500-285$^{Q\&As}$

Securing Cisco Networks with FireSIGHT Intrusion Prevention System (SSFIPS)

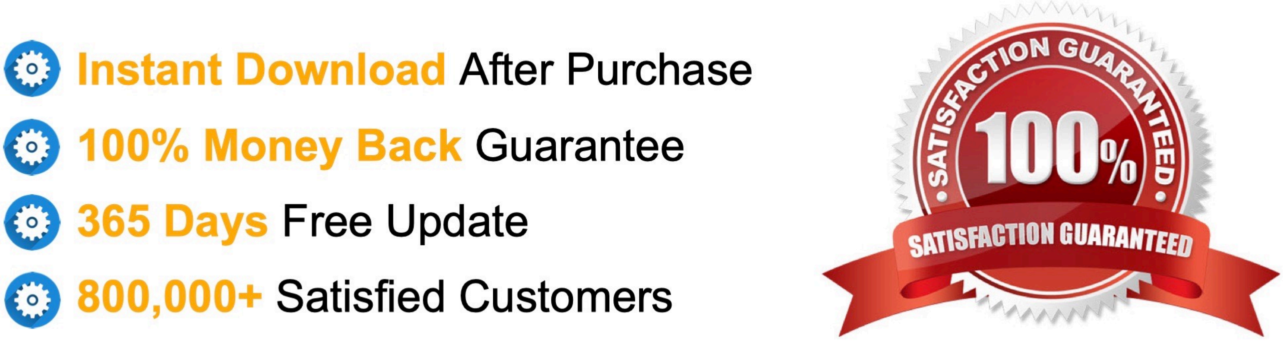
Pass Cisco 500-285 Exam with 100% Guarantee

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

https://www.geekcert.com/500-285.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

A one-to-many type of scan, in which an attacker uses a single host to scan a single port on multiple target hosts, indicates which port scan type?

A. port scan

B. portsweep

C. decoy port scan

D. ACK scan

Correct Answer: B

QUESTION 2

Which interface type allows for bypass mode?

A. inline

B. switched

C. routed

D. grouped

Correct Answer: A

QUESTION 3

When adding source and destination ports in the Ports tab of the access control policy rule editor, which restriction is in place?

A. The protocol is restricted to TCP only.

B. The protocol is restricted to UDP only.

C. The protocol is restricted to TCP or UDP.

D. The protocol is restricted to TCP and UDP.

Correct Answer: C

QUESTION 4

When configuring FireSIGHT detection, an administrator would create a network discovery policy and set the action to "discover". Which option is a possible type of discovery?

A. host

B. IPS event

C. anti-malware

D. networks

Correct Answer: A

QUESTION 5

Which list identifies the possible types of alerts that the Sourcefire System can generate as notification of events or policy violations?

A. logging to database, SMS, SMTP, and SNMP

B. logging to database, SMTP, SNMP, and PCAP

C. logging to database, SNMP, syslog, and email

D. logging to database, PCAP, SMS, and SNMP

Correct Answer: C