 and SBRS Scores of "None"
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Add Sender...

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Sender Group: UNKNOWNLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	UNKNOWNLIST
Order:	5
Comment:	Reviewed but undecided, continue normal acceptance
Policy:	ACCEPTED
SBRS (Optional):	3.0 to 10.0 and SBRS Scores of "None"
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Add Sender...

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Cisco C100V Email Security Virtual Appliance

Monitor Mail Policies Security Services Network System Administration

Sender Group: WHITELIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	WHITELIST
Order:	2
Comment:	My trusted senders have no anti-spam scanning or rate limiting
Policy:	TRUSTED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Add Sender...

Sender	Comment	All Delete
.orange.public	None	<input type="checkbox"/>

Items per page 20

Back to HAT Overview Delete

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



For which domains will the Cisco Email Security Appliance allow up to 5000 recipients per message?

- A. violet.public
- B. violet.public and blue.public
- C. violet.public, blue.public and green.public
- D. red.public
- E. orange.public
- F. red.public and orange.public

Correct Answer: E

Explanation:

Here we see that the TRUSTED policy is being throttled to 5000 recipients per message.



Cisco C100V  
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local  
My Favorites - Options - Help and Support -

Monitor | Mail Policies | Security Services | Network | System Administration

No Changes Pending

### Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:	<input type="text" value="TRUSTED"/>		
Connection Behavior:	<input type="text" value="Accept"/>		
Connections:	Max. Messages Per Connection:	<input type="radio"/> Use Default (10)	<input checked="" type="radio"/> <input type="text" value="5000"/>
	Max. Recipients Per Message:	<input type="radio"/> Use Default (50)	<input checked="" type="radio"/> <input type="text" value="5000"/>
	Max. Message Size:	<input type="radio"/> Use Default (10M)	<input checked="" type="radio"/> <input type="text" value="104857600"/> <small>(add a trailing K for kilobytes; M for megabytes)</small>
	Max. Concurrent Connections From a Single IP:	<input type="radio"/> Use Default (10)	<input checked="" type="radio"/> <input type="text" value="300"/>
SMTP:	Custom SMTP Banner Code:	<input checked="" type="radio"/> Use Default (220)	<input type="text" value="220"/>
	Custom SMTP Banner Text:	<input checked="" type="radio"/> Use Default ( )	<input type="text"/>
	Override SMTP Banner Hostname:	<input checked="" type="radio"/> Use Default (Use Hostname from Interface)	<input type="radio"/> Use Hostname from Interface <input type="text"/>
<b>Mail Flow Limits</b>			
Rate Limit for Hosts:	Max. Recipients Per Hour:	<input type="radio"/> Use Default (Unlimited)	<input checked="" type="radio"/> Unlimited
	Max. Recipients Per Hour Code:	<input checked="" type="radio"/> Use Default (452)	<input type="text"/>
	Max. Recipients Per Hour Text:	<input checked="" type="radio"/> Use Default (Too many recipients received this hour)	<input type="text"/>

By looking at the HAT policy we see that the TRUSTED policy applies to the WHITELIST sender group. By clicking on the WHITELIST sender group we can see that orange.public is listed as the sender.



Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local  
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### HAT Overview

Find Senders

Find Senders that Contain this Text:  Find

Sender Groups (Listener: IncomingMail 172.16.16.25:25)

Add Sender Group... Import HAT...

Order	Sender Group	SenderBase™ Reputation Score (?)											Mail Flow Policy	Delete		
		-10	-8	-6	-4	-2	0	2	4	6	8	+10				
1	RELAYLIST														RELAYED	
2	WHITELIST														TRUSTED	
3	BLACKLIST	=====											BLOCKED			
4	SUSPECTLIST	=====											THROTTLED			
5	UNKNOWNLIST														ACCEPTED	
	ALL														ACCEPTED	

Edit Order... Export HAT...

Key: Custom Default

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

### White-List

No Changes

### Sender Group: WHITELIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	WHITELIST
Order:	2
Comment:	My trusted senders have no anti-spam scanning or rate limiting
Policy:	TRUSTED
SRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List Items per page 20

Add Sender..

Sender	Comment	All Delete
orange.public	None	<input type="checkbox"/>

<< Back to HAT Overview



### QUESTION 2

Which three categories of the seven major risk management categories are covered in the Cyber Risk Reports?  
(Choose three.)

- A. vulnerability
- B. risk rating
- C. legal
- D. confidence level
- E. geopolitical
- F. global reputation

Correct Answer: ACE

---

### QUESTION 3

Which set of commands changes the FTP client timeout when the sensor is communicating with an FTP server?

- A. sensor# configure terminal sensor(config)# service sensor sensor(config-hos)# network-settings sensor(config-hos-net)# ftp-timeout 500
- B. sensor# configure terminal sensor(config)# service host sensor(config-hos)# network-settings parameter ftp sensor(config-hos-net)# ftp-timeout 500
- C. sensor# configure terminal sensor(config)# service host sensor(config-hos)# network-settings sensor(config-hos-net)# ftp-timeout 500
- D. sensor# configure terminal sensor(config)# service network sensor(config-hos)# network-settings sensor(config-hos-net)# ftp-timeout 500

Correct Answer: C

---

### QUESTION 4

Which command verifies that the correct CWS license key information was entered on the Cisco ASA?

- A. sh run scansafe server
- B. sh run scansafe
- C. sh run server
- D. sh run server scansafe

Correct Answer: B

---





**QUESTION 5**

Which Cisco WSA is intended for deployment in organizations of up to 1500 users?

- A. WSA S370
- B. WSA S670
- C. WSA S370-2RU
- D. WSA S170

Correct Answer: D

[300-207 VCE Dumps](#)

[300-207 Practice Test](#)

[300-207 Study Guide](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

## Try our product !

100% Guaranteed Success  
100% Money Back Guarantee  
365 Days Free Update  
Instant Download After Purchase  
24x7 Customer Support  
Average 99.9% Success Rate  
More than 800,000 Satisfied Customers Worldwide  
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.geekcert.com/allproducts>

## Need Help

Please provide as much detail as possible so we can best assist you.  
To update a previously submitted ticket:



 <p><b>One Year Free Update</b> Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p><b>Money Back Guarantee</b> To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.  
All trademarks are the property of their respective owners.  
Copyright © geekcert, All Rights Reserved.