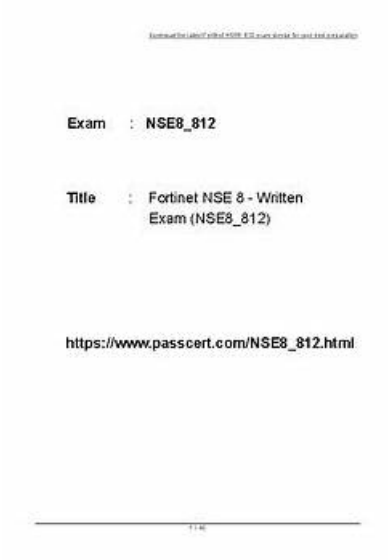
NSE8_812 Deutsch Prüfung & NSE8_812 Pruefungssimulationen



Exam : NSE8_812

Title : Fortinet NSE 8 - Written Exam (NSE8_812)

https://www.passcert.com/NSE8_812.html

Außerdem sind jetzt einige Teile dieser ITZert NSE8_812 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1CeA70wbwJ8vbGAn66XIDQaBkXUHSdxub

Was andere sagen ist nicht so wichtig, was Sie empfinden ist am alle wichtigsten. Wir hoffen, dass Sie unsere Ehrlichkeit und Anstrengung empfinden. Deshalb bieten wir Ihnen kostenlose Demo der Fortinet NSE8_812 Prüfungsunterlagen. Probieren Sie bevor dem Kauf! Lassen Sie sich mehr beruhigen. Nach dem Kauf bieten wir Ihnen weiter Kundendienst. Wenn die Fortinet NSE8_812 Prüfungsunterlagen aktualisieren, geben wir Ihnen sofort Bescheid. Innerhalb einem Jahr können Sie kostenlose Aktualisierung der Fortinet NSE8_812 Prüfungsunterlagen genießen.

Die Fortinet NSE8_812 Prüfung ist eine fortgeschrittene Zertifizierungsprüfung, die entwickelt wurde, um die Fähigkeiten und Expertise von Netzwerksicherheitsprofis zu validieren. Diese Prüfung richtet sich an diejenigen, die umfangreiche Erfahrung in der Gestaltung, Implementierung und Verwaltung komplexer Netzwerksicherheitslösungen haben. Die Fortinet NSE8_812 Zertifizierungsprüfung deckt eine Vielzahl von Themen ab, einschließlich fortgeschrittener Routing- und Switching-Technologien, dynamischer Routing-Protokolle, sicherer VPNs, fortgeschrittener Firewall-Richtlinien und erweiterter Bedrohungsschutz. Die Prüfung basiert auf praktischen Szenarien und realen Herausforderungen, mit denen Netzwerksicherheitsprofis in ihrem täglichen Betrieb konfrontiert werden können.

Die Fortinet NSE8_812-Zertifizierungsprüfung, auch bekannt als Fortinet NSE 8 - Written Exam, ist eine umfassende Bewertung des Wissens und der Fähigkeiten einer Person im Bereich der fortschrittlichen Netzwerksicherheit. Diese Prüfung richtet sich an Fachleute, die ihre Expertise in der Gestaltung, Umsetzung und Verwaltung komplexer Sicherheitsinfrastrukturen validieren möchten.

Die NSE8_812-Prüfung gilt als Benchmark für fortgeschrittene Netzwerksicherheitsfachleute, und das Bestehen dieser Prüfung ist eine Voraussetzung für die Erlangung der NSE 8-Zertifizierung.

>> NSE8_812 Deutsch Prüfung <<

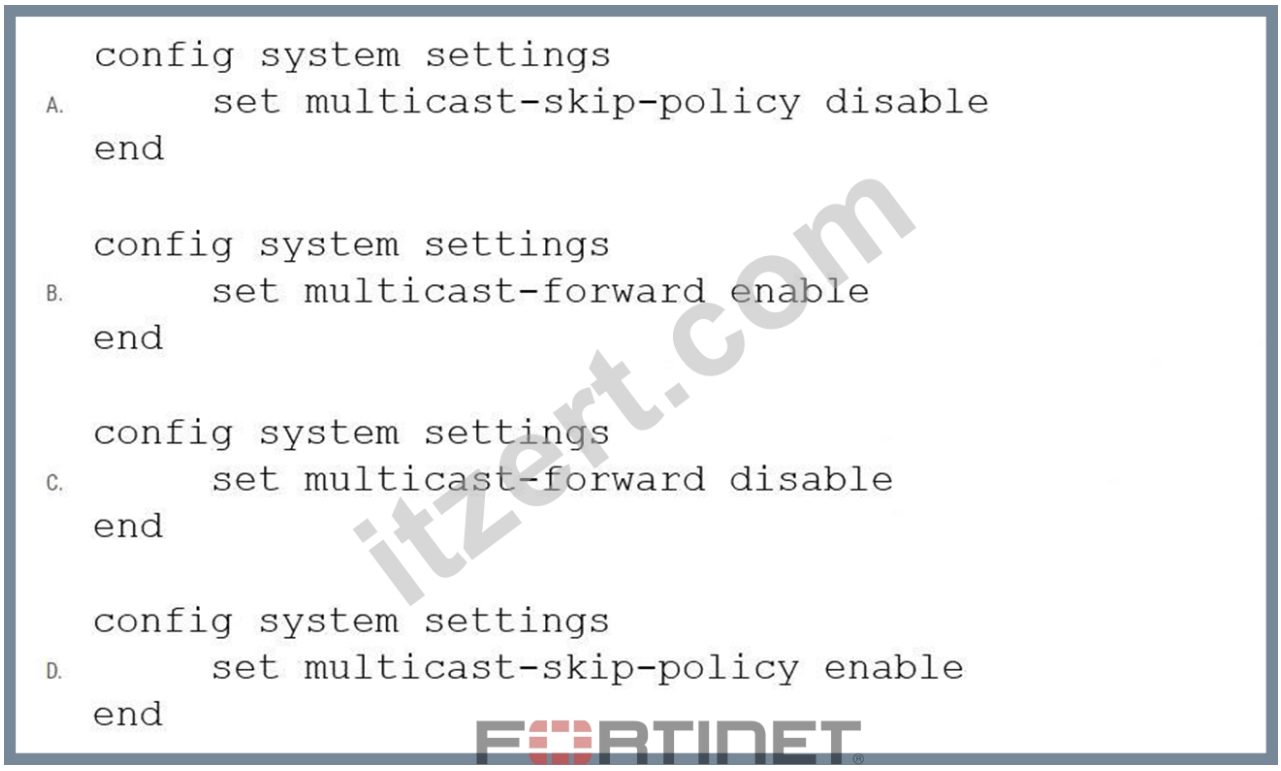
NSE8_812 Pruefungssimulationen - NSE8_812 Fragen Und Antworten

Wenn Sie die Fragen und Antworten zur Fortinet NSE8_812 Zertifizierungsprüfung kaufen, können Sie nicht nur die Fortinet NSE8_812 Zertifizierungsprüfung erfolgreich bestehen, sonder einen einjährigen kostenlosen Update-Service genießen. Falls Sie in der Prüfung durchfallen, zahlen wir Ihnen die gesammte Summe zurück. Sie können im Internet teilweise die Fragen und Antworten zur Fortinet NSE8_812 Zertifizierungsprüfung kostenlos als Probe herunterladen, um die Zuverlässigkeit unserer Produkte zu prüfen.

Die Fortinet NSE8_812 Prüfung ist eine schriftliche Prüfung, die das Fachwissen von Personen im Bereich Netzwerksicherheit testet. Die Prüfung ist Teil des Fortinet Network Security Expert (NSE) Programms, welches ein mehrstufiges Zertifizierungsprogramm ist, das Personen das Wissen und die Fähigkeiten vermittelt, die für das Design, die Konfiguration und Verwaltung komplexer Netzwerksicherheitslösungen benötigt werden.

Fortinet NSE 8 - Written Exam (NSE8_812) NSE8_812 Prüfungsfragen mit Lösungen (Q14-Q19):

14. Frage
On a FortiGate Configured in Transparent mode, which configuration option allows you to control Multicast traffic passing through the?



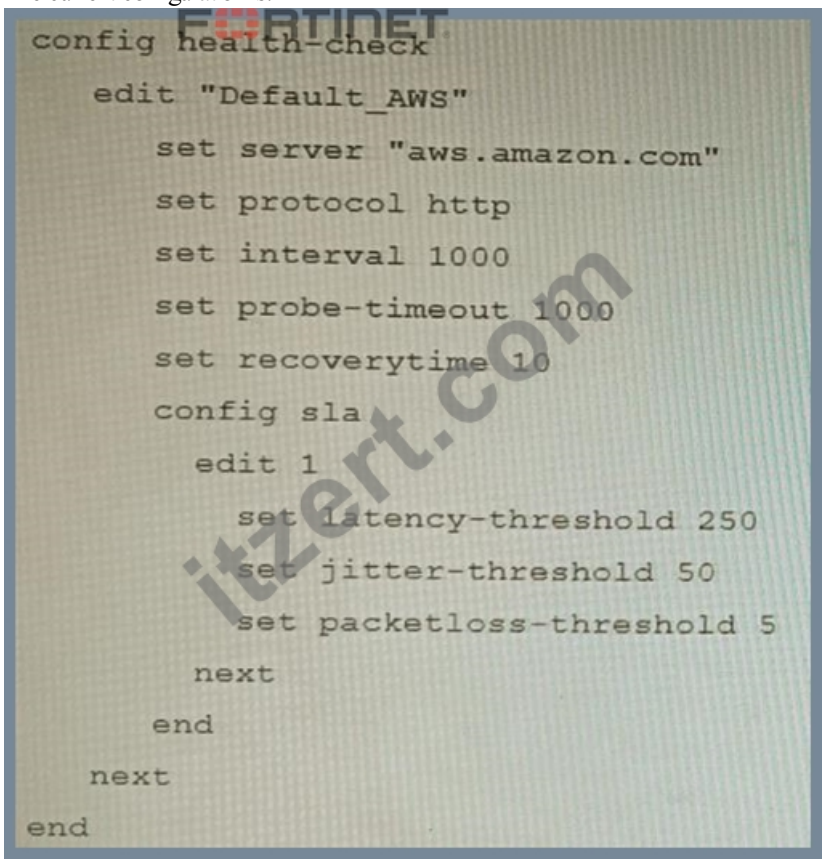
- A. Option C
- B. Option B
- C. Option D
- D. Option A

Antwort: D

Begründung:
When multicast-skip-policy is enabled, no check is performed based on multicast policy. A multicast packet received on an interface is flooded unconditionally to all interfaces (except the incoming interface) belonging to the same forwarding domain. Multicast packets are forwarded even when there is no multicast policy or the multicast policy is set to deny. To forward multicast traffic based on multicast policy, multicast-skip-policy must be disabled. In transparent mode, there is a per-VDOM configuration to skip

policy check and forward all multicast traffic. This command is only available in transparent mode, and is disabled by default.

15. Frage
You are creating the CLI script to be used on a new SD-WAN deployment You will have branches with a different number of internet connections and want to be sure there is no need to change the Performance SLA configuration in case more connections are added to the branch.
The current configuration is:



Which configuration do you use for the Performance SLA members?

- A. set members all
- B. current configuration already fulfills the requirement
- C. set members 0
- D. set members any

Antwort: C

Begründung:
References:
Performance SLA | FortiGate / FortiOS 7.4.0
Configuring Performance SLA | FortiGate / FortiOS 7.4.0

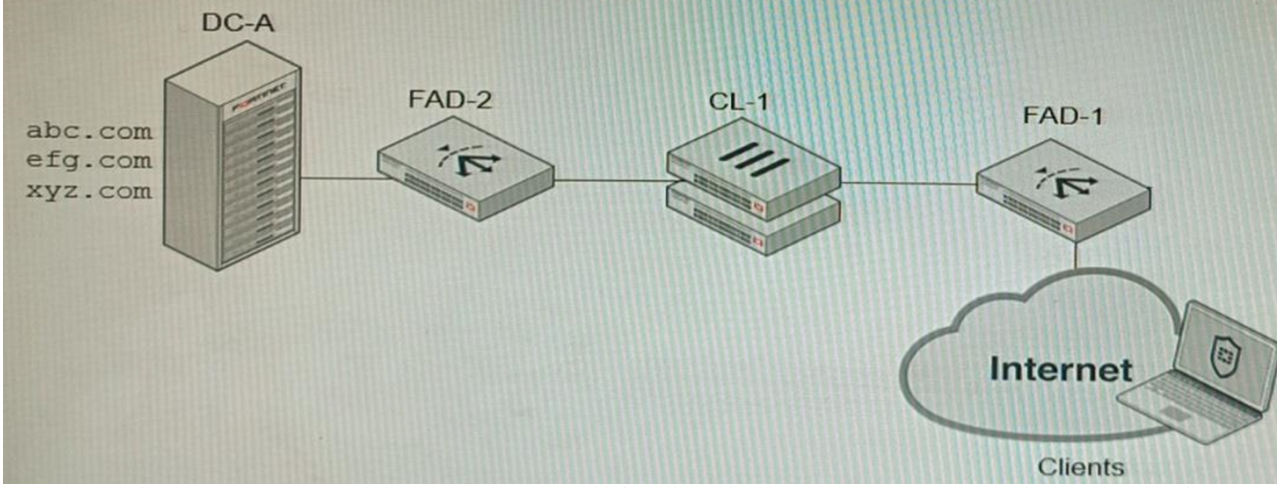
16. Frage
Refer to the exhibits.

Configuration

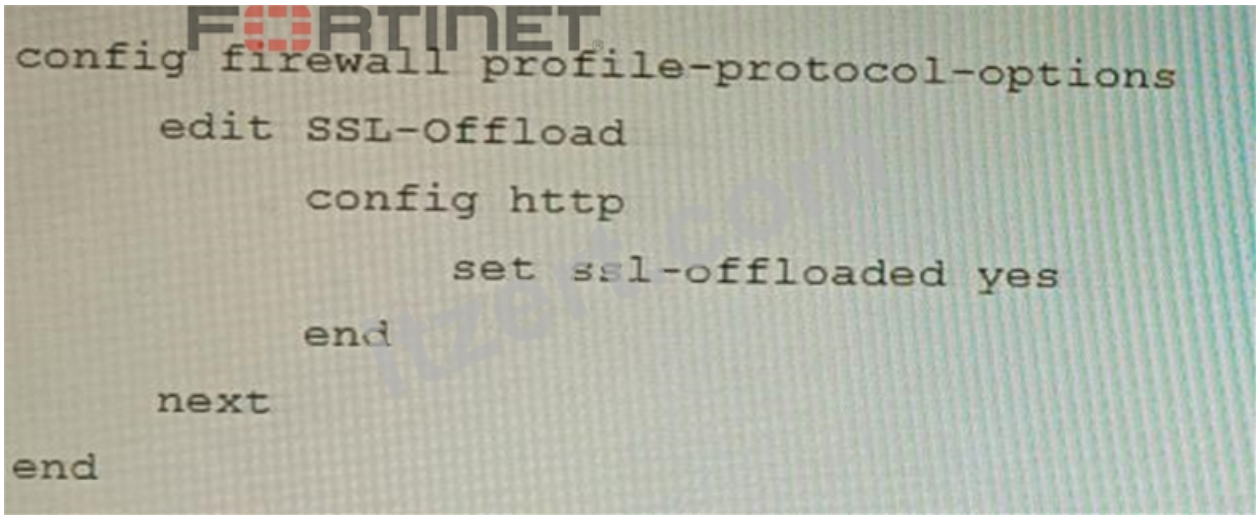
```
config firewall profile-protocol-options
    edit "SSL-Offload"
        set comment "For FAD decrypted traffic"
        config http
            set ports 80
            unset options
            unset post-lang
        end
        config ftp
            set ports 21
            set options splice
        end
        config imap
            set ports 143
            set options fragmail
        end
        ...output omitted...
    next
end

config application list
    edit "SSL-Offload-App-Detect"
        set comment "App detect in decrypted traffic"
        config entries
            edit 1
                set action pass
            next
        end
    next
end
```

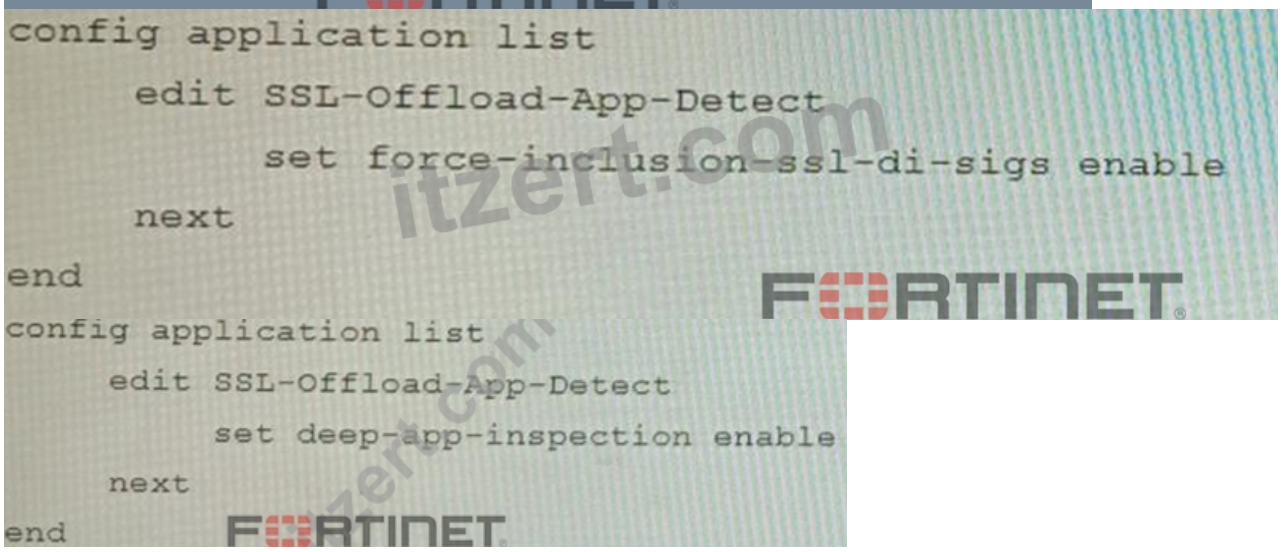

Topology



A FortiGate cluster (CL-1) protects a data center hosting multiple web applications. A pair of FortiADC devices are already configured for SSL decryption (FAD-1), and re-encryption (FAD-2). CL-1 must accept unencrypted traffic from FAD-1, perform application detection on the plain-text traffic, and forward the inspected traffic to FAD-2.
The SSL-Offload-App-Detect application list and SSL-Offload protocol options profile are applied to the firewall policy handling the web application traffic on CL-1.
Given this scenario, which two configuration tasks must the administrator perform on CL-1? (Choose two.) A)



B)

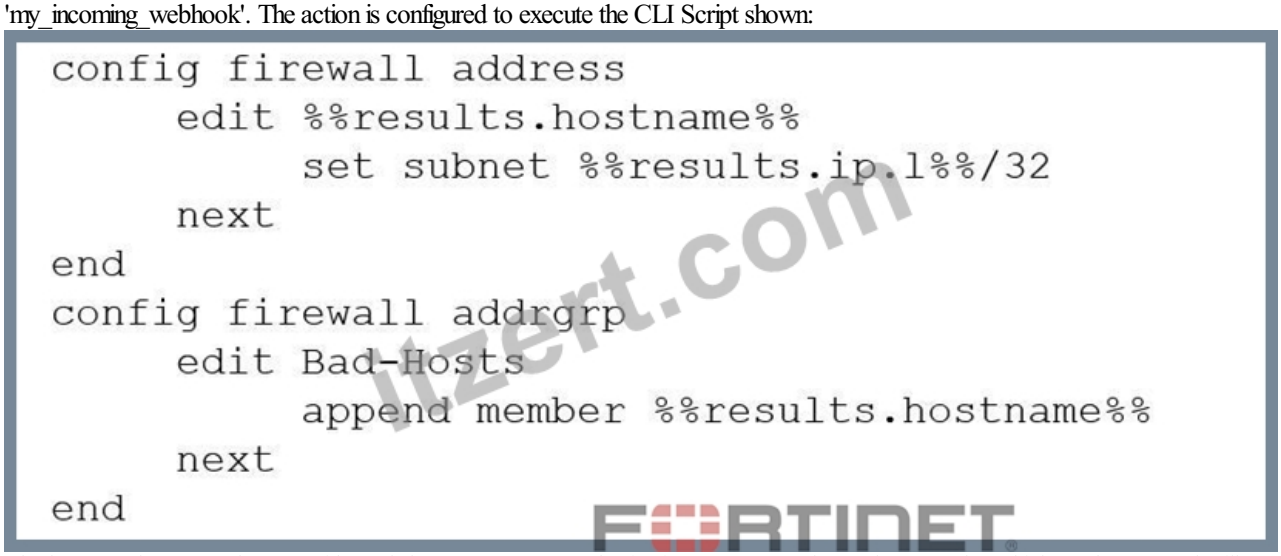


- A. Option D
- B. Option A
- C. Option B
- D. Option C

Antwort: C,D

Begründung:
To enable application detection on plain-text traffic that has been decrypted by FortiADC, the administrator must perform two configuration tasks on CL-1:
Enable SSL offloading in the firewall policy and select the SSL-Offload protocol options profile.
Enable application control in the firewall policy and select the SSL-Offload-App-Detect application list. References:
https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application-detection-on-ssl-offloaded-traffic

17. Frage
An automation stitch was configured using an incoming webhook as the trigger named 'my_incoming_webhook'. The action is configured to execute the CLI Script shown:

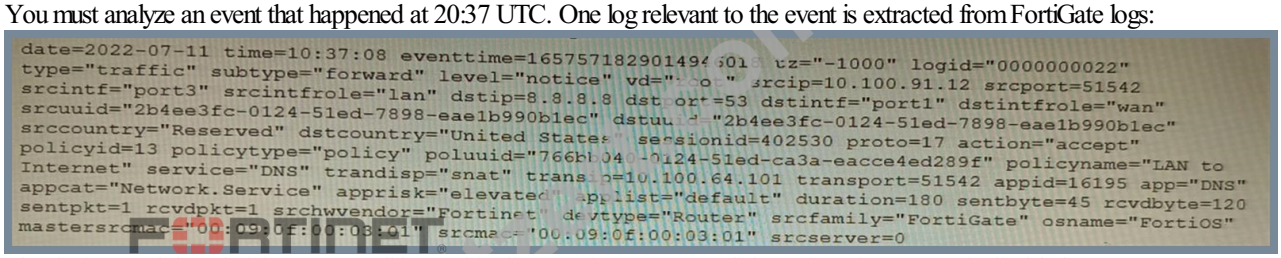


The base Curl command starts with: curl -k -x POST -H 'Authorization: Bearer ' --data <data> <url> Which Curl command will successfully work with the configured automation stitch?

- A. data: '{ "hostname": "bad_host_1", "ip": ["1.1.1.1"]}'
  url:
  http://192.168.226.129/api/v2/monitor/system/automation-stitch/webhook/my_incoming_webhook
- B. data: '{ "hostname": "bad_host_1", "ip": ["1.1.1.1"]}'
  url:
  http://192.168.226.129/api/v2/cmdb/system/automation-stitch/webhook/my_incoming_webhook
- C. data: '{ "hostname": "bad_host_1", "ip": "1.1.1.1"}'
  url: http://192.168.226.129/api/v2/cmdb/system/automation-stitch/webhook/my_incoming_webhook
- D. data: '{ "hostname": "bad_host_1", "ip": "1.1.1.1"}'
  url:
  http://192.168.226.129/api/v2/monitor/system/automation-stitch/webhook/my_incoming_webhook

Antwort: A

18. Frage
You must analyze an event that happened at 20:37 UTC. One log relevant to the event is extracted from FortiGate logs:



The devices and the administrator are all located in different time zones Daylight savings time (DST) is disabled
* The FortiGate is at GMT-1000.
* The FortiAnalyzer is at GMT-0800
* Your browser local time zone is at GMT-03.00
You want to review this log on FortiAnalyzer GUI, what time should you use as a filter?

- A. 10:37:08
- B. 17:37:08
- C. 20:37:08
- D. 12.37:08

Antwort: B

Begründung:
To review this log on FortiAnalyzer GUI, the administrator should use the time filter that matches the local time zone of FortiAnalyzer, which is GMT-0800. Since the log was generated at 20:37 UTC (GMT+0000), the corresponding time in GMT-0800 is 20:37 - 8 hours = 12:37. However, since DST is disabled on FortiAnalyzer, the administrator should add one hour to account for daylight saving time difference, resulting in 12:37 + 1 hour = 13:37. Therefore, the time filter to use is 13:37:08.
References: https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/103664/time-zone-and-daylight-saving-time

19. Frage
.....