FCP_FGT_AD-7.6시험준비공부 - FCP_FGT_AD-7.6인증시험인기덤프문제

Fast2test의Fortinet인증 FCP_FGT_AD-7.6시험대비 덤프는 가격이 착한데 비하면 품질이 너무 좋은 시험전 공부자료입니다. 시험문제적중율이 높아 패스율이 100%에 이르고 있습니다.다른 IT자격증에 관심이 있는 분들은 온라인서비스에 문의하여 덤프유무와 적중율등을 확인할수 있습니다. Fortinet인증 FCP_FGT_AD-7.6덤프로 어려운 시험을 정복하여 IT업계 정상에 오릅시다.

Fortinet FCP_FGT_AD-7.6 시험요강:

주제	소개
주제 1	• Deployment and system configuration: This section of the exam measures the skills of network security engineers and covers essential tasks for setting up a FortiGate device in a production environment. Candidates are expected to perform the initial configuration, establish basic connectivity, and integrate the device within the Fortinet Security Fabric. They must also be able to configure a FortiGate Cluster Protocol (FGCP) high availability setup and troubleshoot resource and connectivity issues to ensure system readiness and network uptime.
주제 2	• Firewall policies and authentication: This section of the exam measures the skills of firewall administrators and covers the implementation and management of security policies. It involves configuring basic and advanced firewall rules, applying Source NAT (SNAT) and Destination NAT (DNAT) options, and enforcing various firewall authentication methods. The section also includes deploying and configuring Fortinet Single Sign-On (FSSO) to streamline user access across the network.
주제 3	• Content inspection: This section of the exam measures the skills of network security engineers and covers the setup and management of content inspection features on FortiGate. Candidates must demonstrate an understanding of encrypted traffic inspection using digital certificates, identify and apply FortiGate inspection modes, and configure web filtering policies. The ability to implement application control for monitoring and regulating network application usage, configure antivirus profiles to detect and block malware, and set up Intrusion Prevention Systems (IPS) to shield the network from threats and vulnerabilities is also assessed.
주제 4	• VPN: This section of the exam measures the skills of network security engineers and covers the configuration and deployment of Virtual Private Network (VPN) solutions. Candidates are required to implement SSL VPNs to grant secure remote access to internal resources and configure IPsec VPNs in either meshed or partially redundant topologies to ensure encrypted communication between distributed network locations.
주제 5	• Routing: This section of the exam measures the skills of firewall administrators and covers the configuration of routing features on FortiGate devices. It includes defining and applying static routes for directing traffic within and outside the network, as well as setting up Software-Defined WAN (SD-WAN) to distribute and balance traffic loads across multiple WAN connections efficiently.

시험패스에 유효한 FCP_FGT_AD-7.6시험준비공부 최신버전 덤프샘플문제 다운

Fortinet인증 FCP_FGT_AD-7.6시험을 한방에 편하게 통과하여 자격증을 취득하려면 시험전 공부가이드가 필수입니다. Fast2test에서 연구제작한 Fortinet인증 FCP_FGT_AD-7.6덤프는Fortinet인증 FCP_FGT_AD-7.6시험을 패스하는데 가장 좋은 시험준비 공부자료입니다. Fast2test덤프공부자료는 엘리트한 IT전문자들이 자신의 노하우와 경험으로 최선을 다해 연구제작한 결과물입니다.IT인증자격증을 취득하려는 분들의 곁은Fast2test가 지켜드립니다.

최신 Network Security FCP_FGT_AD-7.6 무료샘플문제 (Q90-Q95):

질문 # 90
Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

- A. The subject field in the server certificate.
- B. The subject alternative name (SAN) field in the server certificate.
- C. The serial number in the server certificate.
- D. The host field in the HTTP header.
- E. The server name indication (SNI) extension in the client hello message.

정답： A,B,E

설명:
When SSL certificate inspection is enabled on a FortiGate device, the system uses the following three pieces of information to identify the hostname of the SSL server:
* Server Name Indication (SNI) extension in the client hello message (B): The SNI is an extension in the client hello message of the SSL/TLS protocol. It indicates the hostname the client is attempting to connect to. This allows FortiGate to identify the server's hostname during the SSL handshake.
* Subject Alternative Name (SAN) field in the server certificate (C): The SAN field in the server certificate lists additional hostnames or IP addresses that the certificate is valid for. FortiGate inspects this field to confirm the identity of the server.
* Subject field in the server certificate (D): The Subject field contains the primary hostname or domain name for which the certificate was issued. FortiGate uses this information to match and validate the server's identity during SSL certificate inspection.
The other options are not used in SSL certificate inspection for hostname identification:
* Host field in the HTTP header (A): This is part of the HTTP request, not the SSL handshake, and is not used for SSL certificate inspection.
* Serial number in the server certificate (E): The serial number is used for certificate management and revocation, not for hostname identification.
References
* FortiOS 7.4.1 Administration Guide - SSL/SSH Inspection, page 1802.
* FortiOS 7.4.1 Administration Guide - Configuring SSL/SSH Inspection Profile, page 1799.

질문 # 91
What are two features of collector agent advanced mode? (Choose two.)

- A. Advanced mode supports nested or inherited groups.
- B. Advanced mode uses the Windows convention -NetBios: Domain\Username.
- C. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
- D. In advanced mode, security profiles can be applied only to user groups, not individual users.

정답： A,C

설명:
Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups.

In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent.

질문 # 92
Refer to the exhibit.

Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
Implicit 1										
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

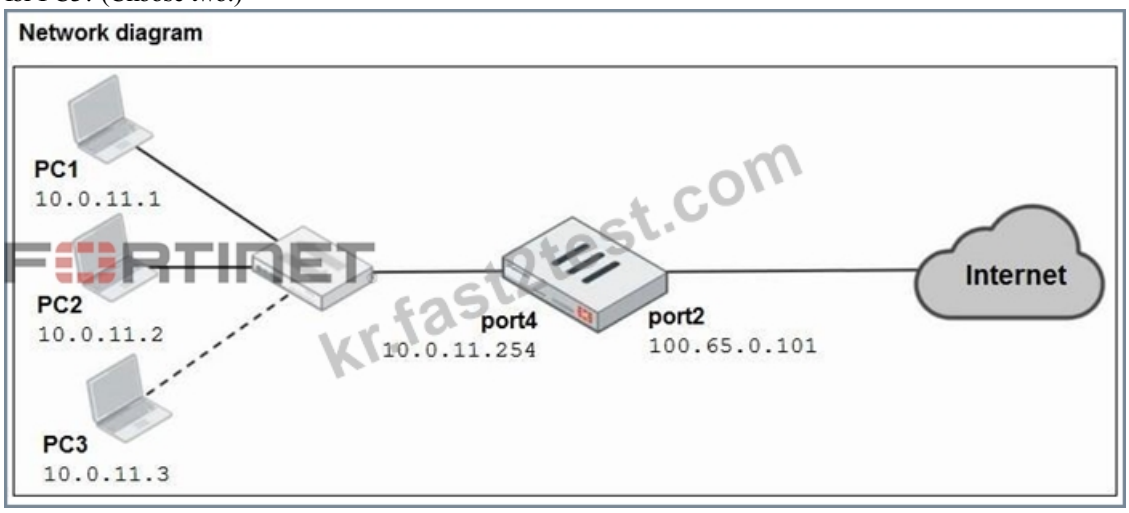
Which statement about this firewall policy list is true?

- A. The firewall policies are listed by ingress and egress interfaces pairing view.
- B. LAN to WAN, WAN to LAN, and Implicit are sequence grouping view lists.
- C. The Implicit group can include more than one deny firewall policy.
- D. The firewall policies are listed by ID sequence view.

정답： B

설명:
The firewall policy list shown is displayed in the sequence grouping view, where policies are grouped based on their traffic direction - such as LAN to WAN, WAN to LAN, and Implicit. This view helps administrators quickly identify and manage policies according to their interface pairings and logical traffic flow, rather than by numerical ID order.

질문 # 93
Refer to the exhibits. The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device.
Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.
Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)



- A. In the IP pool configuration, set typeto overload.
- B. In the firewall policy, set match-vipto enableusing CLI.
- C. In the IP pool configuration, set endipto 100.65.0.112.
- D. In the system settings, set Multiple Interface Policies to enable.

정답： A,C

설명:
The IP pool is configured as One-to-One with a range of only 100.65.0.110-100.65.0.111, which allows NAT for only two internal hosts (PC1 and PC2). When PC3 tries to access the internet, no external IP is available for mapping.
To fix this:
- Change the IP pool type to Overload, allowing multiple internal IPs to share a single external IP.
- Expand the IP pool range by setting endip to 100.65.0.112 (or more) so that additional internal hosts (like PC3) can also be assigned a unique external IP.

질문 # 94
Which two statements are true about an HA cluster? (Choose two.)

- A. Link failover triggers a failover if the administrator sets the interface down on the primary device.
- B. An HA cluster cannot have both in-band and out-of-band management interfaces at the same time.
- C. HA incremental synchronization includes FIB entries and IPsec SAs.
- D. When sniffing the heartbeat interface, the administrator must see the IP address 169.254.0.2.

정답: A,C

설명:
Setting an interface down on the primary device triggers a failover due to link failover detection.
HA incremental synchronization includes forwarding information base (FIB) entries and IPsec security associations (SAs) to maintain session continuity.

질문 # 95
.....

- **시험대비 FCP_FGT_AD-7.6시험준비공부 덤프데모문제 □ 지금□ www.koreadumps.com □을(를) 열고 무료 다운로드를 위해【 FCP_FGT_AD-7.6 】를 검색하십시오FCP_FGT_AD-7.6퍼펙트 덤프데모**
- github.com, myportal.utt.edu.tt, shortcourses.russellcollege.edu.au, www.stes.tyc.edu.tw, www.dkcomposite.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes