



**PASS-GUARANTEED.COM**

**100% Money Back Guarantee!!!**

**Your #1 Certification Training Resource**

Product Details from Pass-Guaranteed.com:

**Securing Networks with Cisco Routers and Switches**

**642-503**

*Demo Version*

*Download Full Version*

*Visit*

<http://www.Pass-Guaranteed.com>

**Complete Certification Training Solutions**



**Practice Exam  
Test Questions**  
Click Here To Learn More  
**Go ->**



**Online Course  
Tutorials**  
with TESTING ENGINE  
**Go ->**



**Study Guides**  
Click Here to Learn More  
About Our Prep Labs  
**Go ->**



**Lab Scenarios**  
Click Here to Learn More  
About Our Prep Labs  
**Go ->**



**Preparation Labs**  
Click Here to Learn More  
About Our Prep Labs  
**Go ->**



**Online  
Testing Engine**  
Click Here To Learn More  
**Go ->**



## **Study Tips**

*This product will provide you with questions and answers carefully compiled and written by our Expert Senior Certified Staff. Our practice questions are designed to help you learn the concepts behind the questions rather than be a strict memorization tool.*

### **Important Note:**

### **Please Read Carefully**

*Repeated readings of our Pass-Guaranteed.com Practice Exam will increase your comprehension. We constantly add to and update our Practice Exams with new questions, answers and explanations, so check that you have the latest version of this Practice Exam before you take your exam.*

*For security purposes, each PDF file is encrypted with a unique serial number associated With your Pass-Guaranteed.com account information. In accordance with International Copyright Law, Pass-Guaranteed.com reserves the right to take legal action against you should we find copies of this PDF file distributed to other parties.*

### **Update Notifications (Latest Version)**

*We are constantly reviewing our products. New material is added and old material is revised. Free Updates are available for 180 days after purchase. If you purchased a bundle, you will have Free Updates for 1 YEAR!*

*You can signup to our newsletter for instant notification whenever an update is released by becoming a Pass-Guaranteed.com member at: <http://www.pass-guaranteed.com/log.htm>*

*By becoming a Pass-Guaranteed.com member, you also get a chance to win a FREE Practice Exam of your choosing. We give away 3 Pass-Guaranteed.com Practice Exams every week to 3 lucky winners.*

### **Pass-Guaranteed.com Product Specials**

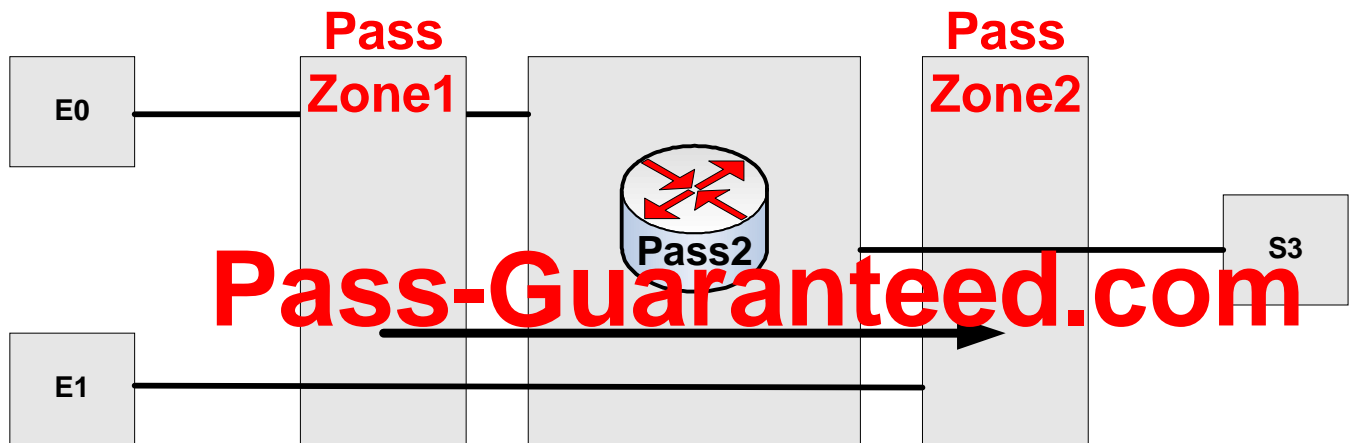
*Pass-Guaranteed.com Custom Bundle Requests, cover all Pass-Guaranteed.com Products!!! You can visit our Special Bundle Discounts from Pass-Guaranteed.com or make your own Custom Bundle Request with Pass-Guaranteed.com here: <http://www.pass-guaranteed.com/bundles.htm>*

***Pass-Guaranteed.com Custom Bundle Request Form let's you create your own Bundle Of Products!!!** You can select and group any of our products for your Custom Bundle and we will give you up to a **50% Discount** on your Custom Bundle Package. This includes our [Practice Test Questions](#), [Online Course Tutorials](#), [Study Guides](#), [Lab Scenarios](#) and our [Certified Online Instructor](#) service.*

*Please visit: <http://www.pass-guaranteed.com/custom-request.htm> If you would like to purchase a Custom Bundle from Pass-Guaranteed.com.*

**QUESTION: 1**

Please study the exhibit carefully.



Which two configuration commands are used to apply an inspect policy map for traffic traversing from the E0 or E1 interface to the S3 interface? (Select TWO).

- A. ip inspect myfwpolicy in
- B. interface E0
- C. ip inspect myfwpolicy out
- D. service-policy type inspect myfwpolicy
- E. zone-pair security test source Z1 destination Z2
- F. policy-map myfwpolicy class class-default inspect

**Answer:** D, E

**QUESTION: 2**

Router Pass1 is being used to prevent Denial of Service attacks on the Pass network.

Which three thresholds does CBAC on the Cisco IOS Firewall provide against DoS attacks? (Select THREE).

- A. The number of half-open sessions based upon time
- B. The total number of half-open TCP or UDP sessions
- C. The number of fully open sessions based upon time
- D. The number of half-open TCP-only sessions per host
- E. The total number of fully open TCP or UDP sessions
- F. The number of fully open TCP-only sessions per host

**Answer:** A, B, D

**Explanation:**

Enhanced denial-of-service detection and prevention defends networks against popular attack modes, such as SYN (synchronize/start) flooding, port scans, and packet injection, by inspecting packet sequence numbers in TCP connections. If numbers are not within expected ranges, the router drops suspicious packets. When the router detects unusually high rates of new connections, it issues an alert message, and subsequently drops half-open TCP connection state tables. This prevents system resource depletion. When the Cisco IOS Firewall detects a possible attack, it tracks user access by source or destination address and port pairs. It also details the transaction, creating an audit trail. The CBAC process can be configured to monitor these half opened sessions based on the total number within a given time frame, the total number at any given point, or the total number per any individual host. When the number of existing half-open sessions exceeds the max-incomplete high number, CBAC deletes half-open sessions as required to accommodate new connection requests. The software continues to delete half-open requests until the number of existing half-open sessions drops below max-incomplete low number.

**Reference:**

[http://www.cisco.com/en/US/products/sw/secursw/ps1018/prod\\_bulletin09186a008010e040.html](http://www.cisco.com/en/US/products/sw/secursw/ps1018/prod_bulletin09186a008010e040.html)

**QUESTION: 3**

Which three of these statements are correct regarding DMVPN configuration? (Select THREE).

- A. The GRE tunnel mode must be set to point-to-point mode:  
tunnel mode gre point-to-point
- B. The GRE tunnel must be associated with an IPsec profile:  
tunnel protection ipsec profile profile-name
- C. At the spoke routers, static NHRP mapping to the hub router is required: ip nhrp map hub-tunnel-ip-address hub-physical-ip-address
- D. The spoke routers must be configured as the NHRP servers:  
ip nhrp nhs spoke-tunnel-ip-address
- E. If running EIGRP over DMVPN, the hub router tunnel interface must have "next hop self" enabled: ip next-hop-self eigrp AS-Number
- F. If running EIGRP over DMVPN, the hub router tunnel interface must have split horizon disabled: no ip split-horizon eigrp AS-Number

**Answer:** B, C, F

**QUESTION: 4**

**DRAG DROP**

You work as a network technician at Pass.com. Your boss, miss Pass, is interested in debug commands which can be used to troubleshoot the WebVPN functions. Match the proper command with appropriate functions. *Note:* not all commands are used.

**Options, select from these**

Debug webvpn webservice	Debug webvpn dns
Debug webvpn port-forward	Debug webvpn aaa

**Definitions**

Users having problems with the ThinClient operations
Users getting unable to connect to server error message when trying to access the Http://www.pass.com url
Users having problems logging into WebVPN

**Options, place here**

Place here
Place here
Place here

**Answer:**

Options, select from these

Debug webvpn webservice

Pass-Guaranteed.com

Definitions

Users having problems with the ThinClient operations

Users getting unable to connect to server error message when trying to access the Http://www.pass.com url

Users having problems logging into WebVPN

Options, place here

Debug webvpn port-forward

Debug webvpn dns

Debug webvpn aaa

Pass-Guaranteed.com

**QUESTION: 5**

The Pass administrator is working on configuring the authentication proxy feature.

Which of the following best describes the authentication proxy feature of the Cisco IOS?

- A. Use a general policy applied across multiple Pass Inc. users
- B. Use a single security policy that is applied to an entire user group or subnet at Pass Inc.
- C. Apply specific security policies on a per-user basis at Pass Inc.
- D. Keep the Pass Inc. user profiles active even where there is no active traffic from the authenticated users.

**Answer: C**

**Explanation:**

The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access was associated with a user's IP address, or a single security policy had to be applied to an entire user group or sub network. Now, users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users.

With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecureACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

**Reference:**

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_configuration\\_guide\\_chapter09186a00800d](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d)

**QUESTION: 6**

Please study the exhibit carefully.

```
appfw policy-name PassPolicy
application http
strict-http action reset alarm
content-length maximum 1 action reset alarm
content-type-verification match-req-rsp action reset alarm
max-header-length request 1 response 1 action reset alarm
max-uri-length 1 action reset alarm
request-method rfc put action reset alarm
transfer-encoding type default action reset alarm
!
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
Interface FastEthernet0/0
ip inspect firewall in
```

What additional configuration is required for the Cisco IOS Firewall to reset the TCP connection if any peer-to-peer, tunneling, or instant messaging traffic is detected over HTTP?

- A. the port-misuse default action reset alarm command in the HTTP application firewall policy configuration
- B. the service default action reset command in the HTTP application firewall policy configuration
- C. the PAM configuration for mapping the peer-to-peer, tunneling, and instant messaging TCP ports to the HTTP application

D. the ip inspect name firewall im, ip inspect name firewall p2p, and ip inspect name firewall tunnel commands

E. class-map configuration for matching peer-to-peer, tunneling, and instant messaging traffic over HTTP, and a policy map specifying the reset action

**Answer:** A

**QUESTION:** 7

You want to increase the security levels at layer 2 within the Pass switched LAN.

Which three are typical Layer 2 attack mitigation techniques? (Select THREE).

- A. Switch security
- B. Port security
- C. ARP snooping
- D. DHCP snooping
- E. Port snooping
- F. 802.1x authentication

**Answer:** B, D, F

**Explanation:**

Network Attack Mitigation:

Use the port security commands to mitigate MAC-spoofing attacks. The port security command provides the capability to specify the MAC address of the system connected to a particular port. The command also provides the ability to specify an action to take if a port-security violation occurs. However, as with the CAM table-overflow attack mitigation, specifying a MAC address on every port is an unmanageable solution. Hold-down timers in the interface configuration menu can be used to mitigate ARP spoofing attacks by setting the length of time an entry will stay in the ARP cache. However, hold-down timers by themselves are insufficient. Modification of the ARP cache expiration time on all end systems would be required as well as static ARP entries. Even in a small network this approach does not scale well. One solution would be to use private VLANs to help mitigate these network attacks. Another solution that can be used to mitigate various ARP-based network exploits is the use of DHCP snooping along with Dynamic ARP Inspection (DAI). These Catalyst feature validate ARP packets in a network and permit the interception, logging, and discarding of ARP packets with invalid MAC address to IP address bindings. DHCP Snooping provides security by filtering trusted DHCP messages and then using these messages to build and maintain a DHCP snooping binding table. DHCP Snooping considers DHCP messages originating from any user facing port that is not a DHCP server port or an uplink to a DHCP server as untrusted. From a DHCP Snooping perspective these untrusted, user-facing ports should not send DHCP server type responses such as DHCP Offer, DHCP Ack, or DHCP Nak. Untrusted DHCP messages are messages received from outside the network or firewall.

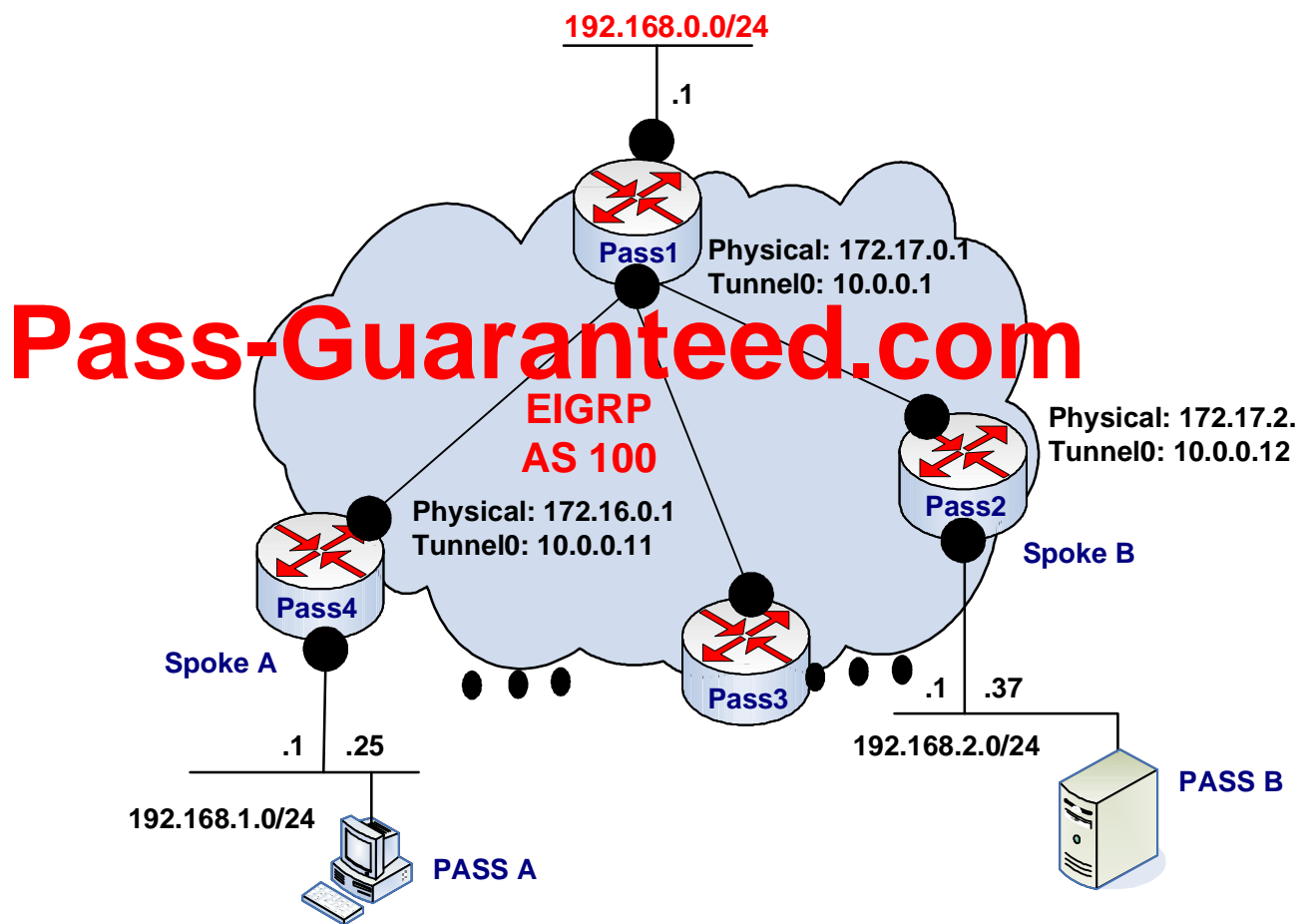
The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information corresponding to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network. The DHCP snooping binding table can contain both dynamic as well as static MAC address to IP address bindings. Another effective mitigation strategy is to deploy 802.1x on access switches and wireless access points to ensure that all access to the network infrastructure requires authentication. Consider deploying PEAP for use with wireless LANs.

**Reference:**

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking\\_solutions\\_white\\_paper09186a0080148](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a0080148)

**QUESTION: 8**

Refer to the DMVPN topology diagram in the exhibit.



Which two statements are correct? (Select TWO).

- A. The hub router Pass1 needs to have EIGRP split horizon disabled.
- B. At the Pass4 router, the next hop to reach the 192.168.0.0/24 network is 172.17.0.1.
- C. The spoke routers Pass2 and Pass4 act as the NHRP servers for resolving the remote spoke physical interface IP address.
- D. At the Pass2, the next hop to reach the 192.168.1.0/24 network is 172.17.0.1.
- E. Before a spoke-to-spoke tunnel can be built, the spoke router needs to send an NHRP query to the hub to resolve the remote spoke router physical interface IP address.
- F. At the Pass4, the next hop to reach the 192.168.2.0/24 network is 10.0.0.1.

**Answer:** A, E

**QUESTION: 9**

Crypto access lists have been configured on a Pass IPSec router.

What are two functions that crypto ACLs perform? (Select TWO).

- A. Bypasses outbound traffic that should be protected by IPSec
- B. Select inbound traffic that should be protected by IPSec
- C. Selects outbound traffic that should be protected by IPSec
- D. Sends outbound traffic that should not be protected by IPSec as clear text
- E. Discards outbound traffic that should not be protected by IPSec
- F. Discards outbound traffic that requires protection by IPSec

**Answer:** C, D

**Explanation:**

Crypto access lists are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto. For example, access lists can be created to protect all IP traffic between Subnet A and Subnet Y or between Host A and Host B. (These access lists are similar to access lists used with the access-group command. With the access-group command, the access-list determines which traffic to forward or block at an interface). The access lists themselves are not specific to IPSec. It is the crypto map entry referencing the specific access list that defines whether IPSec processing is applied to the traffic matching a permit in the access list. For traffic not matching, the packets are to be process normally and forwarded as clear text.

Crypto access lists associated with IPSec crypto map entries have four primary functions:

1. Select outbound traffic to be protected by IPSec (permit = protect).

2. Indicate the data flow to be protected by the new security associations (specified by a single permit entry) when initiating negotiations for IPSec security associations.
3. Process inbound traffic to filter out and discard traffic that should have been protected by IPSec.
4. Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the peer. (Negotiation is only done for ipsec-isakmp crypto map entries.) In order for the peer's request to be accepted during negotiation, the peer must specify a data flow that is "permitted" by a crypto access list associated with an ipsec-isakmp crypto map command entry.

**Reference:**

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/products\\_user\\_guide\\_chapter09186a0080089921.htm](http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_user_guide_chapter09186a0080089921.htm)

**QUESTION: 10**

Select two issues that you should consider when implementing IOS Firewall IDS. (Select TWO).

- A. The memory usage
- B. The number of DMZs
- C. The signature coverage
- D. The number of router interfaces
- E. The signature length

**Answer:** A, C

**Explanation:**

The performance impact of intrusion detection will depend on the configuration of the signatures, the level of traffic on the router, the router platform, and other individual features enabled on the router such as encryption, source route bridging, and so on. Enabling or disabling individual signatures will not alter performance significantly - however, signatures that are configured to use Access Control Lists will have a significant performance impact. Because this router is being used as a security device, no packet will be allowed to bypass the security mechanisms. The IDS process in the Cisco IOS Firewall router sits directly in the packet path and thus will search each packet for signature matches. In some cases, the entire packet will need to be searched, and state information and even application state and awareness must be maintained by the router. For auditing atomic signatures, there is no traffic-dependent memory requirement, but the memory usage should be monitored with IDS. For auditing compound signatures, CBAC allocates memory to maintain the state of each session for each connection. Memory is also allocated for the configuration database and for internal caching.

**Reference:**

***642-503 Demo – Pass-Guaranteed.com***

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800ca](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca)

***642-503 Demo – 100% Money Back Guaranteed!!!***