300-206^{Q&As}

300-206^{Q&As}

Implementing Cisco Edge Network Security Solutions

Pass Cisco 300-206 Exam with 100% Guarantee

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

https://www.geekcert.com/300-206.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which command change secure HTTP port from 443 to 444?

A. IP http secure-port 444

B. IP http secure-server

C. http server enable 444

D. IP http server-secure

Correct Answer: C

QUESTION 2

Refer to the exhibit. Which command can produce this packet tracer output on a firewall?

```
Phase: 1                                          Phase: 5
Type: ROUTE-LOOKUP                                Type: NAT
Subtype: input                                    Subtype:
Result: ALLOW                                     Result: ALLOW
Config:                                           Config:
Additional Information:                            nat (INSIDE,DMZ) source dynamic 192.168.1.100 1.1.1.1
in   0.0.0.0        0.0.0.0        DMZ            Additional Information:

Phase: 2                                          Phase: 6
Type: ACCESS-LIST                                 Type: ACCESS-LIST
Subtype: log                                      Subtype: log
Result: ALLOW                                     Result: ALLOW
Config:                                           Config:
access-group INSIDE_IN in interface INSIDE        access-group DMZ_LEAVING out interface DMZ
access-list INSIDE_IN extended permit tcp host 192.168.1.100 any  access-list DMZ_LEAVING extended permit tcp host 192.168.1.100 any
Additional Information:                            Additional Information:

Phase: 3                                          Phase: 7
Type: CONN-SETTINGS                               Type: IP-OPTIONS
Subtype:                                          Subtype:
Result: ALLOW                                     Result: ALLOW
Config:                                           Config:
class-map classdefault                            Additional Information:
  match any
policy-map global_policy                          Phase: 8
  class classdefault                              Type: FLOW-CREATION
    set connection decrement-ttl                  Subtype:
service-policy global_policy global               Result: ALLOW
Additional Information:                            Config:
                                                  Additional Information:
Phase: 4
Type: IP-OPTIONS                                  Result:
Subtype:                                          input-interface: INSIDE
Result: ALLOW                                     input-status: up
Config:                                           input-line-status: up
Additional Information:                            output-interface: DMZ
                                                  output-status: up
                                                  output-line-status: up
                                                  Action: allow
```

A. packet-tracer input INSIDE tcp 192.168.1.100 88 192.168.2.200 3028

B. packet-tracer output INSIDE tcp 192.168.1.100 88 192.168.2.200 3028

C. packet-tracer input INSIDE tcp 192.168.2.200 3028 192.168.1.100 88

D. packet-tracer output INSIDE tcp 192.168.2.200 3028 192.168.1.100 88

Correct Answer: A

QUESTION 3

Which utility can you use to troubleshoot and determine the timeline of packet changes in a data path within a Cisco firewall?

A. packet tracer

B. ping

C. traceroute

D. SNMP walk

Correct Answer: A

QUESTION 4

You are going to add ASA to CSM (Cisco Security Manager). Which port on ASA must be reachable for CSM to succeed?

A. 21

B. 22

C. 80

D. 443

Correct Answer: D

Security Manager can use these transport protocols:

SSL (HTTPS)--Secure Socket Layer, which is an HTTPS connection, is the only transport protocol used with PIX Firewalls, Adaptive Security Appliances (ASA), and Firewall Services Modules (FWSM). It is also the default protocol for IPS

devices and for routers running Cisco IOS Software release 12.3 or higher.

If you use SSL as the transport protocol on Cisco IOS routers, you must also configure SSH on the routers. Security Manager uses SSH connections to handle interactive command deployments during SSL deployments. Cisco Security

Manager was using OpenSSL for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. Beginning with version 4.13, Cisco Security Manager replaced OpenSSL version 1.0.2 with Cisco SSL version 6.x. Cisco SSL

enables FIPS compliance over full FIPS Validation which results in fast and cost-effective connectivity. The Common Criteria mode in Cisco SSL allows easier compliance. Cisco SSL is feature-forward when compared to OpenSSL. The

product Security Baseline (PSB) requirements for Cisco SSL ensures important security aspects such as credential and key management, cryptography standards, antispoofing capabilities, integrity and tamper protection, and session, data,

and stream management and administration are taken care of.

SSH--Secure Shell is the default transport protocol for Catalyst switches and Catalyst 6500/7600 devices. You can also use it with Cisco IOS routers.

Telnet--Telnet is the default protocol for routers running Cisco IOS software releases 12.1 and

12.2. You can also use it with Catalyst switches, Catalyst 6500/7600 devices, and routers running Cisco IOS Software release 12.3 and higher. See the Cisco IOS software documentation for configuring Telnet.

HTTP--You can use HTTP instead of HTTPS (SSL) with IPS devices. HTTP is not the default protocol for any device type.

TMS--Token Management Server is treated like a transport protocol in Security Manager, but it is not a real transport protocol. Instead, by configuring TMS as the transport protocol of a router, you are telling Security Manager to deploy

configurations to a TMS. From the TMS, you can download the configuration to an eToken, plug the eToken into the router\\'s USB bus, and update the configuration. TMS is available only for certain routers running Cisco IOS Software 12.3 or

higher.

Security Manager can also use indirect methods to deploy configurations to devices, staging the configuration on a server that manages the deployment to the devices. These indirect methods also allow you to use dynamic IP addresses on

your devices. The methods are not treated as transport protocols, but as adjuncts to the transport protocol for the device. You can use these indirect methods:

AUS (Auto Update Server)--When you add a device to Security Manager, you can select the AUS server that is managing it. You can use AUS with PIX Firewalls and ASA devices.

Configuration Engine--When you add a router to Security Manager, you can select the Configuration Engine that is managing it.

QUESTION 5

Which option is a valid action for a port security violation ?

A. Restrict

B. Reject

C. Disable

D. Reset

Correct Answer: A

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
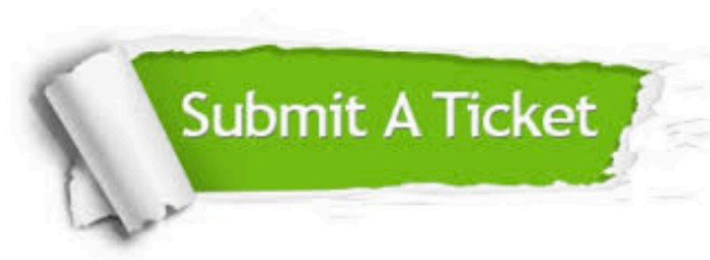Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.geekcert.com/allproducts

Need Help

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