Vendor: Fortinet

Exam Code: FCSS_LED_AR-7.6

Exam Name: Fortinet NSE 6 - LAN Edge 7.6 Architect

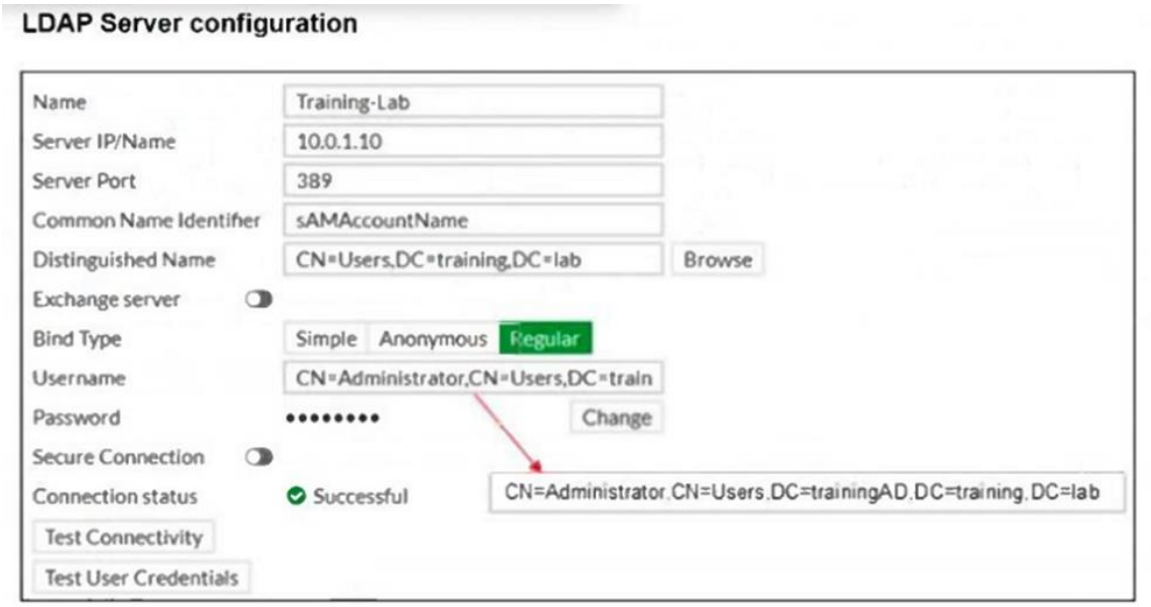
Version: DEMO

QUESTION 1
How does the Syslog-based single sign-on (SSO) feature in FortiAuthenticator function to correlate user activity with authentication events across multiple network devices?

A. It uses syslog messages to monitor authentication events and correlate them with user activities.
B. It modifies user credentials based on the outcome of authentication events.
C. It relies on external servers to analyze syslog messages for user authentication.
D. It authenticates users through a captive portal by monitoring login attempts.

Answer: A
Explanation:
Syslog-based SSO in FortiAuthenticator works by listening to syslog messages from network devices (such as firewalls, VPNs, or wireless controllers). It parses authentication events from these logs and correlates them with user IPs or sessions, enabling user identity tracking and seamless single sign-on across the network.

QUESTION 2
Refer to the exhibit.



The exhibit shows an LDAP server configuration with the Username setting has been expanded to display its full content.

The administrator has configured the LDAP settings on FortiGate and is troubleshooting for authentication issues.

As part of the troubleshooting steps, the administrator runs the command dsquery user -samid student on the Windows Active Directory (AD) server with an IP address 10.0.1.10 and received the output CN=student, CN=Users, DC=trainingAD, DC=training, DC=lab.

Based on the dsquery output, which LDAP setting on FortiGate is misconfigured?

A. The **Common Name Identifier** is incorrectly set, causing authentication failures.

B. The Bind Type is incorrectly configured, preventing FortiGate from connecting to the LDAP server.
C. The **Distinguished N** setting is incorrectly configured, causing issues with user authentication.
D. **Sever IP/Name** is misconfigured so FortiGate can't reach the LDAP server.

Answer: C
Explanation:
The Distinguished Name (DN) is misconfigured. In the FortiGate LDAP settings, it is set as CN=Users,DC=training,DC=lab, but the dsquery output shows the correct DN path should include DC=trainingAD (CN=Users,DC=trainingAD,DC=training,DC=lab). Because of this mismatch, FortiGate cannot properly search for or authenticate AD users.

QUESTION 3
In a Windows environment using AD machine authentication, how does FortiAuthenticator ensure that a previously authenticated device is maintaining its network access once the device resumes operating after sleep or hibernation?

A. It sends a wake-on-LAN packet to trigger reauthentication.
B. It caches the MAC address of authenticated devices for a configurable period of time.
C. It temporarily assigns the device to a guest VLAN until full reauthentication is completed.
D. It uses machine authentication based on the device IP address.

Answer: B
Explanation:
FortiAuthenticator maintains network access for devices resuming from sleep or hibernation by caching the MAC address of previously authenticated devices for a configurable period. This allows the device to reconnect without requiring immediate full reauthentication, ensuring seamless access continuity.

QUESTION 4
You are troubleshooting an issue where users are being intermittently redirected to an error page after submitting their login credentials on a captive portal. As part of your troubleshooting steps, you review the POST parameters sent from the client to the authentication server.

What should you check in the magic ID within the POST parameters to help resolve the issue?

A. Determine whether the magic ID has expired, which could cause the server to reject the authentication request.
B. Validate that the magic ID contains encryption keys for securing the user's password during transmission.
C. Verify whether the magi ID matches the session generated by the server to ensure the request is valid.
D. Confirm that the magic ID is tied to the correct redirection URL for the user session.

Answer: C
Explanation:
The magic ID in the POST parameters must match the session generated by the authentication server. If the magic ID does not align with the active session, the server treats the request as invalid, leading to errors after login attempts.

QUESTION 5
Refer to the exhibit.

Debug output

```
FortiGate # diagnose switch-controller switch-info 802.1X
Managed Switch : S224EPTF19006016

   port2 : Mode: port-based (mac-by-pass disable)
           Link: Link up
           Port State: unauthorized: (  )
           Dynamic Authorized Vlan : 0
           Dynamic Allowed Vlan list:
           Dynamic Untagged Vlan list:
           EAP pass-through : Enable
           EAP egress-frame-tagged : Enable
           EAP auto-untagged-vlans : Enable
           Allow MAC Move : Disable
           Dynamic Access Control List : Disable
           Quarantine VLAN (4093) detection : Enable
           Native Vlan : 10
           Allowed Vlan list: 10,4093
           Untagged Vlan list: 4093
           Guest VLAN :
           Auth-Fail Vlan :
           AuthServer-Timeout Vlan :

           Sessions info:
           00:09:0f:02:02:02     Type=802.1x,,state=AUTHENTICATING,etime=0,eap_cnt=0 params:reAuth=3600
```

Port2 on FortiSwitch is configured with an 802.1X authentication security policy, but a device connected to port2 is unable to access the network. The administrator has gathered the diagnose output, as shown in the exhibit, to investigate the issue.

Which two scenarios could explain why the device is failing to gain network access? (Choose two.)

A. The device is not configured for 802.1X authentication.
B. The device has been quarantined for 3600 seconds.
C. The device does not support 802.1X authentication.
D. The device has been assigned the guest VLAN.

Answer: AC
Explanation:
The port is in state AUTHENTICATING with eap_cnt=0, indicating no 802.1X EAP exchange occurred. Since MAB is disabled (mac-by-pass disable), a device that is not configured for 802.1X or does not support 802.1X cannot gain access.

QUESTION 6
How does Syslog SSO on FortiAuthenticator establish user identity?

A. By directly communicating with the domain controller to retrieve user login events
B. By using predefined user credentials stored on ForitAuthenticator
C. By intercepting and decrypting network traffic to extract user credentials
D. By parsing syslog messages from network devices to extract user login events and associate them with IP addresses

Answer: D

Explanation:
Syslog SSO on FortiAuthenticator works by parsing syslog messages from network devices (such as firewalls, VPN gateways, or wireless controllers). These syslog entries contain user login events, which FortiAuthenticator extracts and maps to the corresponding IP addresses, establishing user identity for single sign-on.

QUESTION 7
Your office wants to set up a Wi-Fi network for visitors. Your company would like to require them to log in for tracking purposes.

Which two types of captive portals could be enabled on an interface? (Choose two.)

A. Authentication
B. Guest Pass Access
C. Disclaimer + Authentication
D. Email Notification Only
E. Terms Acknowledgement Without Authentication

Answer: AC
Explanation:
FortiGate supports captive portals that require Authentication or a combination of Disclaimer + Authentication. These options enforce login for visitors, allowing user tracking and ensuring compliance with company access policies.

QUESTION 8
You have decided to manage multiple FortiSwitch devices using FortiManager and its FortiSwitch Manager feature.

Which two statements accurately describe FortiSwitch Manager feature functionality? (Choose two.)

A. FortiSwitch Manager displays the following statuses for FortiSwitch: online, offline, unauthorized, and unknown.
B. Per-device management is useful for deploying multiple switches with the same configuration.
C. FortiSwitch Manager displays the following statuses for FortiSwitch: active, inactive, pending, and unknown.
D. In per-device management mode, you apply settings and profiles to individual FortiSwitch devices.

Answer: AD
Explanation:
FortiSwitch Manager correctly shows switch statuses such as online, offline, unauthorized, and unknown.

In per-device management mode, configuration is applied individually to each FortiSwitch, allowing customized settings and profiles per device.

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**