PassQueen
a.k.a dumpsqueen.com

FCPFortiSandbox 5.0 Administrator

Fortinet FCP_FSA_AD-5.0

Version Demo

Total Demo Questions: 5

Total Premium Questions: 53

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiSandbox Deployment and Configuration	21
Topic 2, FortiSandbox Administration	9
Topic 3, FortiSandbox Integration	17
Topic 4, FortiSandbox Troubleshooting	6
Total	53

QUESTION NO: 1

You are attempting to troubleshoot a FortiGate device that is not sending samples to FortiSandbox. Which CLI command will provide you with useful diagnostic information? (Choose one answer)

A. diagnose antivirus quarantine purge

B. diagnose test application quarantined 8

C. diagnose test application ipsmonitor 99

D. diagnose debug application quarantine -1

ANSWER: D

Explanation:

`diagnose debug application quarantine -1` is the appropriate diagnostic command because FortiGate uses its quarantine process to handle file submissions to FortiSandbox. Enabling debug output at level `-1` provides detailed messages from that process, allowing an administrator to observe events associated with sample submission and communication with the configured FortiSandbox appliance. This information is useful for identifying operational issues such as attempts to submit a file, connection failures, transfer-related events, and responses associated with sandbox analysis.

In practice, the command configures the application-specific debug stream; debugging must then be activated globally with `diagnose debug enable` so that messages are displayed. Administrators should reproduce the issue while collecting the output, then disable debugging with `diagnose debug disable` when finished. Fortinet's FortiGate documentation describes the use of CLI debugging commands to gather detailed runtime information during troubleshooting, while FortiSandbox documentation covers the FortiGate integration used to submit suspicious files for analysis. See the FortiGate Administration Guide and the FortiSandbox documentation portal.

QUESTION NO: 2

Which two statements are true about creating an API interface? (Choose two answers)

A. Ports configured for HA communication can also be configured as API ports.

B. API ports will not accept HTTP traffic.

C. The configuration must be performed using the CLI

D. The interface must also be designated as an administrative interface.

ANSWER: B C

Explanation:

"API ports will not accept HTTP traffic." is correct because FortiSandbox API communications use HTTPS on TCP port 4443. This provides encrypted management and integration connectivity, including communication used when a FortiGate submits files to FortiSandbox for inline scanning. An API-enabled interface therefore does not expose an unencrypted HTTP API service.

"The configuration must be performed using the CLI" is also correct for FortiSandbox 5.0. The API interface is enabled by assigning an interface with the CLI command `set api-port <interface>` in the relevant system configuration. This explicitly identifies the port that will listen for API requests on the FortiSandbox HTTPS API service. A reachable IP address and appropriate network routing for that interface are also required for external devices to use the service, but the API-port assignment itself is made from the CLI.

Fortinet's FortiSandbox documentation describes API access and its HTTPS transport requirements, while the product documentation portal provides the version-specific administration references for interface and appliance configuration: FortiSandbox documentation and FortiSandbox 5.0 Administration Guide.

QUESTION NO: 3

You are asked to configure a FortiSandbox HA cluster. Port 4 on the primary and secondary nodes is dedicated for HA-specific communication. Which command must you use to configure the primary node? (Choose one answer)

A. hc-settings -sc -tN -nPrimaryNode -cFSAGrp -p -iport4

B. hc-settings -sc -tR -nPrimaryNode -cFSAGrp -p -iport4

C. hc-settings -sc -tF -nPrimaryNode -cFSAGrp -p -iport4

D. hc-settings -sc -tM -nPrimaryNode -cFSAGrp -p -iport4

ANSWER: D

Explanation:

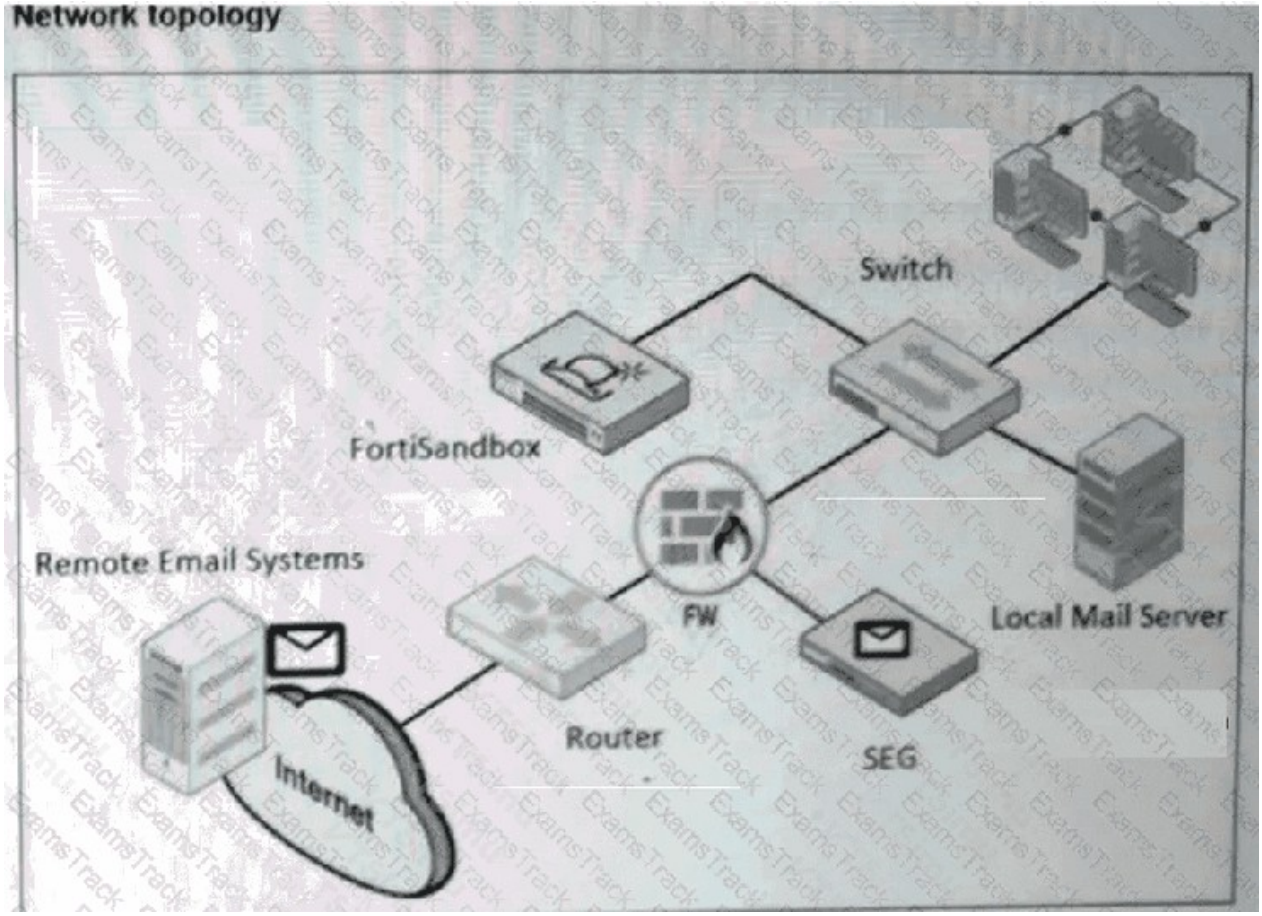
`hc-settings -sc -tM -nPrimaryNode -cFSAGrp -p -iport4` is the appropriate command for configuring the primary FortiSandbox appliance in this HA scenario. FortiSandbox HA configuration is performed from the CLI, using the `hc-settings` command to define the cluster's fundamental parameters. These parameters include the local node alias, the cluster group name, group password, and the dedicated interface used for HA communication.

The `-tM` setting identifies the system as the master node, which is the primary member of the HA pair. The node name supplied with `-nPrimaryNode` establishes the primary appliance alias, while `-cFSAGrp` assigns the appliance to the specified HA cluster group. The `-p` parameter is used to provide or prompt for the shared cluster password, depending on the command environment and software version. Finally, `-iport4` assigns port4 as the HA interface. Both cluster members must use their dedicated HA-connected interfaces for synchronization and HA-specific traffic, so selecting port4 directly fulfills the stated topology requirement.

Fortinet's FortiSandbox documentation describes HA configuration and CLI administration in the FortiSandbox 5.0 Administration Guide. General versioned FortiSandbox documentation is also available from the Fortinet documentation portal.

QUESTION NO: 4

Refer to the exhibit.



A network topology is shown. Which two important steps must you take before you enable a BCC adapter on FortiSandbox? (Choose two answers)

A. Configure the upstream SEG to extract files and URLs from emails and send them to FortiSandbox for analysis.

B. Configure an A record on the DNS server for the FortiSandbox IP.

C. Configure the sub-domain on the upstream SEG to BCC emails to FortiSandbox.

D. Add an MX record on the DNS server for the BCC email sub-domain to resolve to the FortiSandbox IP.

ANSWER: C D

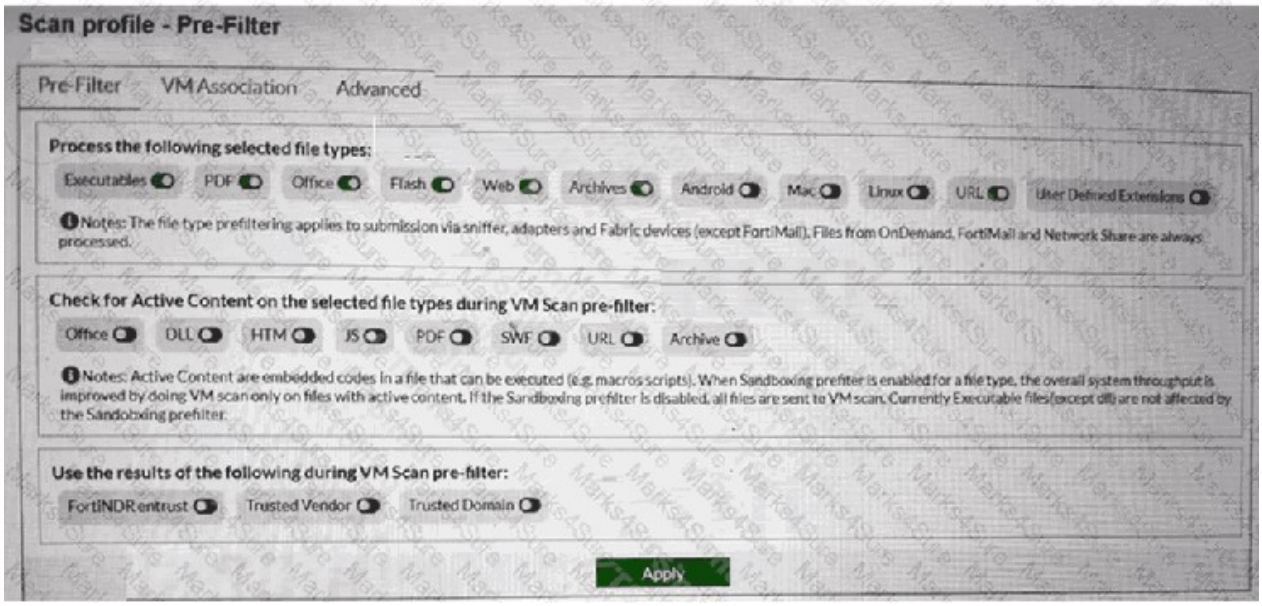
Explanation:

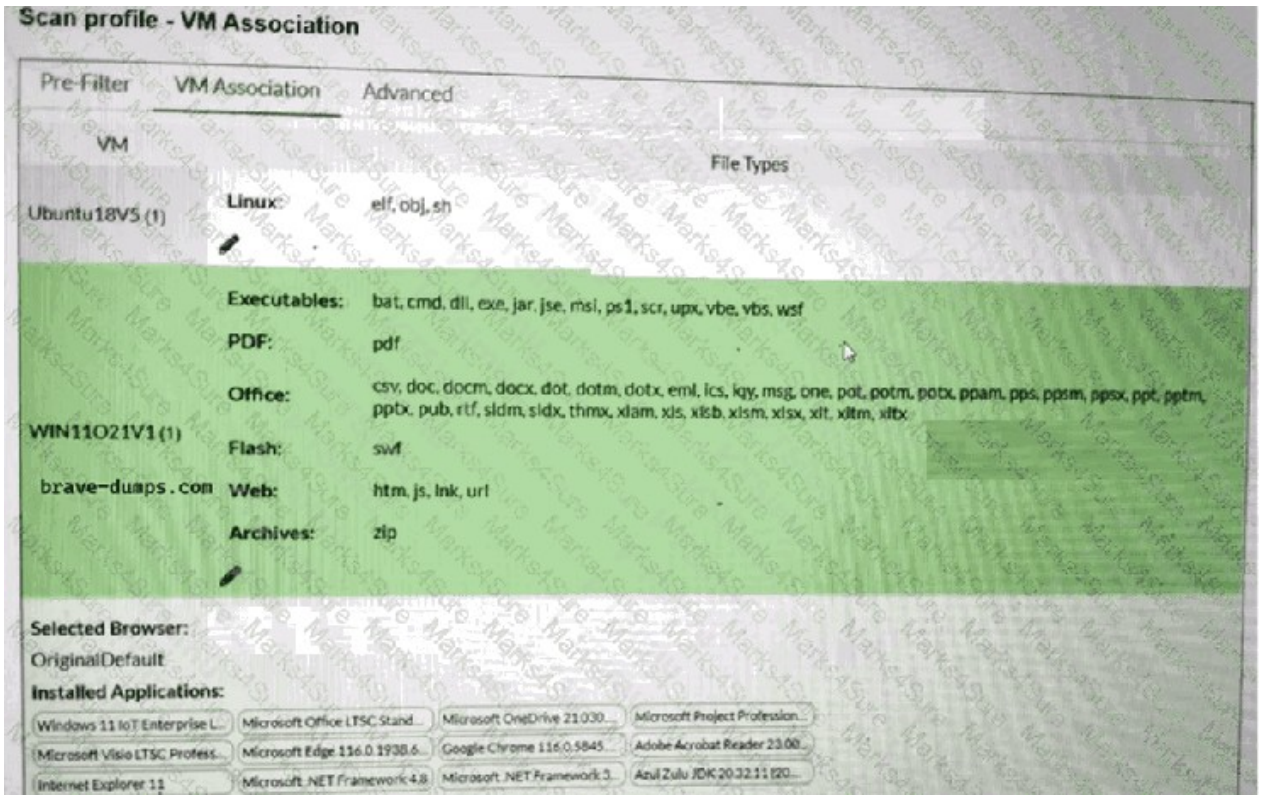
A FortiSandbox BCC adapter receives complete copies of email messages from an upstream secure email gateway or mail transfer agent. Therefore, **Configure the sub-domain on the upstream SEG to BCC emails to FortiSandbox** is required so the upstream mail system sends a copy of each applicable message to the dedicated FortiSandbox BCC address. FortiSandbox can then parse the delivered message and submit discovered attachments and URLs for analysis.

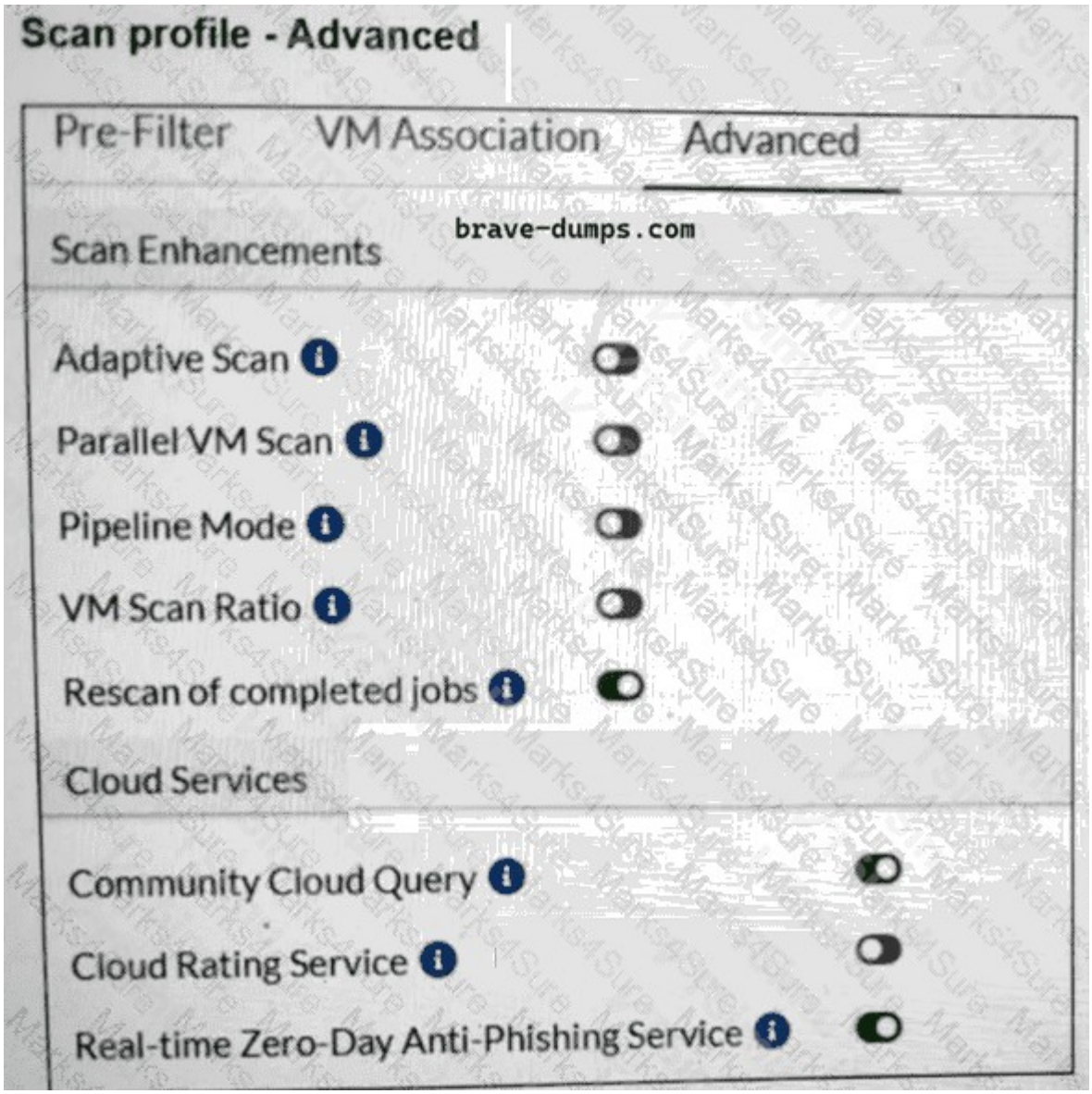
Add an MX record on the DNS server for the BCC email sub-domain to resolve to the FortiSandbox IP is also required because SMTP delivery is based on DNS mail-exchanger lookups. The BCC subdomain must be routable to the FortiSandbox appliance so that the SEG can successfully deliver the copied messages to its SMTP listener. Together, the SEG BCC-routing configuration and the DNS MX configuration establish the mail-delivery path needed before enabling and using the adapter. Fortinet documents BCC adapter deployment as an email-submission method in the FortiSandbox Administration Guide: FortiSandbox 5.0 Administration Guide. The DNS role of MX records in directing SMTP mail is defined in RFC 5321.

QUESTION NO: 5

Refer to the exhibits.


Scan profile - Pre-Filter
Pre-Filter
VM Association
Advanced
Process the following selected file types:
Executables
PDF
Office
Flash
Web
Archives
Android
Mac
Linux
URL
User Defined Extensions
Notes: The file type prefiltering applies to submission via sniffer, adapters and Fabric devices (except FortiMail). Files from OnDemand, FortiMail and Network Share are always processed.
Check for Active Content on the selected file types during VM Scan pre-filter:
Office
DLL
HTM
JS
PDF
SWF
URL
Archive
Notes: Active Content are embedded codes in a file that can be executed (e.g. macros scripts). When Sandboxing prefilter is enabled for a file type, the overall system throughput is improved by doing VM scan only on files with active content. If the Sandboxing prefilter is disabled, all files are sent to VM scan. Currently Executable files(except dll) are not affected by the Sandobxing prefilter.
Use the results of the following during VM Scan pre-filter:
FortiNDR entrust
Trusted Vendor
Trusted Domain
Apply


Scan profile - VM Association
Pre-Filter
VM Association
Advanced
VM
File Types
Ubuntu18V5 (1)
Linux:
elf, obj, sh
Executables:
bat, cmd, dll, exe, jar, jse, msi, ps1, scr, upx, vbe, vbs, wsf
PDF:
pdf
Office:
csv, doc, docm, docx, dot, dotm, dotx, eml, ics, iqy, msg, one, pot, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, pub, rtf, sldm, sldx, thmx, xlam, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx
WIN11O21V1 (1)
Flash:
swf
brave-dumps.com
Web:
htm, js, lnk, url
Archives:
zip
Selected Browser:
OriginalDefault
Installed Applications:
Windows 11 IoT Enterprise L...
Microsoft Office LTSC Stand...
Microsoft OneDrive 21.030...
Microsoft Project Profession...
Microsoft Visio LTSC Profess...
Microsoft Edge 116.0.1938.6...
Google Chrome 116.0.5845...
Adobe Acrobat Reader 23.00...
Internet Explorer 11
Microsoft .NET Framework 4.8
Microsoft .NET Framework 3...
Azul Zulu JDK 20.32.11 (20...



You are asked to configure a FortiSandbox to leverage the real-time anti-phishing (RTAP) feature. After configuring the scan profile, testing shows that URLs are not being submitted to the RTAP service. What could cause this issue? (Choose one answer)

A. The URL option is not selected as a Web file type.

B. The WEBLink file type is not selected in the profile.

C. The VM scan timeout for URLs should be at least 300 to provide enough time for a FortiGuard response.

D. The URLs are not designated for active content pre-scan.

ANSWER: B

Explanation:

The WEBLink file type is not selected in the profile. FortiSandbox treats a submitted URL as a WEBLink input rather than as a conventional file whose extension happens to be `.url`. Therefore, enabling the URL extension under the Web file-type association does not by itself ensure that URL submissions are assigned to a virtual-machine scan workflow. The scan profile must explicitly include the WEBLink type in its VM association so that the submitted URL reaches the VM scan engine. RTAP evaluation occurs as part of that processing path; consequently, the RTAP setting can be enabled while no URL is sent for RTAP analysis if WEBLink is absent from the assigned types. This distinction is important when URLs originate from an integrated product such as FortiMail, because the integration submits the URL as a URL/WEBLink object for sandbox analysis, not merely as a local `.url` file. Configure the profile's VM association to cover WEBLink, save the profile, and ensure that the submitting device is using that profile. Fortinet's FortiSandbox documentation describes scan

profiles and VM associations in the Scan profile section, and provides product documentation access through the FortiSandbox 5.0 documentation portal.