Implementing Cisco Network Security

1. Which IPSec mode is used to encrypt traffic directly between a client and a server VPN endpoint?

A. tunnel mode

B. transport mode

C. quick mode

D. aggressive mode

Answer(s): B

---

2. Command ip ospf authentication key 1 is implemented in which level.

A. Interface

B. process

C. global

D. enable

Answer(s): A

---

3. What is the effect of the send-lifetime local 23:59:00 31 December 31 2013 infinite command?

A. It configures the device to begin transmitting the authentication key to other devices at 00:00:00 local time on January 1, 2014 and continue using the key indefinitely.

B. It configures the device to begin transmitting the authentication key to other devices at 23:59:00 local time on December 31, 2013 and continue using the key indefinitely.

C. It configures the device to begin accepting the authentication key from other devices immediately and stop accepting the key at 23:59:00 local time on December 31, 2013.

D. It configures the device to generate a new authentication key and transmit it to other devices at 23:59:00 local time on December 31, 2013.

E. It configures the device to begin accepting the authentication key from other devices at 23:59:00 local time on December 31, 2013 and continue accepting the key indefinitely.

F. It configures the device to begin accepting the authentication key from other devices at 00:00:00 local time on January 1, 2014 and continue accepting the key indefinitely.

Answer(s): B

---

4. Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months. What type of attack did your team discover?

A. advanced persistent threat

B. targeted malware

C. drive-by spyware

D. social activism

Answer(s): A,B

---

5. In which stage of an attack does the attacker discover devices on a target network?

A. Reconnaissance

B. Covering tracks

C. Gaining access

D. Maintaining access

Answer(s): A

---

6. Which technology can be used to rate data fidelity and to provide an authenticated hash for data?

A. network blocking

B. file analysis

C. file reputation

D. signature updates

Answer(s): C

---

7. In which two models can the Cisco Web Security Appliance be deployed? (Choose two.)

A. as a transparent proxy using the Secure Sockets Layer protocol

B. as a transparent proxy using the HyperText Transfer Protocol

C. explicit active mode

D. as a transparent proxy using the Web Cache Communication Protocol

E. explicit proxy mode

Answer(s): D,E

---

8. What are two advantages of TACACS+ over RADIUS? (Choose two)

A. TACACS+ decouples authentication and authorization.

B. Only TACACS+ encrypts the body of access-request packets

C. Only TACACS+ encrypts the password in an access-request packet

D. TACACS+ combines authentication and authorization.

E. TACACS+ requires less bandwidth to perform its services.

Answer(s): A,C

---

9. Which statement about command authorization and security contexts is true?

A. If command authorization is configured, it must be enabled on all contexts

B. The changeto command invokes a new context session with the credentials of the currently logged-in user

C. AAA settings are applied on a per-context basis

D. The enable_15 user and admins with changeto permissions have different command authorization levels per context

Answer(s): B

---

10. Which technology do you implement to prevent man in the middle attacks?

A. authentication

B. traffic scrubbing

C. process validation

D. transport layer security

Answer(s): D

---

11. On which operating system does the Cisco Email Security Appliance run?

A. Cisco ESA-OS

B. Cisco AsynOS

C. Cisco IOS XE

D. Cisco IOS XR

E. Cisco NX-OS

Answer(s): B

---

12. When setting up a site-to-site VPN with PSK authentication on a Cisco router, which two elements must be configured under crypto map? (Choose two.)

A. transform-set

B. pfs

C. peer

D. reverse-route

E. nat

Answer(s): A,C

---

13. Which option is the resulting action in a zone-based policy firewall configuration with these conditions?

A. no impact to zoning or policy

B. no policy lookup (pass)

C. drop

D. apply default policy

Answer(s): C

14. Which type of VLANs can communicate to PVLANs? (something like this) (choose 2)

A. secondary

B. backup

C. community

D. isolated

E. promiscuous

Answer(s): D,E

---

15. which port should (or would) be open if VPN NAT-T was enabled

A. port 500

B. port 500 outside interface

C. port 4500 outside interface

D. port 4500 ipsec

Answer(s): D

---

16. What IPSec mode is used to encrypt traffic between a server and VPN endpoint?

A. tunnel

B. Trunk

C. Aggregated

D. Quick

E. Transport

Answer(s): E

---

17. Which term is most closely aligned with the basic purpose of a SIEM solution?

A. Non-Repudiation

B. Repudiation

C. Causality

D. Accountability

Answer(s): D

---

18. How does a zone-based firewall implementation handle traffic between interfaces in the same zone?

A. Traffic between two interfaces in the same zone is allowed by default.

B. Traffic between interfaces in the same zone is blocked unless you configure the same-security permit command.

C. Traffic between interfaces in the same zone is always blocked.

D. Traffic between interfaces in the same zone is blocked unless you apply a service policy to the zone pair.

Answer(s): A

---

19. When you edit an IPS sub signature, what is the effect on the parent signature and the family of subsignature?

A. The change applies to the parent signature and the entire family of subsignature.

B. Other signatures are unaffected, the change applies only to the subsignature that you edit.

C. The change applies only to sub signature that are numbered sequentially after the subsignatre that you edit.

D. The change applies to the parent signature and the subsignature that you edit.

Answer(s): B

---

20. What is the best definition of hairpining?

A. Ingress traffic that traverses the outbound interface on a device.

B. Traffic that tunnels through a device interface

C. Traffic that enters one interface on device and that exist through another interface

D. Traffic that enters and exists a device through the same interface.

Answer(s): C
