



642-618^{Q&As}

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

Pass Cisco 642-618 Exam with 100% Guarantee

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

<https://www.lead4pass.com/642-618.html>

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

The Cisco ASA is configured in multiple mode and the security contexts share the same outside physical interface.

Which two packet classification methods can be used by the Cisco ASA to determine which security context to forward the incoming traffic from the outside interface? (Choose two.)

- A. unique interface IP address
- B. unique interface MAC address
- C. routing table lookup
- D. MAC address table lookup
- E. unique global mapped IP addresses

Correct Answer: BE

<http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/contexts.html>

Unique Interfaces

If only one context is associated with the ingress interface, the ASA classifies the packet into that context. In transparent firewall mode, unique interfaces for contexts are required, so this method is used to classify packets at all times.

Unique MAC Addresses

If multiple contexts share an interface, then the classifier uses the interface MAC address. The ASA lets you assign a different MAC address in each context to the same shared interface, whether it is a shared physical interface or a shared

subinterface. By default, shared interfaces do not have unique MAC addresses; the interface uses the physical interface burned-in MAC address in every context. An upstream router cannot route directly to a context without unique MAC

addresses. You can set the MAC addresses manually when you configure each interface (see the "Configuring the MAC Address" section), or you can automatically generate MAC addresses (see the "Automatically Assigning MAC

Addresses to Context Interfaces" section).

NAT Configuration

If you do not have unique MAC addresses, then the classifier intercepts the packet and performs a destination IP address lookup. All other fields are ignored; only the destination IP address is used. To use the destination address for

classification, the classifier must have knowledge about the subnets located behind each security context. The classifier relies on the NAT configuration to determine the subnets in each context. The classifier matches the destination IP

address to either a static command or a global command. In the case of the global command, the classifier does not need a matching nat command or an active NAT session to classify the packet. Whether the packet can communicate with

the destination IP address after classification depends on how you configure NAT and NAT control.

For example, the classifier gains knowledge about subnets 10.10.10.0, 10.20.10.0 and 10.30.10.0 when the context



administrators configure static commands in

each context:

-Context A:

```
static (inside,shared) 10.10.10.0 10.10.10.0 netmask 255.255.255.0
```


-Context B:

```
static (inside,shared) 10.20.10.0 10.20.10.0 netmask 255.255.255.0
```

QUESTION 2

Refer to the exhibit.

```
class-map type inspect ftp match-all ftp-cmd
  match request-command put
policy-map type inspect ftp ftp-insp
  class ftp-cmd
  reset
access-list ftp-acl extended permit tcp any any eq ftp
class-map ftp-cm
  match access-list ftp-acl
policy-map ftp-pm
  class ftp-cm
    inspect ftp strict ftp-insp
service-policy ftp-pm interface outside
```



Which statement about the MPF configuration is true?

- A. Any non-RFC complaint FTP traffic will go through additional deep FTP packet inspections.
- B. FTP traffic must conform to the FTP RFC, and the FTP connection will be dropped if the PUT command is used.
- C. Deep FTP packet inspections will be performed on all TCP inbound and outbound traffic on the outside interface.
- D. The ftp-pm policy-map type should be type inspect.
- E. Due to a configuration error, all FTP connections through the outside interface will not be permitted.

Correct Answer: B



QUESTION 3

Which statement about the default ACL logging behavior of the Cisco ASA is true?


- A. The Cisco ASA generates system message 106023 for each denied packet when a deny ACE is configured.
- B. The Cisco ASA generates system message 106023 for each packet that matched an ACE.
- C. The Cisco ASA generates system message 106100 only for the first packet that matched an ACE.
- D. The Cisco ASA generates system message 106100 for each packet that matched an ACE.
- E. No ACL logging is enabled by default.

Correct Answer: A

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/acl_logging.html#wp1_076483



To configure logging for an ACE, enter the following command:

Command	Purpose
<pre>access-list access_list_name [extended] {deny permit}...[log [[level] [interval secs] disable default]]</pre> <p>Example:</p> <pre>hostname(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7 interval 600</pre>	<p>Configures logging for an ACE.</p> <p>The access-list access_list_name syntax specifies the access list for which you want to configure logging.</p> <p>The extended option adds an ACE.</p> <p>The deny keyword denies a packet if the conditions are matched. Some features do not allow deny ACEs, such as NAT. (See the command documentation for each feature that uses an access list for more information.)</p> <p>The permit keyword permits a packet if the conditions are matched.</p> <p>If you enter the log option without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 seconds). See the following options:</p> <ul style="list-style-type: none">• level—A severity level between 0 and 7. The default is 6.• interval secs—The time interval in seconds between system messages, from 1 to 600. The default is 300. This value is also used as the timeout value for deleting an inactive flow.• disable—Disables all access list logging.• default—Enables logging to message 106023. This setting is the same as having no log option. <p>(See the access-list command in the <i>Cisco Security Appliance Command Reference</i> for more information about )</p>

QUESTION 4

Which feature is not supported on the Cisco ASA 5505 with the Security Plus license?

- A. security contexts
- B. stateless active/standby failover
- C. transparent firewall
- D. threat detection



E. traffic shaping

Correct Answer: A

QUESTION 5

Which option lists the main tasks in the correct order to configure a new Layer 3 and 4 inspection policy on the Cisco ASA appliance using the Cisco ASDM Configuration > Firewall > Service Policy Rules pane?

A. 1. Create a class map to identify which traffic to match.

2.

Create a policy map and apply action(s) to the traffic class(es).

3.

Apply the policy map to an interface or globally using a service policy.

B. 1. Create a service policy rule.

2.

Identify which traffic to match.

3.

Apply action(s) to the traffic.

C. 1. Create a Layer 3 and 4 type inspect policy map.

2.

Create class map(s) within the policy map to identify which traffic to match.

3.

Apply the policy map to an interface or globally using a service policy.

D. 1. Identify which traffic to match.

2.

Apply action(s) to the traffic.

3.

Create a policy map.

4.

Apply the policy map to an interface or globally using a service policy.

Correct Answer: B



http://www.cisco.com/en/US/docs/security/asdm/6_2/user/guide/inspctrl.html#wpxref87867

Choose Configuration > Firewall > Service Policy Rules. Add or edit a service policy rule click the Protocol Inspection tab In the Edit Service Policy Rule > Rule Actions dialog box, Select each inspection type that you want to apply. You can predefine inspect maps in the Configuration > Firewall > Objects > Inspect Maps pane

[642-618 VCE Dumps](#)

[642-618 Practice Test](#)

[642-618 Braindumps](#)



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

Try our product !

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

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

<https://www.lead4pass.com/allproducts>

Need Help

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



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

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.