



350-701^{Q&As}

Implementing and Operating Cisco Security Core Technologies (SCOR)

Pass Cisco 350-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/350-701.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

- A. Patch for cross-site scripting.
- B. Perform backups to the private cloud.
- C. Protect against input validation and character escapes in the endpoint.
- D. Install a spam and virus email filter.
- E. Protect systems with an up-to-date antimalware program

Correct Answer: DE

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

QUESTION 2

Which algorithm provides encryption and authentication for data plane communication?

- A. AES-GCM
- B. SHA-96
- C. AES-256
- D. SHA-384

Correct Answer: A

Reference:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html>

QUESTION 3

What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?

- A. Cisco Umbrella
- B. External Threat Feeds
- C. Cisco Threat Grid



D. Cisco Stealthwatch

Correct Answer: B

<https://www.cisco.com/c/en/us/support/docs/storage-networking/security/214859-configure-and-troubleshoot-cisco-threat.html>

QUESTION 4

What is the primary benefit of deploying an ESA in hybrid mode?

- A. You can fine-tune its settings to provide the optimum balance between security and performance for your environment
- B. It provides the lowest total cost of ownership by reducing the need for physical appliances
- C. It provides maximum protection and control of outbound messages
- D. It provides email security while supporting the transition to the cloud

Correct Answer: D

Cisco Hybrid Email Security is a unique service offering that facilitates the deployment of your email security infrastructure both on premises and in the cloud. You can change the number of on-premises versus cloud users at any time throughout the term of your contract, assuming the total number of users does not change. This allows for deployment flexibility as your organization's needs change.

QUESTION 5

When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?

- A. Spero analysis
- B. dynamic analysis
- C. sandbox analysis
- D. malware analysis

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Reference_a_wrapper_Chapter_topic_here.html -> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole file. Dynamic analysis sends files to AMP ThreatGrid. Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco ThreatGrid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit. Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. ->



Malware analysis does not upload files to anywhere, it only checks the files locally. There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a virtual machine.

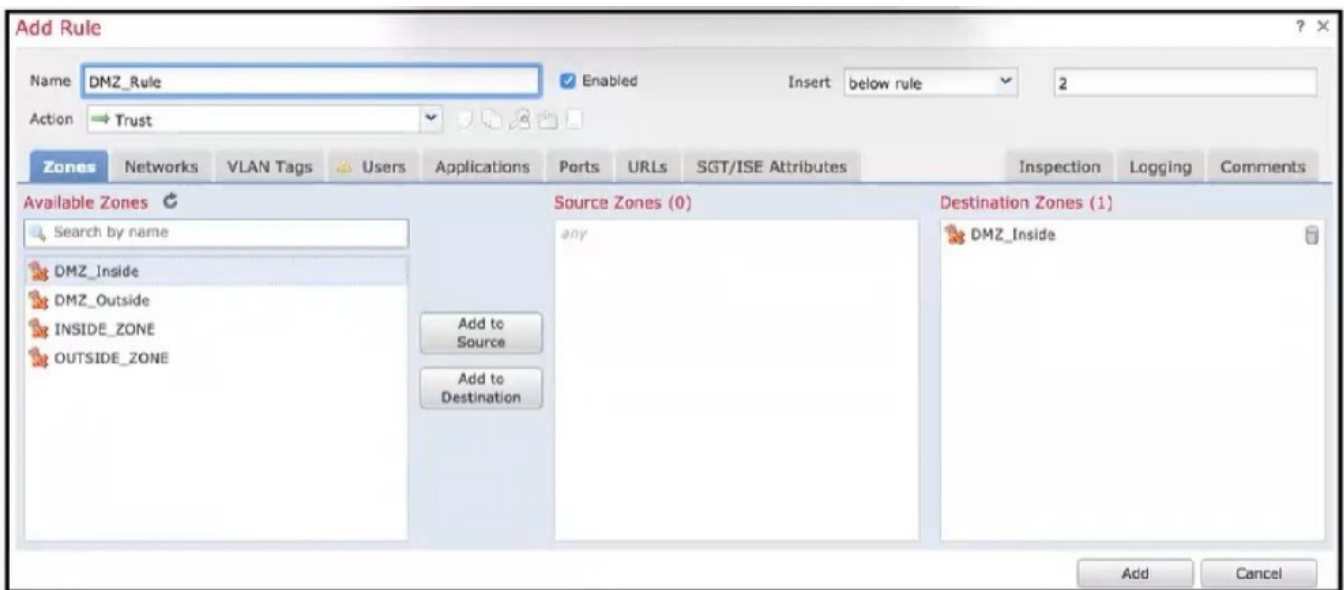
QUESTION 6

What is a benefit of using GET VPN over FlexVPN within a VPN deployment?

- A. GET VPN supports Remote Access VPNs
- B. GET VPN natively supports MPLS and private IP networks
- C. GET VPN uses multiple security associations for connections
- D. GET VPN interoperates with non-Cisco devices

Correct Answer: B

QUESTION 7



Refer to the exhibit. When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZ_Inside zone once the configuration is deployed?

- A. All traffic from any zone to the DMZ_Inside zone will be permitted with no further inspection
- B. No traffic will be allowed through to the DMZ_Inside zone regardless of if it's trusted or not
- C. All traffic from any zone will be allowed to the DMZ_Inside zone only after inspection
- D. No traffic will be allowed through to the DMZ_Inside zone unless it's already trusted

Correct Answer: A

**QUESTION 8**

Refer to the exhibit.

```
interface GigabitEthernet1/0/18
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device-tracking attach-policy IPDT_MAX_10
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
dot1x pae authenticator
dot1x timeout tx-period 7
dot1x max-reauth-req 3
spanning-tree portfast
```

Refer to the exhibit. A Cisco ISE administrator adds a new switch to an 802.1X deployment and has difficulty with some endpoints gaining access.

Most PCs and IP phones can connect and authenticate using their machine certificate credentials. However printer and video cameras cannot base d on the interface configuration provided, what must be to get these devices on to the network using Cisco ISE for authentication and authorization while maintaining security controls?

- A. Change the default policy in Cisco ISE to allow all devices not using machine authentication .
- B. Enable insecure protocols within Cisco ISE in the allowed protocols configuration.
- C. Configure authentication event fail retry 2 action authorize vlan 41 on the interface
- D. Add mab to the interface configuration.

Correct Answer: D

<https://community.cisco.com/t5/network-access-control/problems-with-connecting-printers-via-mab/td-p/3528002>

QUESTION 9

Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers and can be stopped by Cisco Umbrella?

- A. DNS tunneling
- B. DNS flood attack
- C. cache poisoning
- D. DNS hijacking



Correct Answer: A

QUESTION 10

Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?

- A. Advanced Malware Protection
- B. Platform Exchange Grid
- C. Multifactor Platform Integration
- D. Firepower Threat Defense

Correct Answer: B

With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

QUESTION 11

Refer to the exhibit.



```
> show crypto ipsec sa
interface: Outside
  Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
  209.165.200.225

  access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
  255.255.255.0 10.0.10.0 255.255.255.0
  local ident (addr/mask/prot/port): (10.0.11.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0)
  current_peer: 209.165.202.129

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
  failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments
  created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
  reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
  209.165.202.129/500
  path mtu 1500, ipsec overhead 55(36), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: B6F5EA53
  current inbound spi : 84348DEE
```

Traffic is not passing through IPsec site-to-site VPN on the Firepower Threat Defense appliance. What is causing this issue?

- A. No split-tunnel policy is defined on the Firepower Threat Defense appliance.
- B. The access control policy is not allowing VPN traffic in.
- C. Site-to-site VPN peers are using different encryption algorithms.
- D. Site-to-site VPN preshared keys are mismatched.

Correct Answer: B

QUESTION 12

Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with VMware VDS or Microsoft vSwitch?



- A. inter-EPG isolation
- B. inter-VLAN security
- C. intra-EPG isolation
- D. placement in separate EPGs

Correct Answer: C

C. Intra-EPG Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch

Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another. However, conditions exist in which total isolation of the endpoint devices from one another within an EPG is desirable. For example, you may want to enforce intra-EPG isolation if the endpoint VMs in the same EPG belong to multiple tenants, or to prevent

QUESTION 13

Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?

- A. VMware APIC
- B. VMwarevRealize
- C. VMware fusion
- D. VMware horizons

Correct Answer: B

[350-701 PDF Dumps](#)

[350-701 Exam Questions](#)

[350-701 Braindumps](#)