300-210Q&As

Cisco Threat Control Solutions

Pass Cisco 300-210 Exam with 100% Guarantee

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

https://www.certbus.com/300-210.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

When a Cisco Email Security Appliance joins a cluster, which four settings are inherited? (Choose four.)

A. IP address

B. DNS settings

C. SMTP routes

D. HAT

E. RAT

F. hostname

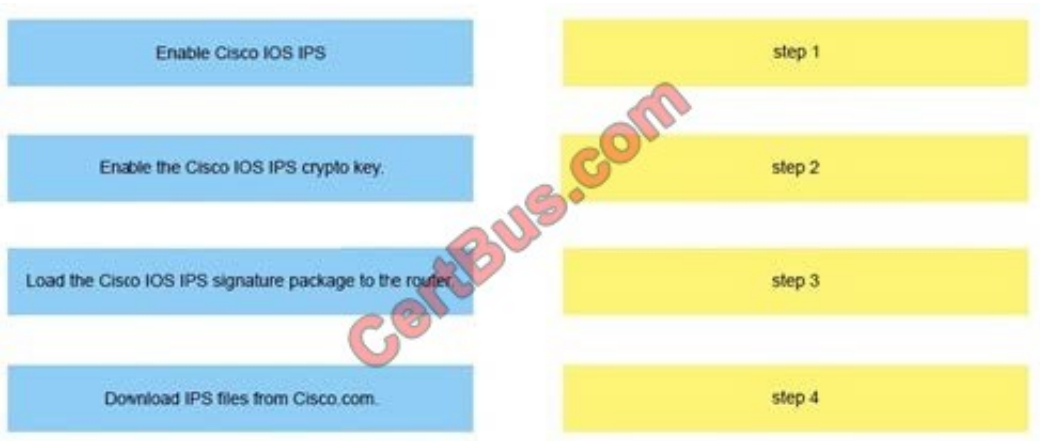
G. certificates

Correct Answer: BCDE

QUESTION 2

Drag and drop the steps on the left into the correct order of initial Cisco IOS IPS configuration on the right.

Select and Place:



Correct Answer:

CertBus.com

QUESTION 3

Which option describes a customer benefit of the Cisco Security IntelliShield Alert Manager?

A. It provides access to threat and vulnerability information for Cisco related products only.

B. It consolidates vulnerability information from an internal Cisco source, which allows security personnel to focus on remediation and proactive protection versus research.

C. It provides effective and timely security intelligence via early warnings about new threats and technology vulnerabilities.

D. It enhances the efficiency of security staff with accurate, noncustomizable threat intelligence, critical remediation information, and easy-to-use workflow tools.

Correct Answer: C

QUESTION 4

Which Cisco ASA platform should be selected if the requirements are to support 35,000 connections per second, 600,000 maximum connections, and traffic shaping?

A. 5540

B. 5550

C. 5580-20

D. 5580-40

Correct Answer: C

QUESTION 5

Which two methods are used to deploy transparent mode traffic redirection? (Choose two)

A. Microsoft GPO

B. policy-based routing

C. DHCP server

D. PAC files

E. Web Cache Communication Protocol

Correct Answer: BE

QUESTION 6

Which two pieces of information are required to implement transparent user identification using context Directory Agent? (Choose two.)

A. the shared secret

B. the server name where Context Directory Agent is installed

C. the server name of the global catalog domaint controller

D. the syslog server IP address

Correct Answer: AB

QUESTION 7

The Web Security Appliance has identities defined for faculty and staff, students, and default access. The faculty and staff identity identifies users based on the source network and authenticated credentials. The identity for students identifies users based on the source network along with successful authentication credentials. The global identity is for guest users not authenticated against the domain. Recently, a change was made to the organization\\'s security policy to allow faculty and staff access to a social network website, and the security group changed the access policy for faculty and staff to allow the social networking category.

Which are the two most likely reasons that the category is still being blocked for a faculty and staff user? (Choose two.)

A. The user is being matched against the student policy because the user did not enter credentials.

B. The user is using an unsupported browser so the credentials are not working.

C. The social networking URL was entered into a custom URL category that is blocked in the access policy.

D. The user is connected to the wrong network and is being blocked by the student policy.

E. The social networking category is being allowed but the AVC policy is still blocking the website.

Correct Answer: CE

QUESTION 8

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.

\i120 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

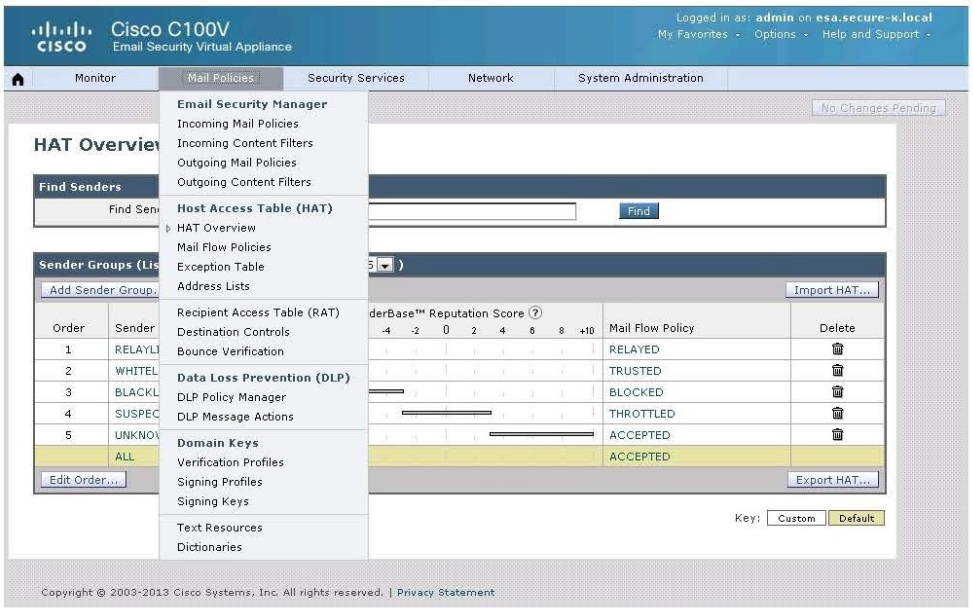
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the HAT Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

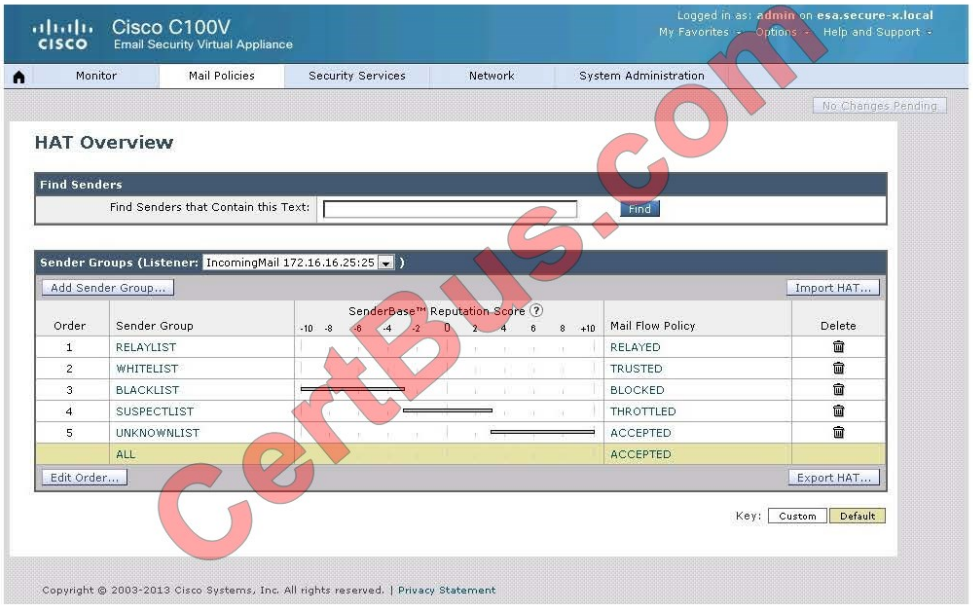
Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.

- 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.

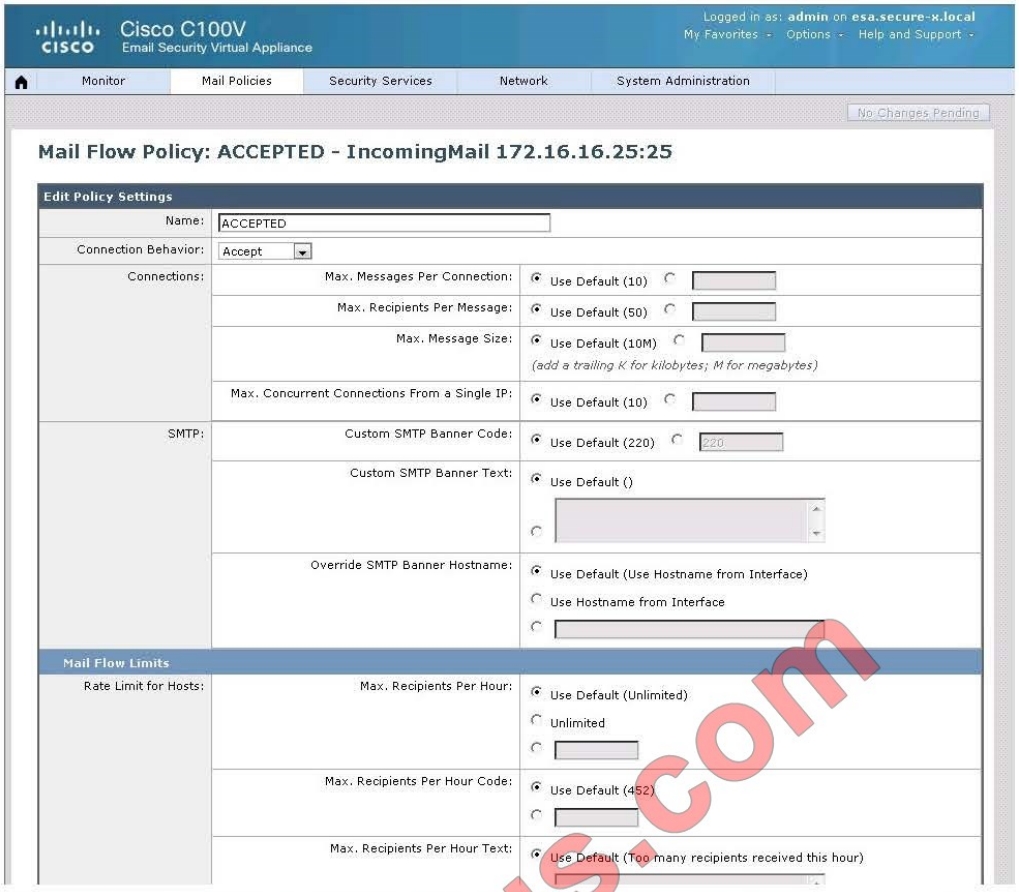
CertBus.com

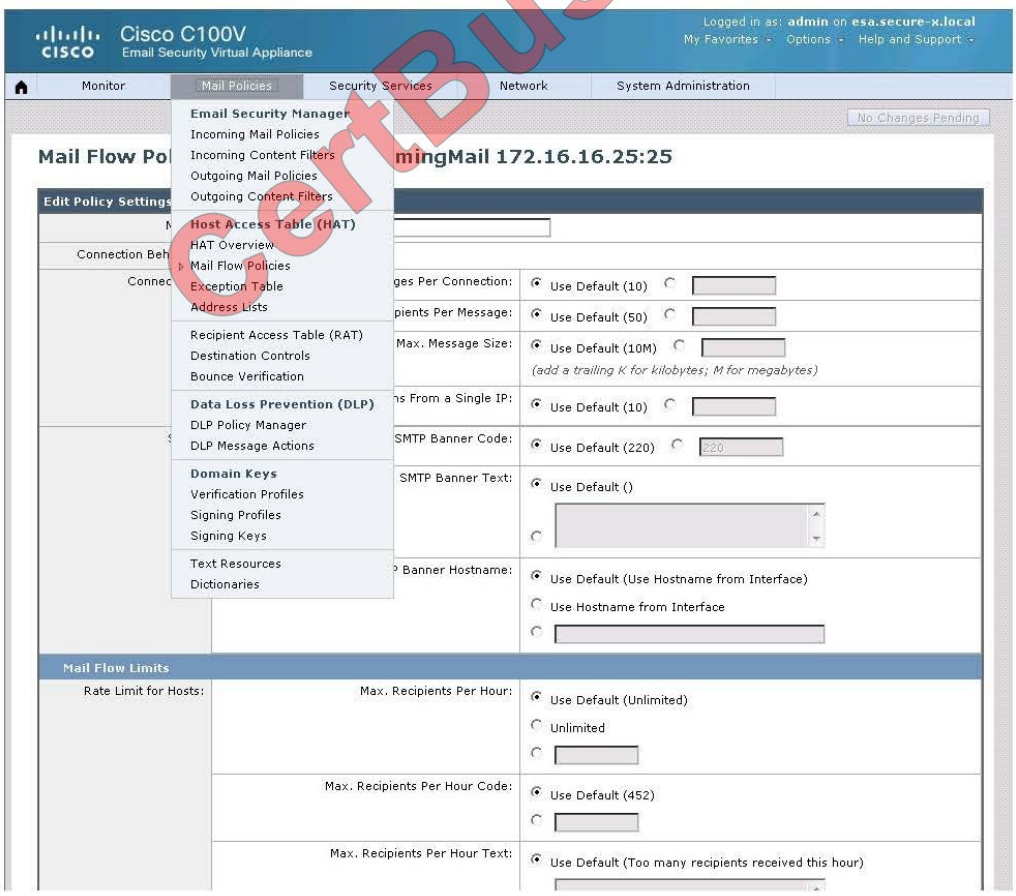

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
HAT Overview
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
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
Find Senders
Find
Add Sender Group...
Import HAT...
Order
Sender
Mail Flow Policy
Delete
1 RELAYLI RELAYED
2 WHITEL TRUSTED
3 BLACKL BLOCKED
4 SUSPEC THROTTLED
5 UNKNO ACCEPTED
ALL ACCEPTED
Edit Order...
Export HAT...
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
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
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

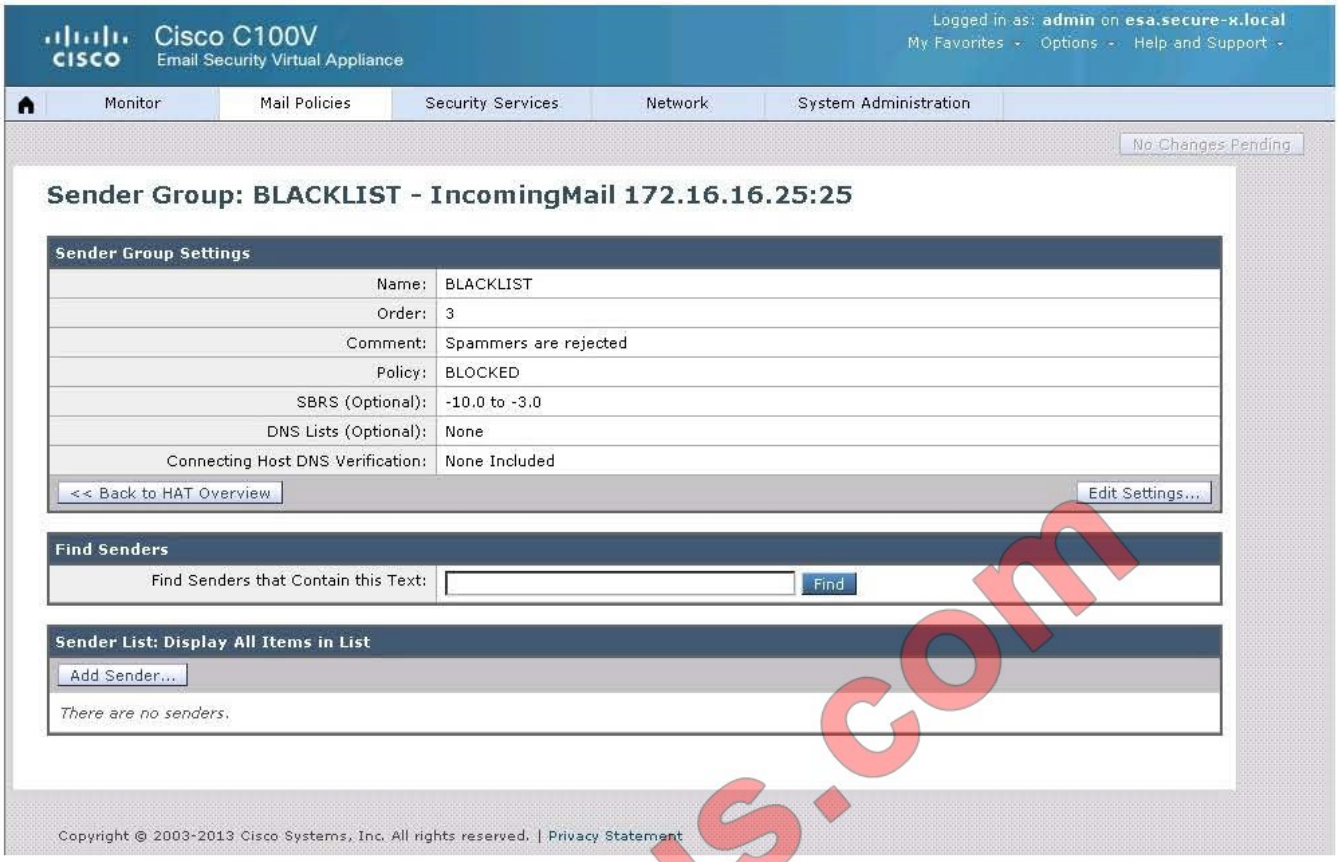

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Mail Flow Po
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
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
Policies (Listener:
Add Policy...
Policy Name
Behavior
Delete
ACCEPTED Accept
BLOCKED Reject
RELAYED Relay
THROTTLED Accept
TRUSTED Accept
Default Policy Param
Privacy Statement

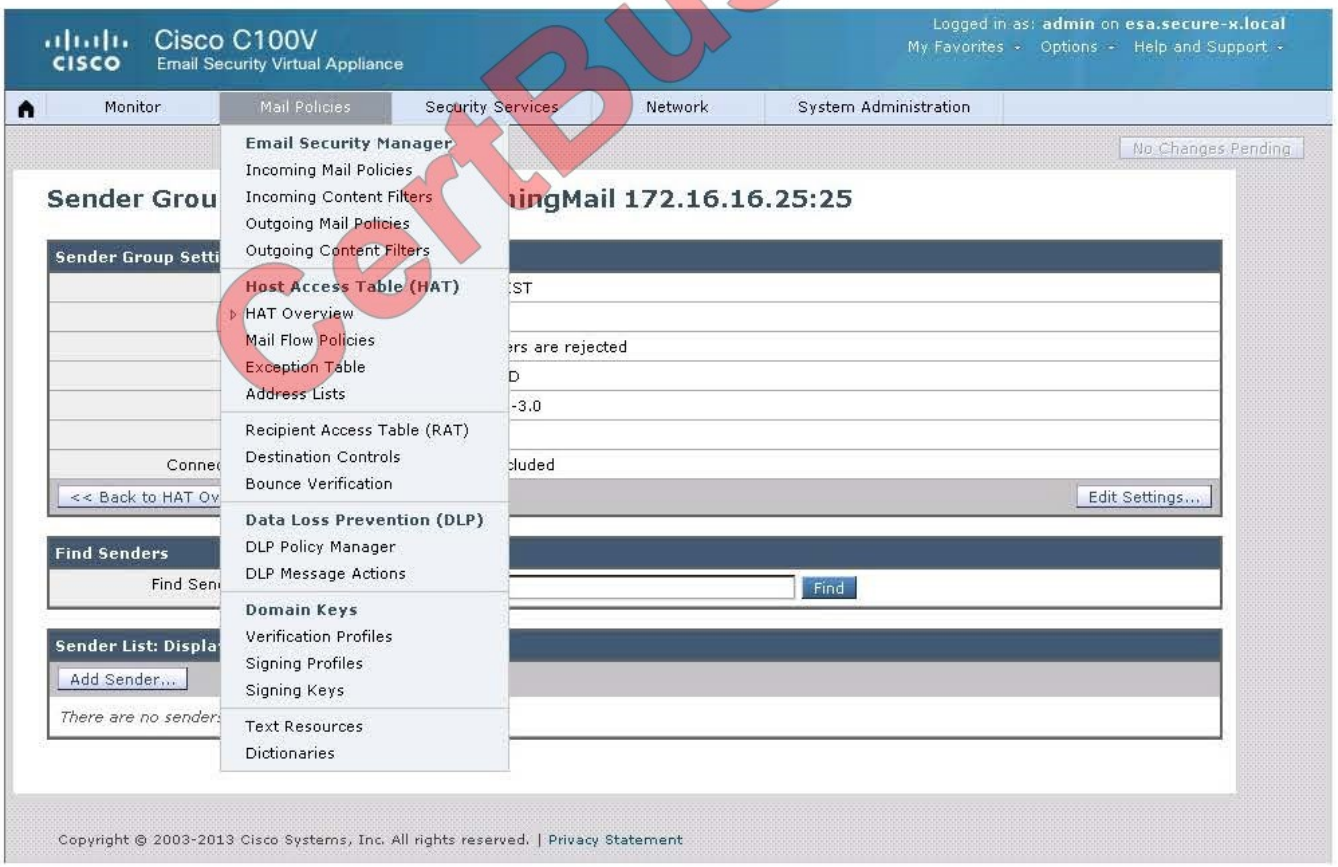
CertBus.com


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: ACCEPTED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: ACCEPTED
Connection Behavior: Accept
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)

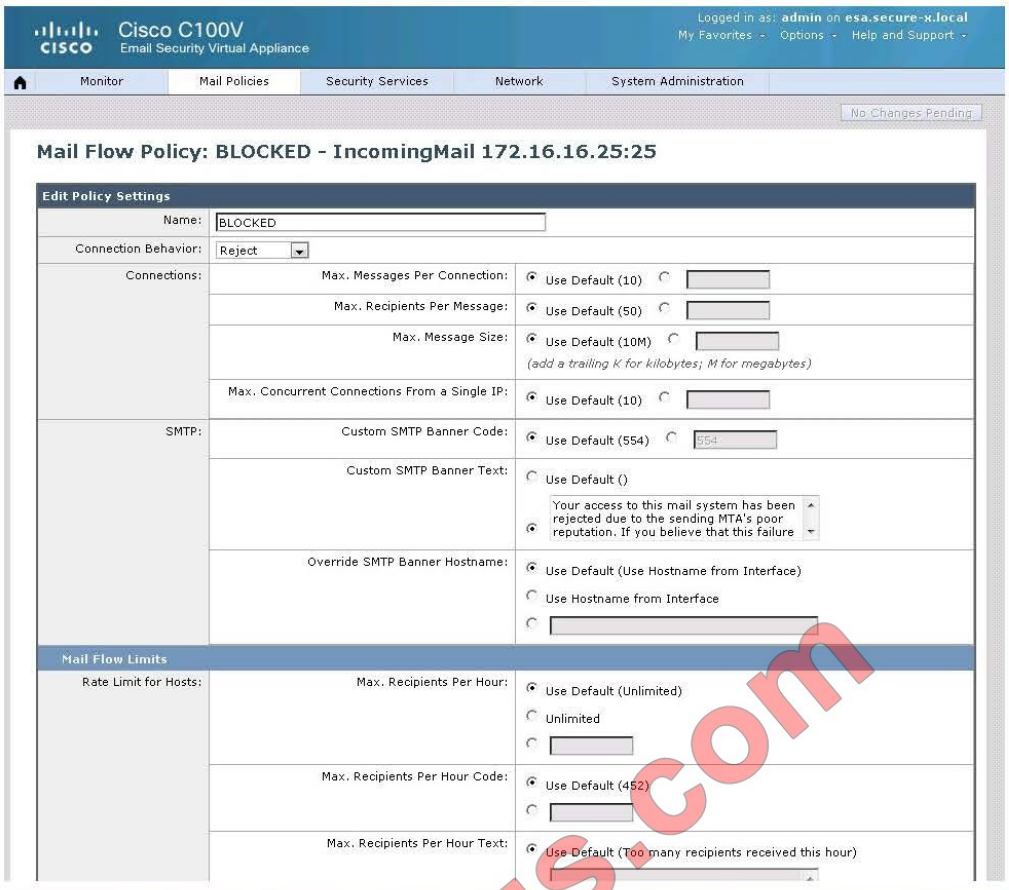

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail 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
Edit Policy Settings
Use Default (10)
Use Default (50)
Use Default (10M)
Use Default (220)
Use Default ()
Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Use Default (Unlimited)
Unlimited
Use Default (452)
Use Default (Too many recipients received this hour)

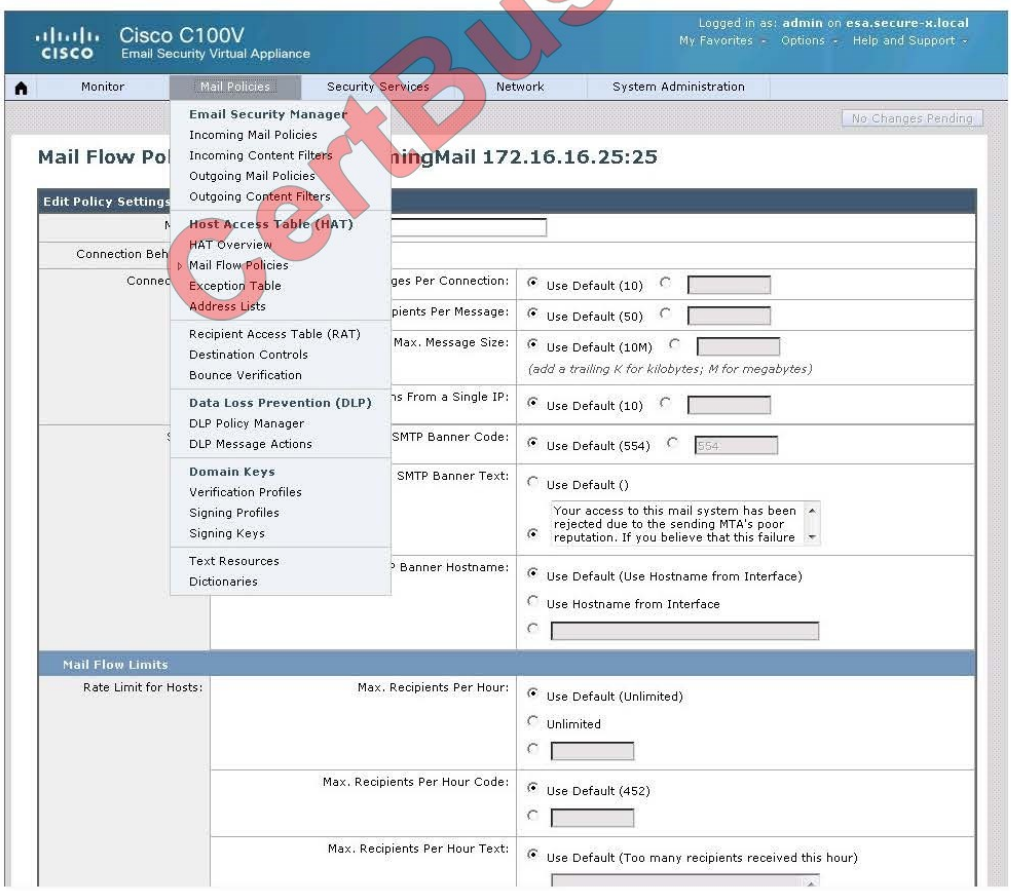
CertBus.com


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: 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

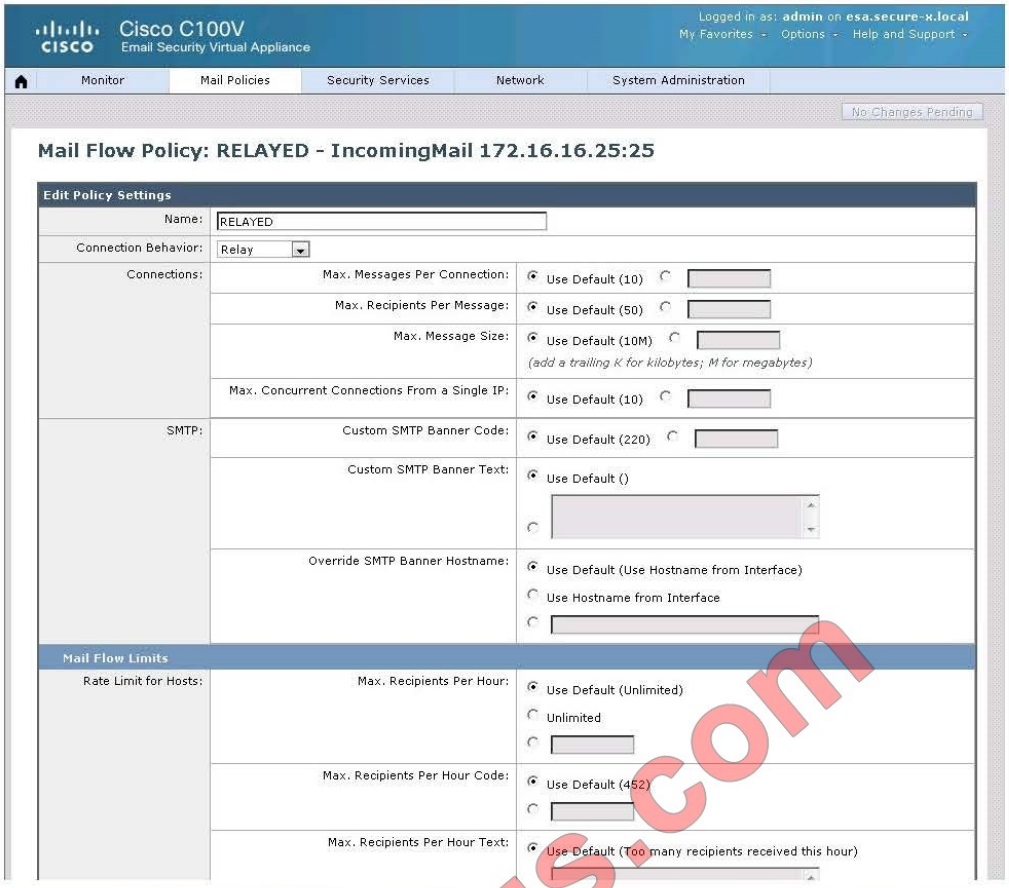

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail 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
Find
Add Sender...
Edit Settings...
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

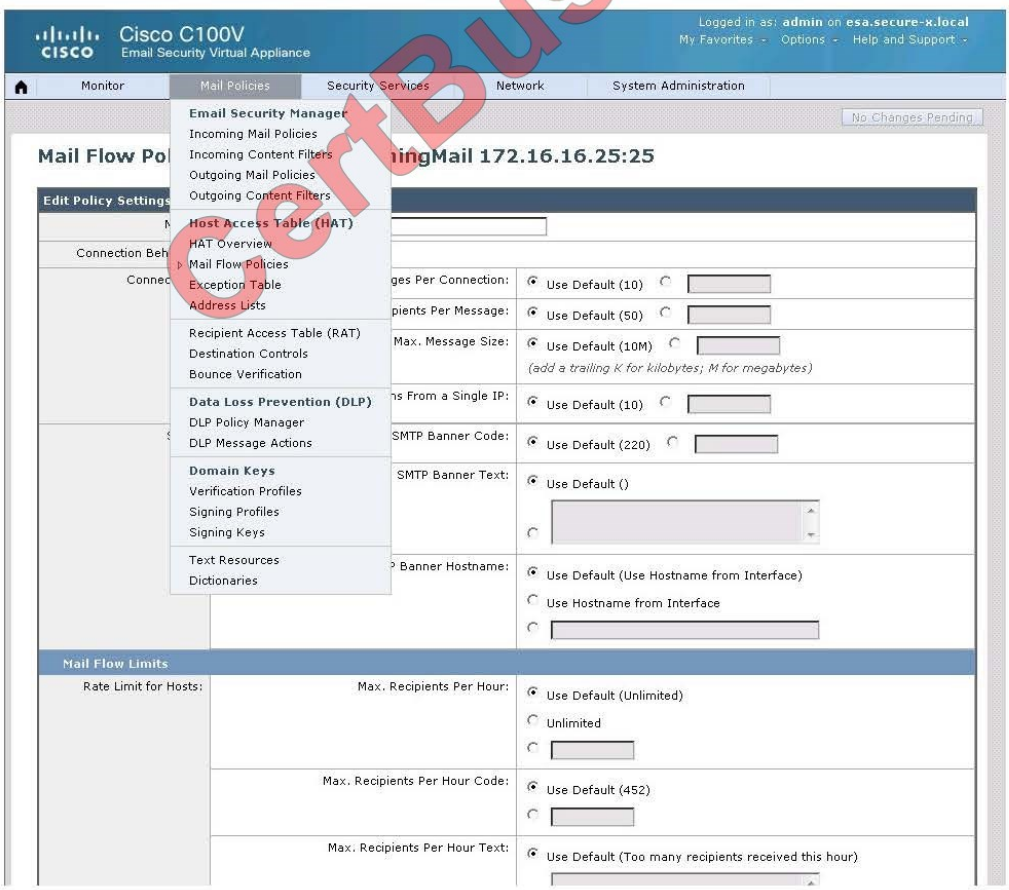
CertBus.com


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: BLOCKED
Connection Behavior: Reject
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) 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
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
Edit Policy Settings
Use Default (10)
Use Default (50)
Use Default (10M)
(add a trailing K for kilobytes; M for megabytes)
Use Default (10)
Use Default (554) 554
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
Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Rate Limit for Hosts:
Use Default (Unlimited)
Unlimited
Use Default (452)
Use Default (Too many recipients received this hour)

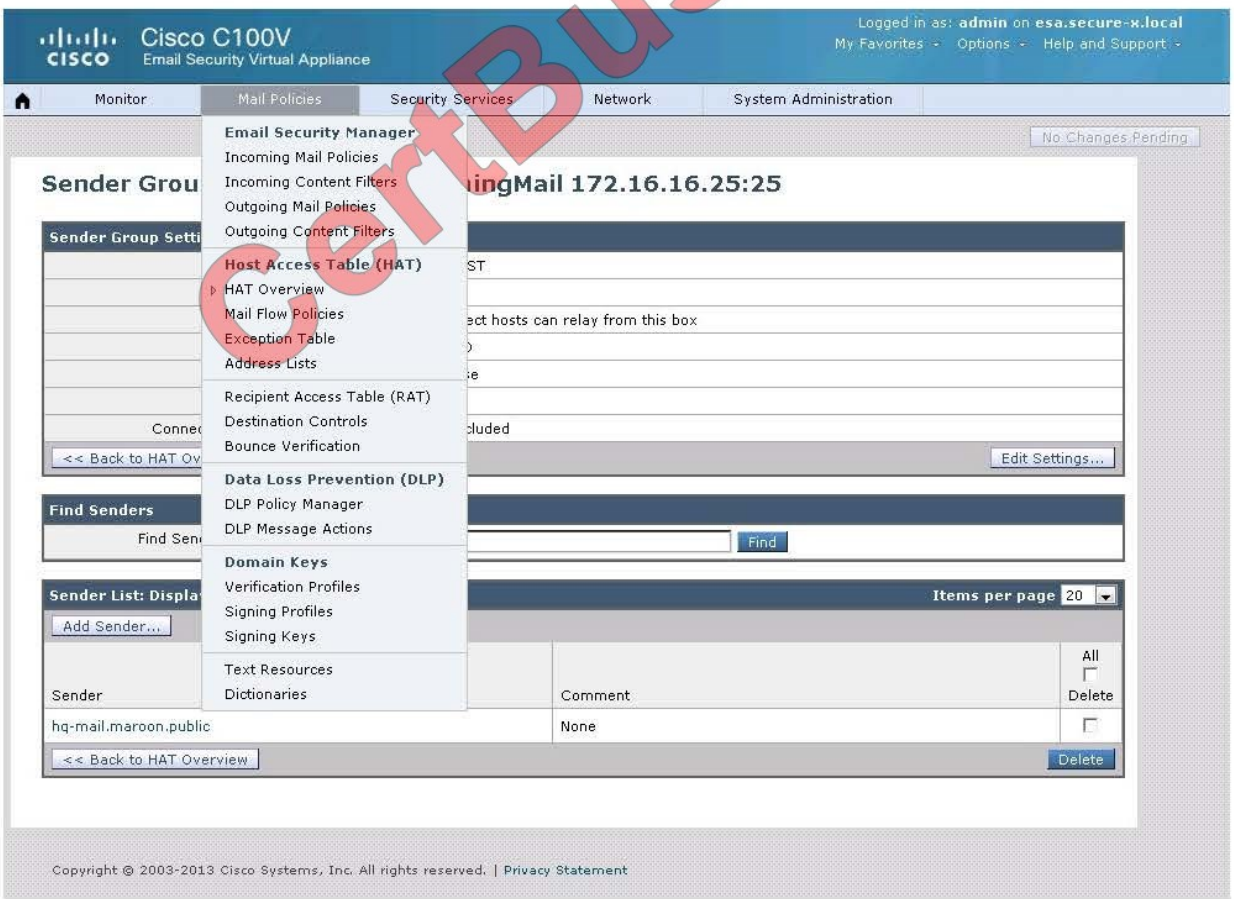
CertBus.com


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: 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:
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
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
Edit Policy Settings
Use Default (10)
Use Default (50)
Use Default (10M)
(add a trailing K for kilobytes; M for megabytes)
Use Default (10)
Use Default (220)
Use Default ()
Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Use Default (Unlimited)
Unlimited
Use Default (452)
Use Default (Too many recipients received this hour)

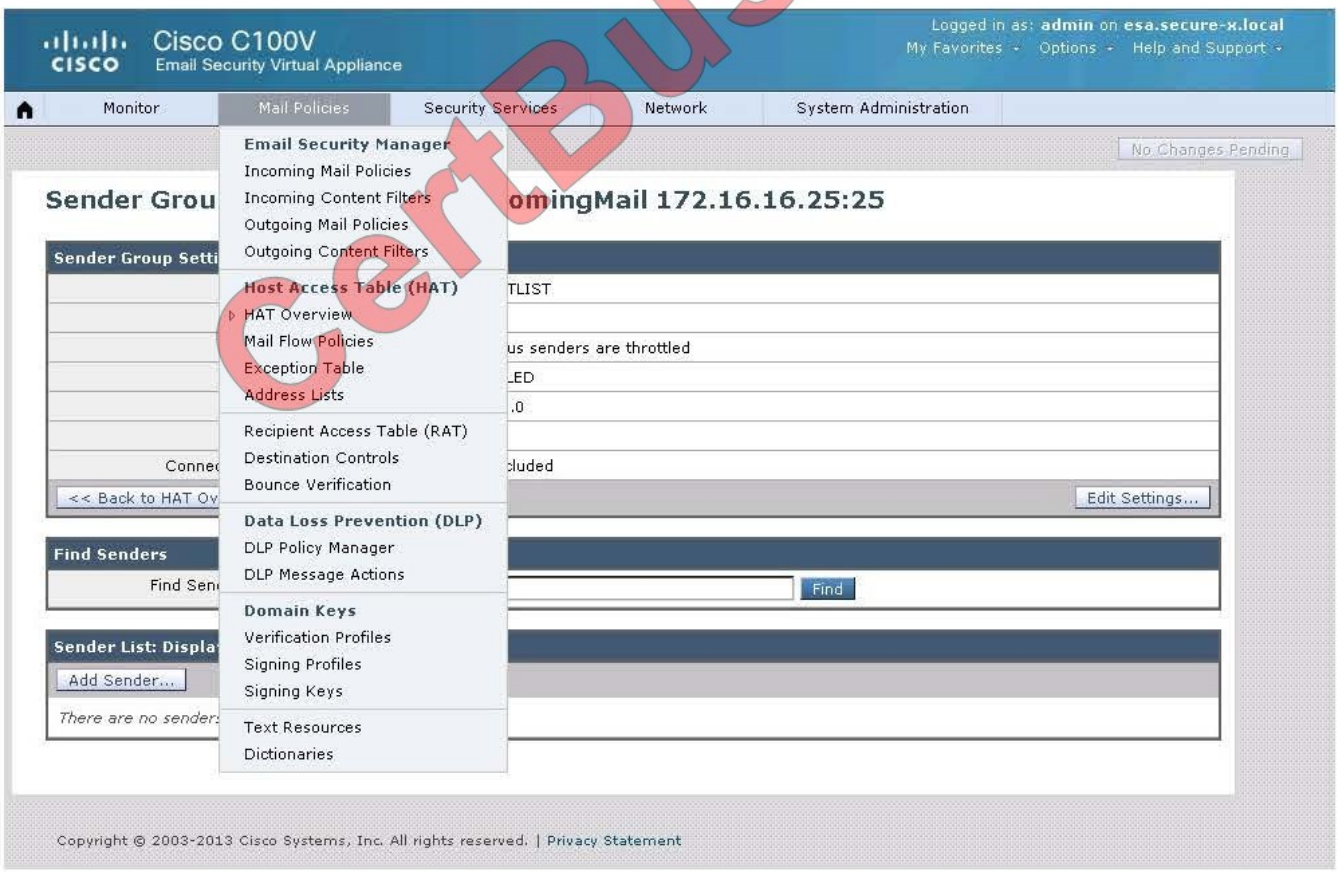
CertBus.com


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: 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
<< 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
hq-mail.maroon.public
None
<< Back to HAT Overview
Delete
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

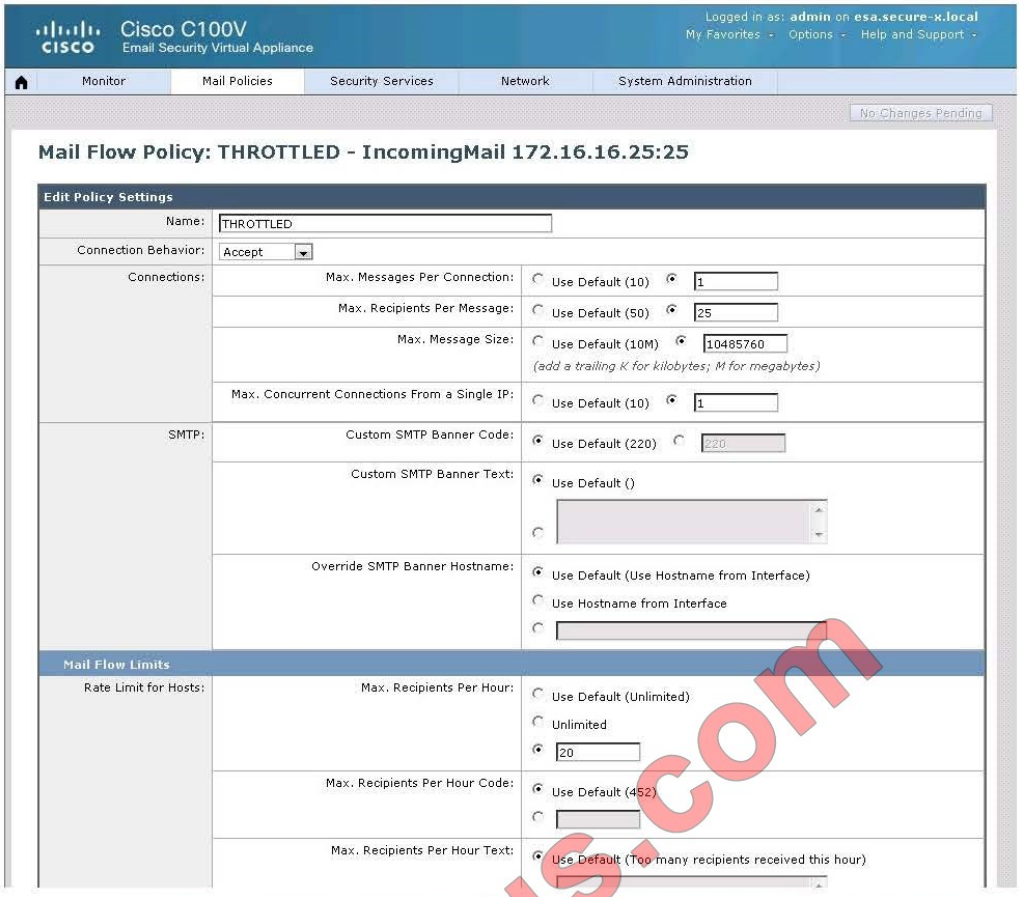

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail 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
Edit Settings...
Find
Items per page 20
Add Sender...
Sender
Comment
All
Delete
hq-mail.maroon.public
None
<< Back to HAT Overview
Delete
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

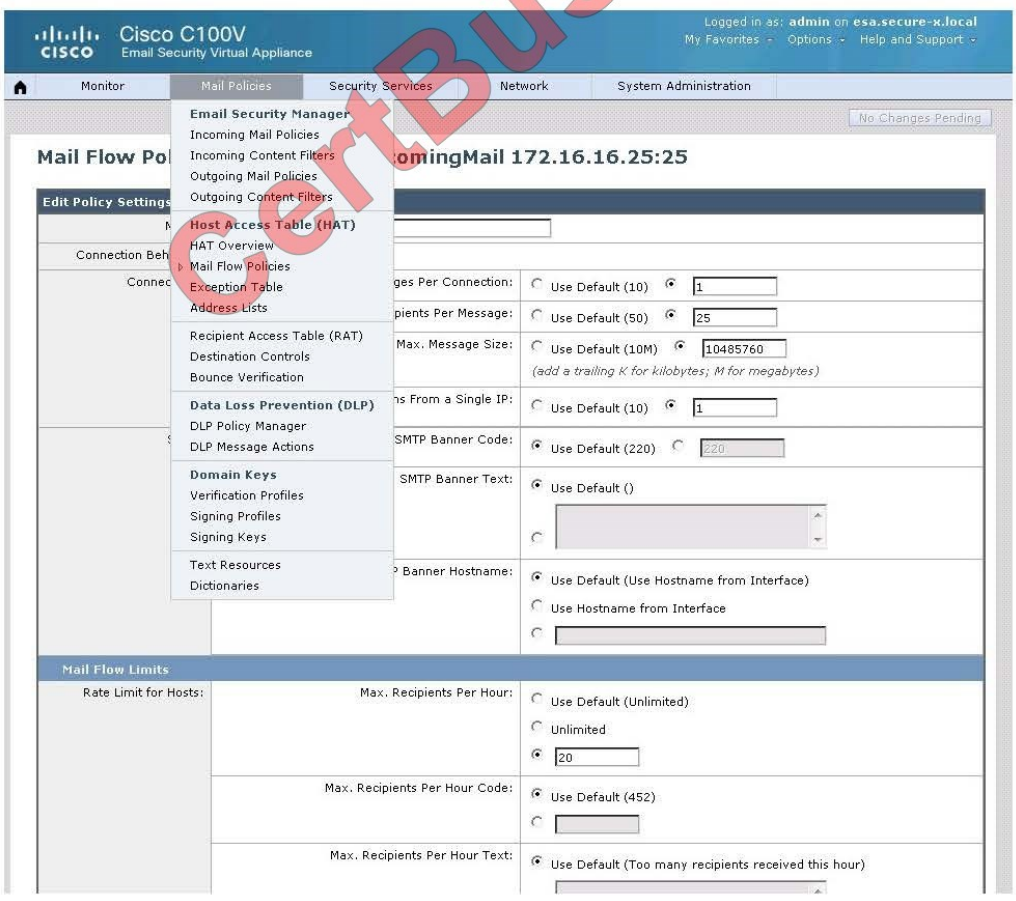
CertBus.com


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

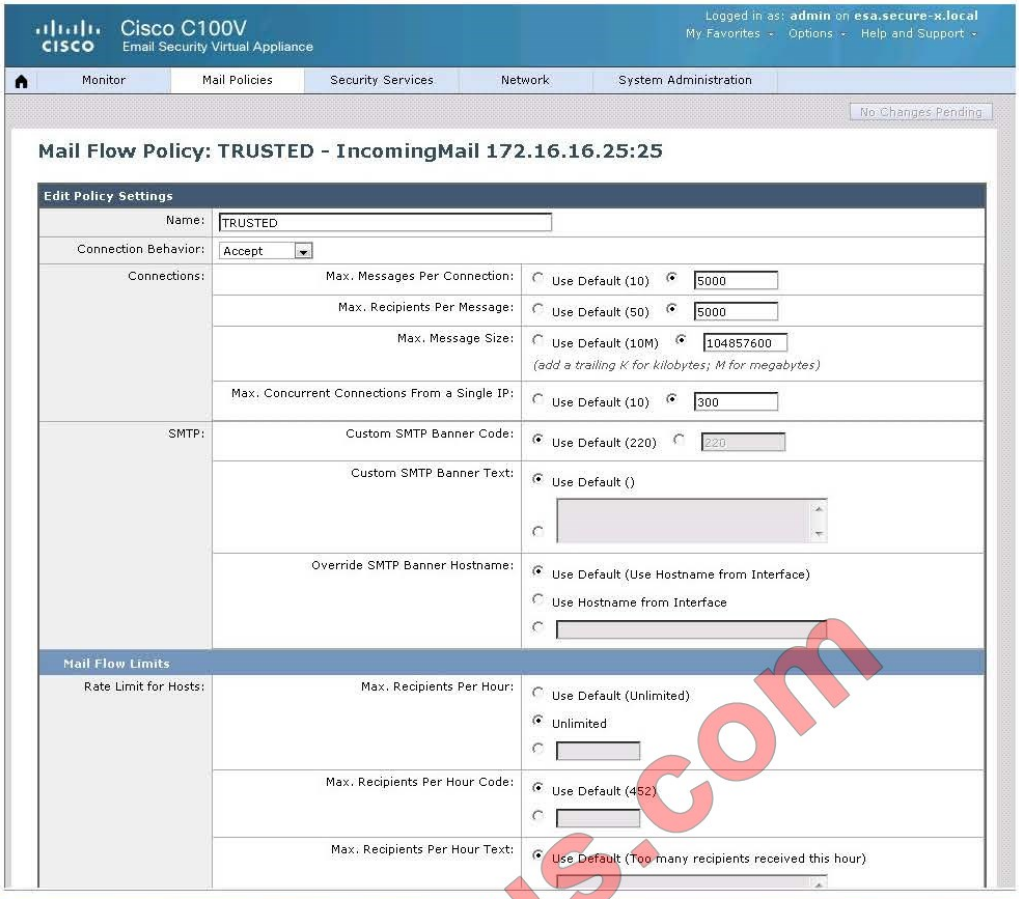

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail 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
Find
Add Sender...
Edit Settings...
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

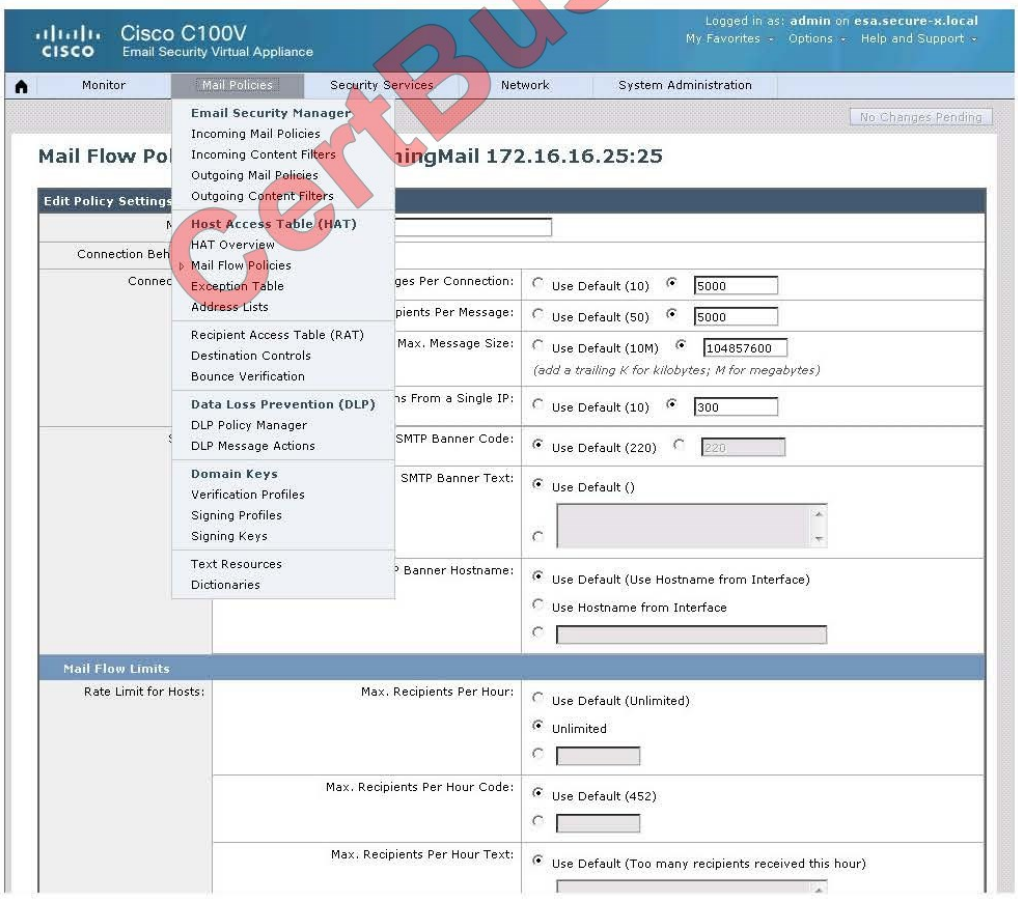
CertBus.com


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: 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)
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)

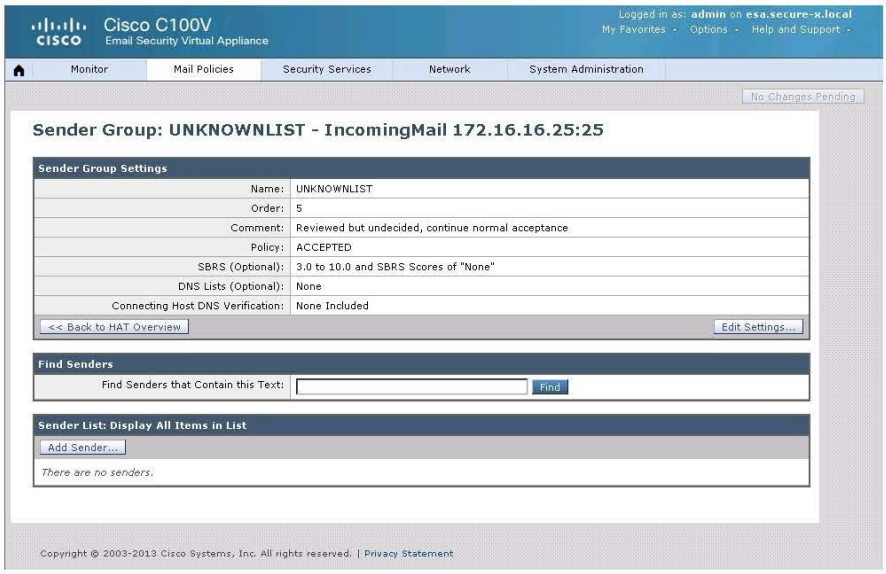

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail 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
Edit Policy Settings
Use Default (10) 1
Use Default (50) 25
Use Default (10M) 10485760
(add a trailing K for kilobytes; M for megabytes)
Use Default (10) 1
Use Default (220) 220
Use Default ()
Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Use Default (Unlimited)
Unlimited
20
Use Default (452)
Use Default (Too many recipients received this hour)

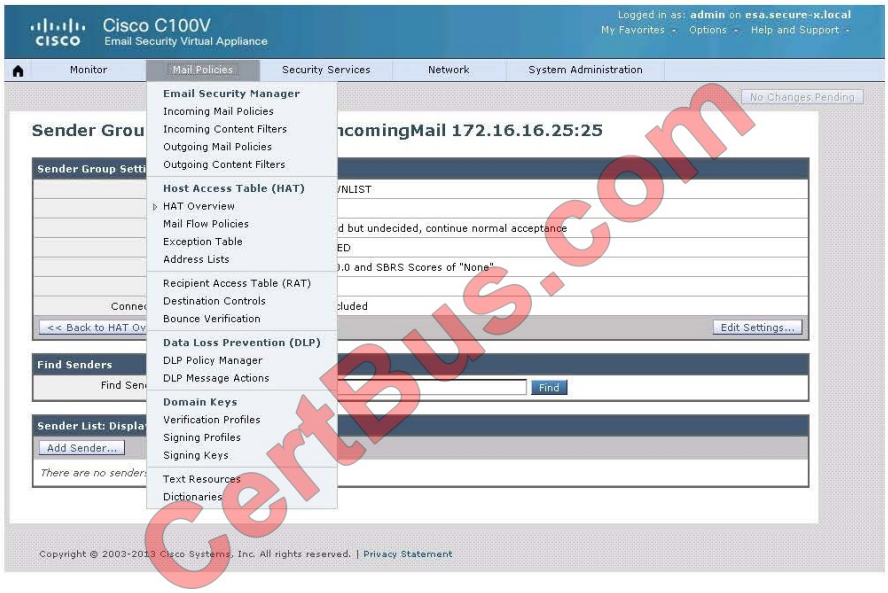
CertBus.com

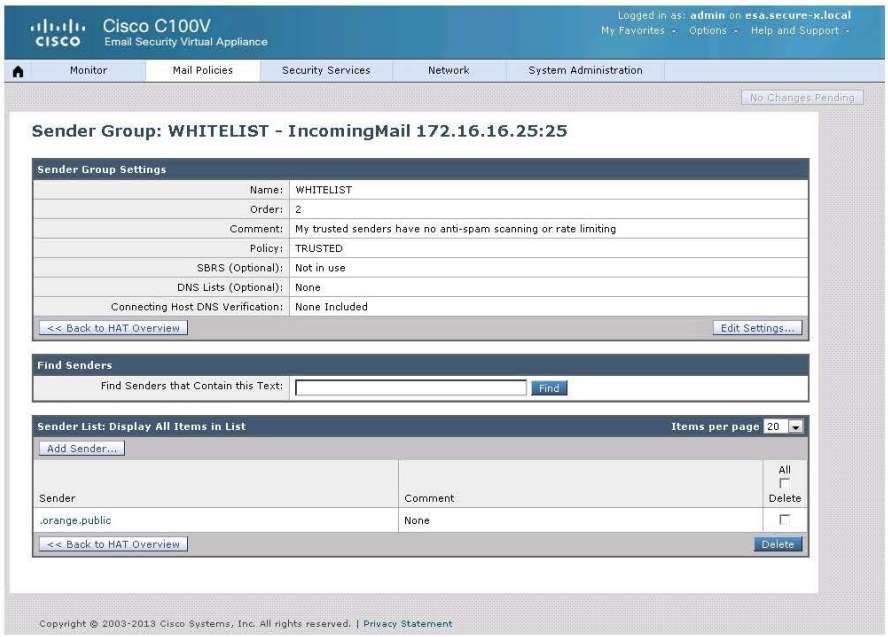

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: 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 ()
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
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
Edit Policy Settings
Use Default (10) 5000
Use Default (50) 5000
Use Default (10M) 104857600
(add a trailing K for kilobytes; M for megabytes)
Use Default (10) 300
Use Default (220) 220
Use Default ()
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)
Use Default (Too many recipients received this hour)

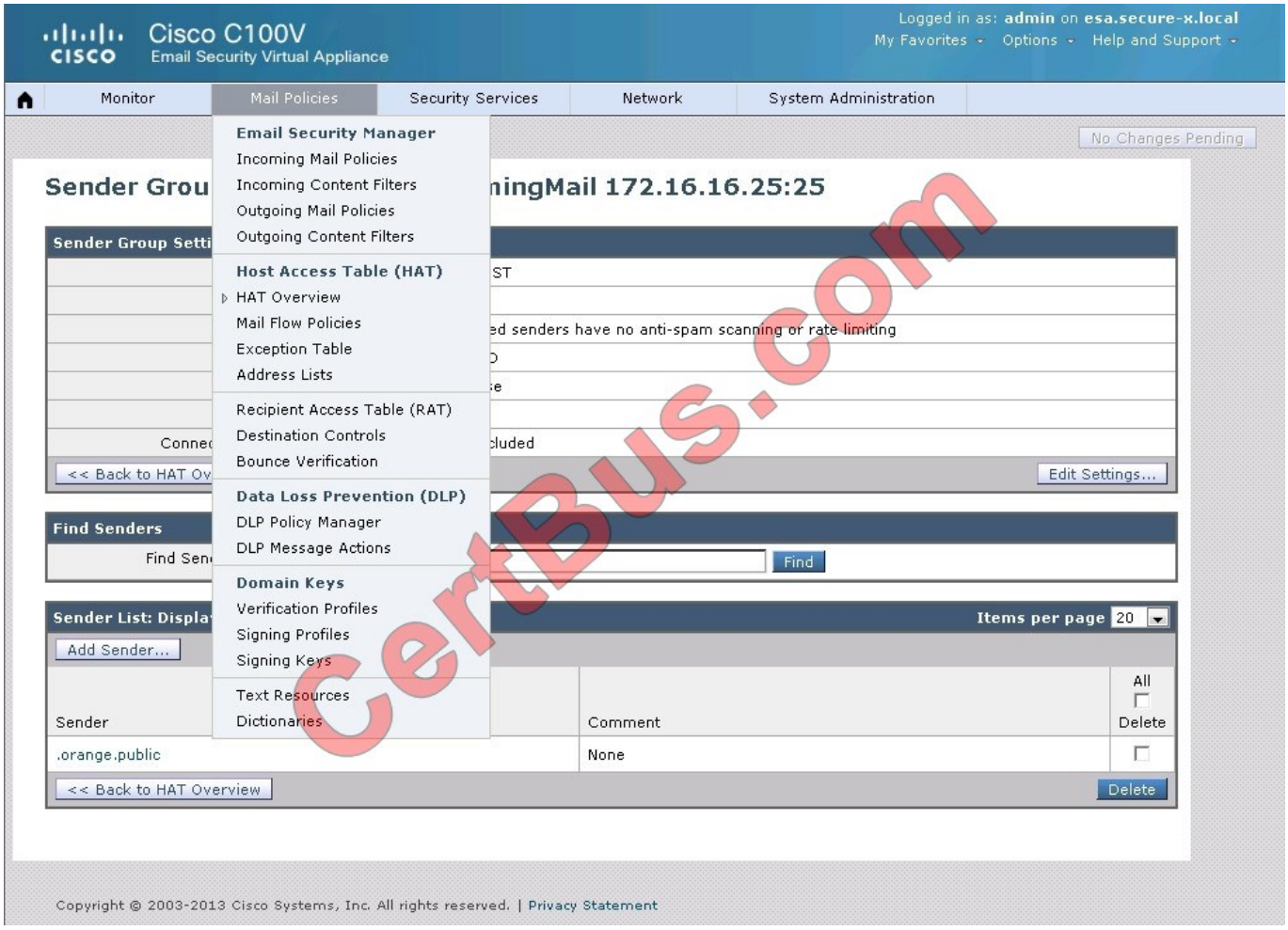
CertBus.com


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: 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
<< 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
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
Find
Add Sender...
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: 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
<< 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
<< Back to HAT Overview
Delete
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

CertBus.com



What is the maximum message size that the Cisco Email Security Appliance will accept from the violet.public domain?

A. 1 KB

B. 100 KB

C. 1 MB

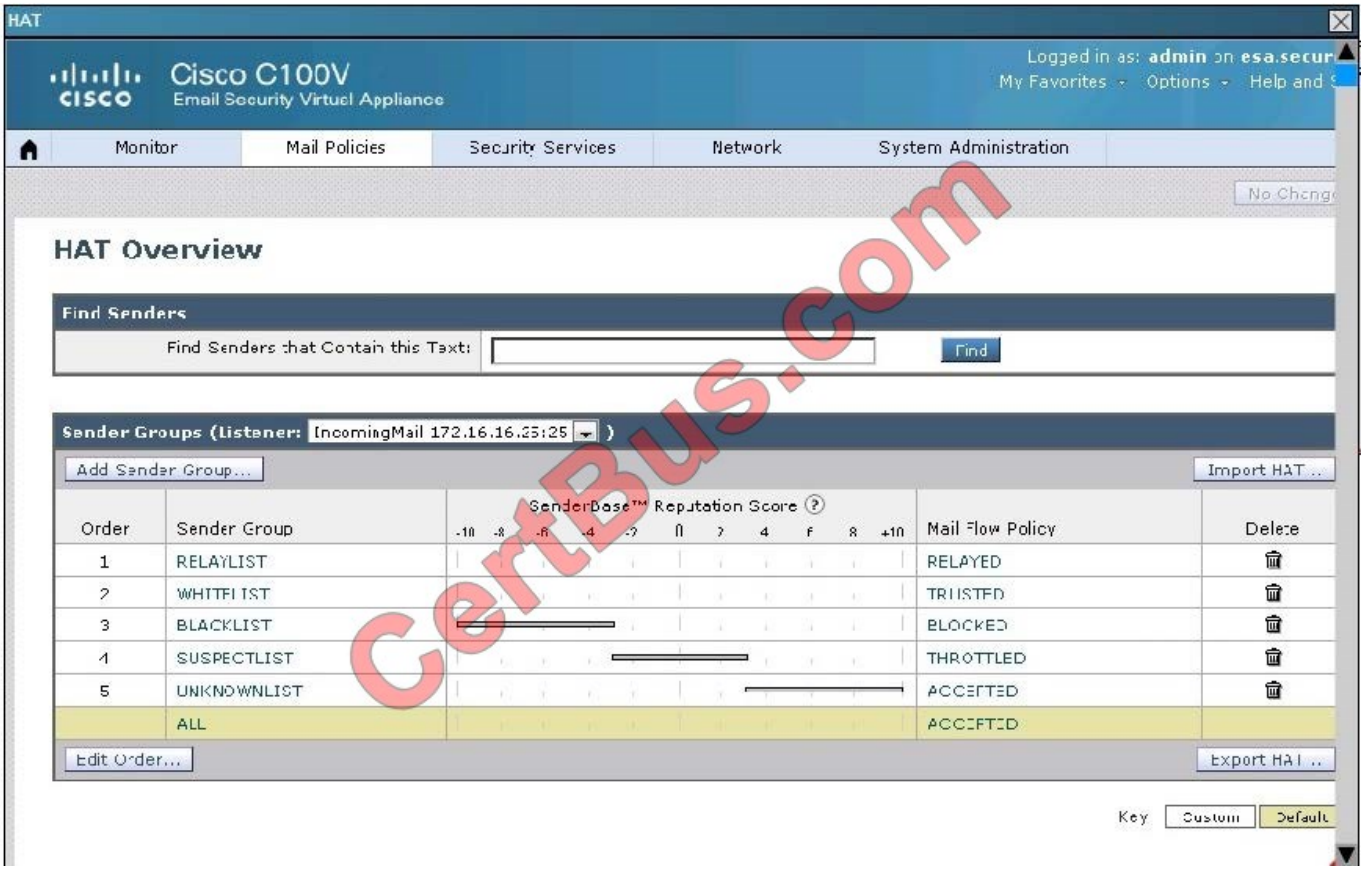
D. 10 MB

E. 100 MB

F. Unlimited

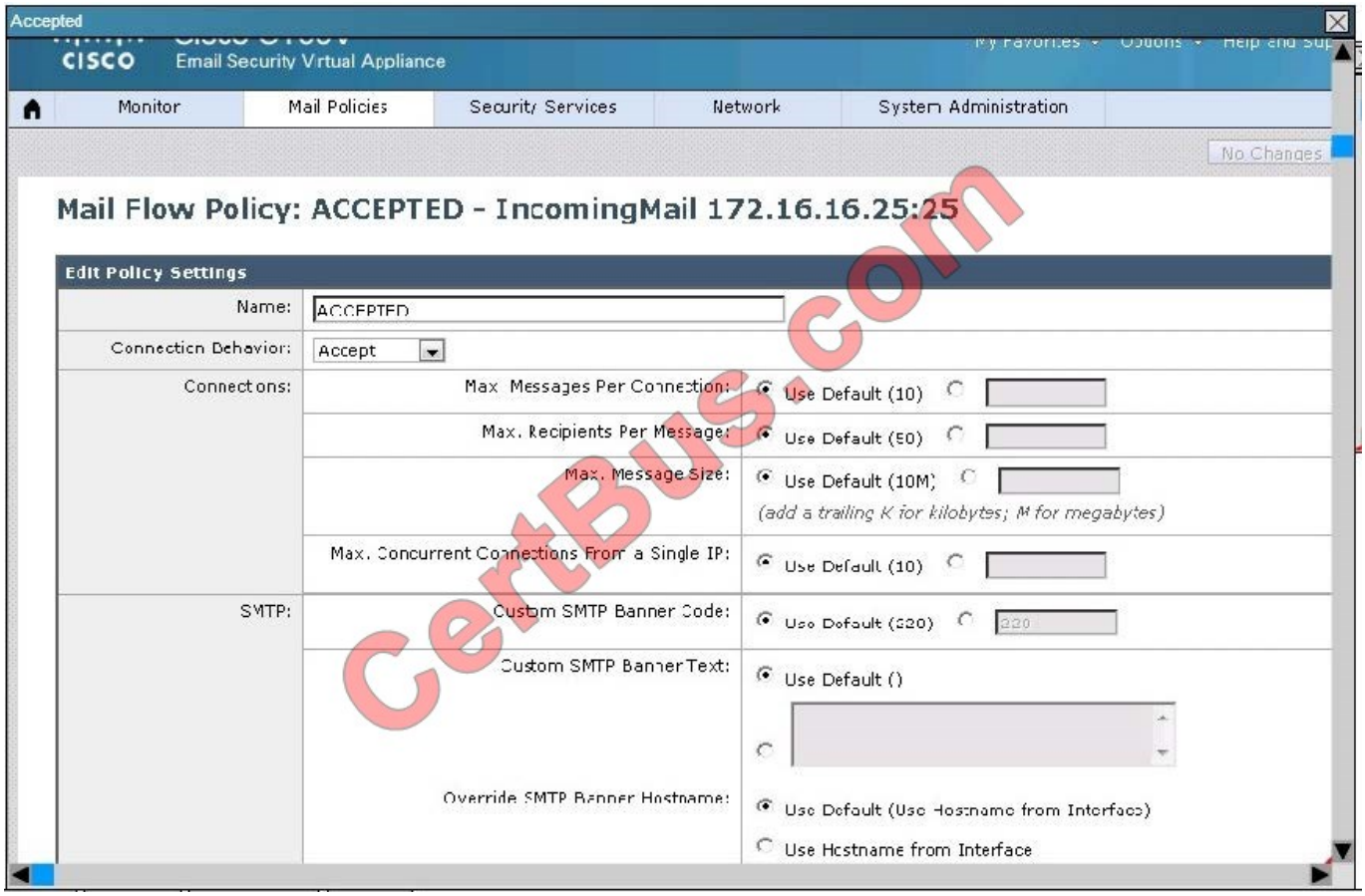
Correct Answer: D

From the instructions we know that the reputation score for the violet.public domain has been set to 8. From the HAT table shown below we know that a score of 8 belongs to the UNKNOWNLIST group, which is assigned the ACCEPTED policy.



Capture

By clicking on the ACCEPTED policy we see that max message size has been set to the default value of 10M:



Capture

QUESTION 9

Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?

A. cloud web services

B. network AMP

C. private cloud

D. public cloud

Correct Answer: C

QUESTION 10

An engineer wants to configure a method to verify the authenticity of emails on cisco ESA and noticed the sender policy framework. How can the SPF help in that task?

A. SPF allows the sender to sign the email using preshared key

B. SPF allows the sender to sign the email using public key

C. SPF allows the owner of an internet domain to use DNS TXT records to specify which machines are authorized to transmit email for that domain.

D. The list of authorized sending hosts for a domain is published in the Domain Name System (DNS) records for that domain in the form of a specially formatted TXT record

Correct Answer: B

QUESTION 11

When a user receives an encrypted email from a Cisco ESA, which technology is used to retrieve the key to open the email?

A. trusted certificate authority

B. private certificate authority

C. Cisco Registered Envelope Service

D. Simple Certificate Enrollment Protocol

Correct Answer: C

QUESTION 12

An engineer is configuring AMP for the first time and can\\'t afford any interruption to which traffic.

Which policy type does not disrupt?

A. Triage

B. Audit

C. Server

D. Protect

Correct Answer: B

300-210 PDF Dumps 300-210 VCE Dumps 300-210 Practice Test

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

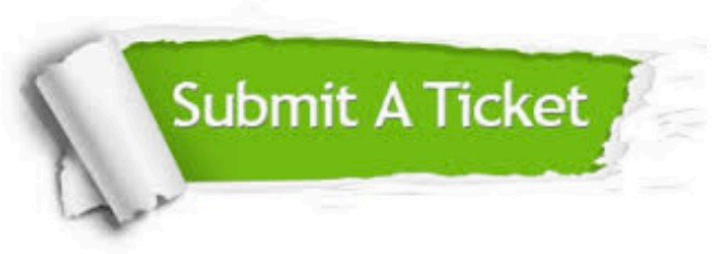
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.certbus.com/allproducts

Need Help

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



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