New Test 300-710 Questions Fee 100% Pass | High Pass-Rate 300-710: Securing Networks with Cisco Firepower 100% Pass

What's more, part of that FreeDumps 300-710 dumps now are free: https://drive.google.com/open?id=13REA7XZefqLK6ZN9WCZxraEBrVNHldyu

As you know, the low-quality latest 300-710 exam torrent may do harmful influence on you which may causes results past redemption. Whether you have experienced that problem or not was history by now. The free demos do honor to the perfection of our latest 300-710 exam torrent, and also a performance of our considerate after sales services. Those demos serve as epitomes of real 300-710 Quiz guides for your reference. In our demos, some examples or question points were enumerated as some representatives of our 300-710 test prep. How convenient and awesome of it!

Cisco 300-710 Exam Overview:

Certification Vendor:	Cisco
Exam Name:	Securing Networks with Cisco Firepower
Exam Number:	300-710 SNCF
Certificate Validity Period:	3 years
Passing Score:	Not publicly disclosed / Approx 750–850 (scale 1000)
Exam Format:	Multiple choice, Simulation, Drag and drop
Real Exam Qty:	55–65
Exam Price:	USD 300
Exam Duration:	90 minutes
Related Certifications:	CCIE Security Cisco Certified Specialist – Network Security Firepower
Available Languages:	English, Japanese
Recommended Training:	Cisco Secure Firewall Management and Configuration Securing Networks with Cisco Firepower (SFWIPA) v1.1

Exam Registration:	Pearson VUE Registration
Sample Questions:	Cisco 300-710 Sample Questions
Exam Way:	Online proctored or Onsite at Pearson VUE test centers
Pre Condition:	No mandatory prerequisites; recommended knowledge: CCNA Security or equivalent experience, understanding of network security protocols and firewall technologies
Official Syllabus URL:	https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/300-710-sncf.html

300-710 Exam Course, Pdf 300-710 Torrent

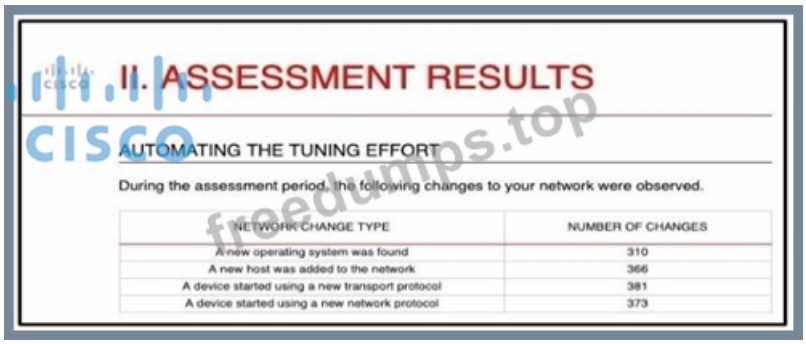
The FreeDumps acknowledges that Cisco aspirants are continuously juggling a couple of responsibilities, so 300-710 questions are ideal for short practise. Candidates can access those questions everywhere and at any time, the usage of any clever device, which allows them to examine at their very own tempo. The 300-710 Questions are portable and you can also print them.

Passing the Cisco 300-710 exam is an excellent way for professionals to demonstrate their expertise in network security and their ability to implement effective security solutions using Cisco Firepower. Securing Networks with Cisco Firepower certification also provides a competitive edge in the job market, as it is highly valued by employers. Candidates who pass the exam will receive the Cisco Certified Network Professional Security (CCNP Security) certification, which is recognized worldwide as a mark of excellence in network security.

Cisco 300-710 Certification Exam is a challenging and rigorous exam that requires a deep understanding of Cisco Firepower NGFW technology. Candidates must have a strong understanding of network security concepts, as well as experience working with Cisco Firepower technology. Passing this certification exam demonstrates a high level of expertise and proficiency in securing network infrastructures using Cisco Firepower technology.

Cisco Securing Networks with Cisco Firepower Sample Questions (Q33-Q38):

NEW QUESTION # 33
Refer to the exhibit.



And engineer is analyzing the Attacks Risk Report and finds that there are over 300 instances of new operating systems being seen on the network How is the Firepower configuration updated to protect these new operating systems?

- A. Cisco Firepower automatically updates the policies.
- B. The administrator manually updates the policies.
- C. The administrator requests a Remediation Recommendation Report from Cisco Firepower
- D. Cisco Firepower gives recommendations to update the policies.

Answer: D

Explanation:
Ref: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailoring_Intrusion_Protection_to_Your_Network_Assets.html

NEW QUESTION # 34
Which command is entered in the Cisco FMC CLI to generate a troubleshooting file?

- A. show tech-support chassis
- B. show running-config
- C. sudo sf_troubleshoot.pl
- D. system support diagnostic-cli

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

NEW QUESTION # 35
Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?

- A. base
- B. mobility
- C. apex
- D. plus

Answer: A

Explanation:
Only base licensing is required for pxGrid integration. You can use PassiveID with just base licensing which passes that onto the FMC through pxGrid. If you want to use context sharing and Rapid Threat Containment, THEN you need Plus licensing.
https://www.routexp.com/2017/11/cisco-ise-base-plus-and-apex-licenses.html

NEW QUESTION # 36
Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

- A. configure manager local 10.0.0.10 Cisco123
- B. configure manager add 10.0.0.10 Cisco123
- C. configure manager local Cisco123 10.0.0.10
- D. configure manager add Cisco123 10.0.0.10

Answer: B

Explanation:
Section: Configuration
Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

NEW QUESTION # 37
A network administrator wants to configure a Cisco Secure Firewall Threat Defense instance managed by Cisco Secure Firewall Management Center to block traffic to known cryptomining networks. Which system settings must the administrator configure in Secure Firewall Management Center to meet the requirement?

- A. Access Policy, Rules
- B. Access Policy, Security Intelligence
- C. Intrusion Policy, Security Intelligence
- D. Malware Policy, Rules

Answer: B

Explanation:
To block traffic to known cryptomining networks using Cisco Secure Firewall Threat Defense (FTD) managed by Cisco Secure

Firewall Management Center (FMC), the network administrator needs to configure Security Intelligence in an Access Control Policy. Security Intelligence allows administrators to block traffic based on threat intelligence feeds, which include known malicious IP addresses, domains, and URLs.
Steps:
Navigate to Policies > Access Control > Access Control Policy in FMC.
Edit or create an Access Control Policy.
Go to the Security Intelligence tab.
Enable the relevant threat intelligence feeds that include cryptomining networks.
Apply the policy to the FTD device.
This configuration ensures that traffic to known cryptomining networks is blocked, enhancing the network's security posture against cryptomining threats.

NEW QUESTION # 38
......