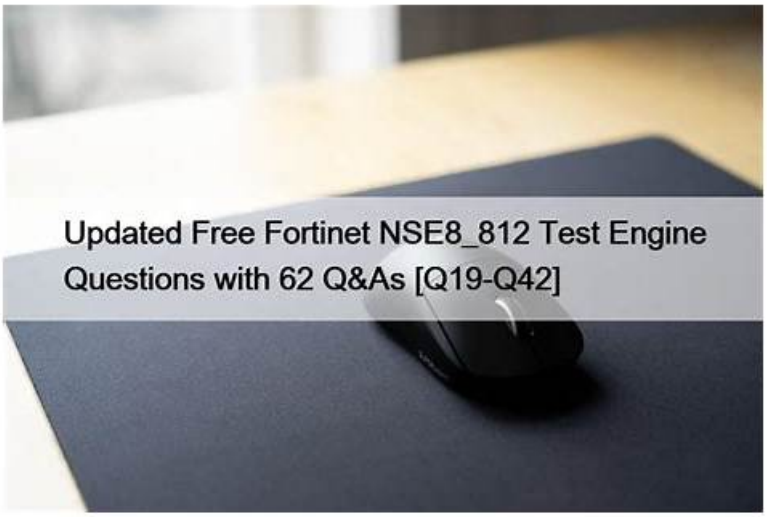
NSE8_812 Demotesten - NSE8_812 Fragenpool



P.S. Kostenlose und neue NSE8_812 Prüfungsfragen sind auf Google Drive freigegeben von ZertSoft verfügbar: https://drive.google.com/open?id=1zNyqB42sk97oXdXXBRpRriitdV__82wB

Unser ZertSoft ist international ganz berühmt. Die Anwendbarkeit von den Schulungsunterlagen ist sehr groß. Sie werden von den IT-Experten nach ihren Kenntnissen und Erfahrungen bearbeitet. Die Feedbacks von den Kandidaten haben sich gezeigt, dass unsere Prüdukte eher von guter Qualität sind. Wenn Sie einer der IT-Kandidaten sind, sollen Sie die Schulungsunterlagen zur Fortinet NSE8_812 Zertifizierungsprüfung von ZertSoft ohne Zweifel wählen.

Die Fortinet NSE8_812 -Zertifizierungsprüfung ist ein wichtiger Berechtigungsnachweis für Network -Sicherheitsfachleute, die mit Fortinet -Produkten und -Lösungen zusammenarbeiten. Wenn Sie diese Prüfung bestehen, können Sie Ihr Fachwissen in der Netzwerksicherheit nachweisen und Ihre Karriere in diesem Bereich vorantreiben. Wenn Sie an dieser Zertifizierung interessiert sind, ist es wichtig, sich gründlich vorzubereiten und alle in der Prüfung behandelten Themen ein solides Verständnis zu haben.

>> NSE8_812 Demotesten <<

NSE8_812 Fragenpool & NSE8_812 Unterlage

Wie viel wissen Sie über ZertSoft? Haben Sie Prüfungsfragen und Antworten zur Fortinet NSE8_812 IT-Zertifizierung von ZertSoft benutzt? Oder Haben Sie von anderen die ZertSoft Prüfungsunterlagen gehört? Als der professionelle Lieferant der IT-Zertifizierungsprüfungen, ist ZertSoft unbedingt die beste Website, die Sie nie gesehen haben. Warum sind wir so zuversichtlich? Weil es keine andere Website wie wir ZertSoft gibt， die die besten NSE8_812 Unterlagen und den besten Service anbieten.

Die NSE8_812 -Prüfung deckt ein breites Spektrum von Themen ab, einschließlich Prinzipien für Netzwerksicherheit, Sicherheitsprotokolle, fortschrittlicher Bedrohungsschutz, Netzwerksicherheitsrichtlinien und Sicherheitsmanagement. Die Prüfung soll Ihre Fähigkeit testen, komplexe Netzwerksicherheitsprobleme zu lösen und Ihr Wissen auf reale Szenarien anzuwenden. Die Prüfung besteht aus Multiple-Choice-Fragen und virtuellen Laborübungen, die reale Szenarien simulieren, um Ihre Fähigkeit zum Entwerfen und Verwalten erweiterter Sicherheitslösungen zu bewerten.

Fortinet NSE 8 - Written Exam (NSE8_812) NSE8_812 Prüfungsfragen mit Lösungen (Q26-Q31):

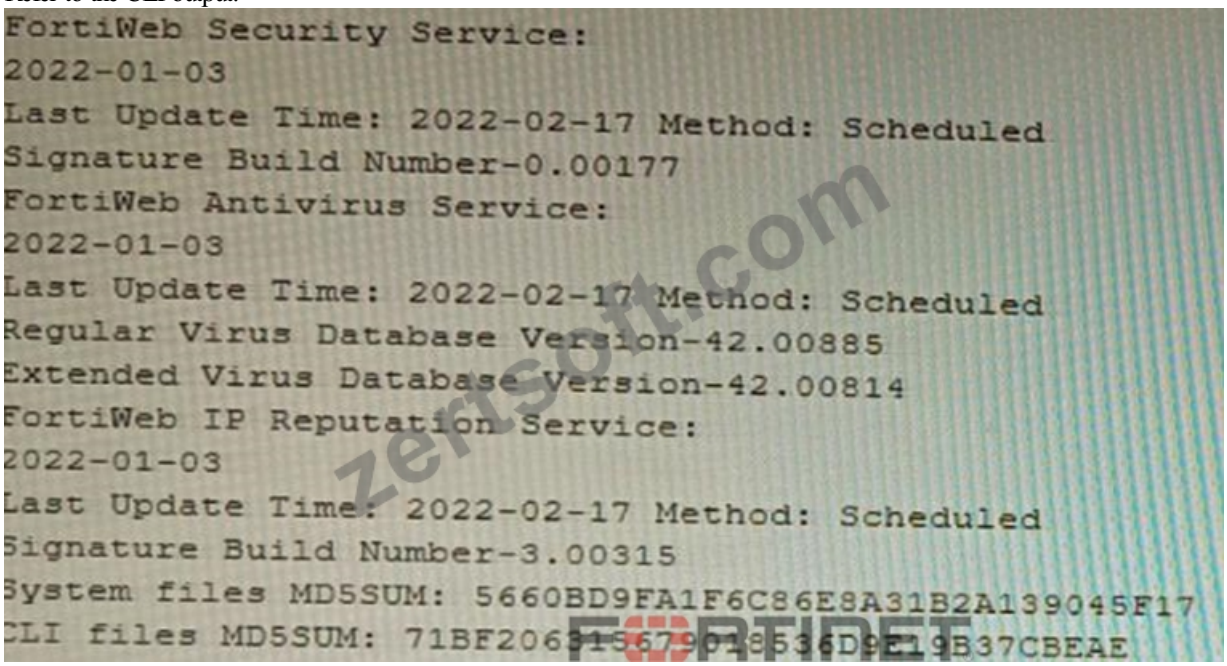
26. Frage
Refer to The exhibit showing a FortiEDR configuration.

Based on the exhibit, which statement is correct?

- A. The presence of a cryptolocker malware at rest on the filesystem will be detected by the Ransomware Prevention security policy.
- B. If a malicious file is executed and attempts to establish a connection it will generate duplicate events.
- C. FortiEDR Collector will not collect OS Metadata.
- D. If an unresolved file rule is triggered, by default the file is logged but not blocked.

Antwort: D

27. Frage
Refer to the CLI output:



Given the information shown in the output, which two statements are correct? (Choose two.)

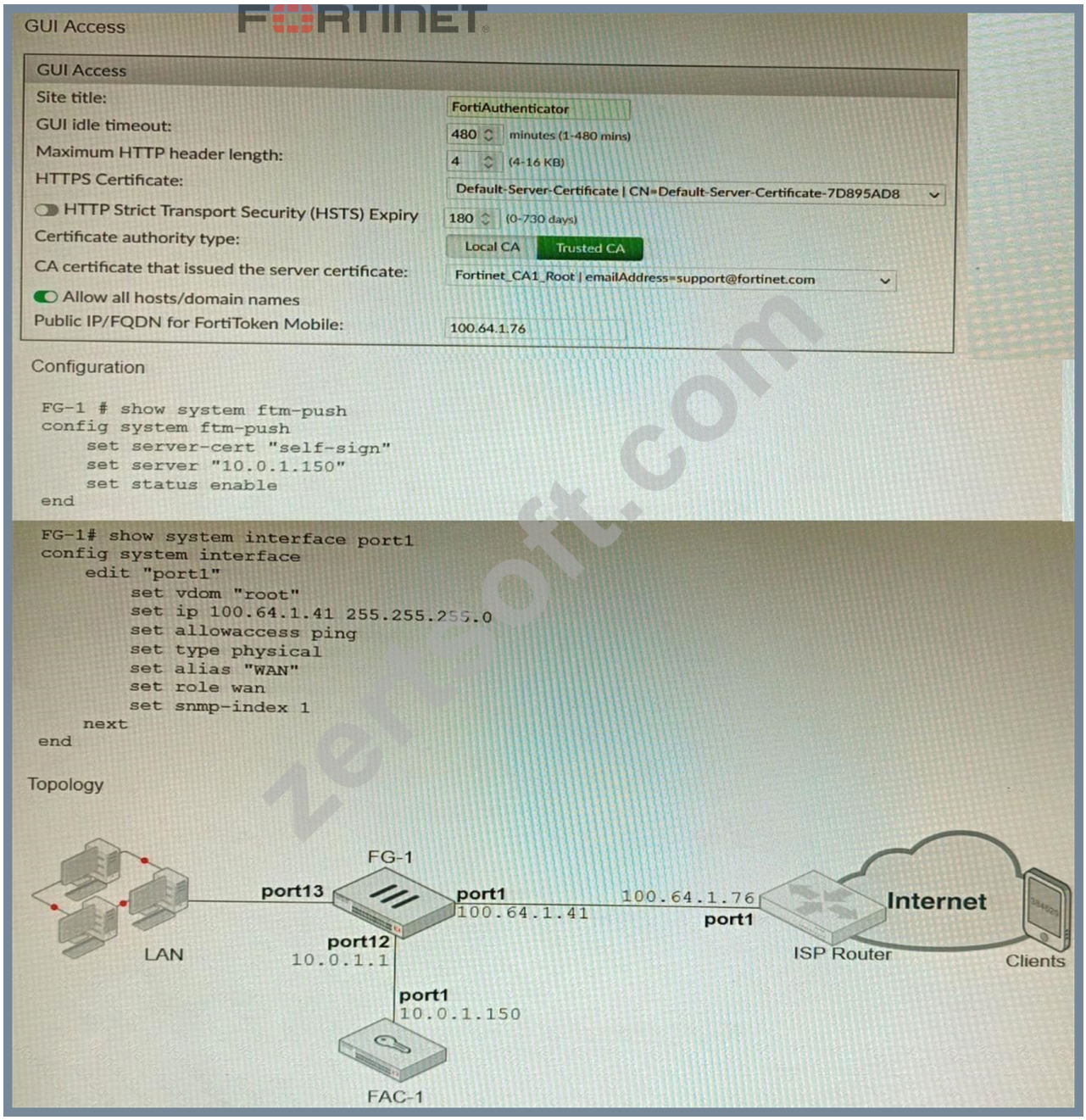
- A. Attackers can be blocked before they target the servers behind the FortiWeb.
- B. Geographical IP policies are enabled and evaluated after local techniques.
- C. The IP Reputation feature has been manually updated
- D. An IP address that was previously used by an attacker will always be blocked
- E. Reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored

Antwort: A,E

Begründung:
The CLI output shown in the exhibit indicates that FortiWeb has enabled IP Reputation feature with local techniques enabled and

geographical IP policies enabled after local techniques (set geoip-policy-order after-local). IP Reputation feature is a feature that allows FortiWeb to block or allow traffic based on the reputation score of IP addresses, which reflects their past malicious activities or behaviors. Local techniques are methods that FortiWeb uses to dynamically update its own blacklist based on its own detection of attacks or violations from IP addresses (such as signature matches, rate limiting, etc.). Geographical IP policies are rules that FortiWeb uses to block or allow traffic based on the geographical location of IP addresses (such as country, region, city, etc.). Therefore, based on the output, one correct statement is that attackers can be blocked before they target the servers behind the FortiWeb. This is because FortiWeb can use IP Reputation feature to block traffic from IP addresses that have a low reputation score or belong to a blacklisted location, which prevents them from reaching the servers and launching attacks. Another correct statement is that reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored. This is because FortiWeb can use local techniques to remove IP addresses from its own blacklist if they stop sending malicious traffic for a certain period of time (set local-techniques-expire-time), which allows them to regain their reputation and access the servers. This is useful for IP addresses that are dynamically assigned by DHCP or PPPoE and may change frequently. References:
https://docs.fortinet.com/document/fortiweb/6.4.0/administration-guide/19662/ip-reputation
https://docs.fortinet.com/document/fortiweb/6.4.0/administration-guide/19662/geographical-ip-policies

28. Frage
Refer to the exhibits.



An administrator has configured a FortiGate and Forti Authenticator for two-factor authentication with FortiToken push notifications

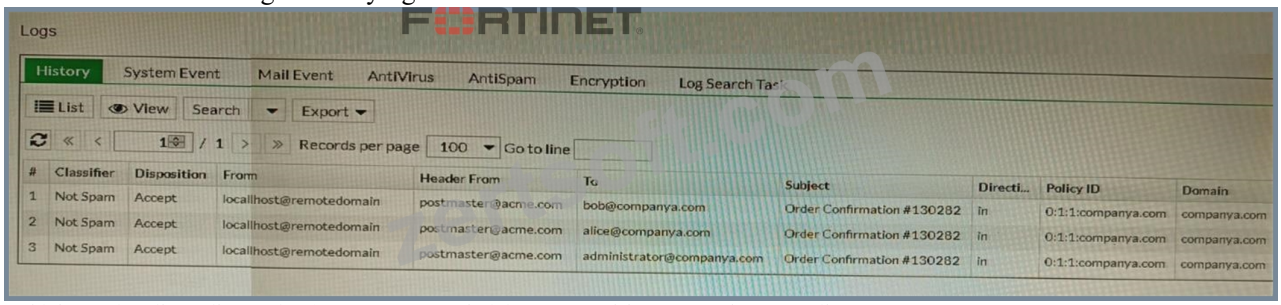
for their SSL VPN login. Upon initial review of the setup, the administrator has discovered that the customers can manually type in their two-factor code and authenticate but push notifications do not work Based on the information given in the exhibits, what must be done to fix this?

- A. On FAC-1, the FortiToken public IP setting must point to 100.64.1 41
- B. FAC-1 must have an internet routable IP address for push notifications.
- C. On FG-1 CLI, the ftm-push server setting must point to 100.64.141.
- D. On FG-1 port1, the ftm access protocol must be enabled.

Antwort: A

Begründung:
https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-FortiToken-Push-on-FortiAuthenticator- operation/ta-p/190810

29. Frage
Refer to the exhibit showing the history logs from a FortiMail device.



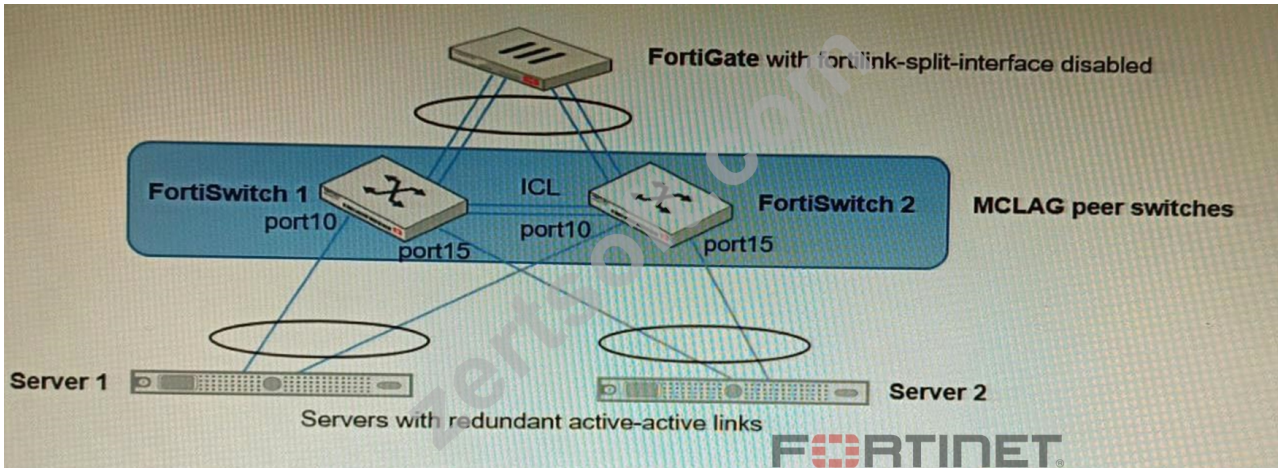
Which FortiMail email security feature can an administrator enable to treat these emails as spam?

- A. DKIM validation in a session profile
- B. Soft fail SPF validation in an antispam profile
- C. Sender domain validation in a session profile
- D. Impersonation analysis in an antispam profile

Antwort: D

Begründung:
Impersonation analysis is a feature that detects emails that attempt to impersonate a trusted sender, such as a company executive or a well-known brand, by using spoofed or look-alike email addresses. This feature can help prevent phishing and business email compromise (BEC) attacks. Impersonation analysis can be enabled in an antispam profile and applied to a firewall policy.
References: https://docs.fortinet.com/document
/fortimail/6.4.0/administration-guide/103663/impersonation-analysis
https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/221814/protecting-against-email-impersonation- in-fortimail

30. Frage
Refer to the exhibit.



You have been tasked with replacing the managed switch Forti Switch 2 shown in the topology.
Which two actions are correct regarding the replacement process? (Choose two.)

- A. After replacing the FortiSwitch unit, the automatically created trunk name does not change
- B. After replacing the FortiSwitch unit, the automatically created trunk name changes.
- C. CLAG-ICL needs to be manually reconfigured once the new switch is connected to the FortiGate
- D. MCLAG-ICL will be automatically reconfigured once the new switch is connected to the FortiGate.

Antwort: A,C

Begründung:
* A is correct because the automatically created trunk name is based on the MAC address of the FortiSwitch unit. When the FortiSwitch unit is replaced, the MAC address will change, but the trunk name will not change.
* B is correct because CLAG-ICL is a manually configured link aggregation group. When the FortiSwitch unit is replaced, the CLAG-ICL configuration will need to be manually reconfigured on the new FortiSwitch unit.
The other options are incorrect. Option C is incorrect because the automatically created trunk name does not change when the FortiSwitch unit is replaced. Option D is incorrect because MCLAG-ICL is a manually configured link aggregation group and will not be automatically reconfigured when the FortiSwitch unit is replaced.
References:
* Configuring link aggregation on FortiSwitches | FortiSwitch / FortiOS 7.0.4 - Fortinet Document Library
* Managing FortiLink | FortiGate / FortiOS 7.0.4 - Fortinet Document Library
https://docs.fortinet.com/document/fortiswitch/7.0.8/devices-managed-by-fortios/173284/replacing-a- managed-fortiswitch-unit

31. Frage
.....

myportal.utt.edu.tt, Disposable vapes

BONUS!!! Laden Sie die vollständige Version der ZertSoft NSE8_812 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1zNyqB42sk97oXdXXBRpRriitdV__82wB