Exam Code: 642-566

Exam Name: Security Solutions for Systems Engineers

Vendor: CISCO

Version: DEMO

Part: A

1: Which essential element is needed to perform events analysis and correlation?

A.elimination of all the true positive events

B.implementation of the same IPS and firewall policies throughout the network

C.time synchronization between all the devices

D.implementation of a centralized provisioning system, such as Cisco Security Manager

E.implementation of different security controls and platforms when using the defense-in-depth approach

Correct Answers: C

2: Which two Cisco products can be used to provide a captive portal to authenticate wireless users? (Choose two.)

A.Cisco Secure ACS

B.WLAN Controller

C.Cisco NAC Guest Server

D.Cisco NAC Profiler

E.Cisco ASA

Correct Answers: B C

3: What is implemented on Cisco IP Phones so that they can authenticate itself before gaining network access?

A.Cisco Secure Services Client

B.Cisco NAC Appliance Agent (NAA)

C.IEEE 802.1X supplicant

D.AAA client

E.Cisco Security Agent

F.one-time password

Correct Answers: C

4: Which platform has the highest IPsec throughput and can support the highest number of tunnels?

A.Cisco 3845 with AIM-VPN/SSL-3

B.Cisco 7200 NPE-GE+VSA

C.Cisco 7200 NPE-GE+VAM2+

D.Cisco ASR 1000-5G

E.Cisco 6500/7600 + VPN SPA

F.Cisco ASA 5580

Correct Answers: E

5: Which three security components can be found in today's typical single-tier firewall system? (Choose three.)

A.Stateful Packet Filtering with Application Inspection and Control

B.IPS

C.Network Admission Control

D.application proxy

E.cache engine

F.server load balancing

Correct Answers: A B D

6: When SSL uses TCP encapsulation on Cisco SSL VPNs, the user's TCP session is transported over another TCP session, thus making flow control inefficient if a packet is lost. Which solution solves this problem?
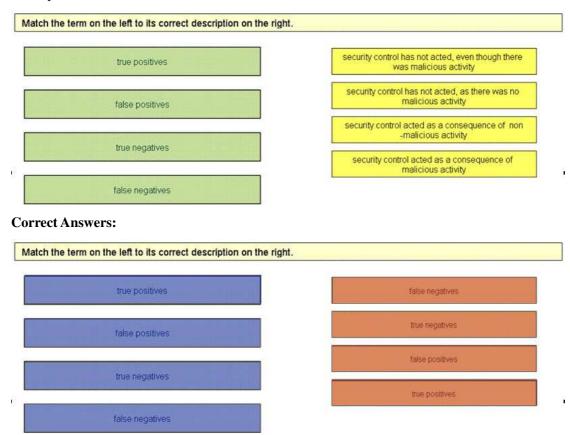
A.smart tunnel

B.application plug-ins

C.DTLS

D.Cisco Secure Desktop

E.DAP

F.SSL traversal

Correct Answers: C

7: Drop

Match the term on the left to its correct description on the right.

true positives		security control has not acted, even though there was malicious activity
false positives		security control has not acted, as there was no malicious activity
true negatives		security control acted as a consequence of non-malicious activity
false negatives		security control acted as a consequence of malicious activity

Correct Answers:

Match the term on the left to its correct description on the right.

true positives		false negatives
false positives		true negatives
true negatives		false positives
false negatives		true positives

8: Which Cisco software agent uses content scanning to identify sensitive content and controls the transfer of sensitive content off the local endpoint over removable storage, locally or network-attached hardware, or network applications?

A.Cisco Trust Agent 2.0

B.Cisco NAC Appliance Agent 4.1.3
C.Cisco NAC Appliance Web Agent 1.0
D.Cisco Security Agent 6.0
E.Cisco IronPort Agent 3.0
Correct Answers: D

9: Which statement regarding the hybrid user authentication model for remote-access IPsec VPNs is correct?
A.VPN servers authenticate by using pre-shared keys, and users authenticate by using usernames and passwords.
B.VPN servers authenticate by using digital certificates, and users authenticate by using usernames and passwords.
C.VPN servers authenticate by using digital certificates, and users authenticate by using pre-shared keys.
D.VPN servers and users authenticate by using digital certificates.
E.VPN servers and users authenticate by using pre-shared keys.
Correct Answers: B

10: Which Cisco ASA's Unified Communications proxy feature manipulates both the signaling and the media channels?
A.TLS Proxy
B.H.323 Proxy
C.SIP Proxy
D.Phone Proxy
E.CUMA Proxy
Correct Answers: D