

Exam : 300-207

Title: Implementing Cisco ThreatControl Solutions

Version : DEMO

1.Which Cisco technology prevents targeted malware attacks, provides data loss prevention and spam protection, and encrypts email?

A. SBA

- B. secure mobile access
- C. IPv6 DMZ web service
- D. ESA
- Answer: D

2.What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?

- A. sslconfig
- B. sslciphers
- C. tlsconifg
- D. certconfig

Answer: A

3. Which command verifies that CWS redirection is working on a Cisco IOS router?

- A. show content-scan session active
- B. show content-scan summary
- C. show interfaces stats
- D. show sessions

Answer: A

4.

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 o these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.	M
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 four multiple choice question about the behavior of the Cisco Email Security Appliance given the configuration and the domain SenderBase Reputation Scores.	ns
	and the second

instructions	8
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can havigate between the Host Access 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	rable A
Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.	Contraction of the
• red.public, -6	
 orange public, -4 	
yellow public, -2	
• green public, 2	1 net
• blue public, 6	22370
Wolet public, 8	

 Monitor
 Mail Policies
 Security Services
 Notwork
 System Administration

Mail Flow Policies			
Policies (Listener: IncomingMail 172.)	16.16.25:25 💌)		CIDA BUILDING CHICK
Add Policy			Constant No. 201
Policy Name		Behavior	State of the second second second
renet manie		behavior	Dele
		Accept	Dele
ACCEPTED BLOCKED			
ACCEPTED		Accept	(7)
ACCEPTED BLOCKED		Accept Reject	() () ()

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 orange. public red. public and orange. public

Answer: B

5. You ran the ssh generate-key command on the Cisco IPS and now administrators are unable to connect. Which action can be taken to correct the problem?

- A. Replace the old key with a new key on the client.
- B. Run the ssh host-key command.
- C. Add the administrator IP addresses to the trusted TLS host list on the IPS.
- D. Run the ssh authorized-keys command.

Answer: A