NSE7_LED-7.0 Dumps - NSE7_LED-7.0 Deutsche

P.S. Kostenlose 2025 Fortinet NSE7_LED-7.0 Prüfungsfragen sind auf Google Drive freigegeben von Pass4Test verfügbar: https://drive.google.com/open?id=13qM1UM2wAdqyMxWvjGIZ-tqCpjgbaaps

Die neuesten Schulungsunterlagen zur Fortinet NSE7_LED-7.0 (Fortinet NSE 7 - LAN Edge 7.0) Zertifizierungsprüfung von Pass4Test sind von den Expertenteams bearbeitet, die vielen beim Verwirklichen ihres Traums verhelfen. In der konkurrenzfähigen Gesellschaft muss man die Fachleute seine eigenen Kenntinisse und Technikniveau unter Beweis stellen, um seine Position zu verstärken. Durch die Fortinet NSE7_LED-7.0 Zertifizierungsprüfung kann man seine Fähigkeiten beweisen. Mit dem Fortinet NSE7_LED-7.0 Zertifikat werden große Veränderungen in Ihrer Arbeit stattfinden. Ihr Gehalt wird erhöht und Sie werden sicher befördert.

Die Fortinet NSE7_LED-7.0-Zertifizierung wird in der Branche sehr geschätzt, da sie die Fähigkeiten der Kandidaten in Bezug auf die Bereitstellung und Verwaltung von Fortinets Lan Edge-Lösungen demonstriert. Die Zertifizierung bietet Fachleuten einen Wettbewerbsvorteil, der eine Beschäftigung im Networking -Bereich anstrebt. Die Zertifizierung bietet auch die Möglichkeit, Anerkennung innerhalb der Fortinet -Community sowie Zugang zu exklusiven Ressourcen und Veranstaltungen zu erhalten. Insgesamt ist die Fortinet NSE7_LED-7.0-Zertifizierung eine hervorragende Investition für Netzwerkfachleute, die ihre Karriereaussichten verbessern und dem Wettbewerb voraus sind.

>> NSE7_LED-7.0 Dumps <<

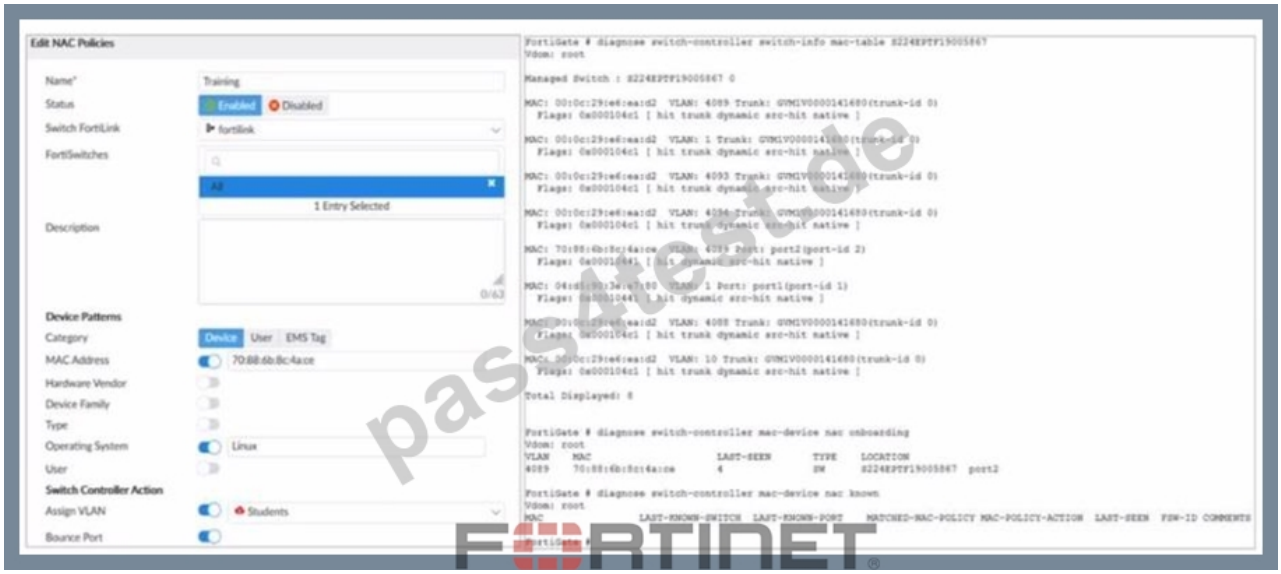
NSE7_LED-7.0 Deutsche & NSE7_LED-7.0 Pruefungssimulationen

Nun ist die Fortinet NSE7_LED-7.0 Zertifizierungsprüfung eine beliebte Prüfung in der IT-Branche. Viele IT-Fachleute wollen das Fortinet NSE7_LED-7.0 Zertfikat erhalten. So ist die Fortinet NSE7_LED-7.0 Zertifizierungsprüfung eine beliebte Prüfung. Das Fortinet NSE7_LED-7.0 Zertfikat ist sehr hilfreich, um Ihre Arbeit in der IT-Industrie zu verbessern und Ihr Gehalt zu erhöhen und

Ihrem Leben eine zuverlässige Garantie zu geben.

Fortinet NSE 7 - LAN Edge 7.0 NSE7_LED-7.0 Prüfungsfragen mit Lösungen (Q33-Q38):

33. Frage
Refer to the exhibit.



Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit An administrator is testing the NAC feature The test device is connected to a managed FortiSwitch device
{S224EPTF19"53C7)onpOrt2
After applying the NAC policy on port2 and generating traffic on the test device the test device is not matching the NAC policy therefore the test device remains m the onboarding VLAN Based on the information shown in the exhibit which two scenarios are likely to cause this issue? (Choose two.)

- A. The MAC address configured on the NAC policy is incorrect
- B. The device operating system detected by FortiGate is not Linux
- C. Management communication between FortiGate and FortiSwitch is down
- D. Device detection is not enabled on VLAN 4089

Antwort: A,C

Begründung:
Explanation
According to the FortiManager configuration, the NAC policy is set to match devices with the MAC address of 00:0c:29:6a:2b:3c and the operating system of Linux.However, according to the FortiGate CLI output, the test device has a different MAC address of 00:0c:29:6a:2b:3d. Therefore, option B is true. Option A is also true because the FortiSwitch device status is shown as down, which means that the management communication between FortiGate and FortiSwitch is not working properly. This could prevent the NAC policy from being applied correctly. Option C is false because the device operating system detected by FortiGate is Linux, which matches the NAC policy. Option D is false because device detection is enabled on VLAN 4089, as shown by the command "config switch-controller vlan".

34. Frage
Refer to the exhibit.

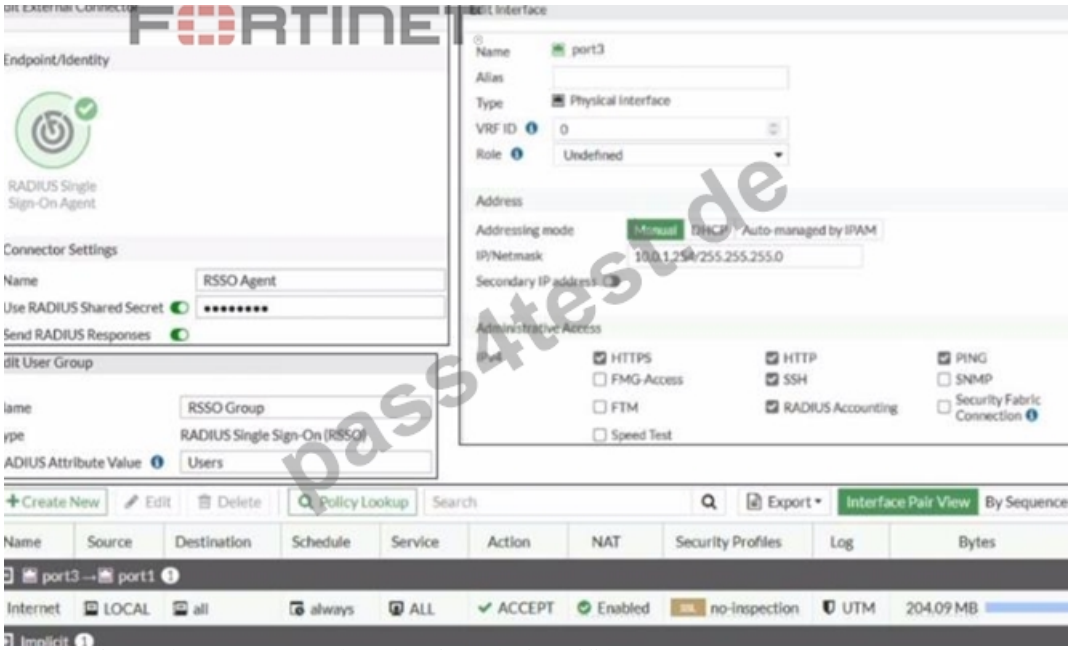
Examine the RADIUS server configuration shown in the exhibit
An administrator has configured a RADIUS server on FortiGate that points to FortiAuthenticator FortiAuthenticator is acting as an authentication proxy and is configured to relay all authentication requests to a remote Windows AD server using LDAP While testing the configuration the administrator noticed that the diagnosetest authserver command worked with PAP, however authentication requests failed when using MSCHAP2 Which two solutions can the administrator implement to get MSCHAP2 authentication to work" (Choose two.)

- A. On FortiGate update the Secret setting on the RADIUS server
- B. On FortiGate configure the NAS IP setting on the RADIUS server
- C. On FortiAuthenticator enable Windows Active Directory Domain Authentication to add FortiAuthenticator to the Windows domain
- D. On FortiAuthenticator change the back-end authentication server from LDAP to RADIUS

Antwort: C,D

Begründung:
Explanation
According to the exhibit, the RADIUS server configuration on FortiGate points to FortiAuthenticator, which is acting as an authentication proxy and is configured to relay all authentication requests to a remote Windows AD server using LDAP. However, LDAP does not support MSCHAP2 authentication, which is required for RADIUS. Therefore, option A is true because on FortiAuthenticator, enabling Windows Active Directory Domain Authentication will add FortiAuthenticator to the Windows domain and allow it to use MSCHAP2 authentication with the AD server. Option C is also true because on FortiAuthenticator, changing the back-end authentication server from LDAP to RADIUS will allow it to use MSCHAP2 authentication with the AD server. Option B is false because on FortiGate, configuring the NAS IP setting on the RADIUS server will not affect the MSCHAP2 authentication, but rather the source IP address of the RADIUS packets. Option D is false because on FortiGate, updating the Secret setting on the RADIUS server will not affect the MSCHAP2 authentication, but rather the shared secret between FortiGate and FortiAuthenticator.

35. Frage
Refer to the exhibit



Examine the FortiGate RSSO configuration shown in the exhibit
FortiGate is configured to receive RADIUS accounting messages on port3 to authenticate RSSO users The users are located behind port3 and the internet link is connected to port1 FortiGate is processing incoming RADIUS accounting messages successfully and RSSO users are getting associated with the RSSO Group user group However all the users are able to access the internet, and the administrator wants to restrict internet access to RSSO users only Which configuration change should the administrator make to fix the problem?

- A. Change the RADIUS Attribute Value selling to match the name of the RADIUS attribute containing the group membership information of the RSSO users
- B. Add RSSO Group to the firewall policy
- C. Create a second firewall policy from port3 lo port1 and select the target destination subnets
- D. Enable Security Fabric Connection on port3

Antwort: B

Begründung:
Explanation
According to the exhibit, the firewall policy from port3 to port1 has no user group specified, which means that it allows all users to access the internet. Therefore, option B is true because adding RSSO Group to the firewall policy will restrict internet access to RSSO users only. Option A is false because changing the RADIUS Attribute Value setting will not affect the firewall policy, but rather the RSSO user group membership. Option C is false because enabling Security Fabric Connection on port3 will not affect the firewall policy, but rather the communication between FortiGate and other Security Fabric devices. Option D is false because creating a second firewall policy from port3 to port1 will not affect the existing firewall policy, but rather create a redundant or conflicting policy.

36. Frage
An administrator is testing the connectivity for a new VLAN The devices in the VLAN are connected to a FortiSwitch device that is managed by FortiGate Quarantine is disabled on FortiGate While testing the administrator noticed that devices can ping FortiGate and FortiGate can ping the devices The administrator also noticed that inter-VLAN communication works However intra-VLAN communication does not work Which scenario is likely to cause this issue?

- A. The native VLAN configured on the ports is incorrect
- B. The FortiSwitch MAC address table is missing entries
- C. The FortiGate ARP table is missing entries
- D. Access VLAN is enabled on the VLAN

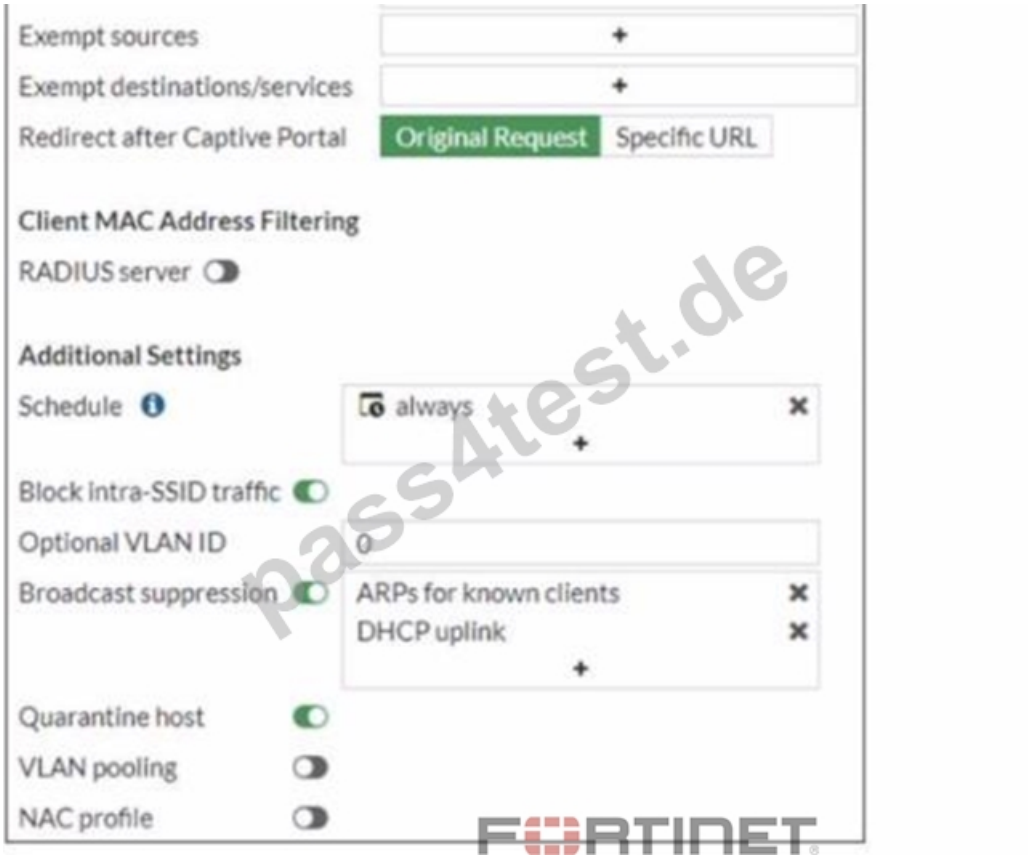
Antwort: B

Begründung:
Explanation

According to the scenario, the devices in the VLAN are connected to a FortiSwitch device that is managed by FortiGate. Quarantine is disabled on FortiGate, which means that the devices are not blocked by any security policy. The devices can ping FortiGate and FortiGate can ping the devices, which means that the IP connectivity is working. Inter-VLAN communication works, which means that the routing between VLANs is working. However, intra-VLAN communication does not work, which means that the switching within the VLAN is not working. Therefore, option C is true because the FortiSwitch MAC address table is missing entries, which means that the FortiSwitch does not know how to forward frames to the destination MAC addresses within the VLAN. Option A is false because access VLAN is enabled on the VLAN, which means that the VLAN ID is added to the frames on ingress and removed on egress. This does not affect intra-VLAN communication. Option B is false because the native VLAN configured on the ports is incorrect, which means that the frames on the native VLAN are not tagged with a VLAN ID. This does not affect intra-VLAN communication. Option D is false because the FortiGate ARP table is missing entries, which means that FortiGate does not know how to map IP addresses to MAC addresses. This does not affect intra-VLAN communication.

37. Frage

Refer to the exhibits.



Firewall Policy

```
config firewall policy
    edit 11
        set name "Guest to Internal"
        set uuid c5e45130-aada-51e8-ee0c-bc1204f9f163
        set srcintf "guest"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "FortiAuthenticator" "WindowsAD"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Examine the firewall policy configuration and SSID settings

An administrator has configured a guest wireless network on FortiGate using the external captive portal The administrator has verified that the external captive portal URL is correct However wireless users are not able to see the captive portal login page

Given the configuration shown in the exhibit and the SSID settings which configuration change should the administrator make to fix the problem?

- A. Apply a guest.portal user group in the firewall policy with the ID 11.
- B. Enable the captivs-portal-exempt option in the firewall policy with the ID 11.
- C. Include the wireless client subnet range in the Exempt Source section
- D. Disable the user group from the SSID configuration

Antwort: A

Begründung:
Explanation
According to the FortiGate Administration Guide, "To use an external captive portal, you must configure a user group that uses the external captive portal as the authentication method and apply it to a firewall policy." Therefore, option C is true because it will allow the wireless users to be redirected to the external captive portal URL when they try to access the Internet. Option A is false because disabling the user group from the SSID configuration will prevent the wireless users from being authenticated by the FortiGate device. Option B is false because enabling the captive-portal-exempt option in the firewall policy will bypass the captive portal authentication for the wireless users, which is not the desired outcome. Option D is false because including the wireless client subnet range in the Exempt Source section will also bypass the captive portal authentication for the wireless users, which is not the desired outcome.

38. Frage
.....

Die Zertifikat der Fortinet NSE7_LED-7.0 ist international anerkannt. Sie zu erwerben bedeutet, dass Sie den Schlüssel zur höheren Stelle besitzen. Die Fortinet NSE7_LED-7.0 Prüfungsunterlagen von Pass4Test werden von erfahrenen IT-Profis herstellt und immer wieder aktualisiert. Jetzt können Sie mit günstigem Preis die verlässliche Fortinet NSE7_LED-7.0 Prüfungsunterlagen genießen. Nachdem Sie die Zertifizierung erwerbt haben, können Sie leicht eine höhere Arbeitsposition oder Gehalten bekommen.

Sie □ de.fast2test.com □ ein und suchen Sie nach kostenloser Download von 「 NSE7_LED-7.0 」 □NSE7_LED-7.0 Echte Fragen

- approved100.co.uk, pct.edu.pk, barclaytraininginstitute.com, coursewingsportal.com, arrayholding.com, proweblearn.com, rent2renteducation.co.uk, study.stcs.edu.np, shortcourses.russellcollege.edu.au, bacsihoangoanh.com

Übrigens, Sie können die vollständige Version der Pass4Test NSE7_LED-7.0 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=13qM1UM2wAdqyMxWvjGIZ-tqCpjgbaaps