IT Questions Bank | >_ IOS Command List | Ebooks | IP Calculators »

Donations

Search the site

ITExamAnswers.net

Home | CCNA » | Security » | CyberOps »

IT Questions Bank | >_ IOS Command List | CCNA » | CCNA Security v2.0 »

Cybersecurity » | Networking Essentials | IP Subnet Calculators » | Donation | Contact

Network Security 1.0 Exam Answers

Network Security v1.0 Answers

Modules 1 - 4: Securing Networks Group Exam Answers

Modules 5 - 7: Monitoring and Managing Devices Group Exam Answers

Modules 8 - 10: ACLs and Firewalls Group Exam Answers

Modules 11 - 12: Intrusion Prevention Group Exam Answers

Modules 13 - 14: Layer 2 and Endpoint Security Group Exam Answers

Modules 15 - 17: Cryptography Group Exam Answers

Network Security (Version 1.0) – Course Final Exam Answers

May 20, 2021 | Last Updated: Dec 16, 2024 |

Network Security 1.0 | 65 Comments

How to find: Press **“Ctrl + F”** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

Network Security (Version 1.0) – Network Security Course Final Exam Answers

1. Match the type of ASA ACLs to the description. (Not all options are used.)

Modules 18 - 19: VPNs Group Exam Answers

Modules 20 - 22: ASA Group Exam Answers

Network Security 1.0 Practice Final Exam Answers

Network Security 1.0 Final PT Skills Exam (PTSA) Answers

Network Security Course Final Exam Answers

Related Posts

Module 14: Quiz – Layer 2 Security Considerations (Answers) Network Security

Network Security (Version1.0) Modules 5 – 7: Monitoring and Managing Devices Group Test Online

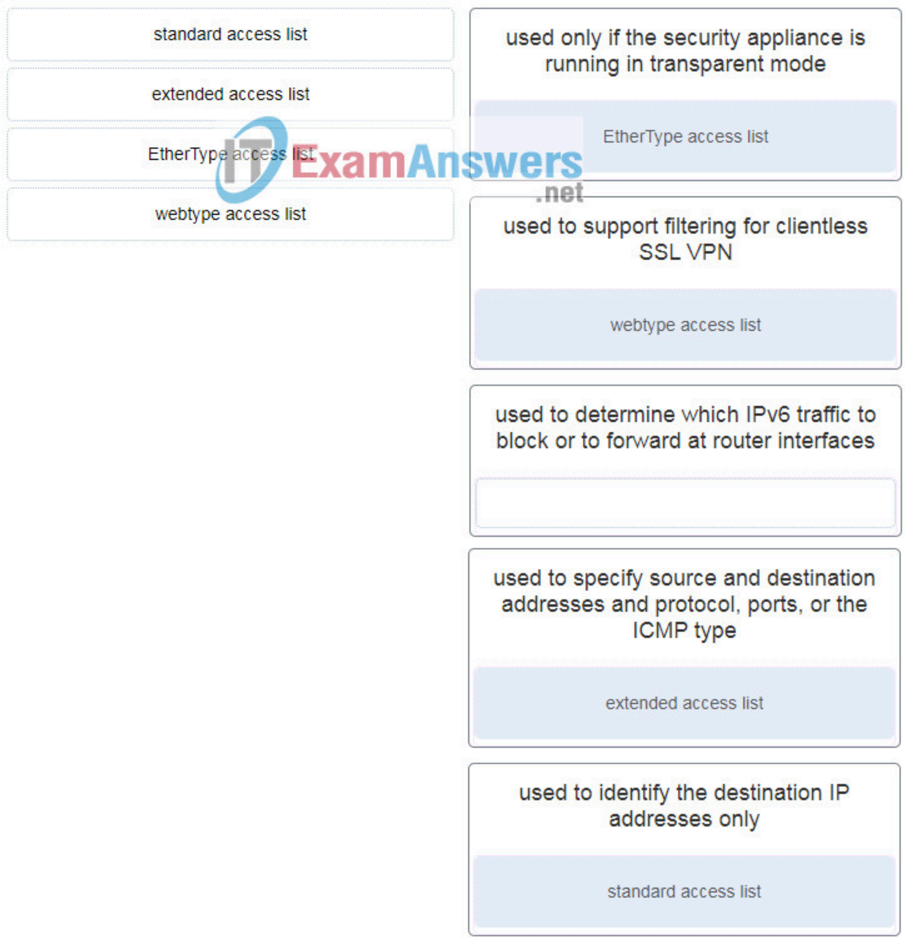
Modules 1 – 4: Securing Networks Group Exam Answers Full

16.3.10 Lab – Encrypting and Decrypting Data Using OpenSSL Answers

Module 13: Quiz – Endpoint Security (Answers) Network Security

Module 1: Quiz – Securing Networks (Answers) Network Security

Module 17: Quiz – Configure Network and Device Security (Answers) Network Security



standard access list

extended access list

EtherType access list

webtype access list

used only if the security appliance is running in transparent mode

EtherType access list

used to support filtering for clientless SSL VPN

webtype access list

used to determine which IPv6 traffic to block or to forward at router interfaces

used to specify source and destination addresses and protocol, ports, or the ICMP type

extended access list

used to identify the destination IP addresses only

standard access list

Place the options in the following order:

extended access lists	used to specify source and destination addresses and protocol, ports, or the ICMP type
webtype access lists	used to support filtering for clientless SSL VPN
standard access lists	used to identify the destination IP addresses only
EtherType access lists	used only if the security appliance is running in transparent mode

2. Which statement describes a difference between the Cisco ASA IOS CLI feature and the router IOS CLI feature?

- ASA uses the ? command whereas a router uses the help command to receive help on a brief description

9.1.3 Check Your Understanding – Identify the Type of Firewall Answers

6.2.7 Lab – Configure Automated Security Features Answers

14.9.11 Packet Tracer – Layer 2 VLAN Security Answers

Recent Comments

Nic on 5.5.1 Packet Tracer – IPv4 ACL Implementation Challenge (Answers)

Yeik on CCNA 1 v7.0 Final Exam Answers Full – Introduction to Networks

Ejay on CCNA 1 (v5.1 + v6.0) Chapter 1 Exam Answers 2020 – 100% Full

belkata on ITN (Version 7.00) Final PT Skills Assessment (PTSA) Exam Answers

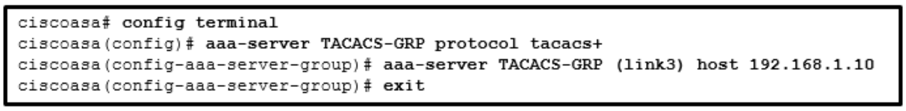
lora on CCNA 1 ITN (v5.1 + v6.0) Practice Final Exam Answers 100% Full 2020

and the syntax of a command.

- **To use a show command in a general configuration mode, ASA can use the command directly whereas a router will need to enter the do command before issuing the show command.**
- To complete a partially typed command, ASA uses the Ctrl+Tab key combination whereas a router uses the Tab key.
- To indicate the CLI EXEC mode, ASA uses the % symbol whereas a router uses the # symbol.

Explanation: The ASA CLI is a proprietary OS which has a similar look and feel to the Cisco router IOS. Although it shares some common features with the router IOS, it has its unique features. For example, an ASA CLI command can be executed regardless of the current configuration mode prompt. The IOS do command is not required or recognized. Both the ASA CLI and the router CLI use the # symbol to indicate the EXEC mode. Both CLIs use the Tab key to complete a partially typed command. Different from the router IOS, the ASA provides a help command that provides a brief command description and syntax for certain commands.

3. Refer to the exhibit. A network administrator is configuring AAA implementation on an ASA device. What does the option link3 indicate?



```
ciscoasa# config terminal
ciscoasa(config)# aaa-server TACACS-GRP protocol tacacs+
ciscoasa(config-aaa-server-group)# aaa-server TACACS-GRP (link3) host 192.168.1.10
ciscoasa(config-aaa-server-group)# exit
```

- the network name where the AAA server resides
- the specific AAA server name
- the sequence of servers in the AAA server group
- **the interface name**

4. What provides both secure segmentation and threat defense in a Secure Data Center solution?

- Cisco Security Manager software

- AAA server
- **Adaptive Security Appliance**
- intrusion prevention system

5. What are the three core components of the Cisco Secure Data Center solution? (Choose three.)

- mesh network
- **secure segmentation**
- **visibility**
- **threat defense**
- servers
- infrastructure

Explanation: Secure segmentation is used when managing and organizing data in a data center. Threat defense includes a firewall and intrusion prevention system (IPS). Data center visibility is designed to simplify operations and compliance reporting by providing consistent security policy enforcement.

6. What are three characteristics of ASA transparent mode? (Choose three.)

- **This mode does not support VPNs, QoS, or DHCP Relay.**
- It is the traditional firewall deployment mode.
- **This mode is referred to as a "bump in the wire."**
- NAT can be implemented between connected networks.
- **In this mode the ASA is invisible to an attacker.**
- The interfaces of the ASA separate Layer 3 networks and require IP addresses in different subnets.

7. What is needed to allow specific traffic that is sourced on the outside network of an ASA firewall to reach an internal network?

- **ACL**
- NAT
- dynamic routing protocols

- outside security zone level 0

Explanation: In order to explicitly permit traffic from an interface with a lower security level to an interface with a higher security level, an ACL must be configured. By default, traffic will only flow from a higher security level to a lower.

8. What will be the result of failed login attempts if the following command is entered into a router?

```
login block-for 150 attempts 4 within 90
```

- **All login attempts will be blocked for 150 seconds if there are 4 failed attempts within 90 seconds.**
- All login attempts will be blocked for 90 seconds if there are 4 failed attempts within 150 seconds.
- All login attempts will be blocked for 1.5 hours if there are 4 failed attempts within 150 seconds.
- All login attempts will be blocked for 4 hours if there are 90 failed attempts within 150 seconds.

Explanation: The components of the login block-for 150 attempts 4 within 90 command are as follows:
The expression block-for 150 is the time in seconds that logins will be blocked.
The expression attempts 4 is the number of failed attempts that will trigger the blocking of login requests.
The expression within 90 is the time in seconds in which the 4 failed attempts must occur.

9. Which two tasks are associated with router hardening? (Choose two.)

- placing the router in a secure room
- **disabling unused ports and interfaces**
- installing the maximum amount of memory possible
- **securing administrative access**
- using uninterruptible power supplies

10. Which threat protection capability is provided by Cisco ESA?

- web filtering
- cloud access security
- **spam protection**
- Layer 4 traffic monitoring

Explanation: Email is a top attack vector for security breaches. Cisco ESA includes many threat protection capabilities for email such as spam protection, forged email detection, and Cisco advanced phishing protection.

11. What are two security measures used to protect endpoints in the borderless network? (Choose two.)

- **denylisting**
- Snort IPS
- **DLP**
- DMZ
- rootkit

Explanation:

Measure	Purpose
antimalware software	Protect endpoints from malware.
spam filtering	Prevent spam emails from reaching endpoints.
blocklisting	Prevent endpoints from connecting to websites with bad reputations by immediately blocking connections based on the latest reputation intelligence.
data loss prevention	Prevent sensitive information from being lost or stolen.

Measure	Purpose
(DLP)	

12. Which three types of traffic are allowed when the authentication port-control auto command has been issued and the client has not yet been authenticated? (Choose three.)

- **CDP**
- 802.1Q
- IPsec
- TACACS+
- **STP**
- **EAPOL**

Explanation: Until the workstation is authenticated, 802.1X access control enables only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the workstation is connected. After authentication succeeds, normal traffic can pass through the port.

13. Which statement describes a characteristic of the IKE protocol?

- **It uses UDP port 500 to exchange IKE information between the security gateways.**
- IKE Phase 1 can be implemented in three different modes: main, aggressive, or quick.
- It allows for the transmission of keys directly across a network.
- The purpose of IKE Phase 2 is to negotiate a security association between two IKE peers.

14. Which action do IPsec peers take during the IKE Phase 2 exchange?

- exchange of DH keys

- **negotiation of IPsec policy**
- negotiation of IKE policy sets
- verification of peer identity

Explanation: The IKE protocol executes in two phases. During Phase 1 the two sides negotiate IKE policy sets, authenticate each other, and set up a secure channel. During the second phase IKE negotiates security associations between the peers.

15. What are two hashing algorithms used with IPsec AH to guarantee authenticity? (Choose two.)

- **SHA**
- RSA
- DH
- **MD5**
- AES

Explanation: The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. Two popular algorithms used to ensure that data is not intercepted and modified (data integrity and authenticity) are MD5 and SHA.

16. Which command raises the privilege level of the ping command to 7?

- user exec ping level 7
- authorization exec ping level 7
- accounting exec level 7 ping
- **privilege exec level 7 ping**

17. What is a characteristic of a role-based CLI view of router configuration?

- A CLI view has a command hierarchy, with higher and lower views.

- When a superview is deleted, the associated CLI views are deleted.
- **A single CLI view can be shared within multiple superviews.**
- Only a superview user can configure a new view and add or remove commands from the existing views.

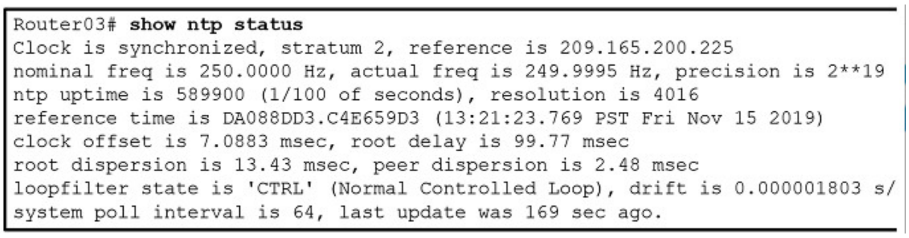
Explanation: A CLI view has no command hierarchy, and therefore, no higher or lower views. Deleting a superview does not delete the associated CLI views. Only a root view user can configure a new view and add or remove commands from the existing views.

18. What is a limitation to using OOB management on a large enterprise network?

- Production traffic shares the network with management traffic.
- Terminal servers can have direct console connections to user devices needing management.
- OOB management requires the creation of VPNs.
- **All devices appear to be attached to a single management network.**

Explanation: OOB management provides a dedicated management network without production traffic. Devices within that network, such as terminal servers, have direct console access for management purposes. Because in-band management runs over the production network, secure tunnels or VPNs may be needed. Failures on the production network may not be communicated to the OOB network administrator because the OOB management network may not be affected

19. Refer to the exhibit. A corporate network is using NTP to synchronize the time across devices. What can be determined from the displayed output?

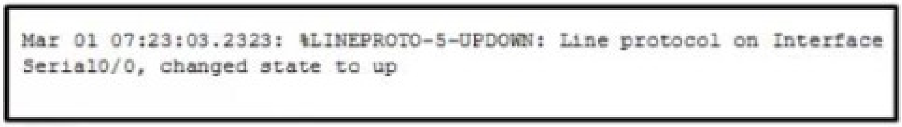


```
Router03# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
ntp uptime is 589900 (1/100 of seconds), resolution is 4016
reference time is DA088DD3.C4E659D3 (13:21:23.769 PST Fri Nov 15 2019)
clock offset is 7.0883 msec, root delay is 99.77 msec
root dispersion is 13.43 msec, peer dispersion is 2.48 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000001803 s/
system poll interval is 64, last update was 169 sec ago.
```

- **Router03 is a stratum 2 device that can provide NTP service to other devices in the network.**
- The time on Router03 may not be reliable because it is offset by more than 7 seconds to the time server.
- The interface on Router03 that connects to the time sever has the IPv4 address 209.165.200.225.
- Router03 time is synchronized to a stratum 2 time server.

Explanation: The **show ntp status** command displays that Router03 is now a stratum 2 device synchronized with the NTP server at 209.165.220.225 and can provide NTP service to other devices in the network. The clock offset is only 7.0883 milliseconds, not 7.0883 seconds.

20. Refer to the exhibit. Which two conclusions can be drawn from the syslog message that was generated by the router? (Choose two.)



```
Mar 01 07:23:03.2323: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to up
```

- This message resulted from an unusual error requiring reconfiguration of the interface.
- **This message indicates that service timestamps have been configured.**
- This message indicates that the interface changed state five times.
- **This message is a level 5 notification message.**
- This message indicates that the interface should be replaced.

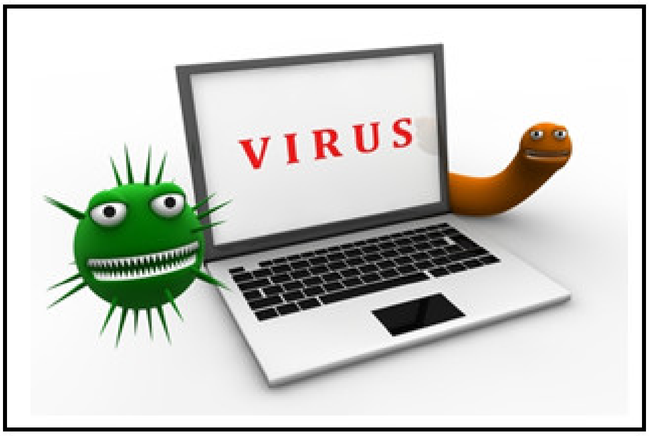
Explanation: The message is a level 5 notification message as shown in the %LINEPROTO-5 section of the output. Messages reporting the link status are common and do not require replacing the interface or reconfiguring the interface. The date and time displayed at the beginning of the message indicates that service timestamps have been configured on the router.

21. Which two types of hackers are typically classified as grey hat hackers? (Choose two.)

- **hacktivists**
- cyber criminals
- **vulnerability brokers**
- script kiddies
- state-sponsored hackers

Explanation: Grey hat hackers may do unethical or illegal things, but not for personal gain or to cause damage. Hacktivists use their hacking as a form of political or social protest, and vulnerability brokers hack to uncover weaknesses and report them to vendors. Depending on the perspective one possesses, state-sponsored hackers are either white hat or black hat operators. Script kiddies create hacking scripts to cause damage or disruption. Cyber criminals use hacking to obtain financial gain by illegal means.

22. When describing malware, what is a difference between a virus and a worm?



Network Security (Version 1) – Network Security 1.0 Final Exam

- A virus focuses on gaining privileged access to a device, whereas a worm does not.
- **A virus replicates itself by attaching to another file, whereas a worm can replicate itself independently.**
- A virus can be used to launch a DoS attack (but not a DDoS), but a worm can be used to launch both DoS and DDoS attacks.
- A virus can be used to deliver advertisements without user consent, whereas a worm cannot.

Explanation: Malware can be classified as follows:
Virus (self-replicates by attaching to another program or file)
Worm (replicates independently of another program)
Trojan horse (masquerades as a legitimate file or program)
Rootkit (gains privileged access to a machine while concealing itself)
Spyware (collects information from a target system)
Adware (delivers advertisements with or without consent)
Bot (waits for commands from the hacker)
Ransomware (holds a computer system or data captive until payment isreceived)

23. Which type of packet is unable to be filtered by an outbound ACL?

- multicast packet
- ICMP packet
- broadcast packet
- **router-generated packet**

Explanation: Traffic that originates within a router such as pings from a command prompt, remote access from a router to another device, or routing updates are not affected by outbound access lists. The traffic must flow through the router in order for the router to apply the ACEs.

24. Consider the access list command applied outbound on a router serial interface.

```
access-list 100 deny icmp 192.168.10.0 0.0.
```

What is the effect of applying this access list command?

- The only traffic denied is echo-replies sourced from the 192.168.10.0/24 network. All other traffic is allowed.
- The only traffic denied is ICMP-based traffic. All other traffic is allowed.
- **No traffic will be allowed outbound on the serial interface.**
- Users on the 192.168.10.0/24 network are not allowed to transmit traffic to any other destination.

25. Which command is used to activate an IPv6 ACL named ENG_ACL on an interface so that the router filters traffic prior to accessing the routing table?

- ipv6 access-class ENG_ACL in
- ipv6 traffic-filter ENG_ACL out
- **ipv6 traffic-filter ENG_ACL in**
- ipv6 access-class ENG_ACL out

Explanation: For the purpose of applying an access list to a particular interface, the ipv6 traffic-filter IPv6 command is equivalent to the access-group IPv4 command. The direction in which the traffic is examined (in or out) is also required.

26. What technology has a function of using trusted third-party protocols to issue credentials that are accepted as an authoritative identity?

- digital signatures
- hashing algorithms
- **PKI certificates**
- symmetric keys

Explanation: Digital certificates are used to prove the authenticity and integrity of PKI certificates, but a PKI Certificate Authority is a trusted third-party entity that issues PKI certificates. PKI certificates are public information and are used to provide authenticity, confidentiality, integrity, and nonrepudiation services that can scale to large requirements.

27. What are two methods to maintain certificate revocation status? (Choose two.)

- subordinate CA
- **OCSP**
- DNS
- LDAP
- **CRL**

Explanation: A digital certificate might need to be revoked if its key is compromised or it is no longer needed. The certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP), are two common methods to check a certificate revocation status.

28. Which protocol is an IETF standard that defines the PKI digital certificate format?

- SSL/TLS
- X.500
- LDAP
- **X.509**

Explanation: To address the interoperability of different PKI vendors, IETF published the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527). The standard defines the format of a digital certificate.

29. A network administrator is configuring DAI on a switch. Which command should be used on the uplink interface that connects to a router?

- **ip arp inspection trust**
- ip dhcp snooping
- ip arp inspection vlan
- spanning-tree portfast

Explanation: In general, a router serves as the default gateway for the LAN or VLAN on the switch. Therefore, the uplink interface that connects to a router should be a trusted port for forwarding ARP requests.

30. What is the best way to prevent a VLAN hopping attack?

- **Disable trunk negotiation for trunk ports and statically set nontrunk ports as access ports.**
- Disable STP on all nontrunk ports.
- Use VLAN 1 as the native VLAN on trunk ports.
- Use ISL encapsulation on all trunk links.

Explanation: VLAN hopping attacks rely on the attacker being able to create a trunk link with a switch. Disabling DTP and configuring user-facing ports as static access ports can help prevent these types of attacks. Disabling the Spanning Tree Protocol (STP) will not eliminate VLAN hopping attacks.

31. What would be the primary reason an attacker would launch a MAC address overflow attack?

- so that the switch stops forwarding traffic
- so that legitimate hosts cannot obtain a MAC address
- **so that the attacker can see frames that are destined for other hosts**
- so that the attacker can execute arbitrary code on the switch

32. What is the main difference between the implementation of IDS and IPS devices?

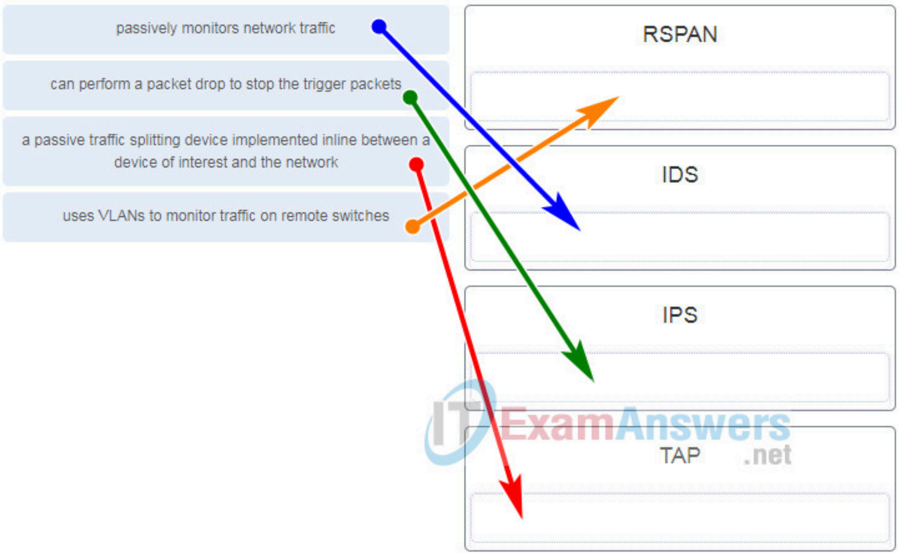
- An IDS can negatively impact the packet flow, whereas an IPS can not.
- An IDS needs to be deployed together with a firewall device, whereas an IPS can replace a firewall.
- **An IDS would allow malicious traffic to pass before it is addressed, whereas an IPS stops it immediately.**
- An IDS uses signature-based technology to detect malicious packets, whereas an IPS uses profile-based technology.

Explanation: An IPS is deployed in inline mode and will not allow malicious traffic to enter the internal network without first analyzing it. An advantage of this is that it can stop an attack immediately. An IDS is deployed in promiscuous mode. It copies the traffic patterns and analyzes them offline, thus it cannot stop the attack immediately and it relies on another device to take further actions once it detects an attack. Being deployed in inline mode, an IPS can negatively impact the traffic flow. Both IDS and IPS can use signature-based technology to detect malicious packets. An IPS cannot replace other security devices, such as firewalls, because they perform different tasks.

33. Which attack is defined as an attempt to exploit software vulnerabilities that are unknown or undisclosed by the vendor?

- zero-day
- Trojan horse
- brute-force
- man-in-the-middle

34. Match the network monitoring technology with the description.



passively monitors network traffic

can perform a packet drop to stop the trigger packets

a passive traffic splitting device implemented inline between a device of interest and the network

uses VLANs to monitor traffic on remote switches

RSPAN

IDS

IPS

TAP

Place the options in the following order:

passively monitors network traffic	IDS
uses VLANs to monitor traffic on remote switches	RSPAN
a passive traffic splitting device implemented inline between a device of interest and the network	TAP
can perform a packet drop to stop the trigger packets	IPS

35. What are the three signature levels provided by Snort IPS on the 4000 Series ISR? (Choose three.)

- **security**
- drop
- reject
- **connectivity**
- inspect
- **balanced**

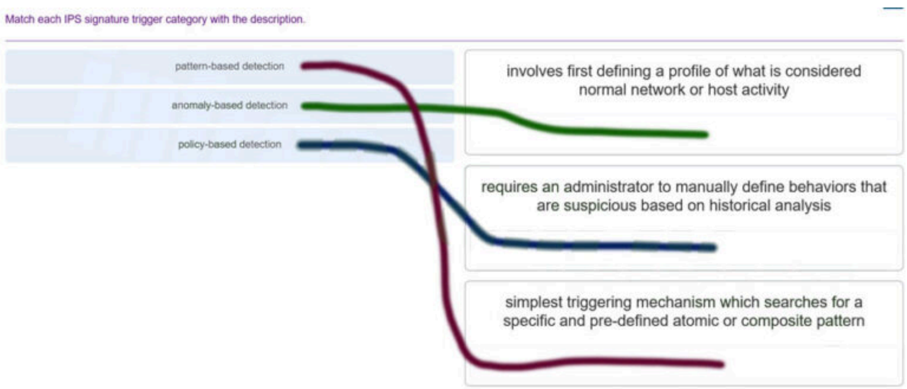
36. What are three attributes of IPS signatures? (Choose three.)

- **action**
- length
- **trigger**
- **type**
- depth
- function

Explanation: IPS signatures have three distinctive attributes:

- type
- trigger (alarm)
- action

37. Match each IPS signature trigger category with the description.

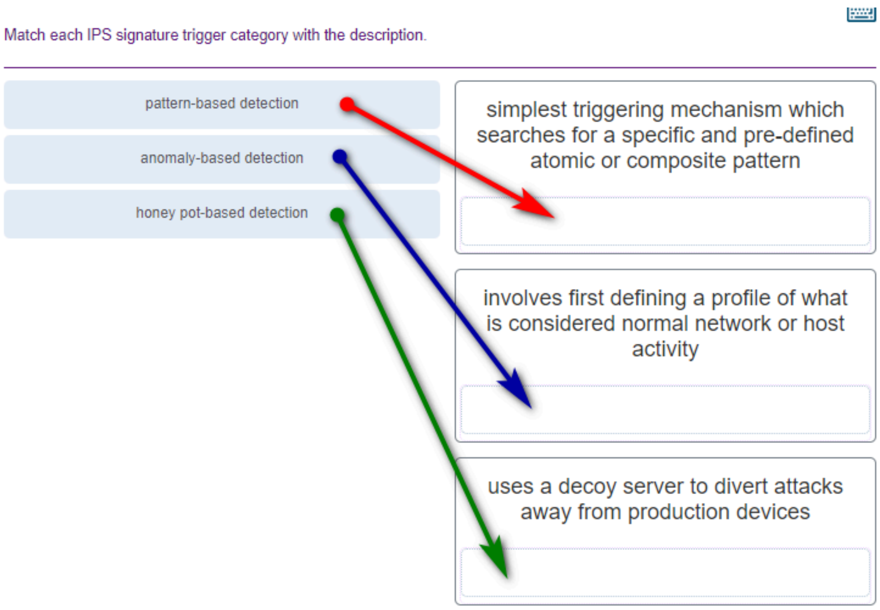


Match each IPS signature trigger category with the description.

- pattern-based detection
- anomaly-based detection
- policy-based detection

- involves first defining a profile of what is considered normal network or host activity
- requires an administrator to manually define behaviors that are suspicious based on historical analysis
- simplest triggering mechanism which searches for a specific and pre-defined atomic or composite pattern

Other case:



Match each IPS signature trigger category with the description.

pattern-based detection

anomaly-based detection

honey pot-based detection

simplest triggering mechanism which searches for a specific and pre-defined atomic or composite pattern

involves first defining a profile of what is considered normal network or host activity

uses a decoy server to divert attacks away from production devices

- **pattern-based detection:** simplest triggering mechanism which searches for a specific and pre-defined atomic or composite pattern
- **anomaly-based detection:** involves first defining a profile of what is considered normal network or host activity
- **honey pot-based detection:** uses a decoy server to divert attacks away from production devices

38. Which two features are included by both TACACS+ and RADIUS protocols? (Choose two.)

- SIP support
- **password encryption**
- 802.1X support
- separate authentication and authorization processes
- **utilization of transport layer protocols**

Explanation: Both TACACS+ and RADIUS support password encryption (TACACS+ encrypts all communication) and use Layer 4 protocol (TACACS+ uses TCP and RADIUS uses UDP). TACACS+ supports separation of authentication and authorization processes, while RADIUS combines authentication and authorization as one process. RADIUS supports remote access technology, such as 802.1x and SIP; TACACS+ does not.

39. What function is provided by the RADIUS protocol?

- RADIUS provides encryption of the complete packet during transfer.
- RADIUS provides separate AAA services.
- **RADIUS provides separate ports for authorization and accounting.**
- RADIUS provides secure communication using TCP port 49.

Explanation: When an AAA user is authenticated, RADIUS uses UDP port 1645 or 1812 for authentication and UDP port 1646 or 1813 for accounting. TACACS provides separate authorization and accounting services. When a RADIUS client is authenticated, it is also authorized. TACACS provides secure connectivity using TCP port 49. RADIUS hides passwords during transmission and does not encrypt the complete packet.

40. What are three characteristics of the RADIUS protocol? (Choose three.)

- utilizes TCP port 49
- **uses UDP ports for authentication and accounting**
- **supports 802.1X and SIP**
- separates the authentication and authorization processes
- encrypts the entire body of the packet
- **is an open RFC standard AAA protocol**

Explanation: RADIUS is an open-standard AAA protocol using UDP port 1645 or 1812 for authentication and UDP port 1646 or 1813 for accounting. It combines authentication and authorization into one process; thus, a password is encrypted for transmission while the rest of the packet will be sent in plain text. RADIUS offers the expedited service and more comprehensive accounting desired by remote-access providers but provides lower security and less potential for customization than TACACS+.

41. Which zone-based policy firewall zone is system-defined and applies to traffic destined for the router or originating from the router?

- local zone
- inside zone
- **self zone**
- system zone
- outside zone

Explanation: Zone-based policy firewalls typically have the private (internal or trusted) zone, the public (external or untrusted) zone, and the default self zone, which does not require any interfaces. The private or internal zone is commonly used for internal LANs. The public zone would include the interfaces that connect to an external (outside the business) interface.

42. What are two benefits of using a ZPF rather than a Classic Firewall? (Choose two.)

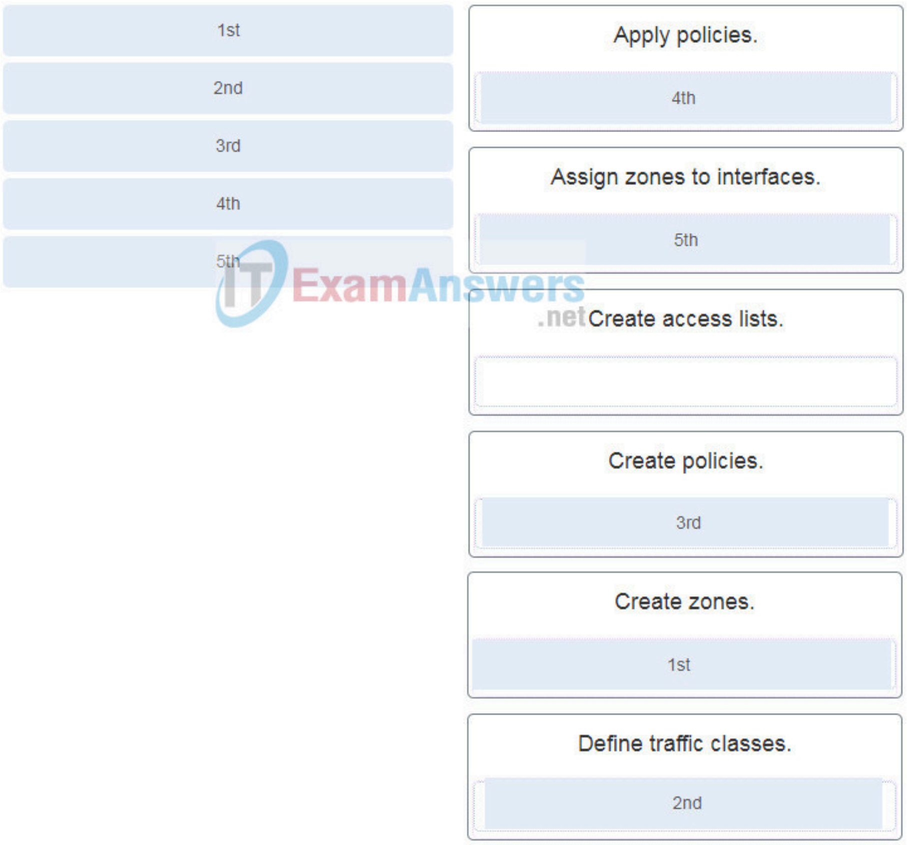
- ZPF allows interfaces to be placed into zones for IP inspection.
- **The ZPF is not dependent on ACLs.**
- Multiple inspection actions are used with ZPF.
- **ZPF policies are easy to read and troubleshoot.**
- With ZPF, the router will allow packets unless they are explicitly blocked.

Explanation: There are several benefits of a ZPF:
– It is not dependent on ACLs.
– The router security posture is to block unless explicitly allowed.
– Policies are easy to read and troubleshoot with C3PL.

– One policy affects any given traffic, instead of needing multiple ACLs and inspection actions.

In addition, an interface cannot be simultaneously configured as a security zone member and for IP inspection.

43. Place the steps for configuring zone-based policy (ZPF) firewalls in order from first to last. (Not all options are used.)



1st

2nd

3rd

4th

5th

Apply policies. 4th

Assign zones to interfaces. 5th

Create access lists.

Create policies. 3rd

Create zones. 1st

Define traffic classes. 2nd

Place the options in the following order:

2nd	Define traffic classes.
1st	Create zones.
4th	Apply policies.
5th	Assign zones to interfaces.
3rd	Create policies.

44. How does a firewall handle traffic when it is originating from the private network and traveling to the DMZ network?

- The traffic is selectively denied based on service requirements.
- **The traffic is usually permitted with little or no restrictions.**
- The traffic is selectively permitted and inspected.
- The traffic is usually blocked.

Explanation: Traffic originating from the private network is inspected as it travels toward the public or DMZ network. This traffic is permitted with little or no restriction. Inspected traffic returning from the DMZ or public network to the private network is permitted.

45. Which two protocols generate connection information within a state table and are supported for stateful filtering? (Choose two.)

- ICMP
- UDP
- DHCP
- **TCP**
- **HTTP**

46. Which type of firewall is supported by most routers and is the easiest to implement?

- next generation firewall
- **stateless firewall**
- stateful firewall
- proxy firewall

Explanation: Packet Filtering (Stateless) Firewall uses a simple policy table look-up that filters traffic based on specific criteria and is considered the easiest firewall to implement.

47. What network testing tool would an administrator use to assess and validate system configurations against security policies and compliance standards?

- **Tripwire**
- L0phtcrack
- Nessus
- Metasploit

Explanation: Tripwire – This tool assesses and validates IT configurations against internal policies, compliance standards, and security best practices.

48. What type of network security test can detect and report changes made to network systems?

- vulnerability scanning
- network scanning
- **integrity checking**
- penetration testing

Explanation: Integrity checking is used to detect and report changes made to systems. Vulnerability scanning is used to find weaknesses and misconfigurations on network systems. Network scanning is used to discover available resources on the network.

49. What network security testing tool has the ability to provide details on the source of suspicious network activity?

- **SIEM**
- SuperScan
- Zenmap
- Tripwire

Explanation: There are various network security tools available for network security testing and evaluation.

SuperScan is a Microsoft port scanning software that detects open TCP and UDP ports on systems. Nmap and Zenmap are low-level network scanners available to the public. Tripwire is used to assess if network devices are compliant with network security policies. SIEM is used to provide real-time reporting of security events on the network.

50 **How do modern cryptographers defend against brute-force attacks?**

- Use statistical analysis to eliminate the most common encryption keys.
- **Use a keyspace large enough that it takes too much money and too much time to conduct a successful attack.**
- Use an algorithm that requires the attacker to have both ciphertext and plaintext to conduct a successful attack.
- Use frequency analysis to ensure that the most popular letters used in the language are not used in the cipher message.

Explanation: In a brute-force attack, an attacker tries every possible key with the decryption algorithm knowing that eventually one of them will work. To defend against the brute-force attacks, modern cryptographers have as an objective to have a keyspace (a set of all possible keys) large enough so that it takes too much money and too much time to accomplish a brute-force attack. A security policy requiring passwords to be changed in a predefined interval further defend against the brute-force attacks. The idea is that passwords will have been changed before an attacker exhausts the keyspace.

51. How does a Caesar cipher work on a message?

- **Letters of the message are replaced by another letter that is a set number of places away in the**

alphabet.
- Letters of the message are rearranged randomly.
- Letters of the message are rearranged based on a predetermined pattern.
- Words of the message are substituted based on a predetermined pattern.

52. What is the main factor that ensures the security of encryption of modern algorithms?

- complexity of the hashing algorithm
- the use of 3DES over AES
- **secrecy of the keys**
- secrecy of the algorithm

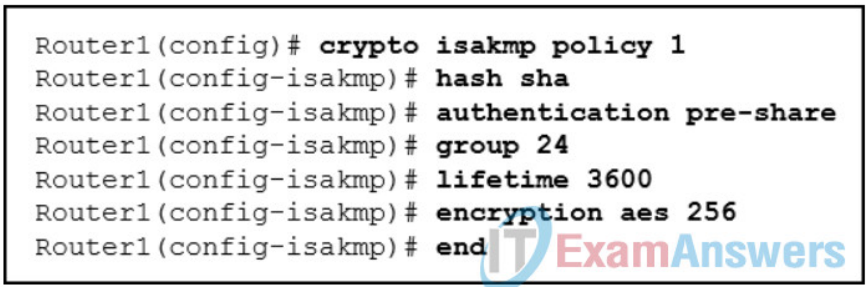
Explanation: With most modern algorithms, successful decryption requires knowledge of the appropriate cryptographic keys. This means that the security of encryption lies in the secrecy of the keys, not the algorithm.

53 **What is the next step in the establishment of an IPsec VPN after IKE Phase 1 is complete?**

- negotiation of the ISAKMP policy
- **negotiation of the IPsec SA policy**
- detection of interesting traffic
- authentication of peers

Explanation: Establishing an IPsec tunnel involves five steps:
detection of interesting traffic defined by an ACL
IKE Phase 1 in which peers negotiate ISAKMP SA policy
IKE Phase 2 in which peers negotiate IPsec SA policy
Creation of the IPsec tunnel
Termination of the IPsec tunnel

54. Refer to the exhibit. What algorithm will be used for providing confidentiality?



```
Router1(config)# crypto isakmp policy 1
Router1(config-isakmp)# hash sha
Router1(config-isakmp)# authentication pre-share
Router1(config-isakmp)# group 24
Router1(config-isakmp)# lifetime 3600
Router1(config-isakmp)# encryption aes 256
Router1(config-isakmp)# end
```

Network Security (Version 1) – Network Security 1.0 Final Exam

- RSA
- Diffie-Hellman
- DES
- **AES**

Explanation: The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. Two popular algorithms that are used to ensure that data is not intercepted and modified (data integrity) are MD5 and SHA. AES is an encryption protocol and provides data confidentiality. DH (Diffie-Hellman) is an algorithm that is used for key exchange. RSA is an algorithm used for authentication.

55. After issuing a show run command, an analyst notices the following command:

```
crypto ipsec transform-set MYSET esp-aes 25
```

What is the purpose of this command?

- **It establishes the set of encryption and hashing algorithms used to secure the data sent through an IPsec tunnel.**
- It defines the default ISAKMP policy list used to establish the IKE Phase 1 tunnel.

- It establishes the criteria to force the IKE Phase 1 negotiations to begin.
- It indicates that IKE will be used to establish the IPsec tunnel for protecting the traffic.

56. Which algorithm can ensure data integrity?

- RSA
- AES
- **MD5**
- PKI

Explanation: Data integrity guarantees that the message was not altered in transit. Integrity is ensured by implementing either of the Secure Hash Algorithms (SHA-2 or SHA-3). The MD5 message digest algorithm is still widely in use.

57. A company implements a security policy that ensures that a file sent from the headquarters office to the branch office can only be opened with a predetermined code. This code is changed every day. Which two algorithms can be used to achieve this task? (Choose two.)

- HMAC
- MD5
- **3DES**
- SHA-1
- **AES**

Explanation: The task to ensure that only authorized personnel can open a file is data confidentiality, which can be implemented with encryption. AES and 3DES are two encryption algorithms. HMAC can be used for ensuring origin authentication. MD5 and SHA-1 can be used to ensure data integrity.

58. A network technician has been asked to design a virtual private network between two branch routers. Which type of cryptographic key should be used in this scenario?

- hash key
- **symmetric key**
- asymmetric key
- digital signature

Explanation: A symmetric key requires that both routers have access to the secret key that is used to encrypt and decrypt exchanged data.

59. Which two options can limit the information discovered from port scanning? (Choose two.)

- **intrusion prevention system**
- **firewall**
- authentication
- passwords
- encryption

Explanation: Using an intrusion prevention system (IPS) and firewall can limit the information that can be discovered with a port scanner. Authentication, encryption, and passwords provide no protection from loss of information from port scanning.

60. An administrator discovers that a user is accessing a newly established website that may be detrimental to company security. What action should the administrator take first in terms of the security policy?

- Ask the user to stop immediately and inform the user that this constitutes grounds for dismissal.
- Create a firewall rule blocking the respective website.
- **Revise the AUP immediately and get all users to sign the updated AUP.**

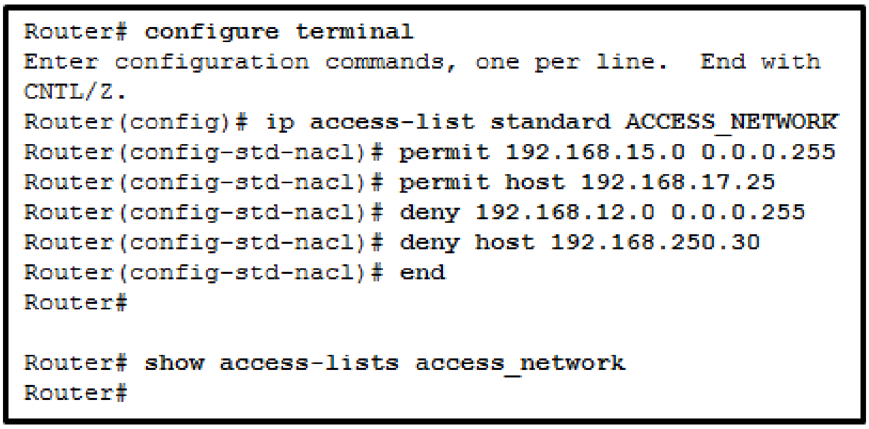
- Immediately suspend the network privileges of the user.

61. If AAA is already enabled, which three CLI steps are required to configure a router with a specific view? (Choose three.)

- Create a superview using the parser view view-name command.
- Associate the view with the root view.
- Assign users who can use the view.
- **Create a view using the parser viewcommand.**
- **Assign a secret password to the view.**
- **Assign commands to the view.**

Explanation: There are five steps involved to create a view on a Cisco router.
1) AAA must be enabled.
2) the view must be created.
3) a secret password must be assigned to the view.
4) commands must be assigned to the view.
5) view configuration mode must be exited.

62. Refer to the exhibit. A network administrator configures a named ACL on the router. Why is there no output displayed when the show command is issued?



```
Router# configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)# ip access-list standard ACCESS_NETWORK
Router(config-std-nacl)# permit 192.168.15.0 0.0.0.255
Router(config-std-nacl)# permit host 192.168.17.25
Router(config-std-nacl)# deny 192.168.12.0 0.0.0.255
Router(config-std-nacl)# deny host 192.168.250.30
Router(config-std-nacl)# end
Router#

Router# show access-lists access_network
Router#
```

A network administrator configures a named ACL on the router

- The ACL is not activated.
- **The ACL name is case sensitive.**

- The ACL has not been applied to an interface.
- No packets have matched the ACL statements yet.

63. ACLs are used primarily to filter traffic. What are two additional uses of ACLs? (Choose two.):

- **specifying internal hosts for NAT**
- **identifying traffic for QoS**
- specifying source addresses for authentication
- reorganizing traffic into VLANs
- filtering VTP packets

Explanation: ACLs are used to filter traffic to determine which packets will be permitted or denied through the router and which packets will be subject to policy-based routing. ACLs can also be used to identify traffic that requires NAT and QoS services. Prefix lists are used to control which routes will be redistributed or advertised to other routers.

64. What two features are added in SNMPv3 to address the weaknesses of previous versions of SNMP? (Choose two.)

- **authentication**
- authorization with community string priority
- bulk MIB objects retrieval
- ACL management filtering
- **encryption**

65. What network testing tool is used for password auditing and recovery?

- Nessus
- Metasploit
- **L0phtcrack**
- SuperScan

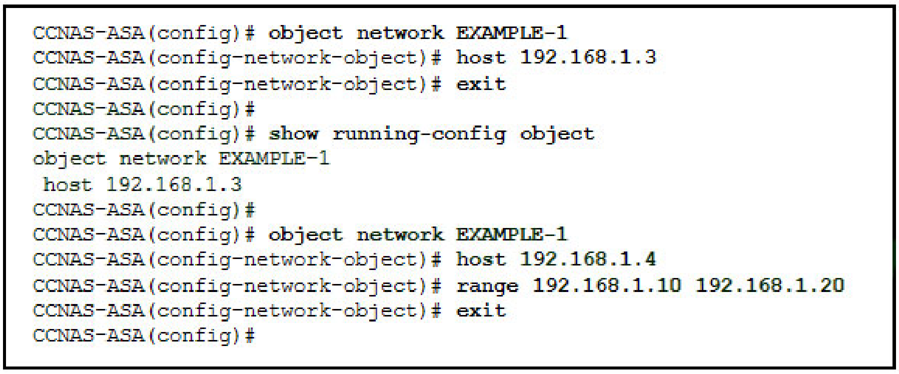
Explanation: The Nesus tool provides remote vulnerability scanning that focuses on remote access, password misconfiguration, and DoS against the TCP/IP stack. L0phtcrack provides password auditing and recovery. Metasploit provides information about vulnerabilities and aids in penetration testing and IDS signature development.

66. Which type of firewall makes use of a server to connect to destination devices on behalf of clients?

- packet filtering firewall
- **proxy firewall**
- stateless firewall
- stateful firewall

Explanation: An application gateway firewall, also called a proxy firewall, filters information at Layers 3, 4, 5, and 7 of the OSI model. It uses a proxy server to connect to remote servers on behalf of clients. Remote servers will see only a connection from the proxy server, not from the individual clients.

67. Refer to the exhibit. What will be displayed in the output of the show running-config object command after the exhibited configuration commands are entered on an ASA 5506-X?

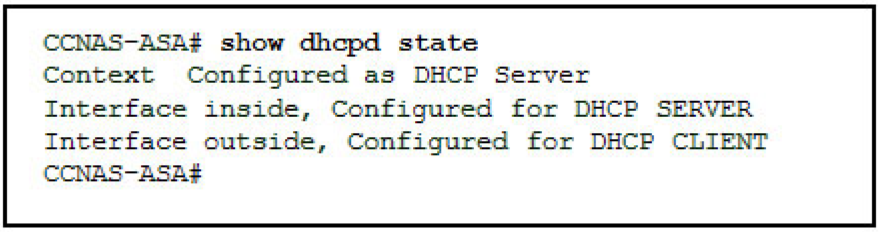


```
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.3
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object network EXAMPLE-1
 host 192.168.1.3
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.4
CCNAS-ASA(config-network-object)# range 192.168.1.10 192.168.1.20
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
```

- host 192.168.1.4
- **range 192.168.1.10 192.168.1.20**
- host 192.168.1.3, host 192.168.1.4, and range 192.168.1.10 192.168.1.20
- host 192.168.1.3
- host 192.168.1.3 and host 192.168.1.4
- host 192.168.1.4 and range 192.168.1.10 192.168.1.20

Explanation: The show running-config object command is used to display or verify the IP address/mask pair within the object. There can only be one statement in the network object. Entering a second IP address/mask pair will replace the existing configuration.

68. Refer to the exhibit. According to the command output, which three statements are true about the DHCP options entered on the ASA? (Choose three.)



```
CCNAS-ASA# show dhcpd state
Context  Configured as DHCP Server
Interface inside, Configured for DHCP SERVER
Interface outside, Configured for DHCP CLIENT
CCNAS-ASA#
```

- **The dhcpd address [start-of-pool]-[end-of-pool] inside command was issued to enable the DHCP server.**
- The dhcpd address [start-of-pool]-[end-of-pool] inside command was issued to enable the DHCP client.
- **The dhcpd enable inside command was issued to enable the DHCP server.**
- **The dhcpd auto-config outside command was issued to enable the DHCP client.**
- The dhcpd auto-config outside command was issued to enable the DHCP server.
- The dhcpd enable inside command was issued to enable the DHCP client.

69. Which two statements describe the characteristics of symmetric algorithms? (Choose two.)

- **They are commonly used with VPN traffic.**
- They use a pair of a public key and a private key.
- They are commonly implemented in the SSL and SSH protocols.
- They provide confidentiality, integrity, and availability.
- **They are referred to as a pre-shared key or secret key.**

Explanation: Symmetric encryption algorithms use the same key (also called shared secret) to encrypt and decrypt the data. In contrast, asymmetric encryption algorithms use a pair of keys, one for encryption and another for decryption.

70. A web server administrator is configuring access settings to require users to authenticate first before accessing certain web pages. Which requirement of information security is addressed through the configuration?

- availability
- integrity
- scalability
- **confidentiality**

Explanation: Confidentiality ensures that data is accessed only by authorized individuals. Authentication will help verify the identity of the individuals.

71. The use of 3DES within the IPsec framework is an example of which of the five IPsec building blocks?

- authentication
- nonrepudiation
- integrity
- Diffie-Hellman
- **confidentiality**

Explanation: The IPsec framework consists of five building blocks. Each building block performs a specific securty function via specific protocols. The function of providing confidentiality is provided by protocols such as DES, 3DES, and AES.

72. What function is provided by Snort as part of the Security Onion?

- **to generate network intrusion alerts by the use of rules and signatures**
- to normalize logs from various NSM data logs so they can be represented, stored, and accessed through a common schema
- to display full-packet captures for analysis
- to view pcap transcripts generated by intrusion detection tools

Explanation: Snort is a NIDS integrated into Security Onion. It is an important source of the alert data that is indexed in the Sguil analysis tool. Snort uses rules and signatures to generate alerts.

73. What are two drawbacks to using HIPS? (Choose two.)

- With HIPS, the success or failure of an attack cannot be readily determined.
- **With HIPS, the network administrator must verify support for all the different operating systems used in the network.**
- **HIPS has difficulty constructing an accurate network picture or coordinating events that occur across the entire network.**
- If the network traffic stream is encrypted, HIPS is unable to access unencrypted forms of the traffic.
- HIPS installations are vulnerable to fragmentation attacks or variable TTL attacks.

Explanation: Two disadvantages of deploying HIPS are (1) that it cannot create a complete view of the network or have knowledge of events that might be occurring beyond an individual host and (2) every host operating system within the organization must be supported. However, an advantage of using HIPS is that it can monitor and protect the operating system as well as critical system processes on each network host.

74. In an AAA-enabled network, a user issues the configure terminal command from the privileged executive mode of operation. What AAA function is at work if this command is rejected?

- **authorization**
- authentication
- auditing
- accounting

Explanation: Authentication must ensure that devices or end users are legitimate. Authorization is concerned with allowing and disallowing authenticated users access to certain areas and programs on the network. The configure terminal command is rejected because the user is not authorized to execute the command.

75. A company has a file server that shares a folder named Public. The network security policy specifies that the Public folder is assigned Read-Only rights to anyone who can log into the server while the Edit rights are assigned only to the network admin group. Which component is addressed in the AAA network service framework?

- automation
- accounting
- authentication
- **authorization**

Explanation: After a user is successfully authenticated (logged into the server), the authorization is the process of determining what network resources the user can access and what operations (such as read or edit) the user can perform.

76. What is a characteristic of a DMZ zone?

- Traffic originating from the inside network going to the DMZ network is not permitted.
- **Traffic originating from the outside network going to the DMZ network is selectively permitted.**
- Traffic originating from the DMZ network going to the inside network is permitted.
- Traffic originating from the inside network going to the DMZ network is selectively permitted.

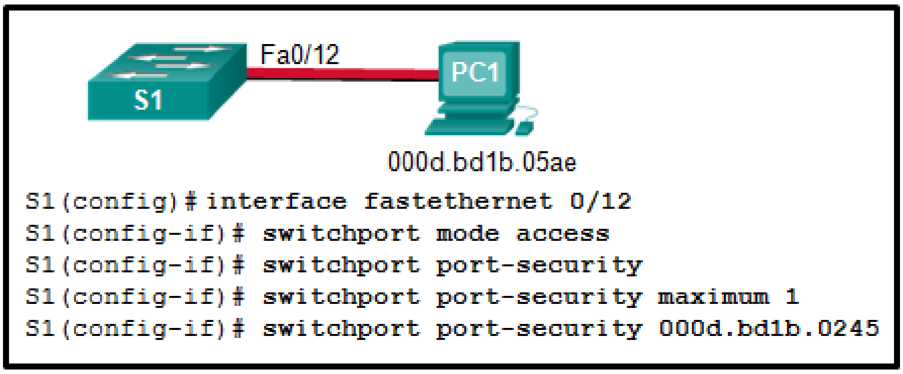
Explanation: The characteristics of a DMZ zone are as follows:
Traffic originating from the inside network going to the DMZ network is permitted.
Traffic originating from the outside network going to the DMZ network is selectively permitted.
Traffic originating from the DMZ network going to the inside network is denied.

77. Which measure can a security analyst take to perform effective security monitoring against network traffic encrypted by SSL technology?

- Use a Syslog server to capture network traffic.
- **Deploy a Cisco SSL Appliance.**
- Require remote access connections through IPsec VPN.
- Deploy a Cisco ASA.

Explanation: Deploy a Cisco SSL Appliance to decrypt SSL traffic and send it to intrusion prevention system (IPS) appliances to identify risks normally hidden by SSL.

78. Refer to the exhibit. Port security has been configured on the Fa 0/12 interface of switch S1. What action will occur when PC1 is attached to switch S1 with the applied configuration?



```
S1(config)#interface fastethernet 0/12
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 1
S1(config-if)# switchport port-security 000d.bd1b.0245
```

- Frames from PC1 will be forwarded since the switchport port-security violation command is missing.
- Frames from PC1 will be forwarded to its destination, and a log entry will be created.
- Frames from PC1 will be forwarded to its destination, but a log entry will not be created.
- **Frames from PC1 will cause the interface to shut down immediately, and a log entry will be made.**
- Frames from PC1 will be dropped, and there will be no log of the violation.
- Frames from PC1 will be dropped, and a log message will be created.

Explanation: Manual configuration of the single allowed MAC address has been entered for port fa0/12. PC1 has a different MAC address and when attached will cause the port to shut down (the default action), a log message to be automatically created, and the violation counter to increment. The default action of shutdown is recommended because the restrict option might fail if an attack is underway.

79. What security countermeasure is effective for preventing CAM table overflow attacks?

- DHCP snooping
- Dynamic ARP Inspection
- IP source guard
- **port security**

Explanation: Port security is the most effective method for preventing CAM table overflow attacks. Port security gives an administrator the ability to manually specify what MAC addresses should be seen on given switch ports. It provides a method for limiting the number of MAC addresses that can be dynamically learned over a switch port.

80. What are two examples of DoS attacks? (Choose two.)

- port scanning
- SQL injection
- **ping of death**
- phishing
- **buffer overflow**

Explanation: The buffer overflow and ping of death DoS attacks exploit system memory-related flaws on a server by sending an unexpected amount of data or malformed data to the server.

81. Which method is used to identify interesting traffic needed to create an IKE phase 1 tunnel?

- transform sets
- **a permit access list entry**
- hashing algorithms
- a security association

82. When the CLI is used to configure an ISR for a site-to-site VPN connection, which two items must be specified to enable a crypto map policy? (Choose two.)

- the hash
- **the peer**
- encryption
- the ISAKMP policy
- **a valid access list**
- IP addresses on all active interfaces
- the IKE Phase 1 policy

Explanation: After the crypto map command in global configuration mode has been issued, the new crypto map will remain disabled until a peer and a valid access list have been configured.

83. How does a firewall handle traffic when it is originating from the public network and traveling to the DMZ network?

- **Traffic that is originating from the public network is inspected and selectively permitted when traveling to the DMZ network.**
- Traffic that is originating from the public network is usually permitted with little or no restriction when traveling to the DMZ network.
- Traffic that is originating from the public network is usually forwarded without inspection when traveling to the DMZ network.
- Traffic that is originating from the public network is usually blocked when traveling to the DMZ network.

Explanation: Traffic originating from the public network and traveling toward the DMZ is selectively permitted and inspected. This type of traffic is typically email, DNS, HTTP, or HTTPS traffic. Return traffic from the DMZ to the public network is dynamically permitted.

84. A client connects to a Web server. Which component of this HTTP connection is not examined by a stateful firewall?

- the source IP address of the client traffic
- the destination port number of the client traffic
- **the actual contents of the HTTP connection**
- the source port number of the client traffic

Explanation: Stateful firewalls cannot prevent application layer attacks because they do not examine the actual contents of the HTTP connection.

85. Which network monitoring technology uses VLANs to monitor traffic on remote switches?

- IPS
- IDS
- TAP
- **RSPAN**

Explanation: Remote SPAN (RSPAN) enables a network administrator to use the flexibility of VLANs to monitor traffic on remote switches.

86. Which rule action will cause Snort IPS to block and log a packet?

- log
- **drop**
- alert
- Sdrop

Explanation: Snort IPS mode can perform all the IDS actions plus the following:
– Drop – Block and log the packet.
– Reject – Block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
– Sdrop – Block the packet but do not log it.

87. What is typically used to create a security trap in the data center facility?

- **IDs, biometrics, and two access doors**
- high resolution monitors
- redundant authentication servers
- a server without all security patches applied

Explanation: Security traps provide access to the data halls where data center data is stored. As shown in the figure below, a security trap is similar to an air lock. A person must first enter the security trap using their badge ID proximity card. After the person is inside the security trap, facial recognition, fingerprints, or other biometric verifications are used to open the second door. The user must repeat the process to exit the data hall.

88. A company is concerned with leaked and stolen corporate data on hard copies. Which data loss mitigation technique could help with this situation?

- strong PC security settings
- strong passwords
- **shredding**
- encryption

Explanation: Confidential data should be shredded when no longer required. Otherwise, a thief could retrieve discarded reports and gain valuable information.

89. Upon completion of a network security course, a student decides to pursue a career in cryptanalysis. What job would the student be doing as a cryptanalyst?

- **cracking code without access to the shared secret key**
- creating hashing codes to authenticate data
- making and breaking secret codes
- creating transposition and substitution ciphers

Explanation: Cryptanalysis is the practice and study of determining the meaning of encrypted information (cracking the code), without access to the shared secret key. This is also known as codebreaking.

90. What command is used on a switch to set the port access entity type so the interface acts only as an authenticator and will not respond to any messages meant for a supplicant?

- **dot1x pae authenticator**
- authentication port-control auto
- aaa authentication dot1x default group radius
- dot1x system-auth-control

Explanation: Sets the Port Access Entity (PAE) type.
dot1x pae [supplicant | authenticator | both]

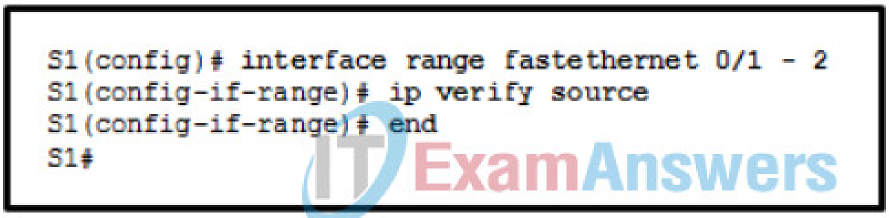
- supplicant—The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator.
- authenticator-—The interface acts only as an authenticator and does not respond to any messages meant for a supplicant.
- both—The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages.

91. What are two disadvantages of using an IDS? (Choose two.)

- **The IDS does not stop malicious traffic.**
- The IDS works offline using copies of network traffic.
- The IDS has no impact on traffic.
- The IDS analyzes actual forwarded packets.
- **The IDS requires other devices to respond to attacks.**

Explanation: The disadvantage of operating with mirrored traffic is that the IDS cannot stop malicious single-packet attacks from reaching the target before responding to the attack. Also, an IDS often requires assistance from other networking devices, such as routers and firewalls, to respond to an attack. An advantage of an IDS is that by working offline using mirrored traffic, it has no impact on traffic flow.

92. Refer to the exhibit. The ip verify source command is applied on untrusted interfaces. Which type of attack is mitigated by using this configuration?



```
S1(config)# interface range fastethernet 0/1 - 2
S1(config-if-range)# ip verify source
S1(config-if-range)# end
S1#
```

- DHCP spoofing
- DHCP starvation
- STP manipulation
- **MAC and IP address spoofing**

Explanation: To protect against MAC and IP address spoofing, apply the IP Source Guard security feature, using the **ip verify source** command, on untrusted ports.

93. What ports can receive forwarded traffic from an isolated port that is part of a PVLAN?

- other isolated ports and community ports
- **only promiscuous ports**
- all other ports within the same community
- only isolated ports

Explanation: PVLANs are used to provide Layer 2 isolation between ports within the same broadcast domain. The level of isolation can be specified with three types of PVLAN ports:
– Promiscuous ports that can forward traffic to all other ports
– Isolated ports that can only forward traffic to promiscuous ports

– Community ports that can forward traffic to other community ports and promiscuous ports

94. A user complains about being locked out of a device after too many unsuccessful AAA login attempts. What could be used by the network administrator to provide a secure authentication access method without locking a user out of a device?

- **Use the login delay command for authentication attempts.**
- Use the login local command for authenticating user access.
- Use the aaa local authentication attempts max-fail global configuration mode command with a higher number of acceptable failures.
- Use the none keyword when configuring the authentication method list.

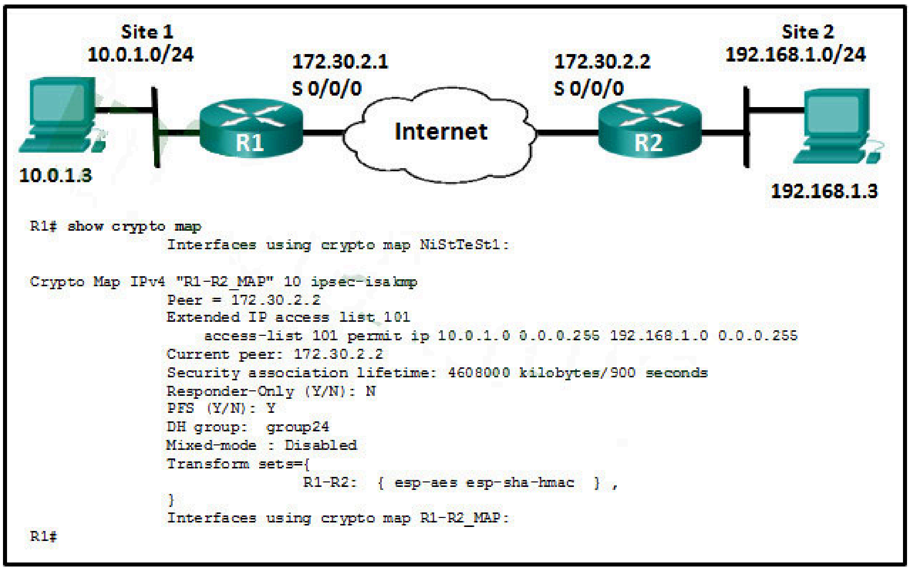
Explanation: The login delay command introduces a delay between failed login attempts without locking the account. This provides a user with unlimited attempts at accessing a device without causing the user account to become locked and thus requiring administrator intervention.

95. What are two drawbacks in assigning user privilege levels on a Cisco router? (Choose two.)

- Only a root user can add or remove commands.
- Privilege levels must be set to permit access control to specific device interfaces, ports, or slots.
- **Assigning a command with multiple keywords allows access to all commands using those keywords.**
- **Commands from a lower level are always executable at a higher level.**
- AAA must be enabled.

Explanation: Privilege levels may not provide desired flexibility and specificity because higher levels always inherit commands from lower levels, and commands with multiple keywords give the user access to all commands available for each keyword. Privilege levels cannot specify access control to interfaces, ports, or slots. AAA is not required to set privilege levels, but is required in order to create role-based views. The role of root user does not exist in privilege levels.

96. Refer to the exhibit. Which conclusion can be made from the show crypto map command output that is shown on R1?



```
R1# show crypto map
               Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "R1-R2_MAP" 10 ipsec-isakmp
               Peer = 172.30.2.2
               Extended IP access list 101
                   access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
               Current peer: 172.30.2.2
               Security association lifetime: 4608000 kilobytes/900 seconds
               Responder-Only (Y/N): N
               PFS (Y/N): Y
               DH group:  group24
               Mixed-mode : Disabled
               Transform sets={
                              R1-R2:  { esp-aes esp-sha-hmac  } ,
               }
               Interfaces using crypto map R1-R2_MAP:
R1#
```

- **The crypto map has not yet been applied to an interface.**
- The current peer IP address should be 172.30.2.1.
- There is a mismatch between the transform sets.
- The tunnel configuration was established and can be tested with extended pings.

Explanation: According to the **show crypto map** command output, all required SAs are in place, but no interface is currently using the crypto map. To complete the tunnel configuration, the crypto map has to be applied to the outbound interface of each router.

97. What are two reasons to enable OSPF routing protocol authentication on a network? (Choose two.)

- **to prevent data traffic from being redirected and then discarded**
- to ensure faster network convergence
- to provide data security through encryption
- **to prevent redirection of data traffic to an insecure link**
- to ensure more efficient routing

Explanation: The reason to configure OSPF authentication is to mitigate against routing protocol attacks like redirection of data traffic to an insecure link, and redirection of data traffic to discard it. OSPF authentication does not provide faster network convergence, more efficient routing, or encryption of data traffic.

98. Which three functions are provided by the syslog logging service? (Choose three.)

- **gathering logging information**
- authenticating and encrypting data sent over the network
- retaining captured messages on the router when a router is rebooted
- **specifying where captured information is stored**
- **distinguishing between information to be captured and information to be ignored**
- setting the size of the logging buffer

Explanation: Syslog operations include gathering information, selecting which type of information to capture, and directing the captured information to a storage location. The logging service stores messages in a logging buffer that is time-limited, and cannot retain the information when a router is rebooted. Syslog does not authenticate or encrypt messages.

99. What two ICMPv6 message types must be permitted through IPv6 access control lists to allow resolution of Layer 3 addresses to Layer 2 MAC addresses? (Choose two.)

- **neighbor solicitations**
- echo requests
- **neighbor advertisements**
- echo replies
- router solicitations
- router advertisements

100. Which three services are provided through digital signatures? (Choose three.)

- accounting
- **authenticity**
- compression
- **nonrepudiation**
- **integrity**
- encryption

Explanation: Digital signatures use a mathematical technique to provide three basic security services:Integrity; Authenticity; Nonrepudiation

101. A technician is to document the current configurations of all network devices in a college, including those in off-site buildings. Which protocol would be best to use to securely access the network devices?

- FTP
- HTTP
- **SSH**
- Telnet

Explanation: Telnet sends passwords and other information in clear text, while SSH encrypts its data.

FTP and HTTP do not provide remote device access for configuration purposes.

102. An administrator is trying to develop a BYOD security policy for employees that are bringing a wide range of devices to connect to the company network. Which three objectives must the BYOD security policy address? (Choose three.)

- All devices must be insured against liability if used to compromise the corporate network.
- All devices must have open authentication with the corporate network.
- **Rights and activities permitted on the corporate network must be defined.**
- **Safeguards must be put in place for any personal device being compromised.**
- **The level of access of employees when connecting to the corporate network must be defined.**
- All devices should be allowed to attach to the corporate network flawlessly.

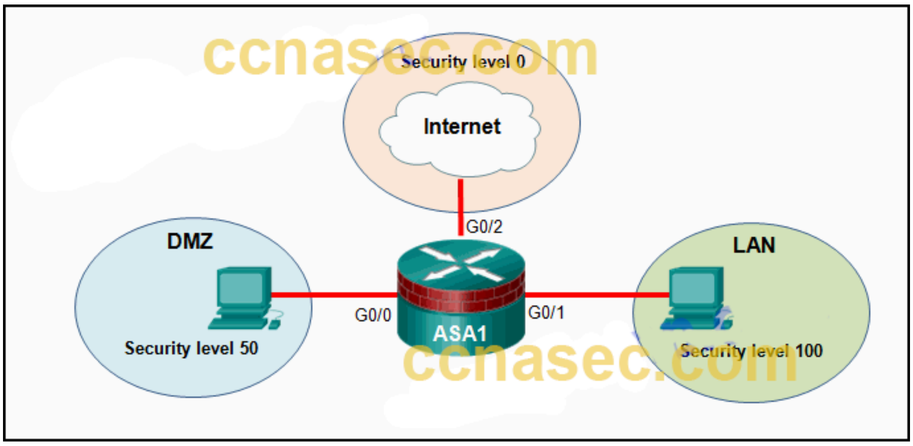
103. What is the function of the pass action on a Cisco IOS Zone-Based Policy Firewall?

- logging of rejected or dropped packets
- inspecting traffic between zones for traffic control
- tracking the state of connections between zones
- **forwarding traffic from one zone to another**

Explanation: The pass action performed by Cisco IOS ZPF permits forwarding of traffic in a manner similar to the permit statement in an access control list.

104. Refer to the exhibit. Based on the security levels of the interfaces on ASA1, what traffic will be allowed on

the interfaces?



- Traffic from the Internet and DMZ can access the LAN.
- Traffic from the Internet and LAN can access the DMZ.
- Traffic from the Internet can access both the DMZ and the LAN.
- **Traffic from the LAN and DMZ can access the Internet.**

Explanation: ASA devices have security levels assigned to each interface that are not part of a configured ACL. These security levels allow traffic from more secure interfaces, such as security level 100, to access less secure interfaces, such as level 0. By default, they allow traffic from more secure interfaces (higher security level) to access less secure interfaces (lower security level). Traffic from the less secure interfaces is blocked from accessing more secure interfaces.

105. What network testing tool can be used to identify network layer protocols running on a host?

- SIEM
- **Nmap**
- L0phtcrack
- Tripwire

106. In the implementation of security on multiple devices, how do ASA ACLs differ from Cisco IOS ACLs?

- Cisco IOS routers utilize both named and numbered ACLs and Cisco ASA devices utilize only numbered ACLs.
- **Cisco IOS ACLs are configured with a wildcard mask and Cisco ASA ACLs are configured with a subnet mask.**
- Cisco IOS ACLs are processed sequentially from the top down and Cisco ASA ACLs are not processed sequentially.
- Cisco IOS ACLs utilize an implicit deny all and Cisco ASA ACLs end with an implicit permit all.

Explanation: The Cisco IOS ACLs are configured with a wildcard mask and the Cisco ASA ACLs are configured with a subnet mask. Both devices use an implicit deny, top down sequential processing, and named or numbered ACLs.

107. Which statement describes an important characteristic of a site-to-site VPN?

- **It must be statically set up.**
- It is ideally suited for use by mobile workers.
- It requires using a VPN client on the host PC.
- After the initial connection is established, it can dynamically change connection information.
- It is commonly implemented over dialup and cable modem networks.

Explanation: A site-to-site VPN is created between the network devices of two separate networks. The VPN is static and stays established. The internal hosts of the two networks have no knowledge of the VPN.

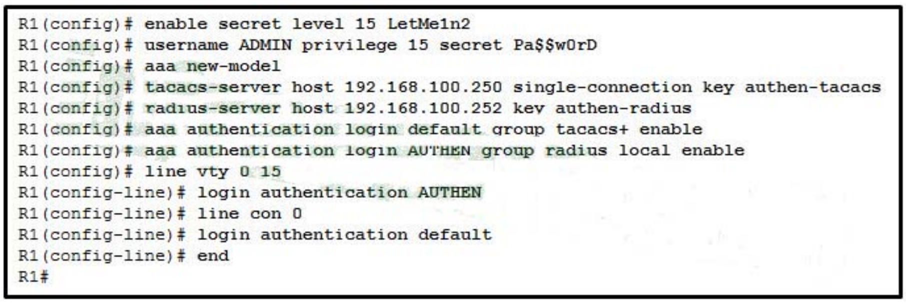
108. Which two options are security best practices that help mitigate BYOD risks? (Choose two.)

- Use paint that reflects wireless signals and glass that prevents the signals from going outside the building.
- **Keep the device OS and software updated.**

- Only allow devices that have been approved by the corporate IT team.
- **Only turn on Wi-Fi when using the wireless network.**
- Decrease the wireless antenna gain level.
- Use wireless MAC address filtering.

Explanation: Many companies now support employees and visitors attaching and using wireless devices that connect to and use the corporate wireless network. This practice is known as a bring-your-own-device policy or BYOD. Commonly, BYOD security practices are included in the security policy. Some best practices that mitigate BYOD risks include the following:
Use unique passwords for each device and account.
Turn off Wi-Fi and Bluetooth connectivity when not being used. Only connect to trusted networks.
Keep the device OS and other software updated.
Backup any data stored on the device.
Subscribe to a device locator service with a remote wipe feature.
Provide antivirus software for approved BYODs.
Use Mobile Device Management (MDM) software that allows IT teams to track the device and implement security settings and software controls.

109. Refer to the exhibit. A network administrator configures AAA authentication on R1. Which statement describes the effect of the keyword single-connection in the configuration?



```
R1(config)# enable secret level 15 LetMe1n2
R1(config)# username ADMIN privilege 15 secret Pa$$w0rD
R1(config)# aaa new-model
R1(config)# tacacs-server host 192.168.100.250 single-connection key authen-tacacs
R1(config)# radius-server host 192.168.100.252 key authen-radius
R1(config)# aaa authentication login default group tacacs+ enable
R1(config)# aaa authentication login AUTHEN group radius local enable
R1(config)# line vty 0 15
R1(config-line)# login authentication AUTHEN
R1(config-line)# line con 0
R1(config-line)# login authentication default
R1(config-line)# end
R1#
```

- R1 will open a separate connection to the TACACS+ server for each user authentication session.
- **The authentication performance is enhanced by keeping the connection to the TACACS+ server open.**
- The TACACS+ server only accepts one successful try for a user to authenticate with it.
- R1 will open a separate connection to the TACACS server on a per source IP address basis for each authentication session.

Explanation: The single-connection keyword enhances TCP performance with TACACS+ by maintaining a single TCP connection for the life of the session. Without the single-connection keyword, a TCP connection is opened and closed per session.

110. A recently created ACL is not working as expected. The admin determined that the ACL had been applied inbound on the interface and that was the incorrect direction. How should the admin fix this issue?

- **Delete the original ACL and create a new ACL, applying it outbound on the interface.**
- Add an association of the ACL outbound on the same interface.
- Fix the ACE statements so that it works as desired inbound on the interface.
- Remove the inbound association of the ACL on the interface and reapply it outbound.

111. What characteristic of the Snort term-based subscriptions is true for both the community and the subscriber rule sets?

- Both have a 30-day delayed access to updated signatures.
- Both use Cisco Talos to provide coverage in advance of exploits.
- Both are fully supported by Cisco and include Cisco customer support.

- **Both offer threat protection against security threats.**

Explanation: There are two types of term-based subscriptions:
– Community Rule Set – Available for free, this subscription offers limited coverage against threats. The community rule set focuses on reactive response to security threats versus proactive research work. There is also a 30-day delayed access to updated signatures meaning that newest rule will be a minimum of 30 days old. In addition, there is no Cisco customer support available.
– Subscriber Rule Set – Available for a fee, this service provides the best protection against threats. It includes coverage of advance exploits by using the research work of the Cisco Talos security experts. The Subscriber Rule Set also provides the fastest access to updated signatures in response to a security incident or the proactive discovery of a new threat. This subscription is fully supported by Cisco.

112. A security analyst is configuring Snort IPS. The analyst has just downloaded and installed the Snort OVA file. What is the next step?

- Verify Snort IPS.
- **Configure Virtual Port Group interfaces.**
- Enable IPS globally or on desired interfaces.
- Activate the virtual services.

Explanation: To deploy Snort IPS on supported devices, perform the following steps:
– Step 1. Download the Snort OVA file.
– Step 2. Install the OVA file.
– Step 3. Configure Virtual Port Group interfaces.
– Step 4. Activate the virtual services.
– Step 5. Configure Snort specifics.

– Step 6. Enable IPS globally or on desired interfaces.
– Step 7. Verify Snort IPS.

113. The security policy in a company specifies that employee workstations can initiate HTTP and HTTPS connections to outside websites and the return traffic is allowed. However, connections initiated from outside hosts are not allowed. Which parameter can be used in extended ACLs to meet this requirement?

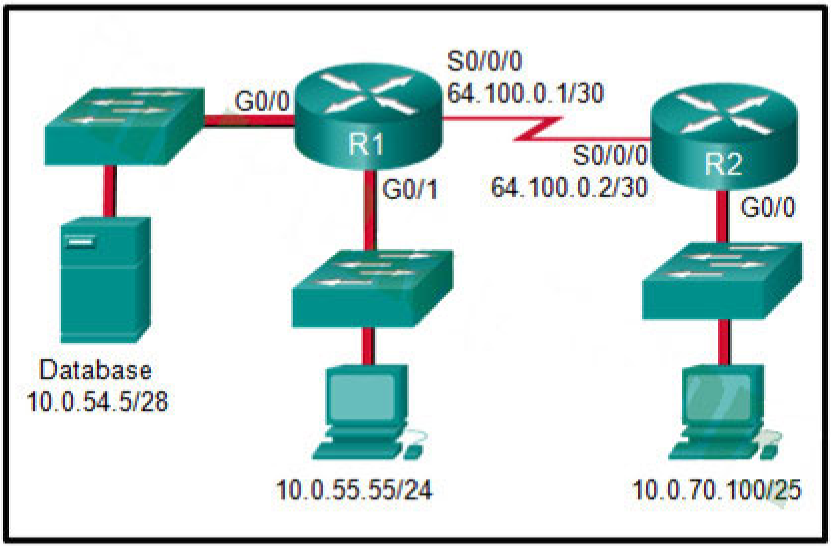
- dscp
- precedence
- eq
- **established**

114. A researcher is comparing the differences between a stateless firewall and a proxy firewall. Which two additional layers of the OSI model are inspected by a proxy firewall? (Choose two.)

- Layer 3
- Layer 4
- **Layer 5**
- Layer 6
- **Layer 7**

Explanation: Packet filtering firewalls are usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
An application gateway firewall (proxy firewall), as shown in the figure, filters information at Layers 3, 4, 5, and 7 of the OSI reference model.

115. Refer to the exhibit. A network administrator is configuring a VPN between routers R1 and R2. Which commands would correctly configure a pre-shared key for the two routers?



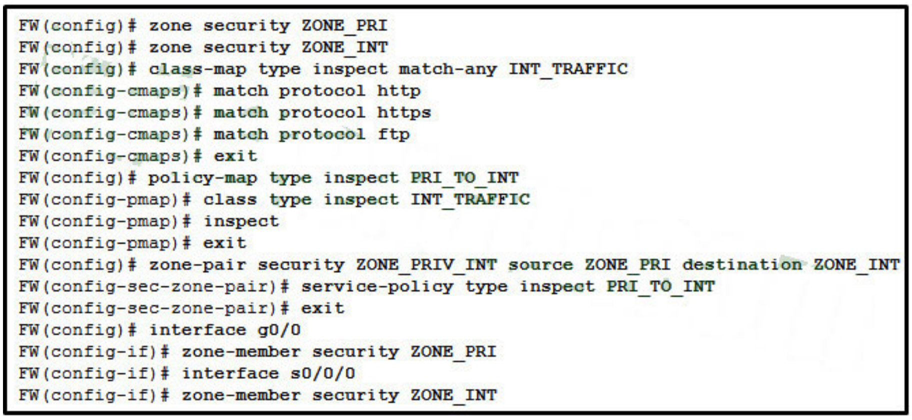
R1(config)# username R2 password 5tayout!
R2(config)# username R1 password 5tayout!

R1(config)# crypto isakmp key 5tayout! address 64.100.0.2
R2(config)# crypto isakmp key 5tayout! address 64.100.0.1

R1(config)# crypto isakmp key 5tayout! hostname R1
R2(config)# crypto isakmp key 5tayout! hostname R2

R1(config-if)# ppp pap sent-username R1 password 5tayout!
R2(config-if)# ppp pap sent-username R2 password 5tayout!

116. Refer to the exhibit. Which statement is true about the effect of this Cisco IOS zone-based policy firewall configuration?



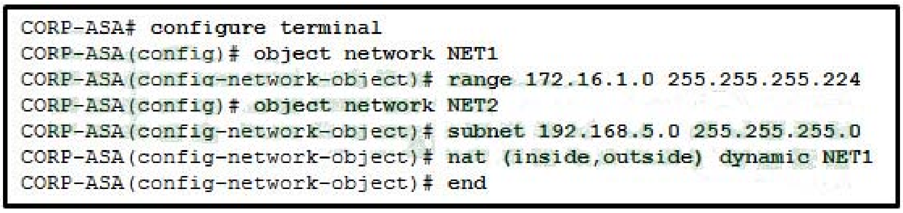
```
FW(config)# zone security ZONE_PRI
FW(config)# zone security ZONE_INT
FW(config)# class-map type inspect match-any INT_TRAFFIC
FW(config-cmaps)# match protocol http
FW(config-cmaps)# match protocol https
FW(config-cmaps)# match protocol ftp
FW(config-cmaps)# exit
FW(config)# policy-map type inspect PRI_TO_INT
FW(config-pmap)# class type inspect INT_TRAFFIC
FW(config-pmap)# inspect
FW(config-pmap)# exit
FW(config)# zone-pair security ZONE_PRIV_INT source ZONE_PRI destination ZONE_INT
FW(config-sec-zone-pair)# service-policy type inspect PRI_TO_INT
FW(config-sec-zone-pair)# exit
FW(config)# interface g0/0
FW(config-if)# zone-member security ZONE_PRI
FW(config-if)# interface s0/0/0
FW(config-if)# zone-member security ZONE_INT
```

- The firewall will automatically drop all HTTP, HTTPS, and FTP traffic.
- The firewall will automatically allow HTTP, HTTPS, and FTP traffic from s0/0/0 to g0/0 and will track the connections. Tracking the connection allows only return traffic to be permitted through the firewall in the opposite direction.
- The firewall will automatically allow HTTP, HTTPS, and FTP traffic from s0/0/0 to g0/0, but will not track the state of connections. A corresponding policy must be applied to allow return traffic to be permitted through the firewall in the opposite direction.
- **The firewall will automatically allow HTTP, HTTPS, and FTP traffic from g0/0 to s0/0/0 and will track the connections. Tracking the connection allows only return traffic to be permitted through the firewall in the opposite direction.**
- return traffic to be permitted through the firewall in the opposite direction.
- The firewall will automatically allow HTTP, HTTPS, and FTP traffic from g0/0 to s0/0/0, but will not track the state of connections. A corresponding policy must be applied to allow return traffic to be permitted through the firewall in the opposite direction.

117. Which privilege level has the most access to the Cisco IOS?

- level 0
- **level 15**
- level 7
- level 16
- level 1

118. Refer to the exhibit. A network administrator has configured NAT on an ASA device. What type of NAT is used?



```
CORP-ASA# configure terminal
CORP-ASA(config)# object network NET1
CORP-ASA(config-network-object)# range 172.16.1.0 255.255.255.224
CORP-ASA(config)# object network NET2
CORP-ASA(config-network-object)# subnet 192.168.5.0 255.255.255.0
CORP-ASA(config-network-object)# nat (inside,outside) dynamic NET1
CORP-ASA(config-network-object)# end
```

- **inside NAT**
- static NAT
- bidirectional NAT
- outside NAT

Explanation: NAT can be deployed on an ASA using one of these methods:
inside NAT – when a host from a higher-security interface has traffic destined for a lower-security interface and the ASA translates the internal host address to a global address
outside NAT – when traffic from a lower-security interface destined for a host on the higher-security interface is translated
bidirectional NAT – when both inside NAT and outside NAT are used together
Because the nat command is applied so that the inside interface is mapped to the outside interface, the NAT type is inside. Also, the dynamic keyword in the nat command indicates that it is a dynamic mapping.

119. A network analyst is configuring a site-to-site IPsec VPN. The analyst has configured both the ISAKMP and IPsec policies. What is the next step?

- Configure the hash as SHA and the authentication as pre-shared.
- **Apply the crypto map to the appropriate outbound interfaces.**
- Issue the show crypto ipsec sa command to verify the tunnel.
- Verify that the security feature is enabled in the IOS.

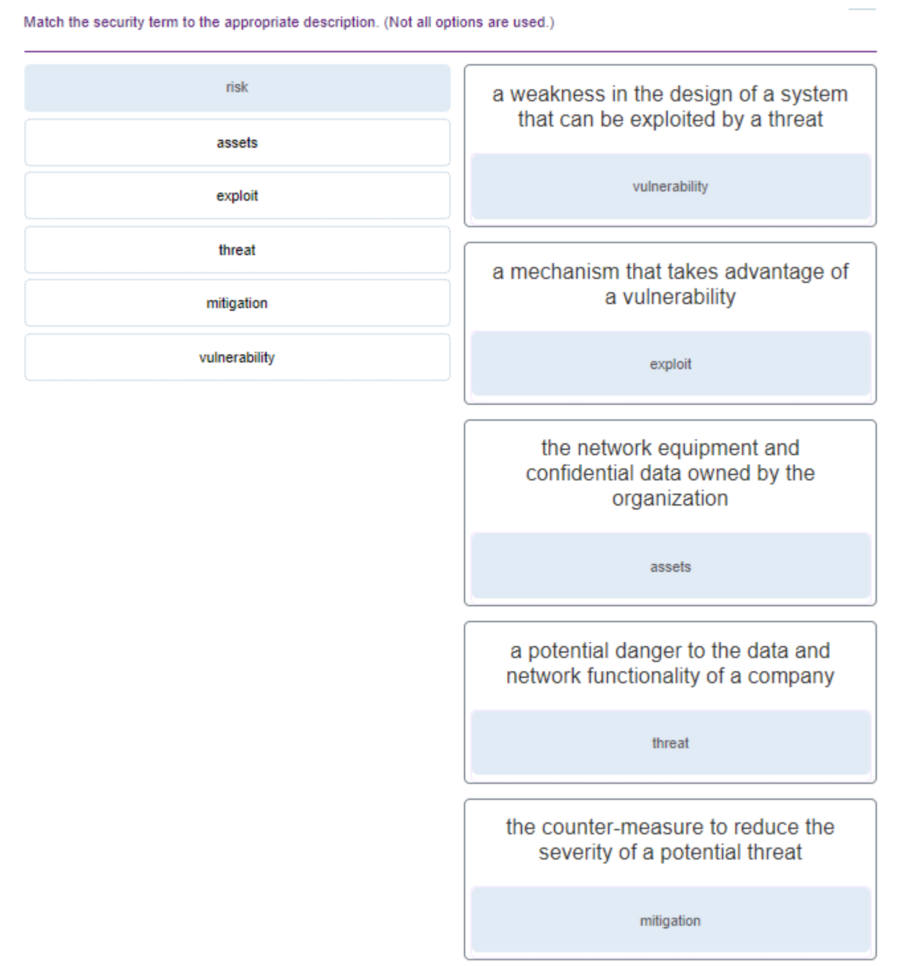
120. When an inbound Internet-traffic ACL is being implemented, what should be included to prevent the spoofing of internal networks?

- **ACEs to prevent traffic from private address spaces**
- ACEs to prevent broadcast address traffic

- ACEs to prevent ICMP traffic
- ACEs to prevent HTTP traffic
- ACEs to prevent SNMP traffic

Explanation: Common ACEs to assist with antispoofing include blocking packets that have a source address in the 127.0.0.0/8 range, any private address, or any multicast addresses. Furthermore, the administrator should not allow any outbound packets with a source address other than a valid address that is used in the internal networks of the organization.

121. Match the security term to the appropriate description. (Not all options are used.)



Match the security term to the appropriate description. (Not all options are used.)

- risk
- assets
- exploit
- threat
- mitigation
- vulnerability

a weakness in the design of a system that can be exploited by a threat	vulnerability
a mechanism that takes advantage of a vulnerability	exploit
the network equipment and confidential data owned by the organization	assets
a potential danger to the data and network functionality of a company	threat
the counter-measure to reduce the severity of a potential threat	mitigation

Match the security term to the appropriate description

122. Which two types of attacks are examples of reconnaissance attacks? (Choose two.)

- brute force
- **port scan**

- **ping sweep**
- man-in-the-middle
- SYN flood

Explanation: Reconnaissance attacks attempt to gather information about the targets. Ping sweeps will indicate which hosts are up and responding to pings, whereas port scans will indicate on which TCP and UDP ports the target is listening for incoming connections. Man-in-the-middle and brute force attacks are both examples of access attacks, and a SYN flood is an example of a denial of service (DoS) attack.

123. Which Cisco solution helps prevent ARP spoofing and ARP poisoning attacks?

- **Dynamic ARP Inspection**
- IP Source Guard
- DHCP Snooping
- Port Security

124. When the Cisco NAC appliance evaluates an incoming connection from a remote device against the defined network policies, what feature is being used?

- **posture assessment**
- remediation of noncompliant systems
- authentication and authorization
- quarantining of noncompliant systems

125. Which two steps are required before SSH can be enabled on a Cisco router? (Choose two.)

- **Give the router a host name and domain name.**
- Create a banner that will be displayed to users when they connect.
- **Generate a set of secret keys to be used for encryption and decryption.**
- Set up an authentication server to handle incoming connection requests.

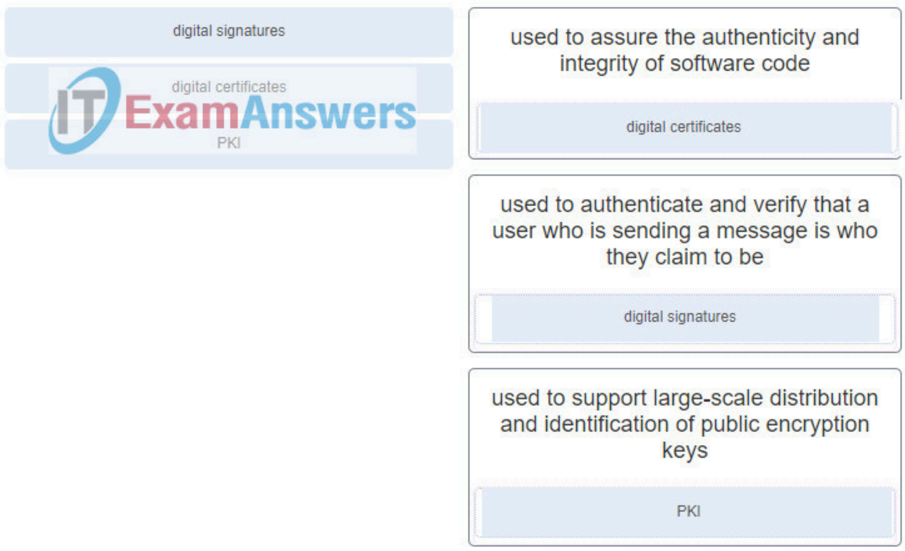
- Enable SSH on the physical interfaces where the incoming connection requests will be received.

Explanation: There are four steps to configure SSH on a Cisco router. First, set the host name and domain name. Second, generate a set of RSA keys to be used for encrypting and decrypting the traffic. Third, create the user IDs and passwords of the users who will be connecting. Lastly, enable SSH on the vty lines on the router. SSH does not need to be set up on any physical interfaces, nor does an external authentication server need to be used. While it is a good idea to configure a banner to display legal information for connecting users, it is not required to enable SSH.

126. The network administrator for an e-commerce website requires a service that prevents customers from claiming that legitimate orders are fake. What service provides this type of guarantee?

- confidentiality
- authentication
- integrity
- **nonrepudiation**

127. Match the security technology with the description.



digital signatures

digital certificates

PKI

used to assure the authenticity and integrity of software code

digital certificates

used to authenticate and verify that a user who is sending a message is who they claim to be

digital signatures

used to support large-scale distribution and identification of public encryption keys

PKI

128. What functionality is provided by Cisco SPAN in a switched network?

- **It mirrors traffic that passes through a switch port or VLAN to another port for traffic analysis.**
- It prevents traffic on a LAN from being disrupted by a broadcast storm.
- It protects the switched network from receiving BPDUs on ports that should not be receiving them.
- It copies traffic that passes through a switch interface and sends the data directly to a syslog or SNMP server for analysis.
- It inspects voice protocols to ensure that SIP, SCCP, H.323, and MGCP requests conform to voice standards.
- It mitigates MAC address overflow attacks.

Explanation: SPAN is a Cisco technology used by network administrators to monitor suspicious traffic or to capture traffic to be analyzed.

129. Which three statements are generally considered to be best practices in the placement of ACLs? (Choose three.)

- **Filter unwanted traffic before it travels onto a low-bandwidth link.**
- **Place standard ACLs close to the destination IP address of the traffic.**
- Place standard ACLs close to the source IP address of the traffic.
- Place extended ACLs close to the destination IP address of the traffic.
- **Place extended ACLs close to the source IP address of the traffic.**
- For every inbound ACL placed on an interface, there should be a matching outbound ACL.

Explanation: Extended ACLs should be placed as close as possible to the source IP address, so that traffic that needs to be filtered does not cross the network and use network resources. Because standard ACLs do not specify a destination address, they should be placed as close to the destination as possible. Placing a standard ACL close to the source may have the effect of filtering all traffic, and limiting services to other hosts. Filtering unwanted traffic before it enters low-bandwidth links preserves bandwidth and supports network functionality. Decisions on placing ACLs inbound or outbound are dependent on the requirements to be met.

130. What function is performed by the class maps configuration object in the Cisco modular policy framework?

- **identifying interesting traffic**
- applying a policy to an interface
- applying a policy to interesting traffic
- restricting traffic through an interface

Explanation: There are three configuration objects in the MPF; class maps, policy maps, and service policy. The class maps configuration object uses match criteria to identify interesting traffic.

131. In an attempt to prevent network attacks, cyber analysts share unique identifiable attributes of known attacks with colleagues. What three types of attributes or indicators of compromise are helpful to share? (Choose three.)

- **IP addresses of attack servers**
- **changes made to end system software**
- netbios names of compromised firewalls
- **features of malware files**
- BIOS of attacking systems
- system ID of compromised systems

Explanation: Many network attacks can be prevented by sharing information about indicators of compromise

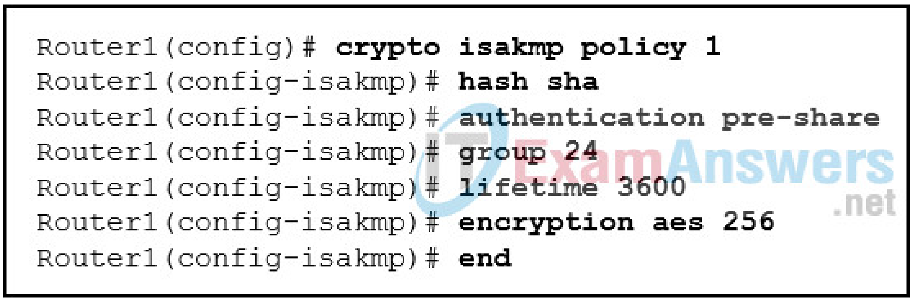
(IOC). Each attack has unique identifiable attributes. Indicators of compromise are the evidence that an attack has occurred. IOCs can be identifying features of malware files, IP addresses of servers that are used in the attack, filenames, and characteristic changes made to end system software.

132. What two assurances does digital signing provide about code that is downloaded from the Internet? (Choose two.)

- **The code is authentic and is actually sourced by the publisher.**
- The code contains no errors.
- **The code has not been modified since it left the software publisher.**
- The code contains no viruses.
- The code was encrypted with both a private and public key.

Explanation: Digitally signing code provides several assurances about the code:
The code is authentic and is actually sourced by the publisher.
The code has not been modified since it left the software publisher.
The publisher undeniably published the code. This provides nonrepudiation of the act of publishing.

133. Refer to the exhibit. What algorithm is being used to provide public key exchange?



```
Router1(config)# crypto isakmp policy 1
Router1(config-isakmp)# hash sha
Router1(config-isakmp)# authentication pre-share
Router1(config-isakmp)# group 24
Router1(config-isakmp)# lifetime 3600
Router1(config-isakmp)# encryption aes 256
Router1(config-isakmp)# end
```

- SHA
- RSA
- **Diffie-Hellman**
- AES

Explanation: The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. DH (Diffie-Hellman) is an algorithm used for key exchange. DH is a public key exchange method and allows two IPsec peers to establish a shared secret key over an insecure channel.

134. Which two statements describe the use of asymmetric algorithms? (Choose two.)

- Public and private keys may be used interchangeably.
- If a public key is used to encrypt the data, a public key must be used to decrypt the data.
- **If a private key is used to encrypt the data, a public key must be used to decrypt the data.**
- **If a public key is used to encrypt the data, a private key must be used to decrypt the data.**
- If a private key is used to encrypt the data, a private key must be used to decrypt the data.

Explanation: Asymmetric algorithms use two keys: a public key and a private key. Both keys are capable of the encryption process, but the complementary matched key is required for decryption. If a public key encrypts the data, the matching private key decrypts the data. The opposite is also true. If a private key encrypts the data, the corresponding public key decrypts the data.

135. Which statement is a feature of HMAC?

- HMAC uses a secret key that is only known to the sender and defeats man-in-the-middle attacks.

- HMAC uses protocols such as SSL or TLS to provide session layer confidentiality.
- **HMAC uses a secret key as input to the hash function, adding authentication to integrity assurance.**
- HMAC is based on the RSA hash function.

Explanation: A keyed-hash message authentication code (HMAC or KHMAC) is a type of message authentication code (MAC). HMACs use an additional secret key as input to the hash function, adding authentication to data integrity assurance.

136. What is the purpose of the webtype ACLs in an ASA?

- to inspect outbound traffic headed towards certain web sites
- to restrict traffic that is destined to an ASDM
- to monitor return traffic that is in response to web server requests that are initiated from the inside interface
- **to filter traffic for clientless SSL VPN users**

Explanation: The webtype ACLs are used in a configuration that supports filtering for clientless SSL VPN users.

137. Which two statements describe the effect of the access control list wildcard mask 0.0.0.15? (Choose two.)

- **The first 28 bits of a supplied IP address will be matched.**
- The last four bits of a supplied IP address will be matched.
- The first 28 bits of a supplied IP address will be ignored.

- **The last four bits of a supplied IP address will be ignored.**
- The last five bits of a supplied IP address will be ignored.
- The first 32 bits of a supplied IP address will be matched.

Explanation: A wildcard mask uses 0s to indicate that bits must match. 0s in the first three octets represent 24 bits and four more zeros in the last octet, represent a total of 28 bits that must match. The four 1s represented by the decimal value of 15 represents the four bits to ignore.

138. Which type of firewall is the most common and allows or blocks traffic based on Layer 3, Layer 4, and Layer 5 information?

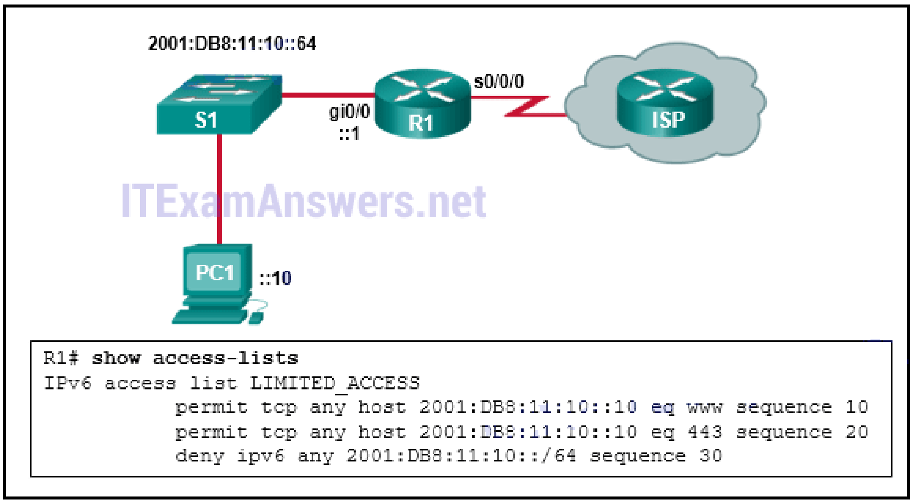
- stateless firewall
- packet filtering firewall
- next generation firewall
- **stateful firewall**

139. Which protocol or measure should be used to mitigate the vulnerability of using FTP to transfer documents between a teleworker and the company file server?

- **SCP**
- TFTP
- ACLs on the file server
- out-of-band communication channel

Explanation: File transfer using FTP is transmitted in plain text. The username and password would be easily captured if the data transmission is intercepted. Secure Copy Protocol (SCP) conducts the authentication and file transfer under SSH, thus the communication is encrypted. Like FTP, TFTP transfers files unencrypted. ACLs provide network traffic filtering but not encryption. Using an out-of-band communication channel (OOB) either requires physical access to the file server or, if done through the internet, does not necessarily encrypt the communication.

140. Refer to the exhibit. The IPv6 access list LIMITED_ACCESS is applied on the S0/0/0 interface of R1 in the inbound direction. Which IPv6 packets from the ISP will be dropped by the ACL on R1?



```
R1# show access-lists
IPv6 access list LIMITED_ACCESS
           permit tcp any host 2001:DB8:11:10::10 eq www sequence 10
           permit tcp any host 2001:DB8:11:10::10 eq 443 sequence 20
           deny ipv6 any 2001:DB8:11:10::/64 sequence 30
```

- HTTPS packets to PC1
- **ICMPv6 packets that are destined to PC1**
- packets that are destined to PC1 on port 80
- neighbor advertisements that are received from the ISP router

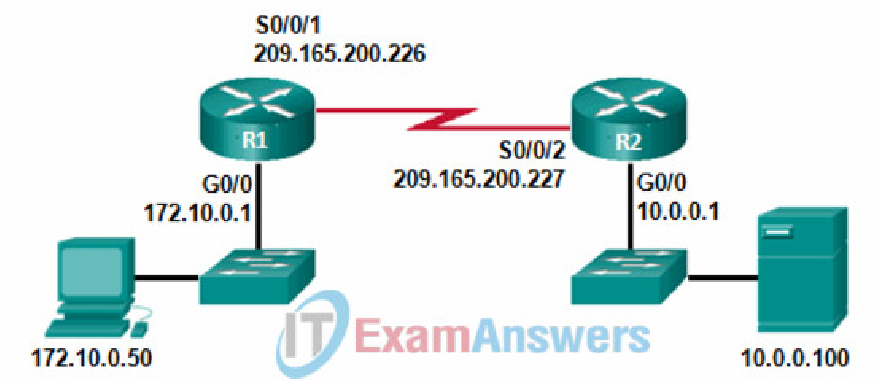
Explanation: The access list LIMITED_ACCESS will block ICMPv6 packets from the ISP. Both port 80, HTTP traffic, and port 443, HTTPS traffic, are explicitly permitted by the ACL. The neighbor advertisements from the ISP router are implicitly permitted by the implicit permit icmp any any nd-na statement at the end of all IPv6 ACLs.

141. What tool is available through the Cisco IOS CLI to initiate security audits and to make recommended configuration changes with or without administrator input?

- Control Plane Policing

- **Cisco AutoSecure**
- Cisco ACS
- Simple Network Management Protocol

142. Refer to the exhibit. Which pair of crypto isakmp key commands would correctly configure PSK on the two routers?



Network Security Course Final Exam Q142

- **R1(config)# crypto isakmp key cisco123 address 209.165.200.227**
  R2(config)# crypto isakmp key cisco123 address 209.165.200.226
- R1(config)# crypto isakmp key cisco123 address 209.165.200.226
  R2(config)# crypto isakmp key cisco123 address 209.165.200.227
- R1(config)# crypto isakmp key cisco123 hostname R1
  R2(config)# crypto isakmp key cisco123 hostname R2
- R1(config)# crypto isakmp key cisco123 address 209.165.200.226
  R2(config)# crypto isakmp key secure address 209.165.200.227

Explanation: The correct syntax of the crypto isakmp key command is as follows:
crypto isakmp key keystring address peer-address
or
crypto isakmp keykeystring hostname peer-hostnameSo, the correct answer would be the following:
R1(config)# crypto isakmp key cisco123 address

```
209.165.200.227
R2(config)# crypto isakmp key cisco123 address
209.165.200.226
```

143. Which two technologies provide enterprise-managed VPN solutions? (Choose two.)

- Layer 3 MPLS VPN
- Frame Relay
- **site-to-site VPN**
- Layer 2 MPLS VPN
- **remote access VPN**

144. What are the three components of an STP bridge ID? (Choose three.)

- the date and time that the switch was brought online
- the hostname of the switch
- **the MAC address of the switch**
- **the extended system ID**
- **the bridge priority value**
- the IP address of the management VLAN

145. What are two differences between stateful and packet filtering firewalls? (Choose two.)

- A packet filtering firewall will prevent spoofing by determining whether packets belong to an existing connection while a stateful firewall follows pre-configured rule sets.
- **A stateful firewall provides more stringent control over security than a packet filtering firewall.**
- A packet filtering firewall is able to filter sessions that use dynamic port negotiations while a stateful firewall cannot.
- **A stateful firewall will provide more logging information than a packet filtering firewall.**
- A statefull firewall will examine each packet individually while a packet filtering firewall observes the state of a connection.

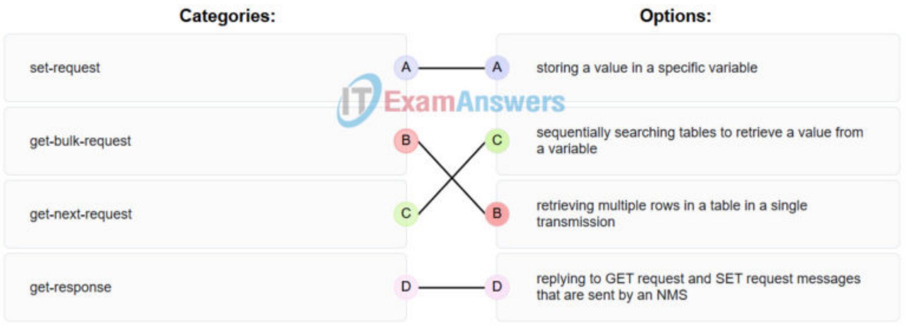
Explanation: *There are many differences between a stateless and stateful firewall.*
Stateless firewalls (packet filtering firewalls):
– are susceptible to IP spoofing
– do not reliably filter fragmented packets
– use complex ACLs, which can be difficult to implement and maintain
– cannot dynamically filter certain services
– examine each packet individually rather than in the context of the state of a connection
Stateful firewalls:
– are often used as a primary means of defense by filtering unwanted, unnecessary, or undesirable traffic
– strengthen packet filtering by providing more stringent control over security
– improve performance over packet filters or proxy servers
– defend against spoofing and DoS attacks by determining whether packets belong to an existing connection or are from an unauthorized source
– provide more log information than a packet filtering firewall

146. Which portion of the Snort IPS rule header identifies the destination port?

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $H
```

any
$HTTP_PORTS
$HOME_NET
tcp

147. Match each SNMP operation to the corresponding description. (Not all options are used.)



set-request — storing a value in a specific variable

get-bulk-request — sequentially searching tables to retrieve a value from a variable

get-next-request — retrieving multiple rows in a table in a single transmission

get-response — replying to GET request and SET request messages that are sent by an NMS

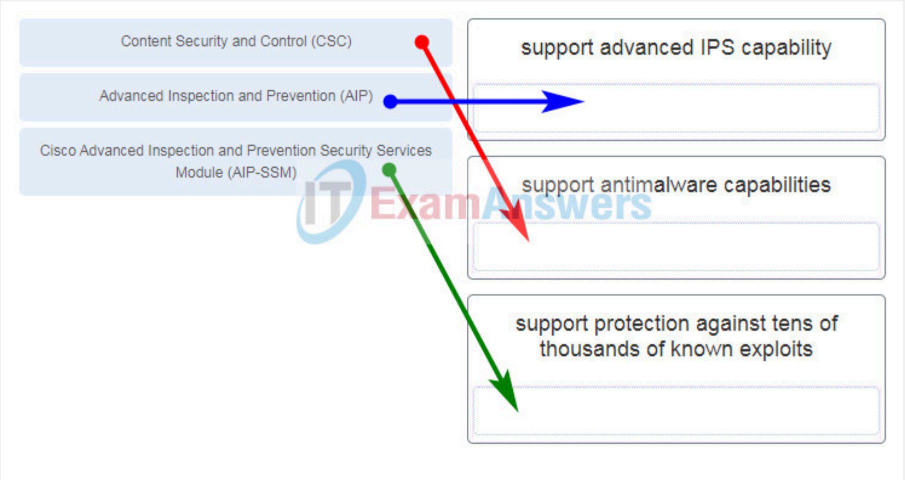
Place the options in the following order:

set-request	storing a value in a specific variable
get-bulk-request	retrieving multiple rows in a table in a single transmission
get-next-request	sequentially searching tables to retrieve a value from a variable
get-response	replying to GET request and SET request messages that are sent by an NMS

148. What port state is used by 802.1X if a workstation fails authorization?

- disabled
- down
- **unauthorized**
- blocking

149. Match the ASA special hardware modules to the description.


Content Security and Control (CSC)

Advanced Inspection and Prevention (AIP)

Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM)

support advanced IPS capability

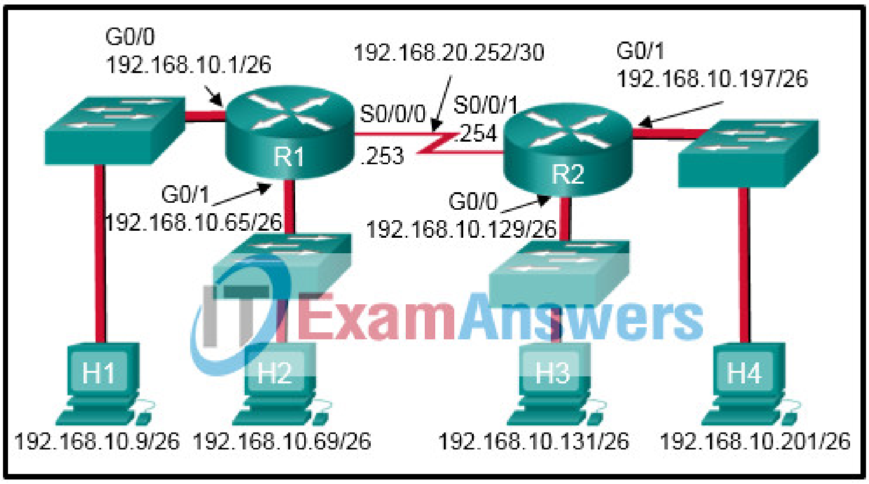
support antimalware capabilities

support protection against tens of thousands of known exploits

Network Security 1.0 Final Exam Answers

Explanation: The advanced threat control and containment services of an ASA firewall are provided by integrating special hardware modules with the ASA architecture. These special modules include:
– Advanced Inspection and Prevention (AIP) module – supports advanced IPS capability.
– Content Security and Control (CSC) module – supports antimalware capabilities.
– Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM) and Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC) – support protection against tens of thousands of known exploits.

150. Refer to the exhibit. Which two ACLs, if applied to the G0/1 interface of R2, would permit only the two LAN networks attached to R1 to access the network that connects to R2 G0/1 interface? (Choose two.)



Network Security 1.0 Final Exam Answers

- access-list 3 permit 192.168.10.128 0.0.0.63
- **access-list 1 permit 192.168.10.0 0.0.0.127**
- access-list 4 permit 192.168.10.0 0.0.0.255
- access-list 2 permit host 192.168.10.9
  access-list 2 permit host 192.168.10.69
- **access-list 5 permit 192.168.10.0 0.0.0.63**
  access-list 5 permit 192.168.10.64 0.0.0.63

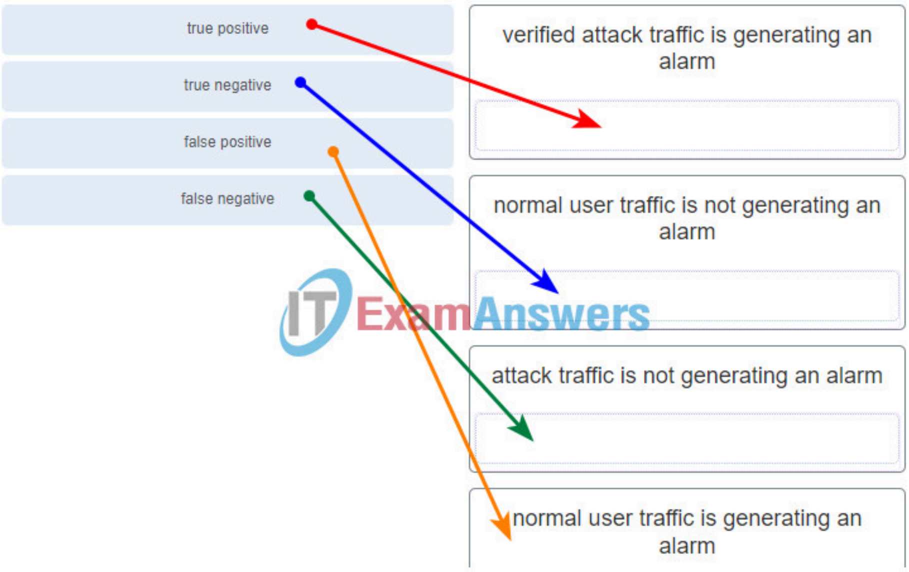
Explanation: The permit 192.168.10.0 0.0.0.127 command ignores bit positions 1 through 7, which means that addresses 192.168.10.0 through 192.168.10.127 are allowed through. The two ACEs of permit 192.168.10.0 0.0.0.63 and permit 192.168.10.64 0.0.0.63 allow the same address range through the router.

151. Which two characteristics apply to role-based CLI access superviews? (Choose two.)

- **A specific superview cannot have commands added to it directly.**
- CLI views have passwords, but superviews do not have passwords.
- A single superview can be shared among multiple CLI views.
- Deleting a superview deletes all associated CLI views.
- **Users logged in to a superview can access all commands specified within the associated CLI views.**

Explanation: By using a superview an administrator can assign users or groups of users to CLI views which contain a specific set of commands those users can access. Commands cannot be added directly to a superview but rather must be added to a CLI view and the CLI view added to the superview.

152. Match the IPS alarm type to the description.


true positive
true negative
false positive
false negative
verified attack traffic is generating an alarm
normal user traffic is not generating an alarm
attack traffic is not generating an alarm
normal user traffic is generating an alarm
ITExamAnswers

Place the options in the following order:

true negative	normal user traffic is not generating an alarm
false positive	normal user traffic is generating an alarm
true positive	verified attack traffic is generating an alarm
false negative	attack traffic is not generating an alarm

153. What are two security features commonly found in a WAN design? (Choose two.)

- WPA2 for data encryption of all data between sites
- **firewalls protecting the main and remote sites**
- outside perimeter security including continuous video surveillance
- port security on all user-facing ports
- **VPNs used by mobile workers between sites**

Explanation: WANs span a wide area and commonly have connections from a main site to remote sites including a branch office, regional site, SOHO sites, and mobile workers. WANs typically connect over a public internet connection. Each site commonly has a firewall and VPNs used by remote workers between sites.

← Previous Article

Network Security (Version 1.0) – Practice Final Exam Answers

Next Article →

Network Security 1.0 Final PT Skills Assessment (PTSA) Exam

Subscribe

Join the discussion

65 COMMENTS

Lasse E. Jensen 1 month ago

110. A recently created ACL is not working as expected. The admin determined that the ACL had been applied inbound on the interface and that was the incorrect direction. How should the admin fix this issue?

- Delete the original ACL and create a new ACL, applying it outbound on the interface.
- Add an association of the ACL outbound on the same interface.
- Fix the ACE statements so that it works as desired inbound on the interface.
- Remove the inbound association of the ACL on the interface and reapply it outbound.

The correct answer is “Remove the inbound association of the ACL on the interface and reapply it outbound.”

There is no need to delete a correctly configured ACL. I just scored 100% on the final test with that answer.

Reply

Lasse E. Jensen 1 month ago

I followed every single question in my exam and scored 98%, so there are some incorrect answers here.. I am trying to figure out which ones.

Reply

Miguel 1 year ago

Can u explain question 24? I think A is correct: The only traffic denied is echo-replies sourced from the 192.168.10.0/24 network. All other traffic is allowed.

Reply

Danny 11 months ago

Reply to Miguel

I think because there is an implicit deny any any after the deny command so as there is no permit commands all traffic is denied

Reply

Lasse E. Jensen 1 month ago

Reply to Miguel

Sure. In the shown ACL example, a “deny” statement is configured. Since there is no permit statement, all traffic is blocked, because there’s also an implicit deny after the explicitly configured deny statement.

Reply

Harry 1 year ago

Great stuff thanks so much

Reply

Big FOOT 1 year ago

These answers still valid?

Reply

K-min 2 years ago

What are two security features commonly found in a WAN design? (Choose two.)

- outside perimeter security including continuous video surveillance
- port security on all user-facing ports
- VPNs used by mobile workers between sites
- WPA2 for data encryption of all data between sites
- firewalls protecting the main and remote sites

Navigation Bar

I think new question added. Help me

Reply

Author

IT Administrator 2 years ago

Reply to K-min

I added. Thank you.

Reply

gemechu 3 years ago

list parameters included in ip security database?

Reply

VitalyES 3 years ago

Match the IPS alarm type to the description.

verified attack traffic is generating an alarm
True positive

normal user traffic is not generating an alarm
True negative

attack traffic is not generating an alarm
False negative

normal user traffic is generating an alarm
False positive

Reply

guest 3 years ago

138. Which type of firewall is the most common and allows or blocks traffic based on Layer 3, Layer 4, and Layer 5 information?

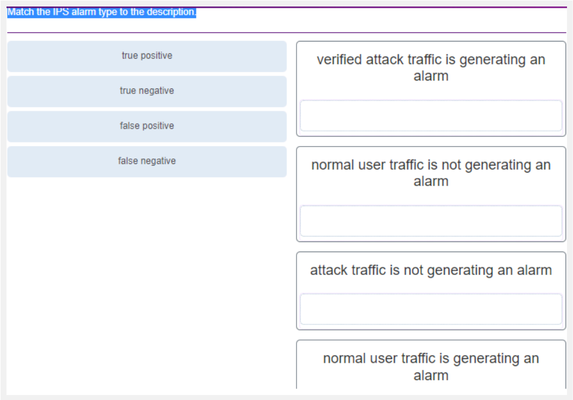
- stateless firewall
- packet filtering firewall
- next generation firewall
- **stateful firewall**

packet filtering == stateless firewall == 3 and 4 layer

Reply

Attia 3 years ago

Match the IPS alarm type to the description



Match the IPS alarm type to the description.

true positive

true negative

false positive

false negative

verified attack traffic is generating an alarm

normal user traffic is not generating an alarm

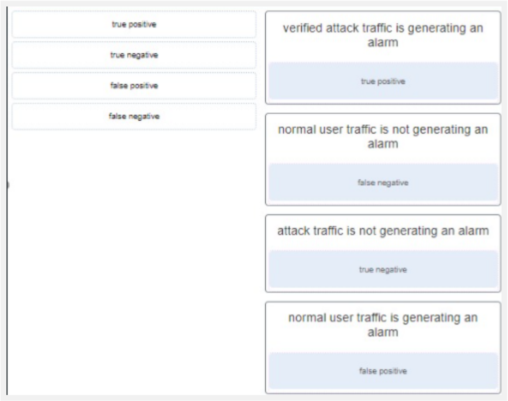
attack traffic is not generating an alarm

normal user traffic is generating an alarm

Reply

Erick 3 years ago

Hi everyone! new attached question



true positive

true negative

false positive

false negative

verified attack traffic is generating an alarm

true positive

normal user traffic is not generating an alarm

false negative

attack traffic is not generating an alarm

true negative

normal user traffic is generating an alarm

false positive

Reply

Dina 3 years ago

Match the ASA special hardware modules to the description.

Reply

Austin Graves 3 years ago

Match the security management function with the description.

Reply

IT Administrator 3 years ago

Author

Reply to Austin Graves

Hi, can you upload image

Reply

Hmidane 3 years ago

Reply to IT Administrator

Reply

Reply

Artur 3 years ago

Which two technologies provide enterprise-managed VPN solutions? (Choose two.)

- Layer 3 MPLS VPN
- Frame Relay
- **site-to-site VPN * correct**
- Layer 2 MPLS VPN
- **remote access VPN * (correct)**

Reply

IT Administrator 3 years ago

Author

Reply to Artur

Thanks for your sharing!

Reply

Koma 3 years ago

46 What are the three components of an STP bridge ID? (Choose three.)

46

What are the three components of an STP bridge ID? (Choose three.)

- the date and time that the switch was brought online
- the hostname of the switch
- the MAC address of the switch
- the extended system ID
- the bridge priority value
- the IP address of the management VLAN
- Navigation Bar

Reply

Author

IT Administrator 3 years ago

Reply to Koma

Added, thanks for your sharing!!

Reply

Koma 3 years ago

What are the three components of an STP bridge ID? (Choose three.)

-

Reply

Koma 3 years ago

What are two differences between stateful and packet filtering firewalls? (Choose two.)

-

33

What are two differences between stateful and packet filtering firewalls? (Choose two.)

- A packet filtering firewall will prevent spoofing by determining whether packets belong to an existing connection while a stateful firewall follows pre-configured rule sets.
- A stateful firewall provides more stringent control over security than a packet filtering firewall.
- A packet filtering firewall is able to filter sessions that use dynamic port negotiations while a stateful firewall cannot.
- A stateful firewall will provide more logging information than a packet filtering firewall.
- A statefull firewall will examine each packet individually while a packet filtering firewall observes the state of a connection.
-

Reply

billionaries_killer 3 years ago

Match each SNMP operation to the corresponding description. (Not all options are used.)

Reply

IT Administrator 3 years ago

Author

Reply to billionaries_killer

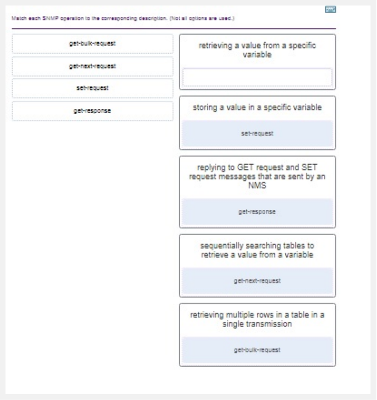
Can you upload image

Reply

xbs 3 years ago

Reply to IT Administrator

here the answer



Match each SNMP operation to the corresponding description. (Not all options are used.)

get-bulk-request

get-next-request

set-request

get-response

retrieving a value from a specific variable	
storing a value in a specific variable	set-request
replying to GET request and SET request messages that are sent by an NMS	get-response
sequentially searching tables to retrieve a value from a variable	get-next-request
retrieving multiple rows in a table in a single transmission	get-bulk-request

Reply

billionaries_killer 3 years ago

Which two technologies provide enterprise-managed VPN solutions? (Choose two.)

* remote access VPN
Layer 3 MPLS VPN
* site-to-site VPN
Layer 2 MPLS VPN
Frame Relay

Reply

IT Administrator 3 years ago

Author

Reply to billionaries_killer

Added, thanks for your sharing!!

Reply

billionaries_killer 3 years ago

What are the three components of an STP bridge ID? (Choose three.)

the date and time that the switch was brought online
* the MAC address of the switch
the IP address of the management VLAN
the hostname of the switch
* the bridge priority value
* the extended system ID

Reply

billionaries_killer 3 years ago

Which portion of the Snort IPS rule header identifies the destination port? alert tcp $HOME_NET any ->

$EXTERNAL_NET $HTTP_PORTS

any
* $HTTP_PORTS
$HOME_NET
tcp

Reply

billionaries_killer 3 years ago

What are two differences between stateful and packet filtering firewalls? (Choose two.)

A statefull firewall will examine each packet individually while a packet filtering firewall observes the state of a connection.

A stateful firewall provides more stringent control over security than a packet filtering firewall.

A packet filtering firewall will prevent spoofing by determining whether packets belong to an existing connection while a stateful firewall follows pre-configured rule sets.

A packet filtering firewall is able to filter sessions that use dynamic port negotiations while a stateful firewall cannot.

A stateful firewall will provide more logging information than a packet filtering firewall.

Reply

joseph climber 3 years ago

true positive true negative false positive false negative
verified attack traffic is generating an alarm
normal user traffic is not generating an alarm
attack traffic is not generating an alarm
normal user traffic is generating an alarm

Reply

efbium 3 years ago

Which two technologies provide enterprise-managed VPN solutions? (Choose two.)

- Frame Relay
- ***remote access VPN***
- Layer 3 MPLS VPN
- Layer 2 MPLS VPN
- ***site-to-site VPN***

Reply

IT Administrator 3 years ago

Author

Reply to efbium

Added, thanks for your sharing!!

Reply

Anon 3 years ago

Refer to the exhibit. Which pair of **crypto isakmp key** commands would correctly configure PSK on the two routers?

- R1(config)# **crypto isakmp key cisco123 address 209.165.200.226**
- R2(config)# **crypto isakmp key secure address 209.165.200.227**
- R1(config)# **crypto isakmp key cisco123 address 209.165.200.226**
- R2(config)# **crypto isakmp key cisco123 address 209.165.200.227**
- **R1(config)# crypto isakmp key cisco123 address 209.165.200.227**
- **R2(config)# crypto isakmp key cisco123 address 209.165.200.226**
- R1(config)# **crypto isakmp key cisco123 hostname R1**

- R2(config)# **crypto isakmp key cisco123 hostname R2**

Reply

Author

IT Administrator 3 years ago

Reply to Anon

Thanks for your sharing!!

Reply

Anon 3 years ago

What tool is available through the Cisco IOS CLI to initiate security audits and to make recommended configuration changes with or without administrator input?

- Control Plane Policing
- **Cisco AutoSecure**
- Cisco ACS
- Simple Network Management Protocol

Reply

Anon 3 years ago

Which two statements describe the effect of the access control list wildcard mask 0.0.0.15? (Choose two.)

- The first 32 bits of a supplied IP address will be matched.
- The first 28 bits of a supplied IP address will be ignored.
- **The last four bits of a supplied IP address will be ignored.**
- **The first 28 bits of a supplied IP address will be matched.**
- The last four bits of a supplied IP address will be matched.

- The last five bits of a supplied IP address will be ignored.

Reply

Anon 3 years ago

Refer to the exhibit. The IPv6 access list LIMITED_ACCESS is applied on the S0/0/0 interface of R1 in the inbound direction. Which IPv6 packets from the ISP will be dropped by the ACL on R1?

- HTTPS packets to PC1
- packets that are destined to PC1 on port 80
- ***ICMPv6 packets that are destined to PC1***
- neighbor advertisements that are received from the ISP router

Reply

Blindvision 3 years ago

Thanks for the materialof study.

Bellow some new questions to be added

Which two statements describe the use of asymmetric algorithms

If a public key is used to encrypt the data, a private key must be used to decrypt the data.

If a private key is used to encrypt the data, a private key must be used to decrypt the data.

If a public key is used to encrypt the data, a public key must be used to decrypt the data.

Public and private keys may be used interchangeably.

If a private key is used to encrypt the data, a public key must be used to decrypt the data.

//

Which statement is a feature of HMAC

HMAC uses a secret key as input to the hash function, adding authentication to integrity assurance.

HMAC uses a secret key that is only known to the sender and defeats man-in-the-middle attacks.

HMAC uses protocols such as SSL or TLS to provide session layer confidentiality.

HMAC is based on the RSA hash function.

///

What is the purpose of the webtype ACLs in an ASA

to monitor return traffic that is in response to web server requests that are initiated from the inside interface

to inspect outbound traffic headed towards certain web sites

to filter traffic for clientless SSL VPN users (Correct Answer)

to restrict traffic that is destined to an ASDM

//

Which two statements describe the effect of the access control list wildcard mask 0.0.0.15? (Choose two.)

The first 32 bits of a supplied IP address will be matched.

The last four bits of a supplied IP address will be ignored.

The last five bits of a supplied IP address will be ignored.

The first 28 bits of a supplied IP address will be matched.

The first 28 bits of a supplied IP address will be ignored.

The last four bits of a supplied IP address will be matched.

//
/////////////////////////////////////

Which type of firewall is the most common and allows or blocks traffic based on Layer 3, Layer 4, and Layer 5 information?

stateless firewall

packet filtering firewall

next generation firewall

stateful firewall

//
/////////////////////////////////////

Which protocol or measure should be used to mitigate the vulnerability of using FTP to transfer documents between a teleworker and the company file server?

SCP

out-of-band communication channel

ACLs on the file server

TFTP

//
/////////////////////////////////////

Reply

Author

IT Administrator 3 years ago

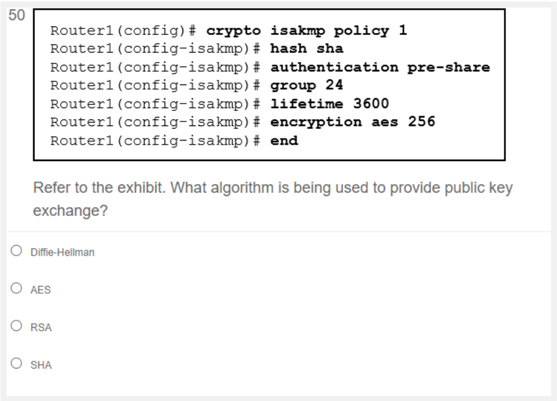
Reply to Blindvision

Added all, thanks for your sharing!!

Reply

3r!v@s 3 years ago

Question



50

```
Router1(config)# crypto isakmp policy 1
Router1(config-isakmp)# hash sha
Router1(config-isakmp)# authentication pre-share
Router1(config-isakmp)# group 24
Router1(config-isakmp)# lifetime 3600
Router1(config-isakmp)# encryption aes 256
Router1(config-isakmp)# end
```

Refer to the exhibit. What algorithm is being used to provide public key exchange?

○ Diffie-Hellman

○ AES

○ RSA

○ SHA

Reply

IT Administrator 3 years ago

Author

Reply to 3r!v@s

Added all, thanks for your sharing!

Reply

3r!v@s 3 years ago

What two assurances does digital signing provide about code that is downloaded from the Internet? (Choose two.)

- The code has not been modified since it left the software publisher.
- The code is authentic and is actually sourced by the publisher.
- The code was encrypted with both a private and public key.
- The code contains no viruses.
- The code contains no errors

Reply

3r!v@s 3 years ago

In an attempt to prevent network attacks, cyber analysts share unique identifiable attributes of known attacks with colleagues. What three types of attributes or indicators of compromise are helpful to share? (Choose three.)

- IP addresses of attack servers
- features of malware files
- changes made to end system software
- BIOS of attacking systems
- system ID of compromised systems
- netbios names of compromised firewalls

Reply

MAKANAKY 8 months ago

Reply to 3r!v@s

- IP addresses of attack servers
- changes made to end system software
- features of malware files

Reply

3r!v@s 3 years ago

What function is performed by the class maps configuration object in the Cisco modular policy framework?

- applying a policy to interesting traffic
- restricting traffic through an interface
- identifying interesting traffic

- applying a policy to an interface

Reply

3r!v@s 3 years ago

Which three statements are generally considered to be best practices in the placement of ACLs? (Choose three.)

- Filter unwanted traffic before it travels onto a low-bandwidth link.
- Place standard ACLs close to the destination IP address of the traffic.
- Place extended ACLs close to the source IP address of the traffic.
- Place extended ACLs close to the destination IP address of the traffic.
- Place standard ACLs close to the source IP address of the traffic.
- For every inbound ACL placed on an interface, there should be a matching outbound ACL.

Reply

3r!v@s 3 years ago

What functionality is provided by Cisco SPAN in a switched network?

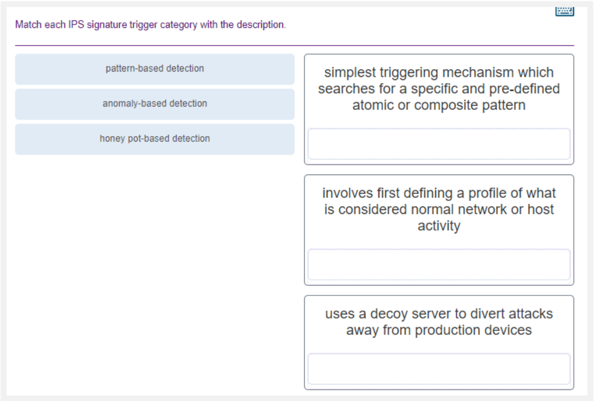
- It prevents traffic on a LAN from being disrupted by a broadcast storm.
- It mitigates MAC address overflow attacks.
- It protects the switched network from receiving BPDUs on ports that should not be receiving them.

- It mirrors traffic that passes through a switch port or VLAN to another port for traffic analysis.
- It copies traffic that passes through a switch interface and sends the data directly to a syslog or SNMP server for analysis.
- It inspects voice protocols to ensure that SIP, SCCP, H.323, and MGCP requests conform to voice standards.

Reply

3r!v@s 3 years ago

Question DRAG-AND-DROP



Match each IPS signature trigger category with the description.

pattern-based detection

anomaly-based detection

honey pot-based detection

simplest triggering mechanism which searches for a specific and pre-defined atomic or composite pattern

involves first defining a profile of what is considered normal network or host activity

uses a decoy server to divert attacks away from production devices

Reply

Max 3 years ago

When an inbound Internet-traffic ACL is being implemented, what should be included to prevent the spoofing of internal networks?

- ACEs to prevent broadcast address traffic
- ACEs to prevent SNMP traffic
- ACEs to prevent traffic from private address spaces
- ACEs to prevent ICMP traffic

- ACEs to prevent HTTP traffic

Reply

IT Administrator 3 years ago

Author

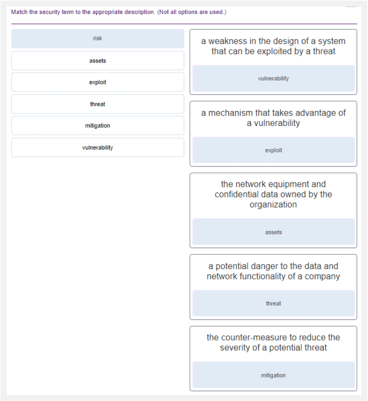
Reply to Max

Added all, many thanks for your sharing!

Reply

Max 3 years ago

more



Match the security term to the appropriate description. (Not all options are used.)

risk

assets

exploit

threat

mitigation

vulnerability

a weakness in the design of a system that can be exploited by a threat	vulnerability
a mechanism that takes advantage of a vulnerability	exploit
the network equipment and confidential data owned by the organization	assets
a potential danger to the data and network functionality of a company	threat
the counter-measure to reduce the severity of a potential threat	mitigation

Reply

Max 3 years ago

Which two types of attacks are examples of reconnaissance attacks? (Choose two.)

- ping sweep
- port scan
- man-in-the-middle
- brute force
- SYN flood

Reply

Max 3 years ago

Which Cisco solution helps prevent ARP spoofing and ARP poisoning attacks?

- DHCP Snooping
- Port Security
- Dynamic ARP Inspection
- IP Source Guard

Reply

Fiel Crente da Terrabola 2 years ago

> *Reply to Max*

Dinamic ARP inspection

Reply

Max 3 years ago

When the Cisco NAC appliance evaluates an incoming connection from a remote device against the defined network policies, what feature is being used?

- posture assessment
- remediation of noncompliant systems
- authentication and authorization
- quarantining of noncompliant systems

Reply

Max 3 years ago

Which two steps are required before SSH can be enabled on a Cisco router? (Choose two.)

- Enable SSH on the physical interfaces where the incoming connection requests will be received.
- Create a banner that will be displayed to users when they connect.
- Give the router a host name and domain name.

- Set up an authentication server to handle incoming connection requests.
- Generate a set of secret keys to be used for encryption and decryption.

Reply

Max 3 years ago

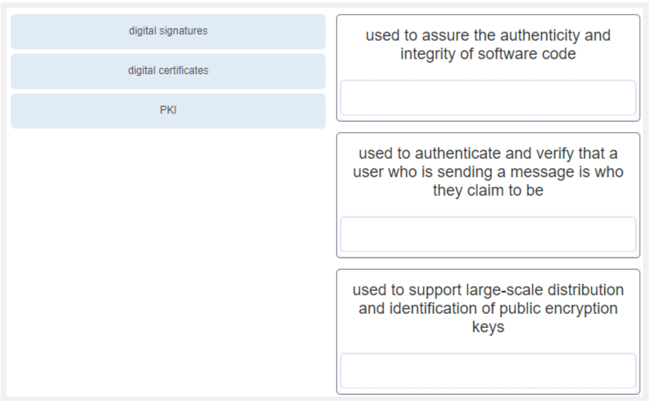
The network administrator for an e-commerce website requires a service that prevents customers from claiming that legitimate orders are fake. What service provides this type of guarantee?

- confidentiality
- authentication
- integrity
- nonrepudiation

Reply

Max 3 years ago

Match the security technology with the description.



digital signatures

digital certificates

PKI

used to assure the authenticity and integrity of software code

used to authenticate and verify that a user who is sending a message is who they claim to be

used to support large-scale distribution and identification of public encryption keys

Reply

Alex43 4 years ago

Thanks so much, how many question in this exam?

Reply

IT Administrator 4 years ago

Author

Reply to Alex43

60Q

Reply

Ahuys 4 years ago

Passed, good site, many thanks

Reply

Hai Truong 4 years ago

Reply to Ahuys

Congrat

Reply