Testpassport問題集

更に上のクオリティ　更に上のサービス

一年で無料進級することに提供する

Http://www.testpassport.jp

Exam : **2B0-104**

Title : Enterasys Certified Internetworking Engineer(ECIE)

Version : Demo

1. 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

2. 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

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. In a multi-vendor environment where 3 rd 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

5. 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

6. 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

7. 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

8. 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

9. 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

10. 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