

Fortinet

Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 Administrator



NEW QUESTION 1

To complete their day-to-day operations, remote users require access to a TCP-based application that is hosted on a private web server. Which FortiSASE deployment use case provides the most efficient and secure method for meeting the remote users' requirements?

- A. SD-WAN private access
- B. inline-CASB
- C. zero trust network access (ZTNA) private access
- D. next generation firewall (NGFW)

Answer: C

Explanation:

Zero Trust Network Access (ZTNA) private access provides the most efficient and secure method for remote users to access a TCP-based application hosted on a private web server. ZTNA ensures that only authenticated and authorized users can access specific applications based on predefined policies, enhancing security and access control.

? Zero Trust Network Access (ZTNA):

? Secure and Efficient Access:

References:

? FortiOS 7.2 Administration Guide: Provides detailed information on ZTNA and its deployment use cases.

? FortiSASE 23.2 Documentation: Explains how ZTNA can be used to provide secure access to private applications for remote users.

NEW QUESTION 2

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 3

Refer to the exhibits.

Managed Endpoints

Endpoint	VPN Username	Management Connection	ZTNA Tags (Simple)	FortiClient Version	Vulnerabilities Detected
Win10-Pro	use2@fortinettraining.lab	Online	FortiSASE-Compliant	7.0.10.0538	140
Win7-Pro	use1@fortinettraining.lab	Online	FortiSASE-Non-Compliant, FortiSASE-Compliant	7.0.8.0427	176

Secure Internet Access Policy

+ Create Edit Delete Search						
<input type="checkbox"/>	Name	Profile Group	Source	User	Destination	Action
<input type="checkbox"/>	Botnet Deny		all	All VPN Users	Botnet-C&C Server	Deny
<input type="checkbox"/>	Non-Compliant		FortiSASE-Non-Compliant	All VPN Users	All Internet Traffic	Deny
<input type="checkbox"/>	Web Traffic	SIA	FortiSASE-Compliant	VPN_Users	All Internet Traffic	Accept
<input type="checkbox"/>	Allow-All	Default		All VPN Users	All Internet Traffic	Accept
<input type="checkbox"/>	Implicit Deny		all	All VPN Users	All Internet Traffic	Deny

WiMO-Pro and Win7-Pro are endpoints from the same remote location. WiMO-Pro can access the internet through FortiSASE, while Wm7-Pro can no longer access the internet. Given the exhibits, which reason explains the outage on Wm7-Pro?

- A. The Win7-Pro device posture has changed.
- B. Win7-Pro cannot reach the FortiSASE SSL VPN gateway
- C. The Win7-Pro FortiClient version does not match the FortiSASE endpoint requirement.
- D. Win-7 Pro has exceeded the total vulnerability detected threshold.

Answer: D

Explanation:

Based on the provided exhibits, the reason why the Win7-Pro endpoint can no longer access the internet through FortiSASE is due to exceeding the total vulnerability detected threshold. This threshold is used to determine if a device is compliant with the security requirements to access the network.

? Endpoint Compliance:

? Vulnerability Threshold:

? Impact on Network Access:

References:

? FortiOS 7.2 Administration Guide: Provides information on endpoint compliance and vulnerability management.

? FortiSASE 23.2 Documentation: Explains how vulnerability thresholds are used to determine endpoint compliance and access control.

NEW QUESTION 4

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 5

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 6

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 7

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:

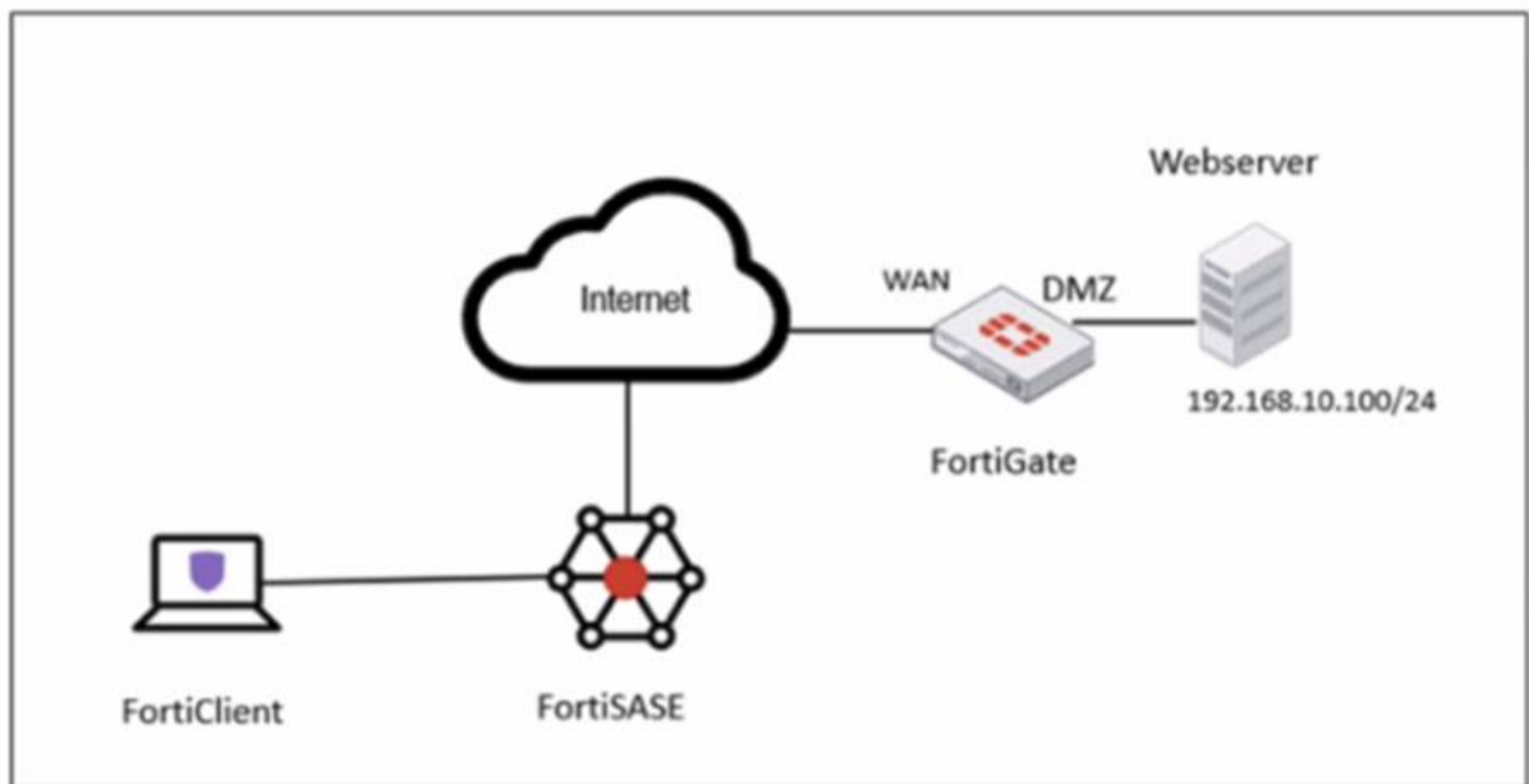
? FortiOS 7.2 Administration Guide: Detailed steps on configuring Application Control and Inline-CASB.

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

NEW QUESTION 8

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=ntf mode=dial_inst/3 encap=none/74664 options[123a8]=npu rgwy-chg rport-chg frag-rfc
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 type="checkbox"/> Security Events All Sessions

BGP route information on FortiSASE

Learned BGP Routes		
<div><div></div><div>Search</div></div>		
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 9

Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles?

- A. It offers hardware-based firewalls for network segmentation.
- B. It integrates with software-defined network (SDN) solutions.
- C. It can identify attributes on the endpoint for security posture check.
- D. It enables VPN connections for remote employees.

Answer: C

Explanation:

FortiSASE supports zero trust network access (ZTNA) principles by identifying attributes on the endpoint for security posture checks. ZTNA principles require continuous verification of user and device credentials, as well as their security posture, before granting access to network resources.

? Security Posture Check:

? Zero Trust Network Access (ZTNA):

References:

? FortiOS 7.2 Administration Guide: Provides information on ZTNA and endpoint security posture checks.

? FortiSASE 23.2 Documentation: Details on how FortiSASE implements ZTNA principles.

NEW QUESTION 10

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_SASE_AD-23 Practice Test Here](#)