642-627 Q&As

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

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

https://www.passapply.com/642-627.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Defining the internal zone, external zone, and illegal zone is associated with which Cisco IPS appliance feature?

A. reputation filtering

B. threat detection

C. event action overrides

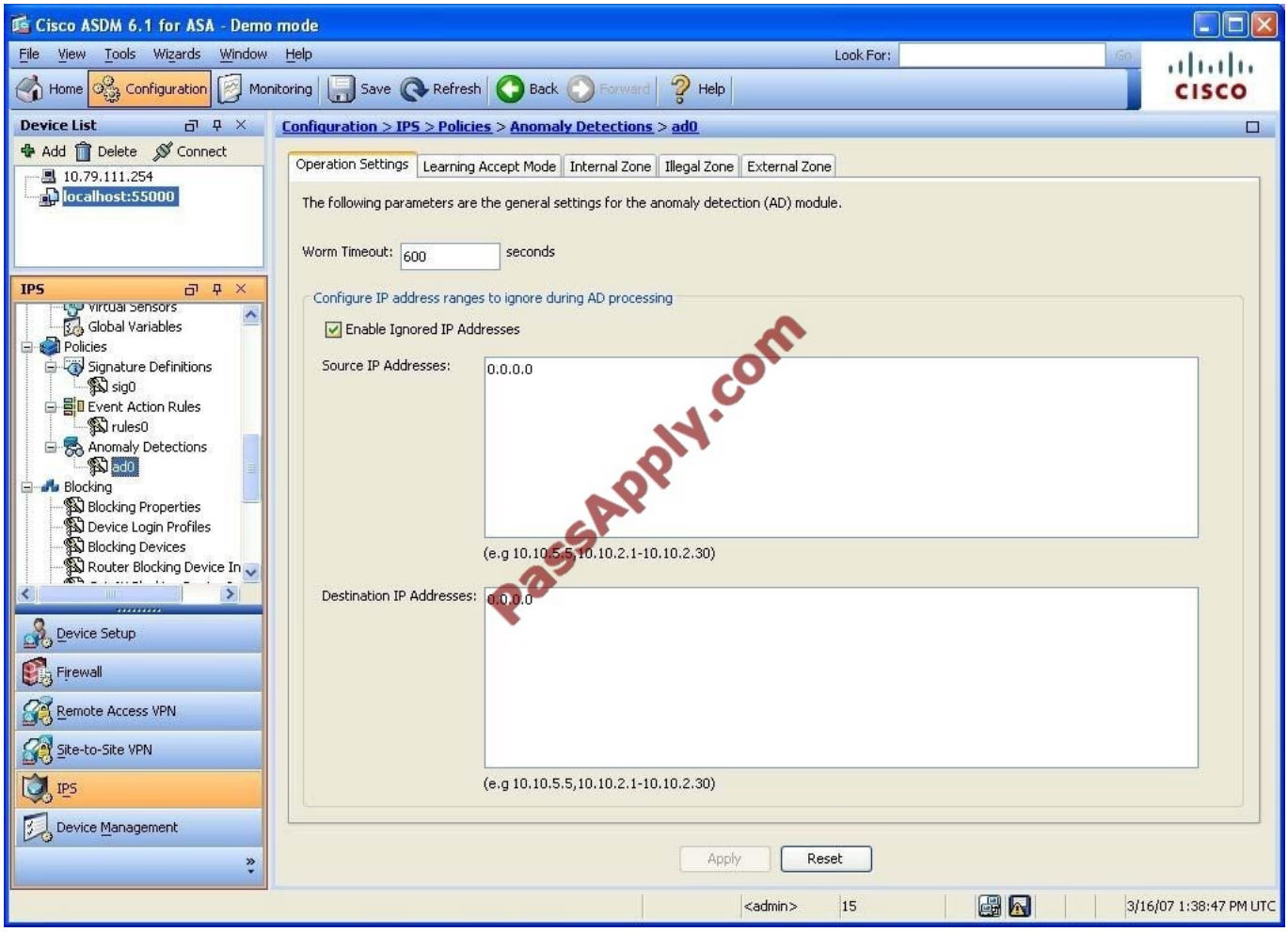
D. global correlation network participation

E. threat rating adjustments

F. anomaly detection

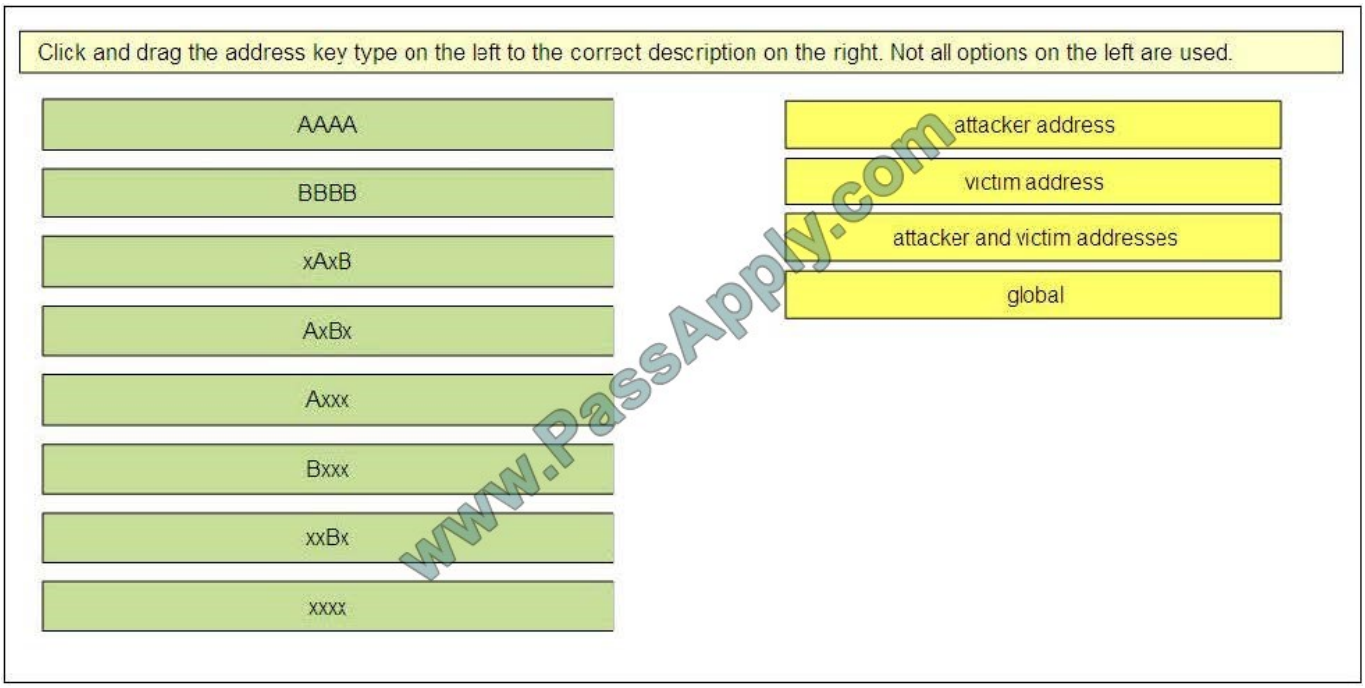
Correct Answer: F

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/cli/cli_anomaly_detection.ht ml#wp1046814

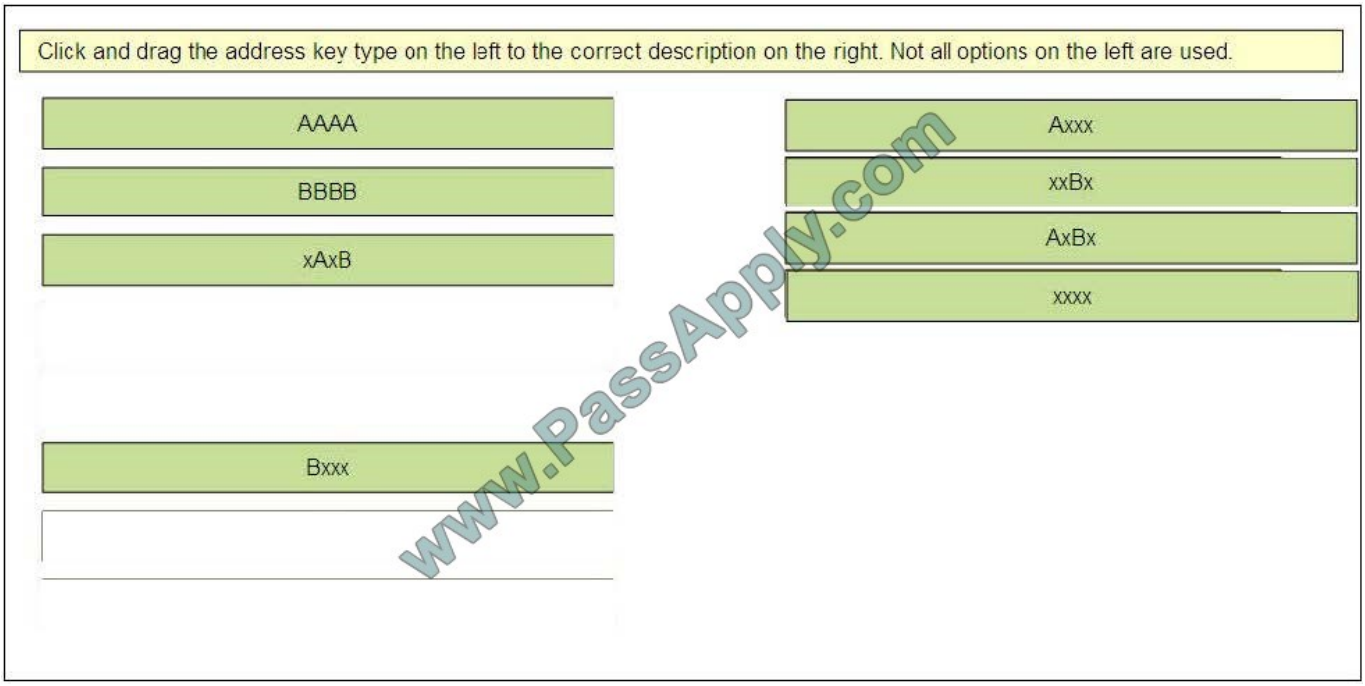


QUESTION 2

Select and Place:



Correct Answer:



QUESTION 3

Which two switching-based mechanisms are used to deploy high availability IPS using multiple Cisco IPS appliances? (Choose two.)

A. Spanning Tree-based HA

B. HSRP-basedHA

C. EtherChannel-based HA

D. VRRP-basedHA

Correct Answer: AC

When network switches are used to provide High Availability you have two options

EtherChannel based HA STP based HA

QUESTION 4

Which IPS alert action is available only in inline mode?

A. produce verbose alert

B. request rate limit

C. reset TCP connection

D. log attacker/victim pair packets

E. deny-packet-inline

F. request block connection

Correct Answer: E

http://www.cisco.com/web/about/security/intelligence/ipsmit.html

Inline Mode Event Actions

The following actions require the device to be deployed in Inline mode and are in affect for a user- configurable default time of 3600 seconds (60 minutes). Deny attacker inline: This action is the most severe and effectively blocks all

communication from the attacking host that passes through the IPS for a specified period of time. Because this event action is severe, administrators are advised to use this only when the probability of false alarms or spoofing is minimal.

Deny attacker service pair inline: This action prevents communication between the attacker IP address and the protected network on the port in which the event was detected. However, the attacker would be able to communicate on another

port that has hosts on the protected network. This event action works well for worms that attack many hosts on the same service port. If an attack occurred on the same host but on another port, this communication would be allowed. This

event action is appropriate when the likelihood of a false alarm or spoofing is minimal. Deny attacker victim pair inline: This action prevents the attacker from communicating with the victim on any port. However, the attacker could

communicate with other hosts, making this action better suited for exploits that target a specific host. This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.

Deny connection inline: This action prevents further communication for the specific TCP flow. This action is appropriate when there is the potential for a false alarm or spoofing and when an administrator wants to prevent the action but not

deny further communication. Deny packet inline: This action prevents the specific offending packet from reaching its intended destination.

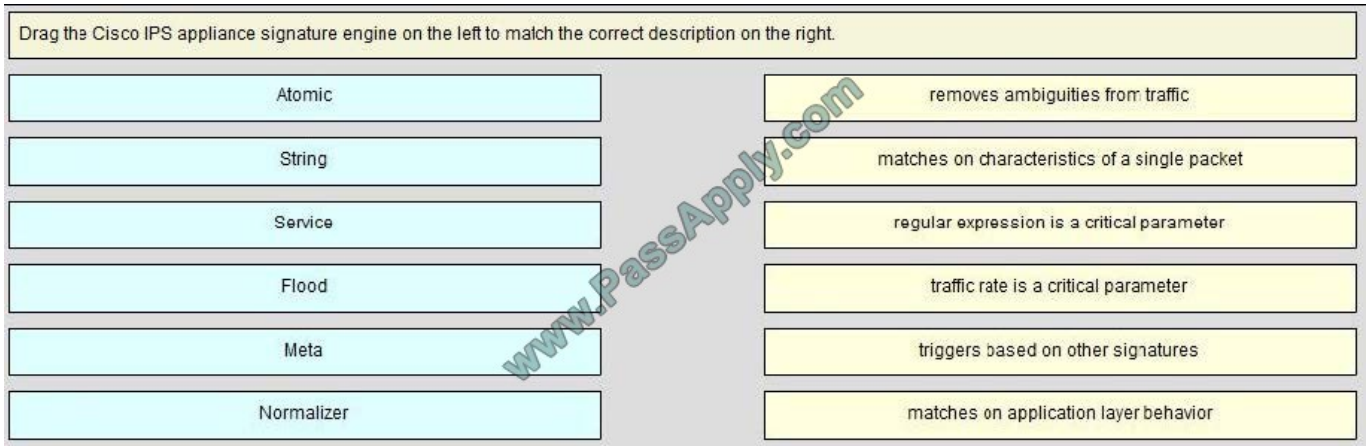
Other communication between the attacker and victim or victim network may still exist. This action is appropriate when there is the potential for a false alarm or spoofing. Note that for this action, the default time has no effect.

Modify packet inline: This action enables the IPS device to modify the offending part of the packet. However, it forwards the modified packet to the destination. This action is appropriate for packet normalization and other anomalies, such as

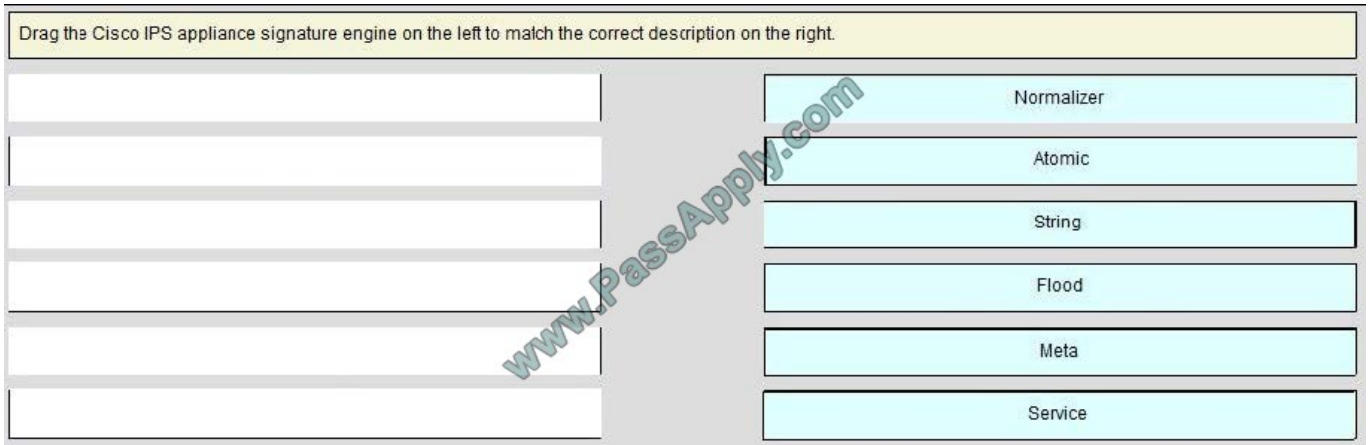
TCP segmentation and IP fragmentation re-ordering.

QUESTION 5

Select and Place:



Correct Answer:



Latest 642-627 Dumps 642-627 Practice Test 642-627 Exam Questions

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.passapply.com/allproducts

Need Help

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