300-710サンプル問題集、300-710最新試験

2026年Fast2testの最新300-710 PDFダンプおよび300-710試験エンジンの無料共有：https://drive.google.com/open?id=1OqdL0gUeN6U-OzYnuqRqRHJdOWYsdQLY

インターネットで信頼できる試験コレクション資料を検索して私たちを見つけた場合、実際には、300-710認定試験に最適な製品が見つかりました。 300-710試験の合格率が高いことで有名です。そのため、多くの古いお客様が300-710試験に参加する前に私たちを信頼して直接選択しています。購入する前に、ダウンロード用の無料のPDFデモを提供して、製品の品質をより深く知ることができ、想像力に応えるだけでなく、300-710学習ガイドを明確に購入できるようにします。

Cisco 300-710認定試験は、Cisco Firpower NGFWテクノロジーを深く理解する必要がある挑戦的で厳密な試験です。候補者は、ネットワークセキュリティの概念を強く理解しているだけでなく、Cisco Firepowerテクノロジーの操作経験が必要です。この認定試験に合格すると、Cisco Firepowerテクノロジーを使用してネットワークインフラストラクチャの保護における高レベルの専門知識と習熟度が示されています。

>> 300-710サンプル問題集 <<

300-710最新試験、300-710試験時間

あなたに安心にネットでCiscoの300-710試験の資料を購入させるために、我々Fast2testは国際の最大の安全的な支払システムPaypalと協力してあなたの支払の安全性を保障します。支払ってから、あなたは直ちにCiscoの300-710試験の資料をダウンロードすることができ、その後の一年間でCiscoの300-710試験ソフトが更新されたら、我々はあなたを通知します。Fast2testを選ぶのは最高のサービスを選んだことです。

認定試験は60-70の多肢選択および複数回答問題で構成され、受験者には90分の時間が与えられます。試験は、Cisco Firepower NGFWのコンセプト、アーキテクチャ、展開、および管理に関する受験者の知識、およびアクセス制御、侵入防止、ネットワーク分析、マルウェア保護などのCisco Firepower NGFWの機能の設定とトラブルシューティング能力をテストします。試験に合格した受験者は、Ciscoネットワークを高度なセキュリティ技術を使用して保護する専門知識を証明する、世界的に認められた資格であるCisco Certified Network Professional Security（CCNP Security）認定を取得します。

Cisco Securing Networks with Cisco Firepower 認定 300-710 試験問題 (Q312-Q317):

質問 # 312
Refer to the exhibit. An administrator is looking at some of the reporting capabilities for Cisco Firepower and noticed this section of the Network Risk report showing a lot of SSL activity that cloud be used for evasion. Which action will mitigate this risk?

- A. Use encrypted traffic analytics to detect attacks
- B. Use Cisco AMP for Endpoints to block all SSL connection
- C. Use SSL decryption to analyze the packets.
- D. Use Cisco Tetration to track SSL connections to servers.

正解：C

解説：
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd- fdm-ssl-decryption.html

質問 # 313
Which command should be used on the Cisco FTD CLI to capture all the packets that hit an interface?

- A. configure coredump packet-engine enable
- B. capture WORD
- C. capture-traffic
- D. capture

正解：D

解説：
Reason: the command "capture-traffic" is used for SNORT Engine Captures. To capture a LINA Engine Capture, you use the "capture" command. Since the Lina Engine represents the actual physical interface of the device, "capture" is the only reasonable choice Reference:https://www.cisco.com/c/en/us/support/docs/security /firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc10 The command is firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100 firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14

質問 # 314
A security engineer is configuring an Access Control Policy for multiple branch locations. These locations share a common rule set and utilize a network object called INSIDE_NET which contains the locally significant internal network subnets at each location. Which technique will retain the policy consistency at each location but allow only the locally significant network subnet within the applicable rules?

- A. utilizing policy inheritance
- B. creating a unique Access Control Policy per device
- C. utilizing a dynamic Access Control Policy that updates from Cisco Talos
- D. creating an Access Control Policy with an INSIDE_NET network object and object overrides

正解：D

質問 # 315
An administrator is attempting to add a Cisco Secure Firewall Threat Defence device to Cisco Secure Firewall Management Center with a password of Cisco0480846211 480846211. The private IP address of the FMC server is 192.168.75.201. Which command must be used in order to accomplish this task?

- A. configure manager add 192.168.75.201 255.255.255.0 <reg_key>
- B. configure manager add 192.168.75.201 <reg_key>
- C. configure manager add 192.168.75.201/24 <reg_key>
- D. configure manager add 192.168.45.45 <reg_key> <nal-ld>

正解：B

解説：
To add a Cisco Secure Firewall Threat Defense (FTD) device to Cisco Secure Firewall Management Center (FMC), the correct command to use is configure manager add
192.168.75.201 <reg_key>.
This command registers the FTD device with the FMC using the FMC's IP address and the registration key provided during the FMC setup.
Command structure:
configure manager add <FMC_IP> <reg_key>
For the given scenario:
FMC IP address: 192.168.75.201

Registration key: provided during FMC setup
Thus, the correct command is:
configure manager add 192.168.75.201 <reg_key>

質問 # 316
What is the role of realms in the Cisco ISE and Cisco Secure Firewall Management Center integration?

- A. AD definition
- B. TACACS+ database
- C. (Option not provided - please confirm or provide)
- D. Cisco Secure Firewall VDC
- E. Cisco ISE context

正解： D

質問 # 317
......