Exam Code: 2B0-019

Exam Name: ES Policy Enabled Networking

Vendor: Enterasys Networks

Version: DEMO

Part: A

1: Authentication is used in Secure Application Provisioning to:

A.Quarantine malicious traffic

B.Persistently apply policy

C.Allow configuration of a switch's host data port

D.provide additional network access

Correct Answers: D

2: Saving a NetSight Atlas Policy Manager configuration to a .pmd file:

A.Writes the configuration to NVRAM on the switches

B.Allows for multiple configurations to be stored on the NMS

C.Notifies the RADIUS server that new policies have been created

D.Temporarily disables communication between all RADIUS clients until the save is complete

Correct Answers: B

3: Certificate services must be installed when using:

A.EAP-TLS

B.EAP-MD5

C.PWA

D.MAC authentication

Correct Answers: A

4: Persistent policy assignment:

A.Can be effective in an incremental deployment of acceptable use policy

B.Is dependent upon a RADIUS back-end configuration

C.Is deployed based on user authentication

D.Cannot be used on uplink ports

Correct Answers: A

5: A distinguishing characteristic of PEAP is:

A.It adds security by running over a VPN tunnel

B.It uses salt encryption

C.It requires that only the supplicant present a certificate

D.It creates keying material using the Pseudo-Random Function

Correct Answers: D

6: In the Enterasys policy-enabled network model, on-demand policy assignment:

A.Is the result of a manual configuration

B.Makes use of the Filter-ID parameter

C.Is overridden by a ports default role

D.Requires the use of 802.1X authentication mechanisms

Correct Answers: B

7: All of the following are services which make up the pre-configured Acceptable Use Policy service group EXCEPT:
A.Deny Spoofing
B.Permit Legacy Protocols
C.Limit Exposure to DoS attacks
D.Protocol Priority Access Control
Correct Answers: B

8: After configuration changes have been made in NetSight Atlas Policy Manager, what must be done before the changes take effect on the devices?
A.The NMS must be rebooted
B.The changes must be enforced
C.The changes must be verified
D.Nothing the changes take effect immediately
Correct Answers: B

9: In the three-level policy model, Enterasys maps:
A.The business/network level to classification rules
B.The service-provisioning level to roles
C.The device level to classification rules
D.All of the above
Correct Answers: C

10: The Active Edge consists of:
A.Policy-enabled switches
B.Core routers
C.SAP servers
D.User resources
Correct Answers: A

11: EAP-TLS:
A.Utilizes uni-directional authentication
B.Generates keying material for use in WEP encryption
C.Does not require a Public Key Infrastructure
D.Is regarded as a weak authentication method
Correct Answers: B

12: The Enforce function in NetSight Atlas Policy Manager:
A.Provides system-level administration
B.Writes information to a switchs flash memory
C.Takes place automatically when the application is closed
D.Is used to save .pmd file information
Correct Answers: A

13: Populating NetSight Atlas Policy Managers device list:
A.Is accomplished using the applications discovery function
B.Can be accomplished by reading information from a .csv file
C.Allows the user to input a manually-created list of addresses
D.Can be automated by first running the MAC Locator utility
Correct Answers: C

14: Acceptable Use Policy:
A.Is based on VLAN membership
B.Should reflect the formal network security policy
C.Requires the use of an authentication method
D.Prevents users from sharing information
Correct Answers: B

15: Enterasys Secure Guest Access solution:
A.Provides guest access without compromising security
B.Prevents guests from seeing each others traffic
C.Allows only specifically-defined protocols
D.All of the above
Correct Answers: D

16: When potentially damaging traffic is introduced at the network edge:
A.Classification rules which discard the unwanted traffic can be pushed to the edge switches quickly
B.A new .pmd file must be opened and enforced to each device in the active edge
C.Policy Manager must contact an IDS in order to determine the source IP address of the malicious traffic
D.(a) and (c)
Correct Answers: A

17: Key elements of a common policy architecture include:
A.A policy decision point
B.A policy enforcement point
C.A policy termination point
D.Both (a) and (b)
Correct Answers: D

18: Classification rules may be written based on all of the following EXCEPT:
A.TCP/UDP port number
B.Logical address
C.PHY and PMD sub-layers
D.Hardware address
Correct Answers: C

19: The RoamAbout R2 WAP supports policy-enabled networking:
A.By mapping MAC addresses to virtual ports
B.By forwarding unauthorized traffic to a Discard VLAN
C.Regardless of firmware version
D.By assigning the same policy to all authenticated users
Correct Answers: A

20: The traditional approach to Secure Guest Access has been:
A.Protocol-based containment
B.Based on Application Level Gateways
C.VLAN containment
D.To control access using Layer 4 classification rules
Correct Answers: C