

Cisco 642-566

**642-566 Security Solutions for Systems Engineers
(SSSE)**

Practice Test

Version 3.10

QUESTION NO: 1

You are the network consultant from Your company. Please point out two requirements call for the deployment of 802.1X.

- A. Authenticate users on switch or wireless ports
- B. Grant or Deny network access at the port level, based on configured authorization policies
- C. Allow network access during the quiet period
- D. Verify security posture using TACAS+

Answer: A,B

QUESTION NO: 2

Open Shortest Path First (OSPF) is a dynamic routing protocol for use in Internet Protocol (IP) networks. An OSPF router on the network is running at an abnormally high CPU rate. By use of different OSPF debug commands on Router, the network administrator determines that router is receiving many OSPF link state packets from an unknown OSPF neighbor, thus forcing many OSPF path recalculations and affecting router's CPU usage. Which OSPF configuration should the administrator enable to prevent this kind of attack on the Router?

- A. Multi-Area OSPF
- B. OSPF stub Area
- C. OSPF MD5 Authentication
- D. OSPF not-so-stubby Area

Answer: C

QUESTION NO: 3

Which one of the following Cisco Security Management products is able to perform (syslog) events normalization?

- A. Cisco IME
- B. Cisco Security Manager
- C. Cisco ASDM
- D. Cisco Security MARS

Answer: D

QUESTION NO: 4

Can you tell me which one of the following platforms has the highest IPSec throughput and can support the highest number of tunnels?

- A. Cisco 6500/7600 + VPN SPA
- B. Cisco ASR 1000-5G
- C. Cisco 7200 NPE-GE+VSA
- D. Cisco 7200 NPE-GE+VAM2+

Answer: A

QUESTION NO: 5

Which two methods can be used to perform IPSec peer authentication? (Choose two.)

- A. One-time Password
- B. AAA
- C. Pre-shared key
- D. Digital Certificate

Answer: C,D

QUESTION NO: 6

Cisco Security Agent is the first endpoint security solution that combines zero-update attack protection, data loss prevention and signature-based antivirus in a single agent. This unique blend of capabilities defends servers and desktops against sophisticated day-zero attacks and enforces acceptable-use and compliance policies within a simple management infrastructure. What are three functions of CSA in helping to secure customer environments?

- A. Control of executable content
- B. Identification of vulnerabilities
- C. Application Control
- D. System hardening

Answer: A,C,D

QUESTION NO: 7

Cisco Secure Access Control Server (ACS) is an access policy control platform that helps you comply with growing regulatory and corporate requirements. Which three of these items are features of the Cisco Secure Access Control Server?

- A. NDS
- B. RSA Certificates
- C. LDAP
- D. Kerberos

Answer: A,B,C

QUESTION NO: 8

Observe the following protocols carefully, which one is used to allow the utilization of Cisco Wide Area Application Engines or Cisco IronPort S-Series web security appliances to localize web traffic patterns in the network and to enable the local fulfillment of content requests?

- A. TLS
- B. DTLS
- C. WCCP
- D. HTTPS

Answer: C

QUESTION NO: 9

Which one is not the factor that can affect the risk rating of an IPS alert?

- A. Relevance
- B. Attacker location
- C. Event severity
- D. Signature fidelity

Answer: B

QUESTION NO: 10

For the following items, which two are differences between symmetric and asymmetric encryption algorithms? (Choose two.)

- A. Asymmetric encryption is slower than symmetric encryption
- B. Asymmetric encryption is more suitable than symmetric encryption for real-time bulk encryption
- C. Symmetric encryption is used in digital signatures and asymmetric encryption is used in HMACs
- D. Asymmetric encryption requires a much larger key size to achieve the same level of protection as symmetric encryption

Answer: A,D

QUESTION NO: 11

Deploying the NAC appliance in in-band mode is better than out-of-band mode. Why?

- A. Nessus scanning
- B. Higher number of users per NAC Appliance
- C. Bandwidth enforcement policy
- D. NAC Appliance Agent deployment

Answer: C

QUESTION NO: 12

IPSec-based site-to-site VPNs is better than traditional WAN networks what?

- A. Delay guarantees, span, performance, security and low cost
- B. Bandwidth guarantees, support for non-IP protocols, scalability and modular design guidelines
- C. Bandwidth guarantees, flexibility, security and low cost
- D. Span, flexibility, security and low cost

Answer: D

QUESTION NO: 13

Which VPN technology can not be used over the internet?

- A. VTI
- B. GRE overIPsec
- C. IPsec direct encapsulation
- D. GET VPN

Answer: D

QUESTION NO: 14 DRAG DROP

Match each IKE component to its supported option:

Options, select from these

IKE authentication	IKE data authentication/integrity
IKE key negotiation	IKE encryption

Definitions

DH Group 1,2 or 5
MD5 or SHA-1
3DES or AES
Pre-shared key or digital certificates

Options place here

Place here
Place here
Place here
Place here

Answer:

Options, select from these

IKE authentication	IKE data authentication/integrity
IKE key negotiation	IKE encryption

Definitions

DH Group 1,2 or 5
MD5 or SHA-1
3DES or AES
Pre-shared key or digital certificates

Options place here

IKE key negotiation
IKE data authentication/integrity
IKE encryption
IKE authentication

Explanation:

best security controls for a web server having

Definitions

Options, place here

- DH Group 1,2 or 5
- MD5 or SHA-1
- 3DES or AES
- Pre-shared key or digital certificates

- IKE key negotiation
- IKE data authentication/integrity
- IKE encryption
- IKE authentication

QUESTION NO: 15 DRAG DROP

Which item is correct about the relationship between the VPN types and their descriptions?

Options, select from these

- Crypto Maps
- Dynamic VTI
- DMVPN

- GET VPN
- DGVPN

Definitions

Options, place here

- Combines two VPN technologies
- Supports routing protocol over VPN tunnels
- Supported on Cisco IOS routers and ASAs
- Provides tunnel-less any-to-any connectivity
- Provides on-demand virtual access interface cloned from a virtual template configuration

- Place here
- Place here
- Place here
- Place here
- Place here

Answer:

Options, select from these

Crypto Maps	GET VPN
Dynamic VT!	DGVPN
DMVPN	

Definitions

- Combines two VPN technologies
- Supports routing protocol over VPN tunnels
- Supported on Cisco IOS routers and ASAs
- Provides tunnel-less any-to-any connectivity
- Provides on-demand virtual access interface cloned from a virtual template configuration

Options, place here

- DGVPN
- DMVPN
- Crypto Maps
- GET VPN
- Dynamic www.pass4sures.com

Explanation:

Definitions

- Combines two VPN technologies
- Supports routing protocol over VPN tunnels
- Supported on Cisco IOS routers and ASAs
- Provides tunnel-less any-to-any connectivity
- Provides on-demand virtual access interface cloned from a virtual template configuration

Options, place here

- DGVPN
- DMVPN
- Crypto Maps
- GET VPN
- Dynamic www.pass4sures.com

QUESTION NO: 16 DRAG DROP

Select the best security control to minimize the WAN security threats. Not all the security controls are required.

Security control. select from these

AAA	IPSec VPNs
Redundant WAN Devices	Host IPS
IPSec VPNs	

Threat	Security control. Place here
Denial of service attacks	Place here
Breaking into the WAN routers	Place here
Network traffic eavesdropping	Place here

Answer:

Security control. select from these

AAA	IPSec VPNs
Redundant WAN Devices	Host IPS
IPSec VPNs	

Threat	Security control. Place here
Denial of service attacks	Redundant WAN Devices
Breaking into the WAN routers	AAA
Network traffic eavesdropping	IPSec VPNs

QUESTION NO: 17

Which is the primary benefit that DTLS offers over TLS?

- A. Both the application and TLS can retransmit loss packets
- B. Improves security
- C. Provides low latency for real-time applications
- D. Uses TCP instead of UDP to provide a reliable Transport mechanism

Answer: C

QUESTION NO: 18 DRAG DROP

Which option is correct about the relationship between the terms and their description?

Options, select from these

True Positives

False Positives

True Negatives

False Negatives

Definitions

Security Control has not acted, through there was malicious activity

Place here

Security Control has not acted, as there was no malicious activity

Place here

Security Control acted as a consequence of non-malicious activity

Place here

Security Control acted as a consequence of non-malicious activity

Place here www.pass4sures.com

Options place here

Answer:

Options, select from these

True Positives

False Positives

True Negatives

False Negatives

Definitions

Security Control has not acted, through there was malicious activity

False Negatives

Security Control has not acted, as there was no malicious activity

True Negatives

Security Control acted as a consequence of non-malicious activity

False Positives

Security Control acted as a consequence of non-malicious activity

True Positives www.pass4sures.com

Options place here

Explanation: