Vendor: Cisco

Exam Code:350-701

Exam Name: Implementing and Operating Cisco Security Core Technologies (SCOR)

Version: Demo

QUESTION 1

A company identified a phishing vulnerability during a pentest.

What are two ways the company can protect employees from the attack? (Choose two.)

A. using Cisco Umbrella

B. using Cisco ESA

C. using Cisco FTD

D. using an inline IPS/IDS in the network E. using Cisco ISE

Correct Answer: AB

QUESTION 2

An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used. However, the connection is failing. Which action should be taken to accomplish this goal?

A. Disable telnet using the no ip telnet command.

B. Enable the SSH server using the ip ssh server command.

C. Configure the port using the ip ssh port 22 command.

D. Generate the RSA key using the crypto key generate rsa command.

Correct Answer: D

In this question, the engineer was trying to secure the connection so maybe he was trying to allow SSH to the device. But maybe something went wrong so the connection was failing (the connection used to be good). So maybe he was missing the "crypto key generate rsa" command.

QUESTION 3

What is provided by the Secure Hash Algorithm in a VPN?

A. integrity

B. key exchange

C. encryption

D. authentication

Correct Answer: A

Reference: https://www.ciscopress.com/articles/article.asp?p=24833andseqNum=4

QUESTION 4

When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?

A. Multiple routers or VRFs are required.

B. Traffic is distributed statically by default.

C. Floating static routes are required.

D. HSRP is used for faliover.

Correct Answer: B

QUESTION 5

On which part of the IT environment does DevSecOps focus?

A. application development

B. wireless network

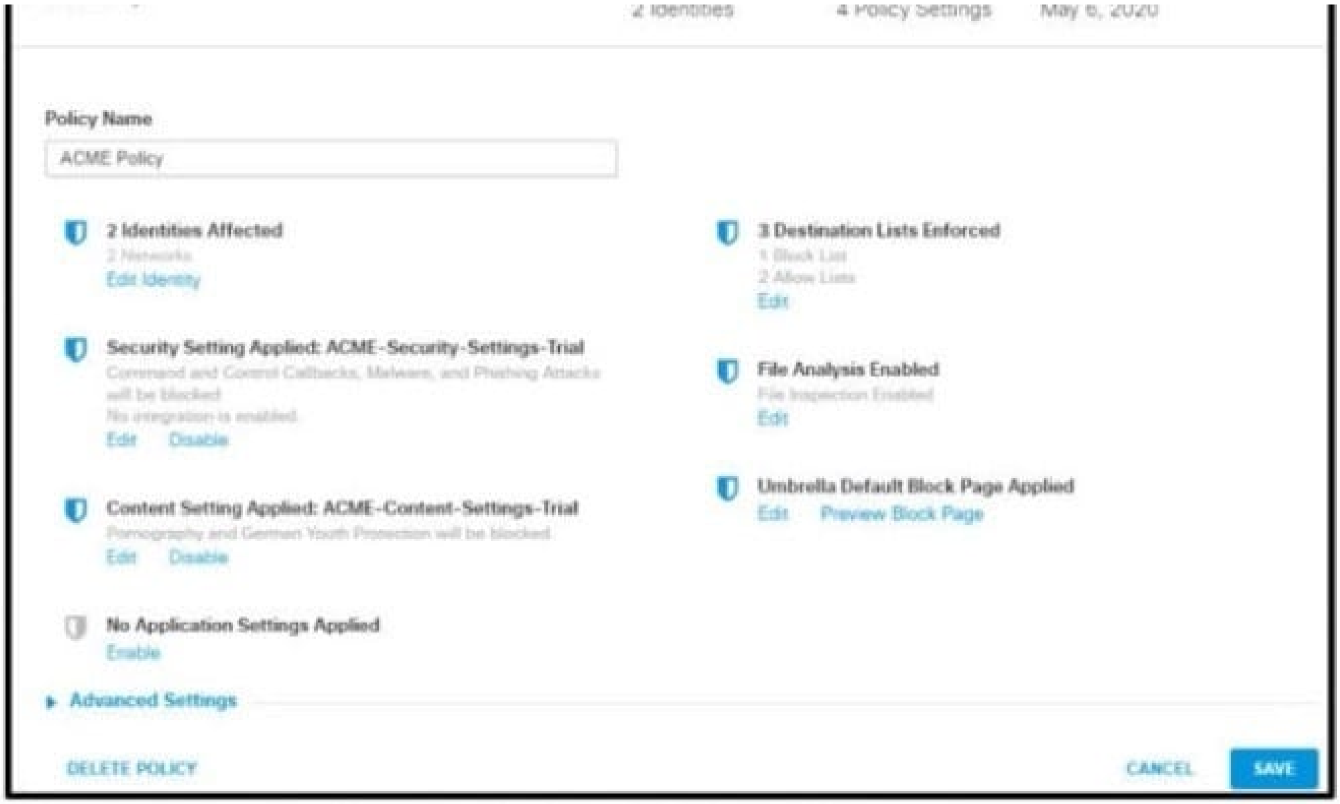
C. data center

D. perimeter network

Correct Answer: A

QUESTION 6

Refer to the exhibit.



2 Identities 4 Policy Settings May 6, 2020

Policy Name

ACME Policy

2 Identities Affected
2 Networks
Edit Identity

Security Setting Applied: ACME-Security-Settings-Trial
Command and Control Callbacks, Malware, and Phishing Attacks will be blocked
No integration is enabled.
Edit Disable

Content Setting Applied: ACME-Content-Settings-Trial
Pornography and German Youth Protection will be blocked.
Edit Disable

No Application Settings Applied
Enable

3 Destination Lists Enforced
1 Block List
2 Allow Lists
Edit

File Analysis Enabled
File Inspection Enabled
Edit

Umbrella Default Block Page Applied
Edit Preview Block Page

How does Cisco Umbrella manage traffic that is directed toward risky domains?

A. Traffic is proximed through the intelligent proxy.

B. Traffic is managed by the security settings and blocked.

C. Traffic is managed by the application settings, unhandled and allowed.

D. Traffic is allowed but logged.

Correct Answer: B

QUESTION 7

Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)

A. NTLMSSP

B. Kerberos

C. CHAP

D. TACACS+

E. RADIUS

Correct Answer: AB

Neither RADIUS or TACACS+ authenticates the user. They facilitate communication to the authentication server.

Kerberos and NTLMSSP do authenticate the user.

QUESTION 8

When a site-to-site VPN is configured in Cisco FMC, which topology is supported when crypto ACLs are used instead of protected networks to define interesting traffic?

A. hub-and-spoke

B. full mesh

C. DMVPN

D. point-to-point

Correct Answer: D

QUESTION 9

What is a characteristic of a bridge group in ASA Firewall transparent mode?

A. It includes multiple interfaces and access rules between interfaces are customizable

B. It is a Layer 3 segment and includes one port and customizable access rules

C. It allows ARP traffic with a single access rule

D. It has an IP address on its BVI interface and is used for management traffic

Correct Answer: A

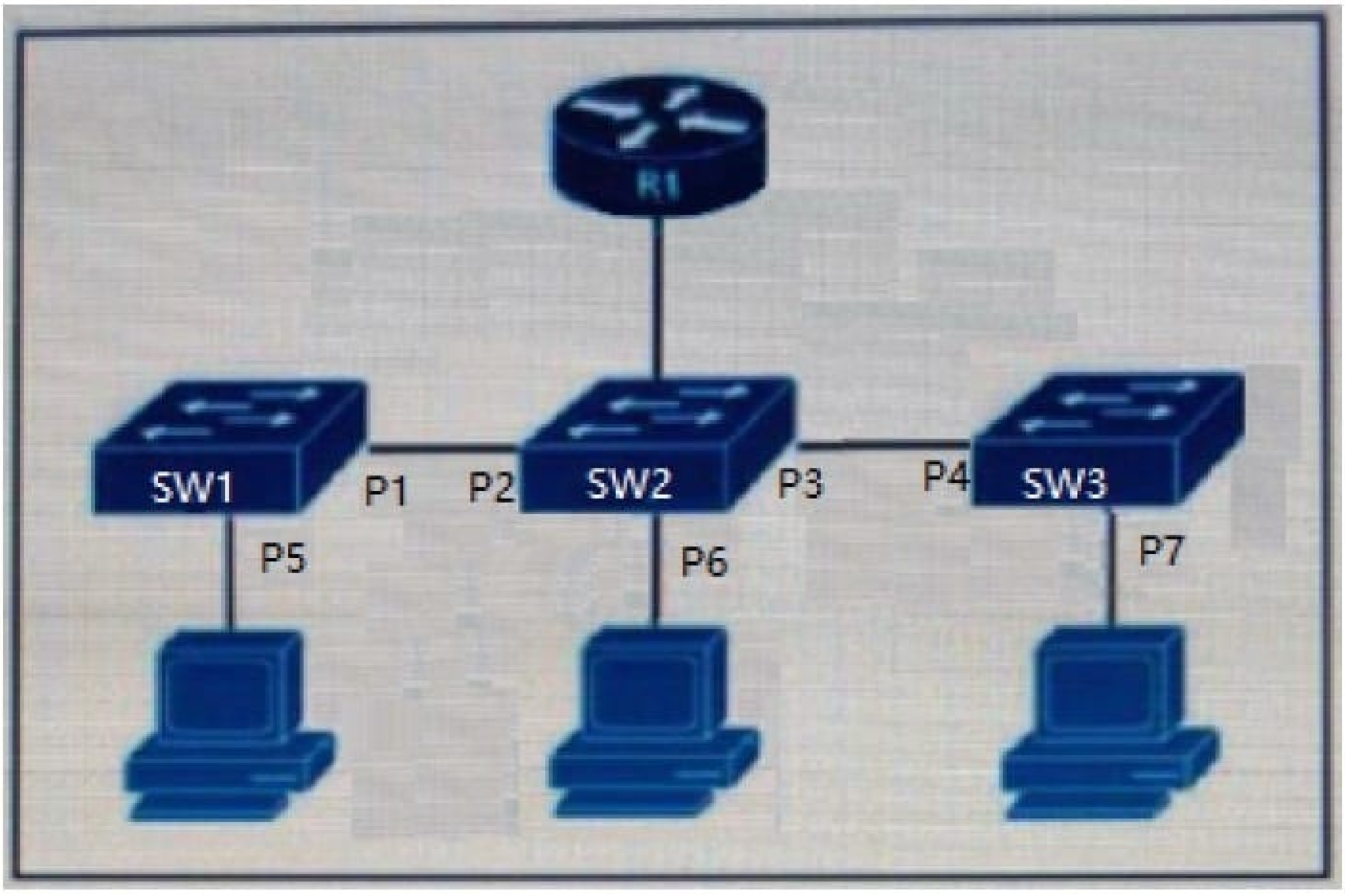
Reference:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95- generalconfig/intro-fw.html

Note: BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

QUESTION 10

Refer to the exhibit.



The DHCP snooping database resides on router R1, and dynamic ARP inspection is configured only on switch SW2. Which ports must be configured as untrusted so that dynamic ARP inspection operates normally?

A. P2 and P3 only

B. P5, P6, and P7 only

C. P1, P2, P3, and P4 only

D. P2, P3, and P6 only

Correct Answer: D

QUESTION 11

Which option is the main function of Cisco Firepower impact flags?

A. They alert administrators when critical events occur.

B. They highlight known and suspected malicious IP addresses in reports.

C. They correlate data about intrusions and vulnerability.

D. They identify data that the ASA sends to the Firepower module.

Correct Answer: C

QUESTION 12

Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting

B. water holing

C. DDoS

D. buffer overflow

Correct Answer: D

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations. Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it\\'s alloted memory space. This happens quite frequently in the case of arrays.