

Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 Administrator

https://www.2passeasy.com/dumps/FCSS_SASE_AD-23/



NEW QUESTION 1

A customer wants to upgrade their legacy on-premises proxy to a cloud-based proxy for a hybrid network. Which FortiSASE features would help the customer to achieve this outcome?

- A. SD-WAN and NGFW
- B. SD-WAN and inline-CASB
- C. zero trust network access (ZTNA) and next generation firewall (NGFW)
- D. secure web gateway (SWG) and inline-CASB

Answer: D

Explanation:

For a customer looking to upgrade their legacy on-premises proxy to a cloud-based proxy for a hybrid network, the combination of Secure Web Gateway (SWG) and Inline Cloud Access Security Broker (CASB) features in FortiSASE will provide the necessary capabilities.

? Secure Web Gateway (SWG):

? Inline Cloud Access Security Broker (CASB):

References:

? FortiOS 7.2 Administration Guide: Details on SWG and CASB features.

? FortiSASE 23.2 Documentation: Explains how SWG and inline-CASB are used in cloud-based proxy solutions.

NEW QUESTION 2

How does FortiSASE hide user information when viewing and analyzing logs?

- A. By hashing data using Blowfish
- B. By hashing data using salt
- C. By encrypting data using Secure Hash Algorithm 256-bit (SHA-256)
- D. By encrypting data using advanced encryption standard (AES)

Answer: B

Explanation:

FortiSASE hides user information when viewing and analyzing logs by hashing data using salt. This approach ensures that sensitive user information is obfuscated, enhancing privacy and security.

? Hashing Data with Salt:

? Security and Privacy:

References:

? FortiOS 7.2 Administration Guide: Provides information on log management and data protection techniques.

? FortiSASE 23.2 Documentation: Details on how FortiSASE implements data hashing and salting to secure user information in logs.

NEW QUESTION 3

Which two components are part of onboarding a secure web gateway (SWG) endpoint? (Choose two)

- A. FortiSASE CA certificate
- B. proxy auto-configuration (PAC) file
- C. FortiSASE invitation code
- D. FortiClient installer

Answer: AB

Explanation:

Onboarding a Secure Web Gateway (SWG) endpoint involves several components to ensure secure and effective integration with FortiSASE. Two key components are the FortiSASE CA certificate and the proxy auto-configuration (PAC) file.

? FortiSASE CA Certificate:

? Proxy Auto-Configuration (PAC) File:

References:

? FortiOS 7.2 Administration Guide: Details on onboarding endpoints and configuring SWG.

? FortiSASE 23.2 Documentation: Explains the components required for integrating endpoints with FortiSASE and the process for deploying the CA certificate and PAC file.

NEW QUESTION 4

Refer to the exhibit.



In the user connection monitor, the FortiSASE administrator notices the user name is showing random characters. Which configuration change must the administrator make to get proper user information?

- A. Turn off log anonymization on FortiSASE.
- B. Add more endpoint licenses on FortiSASE.

- C. Configure the username using FortiSASE naming convention.
- D. Change the deployment type from SWG to VPN.

Answer: A

Explanation:

In the user connection monitor, the random characters shown for the username indicate that log anonymization is enabled. Log anonymization is a feature that hides the actual user information in the logs for privacy and security reasons. To display proper user information, you need to disable log anonymization.

? Log Anonymization:

? Disabling Log Anonymization:

References:

? FortiSASE 23.2 Documentation: Provides detailed steps on enabling and disabling log anonymization.

? Fortinet Knowledge Base: Explains the impact of log anonymization on user monitoring and logging.

NEW QUESTION 5

When you configure FortiSASE Secure Private Access (SPA) with SD-WAN integration, you must establish a routing adjacency between FortiSASE and the FortiGate SD-WAN hub. Which routing protocol must you use?

- A. BGP
- B. IS-IS
- C. OSPF
- D. EIGRP

Answer: A

Explanation:

When configuring FortiSASE Secure Private Access (SPA) with SD-WAN integration, establishing a routing adjacency between FortiSASE and the FortiGate SD-WAN hub requires the use of the Border Gateway Protocol (BGP).

? BGP (Border Gateway Protocol):

? Routing Adjacency:

References:

? FortiOS 7.2 Administration Guide: Provides information on configuring BGP for SD-WAN integration.

? FortiSASE 23.2 Documentation: Details on setting up routing adjacencies using BGP for Secure Private Access with SD-WAN.

NEW QUESTION 6

Which two additional components does FortiSASE use for application control to act as an inline-CASB? (Choose two.)

- A. intrusion prevention system (IPS)
- B. SSL deep inspection
- C. DNS filter
- D. Web filter with inline-CASB

Answer: BD

Explanation:

FortiSASE uses the following components for application control to act as an inline-CASB (Cloud Access Security Broker):

? SSL Deep Inspection:

? Web Filter with Inline-CASB:

References:

? FortiOS 7.2 Administration Guide: Details on SSL deep inspection and web filtering configurations.

? FortiSASE 23.2 Documentation: Explains how FortiSASE acts as an inline-CASB using SSL deep inspection and web filtering.

NEW QUESTION 7

Which FortiSASE feature ensures least-privileged user access to all applications?

- A. secure web gateway (SWG)
- B. SD-WAN
- C. zero trust network access (ZTNA)
- D. thin branch SASE extension

Answer: C

Explanation:

Zero Trust Network Access (ZTNA) is the FortiSASE feature that ensures least-privileged user access to all applications. ZTNA operates on the principle of "never trust, always verify," providing secure access based on the identity of users and devices, regardless of their location.

? Zero Trust Network Access (ZTNA):

? Implementation:

References:

? FortiOS 7.2 Administration Guide: Provides detailed information on ZTNA and its role in ensuring least-privileged access.

? FortiSASE 23.2 Documentation: Explains the implementation and benefits of ZTNA within the FortiSASE environment.

NEW QUESTION 8

An organization wants to block all video and audio application traffic but grant access to videos from CNN Which application override action must you configure in the Application Control with Inline-CASB?

- A. Allow
- B. Pass
- C. Permit
- D. Exempt

Answer: D

Explanation:

? Application Control Configuration:

? Blocking Video and Audio Applications:

? Granting Access to Specific Videos (CNN):

? Configuration Steps:

References:

? FortiOS 7.2 Administration Guide: Detailed steps on configuring Application Control and Inline-CASB.

? Fortinet Training Institute: Provides scenarios and examples of using Application Control with Inline-CASB for specific use cases.

NEW QUESTION 9

What are two advantages of using zero-trust tags? (Choose two.)

A. Zero-trust tags can be used to allow or deny access to network resources

B. Zero-trust tags can determine the security posture of an endpoint.

C. Zero-trust tags can be used to create multiple endpoint profiles which can be applied to different endpoints

D. Zero-trust tags can be used to allow secure web gateway (SWG) access

Answer: AB

Explanation:

Zero-trust tags are critical in implementing zero-trust network access (ZTNA) policies. Here are the two key advantages of using zero-trust tags:

? Access Control (Allow or Deny):

? Determining Security Posture:

References:

? FortiOS 7.2 Administration Guide: Provides detailed information on configuring and using zero-trust tags for access control and security posture assessment.

? FortiSASE 23.2 Documentation: Explains how zero-trust tags are implemented and used within the FortiSASE environment for enhancing security and compliance.

NEW QUESTION 10

An organization needs to resolve internal hostnames using its internal rather than public DNS servers for remotely connected endpoints. Which two components must be configured on FortiSASE to achieve this? (Choose two.)

A. SSL deep inspection

B. Split DNS rules

C. Split tunnelling destinations

D. DNS filter

Answer: BC

Explanation:

To resolve internal hostnames using internal DNS servers for remotely connected endpoints, the following two components must be configured on FortiSASE:

? Split DNS Rules:

? Split Tunneling Destinations:

References:

? FortiOS 7.2 Administration Guide: Provides details on configuring split DNS and split tunneling for VPN clients.

? FortiSASE 23.2 Documentation: Explains the implementation and configuration of split DNS and split tunneling for securely resolving internal hostnames.

NEW QUESTION 10

When deploying FortiSASE agent-based clients, which three features are available compared to an agentless solution? (Choose three.)

A. Vulnerability scan

B. SSL inspection

C. Anti-ransomware protection

D. Web filter

E. ZTNA tags

Answer: ABD

Explanation:

When deploying FortiSASE agent-based clients, several features are available that are not typically available with an agentless solution. These features enhance the security and management capabilities for endpoints.

? Vulnerability Scan:

? SSL Inspection:

? Web Filter:

References:

? FortiOS 7.2 Administration Guide: Explains the features and benefits of deploying agent-based clients.

? FortiSASE 23.2 Documentation: Details the differences between agent-based and agentless solutions and the additional features provided by agent-based deployments.

NEW QUESTION 12

Refer to the exhibits.

Secure private access service connection

Name	To_FortiGate	X
Remote Gateway	203.221.196.6	X
Authentication Method	Pre-shared Key Certificate	
BGP Peer IP	10.1111.1	X
Network Overlay ID	100	X

Secure private access network connection

Service Connections Network Configuration

SECURE PRIVATE ACCESS NETWORK CONFIGURATION

BGP Routing Design	BGP per overlay BGP on loopback
BGP Router ID Subnet	10.12.11.0/24 X
Autonomous System Number (ASN)	65001 X
BGP Recursive Routing	<input type="checkbox"/>
Hub Selection Method	Hub Health and Priority BGP MED

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

i Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.

Health Check IP	10.1.0.254 X
-----------------	--------------

Firewall policy configuration

```
config firewall policy
  edit 5
    set name "Spoke-to-Spoke"
    set uuid 4d949462-216b-51ee-03c7-d0662fdf9451
    set srcintf "To_SASE"
    set dstintf "To_SASE"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set comments "VPN: To_SASE (Created by VPN wizard)"
  next
  edit 6
    set name "Lo-BGP-HC"
    set uuid f5a12c92-216b-51ee-4802-80cd013d6acf
    set srcintf "To_SASE"
    set dstintf "SASE_Health"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
  next
  edit 9
    set name "Spoke-to-Hub"
    set uuid 617b81ee-cc64-51ee-8da6-6cdf3ca2cca
    set srcintf "To_SASE"
    set dstintf "internal3"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
  next
end
```

IPsec VPN configuration

```
# show vpn ipsec phase1-interface To_SASE
config vpn ipsec phase1-interface
  edit "To_SASE"
    set type dynamic
    set interface "wan1"
    set peertype any
    set net-device disable
    set mode-cfg enable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set add-route disable
    set dpd on-idle
    set comments "VPN: To_SASE (Created by VPN wizard)"
    set wizard-type hub-fortigate-auto-discovery
    set auto-discovery-sender enable
    set ipv4-start-ip 10.11.11.10
    set ipv4-end-ip 10.11.11.200
    set ipv4-netmask 255.255.255.0
    set unity-support disable
    set psksecret ENC Sbl0igpvIFFYSpRZ/hyxQVUXv9NZm7uq1tD9v+BViPd+7RWizmUA3ZINn0zbsxq70F
iYkPLkxanwIo7VLiipkye1xt84NAwEfm5jTqqf1dMj/phYvBI3hzU0yXq==
  next
end

# show vpn ipsec phase2-interface To_SASE
config vpn ipsec phase2-interface
  edit "To_SASE"
    set phase1name "To_SASE"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
    set comments "VPN: To_SASE (Created by VPN wizard)"
  next
end
```

BGP protocol configuration

```
#config router bgp
  set as 65001
  set router-id 10.1.0.254
  config neighbor
    edit "10.10.1.3"
      set advertisement-interval 1
      set ebgp-enforce-multihop enable
      set link-down-failover enable
      set remote-as 65001
      set route-reflector-client enable
    next
  end
  config neighbor-group
    edit "To_SASE"
      set capability-graceful-restart enable
      set link-down-failover enable
      set next-hop-self enable
      set interface "To_SASE"
      set remote-as 65001
      set additional-path both
      set adv-additional-path 4
      set route-reflector-client enable
    next
  end
  config neighbor-range
    edit 1
      set prefix 10.11.11.0 255.255.255.0
      set neighbor-group "To_SASE"
    next
  end
  config network
    edit 1
      set prefix 10.190.190.0 255.255.255.0
    next
  end
```

A FortiSASE administrator is trying to configure FortiSASE as a spoke to a FortiGate hub. The VPN tunnel does not establish. Based on the provided configuration, what configuration needs to be modified to bring the tunnel up?

- A. NAT needs to be enabled in the Spoke-to-Hub firewall policy.
- B. The BGP router ID needs to match on the hub and FortiSASE.
- C. FortiSASE spoke devices do not support mode config.
- D. The hub needs IKEv2 enabled in the IPsec phase 1 settings.

Answer: C

Explanation:

The VPN tunnel between the FortiSASE spoke and the FortiGate hub is not establishing due to the configuration of mode config, which is not supported by FortiSASE spoke devices. Mode config is used to assign IP addresses to VPN clients dynamically, but this feature is not applicable to FortiSASE spokes.

? Mode Config in IPsec:

? Configuration Adjustment:

? Steps to Disable Mode Config:

References:

? FortiOS 7.2 Administration Guide: Provides details on configuring IPsec VPNs and mode config settings.

? FortiSASE 23.2 Documentation: Explains the supported configurations for FortiSASE spoke devices and VPN setups.

NEW QUESTION 16
Refer to the exhibit.

Security Logs

Log Details

Destination

Destination IP	151.101.40.81
Destination Port	443
Destination Country/Region	United States
Traffic Type	Internet Access
Destination UUID	4a501662-f85f-51ed-5194-7e45b3d369cd
Hostname	www.bbc.com
URL	https://www.bbc.com/

Application Control

Action

Action	Blocked
Threat	16,777,216
Policy ID	8
Policy UUID	7d56f000-b41e-51ee-f96b-d0b4d9fb3c2b
Policy Type	policy

Security

Web Filter

Profile Group	SIA (Internet Access)
Request Type	direct
Direction	incoming
Banned Word	fight
Message	URL was blocked because it contained banned word(s).

To allow access, which web filter configuration must you change on FortiSASE?

- A. FortiGuard category-based filter
- B. content filter
- C. URL Filter
- D. inline cloud access security broker (CASB) headers

Answer: C

Explanation:

The exhibit indicates that the URL <https://www.bbc.com/> is being blocked due to containing a banned word ("fight"). To allow access to this specific URL, you need to adjust the URL filter settings on FortiSASE.

? URL Filtering:

? Modifying URL Filter:

References:

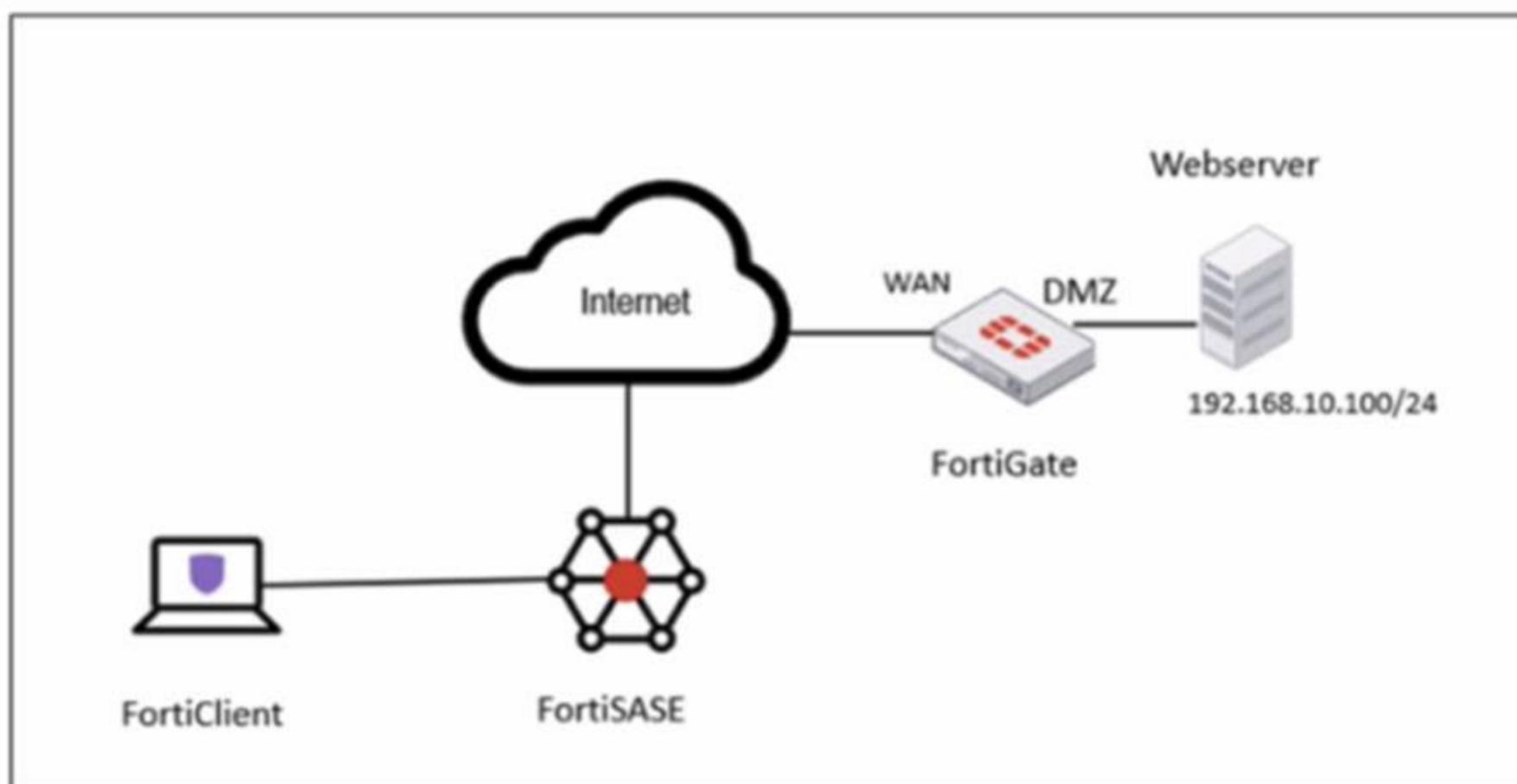
? FortiOS 7.2 Administration Guide: Provides details on configuring and managing URL filters.

? FortiSASE 23.2 Documentation: Explains how to set up and modify web filtering policies, including URL filters.

NEW QUESTION 17

Refer to the exhibits.

Network diagram



VPN tunnel diagnose output on FortiGate Hub

```
# diagnose vpn tunnel list name SASE_0
list ipsec tunnel by names in vd 0
-----
name=SASE_0 ver=2 serial=14 172.16.10.101:4500->172.16.10.1:64916 tun_id=10.11.11.10 tun_id6=::10.0.0.18 dst_mtu=150
bound_if=6 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74664 options[123a8]=npu rgwy-chg rport-chg frag-rtc
d=100

parent=SASE index=0
proxyid_num=1 child_num=0 refcnt=7 ilast=0 olast=0 ad=s/1
stat: rxp=1667 txp=4583 rxb=278576 txb=108695
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=keepalive draft=0 interval=10 remote_port=64916
fec: egress=0 ingress=0
proxyid=SASE proto=0 sa=1 ref=4 serial=1 ads
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:0.0.0.0-255.255.255.255:0
SA: ref=6 options=a26 type=00 soft=0 mtu=1422 expire=42025/00 replaywin=1024
seqno=11cf esn=0 replaywin_lastseq=00000680 qat=0 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=43188/43200
dec: spi=603df878 esp=aes key=16 2e8932908987c1fdeed9242673bc76f5
ah=sha1 key=20 01b6c2a13e6cff22796e428c5fb4e4c5262b1a71
enc: spi=f16ce4a1 esp=aes key=16 90dce5d608caf2714a4f84cff482b557
ah=sha1 key=20 b60cd0c39489a9f509fe720c0c8e36bb9206f824
dec:pkts/bytes=3/120, enc:pkts/bytes=2509/285776
npu_flag=03 npu_rgwy=172.16.10.1 npu_lgwy=172.16.10.101 npu_selid=11 dec_npuid=1 enc_npuid=1
```

Secure Private Access policy on FortiSASE

Name	Allow-All Private Traffic
Source Scope	All VPN Users Edge Device
Source	All Traffic Specify
User	All VPN Users Specify
Destination	Private Access Traffic Specify
Service	ALL_ICMP +
Profile Group	Default Specify
Force Certificate Inspection	<input type="checkbox"/>
Action	Accept Deny
Status	Enable Disable
Logging Options	
Log Allowed Traffic	<input checked="" type="checkbox"/> Security Events All Sessions

BGP route information on FortiSASE

Learned BGP Routes		
+ Q Search		
Prefix	Next Hop	Learned From
10.12.11.4/32	0.0.0.0	0.0.0.0
10.12.11.1/32	10.11.11.10	10.11.11.1
10.12.11.2/32	10.11.11.11	10.11.11.1
10.12.11.3/32	10.11.11.12	10.11.11.1
192.168.1.0/24	10.11.11.1	10.11.11.1

Firewall policies on FortiGate Hub

```
# show firewall policy | grep -f SASE
config firewall policy
  edit 5
    set name "vpn_SASE_spoke2hub_0"
    set uuid 01ba85f2-d45c-51ee-5ff9-2035aa36cb3f
    set srcintf "SASE"
    set dstintf "dmz"
    set action accept
    set srcaddr "all"
    set dstaddr "SASE_local"
    set schedule "always"
    set service "ALL"
    set comments "VPN: SASE (Created by VPN wizard)"
  next
  edit 9
    set name "vpn_SASE_spoke2spoke_0"
    set uuid 01eb72ca-d45c-51ee-bd83-bd2feb606cb6
    set srcintf "SASE"
    set dstintf "SASE"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set comments "VPN: SASE (Created by VPN wizard)"
  next
  edit 10
    set name "SASE Health Check"
    set uuid b9573f5c-d45c-51ee-bc11-d5a3143f082a
    set srcintf "SASE"
    set dstintf "SASE_Health"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
  next
end
```

A FortiSASE administrator is trying to configure FortiSASE as a spoke to a FortiGate hub. The tunnel is up to the FortiGate hub. However, the administrator is not able to ping the webserver hosted behind the FortiGate hub. Based on the output, what is the reason for the ping failures?

- A. The Secure Private Access (SPA) policy needs to allow PING service.
- B. Quick mode selectors are restricting the subnet.
- C. The BGP route is not received.
- D. Network address translation (NAT) is not enabled on the spoke-to-hub policy.

Answer: B

Explanation:

The reason for the ping failures is due to the quick mode selectors restricting the subnet. Quick mode selectors define the IP ranges and protocols that are allowed through the VPN tunnel, and if they are not configured correctly, traffic to certain subnets can be blocked.

? Quick Mode Selectors:

? Diagnostic Output:

? Configuration Check:

References:

- ? FortiOS 7.2 Administration Guide: Provides detailed information on configuring VPN tunnels and quick mode selectors.
- ? FortiSASE 23.2 Documentation: Explains how to set up and manage VPN tunnels, including the configuration of quick mode selectors.

NEW QUESTION 22

When accessing the FortiSASE portal for the first time, an administrator must select data center locations for which three FortiSASE components? (Choose three.)

- A. Endpoint management
- B. Points of presence
- C. SD-WAN hub
- D. Logging
- E. Authentication

Answer: ABD

Explanation:

When accessing the FortiSASE portal for the first time, an administrator must select data center locations for the following FortiSASE components:

- ? Endpoint Management:
- ? Points of Presence (PoPs):
- ? Logging:

References:

- ? FortiOS 7.2 Administration Guide: Details on initial setup and configuration steps for FortiSASE.
- ? FortiSASE 23.2 Documentation: Explains the importance of selecting data center locations for various FortiSASE components.

NEW QUESTION 25

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_SASE_AD-23 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_SASE_AD-23 Product From:

https://www.2passeasy.com/dumps/FCSS_SASE_AD-23/

Money Back Guarantee

FCSS_SASE_AD-23 Practice Exam Features:

- * FCSS_SASE_AD-23 Questions and Answers Updated Frequently
- * FCSS_SASE_AD-23 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_SASE_AD-23 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCSS_SASE_AD-23 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year