

Cisco

CCNA Security

640-553 IINS 640-553 IINS 640-553 IINS 640-553 IINS 640-553 IINS

PRINTABLES

PRINTABLE PRACTICE QUESTIONS

QUESTIONS, ANSWERS, AND
DETAILED EXPLANATIONS IN AN
EASY-TO-USE PRINTABLE FORMAT


 LearnSmart™

Table of Contents

Chapter 1

Describe the security threats facing modern network infrastructures..... 2

Answer Key 87
Explanations 99

Chapter 2

Secure Cisco routers..... 6

Answer Key 88
Explanations 103

Chapter 3

Implement AAA on Cisco routers using local router database and external ACS..... 11

Answer Key 89
Explanations 108

Chapter 4

Mitigate threats to Cisco routers and networks using ACLs..... 17

Answer Key 90
Explanations 113

Chapter 5

Implement secure network management and reporting..... 25

Answer Key 91
Explanations 118



Chapter 6

Mitigate common Layer 2 attacks..... 37

Answer Key 92
Explanations 124

Chapter 7

Implement the Cisco IOS firewall feature set using SDM..... 46

Answer Key 94
Explanations 133

Chapter 8

Implement the Cisco IOS IPS feature set using SDM..... 60

Answer Key 96
Explanations 143

Chapter 9

Implement site-to-site VPNs on Cisco Routers using SDM..... 78

Answer Key 97
Explanations 152



CCNA Security (640-553 IINS) Printables

Copyright © 2011 by LearnSmart, LLC.

Product ID: 12024

Production Date: November 15, 2011

Total Questions: 151

All rights reserved. No part of this document shall be stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein.

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

LearnSmart offers favorable discounts on all products when ordered in quantity. For more information, please contact LearnSmart directly:

1-800-418-6789

solutions@learnsmartsystems.com



Chapter 1

Describe the security threats facing modern network infrastructures

1. Which of the following concepts are used to keep data confidential? Select the best answer.
- A. Usernames and Passwords
 - B. Packet Checksums
 - C. DDoS Protection
 - D. MD5 Hashes

[Find the Answer](#) p. 87

2. Which of the following is the concept of keeping data whole from one point to another without change? Select the best answer.
- A. Data Confidentiality
 - B. Data Integrity
 - C. Data Availability
 - D. Data Secrecy

[Find the Answer](#) p. 87

3. Which of the following is the concept of maintaining access to a data source? Select the best answer.
- A. Data Confidentiality
 - B. Data Integrity
 - C. Data Availability
 - D. Access Control

[Find the Answer](#) p. 87



4. Which of the following attack categories occurs when an attacker is able to get close to the physical equipment? Select the best answer.
- A. Active
 - B. Insider
 - C. Near By
 - D. Close-in

[Find the Answer](#) p. 87

5. Which of the following attack categories occurs when an attacker utilizes a packet sniffer in order to obtain information to gain access to a network? Select the best answer.
- A. Passive
 - B. Distribution
 - C. Active
 - D. Insider

[Find the Answer](#) p. 87

6. Which of the following attack categories occurs when a rogue developer builds a backdoor into a program? Select the best answer.
- A. Passive
 - B. Distribution
 - C. Active
 - D. Backdoor

[Find the Answer](#) p. 87



7. What is the name of the Cisco security solution which involves multiple overlapping levels of defense? Select the best answer.
- A. Deep Defense
 - B. Tiered Protection
 - C. Defense in Depth
 - D. Active Defense

[Find the Answer](#) p. 87

8. Which of the following answers correctly shows a TCP handshake? Select the best answer.
- A. SYN (Sequence Number = 1)
SYN, ACK (Sequence Number = 0, Acknowledgement Number = 1)
ACK (Sequence Number = 2, Acknowledgement Number = 0)
 - B. SYN (Sequence Number = 1)
ACK (Sequence Number = 0, Acknowledgement Number = 2)
SYN, ACK (Sequence Number = 2, Acknowledgement Number = 1)
 - C. SYN (Sequence Number = 1)
SYN, ACK (Sequence Number = 0, Acknowledgement Number = 0)
ACK (Sequence Number = 0, Acknowledgement Number = 2)
 - D. SYN (Sequence Number = 1)
SYN, ACK (Sequence Number = 0, Acknowledgement Number = 2)
ACK (Sequence Number = 2, Acknowledgement Number = 1)

[Find the Answer](#) p. 87



9. What type of spoofing occurs when an attacker is not on the local subnet of the target? Select the best answer.
- A. Blind Spoofing
 - B. Remote Spoofing
 - C. Local Spoofing
 - D. Non-Blind Spoofing

[Find the Answer](#) p. 87



Chapter 2

Secure Cisco routers

1. What command would be used to configure a MD5 hashed password to enter enable mode? Select the best answer.
- A. `router(config)#username username secret password`
 - B. `router(config)#enable secret password`
 - C. `router(config-line)#password password`
 - D. `router(config)#enable password password`

[Find the Answer](#) p. 88

2. What command would be used to configure a reversible password to enter enable mode? Select the best answer.
- A. `router(config)#username username secret password`
 - B. `router(config)#enable secret password`
 - C. `router(config)#enable password password`
 - D. `router(config-line)#password password`

[Find the Answer](#) p. 88

3. What command would be used in order to configure a password on all connections coming in to the router via telnet? Select the best answer.
- A. `router(config)#password password`
 - B. `router(config)#enable secret password`
 - C. `router(config)#enable password password`
 - D. `router(config-line)#password password`

[Find the Answer](#) p. 88



4. What command could be configured to limit the amount of times a router allows login attempts to 3 before causing a login process delay? Select the best answer.
- A. `router(config)#security authentication failure rate 3 log`
 - B. `router(config)#security authentication failure rate 3`
 - C. `router(config)authentication failure login 3`
 - D. `router(config)login failure 3`

[Find the Answer](#) p. 88

5. What command would be used to create a separate privilege level 7 which would only allow the user to run basic show commands including the show running-config? Select the best answer.
- A. `router(config)#enable secret level 7 password`
`router(config)#privilege exec level 7 show`
 - B. `router(config)#enable secret level 7 password`
`router(config)#privilege exec level 7 show`
`router(config)#privilege exec level 7 show running-config`
 - C. `router(config)#privilege exec level 7 show`
`router(config)#privilege exec level 7 show running-config`
 - D. `router(config)#privilege exec level 7 show`

[Find the Answer](#) p. 88

6. When configuring CLI views what is the first command that is required? Select the best answer.
- A. `router#enable view`
 - B. `router(config)#enable view`
 - C. `router(config)#aaa new-model`
 - D. `router(config-view)#aaa new-model`

[Find the Answer](#) p. 88



7. What command would be used to enable security for the IOS image? Select the best answer.
- A. router(config)#secure boot-config
 - B. router(config)#secure bootset
 - C. router(config)#security boot-image
 - D. router(config)#secure boot-image

[Find the Answer](#) p. 88

8. What command would be used to enable security for running-configuration? Select the best answer.
- A. router(config)#secure boot-config
 - B. router(config)#secure boot-set
 - C. router(config)#security boot-config
 - D. router(config)#secure boot-image

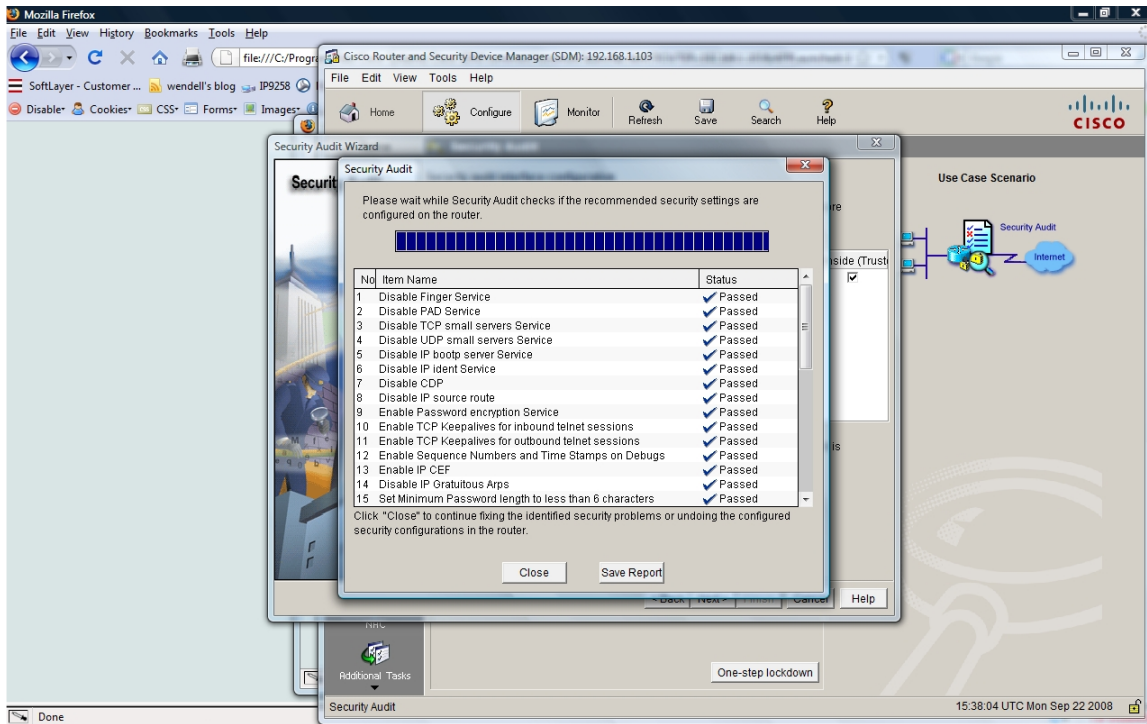
[Find the Answer](#) p. 88

9. What are the items which are clicked on to get to this point in SDM? Select the best answer.
- A. Configure
Security Audit
 - B. Configure
Security Audit
Perform Security Audit
 - C. Configure
Security Audit
One-step Lockdown
 - D. Configure
Perform Security Audit

[Find the Answer](#) p. 88

Exhibit(s):





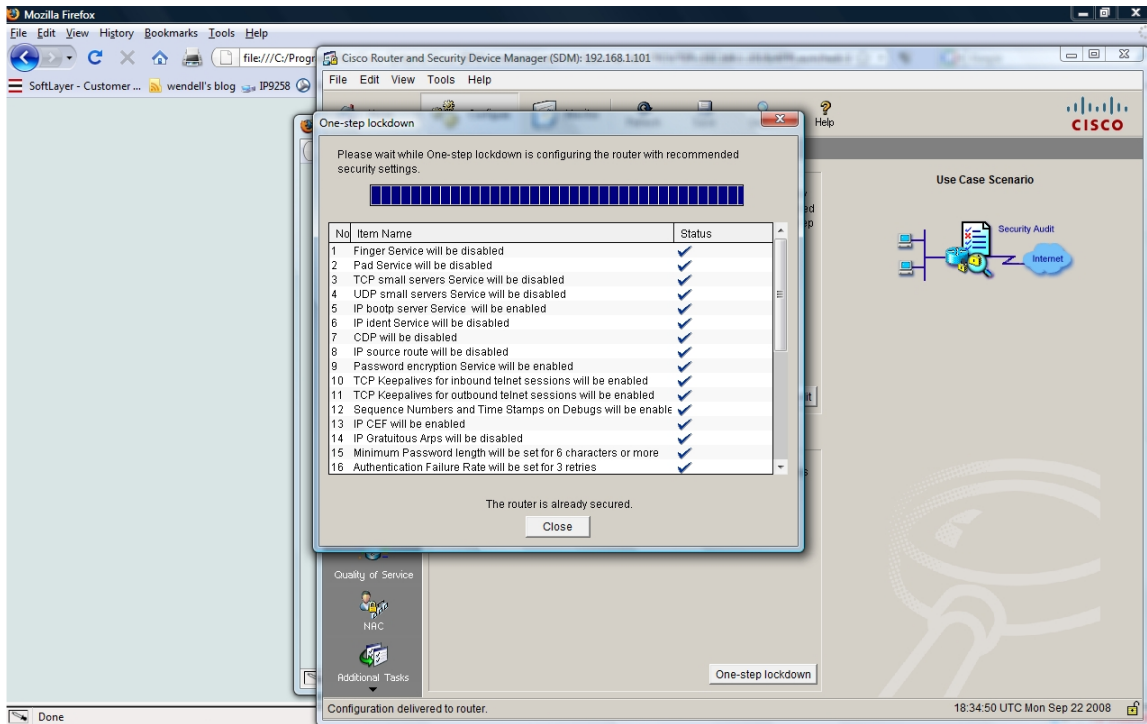
10. Referring to the Exhibit below, What are the items which are clicked on to get to this point in SDM? Select the best answer.

- A. Configure Security Audit
- B. Configure Security Audit Perform Security Audit
- C. Configure Security Audit One-step Lockdown
- D. Configure Perform Security Audit

[Find the Answer](#) p. 88

Exhibit(s):





11. What are the commands which are required (at a minimum) to get SDM up and working without SSL? Select the best answer.

- A. `router(config)#ip http server`
`router(config)#ip http secure-server`
`router(config)#ip http authentication local`
`router(config)#username username privilege 15 secret 0 password`
- B. `router(config)#ip http secure-server`
`router(config)#username username privilege 15 secret 0 password`
- C. `router(config)#ip http server`
`router(config)#ip http secure-server`
`router(config)#ip http authentication local`
- D. `router(config)#ip http server`
`router(config)#ip http authentication local`
`router(config)#username username privilege 15 secret 0 password`

[Find the Answer](#) p. 88



Chapter 3

Implement AAA on Cisco routers using local router database and external ACS

1. What command is used to enable the use of AAA for login? Select the best answer.

- A. router(config)#aaa authentication login
- B. router(config)#aaa authentication
- C. router(config)#aaa local authentication
- D. router#aaa authentication local

[Find the Answer](#) p. 89

2. What command is used to enable the use of AAA using the local database with PPP? Select the best answer.

- A. router(config)#aaa authentication ppp local
- B. router(config)#aaa authentication ppp default local
- C. router(config)#aaa authentication local ppp
- D. router(config)#ppp authentication aaa default local

[Find the Answer](#) p. 89



3. What commands would be used to enable local AAA authentication on initial login to the console? Use 'console-in' as a name of the authentication list. Select the best answer.
- A. `router(config)#username username secret password`
`router(config)#aaa authentication login console-in local`
`router(config-line)#login authentication console-in`
 - B. `router(config)#aaa new-model`
`router(config)#username username secret password`
`router(config)#aaa authentication login console-in local`
`router(config)#login authentication console-in`
 - C. `router(config)#aaa new-model`
`router(config)#username username secret password`
`router(config)#aaa authentication login console-in local`
`router(config-line)#login authentication console-in`
 - D. `router(config)#aaa new-model`
`router(config)#aaa authentication login console-in local`
`router(config-line)#login authentication console-in`

[Find the Answer](#) p. 89

4. What command would be used to configure list-name 'com_auth' to authorize all level 15 commands using the local database? Select the best answer.
- A. `router(config)#aaa authorization commands com_auth local 15`
 - B. `router(config)#aaa authorization commands com_auth 15 local`
 - C. `router(config-line)#aaa authorization commands 15 com_auth local`
 - D. `router(config)#aaa authorization commands 15 com_auth local`

[Find the Answer](#) p. 89



5. What command would be used to configure reverse telnet authorization using TACACS+ by default? Select the best answer.
- A. `router(config)#aaa authorization reverse-access default group tacacs+`
 - B. `router(config)#aaa authorization reverse-access default tacacs+`
 - C. `router(config)#aaa authorization reverse-telnet default group tacacs+`
 - D. `router(config)#aaa authorization reverse-access com_auth group tacacs+`

[Find the Answer](#) p. 89

6. What command would be used to enable level 15 command authorization by default allowing only validly authenticated users? Select the best answer.
- A. `router(config)#aaa authorization commands 15 if-authenticated default`
 - B. `router(config)#aaa authorization commands 15 default if-authenticated`
 - C. `router(config)#aaa authorization commands 15 default`
 - D. `router(config)#aaa authorization commands 15 if-authenticated`

[Find the Answer](#) p. 89



7. What AAA command would you use to log all level 15 commands entered, only sending this information once and send this information to a TACACS+ server? Select the best answer.
- A. router(config)#aaa accounting commands 15 default start-stop group tacacs+
 - B. router(config-line)#aaa accounting commands 15 default stop-only group tacacs+
 - C. router(config)#aaa accounting commands 15 default stop-only group tacacs+
 - D. router#aaa accounting commands 15 default stop-only group tacacs+

[Find the Answer](#) p. 89

8. What AAA command would be used to enable the most thorough accounting on all network related service requests by default using TACACS+? Select the best answer.
- A. router(config)#aaa accounting default start-stop group tacacs+
 - B. router#aaa accounting network default start-stop group tacacs+
 - C. router(config)#aaa accounting network default stop-only group tacacs+
 - D. router(config)#aaa accounting network default start-stop group tacacs+

[Find the Answer](#) p. 89

9. What AAA protocol can be used to limit which commands can specifically be controlled by user? Select the best answer.
- A. TACACS+
 - B. SDM
 - C. LDAP
 - D. RADIUS

[Find the Answer](#) p. 89



10. What AAA command would be used to creating a connection to a TACACS+ server and is configured to open and close TCP sessions throughout each session? Select the best answer.
- A. router(config)#tacacs-server host server-ip-address single-connection
 - B. router(config)#tacacs-server host server-ip-address
 - C. router(config)#tacacs-server server-ip-address single-connection
 - D. router(config)#tacacs-server server-ip-address

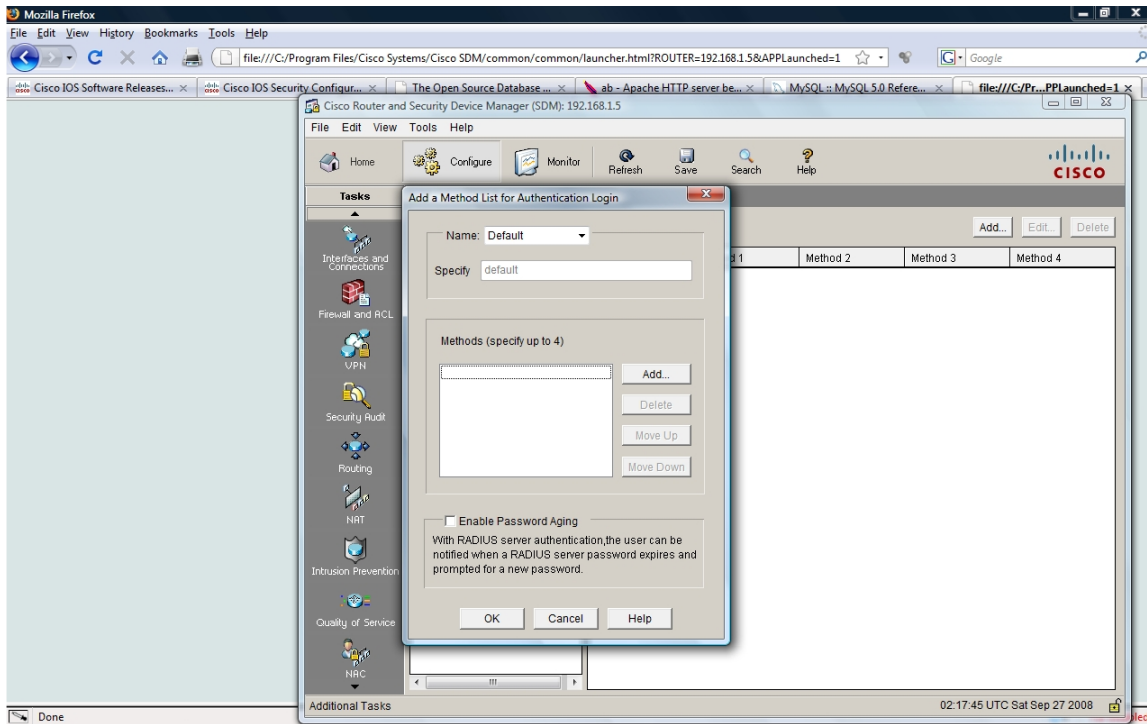
[Find the Answer](#) p. 89

11. Referring to the Exhibit below, What are the items which are clicked on to get to this point in SDM? Select the best answer.
- A. Configure
AAA
Authentication Policies
Login
 - B. Configure
Additional Tasks
AAA
Login
 - C. Configure
Additional Tasks
AAA
Authentication Policies
Login
 - D. Configure
AAA
Login

[Find the Answer](#) p. 89

Exhibit(s):





Chapter 4

Mitigate threats to Cisco routers and networks using ACLs

1. What would be the syntax for a standard access list to deny the 192.168.1.0/24 network using the last available ACL number and log all matches? Select the best answer.

- A. `router(config)#access-list 99 deny 192.168.1.0 0.0.0.255`
- B. `router(config)#access-list 99 deny 192.168.1.0 255.255.255.0 log`
- C. `router(config)#access-list 99 deny 192.168.1.0 255.255.255.0`
- D. `router(config)#access-list 99 deny 192.168.1.0 0.0.0.255 log`

[Find the Answer](#) p. 90

2. What would be the syntax for an extended access list to permit the 172.16.0.0/16 network to send telnet traffic to the 10.10.10.0/24 network using the first available ACL number? Select the best answer.

- A. `router(config)#access-list 100 permit tcp 172.16.0.0 0.0.255.255 10.10.10.0 0.0.0.255 eq telnet`
- B. `router(config)#access-list 100 permit tcp 172.16.0.0 255.255.0.0 10.10.10.0 255.255.0.0 eq telnet`
- C. `router(config)#access-list 1 permit tcp 172.16.0.0 0.0.255.255 10.10.10.0 0.0.0.255 eq telnet`
- D. `router(config)#access-list 1 permit tcp 172.16.0.0 255.255.0.0 10.10.10.0 255.255.0.0 eq telnet`

[Find the Answer](#) p. 90



3. What is the correct command to use to enable the turbo ACL feature? Select the best answer.
- A. `router(config)#access-list turbo`
 - B. `router(config)#access-list compiled`
 - C. This is enabled with the 'turbo' keyword at the end of a access-list statement.
 - D. `router(config-if)#ip access-group list-number turbo`

[Find the Answer](#) p. 90

4. What is the correct command to use to enable access-list 50 coming into the fastethernet 0/0 interface? Select the best answer.
- A. `router(config)#ip access-group in fastethernet 0/0`
 - B. `router(config-if)#ip access-group in 10`
 - C. `router(config-if)#ip access-group 10 in`
 - D. `router(config)#ip access-group fastethernet 0/0 in`

[Find the Answer](#) p. 90

5. Which of the following statements is correct when referring to ACL's? Select the best answer.
- A. Standard ACL's should be placed as close to the source as possible.
 - B. Extended ACL's should be placed as close to the destination as possible.
 - C. Standard ACL's should be placed as close to the destination or source as possible.
 - D. Standard ACL's should be placed as close to the destination as possible.

[Find the Answer](#) p. 90



6. Which of the following statements is correct when referring to ACL's? Select the best answer.
- A. Extended ACL's should be placed as close to the source as possible.
 - B. Extended ACL's should be placed as close to the destination or source as possible.
 - C. Extended ACL's should be placed as close to the destination as possible.
 - D. Standard ACL's should be placed as close to the source as possible.

[Find the Answer](#) p. 90

7. What is the correct command to enable access-list 40 coming into VTY ports 0 through 4? Select the best answer.
- A. router(config-line)#access-class in 40
 - B. router(config-line)#access-class 40 in
 - C. router(config)#access-list 40 in
 - D. router(config-line)#access-list 40 in

[Find the Answer](#) p. 90

8. What is the correct command to enable SNMP RO filtering of community 'public' with access-list 80? Select the best answer.
- A. router(config)#snmp-server community public rw 80
 - B. router(config)#access-class 80 in community public
 - C. router(config)#snmp-server community public ro 80
 - D. router(config)#access-class community public 80 in

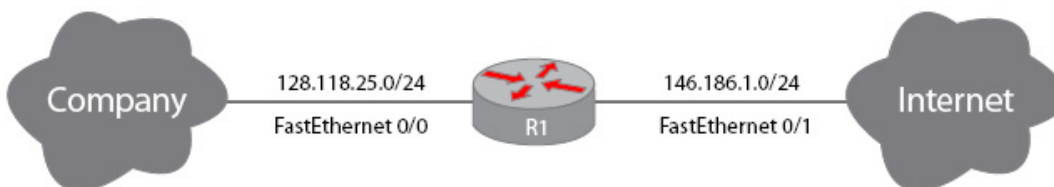
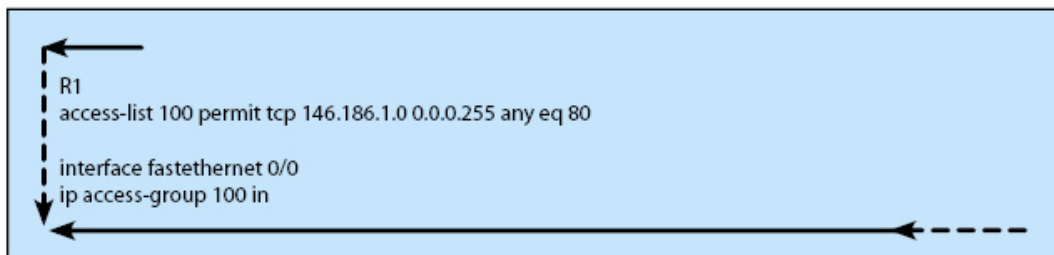
[Find the Answer](#) p. 90



9. Referring to the exhibit, you are trying to limit the traffic coming in from the Internet. Will the configuration in the exhibit work and why? Select the best answer.
- A. No, because the access-list does not match the correct IP addresses used in this exhibit.
 - B. Yes, this configuration will work because the access-list disables all traffic but web traffic coming from the Internet.
 - C. No, this configuration will not work because the access-list is not formatted correctly.
 - D. No, this configuration will not work because the access-list is enabled in the wrong direction.

[Find the Answer](#) p. 90

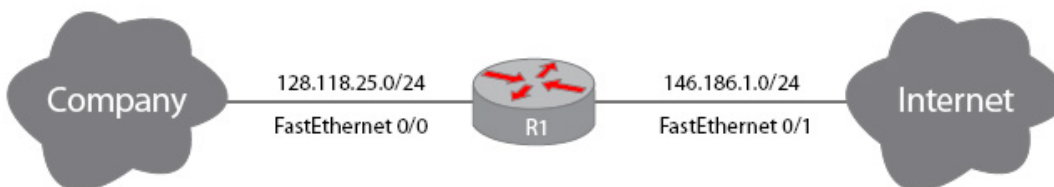
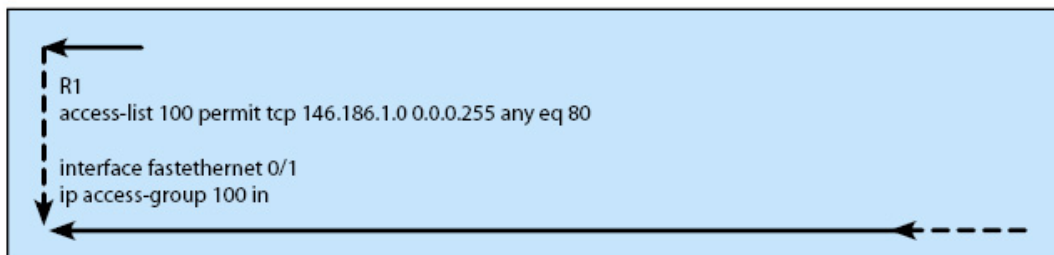
Exhibit(s):



10. Referring to the exhibit, you are trying to limit the traffic coming in from the Internet. Will the configuration in the exhibit work and why? Select the best answer.
- A. Yes, this configuration will work because it only allows traffic from the Internet which is on port 80 (web).
 - B. No, this configuration does not work because of the implicit allow at the end of an access-list.
 - C. No, this configuration will not work because the access-list is not formatted correctly.
 - D. No, this configuration will not work because the access-group statement is formatted incorrectly.

[Find the Answer](#) p. 90

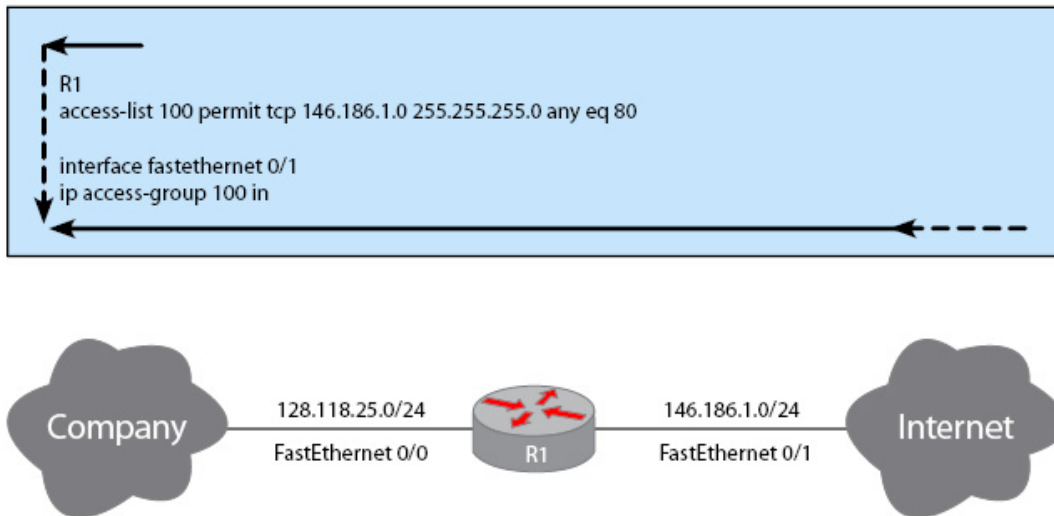
Exhibit(s):



11. Referring to the exhibit, you are trying to limit the traffic coming in from the Internet. Will the configuration in the exhibit work and why? Select the best answer.
- A. No, this will not work because the access-list is enabled in the wrong direction.
 - B. No, this will not work correctly because the format of the access-list is not correct because access-list statements use inverse-masks.
 - C. No, this will not work because the IP addresses matched in the access-list do not match the exhibit.
 - D. Yes, this will correctly only allow Internet web traffic to reach the company's network.

[Find the Answer](#) p. 90

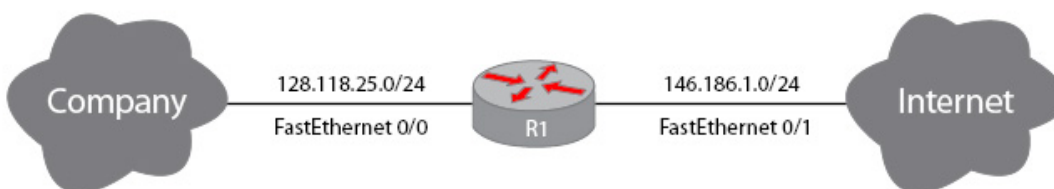
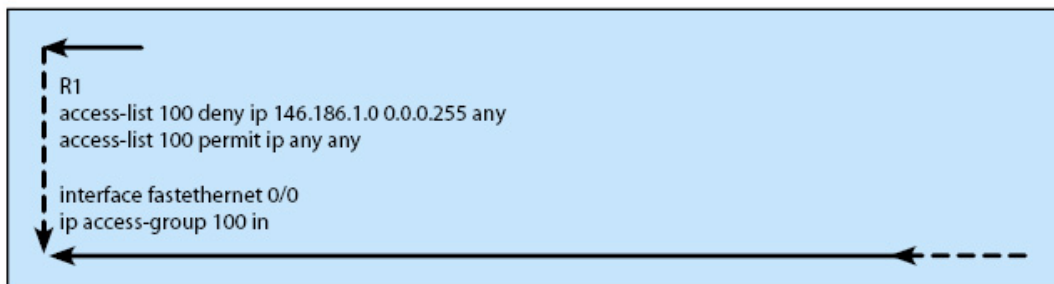
Exhibit(s):



12. Referring to the exhibit, you are trying to configure an access-list to block spoofing attempts. Will the configuration in the exhibit provide a means to accomplish this? Select the best answer.
- A. Yes, this configuration will correctly block Internet traffic from coming in the internal interface.
 - B. No, this configuration will not work because the access-list statement is incorrect.
 - C. Yes, this configuration will correctly block internal traffic from coming in the Internet interface.
 - D. No, this configuration will not work because the access-group command is configured in the wrong direction.

[Find the Answer](#) p. 90

Exhibit(s):



13. Referring to the exhibit, you are trying to configure an access-list to block spoofing attempts. Will the configuration in the exhibit provide a means to accomplish this? Select the best answer.
- A. Yes, this configuration will correctly block traffic from the internal IP network from coming in the Internet port.
 - B. No, this configuration will not work correctly because the access-list is formatted incorrectly.
 - C. No, this configuration will not work because the access-group is not formatted correctly.
 - D. No, this configuration will not work correctly because the access-group is configured in the wrong direction.

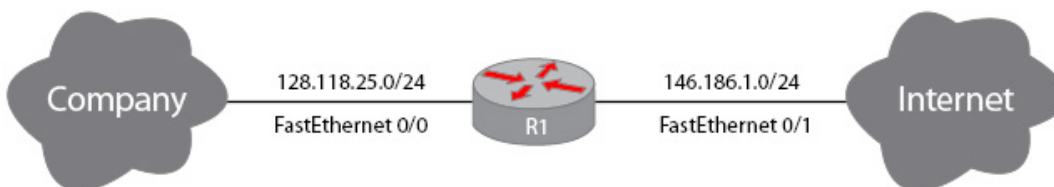
[Find the Answer](#) p. 90

Exhibit(s):

```

R1
access-list 100 deny ip 128.118.25.0 0.0.0.255 any
access-list 100 permit ip any any

interface fastethernet 0/0
ip access-group 100 in
  
```



Chapter 5

Implement secure network management and reporting

1. Which two of the following are Cisco recommendations when planning for secure management and reporting? Select the best 2 answers.
 - A. The selection of appropriate syslog logging levels.
 - B. Use the NTP protocol to keep time synchronized.
 - C. Keep all logging information contained within each individual device.
 - D. Use the LDAP protocol to log information back to a central management solution.

[Find the Answer](#) p. 91

2. Which two of the following are Cisco recommendations when planning for secure management and reporting? Select the best 2 answers.
 - A. Create a logging solution recommended by management.
 - B. Keep all logging levels set to their highest levels to retain the most information.
 - C. Keep all logging information in a central secure facility which can not be tampered with.
 - D. Develop a change management plan to deal with and document the changes being made to the network.

[Find the Answer](#) p. 91



3. What Cisco logging destination is used to record information internally on the device? Select the best answer.
- A. Buffered
 - B. Internal
 - C. Console
 - D. Device Monitor

[Find the Answer](#) p. 91

4. Referring to the exhibit, what is the logging level used for this message? Select the best answer.
- A. Warnings
 - B. Notifications
 - C. Informational
 - D. Debugging

[Find the Answer](#) p. 91

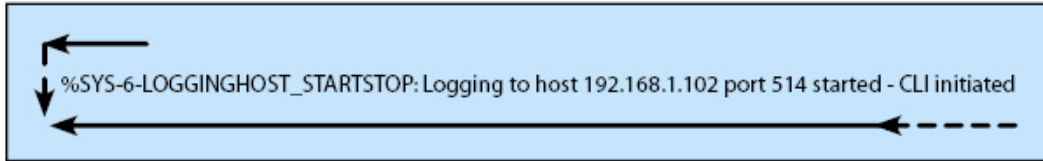
Exhibit(s):



5. Referring to the exhibit, what is the logging level used for this message? Select the best answer.
- A. Warnings
 - B. Notifications
 - C. Informational
 - D. Debugging

[Find the Answer](#) p. 91

Exhibit(s):

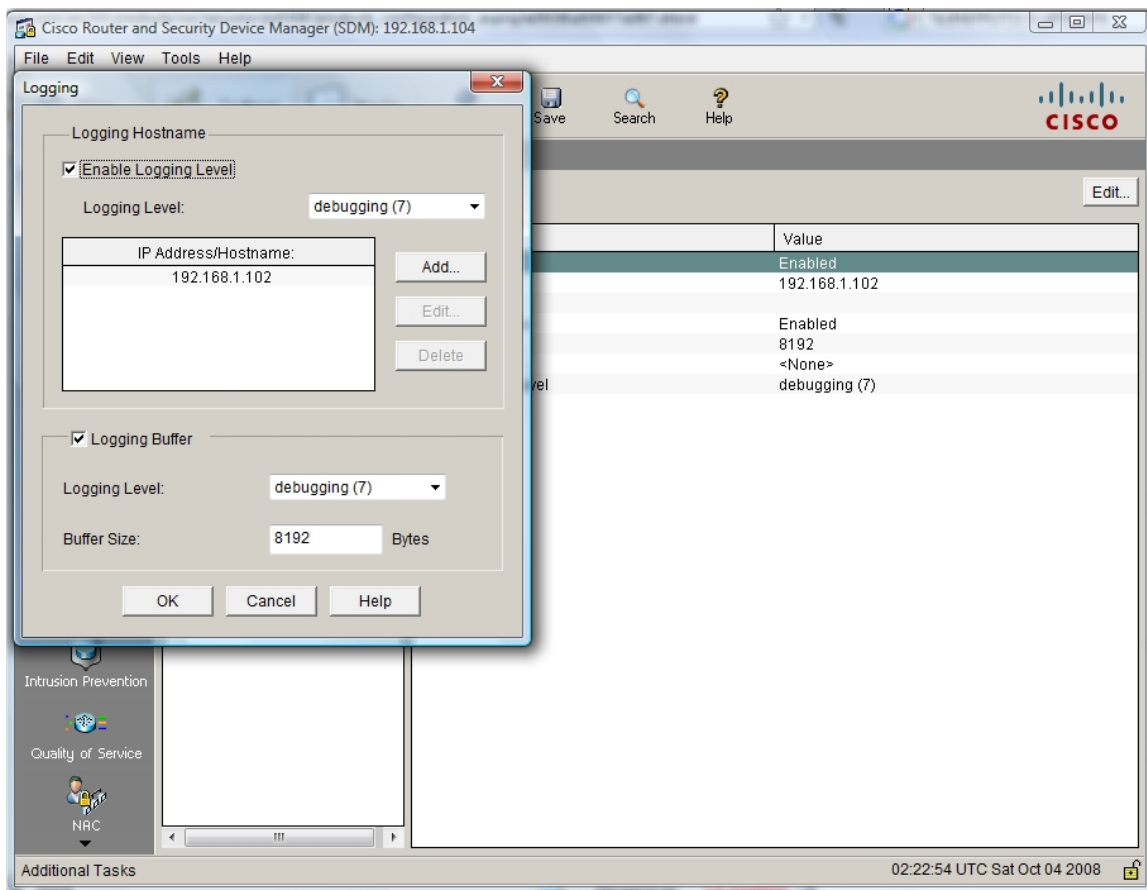


6. Referring to the Exhibit below, What is the process for getting to this point in SDM? Select the best answer.
- A. Configure Router Properties Logging Edit
 - B. Configure Additional Tasks Logging Edit
 - C. Configure Additional Tasks Router Properties Edit
 - D. Configure Additional Tasks Router Properties Logging Edit

[Find the Answer](#) p. 91

Exhibit(s):



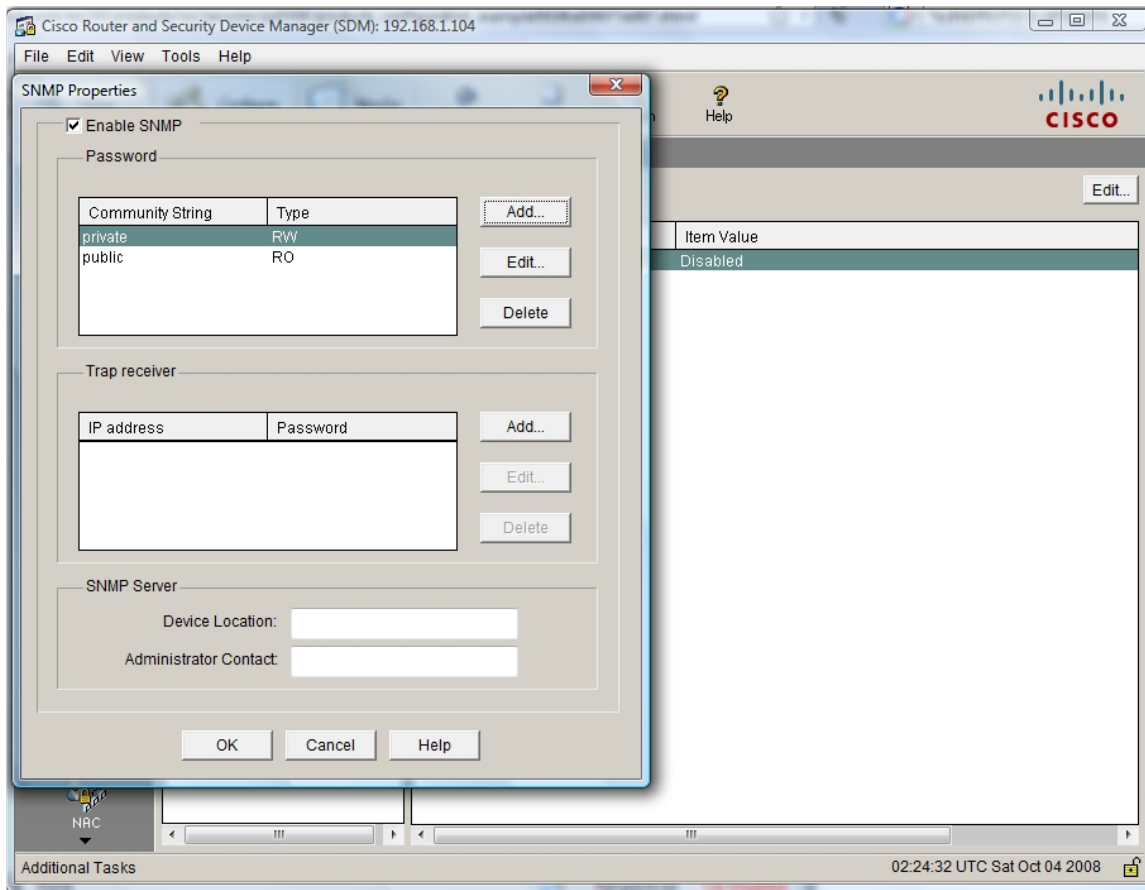


7. Referring to the Exhibit below, What is the process for getting to this point in SDM? Select the best answer.
- A. Configure
Additional Tasks
Router Properties
SNMP
Edit
 - B. Configure
SNMP
Edit
 - C. Configure
Additional Tasks
Router Properties
Edit
 - D. Configure
Additional Tasks
SNMP
Edit

[Find the Answer](#) p. 91

Exhibit(s):





8. What type of encryption is used by SNMPv3? Select the best answer.

- A. AES
- B. DES-56
- C. 3DES-56
- D. 3DES-64

[Find the Answer](#) p. 91



9. What is the minimum Cisco recommended modulus value for SSH? Select the best answer.
- A. 512 bits
 - B. 768 bits
 - C. 1024 bits
 - D. 2048 bits

[Find the Answer](#) p. 91

10. What versions of SNMP are supported on Cisco equipment? Select the best answer.
- A. Versions 1c, 2, and 3
 - B. Versions 1, 2, and 3
 - C. Versions 1, 2c, and 3c
 - D. Versions 1, 2c, and 3

[Find the Answer](#) p. 91

11. What version of IOS is required if you wanted to make sure support for SSH version 2 is included? Select the best answer.
- A. 12.3(4)T
 - B. 12.0
 - C. 12.2(4)T
 - D. 12.4(2)T

[Find the Answer](#) p. 91



12. What is the command which is used to set the number of SSH retries to 2? Select the best answer.
- A. router(config-line)ip ssh authentication-retries 2
 - B. router(config)ip ssh authentication-retries 2
 - C. router(config)ip ssh authentication retries 2
 - D. router(config)ssh authentication-retries 2

[Find the Answer](#) p. 91

13. What is the correct command to use to disable the use of telnet? Select the best answer.
- A. router(config)transport input ssh
 - B. router(config-line)transport ssh
 - C. router(config-line)transport input ssh
 - D. router(config-line)transport secure ssh

[Find the Answer](#) p. 91

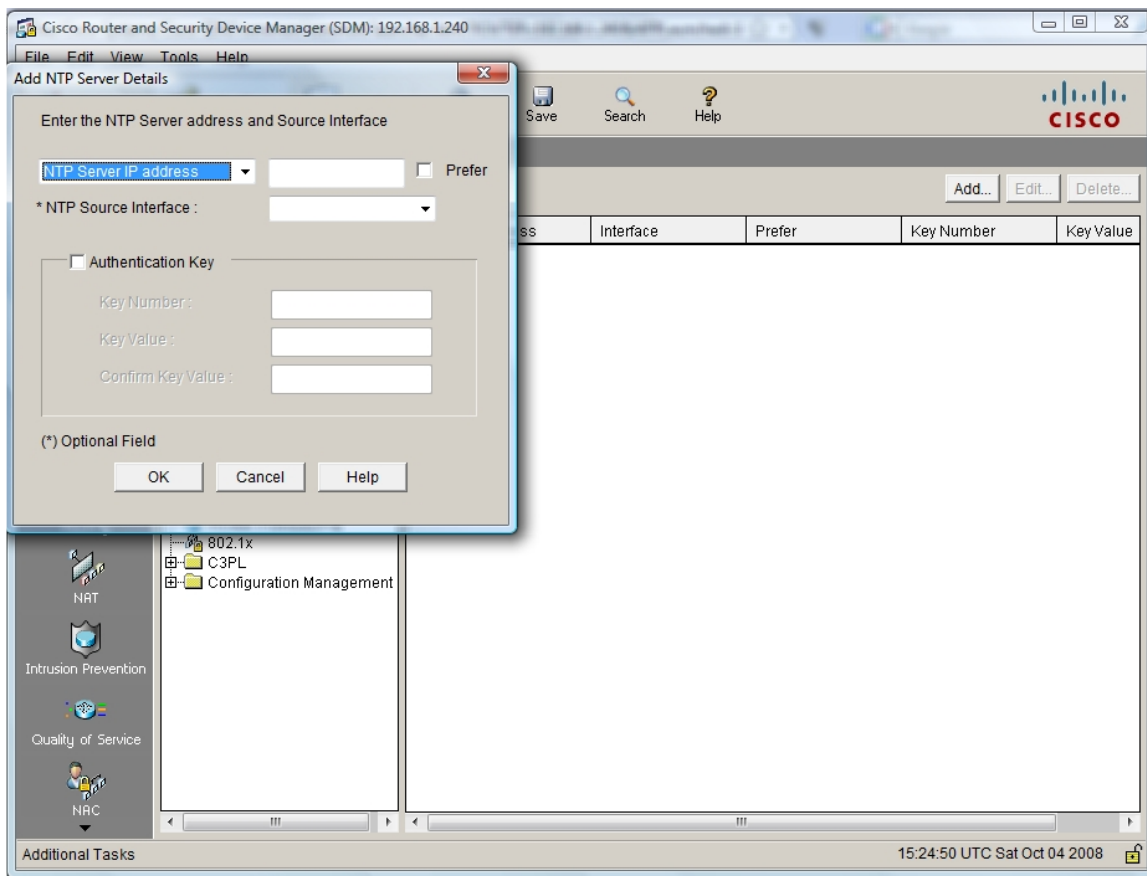


14. Referring to the Exhibit below, What is the process for getting to this point in SDM? Select the best answer.
- A. Configure
Additional Tasks
NTP/SNTP
Add
 - B. Configure
NTP/SNTP
Add
 - C. Configure
Additional Tasks
NTP/SNTP
Add
 - D. Configure
Additional Tasks
Router Properties
NTP/SNTP
Add

[Find the Answer](#) p. 91

Exhibit(s):





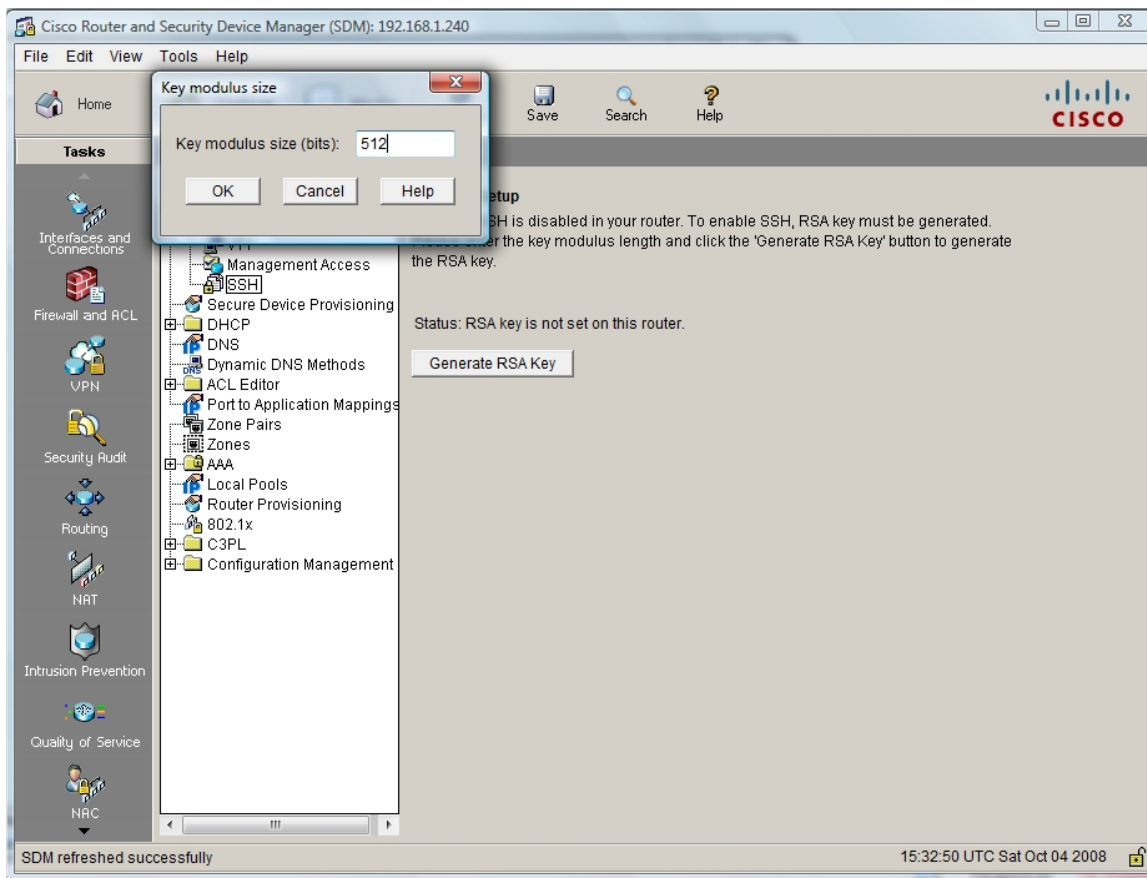
15. What is the process for getting to this point in SDM? Select the best answer.

- A. Configure
Additional Tasks
Router Access
SSH
Generate RSA Key
- B. Configure
Router Access
SSH
Generate RSA Key
- C. Configure
SSH
Generate RSA Key
- D. Configure
Additional Tasks
SSH
Generate RSA Key

[Find the Answer](#) p. 91

Exhibit(s):





Chapter 6

Mitigate common Layer 2 attacks

1. What does a switch do with a frame when it was just powered up? Select the best answer.
- A. Floods the frame out all ports.
 - B. Floods the frame out all ports, except received port.
 - C. Sends frame out the assigned port.
 - D. Sends frame out the port which is in the CAM table.

[Find the Answer](#) p. 92

2. What OSI layer relates to Layer 2? Select the best answer.
- A. Network
 - B. Transport
 - C. Data Link
 - D. Physical

[Find the Answer](#) p. 92

3. What version of SNMP would you use if you were primarily concerned with performance and ease of use? Select the best answer.
- A. version 3
 - B. version 2
 - C. version 1
 - D. version 2c

[Find the Answer](#) p. 92

4. Which two of the following are recommendations for securing VLAN's? Select the best 2 answers.
- A. Disable all non-trunk ports by configuring them with 'switchport mode access'.
 - B. Utilize private VLAN's.
 - C. Disable all non-trunk ports by configuring them with 'switchport trunk off'.
 - D. Utilize the 802.1Q native VLAN.

[Find the Answer](#) p. 92

5. Which one of the following describes the 802.1Q 'double tagging'? Select the best answer.
- A. 'double tagging' is when a frame is tagged once on ingress to a switch and then again on egress.
 - B. 'double tagging' is when a frame is tagged with both 802.1Q and 802.1P.
 - C. 'double tagging' happens when a frame is tagged twice one over the other.
 - D. 'double tagging' happens when a frame is tagged at one router then tagged again at another.

[Find the Answer](#) p. 92

6. What is the correct syntax to change the native VLAN to 200? Select the best answer.
- A. switch(config)#trunk native vlan 200
 - B. switch(config-if)#switchport trunk vlan 200
 - C. switch(config-if)#trunk native vlan 200
 - D. switch(config-if)#switchport trunk native vlan 200

[Find the Answer](#) p. 92



7. What feature is used to prevent a port from transitioning into a root port? Select the best answer.
- A. Root Guard
 - B. Portfast
 - C. Rootfast
 - D. BPDU Guard

[Find the Answer](#) p. 92

8. What feature is used to disable an access port if trunk traffic is received on it? Select the best answer.
- A. Root Guard
 - B. BPDU Guard
 - C. Rootfast
 - D. Portfast

[Find the Answer](#) p. 92

9. What command is used to enable the feature which disables a port if DHCP packets are received? Select the best answer.
- A. switch(config)#ip snooping dhcp
 - B. switch(config-if)#ip dhcp snooping
 - C. switch(config)#ip dhcp snooping
 - D. switch(config-if)#ip snooping dhcp

[Find the Answer](#) p. 92



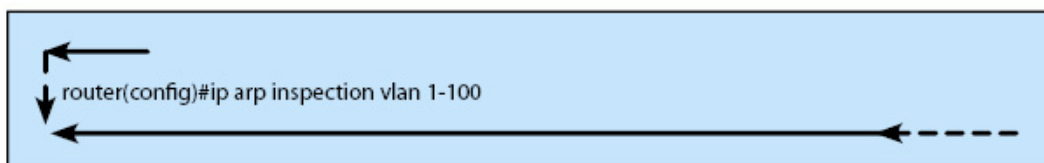
10. What command would be needed to trust a port for DHCP snooping? Select the best answer.
- A. Nothing, all ports are trusted by default.
 - B. `switch(config-if)#ip dhcp trust snooping`
 - C. `switch(config-if)#ip dhcp trust`
 - D. `switch(config-if)#ip dhcp snooping trust`

[Find the Answer](#) p. 92

11. Referring to the exhibit; you configure a brand new router with the configuration shown in the exhibit but notice that DAI is apparently not working correctly, why? Select the best answer.
- A. You must enable DHCP snooping.
 - B. You must add an additional command: `switch(config)#ip arp inspection on`
 - C. The format of this command is incorrect, the following must be entered: `switch(config)#ip arp inspection 1-100`
 - D. This command is correct but must be entered in interface configuration mode.

[Find the Answer](#) p. 92

Exhibit(s):



12. What is the behavior of a Cisco switch if the MAC address table is full? Select the best answer.
- A. The switch will send the frames to the associated switch port.
 - B. The switch will flood all frames out all interfaces.
 - C. The switch will drop all frames coming into the switch until it is rebooted.
 - D. The switch will drop all frames coming into the switch until the table is not full anymore.

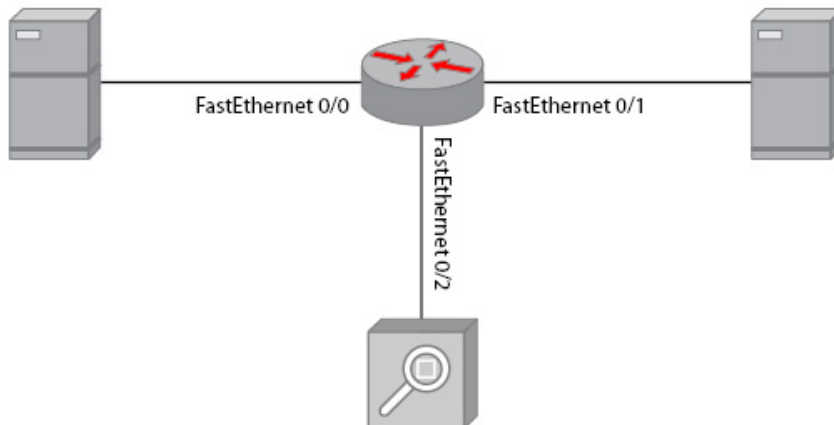
[Find the Answer](#) p. 92

13. Referring to the exhibit, you are trying to setup an Intrusion Detection System (IDS) and need to configure a SPAN port. What is the correct configuration to setup a SPAN port to listen to interface FastEthernet 0/2 and relay this traffic to interface FastEthernet 0/1? Select the best answer.
- A. `switch(config)#monitor session 1 source interface fastethernet 0/2 destination fastethernet 0/1`
 - B. `switch(config-if)#monitor session 1 source (interface fastethernet 0/1)`
`switch(config-if)#monitor session 1 destination (interface fastethernet 0/2)`
 - C. `switch(config)#monitor session 1 source interface fastethernet 0/1`
`switch(config)#monitor session 1 destination interface fastethernet 0/2`
 - D. `switch(config-if)#monitor session 1 source (interface fastethernet 0/2)`
`switch(config-if)#monitor session 1 destination (interface fastethernet 0/1)`

[Find the Answer](#) p. 92

Exhibit(s):





14. What type of VLAN is used with private VLAN's and allows all users to talk to each other in the same group but not to other groups? Select the best answer.
- A. Community VLAN
 - B. Group VLAN
 - C. Isolated VLAN
 - D. Comprehensive VLAN

[Find the Answer](#) p. 92

15. Which Cisco port security violation action is used to report when a violation occurs, and block all non-learned traffic? Select the best answer.
- A. Log
 - B. Restrict
 - C. Protect
 - D. Journal

[Find the Answer](#) p. 92



16. Which Cisco port security violation action is used to report when a violation occurs, and block all learned and non-learned traffic? Select the best answer.
- A. Restrict
 - B. Protect
 - C. Shutdown
 - D. Learned

[Find the Answer](#) p. 92

17. Of the classifications which Cisco uses for secure port MAC addresses, which one is used when you do not want to statically configure MAC-to-port assignments and you want the assignments to stay on reboot? Select the best answer.
- A. Dynamic Sticky Secure MAC Addresses
 - B. Dynamic Secure MAC Addresses
 - C. Static Secure MAC Addresses
 - D. Sticky Secure MAC Addresses

[Find the Answer](#) p. 92

18. Of the classifications which Cisco uses for secure port MAC addresses, which one is used when you do not want to statically configure MAC-to-port assignments and you do not want the assignments to be able to be kept on reboot? Select the best answer.
- A. Dynamic Secure MAC Addresses
 - B. Persistent Secure MAC Addresses
 - C. Sticky Secure MAC Addresses
 - D. Static Secure MAC Addresses

[Find the Answer](#) p. 92



19. What command would be used if you wanted to limit the number of learned MAC addresses per interface to 3? Select the best answer.
- A. switch(config-if)#switchport maximum 3
 - B. switch(config-if)#switchport port-security maximum 3
 - C. switch(config)#switchport port-security max 3
 - D. switch(config)#switchport port-security maximum 3

[Find the Answer](#) p. 92

20. What command would you use if you wanted to configure a port to use dynamic secure MAC addresses? Select the best answer.
- A. switch(config-if)#switchport port-security mac-address mac-address
 - B. switch(config-if)#switchport port-security mac-address sticky mac-address
 - C. No command needed.
 - D. switch(config-if)#switchport port-security mac-address sticky

[Find the Answer](#) p. 92

21. What command would you use to configure a ports violation behavior to shutdown the port? Select the best answer.
- A. switch(config-if)#switchport port-security violation shutdown
 - B. switch(config)#switchport port-security violation shutdown
 - C. switch(config-if)#switchport port-security violation protect
 - D. Nothing

[Find the Answer](#) p. 92



22. What command would you use to configure a RADIUS server to be used on a switch? Select the best answer.
- A. switch(config)#radius-server host [hostname | ip address]
 - B. switch(config)#radius-server server [hostname | ip address]
 - C. switch(config-server)#radius-server host [hostname | ip address]
 - D. switch(config)#aaa radius-server host [hostname | ip address]

[Find the Answer](#) p. 92

23. When configuring 802.1x port authentication what is the default behavior which is used? Select the best answer.
- A. Forced-Unauthorized
 - B. Forced-Authorized
 - C. Auto
 - D. Authorized

[Find the Answer](#) p. 92

24. What command would you use to configure VLAN 66 as the VLAN used for all restricted traffic classified by 802.1x? Select the best answer.
- A. switch(config)#dot1x auth-fail vlan 66
 - B. switch(config-if)#aaa dot1x auth-fail vlan 66
 - C. switch(config-if)#dot1x auth-fail vlan 66
 - D. switch(config)#aaa dot1x auth-fail vlan 66

[Find the Answer](#) p. 93



Chapter 7

Implement the Cisco IOS firewall feature set using SDM

1. What is the maximum number of interfaces which are supported on a transparent firewall? Select the best answer.
- A. three
 - B. four
 - C. five
 - D. two

[Find the Answer](#) p. 94

2. In transparent firewalls what layer of traffic is able to be filtered? Select the best answer.
- A. Layer 2 and 3
 - B. Layer 2,3 and 4
 - C. Layer 1, 2 and 3
 - D. Layer 1, 2, 3 and 4

[Find the Answer](#) p. 94

3. In application layer firewalls what layer of traffic is able to be filtered? Select the best answer.
- A. Layer 2, 3, 4 and 6
 - B. Layer 3, 4, 5 and 7
 - C. Layer 3, 4, 5 and 6
 - D. Layer 2, 3, 4, 5 and 7

[Find the Answer](#) p. 94



4. Which of the following are considered to be advantages for application layer firewalls? Select the best 2 answers.
- A. Requires a minimal amount of processor power.
 - B. Has the ability to monitor all services through a single application.
 - C. Can monitor or filter application data.
 - D. Can provide detailed log information.

[Find the Answer](#) p. 94

5. When referring to a static stateless firewall, at what layer is all unknown traffic allowed before it is filtered? Select the best answer.
- A. Layer 3
 - B. Layer 2
 - C. Layer 4
 - D. Layer 6

[Find the Answer](#) p. 94

6. On which ports does a stateful firewall operate? Select the best answer.
- A. Layer 2, 3, and 4
 - B. Layer 3, 4 and 5
 - C. Layer 3, 4, and 6
 - D. Layer 2, 3, 4 and 6

[Find the Answer](#) p. 94



7. What parts of the IP packet are monitored in order to keep track of state information? Select the best answer.
- A. UDP Port
 - B. RTP
 - C. RST
 - D. MAC

[Find the Answer](#) p. 94

8. Which of the following are used in order to track the state of a connection? Select the best answer(s).
- A. UDP Port
 - B. TCP Sequence Numbers
 - C. SIP Information
 - D. Destination Address

[Find the Answer](#) p. 94

9. Of the following options which are considered uses for a stateful packet filtering firewall? Select the best two answers.
- A. A primary means for defense
 - B. A secondary means for defense
 - C. To improve routing performance
 - D. To have more stringent controls

[Find the Answer](#) p. 94



10. Of the following, what are considered to be limitations of stateful firewalls? Select the best answers.
- A. Not all protocols are stateless.
 - B. No ability to prevent application layer attacks.
 - C. Lack of Layer 3 support.
 - D. Problems tracking protocols which use multiple connections.

[Find the Answer](#) p. 94

11. Of the firewall technologies, which have the ability to prevent state based attacks? Select the best answer(s).
- A. Stateful Firewalls
 - B. Application Layer Firewalls
 - C. Application Inspection Firewalls
 - D. Static Firewalls

[Find the Answer](#) p. 94

12. Of the firewall technologies, which have the ability to control attacks from java and flash type plugins? Select the best answer.
- A. Stateful Firewall
 - B. Application Inspection Firewall
 - C. Transparent Firewalls
 - D. Static Firewalls

[Find the Answer](#) p. 94



13. Which of the following are considered to be weaknesses of application inspection firewalls? Select the best answer.
- A. Not aware of layer 5 states.
 - B. Only provides layer 7 protection.
 - C. Does not support user authentication.
 - D. Does not have the ability to check layer 5 conformity.

[Find the Answer](#) p. 94

14. Of the following, which are considered to be uses for application inspection firewalls? Select the best answer.
- A. A primary means of defense.
 - B. Improve routing performance.
 - C. Defense against DoS attacks.
 - D. Most stringent control over security.

[Find the Answer](#) p. 94

15. Of the following, which is NOT considered a best practice for creating a firewall practice? Select the best answer.
- A. Use a server as a firewall.
 - B. Segment security zones.
 - C. Combine firewall technologies.
 - D. Only allow needed protocols.

[Find the Answer](#) p. 94



16. What is the name of the Cisco technology which is currently used for stateful packet inspection? Select the best answer.
- A. CBAC
 - B. SPI
 - C. ACL
 - D. GPI

[Find the Answer](#) p. 94

17. In what IOS version was Stateful Packet Inspection (SPI) introduced? Select the best answer.
- A. 12.4(4)T
 - B. 12.4(6)T
 - C. 12.3(4)T
 - D. 12.3(6)T

[Find the Answer](#) p. 94

18. In what IOS version was zone based firewall features introduced? Select the best answer.
- A. 12.4(4)T
 - B. 12.3(6)T
 - C. 12.3(4)T
 - D. 12.4(6)T

[Find the Answer](#) p. 94



19. When setting up zone based firewalls what is the number of zones a single interface can be in at the same time? Select the best answer.
- A. 1
 - B. 2
 - C. 3
 - D. 6

[Find the Answer](#) p. 94

20. You are trying to setup an interface into the 'public' zone by using the 'zone-member security public' command but keep getting the '% Security zone name public not defined' message, why? Select the best answer.
- A. The 'security zone public' command was not configured yet.
 - B. The 'zone security public' command was not configured yet.
 - C. The 'zone-member' command syntax was incorrect
 - D. The 'zone-member security public' command was not configured yet.

[Find the Answer](#) p. 94

21. You are setting up a zone based firewall on a new router in your network and have configured an interface into a zone. You notice that no traffic is going in or out of the interface anymore, why? Select the best answer.
- A. You have configured the interface into an incorrect zone.
 - B. Your zones are not configured correctly.
 - C. No other interfaces are configured in this zone and the default behavior is to block all traffic from outside the zone.
 - D. Another firewall technology is configured blocking this traffic.

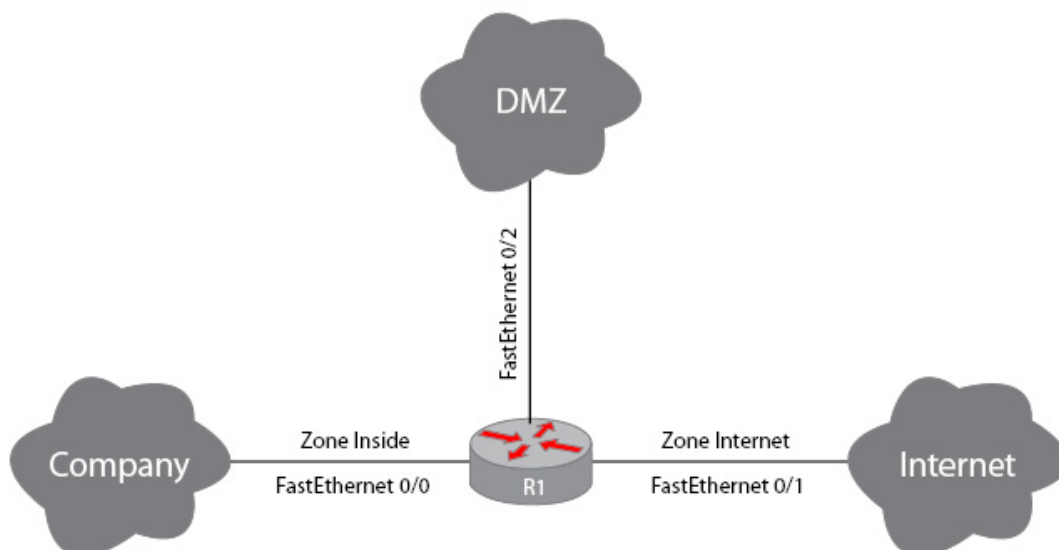
[Find the Answer](#) p. 94



22. Referring to the exhibit, you are trying to configure a policy between your DMZ network and the Internet. When configuring a policy you find it impossible to apply a policy to perform this task, why? Select the best answer.
- A. Your zones were setup incorrectly.
 - B. A class must be setup first.
 - C. A parameter map must be setup first.
 - D. It is not possible for traffic to flow between an interface in a zone and an interface not in a zone.

[Find the Answer](#) p. 94

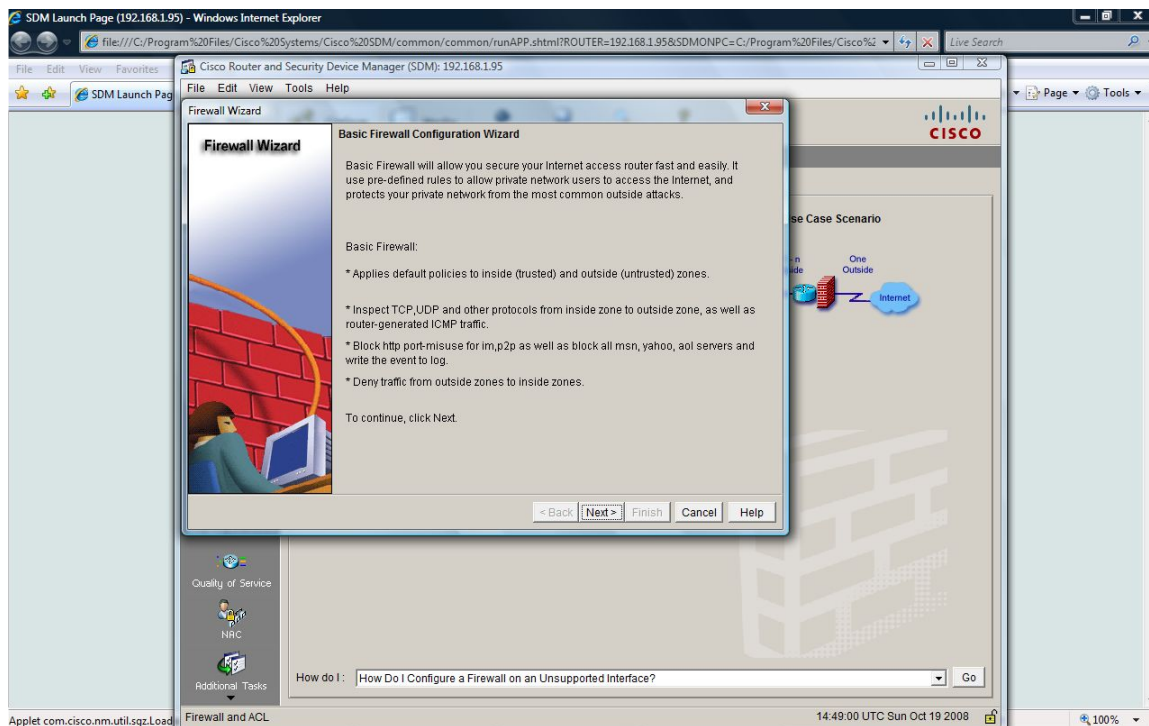
Exhibit(s):



23. Referring to the Exhibit, what are the steps which are required to get into this screen? Select the best answer.
- A. Configure Firewall and ACL
Basic Firewall
Launch the selected task
 - B. Configure Firewall and ACL
Basic Firewall
 - C. Firewall and ACL
Basic Firewall
Launch the selected task
 - D. Configure Firewall and ACL
Advanced Firewall
Launch the selected task

[Find the Answer](#) p. 94

Exhibit(s):

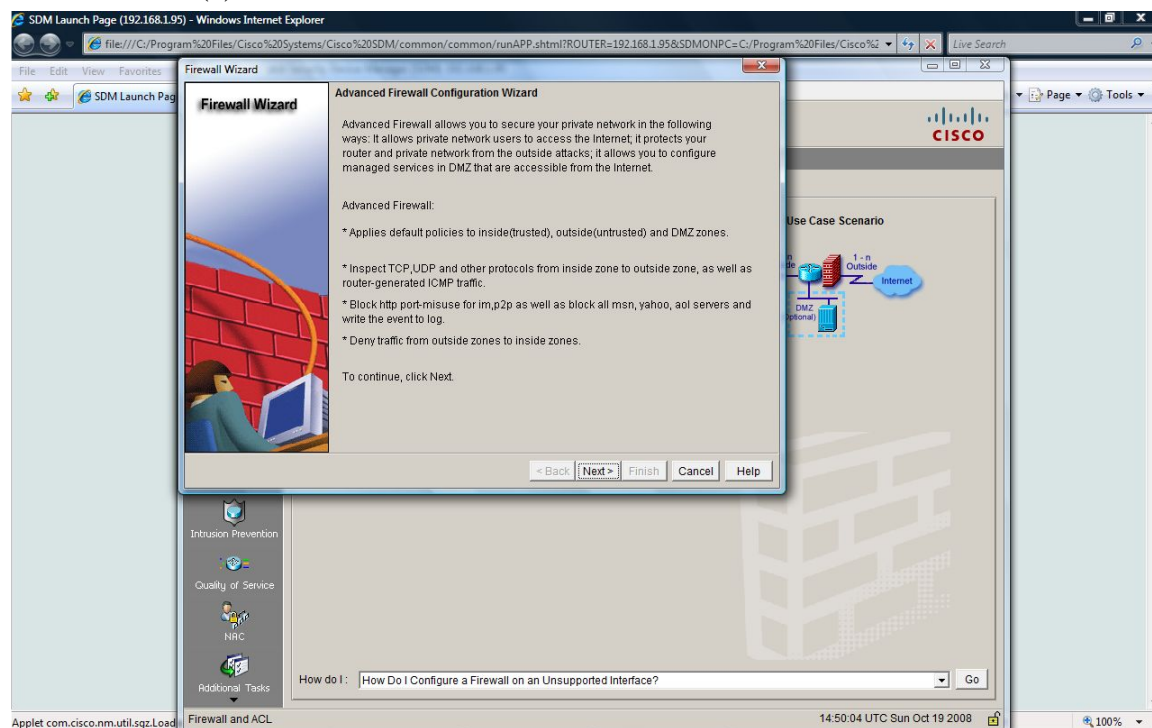


24. Referring to the Exhibit, what are the steps which are required to get into this screen? Select the best answer.

- A. Configure Firewall and ACL
Basic Firewall
Launch the selected task
- B. Configure Firewall and ACL
Basic Firewall
- C. Firewall and ACL
Basic Firewall
Launch the selected task
- D. Configure Firewall and ACL
Advanced Firewall
Launch the selected task

[Find the Answer](#) p. 95

Exhibit(s):

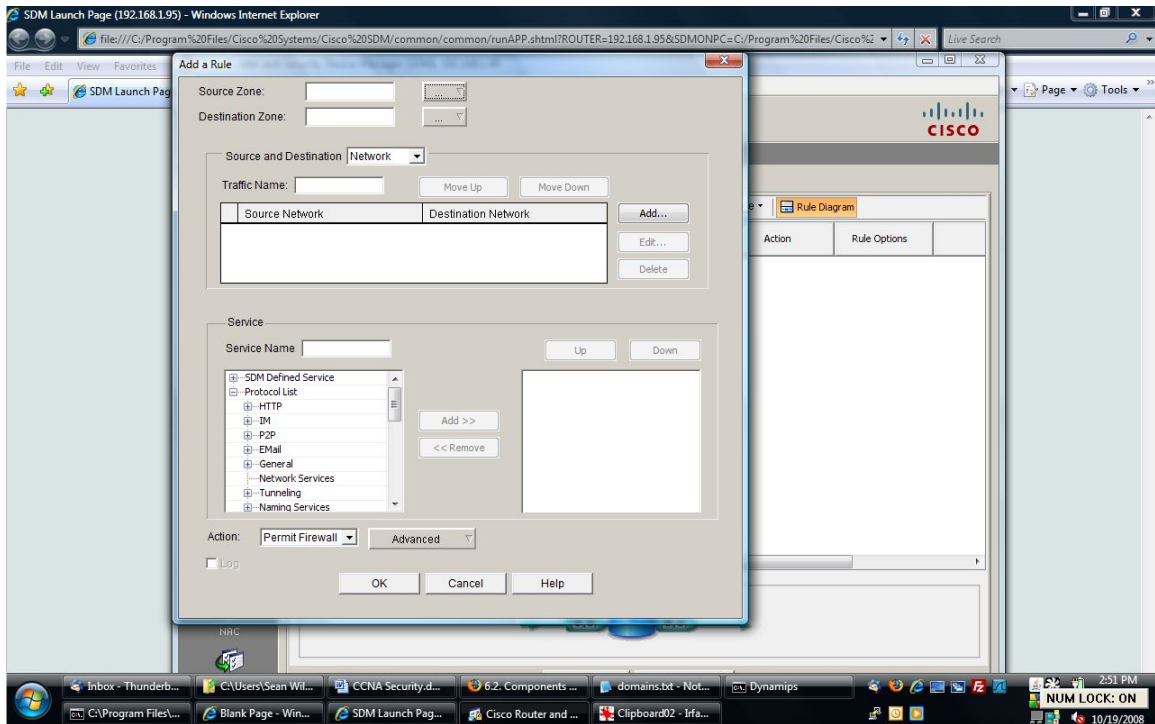


25. Referring to the Exhibit, what are the steps which are required to get into this screen? Select the best answer.
- A. Configure Firewall and ACL
Add New Zone Policy
 - B. Configure Firewall and ACL
Edit Firewall Policy
Add New Zone Policy
 - C. Configure Edit Firewall Policy
Add New Zone Policy
 - D. Configure Firewall and ACL
Advanced Firewall
Edit Firewall Policy
Add New Zone Policy

[Find the Answer](#) p. 95

Exhibit(s):



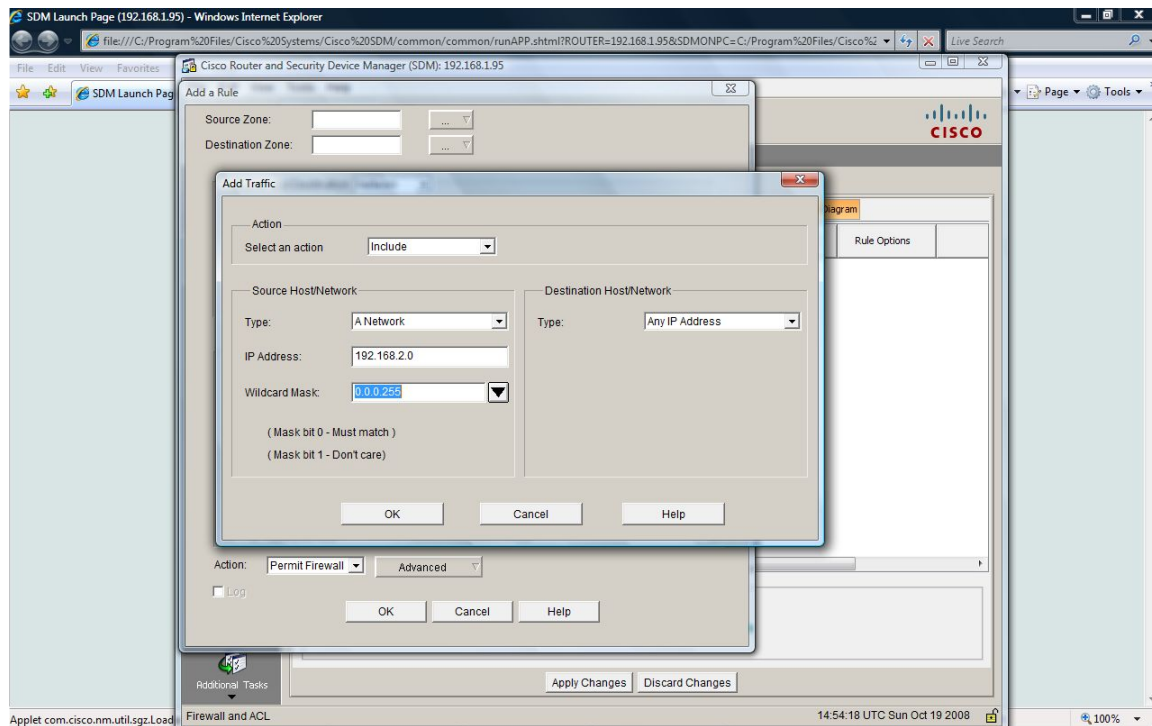


26. Referring to the Exhibit, what are the steps which are required to get into this screen? Select the best answer.
- A. Configure Firewall and ACL
Add New Zone Policy
 - B. Configure Firewall and ACL
Edit Firewall Policy
Add New Zone Policy
 - C. Configure Firewall and ACL
Edit Firewall Policy
Add New Zone Policy
Add
 - D. Configure Firewall and ACL
Basic Firewall
Edit Firewall Policy
Add New Zone Policy

[Find the Answer](#) p. 95

Exhibit(s):





Chapter 8

Implement the Cisco IOS IPS feature set using SDM

1. Which of the follow is NOT a detection method for IPS?Select the best answer.

- A. Honey Pot
- B. Signature-Based
- C. Anomaly-Based
- D. Heuristic-Based

[Find the Answer](#) p. 96

2. Which of the following IPS/IDS detection methods is used as a lure to attackers so they will waste time attacking an artificial target?Select the best answer.

- A. Honey Pot
- B. Signature-Based
- C. Anomaly-Based
- D. Policy-Based

[Find the Answer](#) p. 96

3. Of the following detection methods, which is considered the primary method used for IPS/IDS technologies?Select the best answer.

- A. Honey Pot
- B. Signature-Based
- C. Anomaly-Based
- D. Policy-Based

[Find the Answer](#) p. 96



4. Which of the following IPS/IDS detection methods creates a baseline condition on a network over a period of time and creates alarms based on the traffic differing from this created baseline? Select the best answer.
- A. Honey Pot
 - B. Signature-Based
 - C. Anomaly-Based
 - D. Policy-Based

[Find the Answer](#) p. 96

5. When dealing with Cisco equipment what type of IPS does the Cisco Security Agent (CSA) provide? Select the best answer.
- A. NIPS
 - B. DMZ
 - C. NIDS
 - D. HIPS

[Find the Answer](#) p. 96

6. What is the fundamental difference between an IPS and IDS? Select the best answer.
- A. AN IPS is able to pro-actively protect you while an IDS does not.
 - B. An IDS is used to detect intrusions and the IPS are used to protect from those detected intrusions.
 - C. An IDS is able to pro-actively protect you while an IPS does not.
 - D. An IPS is used to detect intrusions and the IDS are used to protect from those detected intrusions.

[Find the Answer](#) p. 96



7. What solution would be best if a large amount of your network traffic was encrypted and you were concerned with encrypted malicious traffic? Select the best answer.
- A. NIDS
 - B. HIPS
 - C. IPSD
 - D. NIPS

[Find the Answer](#) p. 96

8. What are the two types of interfaces which are located on a network sensor? Select the best two answers.
- A. Ethernet Interface
 - B. Loopback Interface
 - C. Command and Control Interface
 - D. Monitoring Interface

[Find the Answer](#) p. 96

9. What type of sensor operating mode requires the use of more than one monitoring interface? Select the best answer.
- A. Inline Mode
 - B. Promiscuous Mode
 - C. Unrestricted Mode
 - D. Dual-Homed Mode

[Find the Answer](#) p. 96



10. What type of sensor operating mode only requires the use of one port? Select the best answer.
- A. Inline Mode
 - B. Promiscuous Mode
 - C. Restricted Mode
 - D. Single-Homed Mode

[Find the Answer](#) p. 96

11. What type of signature uses a set of rules to recognize how certain protocols should behave? Select the best answer.
- A. Exploit Signatures
 - B. String Signatures
 - C. Connection Signatures
 - D. DoS Signatures

[Find the Answer](#) p. 96

12. What type of signature looks for signs of extraordinary resource consumption and flags this behavior? Select the best answer.
- A. Exploit Signatures
 - B. String Signatures
 - C. Connection Signatures
 - D. DoS Signatures

[Find the Answer](#) p. 96



13. What is the preferred security method to log information between IPS clients and servers? Select the best answer.
- A. SDEE
 - B. syslog
 - C. SNMP
 - D. SMTP

[Find the Answer](#) p. 96

14. What is the name of the file which contains threat signatures? Select the best answer.
- A. Cisco Signature File (CSF)
 - B. Signature Definition File (SDF)
 - C. Universal Signature Definition File (USDF)
 - D. Security Definition File (SDF)

[Find the Answer](#) p. 96

15. When a IPS signature triggers an alarm there are a number of different responses which can be used, which of the following is NOT one of these options? Select the best answer.
- A. Reset the TCP Connection
 - B. Create a log entry
 - C. Block the attackers UDP port
 - D. Block the attackers IP Address

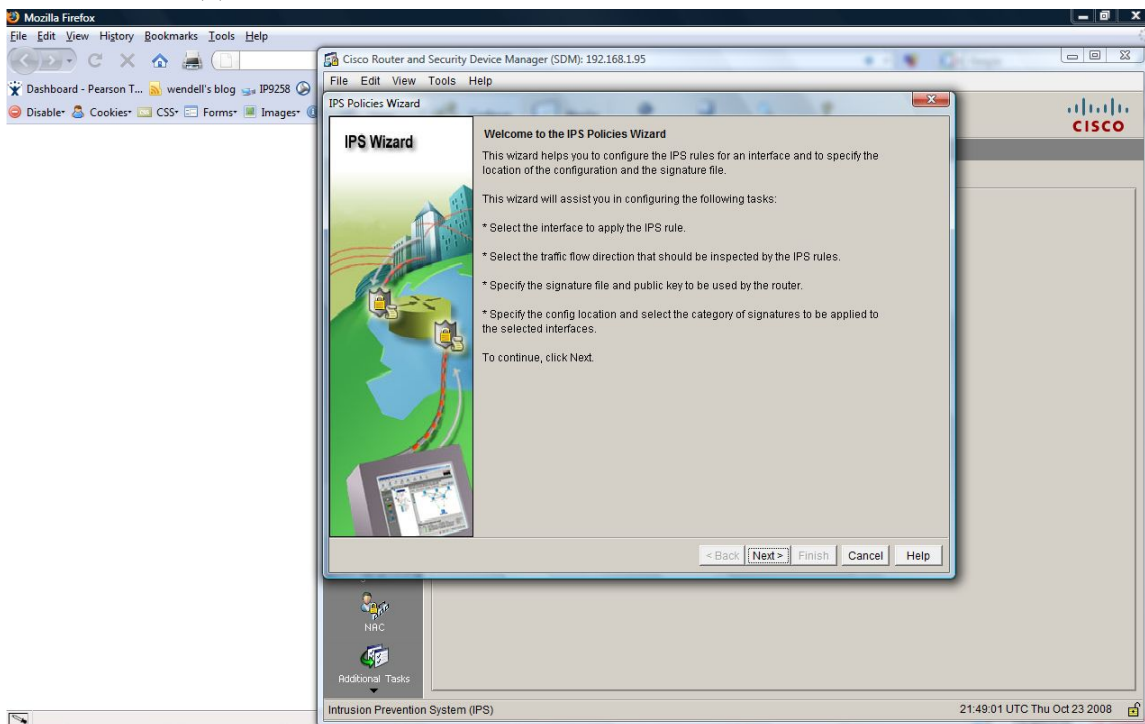
[Find the Answer](#) p. 96



16. Referring to the exhibit, what are the steps that need to be followed to reach this screen? Select the best answer.
- A. Intrusion Protection
Launch IPS Rule Wizard
 - B. Configure
Additional Tasks
Intrusion Protection
Launch IPS Rule Wizard
 - C. Configure
Intrusion Protection
Edit IPS
Launch IPS Rule Wizard
 - D. Configure
Intrusion Protection
Launch IPS Rule Wizard

[Find the Answer](#) p. 96

Exhibit(s):

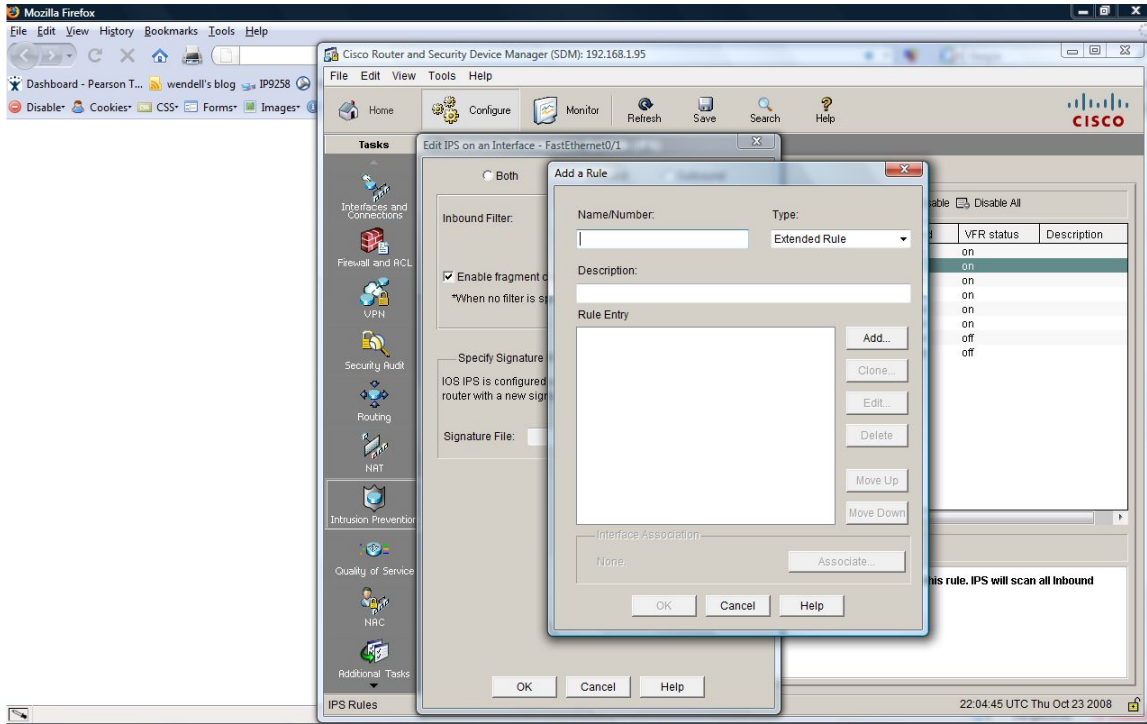


17. Referring to the exhibit, what are the steps that need to be followed to reach this screen? Select the best answer.
- A. Configure
Intrusion Protection
Edit IPS
Edit
Select '...'
Create a new rule (ACL) and select...
 - B. Configure
Intrusion Protection
Edit IPS
Select '...'
Create a new rule (ACL) and select...
 - C. Intrusion Protection
Edit IPS
Edit
Select '...'
Create a new rule (ACL) and select...
 - D. Configure
Intrusion Protection
Edit IPS
Edit
Create a new rule (ACL) and select...

[Find the Answer](#) p. 96

Exhibit(s):



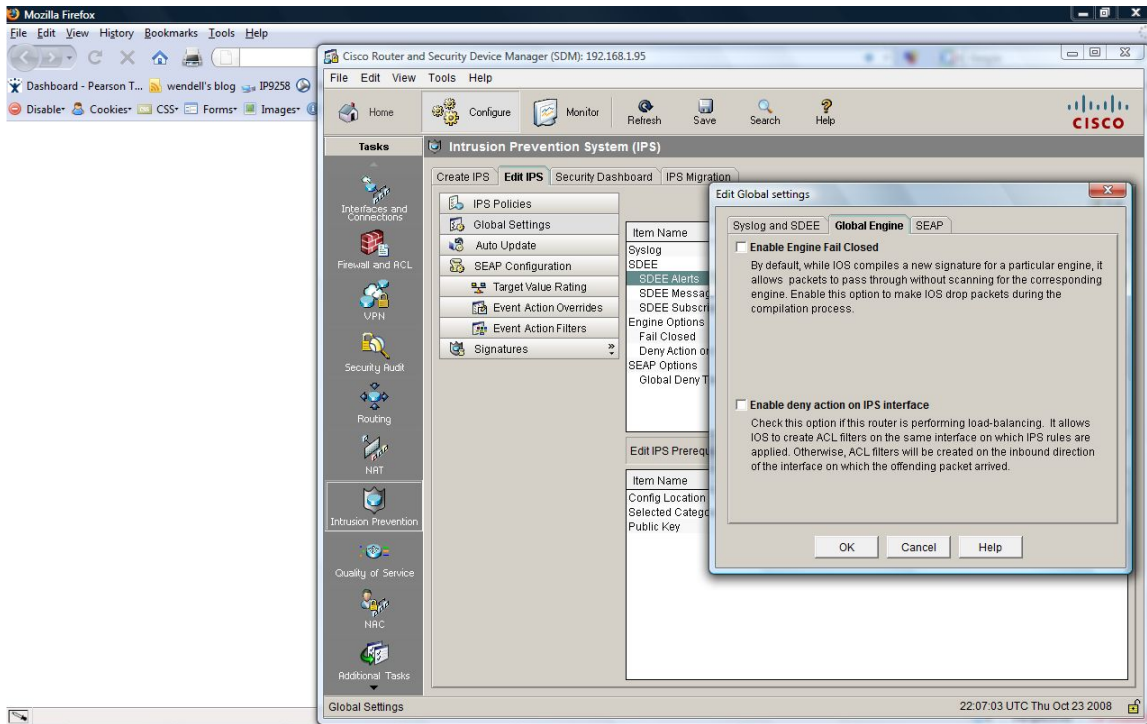


18. Referring to the exhibit, what are the steps that need to be followed to reach this screen? Select the best answer.
- A. Configure
Intrusion Protection
Edit IPS
SEAP Configuration
Global Engine
 - B. Configure
Intrusion Protection
Edit IPS
SEAP Configuration
Edit
Global Engine
 - C. Configure
Intrusion Protection
SEAP Configuration
Edit
Global Engine
 - D. Configure
Intrusion Protection
Edit IPS
Edit
Global Engine

[Find the Answer](#) p. 96

Exhibit(s):



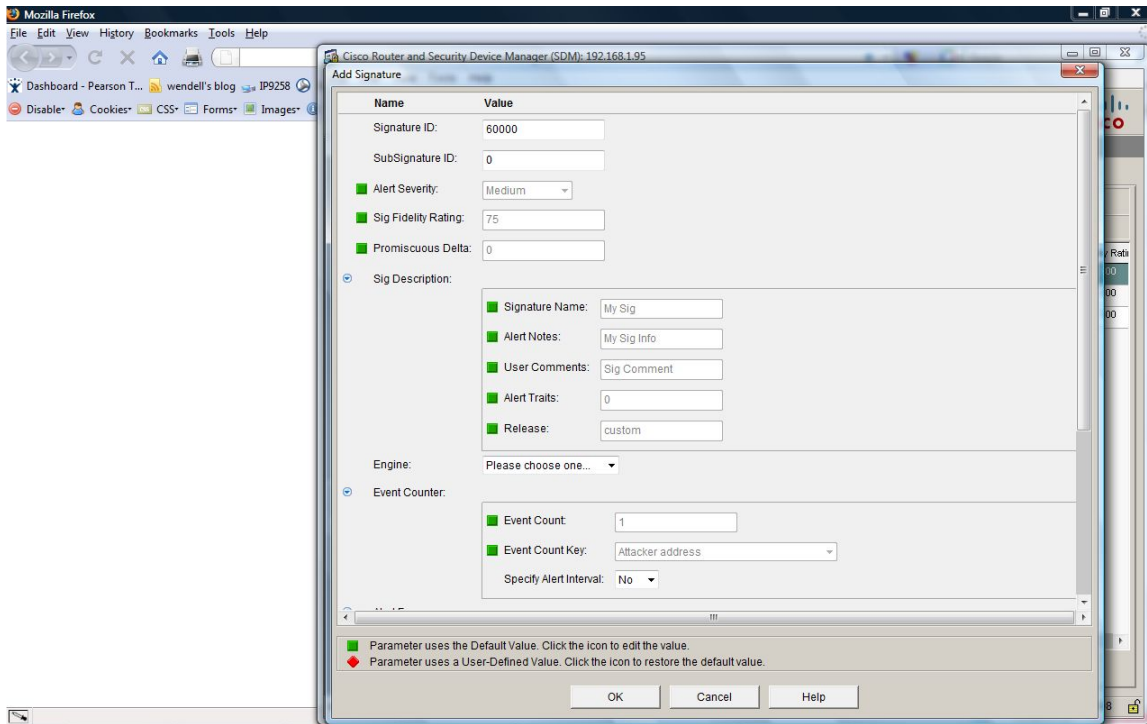


19. Referring to the exhibit, what are the steps that need to be followed to reach this screen? Select the best answer.
- A. Configure
Intrusion Prevention
Signatures
Add New
 - B. Configure
Intrusion Prevention
Edit IPS
Signatures
Add
 - C. Configure
Intrusion Prevention
Edit IPS
Signatures
Add
Add New
 - D. Configure
Intrusion Prevention
Edit IPS
Signatures
Add New

[Find the Answer](#) p. 96

Exhibit(s):





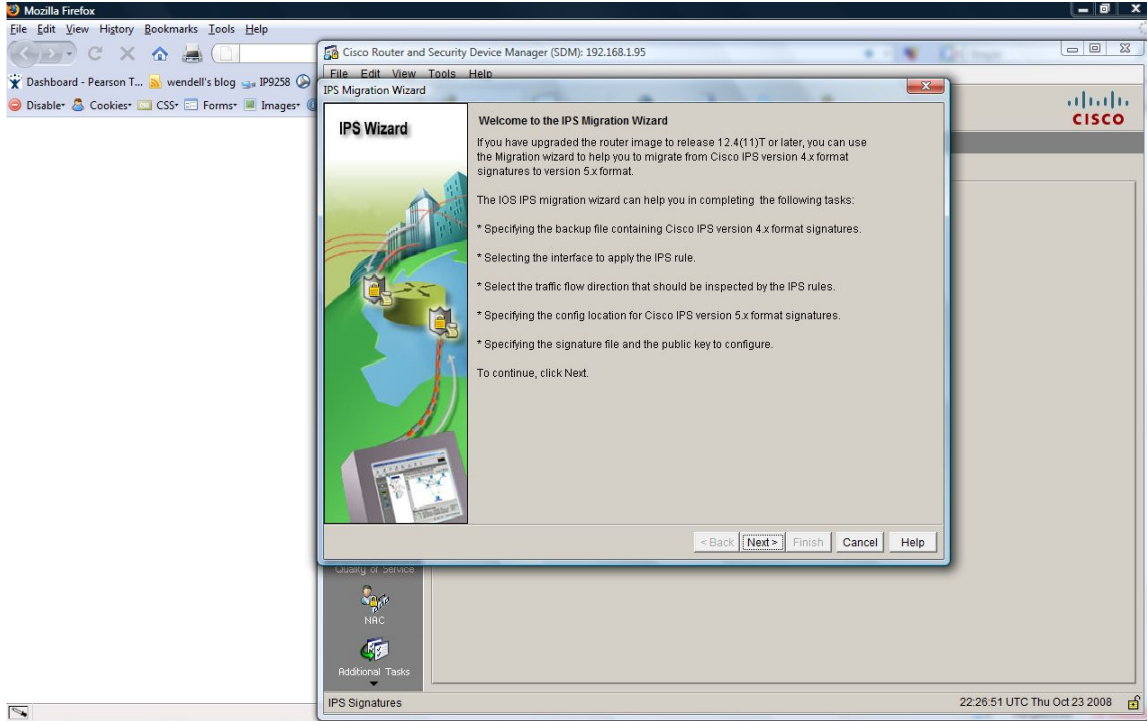
20. Referring to the exhibit, what are the steps that need to be followed to reach this screen? Select the best answer.

- A. Configure
Intrusion Prevention
IPS Migration
Add
Launch IPS Migration Wizard
- B. Configure
IPS Migration
Launch IPS Migration Wizard
- C. Intrusion Prevention
IPS Migration
Launch IPS Migration Wizard
- D. Configure
Intrusion Prevention
IPS Migration
Launch IPS Migration Wizard

[Find the Answer](#) p. 96



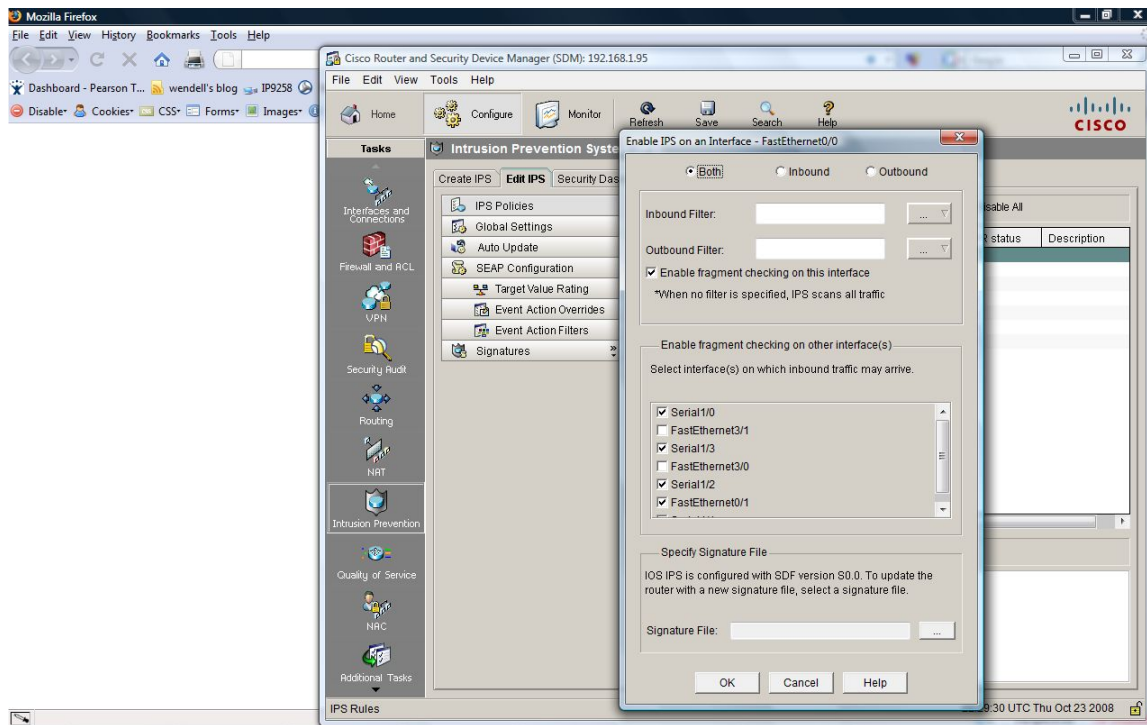
Exhibit(s):



21. Referring to the exhibit, what are the steps that need to be followed to reach this screen? Select the best answer.
- A. Configure
Intrusion Prevention
Edit IPS
Enable
 - B. Configure
Intrusion Prevention
Enable IPS
 - C. Configure
Intrusion Prevention
Edit IPS
Enable IPS
 - D. Configure
Intrusion Protection
Edit IPS
Enable

[Find the Answer](#) p. 96

Exhibit(s):

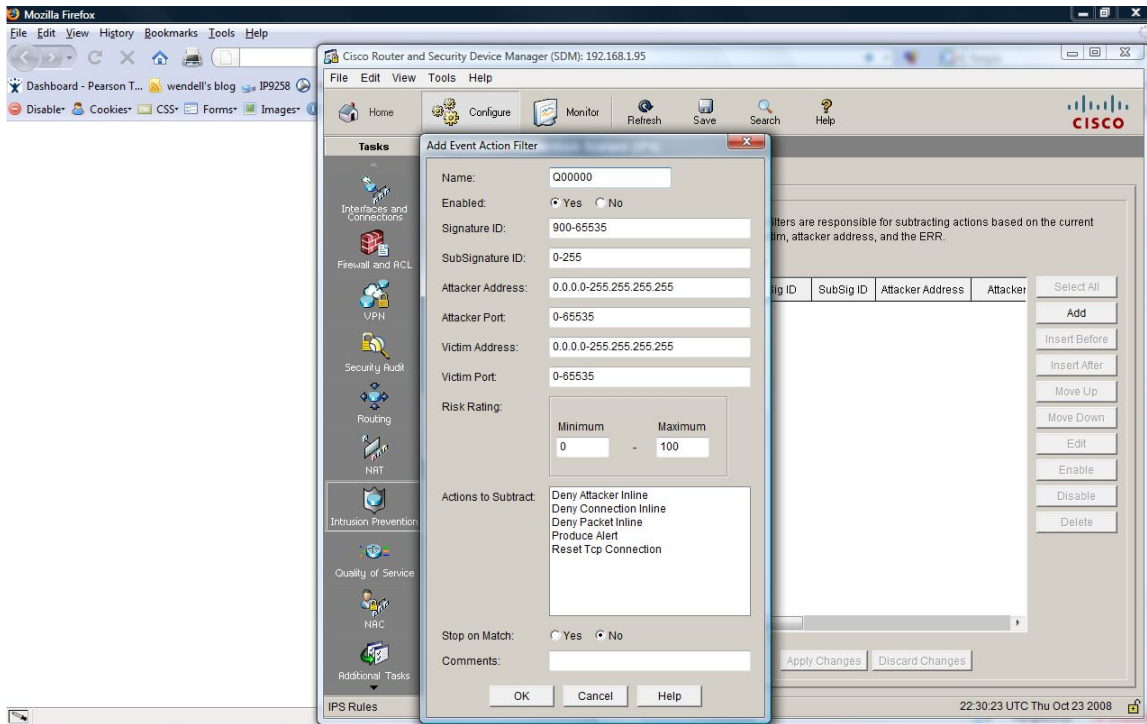


22. Referring to the exhibit, what are the steps that need to be followed to reach this screen? Select the best answer.
- A. Configure
Intrusion Prevention Configure
Intrusion Prevention
Edit IPS
Event Action Filters
Add
Event Action Filters
Add
 - B. Configure
Intrusion Prevention
Edit IPS
Event Action Overrides
Add
 - C. Configure
Intrusion Prevention
Event Action Filters
Add
 - D. Intrusion Prevention
Edit IPS
Event Action Filters
Add

[Find the Answer](#) p. 96

Exhibit(s):



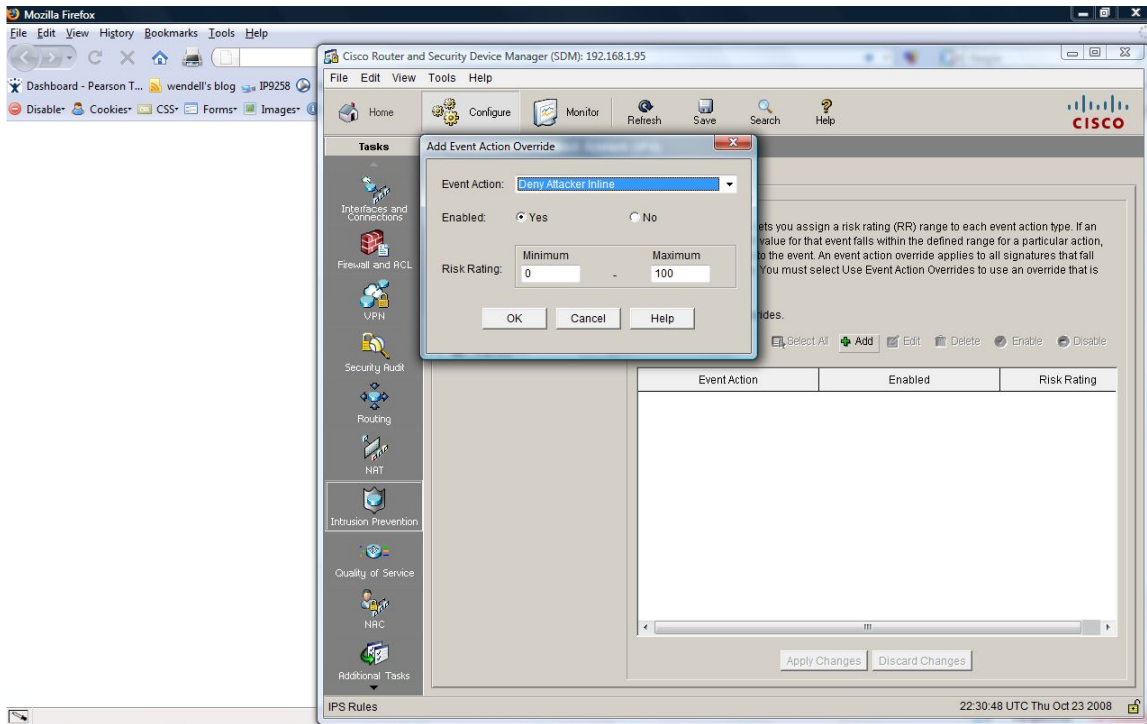


23. Referring to the exhibit, what are the steps that need to be followed to reach this screen? Select the best answer.
- A. Configure
Intrusion Prevention
Edit IPS
Event Action Filters
Add
 - B. Intrusion Prevention
Edit IPS
Event Action Overrides
Add
 - C. Configure
Intrusion Prevention
Edit IPS
Event Action Overrides
Add
 - D. Configure
Intrusion Prevention
Event Action Overrides
Add

[Find the Answer](#) p. 96

Exhibit(s):





Chapter 9

Implement site-to-site VPNs on Cisco Routers using SDM

1. Of the different types of encryption classes which type employs two separate keys? Select the best answer.
 - A. Symmetric encryption
 - B. Geometric encryption
 - C. Multi-Key Encryption
 - D. Asymmetric encryption

[Find the Answer](#) p. 97

2. Which symmetric encryption algorithm offers the key sizes 112-bit and 156-bit? Select the best answer.
 - A. 3DES
 - B. AES
 - C. DES
 - D. MD5

[Find the Answer](#) p. 97

3. Which of the following is NOT considered a difference between Block ciphers and Stream ciphers? Select the best answer.
 - A. Block ciphers use fixed-length sized encryption sections.
 - B. Block ciphers are more efficient.
 - C. Stream ciphers are generally faster.
 - D. Block cipher output is larger than stream ciphers.

[Find the Answer](#) p. 97



4. Of the following which is considered a common stream cipher mode? Select the best answer.
- A. Electronic Code Book (ECB)
 - B. Output Stream Feedback (OSF)
 - C. Cipher Feedback (CFB)
 - D. Cipher Block Chaining (CBC)

[Find the Answer](#) p. 97

5. Of the following which is considered a common block cipher mode? Select the best answer.
- A. Cipher Feedback (CFB)
 - B. Electronic Block Book (EBB)
 - C. Output Feedback (OFB)
 - D. Electronic Code Book (ECB)

[Find the Answer](#) p. 97

6. Which of the following is not considered to be a recommendation when securing data with the DES algorithm? Select the best answer.
- A. Use ECB mode
 - B. Change Keys Frequently
 - C. Use CBC Mode
 - D. Use secure channel to communicate keys

[Find the Answer](#) p. 97



7. In what IOS version was AES introduced? Select the best answer.

- A. 12.3(13)T
- B. 12.2(13)T
- C. 12.2(2)T
- D. 12.3(2)T

[Find the Answer](#) p. 97

8. Of the following algorithms which is one of the three algorithms used to make up a digital signature? Select the best answer.

- A. Rijndael Algorithm
- B. Signature generation algorithm
- C. Signature verification algorithm
- D. Key verification algorithm

[Find the Answer](#) p. 97

9. Of the following encryption types which is used in symmetric encryption? Select the best answer.

- A. Diffie-Hellman
- B. DSA
- C. ECC
- D. DES

[Find the Answer](#) p. 97



10. Of the following encryption types which is used in asymmetric encryption? Select the best answer.
- A. Diffie-Hellman
 - B. AES
 - C. Blowfish
 - D. DES

[Find the Answer](#) p. 97

11. Of the following which is NOT considered to be a use of a X.509 certificate? Select the best answer.
- A. Website Authentication
 - B. Wireless Security
 - C. IPSec VPN's
 - D. Client Certificates

[Find the Answer](#) p. 97

12. Which of the following is not considered to be a caveat of PKI? Select the best answer.
- A. User Private Key Stolen.
 - B. Server Private Key Stolen.
 - C. Client Public Key Stolen.
 - D. Certificate Authority (CA) Compromised.

[Find the Answer](#) p. 97



13. Of the different types of protections that IPSec provides which one verifies that each party is who they say they are? Select the best answer.
- A. Confidentially
 - B. Verification
 - C. Integrity
 - D. Authentication

[Find the Answer](#) p. 97

14. Of the different types of protections that IPSec provides which one verifies that the data has not been modified in transit? Select the best answer.
- A. Integrity
 - B. Verification
 - C. Confidentiality
 - D. Authentication

[Find the Answer](#) p. 97

15. Which of the IKE modes uses three packets for security parameter exchange? Select the best answer.
- A. Quick Mode
 - B. Aggressive Mode
 - C. Normal Mode
 - D. Main Mode

[Find the Answer](#) p. 97



16. What is the protocol number of the protocol which provides IPSec authentication and integrity capabilities as well as encryption capabilities? Select the best answer.
- A. 51
 - B. 48
 - C. 50
 - D. 49

[Find the Answer](#) p. 97

17. Which of the following hashing algorithms is considered preferred? Select the best answer.
- A. MD5
 - B. WHIRLPOOL
 - C. MD6
 - D. SHA

[Find the Answer](#) p. 97

18. Referring to the exhibit, you are trying to configure IPSec encryption between the 192.168.1.0/24 and 192.168.2.0/24 networks and have entered this configuration. This configuration is not working for you why? Select the best answer.
- A. No access-list is defined.
 - B. The peer addresses are set incorrectly.
 - C. This configuration is configured on the wrong routers.
 - D. The group keyword must have group 1 listed.

[Find the Answer](#) p. 97

Exhibit(s):





```

R2
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
crypto isakmp key ipsec-key address 172.16.1.2
!
crypto ipsec transform-set TEST-SET esp-aes esp-sha-hmac
!
crypto map rtr-to-rtr 10 ipsec-isakmp
set peer 172.16.1.2
set transform-set TEST-SET
!
interface Serial1/0
ip address 172.16.1.1 255.255.255.252
crypto map rtr-to-rtr
    
```

```

R3
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
crypto isakmp key ipsec-key address 172.16.1.1
!
crypto ipsec transform-set TEST-SET esp-aes esp-sha-hmac
!
crypto map rtr-to-rtr 10 ipsec-isakmp
set peer 172.16.1.1
set transform-set TEST-SET
!
interface Serial1/0
ip address 172.16.1.2 255.255.255.252
crypto map rtr-to-rtr
    
```

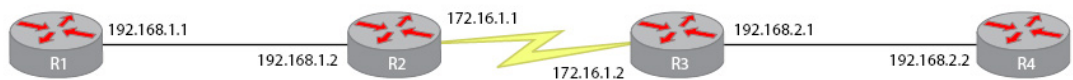
19. Referring to the exhibit, you are trying to configure IPsec encryption between the 192.168.1.0/24 and 192.168.2.0/24 networks and have entered this configuration. This configuration is not working for you why? Select the best answer.

- A. The crypto ipsec transform-set command is incorrect.
- B. The crypto isakmp key command is incorrect.
- C. This configuration is configured on the wrong routers.
- D. The access-list is reversed.

[Find the Answer](#) p. 97

Exhibit(s):





```

R2
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
 crypto isakmp key ipsec-key CISC0 address 172.16.1.2
 !
crypto ipsec transform-set TEST-SET esp-aes esp-sha-hmac
!
crypto map rtr-to-rtr 10 ipsec-isakmp
 set peer 172.16.1.2
 match address 101
 set transform-set TEST-SET
!
interface Serial1/0
 ip address 172.16.1.1 255.255.255.252
 crypto map rtr-to-rtr
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
    
```

```

R3
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
 crypto isakmp key ipsec-key CISC0 address 172.16.1.1
 !
crypto ipsec transform-set TEST-SET esp-aes esp-sha-hmac
!
crypto map rtr-to-rtr 10 ipsec-isakmp
 set peer 172.16.1.1
 match address 101
 set transform-set TEST-SET
!
interface Serial1/0
 ip address 172.16.1.2 255.255.255.252
 crypto map rtr-to-rtr
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
    
```



Answers: Chapter 1

- | | | |
|-------------|--------------------------------------|---|
| 1. A | Review Question p. 2 | Detailed Explanation p. 99 |
| 2. B | Review Question p. 2 | Detailed Explanation p. 99 |
| 3. C | Review Question p. 2 | Detailed Explanation p. 99 |
| 4. D | Review Question p. 3 | Detailed Explanation p. 100 |
| 5. A | Review Question p. 3 | Detailed Explanation p. 100 |
| 6. B | Review Question p. 3 | Detailed Explanation p. 100 |
| 7. C | Review Question p. 4 | Detailed Explanation p. 101 |
| 8. D | Review Question p. 4 | Detailed Explanation p. 101 |
| 9. A | Review Question p. 5 | Detailed Explanation p. 102 |



Answers: Chapter 2

1. B	Review Question p. 6	Detailed Explanation p. 103
2. C	Review Question p. 6	Detailed Explanation p. 103
3. D	Review Question p. 6	Detailed Explanation p. 103
4. A	Review Question p. 7	Detailed Explanation p. 104
5. B	Review Question p. 7	Detailed Explanation p. 104
6. C	Review Question p. 7	Detailed Explanation p. 104
7. D	Review Question p. 8	Detailed Explanation p. 105
8. A	Review Question p. 8	Detailed Explanation p. 105
9. B	Review Question p. 9	Detailed Explanation p. 106
10. C	Review Question p. 10	Detailed Explanation p. 106
11. D	Review Question p. 10	Detailed Explanation p. 106



Answers: Chapter 3

- | | | |
|--------------|---------------------------------------|---|
| 1. A | Review Question p. 11 | Detailed Explanation p. 108 |
| 2. B | Review Question p. 11 | Detailed Explanation p. 108 |
| 3. C | Review Question p. 12 | Detailed Explanation p. 108 |
| 4. D | Review Question p. 12 | Detailed Explanation p. 109 |
| 5. A | Review Question p. 13 | Detailed Explanation p. 109 |
| 6. B | Review Question p. 13 | Detailed Explanation p. 109 |
| 7. C | Review Question p. 14 | Detailed Explanation p. 110 |
| 8. D | Review Question p. 14 | Detailed Explanation p. 110 |
| 9. A | Review Question p. 14 | Detailed Explanation p. 111 |
| 10. B | Review Question p. 15 | Detailed Explanation p. 111 |
| 11. C | Review Question p. 16 | Detailed Explanation p. 111 |



Answers: Chapter 4

- | | | |
|--------------|---------------------------------------|---|
| 1. D | Review Question p. 17 | Detailed Explanation p. 113 |
| 2. A | Review Question p. 17 | Detailed Explanation p. 113 |
| 3. B | Review Question p. 18 | Detailed Explanation p. 113 |
| 4. C | Review Question p. 18 | Detailed Explanation p. 114 |
| 5. D | Review Question p. 18 | Detailed Explanation p. 114 |
| 6. A | Review Question p. 19 | Detailed Explanation p. 114 |
| 7. B | Review Question p. 19 | Detailed Explanation p. 115 |
| 8. C | Review Question p. 19 | Detailed Explanation p. 115 |
| 9. D | Review Question p. 20 | Detailed Explanation p. 115 |
| 10. A | Review Question p. 21 | Detailed Explanation p. 116 |
| 11. B | Review Question p. 22 | Detailed Explanation p. 116 |
| 12. C | Review Question p. 23 | Detailed Explanation p. 116 |
| 13. D | Review Question p. 24 | Detailed Explanation p. 117 |



Answers: Chapter 5

1. A, B	Review Question p. 25	Detailed Explanation p. 118
2. C, D	Review Question p. 25	Detailed Explanation p. 118
3. A	Review Question p. 26	Detailed Explanation p. 118
4. B	Review Question p. 26	Detailed Explanation p. 119
5. C	Review Question p. 27	Detailed Explanation p. 119
6. D	Review Question p. 28	Detailed Explanation p. 119
7. A	Review Question p. 30	Detailed Explanation p. 120
8. B	Review Question p. 30	Detailed Explanation p. 120
9. C	Review Question p. 31	Detailed Explanation p. 120
10. D	Review Question p. 31	Detailed Explanation p. 120
11. A	Review Question p. 31	Detailed Explanation p. 121
12. B	Review Question p. 32	Detailed Explanation p. 121
13. C	Review Question p. 32	Detailed Explanation p. 121
14. D	Review Question p. 34	Detailed Explanation p. 122
15. A	Review Question p. 36	Detailed Explanation p. 122



Answers: Chapter 6

1. B	Review Question p. 37	Detailed Explanation p. 124
2. C	Review Question p. 37	Detailed Explanation p. 124
3. D	Review Question p. 37	Detailed Explanation p. 124
4. A, B	Review Question p. 38	Detailed Explanation p. 125
5. C	Review Question p. 38	Detailed Explanation p. 125
6. D	Review Question p. 38	Detailed Explanation p. 125
7. A	Review Question p. 39	Detailed Explanation p. 126
8. B	Review Question p. 39	Detailed Explanation p. 126
9. C	Review Question p. 39	Detailed Explanation p. 126
10. D	Review Question p. 40	Detailed Explanation p. 127
11. A	Review Question p. 40	Detailed Explanation p. 127
12. B	Review Question p. 41	Detailed Explanation p. 128
13. C	Review Question p. 42	Detailed Explanation p. 128
14. A	Review Question p. 42	Detailed Explanation p. 128
15. B	Review Question p. 42	Detailed Explanation p. 129
16. C	Review Question p. 43	Detailed Explanation p. 129
17. D	Review Question p. 43	Detailed Explanation p. 129
18. A	Review Question p. 43	Detailed Explanation p. 130
19. B	Review Question p. 44	Detailed Explanation p. 130
20. C	Review Question p. 44	Detailed Explanation p. 131
21. D	Review Question p. 44	Detailed Explanation p. 131
22. A	Review Question p. 45	Detailed Explanation p. 131
23. B	Review Question p. 45	Detailed Explanation p. 132



24. C

[Review Question](#) p. 45

[Detailed Explanation](#) p. 132



Answers: Chapter 7

1. D	Review Question p. 46	Detailed Explanation p. 133
2. A	Review Question p. 46	Detailed Explanation p. 133
3. B	Review Question p. 46	Detailed Explanation p. 133
4. C, D	Review Question p. 47	Detailed Explanation p. 134
5. A	Review Question p. 47	Detailed Explanation p. 134
6. B	Review Question p. 47	Detailed Explanation p. 135
7. C	Review Question p. 48	Detailed Explanation p. 135
8. B, D	Review Question p. 48	Detailed Explanation p. 135
9. A, C	Review Question p. 48	Detailed Explanation p. 136
10. B, D	Review Question p. 49	Detailed Explanation p. 136
11. A, C	Review Question p. 49	Detailed Explanation p. 136
12. B	Review Question p. 49	Detailed Explanation p. 137
13. C	Review Question p. 50	Detailed Explanation p. 137
14. D	Review Question p. 50	Detailed Explanation p. 137
15. A	Review Question p. 50	Detailed Explanation p. 138
16. B	Review Question p. 51	Detailed Explanation p. 138
17. C	Review Question p. 51	Detailed Explanation p. 139
18. D	Review Question p. 51	Detailed Explanation p. 139
19. A	Review Question p. 52	Detailed Explanation p. 139
20. B	Review Question p. 52	Detailed Explanation p. 140
21. C	Review Question p. 52	Detailed Explanation p. 140
22. D	Review Question p. 53	Detailed Explanation p. 140
23. A	Review Question p. 54	Detailed Explanation p. 141



24. **D** [Review Question](#) p. 55 [Detailed Explanation](#) p. 141
25. **B** [Review Question](#) p. 57 [Detailed Explanation](#) p. 141
26. **C** [Review Question](#) p. 59 [Detailed Explanation](#) p. 142



Answers: Chapter 8

1. D	Review Question p. 60	Detailed Explanation p. 143
2. A	Review Question p. 60	Detailed Explanation p. 143
3. B	Review Question p. 60	Detailed Explanation p. 143
4. C	Review Question p. 61	Detailed Explanation p. 144
5. D	Review Question p. 61	Detailed Explanation p. 144
6. A	Review Question p. 61	Detailed Explanation p. 144
7. B	Review Question p. 62	Detailed Explanation p. 145
8. C, D	Review Question p. 62	Detailed Explanation p. 145
9. A	Review Question p. 62	Detailed Explanation p. 146
10. B	Review Question p. 63	Detailed Explanation p. 146
11. C	Review Question p. 63	Detailed Explanation p. 146
12. D	Review Question p. 63	Detailed Explanation p. 147
13. A	Review Question p. 64	Detailed Explanation p. 147
14. B	Review Question p. 64	Detailed Explanation p. 147
15. C	Review Question p. 64	Detailed Explanation p. 148
16. D	Review Question p. 65	Detailed Explanation p. 148
17. A	Review Question p. 67	Detailed Explanation p. 148
18. B	Review Question p. 69	Detailed Explanation p. 149
19. C	Review Question p. 71	Detailed Explanation p. 149
20. D	Review Question p. 72	Detailed Explanation p. 149
21. A	Review Question p. 73	Detailed Explanation p. 150
22. B	Review Question p. 75	Detailed Explanation p. 150
23. C	Review Question p. 77	Detailed Explanation p. 150



Answers: Chapter 9

- | | | |
|--------------|---------------------------------------|---|
| 1. D | Review Question p. 78 | Detailed Explanation p. 152 |
| 2. A | Review Question p. 78 | Detailed Explanation p. 152 |
| 3. B | Review Question p. 78 | Detailed Explanation p. 152 |
| 4. C | Review Question p. 79 | Detailed Explanation p. 153 |
| 5. D | Review Question p. 79 | Detailed Explanation p. 153 |
| 6. A | Review Question p. 79 | Detailed Explanation p. 153 |
| 7. B | Review Question p. 80 | Detailed Explanation p. 154 |
| 8. C | Review Question p. 80 | Detailed Explanation p. 154 |
| 9. D | Review Question p. 80 | Detailed Explanation p. 154 |
| 10. A | Review Question p. 81 | Detailed Explanation p. 155 |
| 11. B | Review Question p. 81 | Detailed Explanation p. 155 |
| 12. C | Review Question p. 81 | Detailed Explanation p. 155 |
| 13. D | Review Question p. 82 | Detailed Explanation p. 156 |
| 14. A | Review Question p. 82 | Detailed Explanation p. 156 |
| 15. B | Review Question p. 82 | Detailed Explanation p. 156 |
| 16. C | Review Question p. 83 | Detailed Explanation p. 157 |
| 17. D | Review Question p. 83 | Detailed Explanation p. 157 |
| 18. A | Review Question p. 84 | Detailed Explanation p. 157 |
| 19. B | Review Question p. 85 | Detailed Explanation p. 158 |



Explanations: Chapter 1

1. [Review Question](#) p. 2

Answers: A

Explanation A. Correct, the use of usernames and password as a mechanism are utilized to keep data confidential and only viewable to specific people.

Explanation B. Incorrect, the use of packet checksums is used in order to maintain the integrity of the data.

Explanation C. Incorrect, DDoS protection is used to protect the availability of data services.

Explanation D. Incorrect, an MD5 hash is used to check the integrity of data from one side of a connection to another.

PrepLogic Question: [11691-100](#)

2. [Review Question](#) p. 2

Answers: B

Explanation A. Incorrect, data confidentiality involves keeping data secure and maintaining privacy.

Explanation B. Correct, data integrity involves the concept of keeping data whole from one point to another without change. This is used to make sure that the data was not altered in transit.

Explanation C. Incorrect, data availability involves the access to the data. If this access is restricted for any reason it affects the business involved.

Explanation D. Incorrect, data secrecy is essentially the same as data confidentiality.

PrepLogic Question: [11691-101](#)

3. [Review Question](#) p. 2

Answers: C

Explanation A. Incorrect, data confidentiality involves the privacy of the data.

Explanation B. Incorrect, data integrity makes sure that the data sent across a network is kept intact and not altered.



Explanation C. Correct, data availability involves the access which is provided to the data.

Explanation D. Incorrect, access control over data involves access to the data but specifically the control over who has this access.

PrepLogic Question: [11691-102](#)

4. [Review Question](#) p. 3

Answers: D

Explanation A. Incorrect, an Active attack is one that is obviously directed at a target and can be easily seen if watched for.

Explanation B. Incorrect, an Insider attack occurs when a person inside a company utilizes their existing permissions to breach security.

Explanation C. Incorrect, there is no such attack category.

Explanation D. Correct, the Close-In attack category occurs when an attack is able to gain close physical proximity to a target system.

PrepLogic Question: [11691-103](#)

5. [Review Question](#) p. 3

Answers: A

Explanation A. Correct, a Passive attack uses tools like sniffers to passively obtain information about a target.

Explanation B. Incorrect, a Distribution attack is utilized typically by a rogue developer who builds a backdoor into a program to exploit later.

Explanation C. Incorrect, an Active attack is when an attack directly attacks a target.

Explanation D. Incorrect, an Insider attack occurs when a person inside a company utilizes their existing permissions to breach security.

PrepLogic Question: [11691-104](#)

6. [Review Question](#) p. 3

Answers: B

Explanation A. Incorrect, a Passive attack uses tools like sniffers to passively obtain



information about a target.

Explanation B. Correct, a Distribution attack is utilized typically by a rogue developer who builds a backdoor into a program to exploit later.

Explanation C. Incorrect, an Active attack is when an attack directly attacks a target.

Explanation D. Incorrect, when an attacker builds in a backdoor to exploit this type of attack is called a Distribution attack.

PrepLogic Question: [11691-105](#)

7. [Review Question](#) p. 4

Answers: C

Explanation A. Incorrect, Cisco's security solution which involves overlapping protection is called 'Defense in Depth'.

Explanation B. Incorrect, Cisco's security solution which involves overlapping protection is called 'Defense in Depth'.

Explanation C. Correct, Cisco's overlapping protection is called 'Defense in Depth' and involves implementing several different protection layers which may overlap but provide the best overall protection solution.

Explanation D. Incorrect, Cisco's security solution which involves overlapping protection is called 'Defense in Depth'.

PrepLogic Question: [11691-106](#)

8. [Review Question](#) p. 4

Answers: D

Explanation A. Incorrect, the TCP flags are correct but the SEQ and ACK numbers are not.

Explanation B. Incorrect, The TCP flags are incorrect. The TCP handshake order is SYN, SYN-ACK, ACK.

Explanation C. Incorrect, the TCP flags are correct but the SEQ and ACK numbers are not.

Explanation D. Correct, this correctly shows both the TCP flag order and the SEQ and ACK numbers.



PrepLogic Question: [11691-107](#)

9. [Review Question](#) p. 5

Answers: A

Explanation A. Correct, blind spoofing happens when an attacker launches a spoofing attack but is not on the local subnet.

Explanation B. Incorrect, while this answer is misleading this is not the correct answer. Blind spoofing is what happens when an attacker launches an attack and is not on the local subnet.

Explanation C. Incorrect, blind spoofing is what happens when an attacker launches an attack and is not on the local subnet.

Explanation D. Incorrect, Non-blind spoofing happens when an attacker launches an attack and IS on the local subnet.

PrepLogic Question: [11691-108](#)



Explanations: Chapter 2

1. [Review Question](#) p. 6

Answers: B

Explanation A. Incorrect, this command would setup a local user with a password which utilizes MD5 but will not prompt when going into enable mode.

Explanation B. Correct, this is the correct command which would be used to configure a password which would use MD5 and be prompted on entry to enable mode.

Explanation C. Incorrect, this command would utilize MD5 or be used on entry to enable mode.

Explanation D. Incorrect, this command would not utilize MD5.

PrepLogic Question: [11691-109](#)

2. [Review Question](#) p. 6

Answers: C

Explanation A. Incorrect, this command would setup a local user with a password which utilizes MD5 but will not prompt when going into enable mode.

Explanation B. Incorrect, this is used to configure a password which would use MD5 and be prompted on entry to enable mode but MD5 is not reversible.

Explanation C. Correct, this command would be used. This question requires a little bit of thought because this command by itself would not use encryption however if used with service password-encryption it will use reversible encryption.

Explanation D. Incorrect, this command would utilize encryption if the service password-encryption command was also used.

PrepLogic Question: [11691-110](#)

3. [Review Question](#) p. 6

Answers: D

Explanation A. Incorrect, this command is not valid when entered in global configuration mode.

Explanation B. Incorrect, this command would not prompt when coming in via telnet it



would prompt when going into enable mode.

Explanation C. Incorrect, this command would not prompt when coming in via telnet it would prompt when going into enable mode.

Explanation D. Correct, this command would be used to enable a password on all incoming telnet connections.

PrepLogic Question: [11691-111](#)

4. [Review Question](#) p. 7

Answers: A

Explanation A. Correct, this command would correctly disable the login process for 15 seconds should a login fail 3 times.

Explanation B. Incorrect, the log end portion of this command is mandatory.

Explanation C. Incorrect, this is not a valid command.

Explanation D. Incorrect, this is not a valid command.

PrepLogic Question: [11691-112](#)

5. [Review Question](#) p. 7

Answers: B

Explanation A. Incorrect, these commands would correctly create a privilege level 7 and allow basic show commands but would not allow show running-config.

Explanation B. Correct, these commands would correctly create a privilege level 7, allow basic show commands and allow the show running-config command.

Explanation C. Incorrect, while these commands would properly set the privileges it would not be usable until a password was created for privilege level 7.

Explanation D. Incorrect, this command would correctly set privileges for basic show commands but would not allow the show running-config command. It would also not be usable until a password was created for privilege level 7.

PrepLogic Question: [11691-113](#)

6. [Review Question](#) p. 7



Answers: C

Explanation A. Incorrect, while you must enter root view to configure CLI views this is not the first command. In order to create views AAA must be enabled, this is done through the `aaa new-model` command.

Explanation B. Incorrect, while you must enter root view to configure CLI views this is not the first command, this answer also does not show the correct mode. In order to create views AAA must be enabled, this is done through the `aaa new-model` command.

Explanation C. Correct, this command would be the first command needed to configure CLI views. This command enables AAA which is needed to support CLI views.

Explanation D. Incorrect, while this is the correct first command it is not entered in the correct configuration mode. This command should be entered in global configuration mode.

PrepLogic Question: [11691-114](#)

7. [Review Question](#) p. 8**Answers: D**

Explanation A. Incorrect, this command will correctly secure the running-configuration but will not secure the IOS image.

Explanation B. Incorrect, this command is not valid.

Explanation C. Incorrect, this command is not valid.

Explanation D. Correct, this command will configure the router to save a copy of the IOS image to persistent storage.

PrepLogic Question: [11691-115](#)

8. [Review Question](#) p. 8**Answers: A**

Explanation A. Correct, this command will configure the router to save a copy of the running-configuration to persistent storage.

Explanation B. Incorrect, this command is not valid.

Explanation C. Incorrect, this command is not valid.



Explanation D. Incorrect, this command will correctly secure the IOS image but will not secure the running-configuration.

PrepLogic Question: [11691-116](#)

9. [Review Question](#) p. 9

Answers: B

Explanation A. Incorrect, this will get you into the correct menu but you must also press the 'Perform Security Audit' button to get to this screen.

Explanation B. Correct, to correctly get this screen you must go into the configure screen, then select security audit and click on the 'Perform Security Audit' button.

Explanation C. Incorrect, while this will correctly start a one-step lockdown it will not perform the security audit shown in the diagram.

Explanation D. Incorrect, while this will get you to the proper configure screen there is no 'Perform Security Audit' option on the Configure main screen.

PrepLogic Question: [11691-117](#)

10. [Review Question](#) p. 10

Answers: C

Explanation A. Incorrect, this will get you into the correct menu but you must also press the 'One-step lockdown' button to get to this screen.

Explanation B. Incorrect, while this will correctly start a security audit but it will not perform the One-Step lock-down shown in the diagram.

Explanation C. Correct, to correctly get to this screen you must go into the configure screen, then select security audit and click on the 'One-step Lockdown' button.

Explanation D. Incorrect, while this will get you to the proper configure screen there is no 'Perform Security Audit' option on the Configure main screen.

PrepLogic Question: [11691-118](#)

11. [Review Question](#) p. 10

Answers: D

Explanation A. Incorrect, this would correctly setup SDM for both http and https but this is not the minimal configuration.



Explanation B. Incorrect, this configures two of the commands for SDM configuration with SSL but is not minimal or without SSL.

Explanation C. Incorrect, these commands will setup the http and https server functionality and setup local authentication but it does not setup a user for local authentication. Even if this user was added it is not a minimal configuration.

Explanation D. Correct, this configuration would correctly setup a minimal configuration without SSL.

PrepLogic Question: [11691-119](#)



Explanations: Chapter 3

1. [Review Question](#) p. 11

Answers: A

Explanation A. Correct, this command would correctly enable AAA authentication on login.

Explanation B. Incorrect, this command is not a valid command.

Explanation C. Incorrect, this command is not a valid command.

Explanation D. Incorrect, while this is the correct command to use it is not entered at the enable prompt.

PrepLogic Question: [11691-120](#)

2. [Review Question](#) p. 11

Answers: B

Explanation A. Incorrect, this command is not a valid command.

Explanation B. Correct, this is the correct command to enable AAA authentication on PPP connections and use the local database.

Explanation C. Incorrect, this command is not a valid command.

Explanation D. Incorrect, this command is not a valid command.

PrepLogic Question: [11691-121](#)

3. [Review Question](#) p. 12

Answers: C

Explanation A. Incorrect, these commands are correct but they will not work without issuing the AAA new-model command first.

Explanation B. Incorrect, while these commands are incorrect the last one will not work because it is in the wrong configuration mode. It should be entered in line configuration mode.

Explanation C. Correct, these are the commands required to setup AAA authentication using the local database for the console port.



Explanation D. Incorrect, these commands are correct however without setting up a user no one would be able to login.

PrepLogic Question: [11691-122](#)

4. [Review Question](#) p. 12

Answers: D

Explanation A. Incorrect, the correct syntax is aaa authorization commands level list-name method.

Explanation B. Incorrect, the correct syntax is aaa authorization commands level list-name method.

Explanation C. Incorrect, the correct syntax is aaa authorization commands level list-name method.

Explanation D. Correct, this is the correct syntax which will enable command authorization for all level 15 commands using the com_auth method-list.

PrepLogic Question: [11691-123](#)

5. [Review Question](#) p. 13

Answers: A

Explanation A. Correct, this command would correctly enable AAA TACACS+ authentication when using reverse telnet.

Explanation B. Incorrect, this command is mostly correct. Before the 'tacacs+' keyword 'group' is required.

Explanation C. Incorrect, this command is almost correct except the correct command for reverse telnet is 'reverse-access' not 'reverse-telnet'.

Explanation D. Incorrect, this command is incorrect because it does not create a default method; this would be done by using the 'default' keyword instead of a list-name ('com_auth').

PrepLogic Question: [11691-124](#)

6. [Review Question](#) p. 13

Answers: B

Explanation A. Incorrect, this command syntax is incorrect.



Explanation B. Correct, this command would correctly enable level 15 command authorization as long as the user has been authenticated.

Explanation C. Incorrect, this command syntax is incorrect.

Explanation D. Incorrect, this command syntax is incorrect.

PrepLogic Question: [11691-125](#)

7. [Review Question](#) p. 14

Answers: C

Explanation A. Incorrect, this command is correct except for the fact that it will send information twice; once at the beginning of the request and a second time when the request is finished.

Explanation B. Incorrect, while the command is correct the configuration mode is not. This command needs to be entered in global configuration mode.

Explanation C. Correct, this command would correctly configure to the requirements.

Explanation D. Incorrect, while the command is correct the mode is not. This command needs to be entered in global configuration mode.

PrepLogic Question: [11691-126](#)

8. [Review Question](#) p. 14

Answers: D

Explanation A. Incorrect, this commands syntax is not correct because it omits an accounting type. The correct accounting type for this question would be network.

Explanation B. Incorrect, while this command is correct the mode is incorrect. This command needs to be entered in global configuration mode.

Explanation C. Incorrect, while this command is valid it is not the most thorough command because the 'stop-only' keyword only sends a stop command to the accounting server. In order to get information for both the start and stop of request the 'start-stop' keyword must be used.

Explanation D. Correct, this command will correctly configure accounting on network requests with the most thorough accounting available and send this information to the TACACS+ server.



PrepLogic Question: [11691-127](#)

9. [Review Question](#) p. 14

Answers: A

Explanation A. Correct, TACACS+ provides the ability to provide a command by command authorization.

Explanation B. Incorrect, Security Device Manager (SDM) is not a AAA protocol.

Explanation C. Incorrect, Security Device Manager (SDM) is not a AAA protocol.

Explanation D. Incorrect, RADIUS does not provide command by command authorization it can only provide a specific command level which can be used to control command authorization.

PrepLogic Question: [11691-128](#)

10. [Review Question](#) p. 15

Answers: B

Explanation A. Incorrect, this configuration would setup a connection to the TACACS+ server but it would maintain a connection to the server throughout the session.

Explanation B. Correct, this command would correctly setup a connection to the TACACS+ server and not setup a constant connection throughout the session.

Explanation C. Incorrect, this command does not have correct syntax. The host keyword is required after 'tacacs-server' for it to work correctly.

Explanation D. Incorrect, this command does not have correct syntax. The host keyword is required after 'tacacs-server' for it to work correctly.

PrepLogic Question: [11691-129](#)

11. [Review Question](#) p. 16

Answers: C

Explanation A. Incorrect, there is no main task called AAA.

Explanation B. Incorrect, the login option is only offered once the authentication policies option is opened.



Explanation C. Correct, this would correctly get you to this point in SDM.

Explanation D. Incorrect, there is no main task called AAA.

PrepLogic Question: [11691-130](#)



Explanations: Chapter 4

1. [Review Question](#) p. 17

Answers: D

Explanation A. Incorrect, this statement would do everything except log the entries.

Explanation B. Incorrect, the general syntax is correct but access-lists use wildcard masks.

Explanation C. Incorrect, the general syntax is correct but access-lists use wildcard masks.

Explanation D. Correct, this would deny the 192.168.1.0/24 network while using the last standard ACL number and log all matches.

PrepLogic Question: [11691-131](#)

2. [Review Question](#) p. 17

Answers: A

Explanation A. Correct, this statement would correctly allow telnet traffic from the 172.16.0.0/16 network to the 10.10.10.0/24 network using the first available extended ACL number.

Explanation B. Incorrect, the general syntax is correct except that access-lists use wildcard masks.

Explanation C. Incorrect, this command syntax is correct but the first available extended access-list number is incorrect.

Explanation D. Incorrect, this command syntax is correct but the first available extended access-list number is incorrect and access-lists use wildcard masks.

PrepLogic Question: [11691-132](#)

3. [Review Question](#) p. 18

Answers: B

Explanation A. Incorrect, this command does not exist.

Explanation B. Correct, this command would correctly enable turbo ACL's.



Explanation C. Incorrect, this keyword does not exist for the access-list statement.

Explanation D. Incorrect, this keyword does not exist for the ip access-group statement.

PrepLogic Question: [11691-133](#)

4. [Review Question](#) p. 18

Answers: C

Explanation A. Incorrect, this command is incorrect and is not configured in global configuration mode.

Explanation B. Incorrect, this command should be 'ip access-group 10 in'.

Explanation C. Correct, this command would correctly enable access-list 50 coming into this interface.

Explanation D. Incorrect, the ip access-group command is not configured in global configuration mode and does not reference interfaces in the syntax.

PrepLogic Question: [11691-134](#)

5. [Review Question](#) p. 18

Answers: D

Explanation A. Incorrect, standard ACL's should be configured close to the destination while extended ACL's should be configured close to the source.

Explanation B. Incorrect, standard ACL's should be configured close to the destination while extended ACL's should be configured close to the source.

Explanation C. Incorrect, standard ACL's should be configured close to the destination while extended ACL's should be configured close to the source.

Explanation D. Correct, standard ACL's should be configured close to the destination while extended ACL's should be configured close to the source.

PrepLogic Question: [11691-135](#)

6. [Review Question](#) p. 19

Answers: A

Explanation A. Correct, extended ACL's should be configured close to the source while standard ACL's should be configured close to the destination.



Explanation B. Incorrect, extended ACL's should be configured close to the source while standard ACL's should be configured close to the destination.

Explanation C. Incorrect, extended ACL's should be configured close to the source while standard ACL's should be configured close to the destination.

Explanation D. Incorrect, extended ACL's should be configured close to the source while standard ACL's should be configured close to the destination.

PrepLogic Question: [11691-136](#)

7. [Review Question](#) p. 19

Answers: B

Explanation A. Incorrect, this command to be correct would be 'access-class 40 in'.

Explanation B. Correct, this command would correctly enable access-list 40 coming into a line interface.

Explanation C. Incorrect, this command needs to be 'access-class' and must be configured in line configuration mode.

Explanation D. Incorrect, this command to be correct must be 'access-class'.

PrepLogic Question: [11691-137](#)

8. [Review Question](#) p. 19

Answers: C

Explanation A. Incorrect, this command would filter the read-write community public.

Explanation B. Incorrect, to filter SNMP you don't use the access-class command.

Explanation C. Correct, this command would correctly filter the public read-only community using the access-list 80.

Explanation D. Incorrect, to filter SNMP you don't use the access-class command.

PrepLogic Question: [11691-138](#)

9. [Review Question](#) p. 20

Answers: D

Explanation A. Incorrect, the correct IP addresses are matched in this exhibit.



Explanation B. Incorrect, this configuration is incorrect because the access-list is not enabled in the correct direction.

Explanation C. Incorrect, this access-list is formatted correctly.

Explanation D. Correct, this configuration will not work because the access-list is enabled in the wrong direction.

PrepLogic Question: [11691-139](#)

10. [Review Question](#) p. 21

Answers: A

Explanation A. Correct, this configuration will only allow traffic on port 80 from the Internet.

Explanation B. Incorrect, there is no implicit allow in access-lists there is only an implicit deny.

Explanation C. Incorrect, the access-list command is formatted correctly.

Explanation D. Incorrect, the access-group command is formatted correctly.

PrepLogic Question: [11691-140](#)

11. [Review Question](#) p. 22

Answers: B

Explanation A. Incorrect, the access-list is enabled in the correct direction.

Explanation B. Correct, the access-list in the exhibit uses normal masks while the access-list requires inverse masks.

Explanation C. Incorrect, the IP addresses matched in the exhibit are correct.

Explanation D. Incorrect, this configuration will not work correctly because the access-list in the exhibit uses normal masks while the access-list requires inverse masks.

PrepLogic Question: [11691-141](#)

12. [Review Question](#) p. 23

Answers: C

Explanation A. Incorrect, you are not trying to protect the Internet you are trying to



protect the inside network.

Explanation B. Incorrect, the access-list is correct.

Explanation C. Correct, this configuration is correct and will block spoofing attempts from coming in the Internet interface.

Explanation D. Incorrect, the access-group statement is configured in the correct direction.

PrepLogic Question: [11691-142](#)

13. [Review Question](#) p. 24

Answers: D

Explanation A. Incorrect, this configuration will not work because the access-group command is configured in the wrong direction if it is to be applied on this interface.

Explanation B. Incorrect, the access-list command is formatted correctly.

Explanation C. Incorrect, the access-group command is formatted correctly.

Explanation D. Correct, in the exhibit either the interface needs to change or the direction needs to change for this configuration to work.

PrepLogic Question: [11691-143](#)

Explanations: Chapter 5

1. [Review Question](#) p. 25

Answers: A, B

Explanation A. Correct, logging levels need to be appropriate so that there is not too much logging clutter.

Explanation B. Correct, it is highly recommended that NTP be used on all devices so all logs can be synchronized which is highly helpful when troubleshooting.

Explanation C. Incorrect, while a log on the device is helpful to contain the log only on the device is not recommended.

Explanation D. Incorrect, the LDAP protocol is not used for this purpose.

PrepLogic Question: [11691-144](#)

2. [Review Question](#) p. 25

Answers: C, D

Explanation A. Incorrect, it is recommended that all levels of the team be consulted when recommending a logging solution.

Explanation B. Incorrect, if the highest level of logging is used it is easy for a problem to be missed inside the vast number of messages sent.

Explanation C. Correct, it is recommended that all logging information be sent to a secure central location which is used in case a device is tampered with.

Explanation D. Correct, it is recommended that a change management program be used to track all changes to a system. This is useful because this granular tracking provides vital data for troubleshooting and for reference information for future changes.

PrepLogic Question: [11691-145](#)

3. [Review Question](#) p. 26

Answers: A

Explanation A. Correct, buffered logging on a device will hold a configured amount of information to view.

Explanation B. Incorrect, internal is not a type of logging destination.



Explanation C. Incorrect, logging to the console is useful when connected to the console when an event occurs but it is not logged for future reference.

Explanation D. Incorrect, there is no such thing as a device monitor.

PrepLogic Question: [11691-146](#)

4. [Review Question](#) p. 26

Answers: B

Explanation A. Incorrect, this is not the correct level of this message.

Explanation B. Correct, this is the correct level of this message (5).

Explanation C. Incorrect, this is not the correct level of this message.

Explanation D. Incorrect, this is not the correct level of this message.

PrepLogic Question: [11691-147](#)

5. [Review Question](#) p. 27

Answers: C

Explanation A. Incorrect, this is not the correct level of this message.

Explanation B. Incorrect, this is not the correct level of this message.

Explanation C. Correct, this is the correct level of this message (6).

Explanation D. Incorrect, this is not the correct level of this message.

PrepLogic Question: [11691-148](#)

6. [Review Question](#) p. 28

Answers: D

Explanation A. Incorrect, this is not the correct task list.

Explanation B. Incorrect, this is not the correct task list.

Explanation C. Incorrect, this is not the correct task list.

Explanation D. Correct, this will correctly get you to this screen.



PrepLogic Question: [11691-149](#)

7. [Review Question](#) p. 30

Answers: A

Explanation A. Correct, this will correctly get you to this screen.

Explanation B. Incorrect, this is not the correct task list.

Explanation C. Incorrect, this is not the correct task list.

Explanation D. Incorrect, this is not the correct task list.

PrepLogic Question: [11691-150](#)

8. [Review Question](#) p. 30

Answers: B

Explanation A. Incorrect, AES encryption is not used.

Explanation B. Correct, DES-56 encryption is used in SNMPv3.

Explanation C. Incorrect, 3DES encryption is not used.

Explanation D. Incorrect, there is no such thing as 3DES-64

PrepLogic Question: [11691-151](#)

9. [Review Question](#) p. 31

Answers: C

Explanation A. Incorrect, the minimum recommended value is 1024 bits.

Explanation B. Incorrect, the minimum recommended value is 1024 bits.

Explanation C. Correct, 1024 bits is the minimum recommended value.

Explanation D. Incorrect, the minimum recommended value is 1024 bits.

PrepLogic Question: [11691-152](#)

10. [Review Question](#) p. 31

Answers: D



Explanation A. Incorrect, the supported versions are 1, 2c and 3.

Explanation B. Incorrect, the supported versions are 1, 2c and 3.

Explanation C. Incorrect, the supported versions are 1, 2c and 3.

Explanation D. Correct, these are the correct supported versions.

PrepLogic Question: [11691-153](#)

11. [Review Question](#) p. 31

Answers: A

Explanation A. Correct, from this IOS version forward SSH version 2 is supported.

Explanation B. Incorrect, the correct first IOS version that supports SSH version 2 is 12.3(4)T.

Explanation C. Incorrect, the correct first IOS version that supports SSH version 2 is 12.3(4)T.

Explanation D. Incorrect, the correct first IOS version that supports SSH version 2 is 12.3(4)T.

PrepLogic Question: [11691-154](#)

12. [Review Question](#) p. 32

Answers: B

Explanation A. Incorrect, this command itself is correct but the configuration mode is incorrect. The correct mode to use is global configuration mode.

Explanation B. Correct, this is the correct command to set the number of SSH retries to 2.

Explanation C. Incorrect, this command is almost correct but there needs to be a '-' between authentication and retries to make 'ip ssh authentication-retries 2'.

Explanation D. Incorrect, this command is not correct because it needs to have 'ip' added to the beginning.

PrepLogic Question: [11691-155](#)

13. [Review Question](#) p. 32



Answers: C

Explanation A. Incorrect, the command itself is correct but the configuration mode is incorrect. The correct mode is line configuration mode.

Explanation B. Incorrect, this is not a valid command.

Explanation C. Correct, this command would correctly enable ssh on the configured line.

Explanation D. Incorrect, this is not a valid command.

PrepLogic Question: [11691-156](#)

14. [Review Question](#) p. 34

Answers: D

Explanation A. Incorrect, this would not correctly get you to the point to add an NTP server.

Explanation B. Incorrect, this would not correctly get you to the point to add an NTP server.

Explanation C. Incorrect, this would not correctly get you to the point to add an NTP server.

Explanation D. Correct, this would correctly get you to the point which enables you to add an NTP server.

PrepLogic Question: [11691-157](#)

15. [Review Question](#) p. 36

Answers: A

Explanation A. Correct, this would correctly enable you to generate an SSH key pair.

Explanation B. Incorrect, this would not correctly get you to the point to generate an SSH key pair.

Explanation C. Incorrect, this would not correctly get you to the point to generate an SSH key pair.

Explanation D. Incorrect, this would not correctly get you to the point to generate an SSH key pair.



PrepLogic Question: [11691-158](#)



Explanations: Chapter 6

1. [Review Question](#) p. 37

Answers: B

Explanation A. Incorrect, the switch will flood the frame out all ports except the received until the ports become learned and are entered into the CAM table.

Explanation B. Correct, the switch will flood the frame out all ports except the received port.

Explanation C. Incorrect, there are no assigned ports. The switch will flood the frame out all ports except the received until the ports become learned and are entered into the CAM table.

Explanation D. Incorrect, there are no ports entered into the CAM table yet. The switch will flood the frame out all ports except the received until the ports become learned and are entered into the CAM table.

PrepLogic Question: [11691-159](#)

2. [Review Question](#) p. 37

Answers: C

Explanation A. Incorrect, layer 2 associates with the data link OSI layer.

Explanation B. Incorrect, layer 2 associates with the data link OSI layer.

Explanation C. Correct, layer 2 associates with the data link OSI layer.

Explanation D. Incorrect, layer 2 associates with the data link OSI layer.

PrepLogic Question: [11691-160](#)

3. [Review Question](#) p. 37

Answers: D

Explanation A. Incorrect, SNMP version 3 while more secure will not be the highest performer and will not be the easiest to use.

Explanation B. Incorrect, SNMP version 2 was never really used because of its complicated security features.



Explanation C. Incorrect, while the easiest to use version 1 is not the highest performer.

Explanation D. Correct, version 2c is the easiest to use that adds performance features.

PrepLogic Question: [11691-161](#)

4. [Review Question](#) p. 38

Answers: A, B

Explanation A. Correct, this will force the port into access mode which will not allow switch spoofing.

Explanation B. Correct, private VLAN's provide a means for isolating ports or groups of ports.

Explanation C. Incorrect, this is not a valid command.

Explanation D. Incorrect, the native VLAN transmits to everyone because all untagged traffic goes onto this VLAN.

PrepLogic Question: [11691-162](#)

5. [Review Question](#) p. 38

Answers: C

Explanation A. Incorrect, 'double tagging' happens when a frame is tagged twice one over the other.

Explanation B. Incorrect, 'double tagging' happens when a frame is tagged twice one over the other.

Explanation C. Correct, 'double tagging' happens when a frame is tagged twice one over the other. This is problematic when the native VLAN is the outer tag because some switches will remove the native tag and keep the inner tag.

Explanation D. Incorrect, 'double tagging' happens when a frame is tagged twice one over the other.

PrepLogic Question: [11691-163](#)

6. [Review Question](#) p. 38

Answers: D



Explanation A. Incorrect, the correct command is 'switchport trunk native vlan 200' and it must be entered in interface configuration mode.

Explanation B. Incorrect, the correct command is 'switchport trunk native vlan 200'.

Explanation C. Incorrect, the correct command is 'switchport trunk native vlan 200'.

Explanation D. Correct, this command will correctly change the native vlan on a port.

PrepLogic Question: [11691-164](#)

7. [Review Question](#) p. 39

Answers: A

Explanation A. Correct, the Root Guard feature is used to disable a port from becoming a root port.

Explanation B. Incorrect, portfast is used on access ports to allow for a quick STP transition into the forwarding state.

Explanation C. Incorrect, there is no such feature.

Explanation D. Incorrect, BPDU guard is used to disable an access port if it receives a BPDU.

PrepLogic Question: [11691-165](#)

8. [Review Question](#) p. 39

Answers: B

Explanation A. Incorrect, the Root Guard feature is used to disable a port from becoming a root port.

Explanation B. Correct, BPDU guard is used to disable an access port if it receives a BPDU which is only used on trunks.

Explanation C. Incorrect, there is no such feature.

Explanation D. Incorrect, portfast is used on access ports to allow for a quick STP transition into the forwarding state.

PrepLogic Question: [11691-166](#)

9. [Review Question](#) p. 39



Answers: C

Explanation A. Incorrect, the correct command syntax is 'ip dhcp snooping'.

Explanation B. Incorrect, the command itself is correct but should be entered in global configuration mode.

Explanation C. Correct, this is the correct command to enable DHCP the snooping feature.

Explanation D. Incorrect, the correct command syntax is 'ip dhcp snooping' and should be entered in global configuration mode.

PrepLogic Question: [11691-167](#)

10. [Review Question](#) p. 40

Answers: D

Explanation A. Incorrect, all ports are not trusted by default.

Explanation B. Incorrect, this is not the correct syntax.

Explanation C. Incorrect, this is not the correct syntax.

Explanation D. Correct, this command would correctly enable a port to be trusted for DHCP snooping.

PrepLogic Question: [11691-168](#)

11. [Review Question](#) p. 40

Answers: A

Explanation A. Correct, Dynamic ARP inspection (DAI) requires the DHCP snooping IP-to-MAC table to verify bindings.

Explanation B. Incorrect, this command is correct but requires DHCP snooping to be enabled for it to work correctly.

Explanation C. Incorrect, this command is formatted correctly.

Explanation D. Incorrect, this command is entered in the correct configuration mode.

PrepLogic Question: [11691-169](#)



12. [Review Question](#) p. 41

Answers: B

Explanation A. Incorrect, if a new frame comes in when the MAC table was full it will not be able to be associated with a port.

Explanation B. Correct, the switch will not be able to associate a new frame with a port because the MAC table is full. The switch will flood the frame out all interfaces in this situation.

Explanation C. Incorrect, the MAC address table by default is dynamic and will allow for the timeout of MAC addresses in time. During this time that the MAC table is full the switch will flood frames out all interfaces.

Explanation D. Incorrect, if the MAC table is full the switch will not drop any frames it will flood them out all interfaces.

PrepLogic Question: [11691-170](#)

13. [Review Question](#) p. 42

Answers: C

Explanation A. Incorrect, there is a specific command to configure for each type of port.

Explanation B. Incorrect, these commands are not correct; you must specify each interface in the command and in global configuration mode.

Explanation C. Correct, this configuration would correctly setup the SPAN feature by listening to interface FastEthernet 0/1 and send the traffic to FastEthernet 0/2.

Explanation D. Incorrect, these commands are not correct; you must specify each interface in the command and in global configuration mode.

PrepLogic Question: [11691-171](#)

14. [Review Question](#) p. 42

Answers: A

Explanation A. Correct, a group inside private VLAN is called a community. Community VLAN's are used to allow all members to talk to each other but not to other communities.

Explanation B. Incorrect, a group inside private VLAN is called a community. Community VLAN's are used to allow all members to talk to each other but not to other



communities.

Explanation C. Incorrect, isolated VLAN's are used inside private VLAN's. The isolated VLAN's are used to make sure each device is isolated from all other except the promiscuous VLAN's.

Explanation D. Incorrect, there is no such thing as a comprehensive VLAN.

PrepLogic Question: [11691-173](#)

15. [Review Question](#) p. 42

Answers: B

Explanation A. Incorrect, the correct port security action is Restrict.

Explanation B. Correct, the restrict port security action is used to report violations is Restrict.

Explanation C. Incorrect, the correct port security action is Restrict.

Explanation D. Incorrect, the correct port security action is Restrict.

PrepLogic Question: [11691-174](#)

16. [Review Question](#) p. 43

Answers: C

Explanation A. Incorrect, the correct port security action is Shutdown.

Explanation B. Incorrect, the correct port security action is Shutdown.

Explanation C. Correct, the correct port security action that will report and shutdown the port to all traffic is the Shutdown action.

Explanation D. Incorrect, the correct port security action is Shutdown.

PrepLogic Question: [11691-175](#)

17. [Review Question](#) p. 43

Answers: D

Explanation A. Incorrect, there is no secure port MAC address.

Explanation B. Incorrect, the Dynamic Secure MAC addresses work similarly to Static



Secure MAC Addresses but do not retain this information in the configuration.

Explanation C. Incorrect, this type of secure port MAC address needs to be manually configured.

Explanation D. Correct, this type of secure port MAC address is used to dynamically learn MAC-to-port assignments and to retain this information in the running-configuration.

PrepLogic Question: [11691-176](#)

18. [Review Question](#) p. 43

Answers: A

Explanation A. Correct, dynamic secure MAC addresses allow the IP-to-port tables to be created and kept in the CAM table but this information is not saved in the running-configuration so it does not have the ability to be saved on reboots.

Explanation B. Incorrect, there is no such secure port MAC address type.

Explanation C. Incorrect, the sticky secure MAC addresses are saved to both the local CAM table and to the running configuration.

Explanation D. Incorrect, static secure MAC addresses require static configuration of the IP-to-port relationships.

PrepLogic Question: [11691-177](#)

19. [Review Question](#) p. 44

Answers: B

Explanation A. Incorrect, the correct command would be 'switchport port-security maximum 3'.

Explanation B. Correct, this command would correctly limit the number of MAC addresses learned on an interface to 3.

Explanation C. Incorrect, the correct command would be 'switchport port-security maximum 3'.

Explanation D. Incorrect, this command itself is correct but is entered in the wrong configuration mode. The correct configuration mode is interface configuration mode.

PrepLogic Question: [11691-178](#)



20. [Review Question](#) p. 44

Answers: C

Explanation A. Incorrect, this command is used to configure static secure MAC addresses.

Explanation B. Incorrect, this command is invalid because you do not specify a specific MAC address if the 'sticky' keyword is used.

Explanation C. Correct, dynamic secure addresses are the default.

Explanation D. Incorrect, this command would configure an interface for sticky secure MAC addresses.

PrepLogic Question: [11691-179](#)

21. [Review Question](#) p. 44

Answers: D

Explanation A. Incorrect, while this command is correct in syntax the default port security behavior is to shutdown the port on violation doing this command is unneeded.

Explanation B. Incorrect, this command while correct in syntax is not configured in the correct configuration mode and is unneeded because shutting down the port is the default behavior. The correct configuration mode for the 'switchport port-security violation' command is interface configuration mode.

Explanation C. Incorrect, this command has the correct syntax to use the protect violation behavior which does not shutdown the port but just disallows traffic from all unknown MAC addresses.

Explanation D. Correct, this is correct because the default behavior for the 'switchport port-security violation' command is to shutdown the port.

PrepLogic Question: [11691-180](#)

22. [Review Question](#) p. 45

Answers: A

Explanation A. Correct, this command would correctly configure a switch to use a RADIUS server.

Explanation B. Incorrect, the command syntax is incorrect. The correct command to use would be 'radius-server host [hostname | ip address]'.



Explanation C. Incorrect, while the command syntax is correct it is configured in an invalid configuration mode. The correct mode would be global configuration mode.

Explanation D. Incorrect, this command is incorrect. The correct command to use would be 'radius-server host [hostname | ip address]'.

PrepLogic Question: [11691-181](#)

23. [Review Question](#) p. 45

Answers: B

Explanation A. Incorrect, the correct default option is Forced-Authorized.

Explanation B. Correct, by default the behavior of 802.1x configured ports is to default to Forced-Authorized state.

Explanation C. Incorrect, the correct default option is Forced-Authorized.

Explanation D. Incorrect, this is not an available option.

PrepLogic Question: [11691-182](#)

24. [Review Question](#) p. 45

Answers: C

Explanation A. Incorrect, while the command syntax is correct the configuration mode is not. The correct mode is interface configuration mode.

Explanation B. Incorrect, this command is invalid. The correct command to use is 'switch(config-if)#dot1x auth-fail vlan 66'.

Explanation C. Correct, this command would correctly configure VLAN 66 to be used as the restricted VLAN for all unauthorized traffic.

Explanation D. Incorrect, this command is invalid and is configured in the incorrect configuration mode. The correct command to use is 'switch(config-if)#dot1x auth-fail vlan 66' and it should be entered in interface configuration mode.

PrepLogic Question: [11691-183](#)



Explanations: Chapter 7

1. [Review Question](#) p. 46

Answers: D

Explanation A. Incorrect, a transparent firewall is essentially a bridge with firewall capabilities. Because of this a transparent firewall is limited to two interfaces.

Explanation B. Incorrect, a transparent firewall is essentially a bridge with firewall capabilities. Because of this a transparent firewall is limited to two interfaces.

Explanation C. Incorrect, a transparent firewall is essentially a bridge with firewall capabilities. Because of this a transparent firewall is limited to two interfaces.

Explanation D. Correct, a transparent firewall is essentially a bridge with firewall capabilities. Because of this a transparent firewall is limited to two interfaces.

PrepLogic Question: [11691-184](#)

2. [Review Question](#) p. 46

Answers: A

Explanation A. Correct, a transparent firewall has the option of filtering on layers 2 and 3.

Explanation B. Incorrect, a transparent firewall has the option of filtering on layers 2 and 3.

Explanation C. Incorrect, a transparent firewall has the option of filtering on layers 2 and 3.

Explanation D. Incorrect, a transparent firewall has the option of filtering on layers 2 and 3.

PrepLogic Question: [11691-185](#)

3. [Review Question](#) p. 46

Answers: B

Explanation A. Incorrect, an application layer firewall has the option of filtering on layers 3, 4, 5 and 7.

Explanation B. Correct, an application layer firewall has the option of filtering on



layers 3, 4, 5 and 7.

Explanation C. Incorrect, an application layer firewall has the option of filtering on layers 3, 4, 5 and 7.

Explanation D. Incorrect, an application layer firewall has the option of filtering on layers 3, 4, 5 and 7.

PrepLogic Question: [11691-186](#)

4. [Review Question](#) p. 47

Answers: C, D

Explanation A. Incorrect, application layer firewalls are very processor and memory intensive.

Explanation B. Incorrect, application layer firewalls work with specific services like http and ftp.

Explanation C. Correct, application layer firewalls have the ability to monitor and log various types of application data.

Explanation D. Correct, application layer firewalls have access to various upper layers which enables the ability to log very detailed information.

PrepLogic Question: [11691-187](#)

5. [Review Question](#) p. 47

Answers: A

Explanation A. Correct, with static packet filtering firewalls all unknown traffic is allowed until it reaches layer 3 where it is then filtered.

Explanation B. Incorrect, with static packet filtering firewalls all unknown traffic is allowed until it reaches layer 3.

Explanation C. Incorrect, with static packet filtering firewalls all unknown traffic is allowed until it reaches layer 3.

Explanation D. Incorrect, with static packet filtering firewalls all unknown traffic is allowed until it reaches layer 3.

PrepLogic Question: [11691-188](#)



6. [Review Question](#) p. 47

Answers: B

Explanation A. Incorrect, a stateful firewall operates on layers 3, 4, and 5.

Explanation B. Correct, a stateful firewall operates on layers 3, 4 and 5. This gives a stateful firewall the ability to monitor the state of the connections.

Explanation C. Incorrect, a stateful firewall operates on layers 3, 4 and 5.

Explanation D. Incorrect, a stateful firewall operates on layers 3, 4, and 5.

PrepLogic Question: [11691-189](#)

7. [Review Question](#) p. 48

Answers: C

Explanation A. Incorrect, because UDP is stateless there is no way to keep track of UDP states as they do not exist.

Explanation B. Incorrect, RTP is short for Real-time Transport Protocol which does not affect state.

Explanation C. Correct, RST is short for Reset which is used within TCP to reset a connection.

Explanation D. Incorrect, MAC stands for Media Access Control which is used at layer 2.

PrepLogic Question: [11691-190](#)

8. [Review Question](#) p. 48

Answers: B, D

Explanation A. Incorrect, UDP is a stateless protocol so there would be no ability to track state.

Explanation B. Correct, TCP sequence numbers are used to keep track of TCP session states.

Explanation C. Incorrect, SIP is short for Session Initiation Protocol and is not used for state information.

Explanation D. Correct, the destination address as well as the source address is used to track the state of a session.



PrepLogic Question: [11691-191](#)

9. [Review Question](#) p. 48

Answers: A, C

Explanation A. Correct, stateful firewalls are recommended as a primary means to defense.

Explanation B. Incorrect, stateful firewalls are recommended as a primary means to defense.

Explanation C. Correct, stateful firewalls provide better routing performance over the other firewall options.

Explanation D. Incorrect, stateful firewalls are not used to give granular control of traffic.

PrepLogic Question: [11691-192](#)

10. [Review Question](#) p. 49

Answers: B, D

Explanation A. Incorrect, stateful firewalls require state based protocols to be effective.

Explanation B. Correct, since stateful firewalls only support layers 3, 4 and 5, they do not provide prevention of application layer attacks.

Explanation C. Incorrect, stateful firewalls support layers 3, 4 and 5.

Explanation D. Correct, stateful firewalls have issues tracking protocols which use multiple connections because it is harder to track multiple connections for one session.

PrepLogic Question: [11691-193](#)

11. [Review Question](#) p. 49

Answers: A, C

Explanation A. Correct, stateful firewalls have the ability to track the state of a connection and use this information to prevent attacks.

Explanation B. Incorrect, application layer firewalls are intended to be used for specific services (like http and ftp) and only offer protection which is detailed in the firewall rules.



Explanation C. Correct, application inspection firewalls have the ability to track the state of a connection and to perform other deep inspection is needed.

Explanation D. Incorrect, static firewalls can't be used to track state information.

PrepLogic Question: [11691-194](#)

12. [Review Question](#) p. 49

Answers: B

Explanation A. Incorrect, a stateful firewall only operates at layers 3 through 5 and does not have the ability to control attacks from java or flash.

Explanation B. Correct, application inspection firewalls have the ability to check and affect layer 7. Because of this the ability to control java or flash is possible.

Explanation C. Incorrect, transparent firewalls are limited to layers 2 and 3.

Explanation D. Incorrect, Static firewalls are limited to the capabilities of static ACL's and thus can't control java or flash plugins.

PrepLogic Question: [11691-195](#)

13. [Review Question](#) p. 50

Answers: C

Explanation A. Incorrect, application inspection firewalls do have the ability to track layer 5 states.

Explanation B. Incorrect, application inspection firewalls have the ability to track layers 3, 4, 5 and 7.

Explanation C. Correct, application inspection firewalls do not have the ability natively to support user authentication.

Explanation D. Incorrect, application inspection firewalls do have the ability to monitor and check layer 5 conformity.

PrepLogic Question: [11691-196](#)

14. [Review Question](#) p. 50

Answers: D

Explanation A. Incorrect, application inspection firewalls should be used as a



secondary defense.

Explanation B. Incorrect, application inspection firewalls do not improve routing performance because they are processor intensive.

Explanation C. Incorrect, application inspection firewalls should not be used to defend against DoS attacks.

Explanation D. Correct, application inspection firewalls are considered to be the most stringent of all the firewalls.

PrepLogic Question: [11691-197](#)

15. [Review Question](#) p. 50

Answers: A

Explanation A. Correct, you should never use a firewall as a server.

Explanation B. Incorrect, it is important to segment security zones.

Explanation C. Incorrect, it is always a good idea to have more than one type of system working combined to protect your systems.

Explanation D. Incorrect, it is important to limit the number of protocols running on your network to limit the number of systems vulnerable.

PrepLogic Question: [11691-198](#)

16. [Review Question](#) p. 51

Answers: B

Explanation A. Incorrect, Context-Bases Access Control (CBAC) was the initial technology used to implement a stateful firewall but is no longer current.

Explanation B. Correct, Stateful Packet Inspection (SPI) is the current technology used to implement stateful packet inspection.

Explanation C. Incorrect, Access Control List's (ACL) are used to implement a number of different firewall technologies but stateful firewalls are not one of them.

Explanation D. Incorrect, Granular Protocol Inspection (GPI) is the official name of the initial Cisco classic firewall.

PrepLogic Question: [11691-199](#)



17. [Review Question](#) p. 51

Answers: C

Explanation A. Incorrect, the SPI feature was introduced in IOS version 12.3(4)T.

Explanation B. Incorrect, the SPI feature was introduced in IOS version 12.3(4)T.

Explanation C. Correct, the SPI feature was introduced in IOS version 12.3(4)T.

Explanation D. Incorrect, the SPI feature was introduced in IOS version 12.3(4)T.

PrepLogic Question: [11691-200](#)

18. [Review Question](#) p. 51

Answers: D

Explanation A. Incorrect, the zone based features were introduced in IOS version 12.4(6)T.

Explanation B. Incorrect, the zone based features were introduced in IOS version 12.4(6)T.

Explanation C. Incorrect, the zone based features were introduced in IOS version 12.4(6)T.

Explanation D. Correct, the zone based features were introduced in IOS version 12.4(6)T.

PrepLogic Question: [11691-201](#)

19. [Review Question](#) p. 52

Answers: A

Explanation A. Correct, when setting up a zone based firewall each interface is limited to be in one zone at a time.

Explanation B. Incorrect, when setting up a zone based firewall each interface is limited to be in one zone at a time.

Explanation C. Incorrect, when setting up a zone based firewall each interface is limited to be in one zone at a time.

Explanation D. Incorrect, when setting up a zone based firewall each interface is limited to be in one zone at a time.



PrepLogic Question: [11691-202](#)

20. [Review Question](#) p. 52

Answers: B

Explanation A. Incorrect, the syntax of this command is incorrect. The correct syntax is 'zone security public'.

Explanation B. Correct, it is required that a zone be configured before a zone is assigned to an interface.

Explanation C. Incorrect, the 'zone-member' syntax is correct but a zone must be configured before a zone can be configured onto an interface.

Explanation D. Incorrect, the 'zone-member' command is correct for the interface but can't be configured before a zone is configured.

PrepLogic Question: [11691-203](#)

21. [Review Question](#) p. 52

Answers: C

Explanation A. Incorrect, an incorrect zone could be the problem but is not the best answer in this situation.

Explanation B. Incorrect, this could be one of the problems but is not the best answer in this case.

Explanation C. Correct, since the default behavior is for no traffic to flow outside a zone the best answer is that no other interfaces on the equipment are configured in the same zone.

Explanation D. Incorrect, since this is a new router no other technologies would be configured to block traffic.

PrepLogic Question: [11691-204](#)

22. [Review Question](#) p. 53

Answers: D

Explanation A. Incorrect, all zones were configured as shown in the exhibit.

Explanation B. Incorrect, even if a class was required traffic would not be allowed between an interface in a zone and an interface not in a zone.



Explanation C. Incorrect, even if a parameter was required traffic would not be allowed between an interface in a zone and an interface not in a zone.

Explanation D. Correct, no traffic is able to be passed between an interface in a zone and an interface not in a zone.

PrepLogic Question: [11691-205](#)

23. [Review Question](#) p. 54

Answers: A

Explanation A. Correct, this would be the correct process to get to this screen.

Explanation B. Incorrect, this would not correctly display this screen.

Explanation C. Incorrect, this would not correctly display this screen.

Explanation D. Incorrect, this would not correctly display this screen.

PrepLogic Question: [11691-206](#)

24. [Review Question](#) p. 55

Answers: D

Explanation A. Incorrect, this would not correctly display this screen.

Explanation B. Incorrect, this would not correctly display this screen.

Explanation C. Incorrect, this would not correctly display this screen.

Explanation D. Correct, this would be the correct process to get to this screen.

PrepLogic Question: [11691-207](#)

25. [Review Question](#) p. 57

Answers: B

Explanation A. Incorrect, this would not correctly display this screen.

Explanation B. Correct, this would be the correct process to get to this screen.

Explanation C. Incorrect, this would not correctly display this screen.

Explanation D. Incorrect, this would not correctly display this screen.



PrepLogic Question: [11691-208](#)

26. [Review Question](#) p. 59

Answers: C

Explanation A. Incorrect, this would not correctly display this screen.

Explanation B. Incorrect, this would not correctly display this screen.

Explanation C. Correct, this would be the correct process to get to this screen.

Explanation D. Incorrect, this would not correctly display this screen.

PrepLogic Question: [11691-209](#)



Explanations: Chapter 8

1. [Review Question](#) p. 60

Answers: D

Explanation A. Incorrect, this is one of the detection methods.

Explanation B. Incorrect, this is one of the detection methods.

Explanation C. Incorrect, this is one of the detection methods.

Explanation D. Correct, there is no such thing as a Heuristics-Based method.

PrepLogic Question: [11691-210](#)

2. [Review Question](#) p. 60

Answers: A

Explanation A. Correct, a honey pot is used as a distracter for attackers. This "honey pot" is then used as a sacrificial target.

Explanation B. Incorrect, a signature based attack does not utilize a lure for protection.

Explanation C. Incorrect, an Anomaly-based attack does not utilize a lure for protection.

Explanation D. Incorrect, a Policy-based attack does not utilize a lure for protection.

PrepLogic Question: [11691-211](#)

3. [Review Question](#) p. 60

Answers: B

Explanation A. Incorrect, this method is not considered the primary-method used.

Explanation B. Correct, the signature-based method is considered the primary method used on today's IDS/IPS's.

Explanation C. Incorrect, this method is not considered the primary-method used.

Explanation D. Incorrect, this method is not considered the primary-method used.

PrepLogic Question: [11691-212](#)



4. [Review Question](#) p. 61

Answers: C

Explanation A. Incorrect, the honey-pot method is used as a false target to lure attackers.

Explanation B. Incorrect, a signature-based detection is based on a specific string of bytes which indicate an attack.

Explanation C. Correct, one of the types of anomaly-based detection methods utilizes a baseline which is created over time to indicate abnormal patterns outside the baseline.

Explanation D. Incorrect, a policy-based detection method utilizes a very specific list of traffic policy statements.

PrepLogic Question: [11691-213](#)

5. [Review Question](#) p. 61

Answers: D

Explanation A. Incorrect, NIPS stands for Network-based Intrusion Protection System which CSA is not.

Explanation B. Incorrect, a DMZ is a section of a network which houses front facing networking equipment. CSA is not part of a DMZ.

Explanation C. Incorrect, NIDS stands for Network-based Intrusion Detection System which CSA is not.

Explanation D. Correct, HIPS stands for Host-based Intrusion Protection System which is what CSA is.

PrepLogic Question: [11691-214](#)

6. [Review Question](#) p. 61

Answers: A

Explanation A. Correct, an IPS is a protection system that sits inline in the network and can proactively prevent attacks.

Explanation B. Incorrect, the IDS has the ability to tell IPS's to block traffic as well as other pieces of equipment. An IPS has the ability to block and detect by itself.

Explanation C. Incorrect, an IDS does not have the ability to proactively protect from an attack because it is not inline. It can however catch an attack shortly after it is



launched.

Explanation D. Incorrect, the IPS is used to both detect and protect from attacks. The IDS can also detect attacks and alert several pieces of equipment to take action including an IPS.

PrepLogic Question: [11691-215](#)

7. [Review Question](#) p. 62

Answers: B

Explanation A. Incorrect, a Network-based Intrusion Detection System is limited to traffic it can read if the traffic is encrypted to the host then this traffic would be invisible to the NIDS.

Explanation B. Correct, a Host-based Intrusion Protection System would have the ability to monitor this traffic because the encryption would be stripped off by the time it was read by the HIPS.

Explanation C. Incorrect, there is no such protection system.

Explanation D. Incorrect, a Network-based Intrusion Protection System is limited to traffic it can read if the traffic is encrypted to the host then this traffic would be invisible to the NIPS.

PrepLogic Question: [11691-216](#)

8. [Review Question](#) p. 62

Answers: C, D

Explanation A. Incorrect, while an Ethernet interface may be used it is not needed.

Explanation B. Incorrect, while the sensor may have a loopback interface it is not needed for a network sensor.

Explanation C. Correct, a Command and Control interface is one of the two interfaces which is required on a network sensor.

Explanation D. Correct, a monitoring interface is one of the two interfaces which is required on a network sensor.

PrepLogic Question: [11691-217](#)



9. [Review Question](#) p. 62**Answers: A****Explanation A.** Correct, with inline mode the sensor acts by taking traffic in one port and exiting it back out another.**Explanation B.** Incorrect, in promiscuous mode a copy of all traffic is routed to the port. If the sensor detects an attack then actions are guided.**Explanation C.** Incorrect, there is no such thing as unrestricted sensor operating mode.**Explanation D.** Incorrect, there is no such thing as dual-homed sensor operating mode.PrepLogic Question: [11691-218](#)10. [Review Question](#) p. 63**Answers: B****Explanation A.** Incorrect, with inline mode the sensor acts by taking traffic in one port and exiting it back out another.**Explanation B.** Correct, in promiscuous mode a copy of all traffic is routed to a port. If the sensor detects an attack then actions are guided.**Explanation C.** Incorrect, there is no such thing as restricted sensor operating mode.**Explanation D.** Incorrect, there is no such thing as single-homed sensor operating mode.PrepLogic Question: [11691-219](#)11. [Review Question](#) p. 63**Answers: C****Explanation A.** Incorrect, exploit signatures are used to match specific exploits.**Explanation B.** Incorrect, string signatures look for a specific string inside a traffic stream.**Explanation C.** Correct, connection signatures are programmed to watch for how certain protocols behave and look for abnormalities in this behavior.**Explanation D.** Incorrect, DoS signatures look for a specific sign of DoS attacks.

PrepLogic Question: [11691-220](#)

12. [Review Question](#) p. 63

Answers: D

Explanation A. Incorrect, exploit signatures are used to match specific exploits.

Explanation B. Incorrect, string signatures look for a specific string inside a traffic stream.

Explanation C. Incorrect, connection signatures are programmed to watch for how certain protocols behave and look for abnormalities in this behavior.

Explanation D. Correct, DoS signatures look for a specific sign of DoS attacks. Since DoS attacks function to utilize the resources of piece of network equipment to a point where legitimate traffic can not get through, the way to look for this is through odd patterns in resource consumption.

PrepLogic Question: [11691-221](#)

13. [Review Question](#) p. 64

Answers: A

Explanation A. Correct, the Security Device Event Exchange (SDEE) protocol is used to provide a secure channel between IPS clients and servers.

Explanation B. Incorrect, syslog can be used to relay information between IPS clients and servers but it is not the preferred method.

Explanation C. Incorrect, SNMP is not used to communicate between IPS clients and servers.

Explanation D. Incorrect, SMTP is not used to communicate between IPS clients and servers.

PrepLogic Question: [11691-222](#)

14. [Review Question](#) p. 64

Answers: B

Explanation A. Incorrect, the Signature Definition File is used for this purpose.

Explanation B. Correct, the Signature Definition File is used for this purpose.



Explanation C. Incorrect, the Signature Definition File is used for this purpose.

Explanation D. Incorrect, the Signature Definition File is used for this purpose.

PrepLogic Question: [11691-223](#)

15. [Review Question](#) p. 64

Answers: C

Explanation A. Incorrect, the resetting of the TCP connect is a valid response.

Explanation B. Incorrect, the creation of a log entry is a valid response.

Explanation C. Correct, it is not possible to block only a specific port. However, there is a mechanism to block a specific connection.

Explanation D. Incorrect, the blocking of an attacker's IP address is a valid response. However, it should be noted that you could be potentially blocking a legitimate user's IP address which is being spoofed.

PrepLogic Question: [11691-224](#)

16. [Review Question](#) p. 65

Answers: D

Explanation A. Incorrect, this is not the correct steps to get to the IPS policies wizard.

Explanation B. Incorrect, this is not the correct steps to get to the IPS policies wizard.

Explanation C. Incorrect, this is not the correct steps to get to the IPS policies wizard.

Explanation D. Correct, this is the correct steps to get to the IPS policies wizard.

PrepLogic Question: [11691-225](#)

17. [Review Question](#) p. 67

Answers: A

Explanation A. Correct, these are the correct steps to use to add a new ACL for inbound filtering.

Explanation B. Incorrect, these are not the correct steps to use to add a new ACL for inbound filtering.



Explanation C. Incorrect, these are not the correct steps to use to add a new ACL for inbound filtering.

Explanation D. Incorrect, these are not the correct steps to use to add a new ACL for inbound filtering.

PrepLogic Question: [11691-226](#)

18. [Review Question](#) p. 69

Answers: B

Explanation A. Incorrect, these are not the correct steps to use to edit global engine settings.

Explanation B. Correct, these are the correct steps to use to edit global engine settings.

Explanation C. Incorrect, these are not the correct steps to use to edit global engine settings.

Explanation D. Incorrect, these are not the correct steps to use to edit global engine settings.

PrepLogic Question: [11691-227](#)

19. [Review Question](#) p. 71

Answers: C

Explanation A. Incorrect, these are not the correct steps to add a new signature.

Explanation B. Incorrect, these are not the correct steps to add a new signature.

Explanation C. Correct, these are the correct steps to add a new signature.

Explanation D. Incorrect, these are not the correct steps to add a new signature.

PrepLogic Question: [11691-228](#)

20. [Review Question](#) p. 72

Answers: D

Explanation A. Incorrect, these are not the correct steps to start the IPS migration wizard.

Explanation B. Incorrect, these are not the correct steps to start the IPS migration



wizard.

Explanation C. Incorrect, these are not the correct steps to start the IPS migration wizard.

Explanation D. Correct, these are the correct steps to start the IPS migration wizard.

PrepLogic Question: [11691-229](#)

21. [Review Question](#) p. 73

Answers: A

Explanation A. Correct, these are the correct steps to enable IPS on an interface.

Explanation B. Incorrect, these are not the correct steps to enable IPS on an interface.

Explanation C. Incorrect, these are not the correct steps to enable IPS on an interface.

Explanation D. Incorrect, these are not the correct steps to enable IPS on an interface.

PrepLogic Question: [11691-230](#)

22. [Review Question](#) p. 75

Answers: B

Explanation A. Incorrect, these are not the correct steps to add an event action filter.

Explanation B. Correct, these are the correct steps to add an event action filter.

Explanation C. Incorrect, these are not the correct steps to add an event action filter.

Explanation D. Incorrect, these are not the correct steps to add an event action filter.

PrepLogic Question: [11691-231](#)

23. [Review Question](#) p. 77

Answers: C

Explanation A. Incorrect, these are not the correct steps to add an event action override.

Explanation B. Incorrect, these are not the correct steps to add an event action override.

Explanation C. Correct, these are the correct steps to add an event action override.



Explanation D. Incorrect, these are not the correct steps to add an event action override.

PrepLogic Question: [11691-232](#)



Explanations: Chapter 9

1. [Review Question](#) p. 78

Answers: D

Explanation A. Incorrect, symmetric encryption utilizes one key for encryption and decryption.

Explanation B. Incorrect, this is not a valid encryption type.

Explanation C. Incorrect, this is not a valid encryption type.

Explanation D. Correct, asymmetric encryption uses one key to encrypt and one to decrypt.

PrepLogic Question: [11691-233](#)

2. [Review Question](#) p. 78

Answers: A

Explanation A. Correct, 3DES allows you to use either 112-bit or 156-bit encryption.

Explanation B. Incorrect, AES only allows 128-bit, 192-bit and 256-bit encryption.

Explanation C. Incorrect, DES only provides 56-bit encryption.

Explanation D. Incorrect, MD5 is a hashing function.

PrepLogic Question: [11691-234](#)

3. [Review Question](#) p. 78

Answers: B

Explanation A. Incorrect, block ciphers do utilize fixed-length blocks or sections when encrypting traffic.

Explanation B. Correct, block ciphers are not considered to be more efficient because they require hard block boundaries. Because of this there is always going to be extra bits encrypted and sent.

Explanation C. Incorrect, stream ciphers are generally faster than block ciphers.

Explanation D. Incorrect, block ciphers output is larger because it required hard



boundaries.

PrepLogic Question: [11691-235](#)

4. [Review Question](#) p. 79

Answers: C

Explanation A. Incorrect, ECB is a block cipher mode.

Explanation B. Incorrect, there is no such mode as OSF.

Explanation C. Correct, CFB is a command stream cipher mode.

Explanation D. Incorrect, CBC is a block cipher mode.

PrepLogic Question: [11691-236](#)

5. [Review Question](#) p. 79

Answers: D

Explanation A. Incorrect, CFB is a stream cipher mode.

Explanation B. Incorrect, there is no such block cipher mode.

Explanation C. Incorrect, OFB is a stream cipher mode.

Explanation D. Correct, ECB is one of the two standardized block cipher modes.

PrepLogic Question: [11691-237](#)

6. [Review Question](#) p. 79

Answers: A

Explanation A. Correct, the ECB mode is not considered to be the most secure so it is not recommended.

Explanation B. Incorrect, it is recommended to change your keys frequently.

Explanation C. Incorrect, the CBC mode is considered to be more secure than ECB mode so it is recommended.

Explanation D. Incorrect, it is always recommended that keys not be communicated insecurely.



PrepLogic Question: [11691-238](#)

7. [Review Question](#) p. 80

Answers: B

Explanation A. Incorrect, AES was introduced in IOS version 12.2(13)T.

Explanation B. Correct, AES was introduced in IOS version 12.2(13)T.

Explanation C. Incorrect, AES was introduced in IOS version 12.2(13)T.

Explanation D. Incorrect, AES was introduced in IOS version 12.2(13)T.

PrepLogic Question: [11691-239](#)

8. [Review Question](#) p. 80

Answers: C

Explanation A. Incorrect, Rijndael is the algorithm behind AES.

Explanation B. Incorrect, there is no such algorithm.

Explanation C. Correct, the Signature verification algorithm is one of the three algorithms generally used for digital signatures. The others are the key generation algorithm and the signing algorithm.

Explanation D. Incorrect, there is no such algorithm.

PrepLogic Question: [11691-240](#)

9. [Review Question](#) p. 80

Answers: D

Explanation A. Incorrect, this encryption type is used for asymmetric encryption.

Explanation B. Incorrect, this encryption type is used for asymmetric encryption.

Explanation C. Incorrect, this encryption type is used for asymmetric encryption.

Explanation D. Correct, DES is a symmetric encryption type.

PrepLogic Question: [11691-241](#)



10. [Review Question](#) p. 81**Answers: A****Explanation A.** Correct, this encryption type is used for asymmetric encryption.**Explanation B.** Incorrect, this encryption type is used for symmetric encryption.**Explanation C.** Incorrect, this encryption type is used for symmetric encryption.**Explanation D.** Incorrect, this encryption type is used for symmetric encryption.PrepLogic Question: [11691-242](#)11. [Review Question](#) p. 81**Answers: B****Explanation A.** Incorrect, a X.509 certificate is used for website authentication.**Explanation B.** Correct, a X.509 certificate is not used for wireless security.**Explanation C.** Incorrect, a X.509 certificate is used for IPsec encryption used in VPN's.**Explanation D.** Incorrect, a X.509 certificate is used for client certificates.PrepLogic Question: [11691-243](#)12. [Review Question](#) p. 81**Answers: C****Explanation A.** Incorrect, if any private key is stolen then all information which used this key for security is vulnerable.**Explanation B.** Incorrect, if any private key is stolen then all information which used this key for security is vulnerable.**Explanation C.** Correct, there is no such a thing as a stolen public key because it is simply used to create a message to the key owner and is freely given to people to write secured traffic to the owner.**Explanation D.** Incorrect, the CA being compromised questions the validity of any keys signed by this authority thus making all these keys vulnerable.PrepLogic Question: [11691-244](#)

13. [Review Question](#) p. 82

Answers: D

Explanation A. Incorrect, confidentiality provides encryption which ensures if the traffic is intercepted it cannot be interpreted.

Explanation B. Incorrect, verification is not one of the protections provided.

Explanation C. Incorrect, integrity ensures that the traffic has not been changed in transit.

Explanation D. Correct, authentication provides verification that both parties are who they say they are.

PrepLogic Question: [11691-245](#)

14. [Review Question](#) p. 82

Answers: A

Explanation A. Correct, integrity ensures that the traffic has not been changed in transit.

Explanation B. Incorrect, verification is not one of the protections provided.

Explanation C. Incorrect, confidentiality provides encryption which ensures if the traffic is intercepted it cannot be interpreted.

Explanation D. Incorrect, authentication provides verification that both parties are who they say they are.

PrepLogic Question: [11691-246](#)

15. [Review Question](#) p. 82

Answers: B

Explanation A. Incorrect, quick mode is used to negotiate the parameters for an IPsec session.

Explanation B. Correct, aggressive mode uses three packets to establish a Security Association (SA).

Explanation C. Incorrect, normal mode is not a valid IKE mode.

Explanation D. Incorrect, main mode uses three exchanges to establish a Security Association (SA).



PrepLogic Question: [11691-247](#)

16. [Review Question](#) p. 83

Answers: C

Explanation A. Incorrect, protocol number 51 is used for the Authentication Header (AH) protocol which does not offer encryption.

Explanation B. Incorrect, protocol number 48 is used for the Dynamic Source Routing Protocol.

Explanation C. Correct, protocol number 50 is used for Encapsulating Security Protocol (ESP) which offers encryption.

Explanation D. Incorrect, protocol number 49 is used for the BNA protocol.

PrepLogic Question: [11691-248](#)

17. [Review Question](#) p. 83

Answers: D

Explanation A. Incorrect, MD5 is not the preferred hashing algorithm.

Explanation B. Incorrect, WHIRLPOOL is not the preferred hashing algorithm.

Explanation C. Incorrect, MD6 is not the preferred hashing algorithm.

Explanation D. Correct, SHA is the preferred hashing algorithm.

PrepLogic Question: [11691-249](#)

18. [Review Question](#) p. 84

Answers: A

Explanation A. Correct, an access-list defining what the source and destination networks are to be tunneled is required.

Explanation B. Incorrect, the peer addresses are set correctly.

Explanation C. Incorrect, the configuration should be set between R2 and R3.

Explanation D. Incorrect, the group keyword is used to define the Diffie-Hellman group number and is correct in this configuration.



PrepLogic Question: [11691-250](#)

19. [Review Question](#) p. 85

Answers: B

Explanation A. Incorrect, this command is entered correctly.

Explanation B. Correct, there is an extra word in this command. In this case the ipsec-key is not a keyword but the key itself, so either it would need to be removed or the CiScO word would need to be removed.

Explanation C. Incorrect, the configuration is on the correct routers.

Explanation D. Incorrect, the access-lists are configured in the correct directions.

PrepLogic Question: [11691-251](#)

