

Comprehensive questions and answers about 2B0-104 exam

2B0-104 exam questions accompanied by exhibits

Verified Answers Researched by Industry Experts and almost 100% correct

2B0-104 exam questions updated on regular basis

Same type as the certification exams, 2B0-104 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free 2B0-104 exam demo before you decide to buy it in Test-Inside.com.

Note: This pdf demo do not include the question's picture.

Exam : Enterasys Networks 2B0-104

Title : Enterasys Certified Internetworking Engineer(ECIE)

1. Which of the following services, as defined by demo.pmd in NetSight Policy Manager, protects the network from a user masquerading as a valid service on the network?

- A. Deny Unsupported Protocol Access service
- B. Deny Spoofing & other Administrative Protocols service
- C. Application Provisioning AUP service
- D. Limit Exposure to DoS Attacks service

Answer: B

2. The following components are mandatory for dynamic policy deployment on the network:

- A. NetSight Policy Manager and policy-capable devices
- B. NetSight Policy Manager, policy-capable devices, and authentication services
- C. NetSight Policy Manager and any device
- D. NetSight Policy Manager only

Answer: B

3. Which of the following services, as defined by demo.pmd in NetSight Policy Manager, reduces network congestion by removing legacy protocols from the network such as IPX?

- A. Deny Unsupported Protocol Access service
- B. Deny Spoofing & other Administrative Protocols service
- C. Threat Management service
- D. Limit Exposure to DoS Attacks service

Answer: A

4. Fill in the blank. It is necessary to _____ policy configuration changes to the switches in NetSight Policy Manager before the changes can take effect.

- A. Mediate
- B. Enforce
- C. Compile
- D. Encrypt

Answer: B

5. As defined in NetSight Policy Managers demo.pmd file, the Secure Guest Access Service Group:

- A. Allows PPTP and HTTP traffic only, and discards all other traffic
- B. Allows HTTP, DNS, and DHCP traffic only, and discards all other traffic
- C. Allows PPTP, HTTP, DNS, and DHCP traffic, and denies access to all other TCP/UDP ports and unsupported protocols on the network
- D. Discards all traffic

Answer: C

6. A new policy role, Staff, is created under the Roles tab in NetSight Policy Manager. To use the Staff policy role to classify ingress traffic for static policy deployment, the network administrator must at a minimum:

- A. Do nothing else. Once the Staff policy role is created in NetSight Policy Manager, the network begins classifying traffic according to the configuration of Staff
- B. Enforce NetSight Policy Managers policy configuration to policy-capable devices only
- C. Enforce NetSight Policy Managers policy configuration to policy-capable devices and also assign the Staff policy role to a port
- D. Enforce NetSight Policy Managers policy configuration to policy-capable devices, assign the Staff policy role to a port, and enable authentication on the port.

Answer: C

7. A new virus has been identified on the Internet causing an infected system to listen to TCP port X for allowing remote connections to the infected device. If a network administrator desires to prevent infected devices from being further exploited within the enterprise network, the network administrator should configure and enforce policy for infected devices to the Active Edge of the network that:

- A. Discards traffic destined to TCP port X
- B. Discards traffic sourced from TCP port X
- C. Prioritizes traffic destined or sourced to TCP port X to a low priority
- D. Rate limit traffic destined or sourced to TCP port X

Answer: B

8. A new virus has been identified on the Internet causing an infected system to listen to TCP port X for allowing remote connections to the infected device. If a network administrator desires to prevent an internal user from connecting to an infected device, the network administrator should configure and enforce policy for malicious users to the Active Edge of the network that:

- A. Discards traffic destined to TCP port X
- B. Discards traffic sourced from TCP port X
- C. Prioritizes traffic destined or sourced to TCP port X to a low priority
- D. Rate limit traffic destined or sourced to TCP port X

Answer: A

9. Which of the following services, as defined by demo.pmd in NetSight Policy Manager, protects the network from Denial of Service attacks on the network?

- A. Deny Unsupported Protocol Access service
- B. Deny DoS Attacks service
- C. Limit Exposure to DoS Attacks service
- D. Application Provisioning - AUP service

Answer: C

10. An Acceptable Use Policy for the network should define:

- A. Which types of traffic trusted users only are allowed to generate on the network
- B. Which types of traffic untrusted users only are allowed to generate on the network
- C. Which types of traffic trusted and untrusted users are allowed to generate on the network
- D. Which types of traffic guest users only are allowed to generate on the network

Answer: C

11. In a multi-vendor environment where 3rd party devices are located at the edge of the network and are not policy-capable, installing a policy-capable device in the distribution layer:

- A. Protects the network core from internally sourced attacks
- B. Protects the server farm from internally sourced attacks
- C. Secures other access layer segments connected through the policy-capable distribution layer device
- D. All of the above

Answer: D

12. As defined in NetSight Policy Managers demo.pmd file, the Guest Access policy role is associated to:

- A. No services
- B. The Deny Spoofing & Other Administrative Protocols service only
- C. The Deny Unsupported Protocol Access service only
- D. All services grouped under the Secure Guest Access service group

Answer: D

13. Which of the following is not a pre-defined Port Group in NetSight Policy Manager to:

- A. All ports
- B. Authenticated ports
- C. Logical ports
- D. CDP ports

Answer: B

14. The RADIUS Filter-ID parameter is used to:

- A. Authenticate users
- B. Authenticate a RADIUS client
- C. Pass policy information to a switch to authorize an authenticated user with a level of network access
- D. Discard traffic destined for a RADIUS server

Answer: C

15. In a multi-vendor environment, where is the placement of a policy capable device most effective in discarding malicious traffic and protecting the entire network:

- A. At the access layer edge
- B. At the distribution layer
- C. In the DMZ
- D. In the core

Answer: A

[**More 2B0-104 Information**](#)

Related 2B0-104 Exams

[2B0-012](#) *ES Switching Edition 4.0*

[2B0-011](#) *ES Router Configuration*

[2B0-100](#) *Enterasys Systems Engineer (ESE) Recertification*

[2B0-021](#) *ES XSR Configuration*

[2B0-015](#) *ES Wireless*

[2B0-019](#) *ES Policy Enabled Networking*

[2B0-102](#) *Enterasys Security Systems Engineer-Defense*

[2B0-024](#) *ES Secure Networks*

[2B0-104](#) *Enterasys Certified Internetworking Engineer(ECIE)*

[2B0-020](#) *ES NetSight Atlas*

[2B0-101](#) *Enterasys Security Systems Engineer (ESSE) Recertification*

[2B0-022](#) *ES XSR Security*

[2B0-103](#) *Enterasys Security Systems Engineer-NAC*

[2B0-018](#) *ES Dragon IDS*

[2B0-023](#) *ES Advanced Dragon IDS*

Other Enterasys Networks Exams

<u>2B0-104</u>	<u>2B0-012</u>	<u>2B0-023</u>	<u>2B0-102</u>	<u>2B0-021</u>	<u>2B0-020</u>	<u>2B0-101</u>	<u>2B0-103</u>
<u>2B0-100</u>	<u>2B0-018</u>	<u>2B0-011</u>	<u>2B0-024</u>	<u>2B0-015</u>	<u>2B0-022</u>	<u>2B0-019</u>	