210-260$^{\text{Q\&As}}$

Implementing Cisco Network Security

Pass Cisco 210-260 Exam with 100% Guarantee

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

https://www.passapply.com/210-260.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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which actions can a promiscuous IPS take to mitigate an attack?

A. modifying packets

B. requesting connection blocking

C. denying packets

D. resetting the TCP connection

E. requesting host blocking

F. denying frames

Correct Answer: BDE

Promiscuous Mode Event Actions The following event actions can be deployed in Promiscuous mode. These actions are in affect for a user- configurable default time of 30 minutes. Because the IPS sensor must send the request to another device or craft a packet, latency is associated with these actions and could allow some attacks to be successful. Blocking through usage of the Attack Response Controller (ARC) has the potential benefit of being able to perform to the network edge or at multiple places within the network. Request block host: This event action will send an ARC request to block the host for a specified time frame, preventing any further communication. This is a severe action that is most appropriate when there is minimal chance of a false alarm or spoofing. Request block connection: This action will send an ARC response to block the specific connection. This action is appropriate when there is potential for false alarms or spoofing. Reset TCP connection: This action is TCP specific, and in instances where the attack requires several TCP packets, this can be a successful action. However, in some cases where the attack only needs one packet it may not work as well. Additionally, TCP resets are not very effective with protocols such as SMTP that consistently try to establish new connections, nor are they effective if the reset cannot reach the destination host in time. Event actions can be specified on a per signature basis, or as an event action override (based on risk rating values ?event action override only). In the case of event action override, specific event actions are performed when specific risk rating value conditions are met. Event action overrides offer consistent and simplified management. IPS version 6.0 contains a default event action override with a deny-packet-inline action for events with a risk rating between 90 and 100. For this action to occur, the device must be deployed in Inline mode. Protection from unintended automated action responses Automated event actions can have unintended consequences when not carefully deployed. The most severe consequence can be a self denial of service (DoS) of a host or network. The majority of these unintended consequences can be avoided through the use of Event Action Filters, Never Block Addresses, Network spoofing protections, and device tuning. The following provides an overview of methods used to prevent unintended consequences from occurring. Using Event Action Filters and Never Block By using these capabilities, administrators may prevent a miscreant from spoofing critical IP addresses, causing a self inflicted DoS condition on these critical IP addresses. Note that Never Block capabilities only apply to ARC actions. Actions that are performed inline will still be performed as well as rate limiting if they are configured. Minimize spoofing Administrators can minimize spoofed packets that enter the network through the use of Unicast Reverse Path Forwarding. Administrators can minimize spoofing within their network through the use of IP Source Guard. The white paper titled Understanding Unicast Reverse Path Forwarding provides details on configuration of this feature. More information on IP Source Guard is available in the document titled Configuring DHCP Features and IP Source Guard. Careful Use of Event Actions By judicious use of event actions that block unwanted traffic, such as using the high signature fidelity rating, and not using automated actions on signatures that are easily spoofed, administrators can reduce the probability of an unintended result. For an event to have a high risk rating, it must have a high signature fidelity rating unless the risk rating is artificially increased through the use of Target Value Rating or Watch List Rating, which are IP specific increases. Tuning By tuning the signature set to minimize false positive events, administrators can reduce the chance of an event action that has an unintended consequence. High Base Risk Rating Events In most cases, events with a high base risk rating or a high signature fidelity rating are strong candidates for automated event actions. Care should be taken with protocols that are easily spoofed in order to prevent self DoS conditions.

QUESTION 2

Which IOS command is used to define the authentication key for NTP?

A. Switch(config)#ntp authentication-key 1 md5 C1sc0

B. Switch(config)#ntp trusted-key 1

C. Switch(config)#ntp source 192.168.0.1

D. Switch(config)#ntp authenticate

Correct Answer: A

QUESTION 3

When is the default deny all policy an exception in zone-based firewalls?

A. When traffic traverses two interfaces in in the same zone

B. When traffic terminates on the router via the self zone

C. When traffic sources from the router via the self zone

D. When traffic traverses two interfaces in different zones

Correct Answer: A

QUESTION 4

Which option describes information that must be considered when you apply an access list to a physical interface?

A. Protocol used for filtering

B. Direction of the access class

C. Direction of the access group

D. Direction of the access list

Correct Answer: C

QUESTION 5

Which cisco IOS device support firewall, antispyware, anti-phishing, protection, etc.

A. Cisco IOS router

B. Cisco 4100 IOS IPS appliance

C. Cicso 5500 series ASA D. Cisco 5500x next generation ASA

Correct Answer: D

210-260 VCE Dumps 210-260 Practice Test 210-260 Study Guide

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

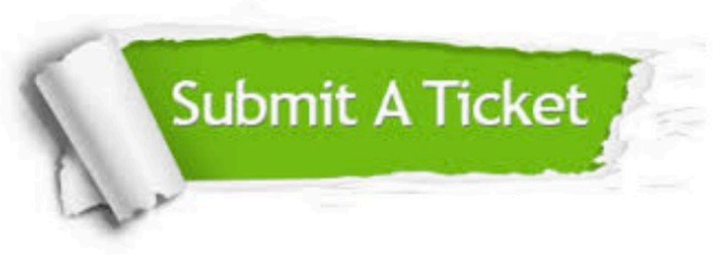
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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:



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.

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.

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.

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