**Vendor:** Fortinet

**Exam Code:** NSE7_SSE_AD-25

**Exam Name:** Fortinet NSE 7 - FortiSASE 25 Enterprise Administrator

**Version:** DEMO

**QUESTION 1**
What is the role of ZTNA tags in the FortiSASE Secure Internet Access (SIA) and Secure Private Access (SPA) use cases?

A. ZTNA tags are created to isolate browser sessions in SIA and enforce data loss prevention in SPA for all devices.
B. ZTNA tags determine device posture for non-web traffic protocols and are applied only in agentless deployments for SIA.
C. ZTNA tags determine device posture for endpoints running FortiClient and are used to grant or deny access in SIA or SPA based on that posture.
D. ZTNA tags are applied to unmanaged endpoints without FortiClient to secure HTTP and HTTPS traffic in SIA and SPA.

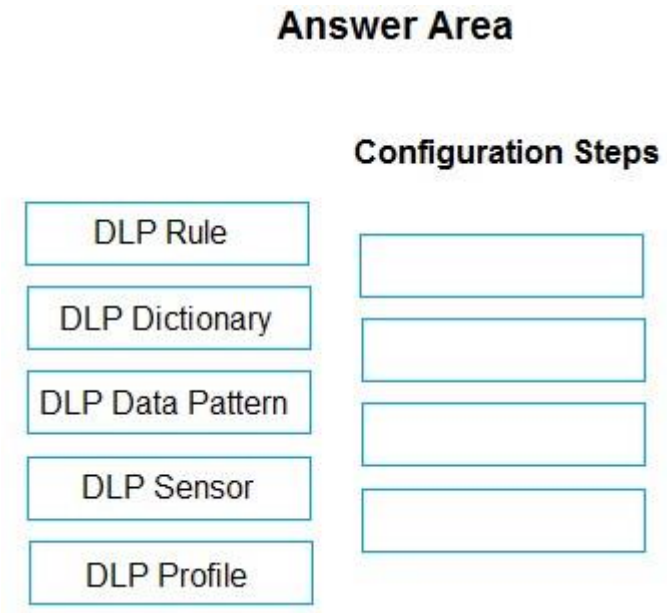
**Answer:** C
**Explanation:**
ZTNA tags represent the security posture of endpoints running FortiClient. They are used in both Secure Internet Access and Secure Private Access to enforce access control by granting or denying access based on the device's compliance with security policies.

**QUESTION 2**
Drag and Drop Question

When configuring the DLP rule in FortiSASE using Regex format, what would be the correct order for the configuration steps?

Select the step in the left column, hold and drag it to a blank position in the column on the right. Place the four correct steps in order, placing the first step in the first position at the top of the column. Once you place a step, you can move it again if you want to change your answer before moving to the next question. You need to drop four steps in the work area.

Select and drag the screen divider to change the viewable area of the source and work areas.




**Answer:**

## Answer Area

### Configuration Steps

DLP Dictionary

DLP Data Pattern

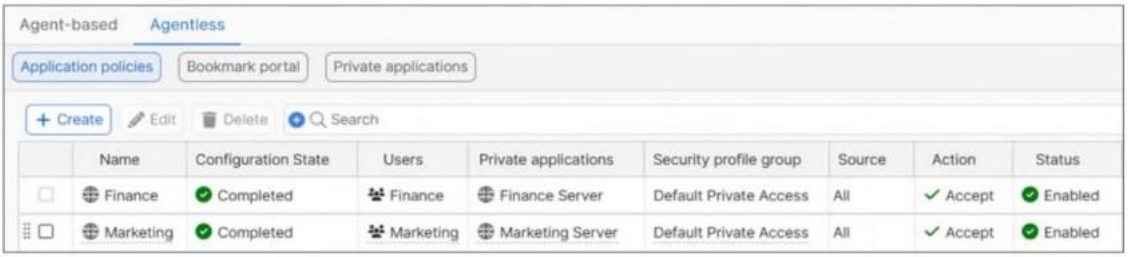
DLP Rule

DLP Sensor

DLP Profile

**Explanation:**
First, you define sensitive information types in a DLP Dictionary, then create the DLP Data Pattern using regex or predefined patterns. Next, you create the DLP Rule that uses the pattern to detect data. The DLP Sensor is then configured to apply the rule to traffic.

**QUESTION 3**
Refer to the exhibit. Which two prerequisites must be met to use the feature shown in the exhibit? (Choose two.)




A. The secure private access (SPA) feature must be configured in FortiSASE.
B. The relevant FortiGate ZTNA application gateway must be configured.
C. FortiClient must be installed on the user's device to access the private application.
D. The proxy and proxy user single sign-on (SSO) features must be configured in FortiSASE.

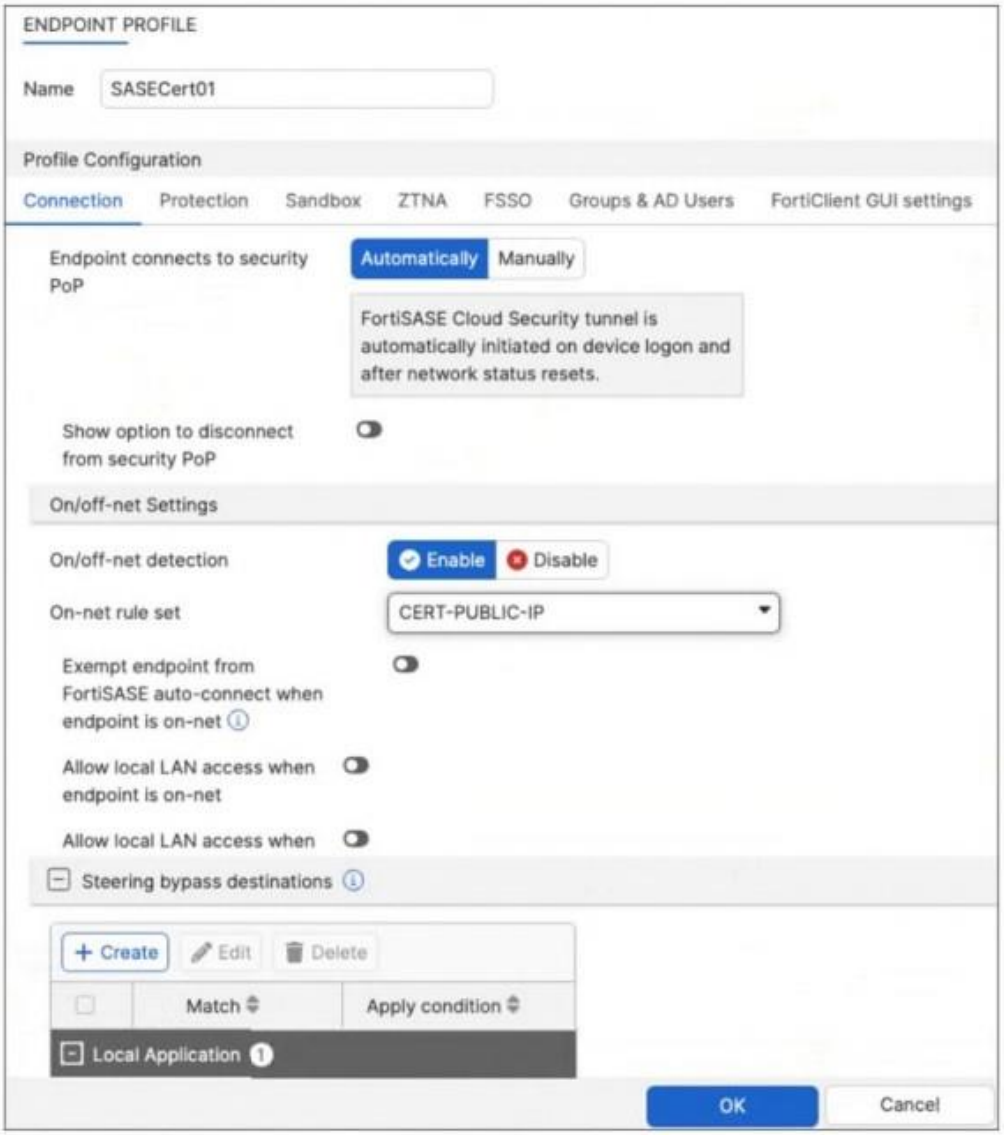
**Answer:** AB
**Explanation:**
To use agentless private application access as shown, the Secure Private Access (SPA) feature must be enabled in FortiSASE, and the relevant FortiGate ZTNA application gateway must be configured to provide access to the private applications. Agentless access does not require FortiClient on the user device, and proxy/SSO configuration is not a prerequisite for this feature.

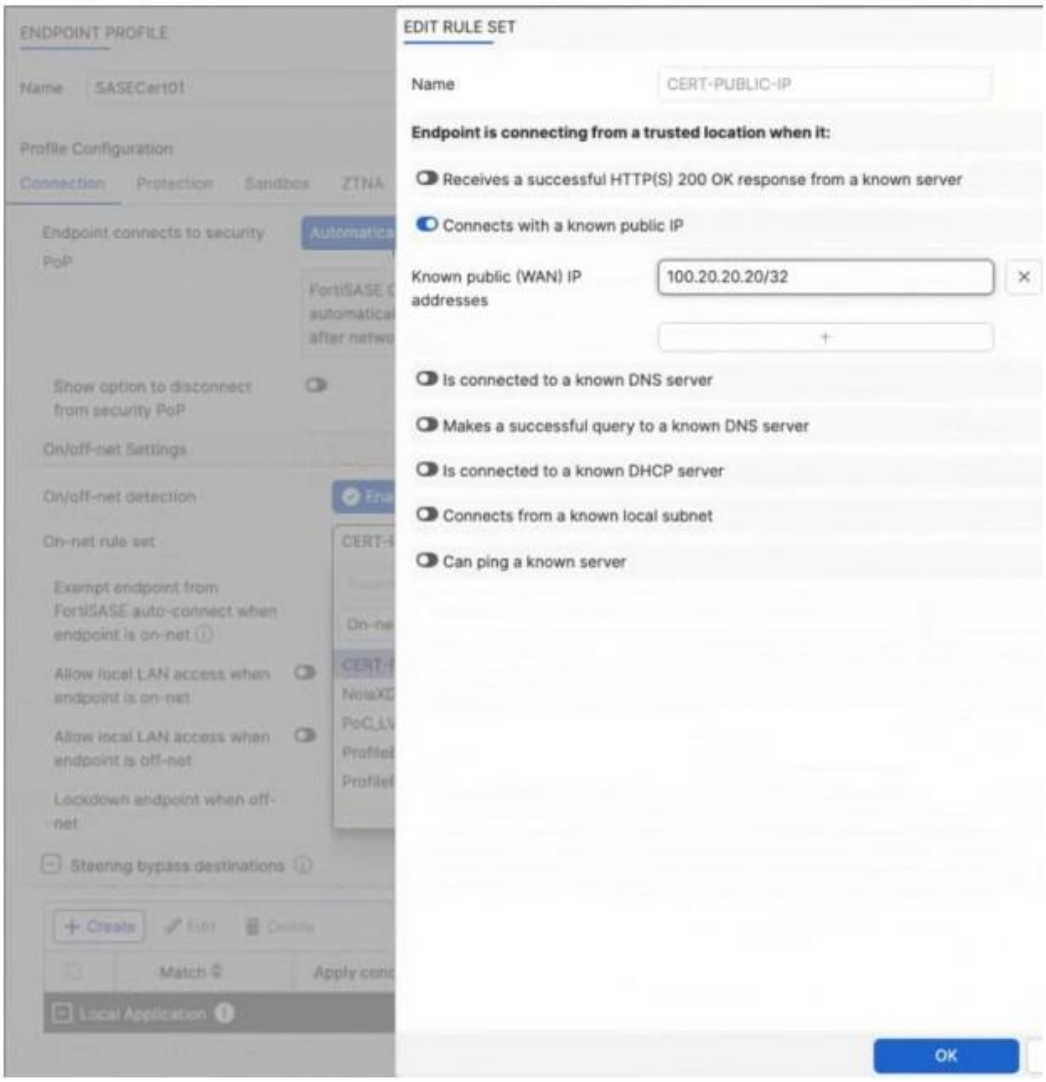
**QUESTION 4**
Refer to the exhibit. A customer configured the **On/off-net detection** rule to disable FortiSASE

VPN auto-connect when users are inside the corporate network. The rule is set to **Connects with a known public IP** using the company's public IP address. However, when the users are on the corporate network, the FortiSASE VPN still auto-connects. The customer has confirmed that traffic is going to the internet with the correct IP address.

Which configuration is causing the issue?

**Endpoint profile**






A. The **On-net rule set** configuration is incorrect.
B. **Allow local LAN access when endpoint is on-net** is disabled when it should be enabled.
C. **Exempt endpoint from FortiSASE auto-connect** is disabled when it should be enabled.
D. **Is connected to a known DNS server** should be enabled and configured.

**Answer:** A
**Explanation:**
The on/off-net detection is set to Connects with a known public IP, but the endpoint's detected public IP may not match exactly due to NAT, multiple public IPs, or routing differences. This causes FortiSASE to consider the endpoint off-net, triggering VPN auto-connect. The issue lies in the on-net rule set configuration, which needs to account for all relevant public IP addresses or use a more reliable detection method.

**QUESTION 5**
How does FortiSASE Secure Private Access (SPA) facilitate connectivity to private resources in a hub-and-spoke network?

A. SPA establishes direct links to spokes without IPsec or BGP and uses an easy configuration key

to secure web traffic for remote users.

B. SPA applies source network address translation (SNAT) for remote user traffic and uses IKEv1 for IPsec tunnels to connect to standalone hubs without BGP support.
C. SPA connects to private resources using HTTP and HTTPS protocols and relies on FortiClient for agentless access to SD-WAN deployments.
D. SPA connects a FortiSASE POP to a FortiGate hub or SD-WAN deployment using IPsec and BGP for dynamic route exchange with an easy configuration key for simplified setup on FortiOS.

**Answer:** D
**Explanation:**
Secure Private Access connects FortiSASE POPs to a FortiGate hub or SD-WAN deployment using IPsec tunnels and BGP to dynamically exchange routes. The easy configuration key simplifies the setup on FortiOS, enabling secure and scalable access to private resources in a hub-and-spoke network.

**QUESTION 6**
A AFortiSASE customer has been enforcing always-on VPN for their remote-users running FortiClient.

What option can be enabled under the customer's Endpoint Profile o allow them access different resources located in the same L2 network?

A. **Allow local LAN Access** into user Endpoint Profile before they get connected to the VPN
B. **Endpoint Sandbox** protection for VPN users
C. **Endpoint Anti-Virus** protection in the Endpoint Profile for VPN
D. **Network Lockdown** for endpoints with VPN enabled

**Answer:** A
**Explanation:**
Enabling Allow local LAN access in the endpoint profile lets remote users access other resources on the same Layer 2 network without routing that traffic through the FortiSASE VPN, while still enforcing the always-on VPN for other traffic.

**QUESTION 7**
Which three traffic flows are supported by FortiSASE Secure Private Access (SPA)? (Choose three.)

A. From private resources to FortiSASE agent-based users.
B. From private resources to the internet.
C. From agent-based users to private resources behind the Fortinet SD-WAN.
D. From private resources to other private resources (SPA to SPA).
E. From thin branches/branch on-ramp to private resources behind the Fortinet SD-WAN.

**Answer:** ACD
**Explanation:**
SPA supports traffic flows from private resources to agent-based users, from agent-based users to private resources behind a Fortinet SD-WAN or FortiGate hub, and between private resources across SPA-to-SPA connections. It does not handle general internet-bound traffic or thin branch traffic outside the SPA scope.

# Thank You for Trying Our Product

## Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

**10% Discount Coupon Code:** **ASTR14**