Exam : 642-542

Title : Cisco SAFE Implementation

Ver : 11-28-07

QUESTION 1:

Threats that come from hackers who are more highly motivated and technically competent are called:

A. Sophisticated
B. Advanced
C. External
D. Structured

Answer: D

Explanation: Structured threats come from adversaries that are highly motivated and technically competent.
Ref: Cisco Secure Intrusion Detection System (Ciscopress) Page 9

QUESTION 2:

The worst attacks are the ones that:

A. Are intermittent.
B. Target the applications
C. You can not stop them.
D. Target the executables.
E. Target the databases.
F. You can not determine the source.

Answer: C

Explanation: The worst attack is the one that you cannot stop. When performed properly, DDoS is just such an attack.

QUESTION 3:

What type of network requires availability to the Internet and public networks as a major requirement and has several access points to other networks, both public and private?

A. Open
B. Closed
C. Intermediate
D. Balanced

Answer: A

Explanation:

The networks of today are designed with availability to the Internet and public networks, which is a major requirement. Most of today's networks have serverla access points to other network both public and private;therefore,securing these networks has become fundamentally important.
Reference: CSI Student guide v2.0 p.2-4

QUESTION 4:

The security team at Certkiller Inc. is working on network security design.
What is an example of a trust model?

A. One example is NTFS
B. One example is NTP
C. One example is NFS
D. One example is NOS

Answer: C

Explanation:
One of the key factors to building a successful network security design is to identify and enforce a proper trust model. The proper trust model defines who needs to talk to whom and what kind of traffic needs to be exchanged; all traffic should be denied. one the proper trust model has been identified, then the security designer should decide how to enforce the model. As more critical resources are globally available and new forms of network attacks evolve, the network security infrastructure tends to become more sophisticated, and more products are available. Firewalls, routers, LAN switches, intrusion detection systems, AAA servers, and VPNs are some of the technologies and products that can help enforce the model. Of course, each one of these products and technologies plays a particular role within the overall security implementation, and it is essential for the designer to understand how these elements can be deployed.
Network File Sharing seems to be the best answer out of all the answers listed.
Reference: Securing Networks with Private VLANs and VLAN Access Control Lists

---

QUESTION 5:

Which type of attack can be mitigated only through encryption?

A. DoS
B. Brute force
C. Man-in-the-middle
D. Trojan horse

Answer: C

Explanation:
1. Man-in-the-middle attacks-Mitigated through encrypted remote traffic

Reference: Safe white papers; page 26
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 6:

The security team at Certkiller Inc. is working on understanding attacks that happen in the network. What type of attack is characterized by exploitation of well-known weaknesses, use of ports that are allowed through a firewall, and can never be completely eliminated?

A. Network reconnaissance
B. Man-in-the-middle
C. Trust exploitation
D. Application layer

Answer: D

Explanation: The primary problem with application layer attacks is that they often use ports that are allowed through a firewall.
Reference: Safe White papers 68
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 7:

You are the security administrator at Certkiller and you need to know the attacks types to the network. Which two general IP spoofing techniques does a hacker use? (Choose two)

A. An IP address within the range of trusted IP addresses.
B. An unknown IP address which cannot be traced.
C. An authorized external IP address that is trusted.
D. An RFC 1918 address.

Answer: A C

Explanation:
IP Spoofing
An IP spoofing attack occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer. A hacker can do this in one of two ways. The hacker uses either an IP address that is within the range of trusted IP addresses for a network or an authorized external IP address that is trusted and to which access is provided to specified resources on a network. IP spoofing attacks are often a launch point for other attacks. The classic example is to launch a denial-of-service (DoS) attack using spoofed source addresses to hide the hacker's identity. Normally, an IP spoofing attack is limited to the injection of malicious data or commands into an existing stream of data that is passed between a client and server application or a peer-to-peer network connection. To enable bidirectional communication, the hacker must change all routing tables to point to the spoofed IP address. Another approach hackers sometimes take is to simply not worry

about receiving any response from the applications. If a hacker tries to obtain a sensitive file from a system, application responses are unimportant.
However, if a hacker manages to change the routing tables to point to the spoofed IP address, the hacker can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can.
Reference:
Safe white papers; page 65
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 8:

John the security administrator at Certkiller Inc. is working on securing the network with strong passwords. What is the definition of a strong password?

A. The definition of a strong password is at least ten characters long and should contain cryptographic characters.
B. The definition of a strong password is at least eight characters long;contains uppercase letters, lowercase letters, numbers, and should not contain special characters.
C. The definition of a strong password is defined by each company depending on the product being used.
D. The definition of a strong password is at least eight characters long;contains uppercase letters, lowercase letters, numbers, and special characters.

Answer: D

Explanation:
Passwords should be at least eight characters long and contain uppercase letters, lowercase
letters, numbers, and special characters (#, %, $, and so forth).
Reference: Safe white papers; page 67
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 9:

The two Denial of Service attack methods are: (Choose two)

A. Out of Band data crash
B. SATAN
C. TCP session hijack
D. Resource Overload

Answer: A, D

Explanation:
When involving specific network server applications; such as a web
server or an FTP server, these attacks can focus on acquiring and keeping open all

the available connections supported by that server, effectively locking out valid users of the server or service. Some attacks compromise the performance of your network by flooding the network with undesired-and often useless-network packets and by providing false information about the status of network resources.
REF; Safe white papers; page 66&67
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks
Incorrect Answers:
B: SATAN is a testing and reporting tool that collects a variety of information about networked hosts.
C: TCP session hijack is when a hacker takes over a TCP session between two machines.

QUESTION 10:

This program does something undocumented which the programmer intended, but that the user would not approve of if he or she knew about it.

A. What is a Virus.
B. What is a Macro Virus.
C. What is a Trojan Horse.
D. What is a Worm.

Answer: C

Explanation: A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on the user's workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every user in the user's address book. Then other users get the game and play it, thus spreading the Trojan horse.
Ref: Safe White papers; Page 70
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 11:

Choose the true statements regarding IP spoofing attack and DoS attack. (Choose all that apply)

A. IP spoofing attack is a prelude for a DoS attack.
B. DoS attack is a prelude for a IP spoofing attack.
C. IP spoofing attack is generally performed by inserting a string of malicious commands into the data that is passed between a client and a server.
D. A DoS attack is generally performed by inserting a string of malicious command into the data that is passed between a client and a server.

Answer: A, C

Explanation: IP spoofing attacks are often a launch point for other attacks. The classic example is to launch a denial-of-service (DoS) attack using spoofed source addresses to hide the hacker's identity.
Normally, an IP spoofing attack is limited to the injection of malicious data or commands into an existing stream of data that is passed between a client and server application or a peer-to-peer network connection.
REF; Safe white papers;page 65
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 12:

What method helps mitigate the threat of IP spoofing?

A. Access control
B. Logging
C. SNMP polling
D. Layer 2 switching

Answer: A

Explanation: The most common method for preventing IP spoofing is to properly configure access control. To reduce the effectiveness of IP spoofing, configure access control to deny any traffic from the external network that has a source address that should reside on the internal network.
REF;Safe white papers;page 67
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 13:

What is an example of a trust model?

A. NTFS
B. NFS
C. NTP
D. NOS

Answer: B

Explanation:
One of the key factors to building a successful network security design is to identify and enforce a proper trust model. The proper trust model defines who needs to talk to whom and what kind of traffic needs to be exchanged; all other traffic should be denied. Once the proper trust model has been identified, then the security designer should decide how to enforce the model. As more critical resources are globally available and new forms of network attacks evolve, the network security infrastructure tends to become more sophisticated, and more products are available. Firewalls, routers, LAN switches,

intrusion detection systems, AAA servers, and VPNs are some of the technologies and products that can help enforce the model. Of course, each one of these products and technologies plays a particular role within the overall security implementation, and it is essential for the designer to understand how these elements can be deployed.
Network File Sharing seems to be the best answer out of all the answers listed.
Reference: Securing Networks with Private VLANs and VLAN Access Control Lists

---

QUESTION 14:

Which type of attack is usually implemented using packet sniffers?

A. Man-in-the-middle
B. DoS
C. Brute force
D. IP spoofing

Answer: A

Explanation: Man-in-the-middle attacks are often implemented using network packet
sniffers and routing and transport protocols.
REF;Safe white papers;page 68
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 15:

Which type of attack is characterized by exploitation of well-known weaknesses, use of ports that are allowed through a firewall, and can never be completely eliminated?

A. Network reconnaissance
B. Application layer
C. Man-in-the-middle
D. Trust exploitation

Answer: B

Explanation: The primary problem with application layer attacks is that they often use ports that are allowed through a firewall.
Ref: Safe White papers 68
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 16:

What is the only way to effectively prevent the Man-in-the-middle attacks?

A. Firewalls

B. ISP filtering and rate limiting
C. HIDS & Firewall filtering
D. Encryption
E. Access Control

Answer: D

Explanation: Man-in-the-middle attacks can be effectively mitigated only through the use of cryptography. If someone hijacks data in the middle of a cryptographically private session, all the hacker will see is cipher text, and not the original message.
Ref: Safe White papers 68
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 17:

What is not a specific type of attack, but refers to most attacks that occur today?

A. DoS
B. Brute force password
C. IP spoofing
D. Unauthorized access

Answer: D

Explanation: Although unauthorized-access attacks are not a specific type of attack, they refer to most attacks executed in networks today.
REF;Safe white papers;page 70
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 18:

This method of attack will always compute the password if it is made up of the character set you have selected to test.

A. What is LOphtCracks
B. What is brute force computation
C. What is dictionary lookup
D. What is brute force mechanism

Answer: B

QUESTION 19:

What is the primary method of mitigating port redirection attacks?

A. Keep firewalls up to date with the latest patches and fixes.
B. Do not allow trust models.
C. Keep OS and applications up to date with the latest patches and fixes.
D. Use proper trust models.

Answer: D

Explanation: Port redirection can be mitigated primarily through the use of proper trust models (as mentioned earlier). If we assume that a system is under attack, host-based IDS can help detect and prevent a hacker installing such utilities on a host.
Ref: Safe white papers;page 70
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks
Reference: Cisco Courseware page 2-28

QUESTION 20:

What are two characteristics of a packet sniffer designed for attack purposes? (Choose two)

A. Captures first 300 to 400 bytes.
B. Typically captures login sessions.
C. Captures the last 300 to 400 bytes.
D. Deciphers encrypted passwords.
E. Enable to capture UDP packets.

Answer: A B

QUESTION 21:

Which attack is executed by Java applets and ActiveX controls?

A. Brute force
B. IP spoofing
C. DoS
D. Application layer

Answer: D

Explanation:
New Internet technologies such as Java and ActiveX, designed to better enable cross-platform communication, have drastically altered the level and approach of computer damaging elements. Anyone seeking to maliciously manipulate corporate information or attack corporate computers now has an accommodating Java and ActiveX environment that offers easy, quick, and discreet methods of attack. Mini-applications like Java applets enter network computers whenever users access Java-enabled Web sites

or use Web browsers, and this distributed computing allows unchecked applets into the network without any warning, announcement, or even opportunity for users to refuse them. SurfinGate technology prevents Java applet attacks that can bypass built-in security systems like the Java Security Manager, offering extensive management controls and features designed for the corporation.
Reference: Cisco Systems Joins the Finjan Java Security Alliance

---

QUESTION 22:

The security team at Certkiller Inc. is working on securing the network by understanding the type of threats. What type of threat consists mainly of random hackers using various common tools (such as malicious shell scripts, password crackers, credit card number generators, and dialer daemons)?

A. A internal threat
B. An external threat
C. A structured threat
D. A unstructured threat

Answer: D

Explanation:
Unstructured threats - These threats primarily consist of random hackers using various common tools, such as malicious shell scripts, password crackers, credit card number generators, and dialer daemons. Although hackers in this category may have malicious intent, many are more interested in the intellectual challenge of cracking safeguards than in creating havoc.
Reference: Cisco Courseware p.2-14

QUESTION 23:

What service is provided by CSA Profiler?

A. Profiler analyzes applications to help in generating useful policies.
B. Profiled monitors and logs security events that occur on CSA protected hosts.
C. Profiler provides a COM component utility that installs with each CSA.
D. Profiler configures agent kits that are deployed on CSA protected hosts.

Answer: A

Explanation:
Writing effective CSA policies requires understanding the resources that applications require for normal operation. The Profiler can provide that information by analyzing applications as they operate in a normal environment and generating useful policies based on that analysis.
Reference: Cisco Courseware p.5-68

QUESTION 24:

James the security administrator is working on cryptographic authentication.
What is the earliest version of NTP that supports a cryptographic authentication mechanism between peers?

A. The earliest version is 5
B. The earliest version is 4
C. The earliest version is 3
D. The earliest version is 2
E. The earliest version is 1

Answer: C

Explanation:
Version 3 and above of NTP supports a cryptographic authentication mechanism between peers.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

QUESTION 25:

You are the administrator at Certkiller Inc. and you need to mitigate threats to the network. How do you mitigate the threats presented when using TFTP?

A. TFTP traffic should use peer authentication for each session.
B. IP packet inspection should be enabled on all routers.
C. TFTP traffic should be encrypted within an IPSec tunnel.
D. IP verify reverse path should be enabled on all routers.

Answer: C

Explanation: Where possible, TFTP traffic should be encrypted within an IPSec tunnel in order to mitigate the chance of its being intercepted.
REF;Safe white papers;page72
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

QUESTION 26:

You are the administrator at Certkiller Inc. and you need to checkout syslogs for information. How do you check syslog information to ensure that it has not been altered in transit?

A. Packets use CRC to ensure data has not been altered in transit.
B. Syslog has no checking to ensure that the packet contents have not been altered in

transit.
C. Host IDS inspects the packet to ensure time stamps are concurrent.
D. The firewall inspects the packet to ensure time stamps are concurrent.
E. IPSec inspects the packet to ensure time stamps are concurrent.

Answer: B

Explanation:
Logging-Syslog is also sent as cleartext between the managed device and the management host. Syslog has no packet-level integrity checking to ensure that the packet contents have not been altered in transit. An attacker may alter syslog data in order to confuse a network administrator during an attack. Where possible, syslog traffic may be encrypted within an IPSec tunnel in order to mitigate the chance of its being altered in transit. Where the syslog data cannot be encrypted within an IPSec tunnel because of cost or the capabilities of the device itself, the network administrator should note that there is a potential for the syslog data to be falsified by an attacker. When allowing syslog access from devices on the outside of a firewall, RFC 2827 filtering at the egress router should be implemented. This scenario will mitigate the chance of an attacker from outside the network spoofing the address of the managed device, and sending false syslog data to the management hosts. ACLs should also be implemented on the firewall in order to allow syslog data from only the managed devices themselves to reach the management hosts. This scenario prevents an attacker from sending large amounts of false syslog data to a management server in order to confuse the network administrator during an attack.
Syslog uses UDP port 514.
Reference:
Safe white papers;page 72
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 27:

If you permit syslog access from devices on the outside of a firewall, what type of filtering at the egress router should be implemented?

A. RFC 1771
B. RFC 1918
C. RFC 1305
D. SAFE design mandates no filtering at this point.
E. RFC 2827

Answer: E

Explanation: When allowing syslog access from devices on the outside of a firewall, RFC 2827 filtering at the egress router should be implemented.
REF;Safe white papers;page 72
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 28:

When allowing syslog access from devices outside a firewall, what filtering at the perimeter router should you implement?

A. No filtering should be implemented since it will block the syslog traffic.
B. RFC 1918
C. RFC 2827
D. RFC 1281
E. RFC 1642

Answer: C

Explanation: When allowing syslog access from devices on the outside of a firewall, RFC 2827 filtering at the egress router should be implemented.
REF;Safe white papers;page 72
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 29:

Many IP services are commonly used by hackers and should be disabled for security reasons. One of these services is Cisco Discovery Protocol which should be disabled in configuration mode.
What is the command that you use for this purpose?

A. no cdp enable
B. no cdp run
C. no ip cdp enable
D. cdp disable

Answer: B

QUESTION 30:

If you are using SNMP for network management, you must make sure that?

A. Configure SNMP for write-only community strings.
B. Configure SNMP for read-only community strings.
C. The access to the device you wish to manage is limited to one management host.
D. Turn off logging.

Answer: B

Explanation: When the community string is compromised, an attacker could reconfigure the device if read-write access via SNMP is allowed. Therefore, it is recommended that you configure SNMP with only read-only community strings.

Ref: Safe White papers 72
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 31:

no isakmp enable
What is the use of the above command on a PIX Firewall?

A. This command disables ISAKMP which is enabled by default.
B. The correct format to disable ISAKMP on a PIX Firewall is "crypto isakmp disable".
C. This is an invalid command.
D. This command disables ISAKMP. ISAKMP is ensabled by default.

Answer: A

QUESTION 32:

How do you mitigate the threats presented when using TFTP?

A. TFTP traffic use peer authentication for each session.
B. TFTP traffic should be encrypted within an IPSec tunnel.
C. IP packet inspection should be enabled on all routers.
D. IP verify reverse path should be enabled on all routers.

Answer: B

Explanation: Where possible, TFTP traffic should be encrypted within an IPSec tunnel in order to mitigate the chance of its being intercepted.
REF;Safe white papers;page 72
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 33:

What is the earliest version of NTP that supports a cryptographic authentication mechanism between peers?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: C

Explanation:

Version 3 and above of NTP supports a cryptographic authentication mechanism between peers.
Reference:
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 34:

What is the recommended if SNMP is used? (Choose two)

A. Allow only the appropriate management hosts access to the device you wish to manage.
B. Configure SNMP with write-only community strings.
C. Configure SNMP with read-only community strings.
D. Allow only the firewall access to the device you wish to manage.
E. Allow only the router access to the device you wish to manage.

Answer: A, C

Explanation:
When the community string is compromised, an attacker could reconfigure the device if read-write access via SNMP is allowed. Therefore, it is recommended that you configure SNMP with only read-only community strings. You can further protect yourself by setting up access control on the device you wish to manage via SNMP to allow only the appropriate management hosts access.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 72

QUESTION 35:

Kathy the security administrator at Certkiller Inc. is working on security solutions. Which is a component of Cisco security solutions?

A. Secure connectivity
B. Secure solution
C. Secure availability
D. Secure productivity

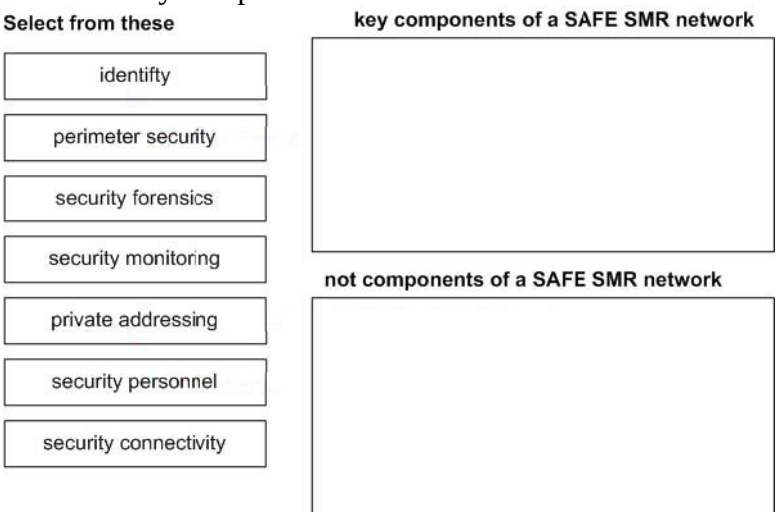
Answer: A

Explanation:
The key components of a SAFE network are fundamental to the success of an implementation. These key components are broken down as follows:
1) Identity - Authentication and digital certificates
2) Perimeter security - ACL firewalls
3) Secure connectivity - VPN tunnelling and encryption

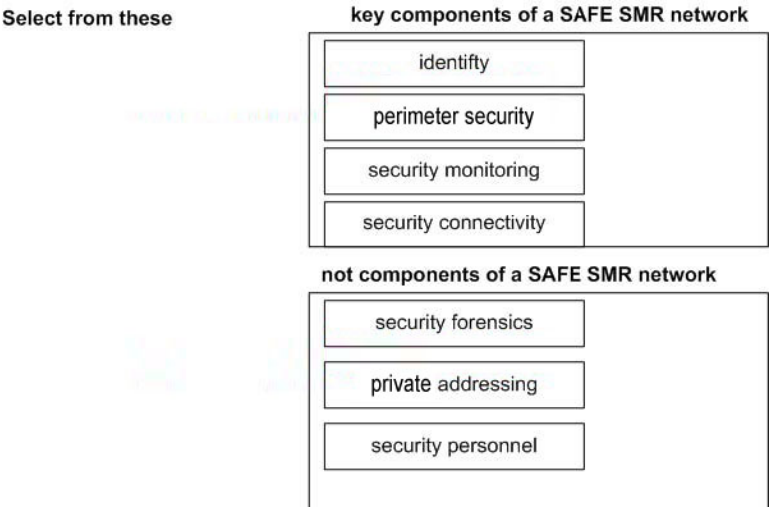
4) Security monitoring - Intrusion detection and scanning
5) Security management - Policy management, device management, and directory services.
Reference: Cisco Courseware p.3-4

QUESTION 36:

What are key components of the SAFE SMR network?



Answer:



Explanation:
http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_design_guidance09186a00

QUESTION 37:

The security team at Certkiller Inc. is working on using systems and appliances.
What are two advantages of using integrated systems and appliances? (Choose two)

A. An advantage is implement on existing equipment.
B. An advantage is achieve better performance.
C. An advantage is achieve better interoperability.
D. An advantage is increased feature functionality.
E. An advantage is improved manageability.

Answer: A, C

Explanation:
The advantages to integrated functionality are as follows:
1) Can be implemented on existing equipment
2) Better interoperability
3) Can reduce overall cost
Reference: Cisco SAFE Implementation Courseware version 1.1 Page 3-11

QUESTION 38:

Which are the functional areas in SAFE Enterprise Network? (Choose two)

A. Enterprise Network VPN/Remote Access
B. Enterprise Network Campus
C. Enterprise Network Distribution
D. Enterprise Network Edge
E. Enterprise Network Corporate Internet

Answer: B, D

Explanation:
The enterprise comprises two functional areas: the Enterprise Network Campus and the Enterprise Network Edge. These two areas are further divided into modules that define the various functions of each area in detail
Reference: Cisco Courseware page 8-3

QUESTION 39:

Which is a design alternative in the SAFE Enterprise network design server module?

A. Proper aggregation and analysis of the Syslog information.
B. Connection state enforcement and detailed filtering.
C. Combine server module with the core module.
D.
A separate router can be used between the server and edge distribution rather than the layer 3 switch.

Answer: C

Explanation:
Combine Server module with the Core module - Combine these modules if performance needs do not dictate separation. For very sensitive high-performance server environments, blades installing more than one NIDS blade and directing policy-matched traffic to specific blades can scale the NIDS capability in the Layer 3 switch.
Reference: Cisco Courseware page 8-22

QUESTION 40:

If you need to choose between using integrated functionality in a network device versus using a specialized function appliance, first and foremost you must make your decision based on:

A. The capacity and functionality of the appliance.
B. The integration advantage of the device.
C. Ease of implementation, use and the maintenance of the system.
D. Limiting the complexity of the design.

Answer: A

Explanation: The integrated functionality is often attractive because you can implement it on existing equipment, or because the features can interoperate with the rest of the device to provide a better functional solution. Appliances are often used when the depth of functionality required is very advanced or when performance needs require using specialized hardware. Make your decisions based on the capacity and functionality of the appliance versus the integration advantage of the device.
REF; Safe white papers; 4
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 41:

What are two advantages of using integrated systems and appliances? (Choose two)

A. Achieve better performance.
B. Implement on existing equipment.
C. Achieve better interoperability.
D. Improved manageability.
E. Increased feature functionality.

Answer: B, E

Explanation: At many points in the network design process, you need to choose between using integrated functionality in a network device versus using a

specialized functional appliance. The integrated functionality is often attractive because you can implement it on existing equipment, or because the features can interoperate with the rest of the device to provide a better functional solution.
REF;Safe white papers;page 4
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 42:

The security team at Certkiller Inc. is working on private VLANs.
What are private VLANs?

A. Private VLANs are tools that allow segregating traffic at Layer 3, turning broadcast segments into non-broadcast, multi-access-like segments.
B. Private VLANs are tools that allow segregating traffic at Layer 2, turning non-broadcast, multi-access-like segments into broadcast segments.
C. Private VLANs are tools that allow segregating traffic at Layer 3, turning non-broadcast, multi-access-like segments into broadcast segments.
D. Private VLANs are tools that allow segregating traffic at Layer 2, turning broadcast segments into non-broadcast, multi-access-like segments

Answer: D

Explanation:

Within an existing VLAN, private VLANs provide some added security to specific network applications. Private VLANs work by limiting which ports within a VLAN can communicate with other ports in the same VLAN. Isolated ports within a VLAN can communicate only with promiscuous ports. Community ports can communicate only with other members of the same community and promiscuous ports. Promiscuous ports can communicate with any port. This is an effective way to mitigate the effects of a single compromised host.
Reference: Safe White papers; Page 5
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 43:

You are the security administrator at Certkiller Inc. and you are working on installing IDS in the network. What IDS guidelines should be allowed according to SAFE SMR?

A. An IDS guideline is to use TCP shunning as opposed to TCP resets.
B. An IDS guideline is to use shunning no longer than 15 minutes.
C. An IDS guideline is to use shunning on only TCP traffic, as it is more difficult to spoof than UDP.
D. An IDS guideline is to use shunning on only UDP traffic, as it is more difficult to spoof than TCP.

Answer: C

Explanation:
To mitigate the risks of shunning, you should generally use it only on TCP traffic, which is much more difficult to successfully spoof than UDP.
Reference: Safe white papers; 8
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 44:

You are the administrator at Certkiller Inc. and you working on shunning attacks to the network. When shunning, why should the shun length be kept short?

A. You should keep it short to eliminate blocking traffic from an invalid address that was spoofed previously.
B. You should keep it short to prevent unwanted traffic from being routed.
C. You should keep it short to prevent TCP resets from occurring.
D. You should keep it short to eliminate blocking traffic from a valid address that was spoofed previously.

Answer: D

Explanation:
To mitigate the risks of shunning, you should generally use it only on TCP traffic, which is much more difficult to successfully spoof than UDP. Use it only in cases where the threat is real and the chance that the attack is a false positive is very low. Also consider setting the shun length very short. This setup will block the user long enough to allow the administrator to decide what permanent action (if any) he/she wants to take against that IP address. However, in the interior of a network, many more options exist. With effectively deployed RFC 2827 filtering, spoofed traffic should be very limited. Also, because customers are not generally on the internal network, you can take a more restrictive stance against internally originated attack attempts. Another reason for this is that internal networks do not often have the same level of stateful filtering that edge connections possess. As such, IDS needs to be more heavily relied upon than in the external environment.
Reference: Safe white papers; 8
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 45:

You the administrator at Certkiller Inc and you are doing research on the type of attacks that occur in the network. What type of attack typically exploits intrinsic characteristics in the way your network operates?

A. Attacks to the network
B. Attacks to the router

C. Attacks to the switch
D. Attacks to the hosts

Answer: A

Explanation:
Network attacks are among the most difficult attacks to deal with because they typically take advantage of an intrinsic characteristic in the way your network operates. These attacks include Address Resolution Protocol (ARP) and Media Access Control (MAC)-based Layer 2 attacks, sniffers, and distributed denial-of-service (DDoS) attacks.
Ref: Safe White papers 6
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 46:

You are the security administrator at Certkiller Inc. working configuring an IDS.
Which IDS guideline should be followed, according to SAFE SMR?

A. According to SAFE SMR, use UDP resets more often than shunning, because UDP traffic is more difficult to spoof.
B. According to SAFE SMR, use TCP resets no longer than 15 minutes.
C. According to SAFE SMR, use UDP resets no longer than 15 minutes.
D. According to SAFE SMR, use TCP resets more often than shunning, because TCP traffic is more difficult to spoof.

Answer: D

Explanation:
As the name implies, TCP resets operate only on TCP traffic and terminate an active attack by sending TCP reset messages to the attacking and attacked host. Because TCP traffic is more difficult to spoof, you should consider using TCP resets more often than shunning.
Reference: Safe white papers; 8
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 47:

Kathy the security administrator at Certkiller Inc. is working on security management.
What type of management provides the highest level of security for devices?

A. The highest level is out of band
B. The highest level is device level
C. The highest level is in-band
D. The highest level is proxy level

Answer: A

Explanation: "the "out-of-band" (OOB) management architecture described in SAFE Enterprise provides the highest levels of security"
Reference: REF;Safe white papers;page 9
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 48:

Which IDS guideline should be followed, according to SAFE SMR?

A. use UDP resets more often than shunning, because UDP traffic is more difficult to spoof
B. use TCP resets more often than shunning, because TCP traffic is more difficult to spoof
C. use TCP resets no longer than 15 minutes
D. use UDP resets no longer than 15 minutes

Answer: B

Explanation:
Because TCP traffic is more difficult to spoof, you should consider using TCP resets more often than shunning - TCP resets operate only on TCP traffic and terminate an active attack by sending a TCP reset to both the attacker and the attacked host.
Reference: Cisco Courseware p.3-27

QUESTION 49:

You have hired a new security administrator for your organization. He calls you in the middle of the night and says "I am receiving too many positives"
What is talking about?

A. Alarms from the Intrusion Sensor are detected by illegitimate traffic.
B. Alarms from the Intrusion Sensor are detected by legitimate traffic.
C. Alarms from the Intrusion Sensor are detected-without any further action.
D. Alarms from the Intrusion Sensor are detected and logged.

Answer: D

Explanation: Positives - are alarms that are detected and logged.
False-positives are defined as alarms caused by legitimate traffic or activity.
False negatives are attacks that the IDS system fails to see.

QUESTION 50:

What is the most likely target during an attack?

A. Router
B. Switch
C. Host
D. Firewall

Answer: C

Explanation: The most likely target during an attack, the host presents some of the most difficult challenges from a security perspective. There are numerous hardware platforms, operating systems, and applications, all of which have updates, patches, and fixes available at different times.
REF;Safe white papers;page 6
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 51:

When shunning, why should the shun length be kept short?

A. To eliminate blocking traffic from an invalid address that as spoofed previously.
B. To eliminate blocking traffic from a valid address that was spoofed previously.
C. To prevent unwanted traffic from being routed.
D. To prevent TCP resets from occurring.

Answer: B

Explanation: This setup will block the user long enough to allow the administrator to decide
what permanent action (if any) he/she wants to take against that IP address.
REF;Safe white papers; 8
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 52:

Which IDS guideline should be followed according to SAFE SMR?

A. Use UDP resets more often than shunning, because UDP traffic is more difficult to spoof.
B. Use TCP resets more often than shunning, because TCP traffic is more difficult to spoof.
C. Use TCP resets no longer than 15 minutes.
D. Use UDP resets no longer than 15 minutes.

Answer: B

Explanation: As the name implies, TCP resets operate only on TCP traffic and terminate an active attack by sending TCP reset messages to the attacking and

attacked host. Because TCP traffic is more difficult to spoof, you should consider using TCP resets more often than shunning.
REF;Safe white papers; 8
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 53:

What type of attack typically exploits an intrinsic characteristic in the way your network operates?

A. Route attacks
B. Switch attacks
C. Network attacks
D. Host attacks

Answer: C

Explanation: Network attacks are among the most difficult attacks to deal with because they typically take advantage of an intrinsic characteristic in the way your network operates. These attacks include Address Resolution Protocol (ARP) and Media Access Control (MAC)-based Layer 2 attacks, sniffers, and distributed denial-of-service (DDoS) attacks.
Ref: Safe White papers 6
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 54:

Which type of management architecture described in SAFE Enterprise offers the best level of security?

A. In-band
B. Out-of-band
C. Proxy
D. All answers are incorrect.

Answer: B

Explanation: "the "out-of-band" (OOB) management architecture described in SAFE Enterprise provides the highest levels of security"
REF;Safe white papers;page 9
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 55:

accesslist 101 deny ip 10.0.0.0 0.255.255.255 any is an example of an ACL entry to filter what type of addresses?

A. RFC 1918
B. RFC 1920
C. RFC 2728
D. RFC 2827

Answer: A

Explanation:
! RFC 1918 filtering. Note network 172.16.x.x was not included in the
! filter here since it is used to simulate the ISP in the lab.
!
access-list 103 deny ip 10.0.0.0 0.255.255.255 any
access-list 103 deny ip 192.168.0.0 0.0.255.255 any
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 47

QUESTION 56:

What type of management provides the highest level of security for devices?

A. Device level
B. In-band
C. Out of band
D. Proxy level

Answer: C

Explanation: "the "out-of-band" (OOB) management architecture described in SAFE Enterprise provides the highest levels of security"
REF;Safe white papers;page 9
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 57:

The security wheel starts with Secure. What are the initials of the other 3 steps?

A. LMR
B. RTM
C. MTI
D. TIT

Answer: C

Explanation:
Step 1. - Secure

Step 2. - Monitor
Step 3. - Test
Step 4. - Improve
Ref: Cisco Secure PIX Firewalls (Ciscopress) Page 10

QUESTION 58:

Which three statements about the monitoring stage of the Security Wheel are true? (Choose three)

A. It detects violations to the security policy.
B. New security policies are created during this stage.
C. It involved system auditing and real-time intrusion detection.
D. It involves the use of security assessments and vulnerability scanning.
E. Adjustments are made to the security policy as security vulnerabilities and risks are identified.
F. It validates the security implementation in step 1.

Answer: A, C, D

Explanation:
Detecting violations in your security policy involves monitoring hosts and network traffic to determine when violations occur. Manual monitoring is usually accomplished by utilizing the audit logging capabilities provided by the host operating system. Automatic monitoring involves watching network traffic to determine whether unauthorized activities are occurring on the network. This level of monitoring can be accomplished through the use of Cisco Secure IDS.
Reference: Cisco Secure Intrusion Detection System (Ciscopress) Page 42
Reference: Cisco Courseware page 2-9

QUESTION 59:

What are three steps of the Security Wheel? (Choose three)

A. Improve
B. Log
C. Maintain
D. Test
E. Secure
F. Report

Answer: A, D, E,

Explanation:
The Security Wheel breaks network security into four separate phases:
* Securing

* Monitoring
* Testing
* Improving
Reference: Cisco Secure Intrusion Detection System (Ciscopress) Page 35

QUESTION 60:

You are the administrator at Certkiller Inc. and you are working on extranet VPNs.
What service do extranet VPNs provide?

A. Extranet VPNs provide link network resources with third-party vendors and business partners.
B. Extranet VPNs provide link corporate headquarters to remote offices.
C. Extranet VPNs provide link telecommuters and mobile users to corporate network resources.
D. Extranet VPNs provide link private networks to public networks.

Answer: A

Explanation:
Extranet VPNs refer to connections between a company and its business partners.
Access between sites should be tightly controlled by both entities at their respective sites.
Reference:REF;Safe white papers;page 76
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 61:

The security team at Certkiller Inc. is working on the SAFE SMR.
What is an assumption of SAFE SMR?

A. SAFE SMR does not assume applications and OS security.
B. Implementing SAFE SMR guarantees a secure environment.
C. The security policy is already in place.
D. Network contains only Cisco devices.

Answer: C

Explanation:
SAFE SMR makes the following assumptions:
1) The security policy is already in place
2) SAFE does not guarantee a secure environment
3) Application and operating system vulnerabilities are not comprehensively covered
Reference: Cisco SAFE Implementation Courseware version 1.1 Page 3-6
Note: If select two then answer would be: A, C

QUESTION 62:

Which is a component of Cisco security solutions?

A. Secure connectivity
B. Secure solution
C. Secure availability
D. Secure productivity

Answer: A

Explanation:
Reference: Cisco Courseware p.3-4

QUESTION 63:

Which three Cisco components encompass secure connectivity? (Choose three)

A. Cisco IDS Sensors
B. Cisco PIX Firewalls
C. Cisco IDS Sensors
D. Cisco VPN Connectors
E. Cisco IOS IDS
F. Cisco IOS VPN

Answer: B, D, F

Explanation:
Secure connectivity - Virtual private network (VPN)
1) Cisco VPN Concentrators
2) Cisco PIX Firewalls
3) Cisco IOS VPN
Reference: Cisco Courseware p.4-3

QUESTION 64:

Which two Cisco components encompass secure management? (Choose two)

A. Cisco VPN Concentrators
B. CiscoWorks
C. Cisco IDS Sensors
D. Cisco PIX Firewalls
E. Web Device Managers

Answer: B, E

QUESTION 65:

Which statement about SAFE SMR principles is true?

A. SAFE SMR principles are based on Cisco products and features.
B. SAFE SMR principles are not necessarily device specific.
C. SAFE SMR principles are device specific.
D. SAFE SMR principles allow you to guarantee network security.

Answer: A

Explanation:
The Cisco SAFE SMR principles tries to go away from the usual Device Specific design templates out there but it is still based on cisco and partner products.
To quote: SAFE "Its not a device!" SAFE was created by Cisco to help designers of network secutity;
its a design philosophy that utilizes Cisco and Cisco partner products. SAFE SMR takes a threat-mitigation-centric
approach to security design instead of the more common device-centric design approach.
I would go with on this one; could one.could have been B but i know how cisco think;they like to promote their own products in their tests.

QUESTION 66:

Which two Cisco components encompass intrusion protection? (Choose two)

A. Cisco VPN Concentrators
B. Cisco IDS Sensors
C. Cisco IDS Access Point
D. Cisco IOS IDS
E. Cisco Wireless IDS

Answer: B, D

Explanation:
Cisco routers with IOS IDS features
Cisco Secure IDS Sensors
Reference: Cisco Threat Response User Guide

QUESTION 67:

What services does remote access VPNs provide?

A. Link corporate headquarters to remote offices.
B. Link network resources with third-party vendors and business partners.
C. Link telecommuters and mobile users to corporate network resources.

D. Link private networks to public networks.

Answer: C

Explanation: The primary function of the remote access VPN concentrator is to provide secure connectivity to the medium network for remote users
REF;Safe white papers;page20
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 68:

What services do intranet VPNsprovide?

A. Link corporate headquarters to remote offices.
B. Link network resources with third-party vendors and business partners.
C. Link telecommuters and mobile users to corporate network resources.
D. Link private networks to public networks.

Answer: A

Explanation:
Intranet VPNs refer to connections between sites that are all part of the same company. As such, access between sites is generally less restrictive.
Reference: SAFE VPN: IPSec Virtual Private Networks in Depth page 76

QUESTION 69:

John the security administrator at Certkiller Inc. is working on purchasing three Cisco 3000 series concentrators. Which three models of the Cisco 3000 Series Concentrator can have redundant power supplies? (Choose three)

A. Model number 3090
B. Model number 3080
C. Model number 3060
D. Model number 3030
E. Model number 3020
F. Model number 3005

Answer: B C D

Explanation:
Redundant SEP modules (optional), power supplies, and fans (Cisco VPN 3015-3080)
Reference: Cisco VPN 3000 Series Concentrators - Cisco VPN 3000 Series Concentrator Data Sheet
Reference: Cisco Courseware page 4-10

QUESTION 70:

What type of authentication does the Cisco 3000 Series Concentrator use?

A. RADIUS
B. TACACS+
C. CHAP
D. PAP

Answer: A

Explanation: Full support of current and emerging security standards, including RADIUS, NT Domain Authentication, RSA SecurID, and digital certificates, allows for integration of external authentication systems and interoperability with third-party products
Ref:
Cisco VPN 3000 Series Concentrators - Cisco VPN 3000 Series Concentrator Overview

---

QUESTION 71:

Which three models of the Cisco 3000 Series Concentrator can provide redundancy? (Choose three)

A. 3005
B. 3010
C. 3015
D. 3030
E. 3060
F. 3080

Answer: D, E, F

Explanation: Redundant 3000 series concentrators are:
Cisco VPN 3030 Concentrator
Cisco VPN 3060 Concentrator
Cisco VPN 3080 Concentrator
Ref
Cisco VPN 3000 Series Concentrators - Cisco VPN 3000 Series Concentrator Data Sheet

---

QUESTION 72:

What does the Cisco Unified Client framework provide?

A. Distributed push policy technology.
B. Centralized push policy technology.
C. Centralized pull policy technology.

D. Multi-tiered policy technology.

Answer: B

Explanation:
Utilizing "push policy" capabilities, the unified VPN client framework allows customers to centrally manage security policies, while easily delivering large-scale VPN connectivity to remote users. All of Cisco's IPsec-based VPN products for the enterprise and service providers will support the unified VPN client framework.
Reference: Cisco Extends VPN Leadership - Announces Unified VPN Client Framework and Multi-protocol VPN Solution at
Cisco Partner Summit 2001

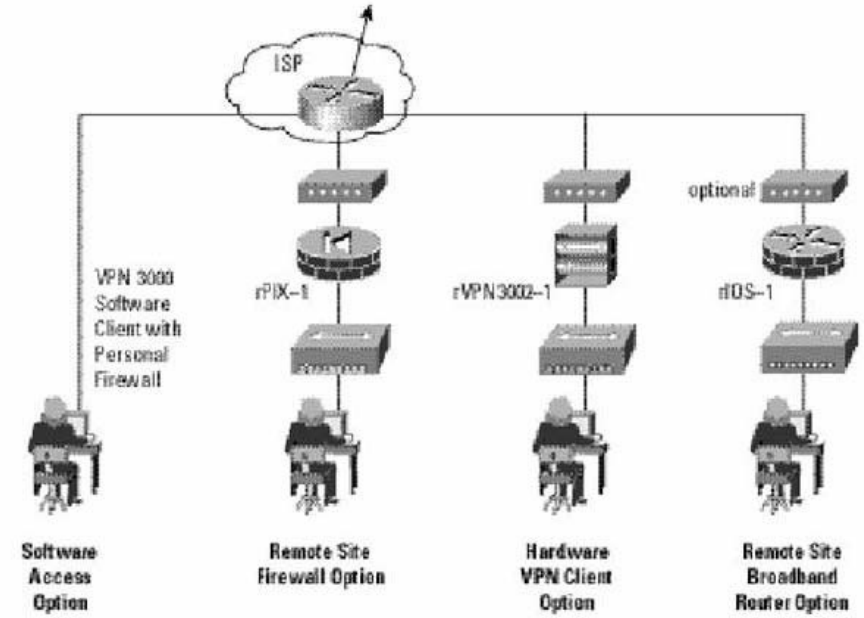
QUESTION 73:

According to SAFE SMR guidelines, where do you implement the Cisco VPN 3000 Series Concentrator?

A. In front of the Internet access router.
B. Behind the PIX Firewall and parallel to the Internet access router.
C. Behind the Internet access router and parallel to the PIX Firewall.
D. Behind the corporate network module.

Answer: C

Explanation:



Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 59

QUESTION 74:

When configuring an IKE proposal on a VPN 3000 Concentrator, which of the following proposal names are valid?

A. Proposal Name: IKE-3DES
B. Proposal Name: IKE-3DES-MD5-DH7
C. Proposal Name: IKE-DH7-3DES-MD5
D. Proposal Name: IKE-3DES-DH7-MD5

Answer: B
Reference: Cisco VPN 3000 Series Concentrators - Tunneling Protocols
Reference: Cisco Courseware page 6-59

QUESTION 75:

James the security administrator at Certkiller Inc. is working on VPNs.
According to SAFE SMR guidelines, what type of VPN uses primarily Cisco VPN optimized routers?

A. Intranet to extranet type of VPN.
B. Extranet to remote user type of VPN.
C. Intranet to remote user type of VPN.
D. Site-to-site type of VPN.

Answer: D

Explanation: The VPN Acceleration Module (VAM) for Cisco 7200 and 7100 Series routers provides high-performance, hardware-assisted encryption, key generation, and compression services suitable for site-to-site virtual private network (VPN) applications.
Ref: VPN Acceleration Module for Cisco 7000 Series VPN Routers

---

QUESTION 76:

The security team at Certkiller Inc. is researching the SAFE SMR White papers.
According to SAFE SMR, which Cisco router is best suited for a remote office?

A. Cisco router 1700 series
B. Cisco router 800 and 900 series
C. Cisco router 2600 and 3600 series
D. Cisco router 7100 and 7200 series

Answer: A

QUESTION 77:

The VPN acceleration module (VAM) is available on what series of VPN optimized routers? (Choose two)

A. 1700 Series
B. 2600 Series
C. 3600 Series
D. 7100 Series
E. 7200 Series

Answer: D, E

Explanation: The VPN Acceleration Module (VAM) for Cisco 7200 and 7100 Series routers provides high-performance, hardware-assisted encryption, key generation, and compression services suitable for site-to-site virtual private network (VPN) applications.
Ref: VPN Acceleration Module for Cisco 7000 Series VPN Routers

---

QUESTION 78:

Which two models of the PIX Firewall make the VPN accelerator card available? (Choose two)

A. Model number 535
B. Model number 515
C. Model number 505
D. Model number 503
E. Model number 501

Answer: A B

Explanation:
System Requirements
Operating System: PIX OS v5.3(1) or later (with DES or 3DES license)
Platforms: PIX 515/515E, 520, 525, 535 (limit one per chassis)
Reference: Cisco PIX 500 Series Firewalls - Cisco PIX Firewall VPN Accelerator Card

---

QUESTION 79:

You are selling PIX firewalls at Certkiller Inc. What size network is best suited for the PIX Firewall 501?

A. Large enterprise or service provider
B. Midsize enterprise
C. Small office or home office

D. Small business or branch office

Answer: C

Explanation:
The Cisco PIX 501 Security Appliance delivers a multilayered defense for small offices through rich security services including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN), in-line intrusion protection, and rich multimedia and voice security in a single device. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b18.html

---

QUESTION 80:

What size network is best suited for the Cisco PIX Firewall 525 or 535?

A. Small office or home office.
B. Small business or branch office.
C. Midsize enterprise.
D. Large enterprise or service provider.

Answer: D

Explanation: The Cisco PIX Firewall 525 is a large, enterprise perimeter firewall solution. The Cisco PIX firewall 535 delivers carrier-class performance to meet the needs of large enterprise networks as well as service providers.
Ref: Cisco Secure PIX Firewalls (Ciscopress) Page 26

QUESTION 81:

What does CBAC dynamically create and delete?

A. TCP sessions
B. Crypto maps
C. Access control lists
D. Security control lists

Answer: C

Explanation: CBAC dynamically creates and deletes access control list entries at each router interface, according to information in the state tables.
Ref:
Cisco IOS Firewall - Cisco IOS Firewall Feature Set

QUESTION 82:

You are the administrator at Certkiller Inc. and you are implementing IDS to the network. Which model is recommended for IDS with at least 100 Mbps performance?

A. Model number 4260
B. Model number 4250
C. Model number 4220
D. Model number 4210

Answer: B

Explanation:
The Cisco IDS 4250 supports unparalleled performance at 500 Mbps and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/ps4079/index.html

QUESTION 83:

What is IP logging, as defined for the Cisco IDS appliance?

A. IDS logs IP address information for hosts being attacked.
B. IDS logs user information from an attacking host.
C. IDS captures packets from an attacking host.
D. IDS logs IP address information from an attacking host.

Answer: C

Explanation: In addition to the packet capture that analyzes the traffic to identify malicious activity, the IDSM-2 can perform IP session logging that can be configured as a response action on a per-signature basis. If configured as such, when the signature fires, session logs will be created over a pre-specified time period in a TCP Dump format.
Ref:
Cisco Services Modules - Cisco Catalyst 6500 IDS (IDSM-2) Services Module

QUESTION 84:

An administrator claims he is receiving too many false positives on his IDS system. What is he referencing?

A. Alarms detected and logged by IDS.
B. Alarms detected by IDS and not acted upon.

C. Alarms caused by illegitimate traffic or activities.
D. Alarms caused by legitimate traffic or activities.

Answer: D

Explanation: False-positives are defined as alarms caused by legitimate traffic or activity.
False negatives are attacks that the IDS system fails to see.
REF;Safe white papers;page 8
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 85:

For the first time you want to set up your IDS Appliance using IDM (IDS Device Manager): Choose the steps that you should take:

A. Specify list of hosts authorized to managed appliance.
B. Communications Infrastructure.
C. Enter network setting.
D. Specify Logging Device.
E. Signatures

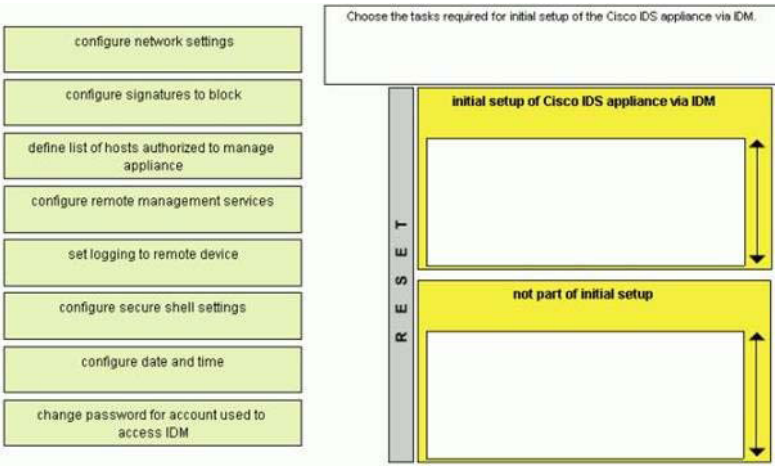
Answer: A, B, C

Explanation:
1. Specify host to manage appliance.
2. Communication Infrastructure - Refers to names and IDs of the sensor and manager
3. Network setting: IP address
IP Netmask
IP Hostname
Default route
Ref:
Cisco Intrusion Detection System - IDS Device Manager Sensor Setup

---

QUESTION 86:

Choose the tasks required for initial setup of the Cisco IDS appliance via IDM.



Answer:

Explanation:
Choose the task required for initial setup of the Cisco IDS Appliance via IDM
Initial setup of Cisco IDS appliance via IDM.
Configure network settings
Define list of hosts authorized to manage appliance
Configure date and time
Change password to account used to access IDM
Not part of Initial Setup
Configure signatures to block.
Configure remote management services
Set logging to remote device
Configure secure shell settings
Reference: Cisco Intrusion Detection System - IDS Device Manager Sensor Setup
Reference: Cisco IDS Courseware page 7-24

QUESTION 87:

Using the default, how does the Cisco IDS appliance log events? (Choose two)

A. Location
B. Type
C. Rule base
D. Effect
E. Severity
F. User option

Answer: B E

Explanation:
Cisco Secure IDS Sensors can be configured to generate log file locally on the sensor. By default, the sensors are configured to send alarms of severity of medium and higher to

CSPM.
Reference:

QUESTION 88:

Which model is recommended for an IDSwith at least 100 Mbps performance?

A. 4210
B. 4220
C. 4250
D. 4260

Answer: C

Explanation:
The Cisco IDS 4250 supports unparalleled performance at 500 Mbps and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/ps4079/index.html
Incorrect Answers
A: Performance: 45 Mbps
B: No such model
D: No such model

QUESTION 89:

The security team at Certkiller Inc. is working on securing their network.
What is the primary identity component in a Cisco security solution?

A. primary identity component Cisco VPN Concentrators
B. primary identity component Cisco PIX Firewalls
C. primary identity component Cisco IDS Sensors
D. primary identity component Cisco IOS Firewalls
E. primary identity component Cisco Access Control servers

Answer: E

Explanation:
Cisco Identity Based Networking Services (IBNS) is an integrated solution combining several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. Cisco IBNS solution enables greater security while simultaneously offering cost-effective management of changes throughout the organization.
IBNS and 802.1x are supported on all Cisco Catalyst switches, including Catalyst 6500, 4500, 3550, and 2950 switches, Cisco ACS Server as well as Cisco Aironet Access

Points.
Reference:
http://www.cisco.com/en/US/netsol/ns110/ns170/ns360/ns373/networking_solutions_package.html

---

QUESTION 90:

What is the default port for Cisco's ACS RADIUS authentication server?

A. 1645
B. 1812
C. 1640
D. 1814

Answer: A.

Explanation: Enabling EAP on the Access Point
Follow these steps to enable EAP on the Access Point:
1. Follow the link path to the Authentication Server Setup page.
2. Enter the name or IP address of the RADIUS server in the Server Name/IP entry field.
3. Enter the port number your RADIUS server uses for authentication. The default setting, 1812, is the port setting
for many RAFIUS servers;
1645 is the port setting for Cisco's RADIUS server, the Cisco Secure Access Control Server (ACS).
Check your server's product documentation to find the correct port setting.
4. Enter the shared secret used by your RADIUS server in the Shared Secret entry field. The shared secret on the
Access Point must match the shared secret on the RADIUS server.
5. Enter the number of seconds the Access Point should wait before authentication fails.
6. Click OK. Returns to the Security Setup page.
7. On the Security Setup page, click Radio Data Encryption (WEP) to browse to the AP Radio Data Encryption
page.
8. Select Network-EAP for the Authentication Type setting. You can also enter this setting on the AP Radio
Advanced page.
9. Check that at least one WEP key has been assigned a

key size and has been selected as the transmit key. If a WEP
key has been set up, skip to Step 13. If no WEP key has been set up, proceed to Step 10.
10. Enter a WEP key in one of the Encryption Key fields. The Access Point uses this key for multicast data signals
(signals sent from the Access Point to several client devices at once). This key does not need to be set on client
devices.
11. Select 128-bit encryption from the Key Size pull-down menu.
12. Select the key as the transmit key.
13. Click OK. Return automatically to the Security Setup page.
Reference: Cisco Courseware Labguidepage 133

QUESTION 91:

Cisco Secure ACS supports with of the following authentication methods? (Choose all that apply)

A. Radius
B. MPPE
C. PAP
D. TACACS+
E. PPP
F. CHAP

Answer: A, C, D, F
Ref: Troubleshooting Information for CiscoSecureACS
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt30/user/aa.htm

---

QUESTION 92:

What three authentication methods are supported by CSACS? (Choose three)

A. PPP
B. RADIUS
C. CHAP
D. TACACS+
E. PAP
F. Static passwords

Answer: B, C, D

Explanation:
Reference: Cisco Secure Access Control Server for Windows - Release Notes for Cisco Secure Access Control Server for Windows Server Version 3.1

QUESTION 93:

You are the administrator at Certkiller Inc. working on managing security on the network. Which two Cisco components encompass secure management? (Choose two)

A. Cisco VPN Concentrators
B. CiscoWorks
C. Cisco IDS Sensors
D. Cisco PIX Firewalls
E. Web Device Managers

Answer: B E

QUESTION 94:

The high availability of network resources in Cisco AVVID Network Infrastructure solutions can be optimized through: (Choose all that apply)

A. Hot swappability
B. Protocol Resiliency
C. Hardware Redundancy
D. Network Capacity Design
E. Fast Network convergence

Answer: B, C, D

Explanation: Determining how resilient a network is to change or disruption is major concern for network managers. This assessment of network availability is critical. It is essential that every network deployment emphasizes availability as the very first consideration in a baseline network design. Key availability issues to address include:
* Protocol Resiliency
* Hardware Redundancy
1. Network Capacity Design
REF;Safe white papers;page 23
Cisco AVVID Network Infrastructure Overview - White Paper

QUESTION 95:

Which of the dimensions of AVVID resilience themes represent the migration from the traditional place-centric enterprise structures to people-centric organizations?

A. Network Resilience
B. Communications Resilience
C. Business Resilience
D. Routing Resilience
E. Applications Resilience

Answer: C

Explanation: Business resilience represents the next phase in the evolution from traditional, place-centric enterprise structures to highly virtualized, people-centric organizations that enable people to work anytime, anywhere.
REF;AVCID white papers;2
Cisco AVVID Network Infrastructure Overview - White Paper

QUESTION 96:

According to SAFE, small network design has how many modules?

A. 2
B. 3
C. As many as the Enterprise architecture.
D. 5
E. 4

Answer: A

Explanation: The small network design has two modules: the corporate Internet module and the campus module.
REF;Safe white papers;10
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 97:

Which commands are used for basic filtering in the SAFE SMR small network campus module? (Choose two)

A. Access-group
B. Ip inspect-name
C. Ip route
D. Access-list

Answer: A, D

Explanation:

REF;Safe white papers;
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 98:

How many modules are in the SAFE SMR small network design?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: B

Explanation:
The small network design has two modules: the corporate Internet module and the campus module.
REF;Safe white papers;10
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 99:

Which two devices in the SAFE SMR small network campus module should have HIDS installed? (Choose two)

A. Layer 2 switches
B. Firewalls
C. Management hosts
D. Desktop workstations
E. Corporate servers
F. Lab workstations

Answer: C, E

Explanation:
Because there are no Layer 3 services within the campus module, it is important to note that this design places an increased emphasis on application and host security because of the open nature of the internal network. Therefore, HIDS was also installed on key systems within the campus, including the corporate servers and management systems.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 15

QUESTION 100:

What two modules are in the SAFE SMR small network design? (Choose two)

A. Edge
B. Internet
C. Corporate Internet
D. Campus

Answer: C, D

Explanation:
The small network design has two modules: the corporate Internet module and the campus module. The corporate Internet module has connections to the Internet and also terminates VPN and public services (DNS, HTTP, FTP, SMTP) traffic. The campus module contains the Layer 2 switching and all the users, as well as the management and intranet servers.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 10

QUESTION 101:

You are the administrator at Certkiller Inc. and you need to implement a firewall in the SAFE SMR small network design.
In which module does the firewall exist in the SAFE SMR small network design?

A. The Internet module
B. The Corporate Internet module
C. The Campus module
D. The Edge module

Answer: B

Explanation:
Corporate Internet Module
Key Devices:
1. SMTP server-Acts as a relay between the Internet and the intranet mail servers
2. DNS server - servers as authoritative external DNS server for the enterprise;relays internal requests to the Internet
3. FTP/HTTP server-Provides public information about the organization
4. Firewall or firewall router-Provides network-level protection of resources, stateful filtering of traffic, and VPN termination for remote sites and users
5. Layer 2 switch (with private VLAN support)-Ensures that data from managed devices can only cross directly to the IOS firewall
Reference: Safe white papers;11
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 102:

Kathy the security administrator at Certkiller Inc. is implementing HIDS in the SAFE SMR small network corporate Internet module.
On what device within the SAFE SMR small network corporate Internet module should Kathy perform HIDS local attack mitigation?

A. HIDS is performed on Public services servers
B. HIDS is performed on Layer 2 switch
C. HIDS is performed on Firewall
D. HIDS is performed on Routers

Answer: A

Explanation:
Application layer attacks-Mitigated through HIDS on the public servers
Reference: Safe white papers;11
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks
Reference: Cisco Courseware page 9-46

QUESTION 103:

According to SAFE SMR, what type of VPN connectivity is typically used with the Cisco PIX Firewall?

A. Remote access
B. Site-to-site
C. Mobile user
D. Corporate

Answer: B

Explanation: The VPN connectivity is provided through the firewall or firewall/router. Remote sites authenticate each other with pre-shared keys and remote users are authenticated through the access control server in the campus module.
REF;Safe white papers;page 13
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 104:

Which method will always compute the password if it is made up of the character set you selected to test?

A. Brute force computation
B. Strong password computation
C. Password reassemble
D. Brute force mechanism

Answer: A

QUESTION 105:

How are application layer attacks mitigated in the SAFE SMR small network corporate Internet module?

A. NIDS
B. Virus scanning at the host level.
C. HIDS on the public servers.
D. Filtering at the firewall.
E. CAR at ISP edge.
F. TCP setup controls at the firewall to limit exposure.

Answer: C

Explanation: Application layer attacks - Mitigated through HIDS on the public servers
REF;Safe white papers;page 11
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 106:

How are packet sniffers attacks mitigated in the SAFE SMR small network corporate Internet module?

A. RFC 2827 and 1918 filtering at ISP edge and local firewall.
B. Switched infrastructure and HIDS.
C. Protocol filtering
D. Restrictive trust model and private VLANs.
E. Restrictive filtering and HIDS.

Answer: B

Explanation: Mitigated Threats
Packet sniffers-Switched infrastructure and host IDS to limit exposure
REF;Safe white papers;page 11
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 107:

HIDS local attack mitigation is performed on what devices within the SAFE SMR small network corporate Internet module?

A. Layer 2 switches

B. Firewalls
C. Routers
D. Public services servers

Answer: D

Explanation: Application layer attacks-Mitigated through HIDS on the public servers

---

QUESTION 108:

Which three key devices are in the SAFE SMR small network corporate Internet module? (Choose three)

A. Servers
B. VPN concentrators
C. Layer 3 switches
D. Firewalls
E. Layer 2 switches
F. NIDS

Answer: A, D, E

Explanation: Key Devices
SMTP server
DNS server
FTP/HTTP server
Firewall or Firewall router
Layer 2 switch(with private VLAN support)
REF;Safe white papers;page11
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 109:

How are trust exploitation attacks mitigated in the SAFE SMR small network corporate Internet module?

A. RFC 2827 and 1918 filtering at ISP edge and local firewall.
B. Switched infrastructure and HIDS.
C. Protocol filtering.
D. Restrictive trust model and private VLANs.
E. Restrictive filtering and HIDS.

Answer: D

Explanation:

Trust exploitation-Restrictive trust model private VLANs to limit trust-based attacks
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 11

QUESTION 110:

John the security administrator at Certkiller Inc. is working on mitigating all threats to the network.
What threats are expected for the SAFE SMR small network campus module? (Choose two)

A. The IP spoofing threat
B. The Packet sniffers threat
C. The Application layer attacks threat
D. The Denial of service threat

Answer: B;C

Explanation:
Threats Mitigated
1. Packet sniffers-A switched infrastructure limits the effectiveness of sniffing
2. Virus and Trojan-horse applications-Host-based virus scanning prevents most viruses and many Trojan horses
3. Unauthorized access-This type of access is mitigated through the use of host-based intrusion detection and application access control
4. Application layer attacks-Operating systems, devices, and applications are kept up-to-date with the latest security fixes, and they are protected by HIDS
5. Trust exploitation-Private VLANs prevent hosts on the same subnet from communicating unless necessary
6. Port redirection-HIDS prevents port redirection agents from being installed
Reference: Safe white papers:14
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 111:

You are the administrator at Certkiller Inc and you are implementing a small filtering router. As an alternative design in the SAFE SRM small network campus module, a small filtering router can be placed between the rest of the network and which devices?

A. The rest of the network and Layer 2 switches
B. The rest of the network and corporate users
C. The rest of the network and management stations
D. The rest of the network and routers

Answer: C

Explanation:
Alternatives
Setting a small filtering router or firewall between the management stations and the rest of the network can improve overall security. This setup will allow management traffic to flow only in the specific direction deemed necessary by the administrators. If the level of trust within the organization is high, HIDS can potentially be eliminated, though this is not recommended.
Reference: Page 15
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 112:

Which commands are used for basic filtering in the SAFE SMR small network campus module? (Select two.)

A. access group
B. ip inspect-name
C. ip route
D. access-list

Answer: A, D

QUESTION 113:

How are packet sniffer attacks mitigated in the SAFE SMR small network campus module?

A. Host based virus scanning.
B. The latest security fixes.
C. The use of HIDS and application access control.
D. Switches infrastructure
E. HIDS

Answer: D

Explanation: Packet snuffers-Threats mitigated; switched infrastructure and host IDS to limit exposure.
REF;Safe white papers;page 18
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 114:

What can be implemented in the SAFE SMR small network campus module to mitigate trust exploitation attacks between devices?

A. Layer 2 switches
B. Firewalls
C. Private VLANs
D. Routers

Answer: C

Explanation: Threats mitigated
Trust exploitation-Restrictive trust model and private VLANs to limit trust-based attacks
REF;Safe white papers;page 18
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 115:

What are three of the key devices in the SAFE SMR small network campus module? (Choose three)

A. Layer 2 switches
B. IOS firewall
C. User workstations
D. PIX firewall
E. Corporate servers
F. NIDS

Answer: A, C, E

Explanation: Key Devices
Layer 2 switching
Corporate server
user workstation
Management host
REF;Safe white papers;page13
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 116:

How are port redirection attacks mitigated in the SAFE SMR small network campus module?

A. Switched infrastructure.
B. Host based virus scanning.
C. The use of NIDS and application access control.
D. The latest security fixes and NIDS.
E. Private VLANs
F. HIDS

Answer: F

Explanation:
Port redirection-HIDS prevents port redirection agents from being installed
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 14

QUESTION 117:

What three commands are used for RFC 1918 and RFC 2827 filtering on the ISP router in the SAFE SMR small network campus module? (Choose three)

A. ip route 1918
B. access-list
C. access-group
D. enable rfc 1918 filtering
E. rate-limit
F. enable rfc 2827 filtering

Answer: B C E

Explanation:
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 47

QUESTION 118:

The security team at Certkiller Inc. is working on implementing IOS firewall in their SAFE SMR small network design.
What is the primary function of the IOS firewall in the SAFE SMR small network design?

A. The primary function is it provides remote site connectivity and general filtering for sessions initiated through the firewall.
B. The primary function is it provides host DoS mitigation.
C. The primary function is it authenticates IPSec tunnels.
D. The primary function is it provides remote site authentication.
E. The primary function is it provides connection state enforcement and detailed filtering for sessions initiated through the firewall.

Answer: E

Explanation:
Layer 2 switch (with private VLAN support)-Ensures that data from managed devices can only cross directly to the IOS firewall

Reference: Safe white papers; 11
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 119:

You are the administrator at Certkiller Inc. and you are configuring the PIX Firewall. The ip verify reverse-path command implements which of the following on the PIX Firewall? (Choose two)

A. The ip verify reverse-path command performs a route lookup based on the destination address.
B. The ip verify reverse-path command performs a route lookup based on the source address.
C. The ip verify reverse-path command provides session state information based on source address.
D. The ip verify reverse-path command provides ingress filtering.
E. The ip verify reverse-path command provides session state information based on destination address.

Answer: B D

Explanation:
Use the ipverify unicast reverse-path interface command on the input interface on the router at the upstream end of the connection. This feature examines each packet received as input on that interface. If the source IP address does not have a route in the CEF tables that points back to the same interface on which the packet arrived, the router drops the packet.
Reference: Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks

---

QUESTION 120:

Jason is the security administrator at
Certkiller Inc. and wants to know which is true with regard to creating an RPC entry with the NFS program number?

A. The true statement is NFS traffic designated as friendly will be allowed through the firewall.
B. The true statement is no NFS traffic will be allowed through the firewall.
C. The true statement is all NFS traffic will be allowed through the firewall.
D. The true statement is NFS traffic designated as hostile will not be allowed through the firewall.

Answer: C

Explanation:
Remote Procedure Call (RPC) inspection enables the specification of various program

numbers. You can define multiple program numbers by creating multiple entries for RPC inspection, each with a different program number. If a program number is specified, all traffic for that program number is permitted. If a program number is not specified, all traffic for that program number is program number, all NFS traffic is allowed through the firewall.
Reference: CSI Student Guide v2.0 p. 5-30

QUESTION 121:

What is the function of SMTP inspection?

A. Monitors SMTP mail for hostile commands.
B. Monitors SMTP commands for illegal commands.
C. Monitors traffic from and STMP server that is designated as friendly.
D. Monitors traffic that has not been encapsulated.

Answer: B

Explanation: SMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns.
Ref: Cisco Pix Firewall Software (Configuring Application Inspection (Fixup)
Cisco PIX Firewall Software - Configuring Application Inspection (Fixup)

QUESTION 122:

How does Java applet filtering distinguish between trusted and untrustedapplets?

A. Examines the applet for suspicious code.
B. Relies on a list of applets that you designate as hostile.
C. Relies on a list of applets that you designate as friendly.
D. Relies on a list of external sites that you designate as friendly.

Answer: D

Explanation:
Java inspection enables Java applet filtering at the firewall. Java applet filtering distinguishes between trusted and untrusted applets by relying on a list of external sites that you designate as "friendly." If an applet is from a friendly site, the firewall allows the applet through. If the applet is not from a friendly site, the applet will be blocked. Alternately, you could permit applets from all sites except for sites specifically designated as "hostile."
Reference: Context-Based Access Control Commands

QUESTION 123:

You are the security administrator at Certkiller Inc. and you are working on filtering

network traffic.
accesslist 101 deny ip 192.168.8.8 0.0.0.255 anyis an example of an ACL entry to filter what type of addresses?

A. It is an example of RFC 1920
B. It is an example of RFC 2728
C. It is an example of RFC 2827
D. It is an example of RFC 1918

Answer: D

Explanation:
! RFC 1918 filtering. Note network 172.16.x.x was not included in the
! filter here since it is used to simulate the ISP in the lab.
!
access-list 103 deny ip 10.0.0.0 0.255.255.255 any
access-list 103 deny ip 192.168.0.0 0.0.255.255 any
Reference: Page 47
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 124:

What is the function of a crypto map on a PIX Firewall?

A. To configure a pre-shared authentication key and associate the key with an IKE peer address or host name.
B. To configure a pre-shared authentication key and associate the key with an IPSec peer address or host name.
C. To specify which algorithms to use with the selected security protocol.
D. To filter and classify the traffic to be protected.

Answer: D

Explanation: Crypto map entries for IPSec set up security association parameters, tying toghter the various parts configured for IPSec,including the following;
* Which traffic should be protected by IPSec
Ref: Cisco Secure PIX Firewalls (Ciscopress) Page 215

QUESTION 125:

What causes the default TCP intercept feature of the IOS Firewall to become more aggressive? (Choose two)

A. The number of incomplete connections exceeds 1100.
B. The number of connections arriving in the last 1 minute exceeds 1100.
C. The number of incomplete connections exceeds 100.

D. The number of connections arriving in the last 10 minutes exceeds 1000.

Answer: A, B

Explanation: If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last 1minute exceeds 1100, the TCP intercept feature becomes more aggressive.
Ref:
Cisco IOS Software Releases 12.1 Mainline - TCP Intercept Commands

---

QUESTION 126:

Which command implements UnicastRPF IP spoofing protection?

A. access-list
B. access-group
C. ip verify reverse-path interface
D. tcp verify reverse-path interface
E. udp verify reverse-path interface

Answer: C

Explanation:
Use the ipverify unicast reverse-path interface command on the input interface on the router at the upstream end of the connection. This feature examines each packet received as input on that interface. If the source IP address does not have a route in the CEF tables that points back to the same interface on which the packet arrived, the router drops the packet.
Reference: Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks

---

QUESTION 127:

How many transforms can be included in a transform set on a PIX Firewall?

A. 1
B. 2
C. 3
D. 4
E. unlimited number

Answer: C

Explanation: Up to three transforms can be in a set. Sets are limited to up to one AH
And up to two ESP transforms.
Reference: Cisco Secure PIX Firewalls (Ciscopress) Page 212

QUESTION 128:

What is the function of a crypto map on a PIX Firewall?

A. To define the policy that will be applied to the traffic.
B. To specify which algorithms will be used with the selected security protocol.
C. To configure a pre-shared authentication key and associate the key with an IPSec peer address or host name.
D. To map transforms to transform sets.

Answer: A

Explanation:
Crypto map entries must be created for IPSec to set up SAs for traffic flows that must be encrypted.
Reference: Cisco Secure PIX Firewalls (Ciscopress) Page 215

QUESTION 129:

Which version of PIX introduces support for the VPN accelerator card?

A. Version 4.0
B. Version 4.3
C. Version 5.0
D. Version 5.3

Answer: D

Explanation:
System Requirements
Operating System: PIX OS v5.3(1) or later (with DES or 3DES license)
Platforms: PIX 515/515E, 520, 525, 535 (limit one per chassis)
Reference: Cisco PIX 500 Series Firewalls - Cisco PIX Firewall VPN Accelerator Card

QUESTION 130:

What version of the Cisco PIX Firewall is required to use the VPN accelerator card?

A. Version 2.3 or higher.
B. Version 3.3 or higher.
C. Version 4.3 or higher.
D. Version 5.3 or higher.
E. Version 6.3 or higher.

Answer: D

Explanation:
System Requirements
Operating System: PIX OS v5.3(1) or later (with DES or 3DES license)
Platforms: PIX 515/515E, 520, 525, 535 (limit one per chassis)
Reference: Cisco PIX 500 Series Firewalls - Cisco PIX Firewall VPN Accelerator Card

---

QUESTION 131:

John the security administrator at Certkiller is working on mitigating DoS in the network. How are DoS attacks mitigated in the SAFE SMR small network corporate Internet module? (Choose two)

A. Mitigated by CAR at ISP edge.
B. Mitigated by NIDS
C. Mitigated by TCP setup controls at the firewall to limit exposure.
D. Mitigated by HIDS on the public serves.
E. Mitigated by virus scanning at the host level.

Answer: A C

Explanation:
Threat Mitigation
Denial of service-Committed access rate (CAR) at ISP edge and TCP setup controls at firewall to limit exposure
Reference: Page 11
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 132:

You are the administrator at Certkiller Inc. and you need pick a device to help you secure the network. Which device in the SAFE SMR midsize network design corporate Internet module determines when to provide TCP shunning or resets?

A. IDS
B. Firewall
C. Router
D. Public services servers
E. Layer 2 switches

Answer: A

Explanation:
The NIDS appliance between the private interface of the firewall and the internal router provides a final analysis of attacks. Very few attacks should be detected on this segment

because only responses to initiated requests, a few select ports from the public services segment, and traffic from the remote access segment are allowed to the inside. Only sophisticated attacks should be seen on this segment because they could mean that a system on the public services segment has been compromised and the hacker is attempting to take advantage of this foothold to attack the internal network. For example, if the public SMTP server were compromised, a hacker might try to attack the internal mail server over TCP port 25, which is permitted to allow mail transfer between the two hosts. If attacks are seen on this segment, the responses to those attacks should be more severe than those on other segments because they probably indicate that a compromise has already occurred. The use of TCP resets or shunning to thwart, for example, the SMTP attack mentioned above, should be seriously considered.
Reference: Safe white papers;page 19
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 133:

You are the leader of the security team at Certkiller Inc and you are working on mitigation trust exploitation attacks. How is trust exploitation attacks mitigated in the SAFE SMR midsize network design corporate Internet module?

A. Mitigated by using restrictive trust model and private VLANs.
B. Mitigated by using OS and IDS detection.
C. Mitigated by using restrictive filtering and host IDS.
D. Mitigated by using IDS at the host and network levels.
E. Mitigated by using filtering at the ISP, edge router, and corporate firewall.

Answer: A

Explanation:
Trust exploitation-Restrictive trust model and private VLANs to limit trust-based attacks
Reference: Safe white papers;page 17
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 134:

Jason the security administrator at Certkiller Inc is working on dial in users for the network. In the SAFE SMR midsize network design, which module does dial-in traffic terminate?

A. It terminates at the campus module
B. It terminates at the WAN module
C. It terminates at the Corporate Internet module
D. It terminates at the ISP edge module
E. It terminates at the PSTN module
F. It terminates at the Frame/ATM module

Answer: C

Explanation:
The SAFE medium network design consists of three modules: the corporate Internet module, the campus module, and the WAN module. As in the small network design, the corporate Internet module has the connection to the Internet and terminates VPN and public-services (DNS, HTTP, FTP, and SMTP) traffic. Dial-in traffic also terminates at the corporate Internet module.
Reference: Safe white papers;page 16
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks
Reference: Cisco Courseware page 6-3

QUESTION 135:

You are the security administrator at Certkiller Inc and you need to authenticate users to the network. After being authenticated, which actions are performed on dial-in access users in the SAFE SMR midsize network design corporate Internet module?

A. After being authenticated, CHAP is used to authenticate the user.
B. After being authenticated, traffic is sent through a Layer 3 switch.
C. After being authenticated, users are provided with IP addresses from an IP pool.
D. After being authenticated, traffic is sent through a router.

Answer: C

Explanation: Last sentence of the paragraph states: When authenticated, the users are provided with IP addresses from an IP pool.
However it also states that CHAP is used to authenticate the user (Answer A)
But the keyword is 'After being authenticated' not 'During or When'.
Reference: Cisco SAFE Implementation Courseware version 1.1 Page 6-17

QUESTION 136:

In which module does VPN traffic terminate in the SAFE SMR midsize network design?

A. WAN module
B. Campus module
C. Corporate Internet module
D. ISP edge module
E. PSTN module
F. Frame/ATM module

Answer: C

Explanation: As in the small network design, the corporate Internet module has the

connection to the Internet and terminates VPN and public-services (DNS, HTTP, FTP, and SMTP) traffic.
REf;Safe white papers;page 16
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 137:

Based on the SAFE Model of Small Networks, which threats can only be mitigated at the corporate Internet module (not at the campus module)? (Choose all that apply)

A. Password attacks
B. Port redirection
C. Virus and Trojan horse
D. IP spoofing
E. Denial of service
F. Network reconnaissance

Answer: A, B, C, D, E, F

Explanation:
Reference: Table 13-3 Page 201 of CCSP CSI Exam Certification Guide AND Page 5-5 and 5-6 of CISCO SAFE Courseware under Expected Treat and Mitigation Roles
The following are threats to be expected:
1)Unauthorised Access
2)Application layer attacks
3)Virus and Trojan horse attacks
4)Password attacks
5)DoS
6)IP spoofing
7)Packet sniffers
8)Network reconnaissance
9)Trust Exploitation
10)Port Redirection

QUESTION 138:

In the corporate Internet module of SAFE SMR midsize network design, following termination of the VPN tunnel, traffic is sent through:

A. A wireless device.
B. A Layer 3 switch
C. A router
D. A Firewall

Answer: D

Explanation: The firewall also acts as a termination point for site-to-site IPSec VPN tunnels for both remote site production and remote site management traffic.
Ref;Safe white papers;page 19
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks
Reference: Cisco Courseware page 6-13

QUESTION 139:

How is denial of service attacks mitigated in the SAFE SMR midsize network design corporate Internet module?

A. IDS at the host and network levels.
B. E-mail content filtering, HIDS, and host-based virus scanning.
C. OS and IDS detection
D. CAR at the ISP edge and TCP setup controls at the firewall.
E. RFC 2827 and 1918 filtering at ISP edge and midsize network edge router.
F. filtering at the ISP, edge router, and corporate firewall

Answer: D

Explanation: Threats Mitigated
Denial of service-CAR at ISP edge and TCP setup controls at firewall
Ref: Safe White papers 17
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 140:

How are application layer attacks mitigated in the SAFE SMR midsize network design corporate Internet module?

A. Filtering at the ISP, edge router, and corporate firewall.
B. IDS at the host and network levels.
C. E-mail content filtering, HIDS, and host-based virus scanning.
D. OS and IDS detection.
E. CAR at the ISP edge and TCP setup controls at the firewall.
F. RFC 2827 and 1918 filtering at ISP edge and midsize network edge.

Answer: B

Explanation: Threats mitigated
Application layer attacks-Mitigated through IDS at the host and network levels
REF;Safe white papers;page 18
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 141:

What is the primary function of the firewall in the SAFE SMR midsize network design corporate Internet module?

A. Provide connectivity to the Internet or ISP network.
B. Provide connectivity to the campus module.
C. Provide connectivity to the WAN module.
D. Provide connectivity to the LAN module.
E. Provide the demarcation point between the ISP and the midsize network.
F. Provide connection state enforcement and detailed filtering for sessions initiated through the firewall.

Answer: F

Explanation: The primary function of the firewall is to provide connection-state enforcement and detailed filtering for sessions initiated through the firewall.
REF;Safe white papers;page 19
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 142:

What is the primary function of the inside router in the SAFE SMR midsize network design corporate Internet module?

A. Detect attacks on ports that the firewall is configured to permit.
B. Provide connection state enforcement and detailed filtering for session initiated through the firewall.
C. Provide connectivity to the LAN Module.
D. Provide Layer 3 separation

Answer: D

Explanation: The primary function of the inside router is to provide Layer 3 separation and routing between the corporate Internet module and the campus module.
REF;Safe white papers;page 20
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 143:

Following termination of the VPN tunnel, what action is performed on remote user traffic in the SAFE SMR midsize network design corporate Internet module?

A. Traffic is sent through a Layer 2 switch.
B. Traffic is sent through a Layer 3 switch.

C. Traffic is sent through a firewall.
D. Traffic is sent through a router.

Answer: C

Explanation:
Following termination of the VPN tunnel, traffic is sent through a firewall to ensure that VPN users are appropriately filtered.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 20

QUESTION 144:

Which two are design alternatives in the SAFE SMR midsize network design corporate Internet module? (Choose two)

A. Place a URL filtering server on the public services segment.
B. Eliminate the router between the firewall and the campus module.
C. Set up a small filtering router between the management stations and the rest of the network.
D. Eliminate HIDS.

Answer: A, B

Explanation:
Two other alternatives are available. First is the elimination of the router between the firewall and the campus module. Although its functions can be integrated into the campus module Layer 3 switch, this setup would eliminate the ability of the corporate Internet module to function without relying on Layer 3 services from another area of the network. Second is the addition of content inspection beyond the mail-content inspection already specified. For example, a URL filtering server could be placed on the public services segment to filter the types of Web pages that employees can access.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 21

QUESTION 145:

What is the NIDS primary function in the SAFE SMR midsize network design corporate Internet module?

A. Provide connectivity to the campus module.
B. Provide connectivity to the WAN module.
C. Provide connectivity to the LAN module.
D. Provides detection of attacks on ports that the firewall is configured to permit.
E. Provide the demarcation point between the ISP and the medium network.
F. Provide connection state enforcement and detailed filtering for session initiated

through the firewall.

Answer: D

Explanation:
The public services segment includes a NIDS appliance. Its primary function is to detect attacks on ports that the firewall is configured to permit. These most often are application layer attacks against specific services.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 19

QUESTION 146:

How are virus and Trojan Horse attacks mitigated in the SAFE SMR midsize network design corporate Internet module?

A. Filtering at the ISP, edge router, and corporate firewall.
B. IDS at the host and networks levels.
C. E-mail content filtering, HIDS, and host-based virus scanning.
D. OS and IDS detection.
E. CAR and the ISP edge and TCP setup controls at the firewall.
F. RFC 2827 and 1918 filtering at ISP edge and midsize network edge.

Answer: C

Explanation:
Virus and Trojan horse attacks-Mitigated through e-mail content filtering, HIDS, and host-based virus scanning
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 17

QUESTION 147:

John the security administrator at Certkiller Inc. is working on the securing the network. How is unauthorized access mitigated in the SAFE SMR midsize network design corporate Internet module?

A. Mitigated by CAR at the ISP edge and TCP setup controls at the firewall.
B. Mitigated by filtering at the ISP, edge router, and corporate firewall.
C. Mitigated by IDS at the host and network levels.
D. Mitigated by OS and IDS detection.
E. Mitigated by e-mail content filtering, HIDS, and host-based virus scanning.
F. Mitigated by RFC 2827 and 1918 filtering at ISP edge and midsize network edge.

Answer: B

Explanation:
Unauthorized access-Mitigated through filtering at the ISP, edge router, and corporate firewall
Reference: Safe white papers;page 17
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 148:

You are the administrator at Certkiller Inc. and you are working on securing the network. How are password attacks mitigated in the SAFE SMR midsize network design corporate Internet module?

A. Mitigated by filtering at the ISP, edge router, and corporate firewall.
B. Mitigated by RFC 2827 and 1918 filtering at ISP edge and midsize network edge router.
C. Mitigated by OS and IDS detection.
D. Mitigated by e-mail content filtering, HIDS, and host-based virus scanning-
E. Mitigated by CAR at the ISP edge and TCP setup controls at the firewall.

Answer: C

Explanation:
Password attacks -Limited services avalibale to brute force;OS and IDS can detect the threat
Reference: Safe white papers;page 17
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 149:

You the security administrator at Certkiller Inc are working on design alternatives to the network. Which two are design alternatives in the SAFE SMR midsize network design corporate Internet module? (Choose two)

A. A design alternative is to set up a small filtering router between the management stations and the rest of the network.
B. A design alternative is to eliminate HIDS.
C. A design alternative is to place a URL filtering server on the public services segment.
D. A design alternative is to eliminate the router between the firewall and the campus module.

Answer: C D

Explanation:
Alternatives
This module has several alternative designs. Rather than implementing basic filtering on the edge router to the medium network, a network administrator may choose to

implement a stateful firewall on this device as well. Having two stateful firewalls provides more of a defense in depth approach to security within the module. Depending on the network administrator's attitude toward attack awareness, a NIDS appliance might be required in front of the firewall. With the appropriate basic filters, the IDS outside the firewall can provide important alarm information that would otherwise be dropped by the firewall Because the amount of alarms generated on this segment is probably large, alarms generated here should have a lower severity than alarms generated behind a firewall. Also, consider logging alarms from this segment to a separate management station to ensure that legitimate alarms from other segments get the appropriate attention. With the visibility that NIDS outside the firewall provides, evaluation of the attack types your organization is attracting can be better seen. In addition, evaluation of the effectiveness of ISP and enterprise edge filters can be performed. Two other alternatives are available. First is the elimination of the router between the firewall and the campus module. Although its functions can be integrated into the campus module Layer 3 switch, this setup would eliminate the ability of the corporate Internet module to function without relying on Layer 3 services from another area of the network. Second is the addition of content inspection beyond the mail-content inspection already specified. For example, a URL filtering server could be placed on the public services segment to filter the types of Web pages that employees can access.
Reference:
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 150:

How are IP spoofing attacks mitigated in the SAFE SMR midsize network design corporate Internet module?

A. Filtering at the ISP, edge router, and corporate firewall.
B. IDS as the host and network levels.
C. E-mail content filtering, HIDS, and host-based virus scanning.
D. OS and ISD detection.
E. CAR at the ISP edge and TCP setup controls at the firewall.
F. RFC 2827 and 1918 filtering at ESP edge and midsize network edge router.

Answer: F

Explanation:
At the egress of the ISP router, RFC 1918 and RFC 2827 filtering is configured to mitigate against source-address spoofing of local networks and private address ranges.
Reference: Cisco Courseware pages 6-8, 6-9

QUESTION 151:

How many modules exist in the SAFE SMR midsize network design?

A. 1

B. 2
C. 3
D. 4
E. 5

Answer: C

Explanation: The SAFE medium network design consists of three modules: the corporate Internet module, the campus module, and the WAN module.
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 152:

What are the two options for the remote sites connecting into the SAFE SMR medium design? (Choose two)

A. ATM Connection only.
B. IPSec VPN into the corporate Internet module.
C. ISDN
D. Frame Relay Connection only.
E. Private WAN connection using the WAN module.

Answer: B, E

Explanation: From a WAN perspective, there are two options for the remote sites connecting into the medium design. The first is a private WAN connection using the WAN module;the second is an IPSec VPN into corporate internet module.?
REF;Safe white papers;page 16
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 153:

Which threats are expected in the SAFE SMR midsize network design midsize network campus module? (Choose three)

A. Port redirection
B. Application layer attacks
C. IP spoofing
D. Packet sniffers
E. Virus and Trojan Horse applications
F. Password attacks

Answer: D, E, F

Explanation: At the top of the list of expected threats are:
1. Packet sniffers-A switched infrastructure limits the effectiveness of sniffing

2. Virus and Trojan horse applications-Host-based virus scanning prevents most viruses and many Trojan horses
3. Password Attacks-The access control server allows for strong two-factor authentication for key applications
REF;Safe white papers;22
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 154:

What can mitigate the chance of a department accessing confidential information on another department's server through the use of access control in the SAFE SMR midsize network design midsize network campus module?

A. Layer 2 switch
B. Layer 3 switch
C. General Layer 4 through 7 analysis
D. General Layer 1 through 3 analysis

Answer: B

Explanation:
The Layer 3 switch provides a line of defense and prevention against internally originated attacks. It can mitigate the chance of a department accessing confidential information on another department's server through the use of access control. For example, a network that contains marketing and research and development might segment off the R&D server to a specific VLAN and filter access to it, ensuring that only R&D staff have access to it.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 23

QUESTION 155:

Which are key devices in the SAFE SMR midsize network design midsize network campus module? (Choose three)

A. Firewalls
B. NIDS host
C. Layer 2 switches
D. VPN Concentrator
E. Corporate servers
F. WAN router

Answer: B, C, E

Explanation:
Key Devices

Layer 3 switch-Route and switch production and management traffic within the campus module, provide distribution
layer services to the building switches, and support advanced services such as traffic filtering
Layer 2 switches (with private VLAN support)-Provides Layer 2 services to user workstations
Corporate servers-Provides e-mail (SMTP and POP3) services to internal users, as well as delivering file, print, and DNS
services to workstations
User workstations-Provide data services to authorized users on the network
SNMP management host-Provides SNMP management for devices
NIDS host-Provides alarm aggregation for all NIDS devices in the network
Syslog host(s)-Aggregates log information for firewall and NIDS hosts
Access control server-Delivers authentication services to the network devices
One-time password (OTP) server-Authorizes one-time password information relayed from the access control server
System admin host-Provides configuration, software, and content changes on devices
NIDS appliance-Provides Layer 4-to-Layer 7 monitoring of key network segments in the module
REF;Safe white papers;page 21
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 156:

The security team at Certkiller Inc is working on securing the network using select key devices. What are key devices in SAFE SMR midsize network design midsize network campus module? (Choose three)

A. A key device is a NIDS host
B. A key device is a VPN Concentrator
C. A key device is a Firewall
D. A key device is a Syslog host
E. A key device is a WAN router
F. A key device is a Layer 3 switch

Answer: A D F

Explanation:
Campus Network:
Key Devices
1. Layer 3 switch-Route and switch production and management traffic within the campus module, provide distribution layer services to the building switches, and support advanced services such as traffic filtering
2. Layer 2 switches (with private VLAN support)-Provides Layer 2 services to user workstations
3. Corporate servers-Provides e-mail (SMTP and POP3) services to internal users, as

well as delivering file, print, and DNS services to workstations
4. User workstations-Provide data services to authorized users on the network
5. SNMP management host-Provides SNMP management for devices
6. NIDS host-Provides alarm aggregation for all NIDS devices in the network
7. Sysloghost(s)-Aggregates log information for firewall and NIDS hosts
8. Access control server-Delivers authentication services to the network devices
9. One-time Password (OTP) Server-Authorizes one-time password information relayed from the access control server
10. System admin host-Provides configuration, software, and content changes on devices
11. NIDS appliance
-Provides Layer 4-to-Layer 7 monitoring of key network segments in the module
Reference: Safe white papers;page 21
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 157:

The security team at Certkiller Inc is working on securing the network using select key devices. Which are the key devices in SAFE SMR midsize network design midsize network campus module? (Choose three)

A. A key device are Firewalls
B. A key device are VPN Concentrator
C. A key device are WAN router
D. A key device are Syslog hosts
E. A key device are Corporate servers
F. A key device are Layer 3 switches

Answer: D E F
Campus Network:
Key Devices
1. Layer 3 switch-Route and switch production and management traffic within the campus module, provide distribution layer services to the building switches, and support advanced services such as traffic filtering
2. Layer 2 switches (with private VLAN support)-Provides Layer 2 services to user workstations
3. Corporate servers-Provides e-mail (SMTP and POP3) services to internal users, as well as delivering file, print, and DNS services to workstations
4. User workstations-Provide data services to authorized users on the network
5. SNMP management host-Provides SNMP management for devices
6. NIDS host-Provides alarm aggregation for all NIDS devices in the network
7. Sysloghost(s)-Aggregates log information for firewall and NIDS hosts
8. Access control server-Delivers authentication services to the network devices
9. One-time Password (OTP) Server-Authorizes one-time password information relayed from the access control server
10. System admin host-Provides configuration, software, and content changes on

devices
11. NIDS appliance-Provides Layer 4-to-Layer 7 monitoring of key network segments in the module
Reference: Safe white papers;page 21
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 158:

The security team at Certkiller Inc is working on securing the network using select key devices. Which are key devices in the SAFE SMR midsize network design midsize network campus module? (Choose three)

A. A key device are WAN router
B. A key device are VPN Concentrator
C. A key device are Firewalls
D. A key device are NIDS hosts
E. A key device are Corporate servers
F. A key device are Layer 2 switches

Answer: D E F
Campus Network:
Key Devices
1. Layer 3 switch-Route and switch production and management traffic within the campus module, provide distribution layer services to the building switches, and support advanced services such as traffic filtering
2. Layer 2 switches (with private VLAN support)-Provides Layer 2 services to user workstations
3. Corporate servers-Provides e-mail (SMTP and POP3) services to internal users, as well as delivering file, print, and DNS services to workstations
4. User workstations-Provide data services to authorized users on the network
5. SNMP management host-Provides SNMP management for devices
6. NIDS host-Provides alarm aggregation for all NIDS devices in the network
7. Sysloghost(s)-Aggregates log information for firewall and NIDS hosts
8. Access control server-Delivers authentication services to the network devices
9. One-time Password (OTP) Server-Authorizes one-time password information relayed from the access control server
10. System admin host-Provides configuration, software, and content changes on devices
11. NIDS appliance-Provides Layer 4-to-Layer 7 monitoring of key network segments in the module
Reference: Safe white papers;page 21
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 159:

The security team at Certkiller Inc is working on alternative designs aspects for the

network.
Which design alternative in the SAFE SMR midsize network design campus module?

A. An alternative design is a separate router and Layer 2 switch can be used for the core and distribution rather than the higher-performing Layer 3 switch.
B. An alternative design is a NIDS appliance can be placed in front of the firewall.
C. An alternative design is a URL filtering server can be placed on the public services segment to filter the types of Web pages employees can access.
D. An alternative design is a router between the firewall and the campus module can be eliminated.

Answer: A

Explanation:
Alternatives
If the medium network is small enough, the functionality of the building switches can be rolled into the core switch, and the building switches can be eliminated. In this case, the end-user workstations would be connected directly to the core switch. Private VLAN functionality would be implemented on the core switch in order to mitigate against trust-exploitation attacks. If the performance requirements of the internal network are not high, a separate router and Layer 2 switch could be used for the core and distribution instead of the higher-performing Layer 3 switch. If desired, the separate NIDS appliance can be replaced with an integrated IDS module that fits into the core switch. This setup provides higher traffic throughput into the IDS module because it sits on the backplane of the switch, rather than being connected via a single 10/100-Mbps Ethernet port. ACLs on the switch can be used to control what traffic is sent to the IDS module.
Reference: Safe white papers;page 23
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 160:

The structure of Campus module in SAFE medium architecture may be altered. Choose the correct statement.

A. Both alternatives are allowed.
B. The functions of the layer 2 switch, can be integrated into the core switch.
C. If the performance requirements are not too high, the core switch can be replaced by a layer 2 switch and a router.
D. None of these alternatives are allowed.

Answer: A

Explanation: If the medium network is small enough, the functionality of the building switches can be rolled into the core switch, and the building switches can be eliminated. If the performance requirements of the internal network are not high, a separate router and Layer 2 switch could be used for the core and distribution

instead of the higher-performing Layer 3 switch.
Reference: Safe white papers;page 23
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 161:

What does RFC 2827 filtering prevent in the SAFE SMR midsize network design campus module?

A. Port redirection attacks.
B. Port mapping through the firewall.
C. Source-address spoofing.
D. Packet sniffers.

Answer: C

Explanation:
RFC 2827 filtering at the ingress router should also be implemented to mitigate the chance of an attacker from outside the network spoofing the addresses of the management hosts.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 71

QUESTION 162:

What is a design alternative in the SAFE SMR midsize network design campus module?

A. A NIDS appliance can be placed in front of the firewall.
B. The end-user workstations can be connected directly to the core switch.
C. The router between the firewall and the campus module can be eliminated.
D. A URL filtering can be placed on the public services segment to filter the types of Web pages employees can access.

Answer: B

Explanation:
If the medium network is small enough, the functionality of the building switches can be rolled into the core switch, and the building switches can be eliminated. In this case, the end-user workstations would be connected directly to the core switch. Private VLAN functionality would be implemented on the core switch in order to mitigate against trust-exploitation attacks. If the performance requirements of the internal network are not high, a separate router and Layer 2 switch could be used for the core and distribution instead of the higher-performing Layer 3 switch. If desired, the separate NIDS appliance can be replaced with an integrated IDS module that fits into the core switch. This setup provides higher traffic throughput into the IDS module because it sits on the backplane of

the switch, rather than being connected via a single 10/100-Mbps Ethernet port. ACLs on the switch can be used to control what traffic is sent to the IDS module.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 23

QUESTION 163:

NO: 1
Which options can be chosen for TCP session reassembly on the IDS Sensor in the SAFE SMR medium network design? (Choose two)

A. IP Reassembly
B. No reassembly
C. Loose reassembly
D. Total reassembly

Answer: B, C

Explanation:
You can choose three options for TCP session reassembly.
* No Reassembly
* Loose Reassembly
* Strict Reassembly
Reference: Cisco Secure Intrusion Detection System (Ciscopress) Page 418

QUESTION 164:

What are the two options in the SAFE SMR midsize network design for WAN connections? (Choose two)

A. IPSec VPN tunnel connections.
B. Only frame relay connections.
C. Private WAN connections.
D. ATM connections.

Answer: A, C

Explanation:
From a WAN perspective, there are two options for the remote sites connecting into the midium design .The first is a private WAN connection using the WAn module; the second is an IPSec VPN into the corporate Internet module.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 16

QUESTION 165:

What is the difference in implementation between the edge router and the ISP router in the SAFE SMR medium network design?

A. The ISP router is configured for rate limiting.
B. The edge router is configured for rate limiting.
C. The ISP router is configured for more aggressive rate limiting.
D. The edge router is configured for more aggressive rate limiting.

Answer: A

Explanation: The primary function of the customer-edge router in the ISP is to provide connectivity to the Internet or ISP network. The egress out of the ISP router rate limits nonessential traffic that exceeds prespecified thresholds in order to mitigates against DDoS attacks.
REF;Safe white papers;page 18
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 166:

Why are all providers of Internet connectivity urged to implement the filtering described in RFC 2827?

A. To prohibit attackers from using source addresses that reside within a range of legitimately advertised prefixes.
B. To prohibit attackers from using forged source addresses that do not reside within a range of legitimately advertised prefixes.
C. To filter Java applications that come from a source that is not trusted.
D. To stop internal users from reaching web sites that violate the established security policy.

Answer: A

Explanation:
RFC 2827 filtering-You can also prevent users of a network from spoofing other networks (and be a good Internet citizen at the same time) by preventing any outbound traffic on your network that does not have a source address in your organization's own IP range. Your Internet service provider (ISP) can also implement this type of filtering, which is collectively referred to as RFC 2827 filtering. This filtering denies any traffic that does not have the source address that was expected on a particular interface. For example, if an ISP is providing a connection to the IP address 15.1.1.0/24, the ISP could filter traffic so that only traffic sourced from address 15.1.1.0/24 can enter the ISP router from that interface.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 66

QUESTION 167:

Jason the security administrator at Certkiller Inc. is working on filtering network traffic.
In the SAFE SMR midsize network design, access list 101 deny ip 10.0.0.0.0 255.255.255 any is an example of what kind of filtering?

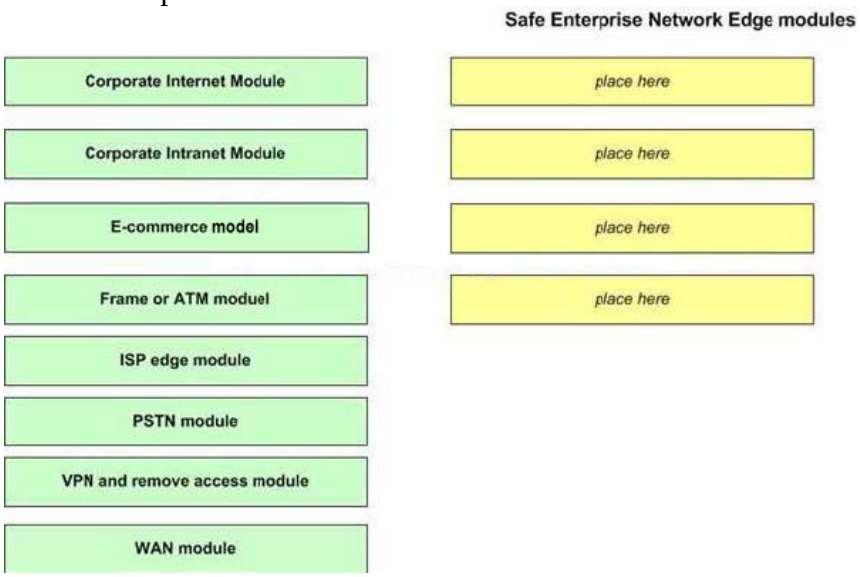
A. It is an example of RFC 2728
B. It is an example of RFC 2827
C. It is an example of RFC 1918
D. It is an example of RFC 1920

Answer: C

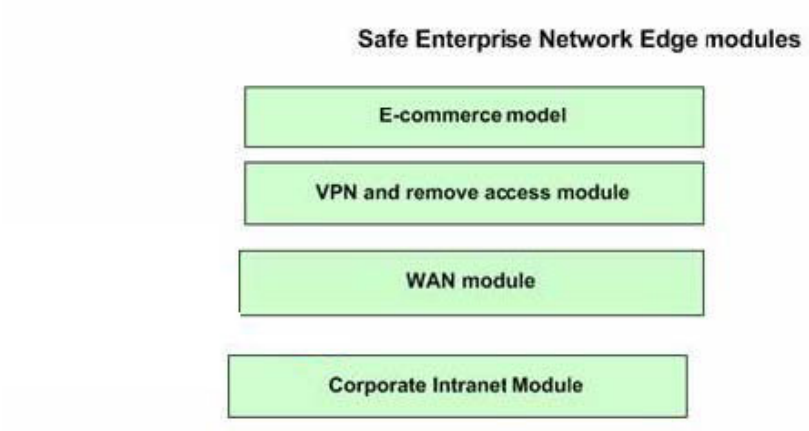
Explanation:
! RFC 1918 filtering. Note network 172.16.x.x was not included in the
! filter here since it is used to simulate the ISP in the lab.
!
access-list 103 deny ip 10.0.0.0 0.255.255.255 any
access-list 103 deny ip 192.168.0.0 0.0.255.255 any
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 47

QUESTION 168:

From the modules listed, select the four that could be part of the SAFE enterprise Network edge. Place them under SAFE Enterprise Network Edge modules. You will not use all options.



Answer:



Reference: Cisco Courseware page 8-3

QUESTION 169:

Based on SAFE Model of Medium Networks, with site-to-site VPNs, the corporate Internet edge router should permit only IKE and IPSec traffic to reach the VPN concentrator or firewall based on:

A. The standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500).
B. Both the IP address of the remote site and the IP address of the headend peer.
C. The IP address of the headend peer only.
D. The IP address of the remote site only.

Answer: B

Explanation: With site-to-site VPNs, the IP address of the remote site is usually Know ;therefor,filtering may bespecified for VPN traffic to from both peers.
REF; Safe white papers;page 19
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 170:

How many transform sets can be included in a crypto map on a PIX Firewall?

A. 1
B. 2
C. 3
D. 4
E. Unlimited number
F. 6

Answer: F
Reference: CiscoPIX Courseware page 14-44

QUESTION 171:

What is the maximum number of transform sets you can specify on a PIX Firewall?

A. As much as the RAM can take.
B. 3 only
C. 1 only
D. Unlimited number
E. 2 only
F. 4 only

Answer: D
Reference: Cisco CSI Courseware page 7-35
Reference: CiscoPIX Courseware page 7-35
Reference: CiscoPIX Courseware page 14-41
Reference: CiscoPIX Courseware page 14-44
...there is no limit of transform sets, BUT ONLY
- up 3 transforms (1 AH, 2 ESPs) can be combined to a set,
- up to 6 sets can be used in a crypto-map

QUESTION 172:

Jason the security administrator at Certkiller Inc is working on installing IDS in the network. Which signature actions can be selected on the IDS Sensor in the SAFE SMR medium network design? (Choose two)

A. Jason can select Block
B. Jason can select TCP reset
C. Jason can select UDP reassembly
D. Jason can select Total reassembly

Answer: A B

Explanation:
The NIDS appliance between the private interface of the firewall and the internal router provides a final analysis of attacks. Very few attacks should be detected on this segment because only responses to initiated requests, a few select ports from the public services segment, and traffic from the remote access segment are allowed to the inside. Only sophisticated attacks should be seen on this segment because they could mean that a system on the public services segment has been compromised and the hacker is attempting to take advantage of this foothold to attack the internal network. For example, if the public SMTP server were compromised, a hacker might try to attack the internal mail server over TCP port 25, which is permitted to allow mail transfer between the two hosts. If attacks are seen on this segment, the responses to those attacks should be more severe than those on other segments because they probably indicate that a compromise has already occurred. The use of TCP resets or shunning to thwart, for example, the

SMTP attack mentioned above, should be seriously considered.
Reference:Safe white papers;page 19
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 173:

How many attacks should the NIDS appliance detect in the SAFE SMR midsize network design midsize network campus module?

A. Very few.
B. A moderate amount, depending on access through the Internet module.
C. A large amount, due to outside placement of the Internet firewall.
D. A large amount, due to outside placement of the edge router.

Answer: A

Explanation: Very few attacks should be detected here because this NIDS appliance provides analysis against attacks that may originate from within the campus module itself.
REF;Safe white papers;23
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 174:

What signature actions can be configured on an IDS Sensor in the SAFE SMR medium network design? (Choose two)

A. UDP reassembly
B. None
C. IP log
D. Total reassembly

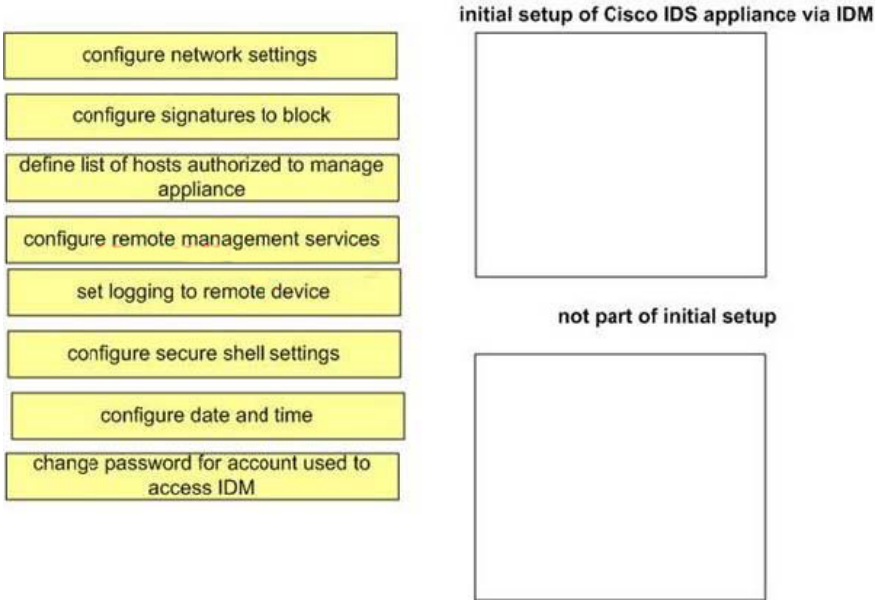
Answer: B, C

Explanation:
Cisco IDS signatures can take one or all of the following actions when triggered:
1) TCP reset - Terminates the TCP session between the source of an attack and the target host
2) IP log - Logs subsequent IP packets from the source of an attack
3) Block - Initiates the blocking of IP traffic from the source of an attack, either a block on the host or the connection.
Reference: Cisco Courseware p.6-35

QUESTION 175:

DRAG DROP

You are the administrator at Certkiller Inc and your assignment is to choose the tasks required for initial setup of the Cisco appliance via IDM.



Answer:

Explanation:
Initial setup of Cisco IDS appliance via IDM.
1. Configure network settings
2. Define list of hosts authorized to manage appliance
3. Configure date and time
4. Change password to account used to access IDM
Not part of Initial Setup
1. Configure signatures to block.
2. Configure remote management services
3. Set logging to remote device
4. Configure secure shell settings
Reference: Cisco Intrusion Detection System - IDS Device Manager Sensor Setup

---

QUESTION 176:

Which of the following is true about CSA?

A. CSA is a signature-based intrusion prevention system and creates significantly fewer true positives than NIDS.
B. CSA is a behavior-based intrusion prevention system and creates significantly fewer false positives than NIDS.
C. CSA is a signature-based intrusion prevention system and creates significantly fewer true negatives than NIDS.
D. CSA is a behavior-based intrusion prevention system and creates significantly fewer false negatives than NIDS.

Answer: B
Reference: Cisco Courseware page 4-33

QUESTION 177:

What is the primary function of the VPN Concentrator in the SAFE SMR midsize network design corporate Internet module?

A. Provide connection state enforcement and detailed filtering for sessions initiated through the firewall.
B. Provide secure connectivity to the LAN Module.
C. Provide secure connectivity to the midsize network for remote users.
D. Provide secure connectivity to the campus module.
E. Provide secure connectivity to the Internet or ISP network.

Answer: C

Explanation: The primary function of the remote access VPN concentrator is to provide secure connectivity to the medium network for remote users.
REF;Safe white papers;20
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 178:

Johnny the security administrator at Certkiller Inc. is working on connecting remote users to the network. How many options exist for remote user connectivity in the SAFE SMR remote user network?

A. 5
B. 4
C. 3
D. 2
E. 1

Answer: B

Explanation:
Remote-User Design
This section discusses four different options for providing remote-user connectivity within the SAFE design. Remote connectivity applies to both mobile workers and home-office workers. The primary focus of these designs is providing connectivity from the remote site to the corporate headquarters and through some means, the Internet. The following four options include software-only, software-with-hardware, and hardware-only solutions:
1. Software access-Remote user with a software VPN client and personal firewall

software on the PC
2. Remote-site firewall option-Remote site is protected with a dedicated firewall that Provides firewalling and IPSec VPN connecttinity to corporate headquarters;WAN connectivity is provided via an ISP-provided broadband access device (i.e. DSL or cable modem).
3. Hardware VPN client option-Remote site using a dedicated hardware VPN client that Provides IPSec VPN connecttinity to corporate headquarters;WAN connecttinity is provided via an ISP-provided broadband access device
4. Remote-site router option-Remote site using a router that provides both firewalling and IPSec VPN connectivity to corporate headquarters. This router can either provide direct broadband access or go through and ISP-provided broadband access device.
REF;Safe white papers;page 25
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 179:

Which are key devices in the SAFE SMR remote user network? (Choose two)

A. Firewall with VPN support
B. Layer 2 switch
C. Broadband access device
D. NIDS
E. Layer 3 switch

Answer: A, C

Explanation: Key Devices
Broadband acess device
Firewall with VPN support
* Personal firewall software
REF;Safe white papers;page 25
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 180:

Which are key devices in the SAFE SMR remote user network? (Choose three)

A. Layer 2 switch
B. Router with firewall and VPN support
C. Layer 3 switch
D. Firewall with VPN support
E. NIDS
F. Personal firewall software

Answer: B, D, F

Explanation:
Firewall with VPN support-provides secure end encrypted tunnels between the remote site and the corporate headend; provides network-level protection of remote-site resources and stateful filtering of traffic
Presonal firewall software-provides-level protection for individual PCs
Router firewall and VPN support-Provides secure end-to-end encrypted tunnels between the remote site and the corporate headand ;provides network-level protection of remote-site resources snd statefull filtring of traffic;can provides advanced services such as voice or QoS.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 25

QUESTION 181:

In the SAFE SMR, if the remote users who do not want to establish VPN tunnel when connected to the Internet, they should use _____ to mitigate against unauthorized access.

A. IPSec with IKE
B. Personal Firewall
C. Cisco PIX Firewall
D. Firewall provided through the corporate connection.

Answer: B

Explanation: Because the remote user may not always want the VPN tunnel established when connected to the Internet or ISP network, personal firewall software is recommended to mitigate against unauthorized access to the PC.
REF;Safe white papers;page 28
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 182:

Which threats are expected in the SAFE SMR remote user network environment? (Choose two)

A. Trust exploitation
B. Port redirection attacks
C. Man in the middle attacks
D. Network reconnaissance

Answer: C, D

Explanation:
Network reconnaissance-Protocols filtered at remote-site device to limit effectiveness
Man-in-the-middle attacks-Mitigated through encrypted remote traffic

REF;Safe white papers;page 26
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 183:

Out of curiosity, an internal user double clicks his Network Neighborhood and finds a Human Resourced file that is left accessible to everyone.
What type of attack is this?

A. Unauthorized escalation
B. Reconnaissance
C. This is not an attack.
This is classified as HUA (Harmless Unintended Access)
D. Access

Answer: D

Explanation:
Access attacks - an intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges.
Reference: Cisco CSI Student Gude v2.0 p.2-15

QUESTION 184:

The security team at Certkiller Inc. is working on mitigating attacks on the network.
Which are attack mitigation roles for the software access option in the SAFE SMR remote user network environment? (Select two.)

A. Mitigating attacks by using host DoS mitigation
B. Mitigating attacks by using terminate IPSec
C. Mitigating attacks by using stateful packet filtering
D. Mitigating attacks by using basic Layer 7 filtering
E. Mitigating attacks by using authenticate remote site

Answer: B E

Explanation:
The following are the specific attack mitigation roles for the software access option:
1)Authenticate remote site - Properly identify and verify a user or service
2) Terminate IPSec - Successfully establish an IPSec tunnel between the remote site and host site
3) Personal firewall and virus scanning for local attack mitigation - Allay the risk of virus infection at remote site
Reference: Cisco SAFE Implementation Courseware version 1.1 Page 7-10
Note:
The software access option is geared toward the mobile worker as well as the

home-office worker. All the remote user requires is a PC with VPN client software and connectivity to the Internet or ISP network via a dial-in or Ethernet connection.
The primary function of the VPN software client is to establish a secure, encrypted tunnel from the client device to a VPN headend device. Access and authorization to the network are controlled from the headquarters location when filtering takes place on the firewall and on the client itself if access rights are pushed down via policy. The remote user is first authenticated, and then receives IP parameters such as a virtual IP address, which is used for all VPN traffic, and the location of name servers (DNS and Windows Internet Name Service [WINS]). Split tunneling can also be enabled or disabled via the central site. For the SAFE design, split tunneling was disabled, making it necessary for all remote users to access the Internet via the corporate connection when they have a VPN tunnel established. Because the remote user may not always want the VPN tunnel established when connected to the Internet or ISP network, personal firewall software is recommended to mitigate against unauthorized access to the PC. Virus-scanning software is also recommended to mitigate against viruses and Trojan horse programs infecting the PC.
REF;Safe white papers;page 27&28
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 185:

You are the administrator at Certkiller Inc. and you need to install personal firewalls to select remote users. When is personal firewall software recommended in the software access option in the SAFE SMR remote user design environment?

A. It is recommended when the VPN tunnel is established.
B. It is recommended when the ISP does not provide firewall protection.
C. It is recommended when the VPN tunnel is not established.
D. It is recommended when firewall protection is provided via the corporate connection.

Answer: C

Explanation: Because the remote user may not always want the VPN tunnel established when connected to the Internet or ISP network, personal firewall software is recommended to mitigate against unauthorized access to the PC.
Reference: Safe White papers 28
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 186:

Which are attack mitigation roles for the software access option in the SAFE SMR remote user network environment? (Choose two)

A. Basic Layer 7 filtering
B. Authenticate remote site
C. Host DoS mitigation

D. Terminate IPSec
E. Stateful packet filtering

Answer: B, D

Explanation:
The following are the specific attack mitigation roles for the software access option:
1) Authenticate remote site - Properly identify and verify a user or service
2) Terminate IPSec - Successfully establish an IPSec tunnel between the remote site and host site
3) Personal firewall and virus scanning for local attack mitigation - Allay the risk of virus infection at the remote site.
Reference: Cisco SAFE Implementation 1.1 Courseware Page 7-10 under Software Access Option
Note: The software access option is geared toward the mobile worker as well as the home-office worker. All the remote user requires is a PC with VPN client software and connectivity to the Internet or ISP network via a dial-in or Ethernet connection.
The primary function of the VPN software client is to establish a secure, encrypted tunnel from the client device to a VPN headend device. Access and authorization to the network are controlled from the headquarters location when filtering takes place on the firewall and on the client itself if access rights are pushed down via policy. The remote user is first authenticated, and then receives IP parameters such as a virtual IP address, which is used for all VPN traffic, and the location of name servers (DNS and Windows Internet Name Service [WINS]). Split tunneling can also be enabled or disabled via the central site. For the SAFE design, split tunneling was disabled, making it necessary for all remote users to access the Internet via the corporate connection when they have a VPN tunnel established. Because the remote user may not always want the VPN tunnel established when connected to the Internet or ISP network, personal firewall software is recommended to mitigate against unauthorized access to the PC. Virus-scanning software is also recommended to mitigate against viruses and Trojan horse programs infecting the PC.
REF;Safe white papers;page 27&28
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 187:

Cisco SAFE Small, Midsize, and Remote-User Networks (SMR) recommends a personal firewall software in the software access option if?

A. He is not using a strong password on his PC.
B. The user established a VPN tunnel.
C. The used DSL service.
D. The user does not establish a VPN tunnel.

Answer: D

Explanation: Because the remote user may not always want the VPN tunnel established when connected to the Internet or ISP network, personal firewall software is recommended to mitigate against unauthorized access to the PC.
.REF;Safe white papers;28
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 188:

When is personal firewall software recommended in the software access option in the SAFE SMR remote user design environment?

A. When the VPN tunnel is established.
B. When the VPN tunnel is not established.
C. When the ISP does not provide firewall protection.
D. When firewall protection is provided via the corporate connection.

Answer: B

Explanation: Because the remote user may not always want the VPN tunnel established when connected to the Internet or ISP network, personal firewall software is recommended to mitigate against unauthorized access to the PC.
Ref: Safe White papers 28
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 189:

If split tunneling is disabled, how do remote users access the Internet when they have a VPN tunnel established in the software access option in the SAFE SMR remote user design environment?

A. Access to the Internet is not allowed.
B. The user must disable the VPN tunnel to access the Internet.
C. Access to the Internet is provided via the corporate connection.
D. Access to the Internet is provided via the ISP connection.

Answer: C

Explanation:
Split tunneling can also be enabled or disabled via the central site. For the SAFE design, split tunneling was disabled, making it necessary for all remote users to access the Internet via the corporate connection when they have a VPN tunnel established.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 28

QUESTION 190:

The security team at Certkiller Inc. is working on mitigating attacks to the network, Which threats are expected in the SAFE SMR remote user network environment? (Choose two)

A. The expected threats are man-in-the-middle attacks
B. The expected threats are Network reconnaissance
C. The expected threats are Trust exploitation
D. The expected threats are Port redirection attacks

Answer: A B

Explanation:
Network reconnaissance-Protocols filtered at remote-site device to limit effectiveness
Man-in-the-middle attacks-Mitigated through encrypted remote traffic
REF;Safe white papers;page 26
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 191:

James the security administrator at Certkiller Inc. is working on establishing VPNs. IF tunneling is disabled, how do remote users access the Internet when they have a VPN tunnel established in the software access option in the SAFE SMR remote user design environment?

A. The remote users access to the Internet is not allowed.
B. The remote access to the Internet is provided via the corporate connection.
C. The remote user must disable the VPN tunnel to access the Internet.
D. The remote access to the Internet is provided via the ISP connection.

Answer: B

Explanation:
Split tunneling can also be enabled or disabled via the central site. For the SAFE design, split tunneling was disabled, making it necessary for all remote users to access the Internet via the corporate connection when they have a VPN tunnel established.
Reference: Page 28
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 192:

The IPSec receiver (the one who receives the IPSec packets) can detect and reject replayed packets.

A. True
B. False

Answer: A
Ref:
Cisco SIP Proxy Server - Maintaining the Cisco SIP Proxy Server

---

QUESTION 193:

What IKE proposal should be chosen on the VPN Concentrator for the Unity Client?

A. Any proposal that ends with DH7.
B. Any IKE proposal, except the IKE proposal that ends with DH7.
C. Any proposal that starts with Cisco VPN Client.
D. Any proposal that starts with DH7.

Answer: C

Explanation:
The CiscoEasy VPN Client feature eliminates much of this tedious work by implementing Cisco's Unity Client protocol, which allows most VPN parameters to be defined at a VPN 3000 series concentrator acting as an IPSec server.
Reference: Cisco Easy VPN Client for the Cisco 1700 Series Routers

---

QUESTION 194:

You are the administrator at Certkiller Inc. and you are implementing QoS. If you want QoS at the remote site, which option should be selected?

A. You should select software access option
B. You should select remote site router option
C. You should select hardware VPN Client option
D. You should select remote site firewall option

Answer: B

Explanation:
Remote-Site Router Option
The remote-site router option is nearly identical to the remote-site firewall option with a few exceptions. When deployed behind a stand-alone broadband access device, the only difference is the router can support advanced applications such as QoS, routing, and more encapulation options. Additionaly, if the broadband capability is integrated into the router, a stand-alone broadband access device is not needed. This option requires that your ISP allow you to manage the broadband router itself, an uncommon scenario.
Reference: Page 29
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 195:

James the security administrator at Certkiller Inc. is working on the crypto map function on the PIX Firewall. What is the function of a crypto map on a PIX Firewall?

A. The function of a crypto map is to specify which algorithms will be used with the selected security protocol.
B. The function of a crypto map is to define the policy that will be applied to the traffic.
C. The function of a crypto map is to configure a pre-shared authentication key and associate the key with an IPSec peer address or host name.
D. The function of a crypto map is to map transforms to transform sets.

Answer: B

Explanation: Crypto map entries for IPSec set up security association parameters,
Tying together the various parts configured for IPSec,including the following;
* The granularity of the traffic to be protected by a set of security associations
Reference: Cisco Secure PIX Firewalls (Ciscopress) Page 215

QUESTION 196:

Kathy the security administrator at Certkiller Inc. is now working on the crypto map function on the PIX Firewall. What is another function of a crypto map on a PIX Firewall?

A. The function of a crypto map is to configure a pre-shared authentication key and associate the key with an IKE peer address or host name.
B. The function of a crypto map is to configure a pre-shared authentication key and associate the key with an IPSec peer address or host name.
C. The function of a crypto map is to filter and classify the traffic to be protected.
D. The function of a crypto map is to specify which algorithms to use with the selected security protocol.

Answer: C

Explanation: Crypto map entries for IPSec set up security association parameters,
Tying together the various parts configured for IPSec,including the following;
* Which traffic should be protected by IPSec
Reference: Cisco Secure PIX Firewalls (Ciscopress) Page 215

QUESTION 197:

Which is true about the PIX Firewall in the remote site firewall option in the SAFE SMR remote user design environment?

A. ISAKMP is enabled when the ISAKMP policy is created.

B. ISAKMP is enabled when the crypto map is applied to the interface.
C. ISAKMP is disabled by default.
D. ISAKMP is enabled by default.

Answer: D

Explanation: IKE is enabled by default.
Ref: Cisco Secure PIX Firewalls (Ciscopress) Page 202

QUESTION 198:

The remote site router option is nearly identical to which option?

A. Software access option
B. Remote site firewall option
C. Hardware VPN Client option
D. Dial-up access option

Answer: B

Explanation: The remote-site router option is nearly identical to the remote-site firewall option with a few exceptions.
REF;Safe white papers;page 29
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 199:

IPSec tunnel mode can only be used when the datagrams are:

A. Sourced from and destined to IPSec systems.
B. Sourced from and destined to non-IPSec systems.

Answer: B

Explanation: Tunnel Mode is used to protect datagrams sourced from or destined to non-IPSec systems (such as in a Virtual Private Network (VPN) scenario).

QUESTION 200:

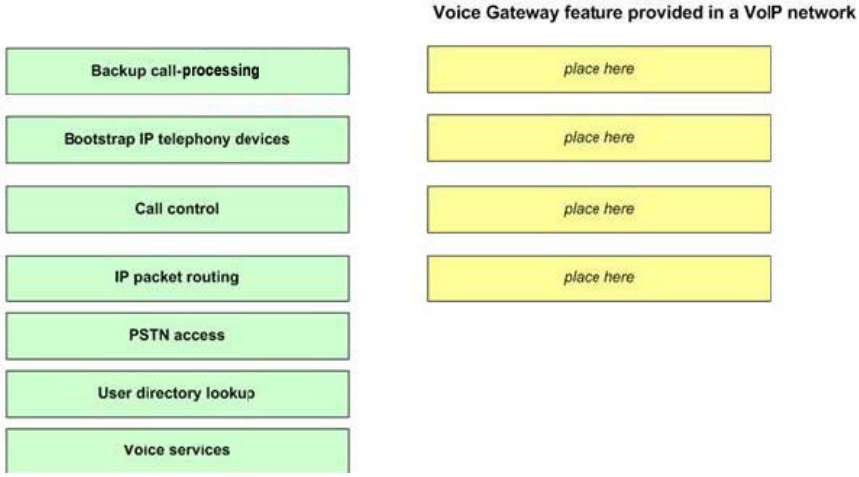
What protocol is used in call setup to allow the IP telephony conversation to commence?

A. MGCP
B. RTP
C. SIP
D. H.323

Answer: B
Reference: Cisco Courseware page 9-5
"...channel uses the RTP to allow the conversation to commence..."

QUESTION 201:

You work as an instructor at Certkiller .com. From the feature list, select the four Voice Gateway features that are provided in a VoIP network. Place them under the Voice Gateway feature. You will not use all options.



Answer:

Explanation: Backup call-processing, IP packet routing, PSTN access, Voice services.
Voice gateway - A general term used to refer to any gateway that provides voice services, including such features as Public Switched Telephone Network (PSTN) access, IP packet routing, backup call-processing, and voice services. This is the device that provides access to legacy voice systems for local calls, toll bypass, and WAN backup in case of failure. Backup call processing allows for the voice gateway to take over call processing in case the primary call processing manager goes offline for any reason. Typically the voice gateway supports a subset of the call-processing functionality supported by the call-processing manager.
Reference: Cisco Courseware p. 9-4

QUESTION 202:

What port numbers are generally used by calls placed between IP telephony devices?

A. TCP port numbers greater than 5060
B. UDP port numbers between 2427 and 2600
C. TCP port numbers between 1720 and 1790
D. UDP port numbers greater than 16384

Answer: D

Explanation:
Calls placed between IP telephony devices generally use dynamically assigned UDP port numbers greater than 16384
Reference: Cisco Courseware page 9-76

QUESTION 203:

What is the primary method for device authentication in a VoIP network?

A. IP address
B. MAC address
C. SIP address
D. IP and MAC address

Answer: B

Explanation:
The primary method for the device authentication of IP phones is the MAC address. If a phone with an unknown MAC address attempts to download a network configuration from the call-processing manager and it has no knowledge of the IP phone's MAC address, then that IP phone will not receive a configuration assuming automatic registration has been disabled.
Reference: Cisco Courseware p.9-24

QUESTION 204:

Which are key devices in the SAFE VoIP large network campus server module? (Choose three)

A. Layer 2 switch
B. Call-processing manager
C. NIDS appliance
D. Proxy server
E. IP phones
F. Stateful firewall

Answer: B, D, F

Explanation:
The following are the key IP telephony devices in the large network campus server module:
1) Layer 3 switch
2) Corporate servers

3) Call-processing manager
4) Stateful firewall
5) Proxy Server
Reference: Cisco Courseware page 9-70

QUESTION 205:

What are the radio frequency bands used by IEEE 802.11 standards? (Choose two.)

A. 2.8 MHz
B. 2.4 GHz
C. 2.2 MHz
D. 5 GHz
E. 900 GHz
F. 900 MHz

Answer: B, D

Explanation:
Standard 802.11 - based wireless technologies take advantage of the radio spectrum deemed usable by the public. This spectrum is known as the Industrial, Scientific, and Medical (ISM) band. The 802.11 standard specifically takes advantage of two of the three frequency bands, the 2.4 GHz -to-2.4835 GHz UHF band used for 802.11b and 802.11g networks, and the 5.15 GHz-to-5.825 GHz SHF band used for 802.11a-based networks.
Reference: Cisco Courseware p.10-6

QUESTION 206:

Network topology exhibit:

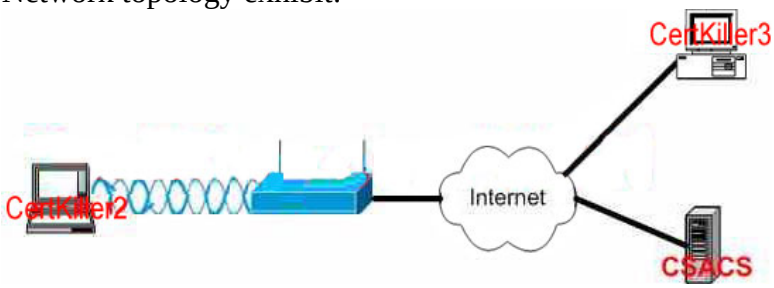
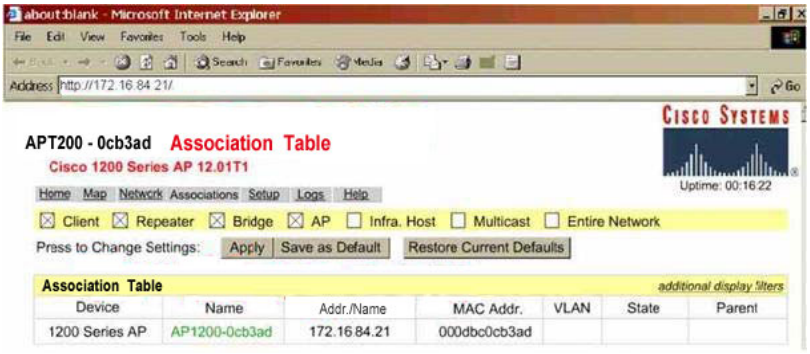


Exhibit #2:



Certkiller .com has moved a wireless access point from Kiev to Minsk. You are required to configure the access point with the necessary parameters for access at the new location in Minsk. To gain entry to the access you point you should launch the browser by clicking on Certkiller 3 workstation and enter the appropriate IP address. After configuration of the access point has been completed the authentication can be verified by closing the browser and launching the LEAP from the laptop. Use the following parameters to accomplish these objectives. All other parameters on the access point were pre-configured in Kiev and do no need to be changed.
1200 Wireless access point 172.16.84.21 255.255.255.0
Wireless Client adapter 172.16.84.15 255.255.255.0
CSACS 172.16.84.50 255.255.255.0
Server name/IP: 172.16.84.50
Server type: RADIUSPORT: 1645
Shared Secret: Certkiller yessecret
Authentication Type: EAPWEP Key
Size: 128 bit
Wep Key: 9876543210 Certkiller 0123456789
Encryption: Full

Answer:

Explanation: Pending. Send your suggestion to feedback@ Certkiller .com
Note: Hint for candidates taking the test on german keyboards: Typing the password only shows **** asterixes.
The password contains a "y", to get it on the german keyboard, you have to enter a "z", otherwhise the password is incorrect, and the "test connection" button fails.
Alternative #1:
1200 Wireless access point 172.16.82.21 255.255.255.0
Wireless Client adapter 172.16.82.15 255.255.255.0
CSACS 172.16.82.50 255.255.255.0
Server name/IP: 172.16.82.50

QUESTION 207:

What services does EAP provide?

A. EAP provides wireless gateway and complementary code keying.
B. EAP provides centralized authentication and dynamic key distribution.
C. EAP provides open authentication and shared key distribution.
D. EAP provides message integrity check and wireless domain service.

Answer: B

Explanation:
EAP is an alternative WLAN security approach focusing on developing a framework for providing centralized authentication and dynamic key distribution. This approach is based on the IEEE 802.11i end-to-end framework using 802.1x and EAP to provide this enhanced functionality. Cisco has incorporated 802.1x and EAP into its WLAN security solution: the Cisco Wireless Security Suite.
Reference: Cisco Courseware page 10-16

QUESTION 208:

What are the features of Temporal Key Integrity Protocol (TKIP)?

A. TKIP is 802.11i standard that offers per-packet keying and message integrity check.
B. TKIP is 802.11q standard that offers complementary code keying and message integrity check.
C. TKIP is 802.11i standard that offers complementary code keying and message integrity check.
D. TKIP is 802.11q standard that offers per-packet keying and message integrity check.

Answer: A

Explanation:
TKIP is a set of software enhancements to RC4-based WEP. Cisco TKIP improvements include the following:
1) Per- packet keying.
2) MIC
Reference: Cisco Courseware page 10-24

QUESTION 209:

Wired Equivalent Privacy (WEP) operates at what layer of the OSI model?

A. Physical
B. Network
C. Transport
D. Data link

Answer: D

Explanation:
Working at the data link layer, WEP requires that all communicating parties share the same secret key. To avoid conflicting with U.S export controls that were in effect at the time the standard was developed, 40-bit encryption keys were required by IEEE 802.11b, through many vendors now support the optional 128-bit standard.
Reference: Cisco Courseware page 10-15

QUESTION 210:

Which are the attack mitigation roles for the VPN Concentrator in the SAFE standard VPN WLAN design? (Choose three)

A. Authentication remote users
B. Two-factor authentication
C. Terminate IPSec
D. RFC 2827 filtering
E. DHCP relay
F. VPN client auto-initiate

Answer: A, C, E
Reference: Cisco Courseware page 10-48

QUESTION 211:

Which threats are expected in the SAFE Enterprise Network Building Distribution module? (Choose three)

A. Port redirection
B. IP spoofing
C. Trust exploitation
D. Packet sniffers
E. Application layer attacks
F. Unauthorized access

Answer: B, D, F

Explanation:
The following are expected threats and mitigation roles to the SAFE Enterprise Network Campus Building Distribution module:
1) Unauthorized access - Attacks against server module resources are limited by Layer 3 filtering of specific subnets.
2) IP spoofing - RFC 2827 filtering stops most spoofing attempts.
3) Packet sniffers - A switched infrastructure limits the effectiveness of sniffing.
Reference: Cisco Courseware page 8-15

QUESTION 212:

Which is a key server found in SAFE Enterprise network design edge corporate Internet module?

A. Database server
B. Application server
C. URL filtering server
D. Proxy server

Answer: C

Explanation:
The following are key devices for the SAFE Enterprise Network Edge Corporate Internet module:
1) SMTKP server
2) DNS server
3) FTP/HTTP server
4) URL filtering server
5) Firewall
6) NIDS appliance
Reference: Cisco Courseware page 8-28

QUESTION 213:

Choose the true statements: (Choose two)

A. Use of HIDS is the mitigation method of port redirection in both small and medium SAFE SMR network design.
B. Use of HIDS is the mitigation method of port redirection only in small SAFE SMR network design.
C. Campus module exists only medium SAFE SMR network design.
D. Campus module exists in both small and medium SAFE SMR network design.

Answer:
A. D

Explanation: Answer A is referred to on pages 14 and 17.
Answer D is referred to on pages 10 and 16.
Ref: Safe White papers
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

---

QUESTION 214:

Encryption technology can solve the problem of:

A. Session replay
B. Both Man-in-the-middle attacks and session replay.
C. Neither Man-in-the-middle attacks no session replay.
D. Man-in-the-middle attacks.

Answer: B

QUESTION 215:

What are the three modules in the SAFE SMR midsize network design? (Choose three)

A. Frame/ATM module
B. Campus module
C. ISP edge module
D. Corporate Internet module
E. WAN module
F. PSTN module

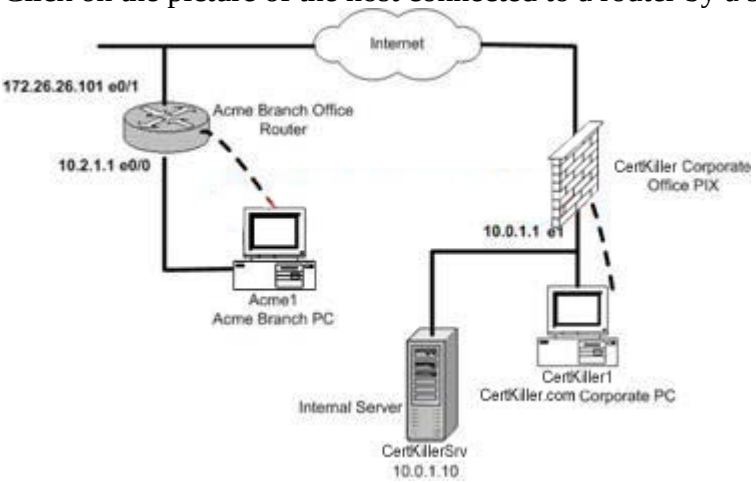
Answer: B, D, E

Explanation:
The SAFE medium network design consists of three modules:
* The corporate Internet module
* The campus module
* The WAN module.
Reference: SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks Page 14

QUESTION 216:

You are the network security administrator for the German company Certkiller Inc. Certkiller Inc. has recently acquired Acme, a small company in another country in Europe, and wants you to start creating a VPN tunnel over the Internet from the outside interface of the Certkiller 's corporate PIX Firewall to the outside interface of Acme's branch office router using pre-shared keys. IKE has already been enabled on both devices. First configure the pre-shared key on each device and then configure the IKE parameters on each device. Use the following values as necessary:
Parameter Value
policy priority number 20
encryption algorithm 3des
has algorithm md5
authentication method pre-share
Diffie-Hellman Group ID 2
SA lifetime 83000
Pre-shared Key my Certkiller
Transform Set Name Certkiller set

ISAKMP Identity Type IP address
PIX Firewall Outside Interface Address 192.168.1.2
Branch Office Outside Interface 172.26.26.101
Crypto Map Name Certkiller map
Netmask 255.255.255.0
1. IPSec parameters are not configured, should not be configured, and consequently the tunnel will not be established.
The Router and PIX have been configured with the following specifications:
Acme Branch Office Routerg
Name: Certkiller 2
E0/0 : 10.2.1.1/24
E0/1 : 172.26.26.101/24
Enable Password: Certkiller
Corporate Office PIX
Name: Certkiller 1
E0 : 192.168.1.2/24
E1 : 10.0.1.1/24
Enable password: Certkiller
Click on the picture of the host connected to a router by a serial console cable.



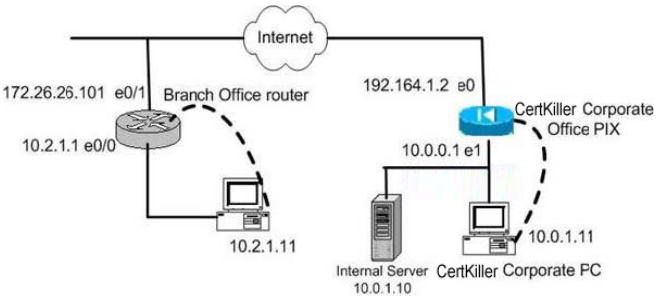
Answer:

Explanation:
Router Configuration
Acme(config)# isakmp enable e0/1
Acme(config-isakmp)# crypto isakmp policy 20
Acme(config-isakmp)# encryption 3des
Acme(config-isakmp)# hash md5
Acme(config-isakmp)# authentication pre-share
Acme(config-isakmp)# group 2
Acme(config-isakmp)# lifetime 83000
Acme(config-isakmp)# crypto isakmp key my Certkiller address 192.164.1.2
Ref:
Configuring Internet Key Exchange Security Protocol

Answer:
PIX Firewall Configuration
Certkiller (config)# isakmp enable outside
Certkiller (config)# isakmp key my Certkiller address 172.26.26.101 netmask 255.255.255.0
Certkiller (config)# isakmp policy 20 authentication pre-share
Certkiller (config)# isakmp policy 20 encryption 3des
Certkiller (config)# isakmp policy 20 hash md5
Certkiller (config)# isakmp policy 20 group 2
Certkiller (config)# isakmp policy 20 lifetime 83000
Ref:
Configuring IPSec - Router to PIX

QUESTION 217:

At Certkiller you work as the network security administrator. Certkiller has recently acquired Acme International, another company in the region. Certkiller wants you to start creating a VPN tunnel over the Internet from the outside interface of Certkiller 's corporate PIX Firewall to the outside interface of Acme International branch office router using pre-shared keys. IKE has already been enabled on both devices. First configure the pre-shared key on each device then configure the IKE parameters on each device. Use the following values as necessary:
Branch Office Router Certkiller Corporate Office PIX
Name: Acme Name: Certkiller
E0/0: 10.2.1.1/24 E0: 192.164.1.2/24
E0/1: 172.26.26.101/24 E1: 10.0.1.1/24
Enable Password: CertK



Assignment: Click on the picture of the host connected to an IDS Sensor by a serial console cable shown in the diagram as a dotted line. Select the Cisco Terminal Option and make the appropriate configuration tasks.
Parameter Value
policy priority number 40
encryption algorithm 3des
hash algorithm md5
authentication method pre-share
Diffie-Hellman group Identifier 2
SA lifetime 81000
Pre-shared Key my Certkiller
Transform Set Name Certkiller set

PIX Firewall Outside Interface Address 192.164.1.2
Branch Office Outside Interface Address 172.26.26.101
Crypto Map Name Certkiller map
Netmask 255.255.255.0
IPSec paramaters are not configured, should not be configured, and consequently the tunnel will not be established.
The Router and PIX have been configured with the following specifications:
Branch Office Router
Name: Acme

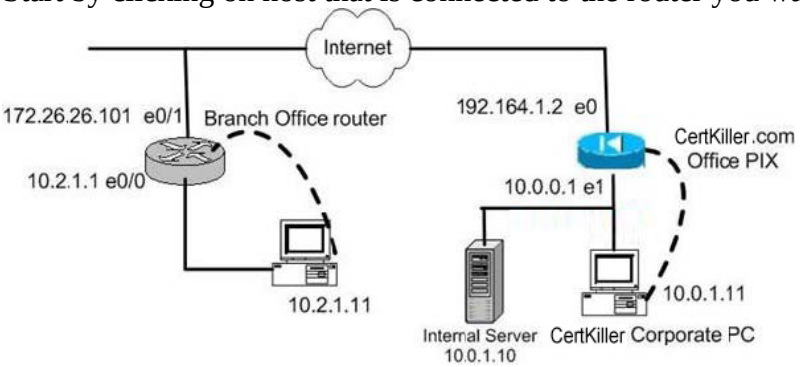
Answer:

Explanation:
For the Certkiller (Corporate PIX firewall):
Correct Answer
Certkiller (config)# isakmp enable outside
Certkiller (config)# isakmp key my Certkiller address 171.26.26.101 netmask 255.255.255.0
Certkiller (config)# isakmp identity address
Certkiller (config)# isakmp policy 40 authentication pre-share
Certkiller (config)# isakmp policy 40 encryption 3des
Certkiller (config)# isakmp policy 40 hash md5
Certkiller (config)# isakmp policy 40 group 2
Certkiller (config)# isakmp policy 40 lifetime 81000
Ref:
Configuring IPSec - Router to PIX
Note: There are 8 more commands that need to be entered to setup IPSEC in order for this to work, but question instructs NOT to do it.
For the Acme (Branch Office Router) the following commands need to be implemented:
Correct Answers
Acme(config)# isakmp enable e0/1
Acme(config-isakmp)# crypto isakmp policy 40
Acme(config-isakmp)# encryption 3des
Acme(config-isakmp)# hash md5
Acme(config-isakmp)# authentication pre-share
Acme(config-isakmp)# group 2
Acme(config-isakmp)# lifetime 8100
Acme(config-isakmp)# crypto isakmp key my Certkiller address 192.164.1.2
Ref:
Configuring Internet Key Exchange Security Protocol

QUESTION 218:

As an employee of Certkiller .com GmBh you are network security administrator. Certkiller .com has recently acquired Acme Ltd, a fast food company in another

country within the European Union. Acme wants you to start creating a VPN tunnel over the Internet from the outside Interface of Certkiller 's corporate PIX Firewall to the outside interface of Acme's branch office router using pre-shared keys. IKE has already been enabled on both devices. First configure the pre-shared key on each device and then configure the IKE parameters on each device. Use the following values as necessary:
Parameter Value
policy priority number 10
encryption algorithm 3des
hash algorithm md5
authentication method pre-share
Diffie-Hellman group Identifier 2
SA lifetime 85000
Pre-shared Key my Certkiller
Transform Set Name Certkiller set
ISAKMP Identity Type IP address
PIX Firewall Outside Interface Address 192.168.1.2
Branch Office Outside Interface Address 172.26.26.101
Crypto Map Name Certkiller map
Netmask 255.255.255.0
1. IPSec parameters are not configured, should not be configured, and consequently the tunnel will not be established
The Router and PIX have been configured with the following specification:
Branch Office Router
Name: Acme
E0/0: 10.2.1.1/24
E0/1: 172.26.26.101/24
Enable password: Certkiller
Corporate Office PIX
Name: Certkiller
E0 192.164.1.2/24
E1 10.0.1.1/24
Enable password: Certkiller
Click on picture of the host connected to a router by a serial cable shown in the diagram as a dotted line.
Start by clicking on host that is connected to the router you want to configure.



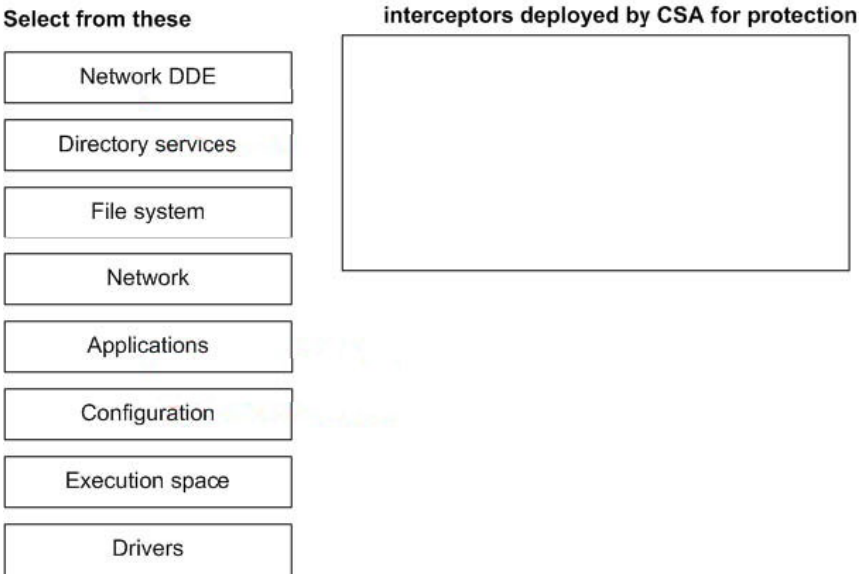
Answer:

Explanation:
Router Configuration
Acme(config)# isakmp enable e0/1
Acme(config-isakmp)# crypto isakmp policy 10
Acme(config-isakmp)# encryption 3des
Acme(config-isakmp)# hash md5
Acme(config-isakmp)# authentication pre-share
Acme(config-isakmp)# group 2
Acme(config-isakmp)# lifetime 85000
Acme(config-isakmp)# crypto isakmp key my Certkiller address 192.164.1.2
Ref:
Configuring Internet Key Exchange Security Protocol

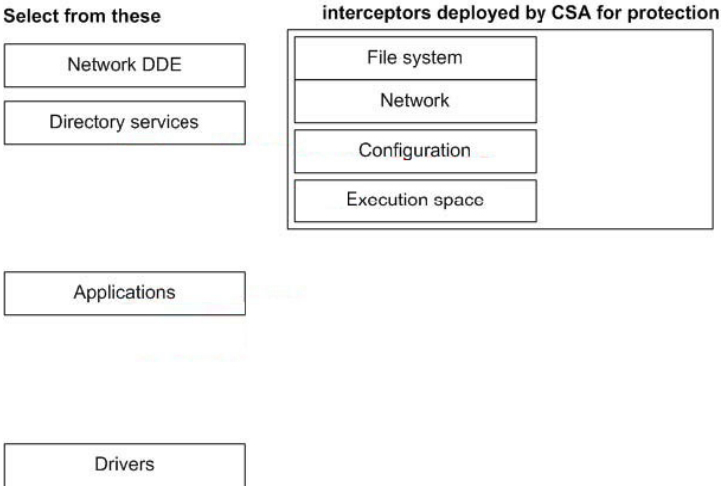
Answer:
PIX Firewall Configuration
Certkiller (config)# isakmp enable outside
Certkiller (config)# isakmp key my Certkiller address 172.26.26.101 netmask 255.255.255.0
Certkiller (config)# isakmp policy 10 authentication pre-share
Certkiller (config)# isakmp policy 10 encryption 3des
Certkiller (config)# isakmp policy 10 hash md5
Certkiller (config)# isakmp policy 10 group 2
Certkiller (config)# isakmp policy 10 lifetime 85000
Ref:
Configuring IPSec - Router to PIX

QUESTION 219:

DRAG DROP
Select four interceptors that are deployed by the CSA to provide protection. Move the four interceptors to the right column. You will not use all options.



Answer:



QUESTION 220:

What threats are expected for the SAFE SMR small network campus module?
Select two.

A. IP Spoofing
B. packet sniffers
C. denial of service
D. applications layer attacks

Answer: B, D

QUESTION 221:

What are the features that Direct Sequencing networks offer to transmit data?

Select three.

A. Direct Sequencing offers 11 overlapping channels.
B. Direct Sequencing offers 13 overlapping channels.
C. Direct Sequencing uses 2.4 GHz RF spectrum.
D. Direct Sequencing uses 5 GHz RF spectrum
E. Direct Sequencing provides Complementatry Code Kying (CCK) to support higher data rates.
F. Direct Sequencing provides Quadrature Phase Shift (QPSK) to support higher data rates.

Answer: A, C, E

QUESTION 222:

When using PC-based IP phones, which threat is expected between data and voice segments if not protected by a stateful firewall?

A. TCP flood DoS attack
B. IP spoofing attack
C. UDP flood DoS attack
D. application layer attack

Answer: C

QUESTION 223:

How many modules exist in the SAFE Enterprise Network Campus?

A. 3
B. 4
C. 5
D. 6

Answer: B

QUESTION 224:

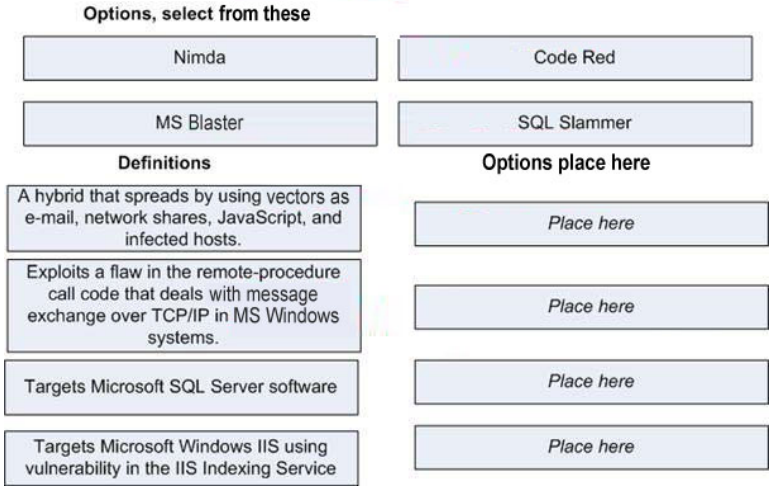
In which module does the firewall exist in the SAFE SMR small network design?

A. Internet
B. campus
C. corporate Internet
D. edge

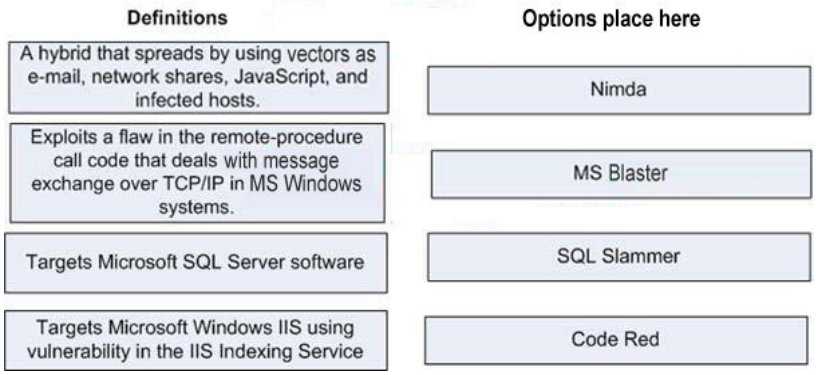
Answer: C

QUESTION 225:

DRAG DROP
Your work as a network administrator at Certkiller .com. Your boss, Mrs. Certkiller, is curious about Internet worms.
Match the characteristics with the proper worm.



Answer:



Explanation:
Nimda is a computer worm, isolated in September 2001. It is also a file infector. It quickly spread, eclipsing the economic damage caused by past outbreaks such as Code Red.
Nimda affected both user workstations (clients) running Windows 95, 98, Me, NT, or 2000 and servers running Windows NT and 2000.
The worm's name spelled backwards is "admin".
Methods of infection
Nimda was so effective partially because it - unlike other famous malware like the Morris worm or Code Red - uses 5 different infection vectors:
via email
via open network shares
via browsing of compromised web sites

exploitation of various Microsoft IIS 4.0 / 5.0 directory traversal vulnerabilities via back doors left behind by the "Code Red II" and "sadmind/IIS" worms.
The Blaster worm (also known as Lovsan or Lovesan) was a computer worm that spread on computers running the Microsoft operating systems, Windows XP and Windows 2000, during August 2003.
The worm was first noticed and started spreading in the wild on August 11. The rate that it spread increased until the number of infections peaked on August 13. Filtering by ISPs and widespread publicity about the worm curbed the spread of Blaster.
The worm was programmed to start a SYN flood on August 15 against port 80 of windowsupdate.com, thereby creating a distributed denial of service attack (DDoS) against the site. The damage to Microsoft was minimal as the site targeted was windowsupdate.com instead of windowsupdate.microsoft.com to which it was redirected. Microsoft temporarily shut down the targeted site to minimize potential effects from the worm.
The worm spread by exploiting a buffer overflow in the DCOM RPC service on the affected operating systems, for which a patch had been released one month earlier in MS03-026 and later in MS03-039.
The SQL slammer worm is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic, starting at 05:30 UTC on January 25, 2003. It spread rapidly, infecting most of its 75,000 victims within 10 minutes. Although titled "SQL slammer worm", the program did not use the SQL language;it exploited two buffer overflow bugs in Microsoft's flagship SQL server database product.
The Code Red worm was a computer worm released on the Internet on July 13, 2001. It attacked computers running Microsoft's IIS web server. The most in-depth research on the worm was performed by the programmers at eEye Digital Security. They also gave the worm its name, a reference to a variety of Mountain Dew soft drink and the phrase "Hacked By Chinese!" with which the worm defaced websites.
The worm exploited a vulnerability in the indexing software distributed with IIS, described in MS01-033, for which a patch had been available a month earlier.

QUESTION 226:

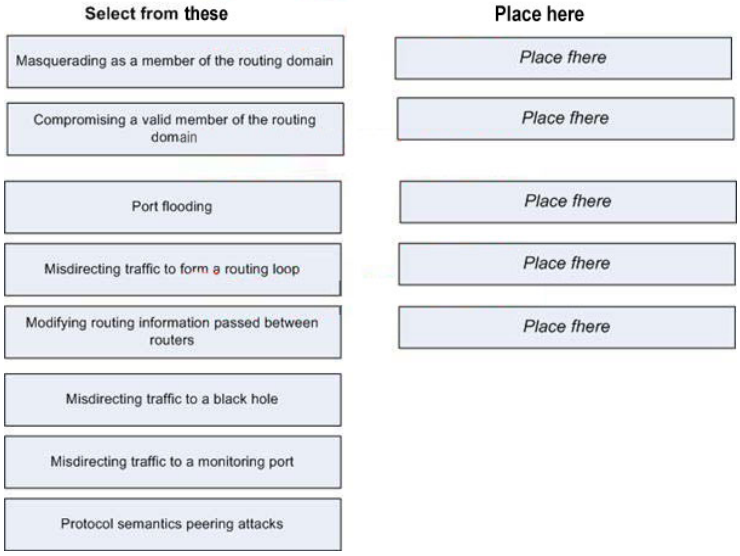
Which techniques does SAFE recommend to mitigate MAC spoofing attacks?
(Select two.)

A. Use port security.
B. Implement IP Source Guard feature.
C. Set all user ports to nontrunking mode.
D. Implement BPDU guard enhancement command.
E. Implement authentication for DHCP messages.
F. Use DHCP snooping along with DAI.

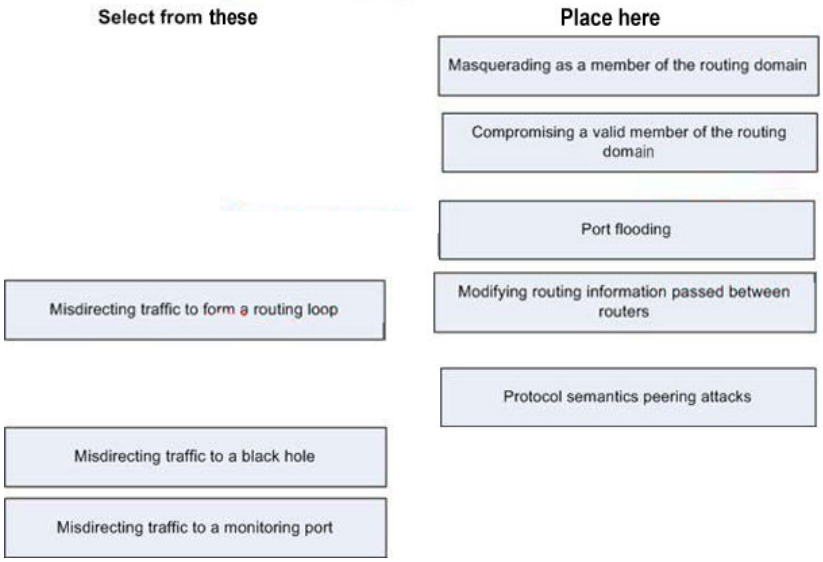
Answer: A,F

QUESTION 227:

DRAG DROP
Your Certkiller Boss, Certkiller, asks you about SAFE best practices for routing protocols.
Which items are examples of disrupting peering attacks?



Answer:



QUESTION 228:

According to SAFE worm mitigation, what happens during the quarantine phase of the worm mitigation?

A. All uninfected systems are patched with the appropriate vendor patch for the vulnerability.

B. The spread of a worm infection is limited to areas of the network that are already affected.
C. An actively infected system is disinfected of the worm.
D. Infected machines are identified, contained, and blocked.

Answer: D

QUESTION 229:

Which of the following is not a SAFE guideline to proactively mitigate Code Red attacks?

A. host intrusion prevention system
B. network-based application recognition
C. antivirus
D. access control

Answer: C

QUESTION 230:

According to SAFE implementation of IPSec VPN, what are key VPN devices in a medium network? (Select three.)

A. VPN router
B. VPN firewall
C. interior firewall
D. VPN Concentrator
E. distribution router
F. NIDS appliance

Answer: B,D,F

QUESTION 231:

According to SAFE implementation of IPSec VPN, what is the function of a VPN router in a large network remote access and VPN module?

A. Authenticates individual remote users using XAUTH and terminates their IPSec tunnels.
B. Tracks the availability of remote site networks across the VPN routers.
C. Authenticates trusted remote sites and provides connectivity using GRE/IPSec tunnels.
D. Authenticates trusted remote sites and provides stateful filtering of remote site traffic.

Answer: C

QUESTION 232:

According to SAFE IPSec VPN, which of these are recommended design guidelines for maintaining high availability? (Select three.)

A. When using VPN routers at the headend, use IKE keepalives for high availability.
B. When using VPN Concentrators or VPN firewalls at the headend, use IKE keepalives for high availability.
C. Regardless of the high-availability mechanism chosen, a headend device should not be deployed in a configuration that results in CPU utilization higher than 50 percent after failure.
D. Regardless of the high-availability mechanism chosen, a headend device should not be deployed in a configuration that results in CPU utilization higher than 75 percent after failure.
E. Cisco recommends running IKE keepalives in combination with routing protocols for resilience to assist in keeping the state current.
F. Cisco does not recommend running IKE keepalives in combination with routing protocols for resilience to assist in keeping the state current.

Answer: B,C,F

QUESTION 233:

According to SAFE guidelines for implementing VPN IPSec, which of these statements are true? (Select two.)

A. Wildcard preshared keys should be used for site-to-site device authentication.
B. Digital certificates are not tied to IP addresses but to unique, signed information on the device that is validated by the CA.
C. Unique preshared keys are recommended between two devices and can scale in a large network.
D. Digital certificates provide nonrepudiation but no public/private key pair aging.
E. Digital certificates scale better but require additional administrative resources to deploy and manage.

Answer: B,E

QUESTION 234:

Which vulnerability is not expected in a network design comprised of multiple security zones, multiple user groups, and a single physical switch?

A. MAC spoofing
B. CAM table overflow
C. VTP attacks
D. VLAN hopping

E. private VLAN attacks

Answer: C

QUESTION 235:

What is the purpose of BGP TTL Security Hash (BTSH)?

A. encrypts private network data when it is being passed through a public network
B. prevents attacker from creating a routing black hole
C. helps to prevent information overload from causing a network to melt
D. prevents attackers from disrupting peering sessions between routers
E. reduces the change rate in the Internet's routing tables

Answer: D

QUESTION 236:

What are the SAFE guidelines when routing information is exchanged with an outside routing domain? (Select two.)

A. Use exterior gateway protocols only.
B. Use exterior gateway protocols that operate between routing domains and do not allow administrators to build and act on policies.
C. Use exterior gateway protocols because they allow administrators to build and act on policies rather than just on reachability information.
D. Do not use autonomous system path filters on every EBGP peering session in network.
E. Use exterior gateway protocols or static routes.
F. Make certain that your outside peer advertises your routes to other peers for maximum reachability.

Answer: C,E

QUESTION 237:

According to SAFE worm mitigation, which of the following is not a mitigation for MS Blaster?

A. private VLANs
B. NBAR
C. CAR
D. sink-hole routers
E. NetFlow

Answer: D

QUESTION 238:

What Radio Frequency (RF) band does the Home RF Shared Wireless Access Protocol (SWAP) specification use?

A. 900 GHz
B. 2.4 GHz
C. 5.7 GHz
D. 900 MHz

Answer: B

QUESTION 239:

What is a feature of SIP?

A. SIP is a transport-layer control protocol that uses IP addresses for transporting multimedia traffic and call management.
B. SIP is a session-layer control protocol that uses SIP addresses for signal and session management.
C. SIP is an application-layer control protocol that uses SIP addresses for signal and session management.
D. SIP is a session-layer control protocol that uses IP addresses for transporting multimedia traffic and session management.

Answer: C

QUESTION 240:

Which routing protocol does not support the use of MD5 authentication?

A. BGP
B. IGRP
C. EIGRP
D. OSPF
E. IS-IS

Answer: B

QUESTION 241:

Which IEEE standards are supported by Cisco Aironet 1200 Series access point? Choose three.

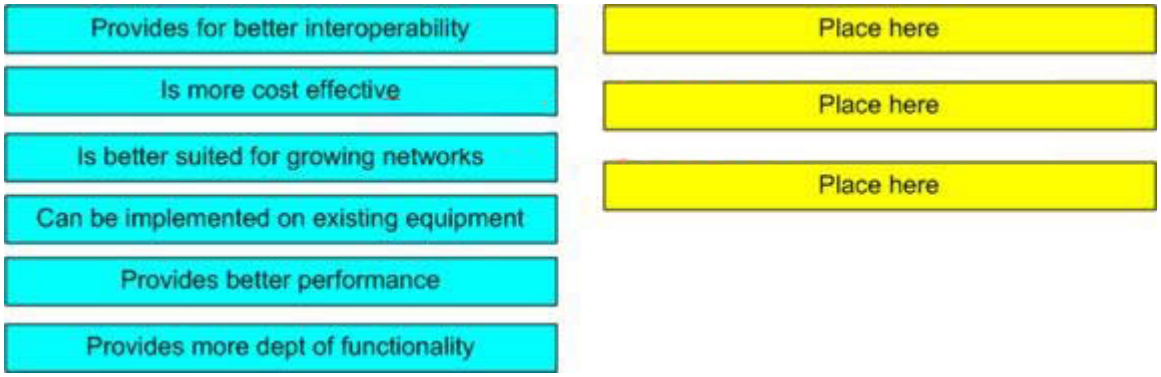
A. 802.11a

B. 802.11b
C. 802.11c
D. 802.11g
E. 802.11h
F. 802.11j

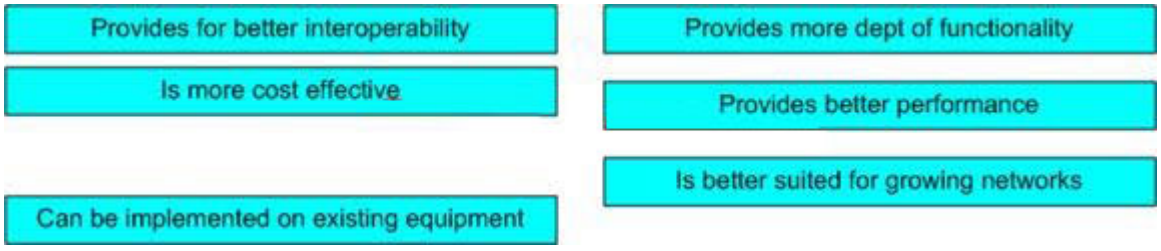
Answer: A,B,D

QUESTION 242:

DRAG DROP
What three advantages does a dedicated VPN appliance have over a device containing integrated VPN functionality?



Answer:



QUESTION 243:

According to SAFE IPSec VPN, which is not a design objective to guide the decision-making process in implementing VPN?

A. secure connectivity and management
B. reliability, performance, and scalability
C. high availability

D. authentication of users and devices in the VPN
E. tuning and reporting
F. security and attack mitigation before and after IPSec

Answer: E

QUESTION 244:

Which threats are expected in the SAFE Enterprise Network Campus Building module? Choose two.

A. IP spoofing
B. packet sniffers
C. unauthorized access
D. virus and trojan horse applications
E. port redirection attacks

Answer: B,D

QUESTION 245:

Which of the following is not a critical element of Cisco Self Defending Network strategy?

A. SAFE
B. threat defense system
C. secure connectivity
D. trust and identity management

Answer: A

QUESTION 246:

Which routing protocol does not support the use of MD5 authentication?

A. BGP
B. IGRP
C. EIGRP
D. OSPF
E. IS-IS

Answer: B

QUESTION 247:

What is a feature of SIP?

A. SIP is a transport-layer control protocol that uses IP addresses for transporting multimedia traffic and call management.
B. SIP is a session-layer control protocol that uses SIP addresses for signal and session management.
C. SIP is an application-layer control protocol that uses SIP addresses for signal and session management.
D. SIP is a session-layer control protocol that uses IP addresses for transporting multimedia traffic and session management.

Answer: C

QUESTION 248:

According to the SAFE Layer 2 security white paper, which is not a threat to switches?

A. CAM table overflow
B. DHCP starvation
C. IP address spoofing
D. VLAN hopping
E. Spanning-Tree Protocol manipulation

Answer: C

QUESTION 249:

According to SAFE IPSec VPN, which is not a design objective to guide the decision-making process in implementing VPN?

A. secure connectivity and management
B. reliability, performance, and scalability
C. high availability
D. authentication of users and devices in the VPN
E. tuning and reporting
F. security and attack mitigation before and after IPSec

Answer: E

QUESTION 250:

According to SAFE worm mitigation, which of the following statements are true about worms and viruses? (Select three.)

A. Worms are self-contained programs that attack a system and try to exploit vulnerability in the target.

B. Viruses require human interaction to facilitate the spread.
C. Worms normally require a vector to carry the code from one system to another.
D. Viruses normally require a vector to carry the code from one system to another.
E. Worms require human interaction to facilitate the spread.
F. Viruses are self-contained programs that attack a system and try to exploit vulnerability in the target.

Answer: A,B,D

QUESTION 251:

Which two Cisco components encompass intrusion protection? Choose two.

A. Cisco VPN Concentrators
B. Cisco IDS Sensors
C. Cisco IDS Access Point
D. Cisco IOS IDS
E. Cisco Wireless IDS

Answer: B,D

QUESTION 252:

Which IEEE standards are supported by Cisco Aironet 1200 Series access point? Choose three.

A. 802.11a
B. 802.11b
C. 802.11c
D. 802.11g
E. 802.11h
F. 802.11j

Answer: A,B,D

QUESTION 253:

According to SAFE IPSec VPN, which of the following design guidelines for implementing NAT are true? (Select three.)

A. Enabling NAT transparency mode will resolve the connection problems associated with client applications that are not NAT friendly.
B. IPSec tunnel will not establish between two networks when address ranges overlap.
C. When applying NAT after IPSec, use AH tunnel mode instead of ESP.
D. Enabling NAT transparency mode will not resolve the connection problems associated with client applications that are not NAT friendly.

E. When applying NAT after IPSec, use ESP tunnel mode instead of AH.
F. IPSec tunnel will establish between two networks even if address ranges overlap.

Answer: B,D,E