PassQueen
a.k.a dumpsqueen.com

Forescout Certified Professional Exam

Forescout FSCP

Version Demo

Total Demo Questions: 10

Total Premium Questions: 101

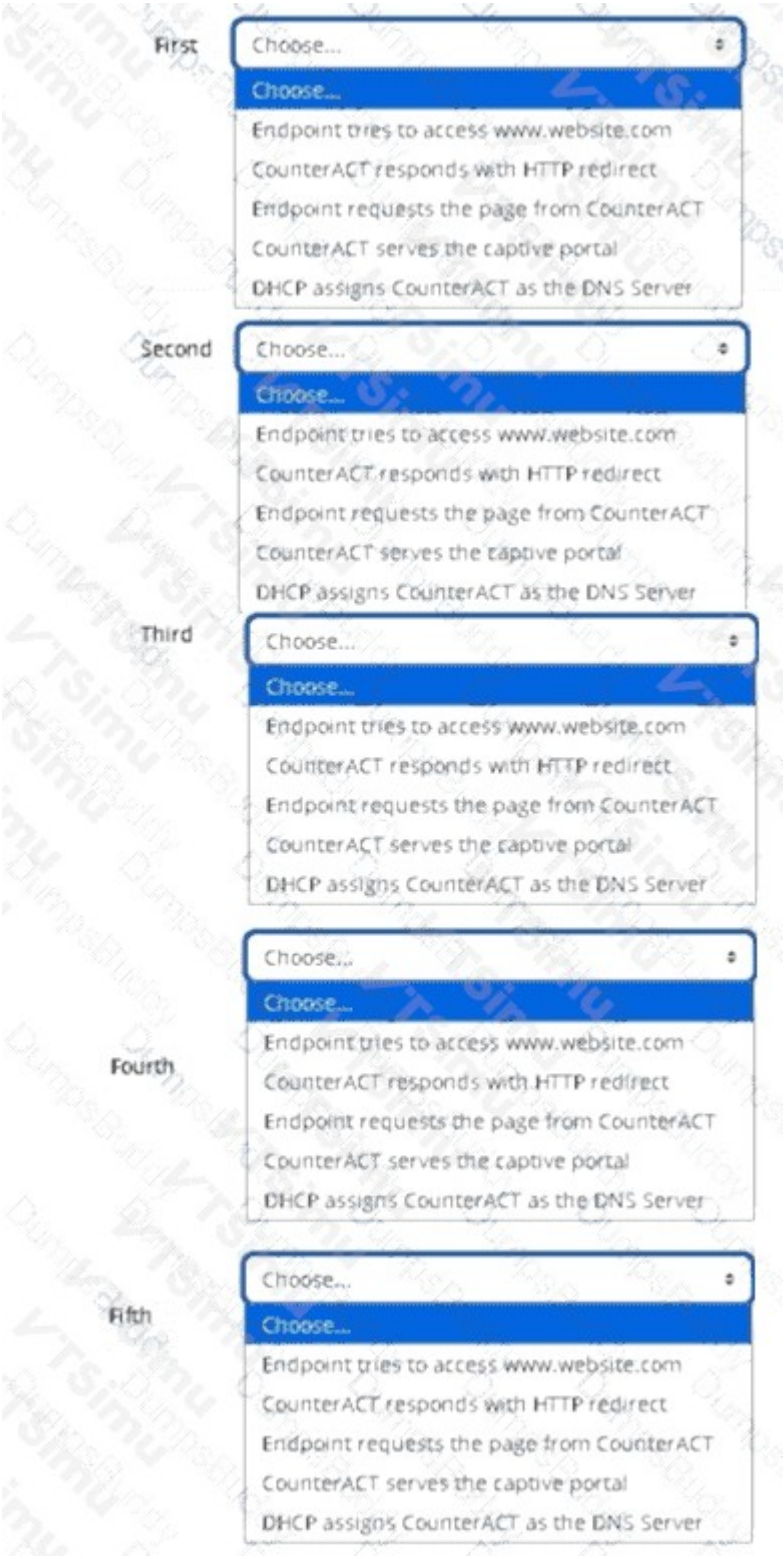
Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1 - (SIMULATION)

Place the DNS Enforce control actions into the correct workflow order for endpoints which have a pending control action.



ANSWER: Check the explanation for the answer

Explanation:

Place the DNS Enforce workflow in this order:

1. **DHCP assigns CounterACT as the DNS Server**
2. **Endpoint tries to access www.website.com**
3. **CounterACT responds with HTTP redirect**
4. **Endpoint requests the page from CounterACT**
5. **CounterACT serves the captive portal**

DNS Enforce first causes the endpoint to use CounterACT for DNS through DHCP. When the endpoint browses to a website, it is directed to CounterACT, which redirects the HTTP request and then presents the captive portal.

QUESTION NO: 2

Select the action that requires symmetrical traffic.

A. Assign to VLAN

B. WLAN block

C. Endpoint ACL

D. Start SecureConnector

E. Virtual Firewall

ANSWER: C

Explanation:

Endpoint ACL is the action that requires symmetrical traffic. An Endpoint ACL is an address-based access-control mechanism that Forescout applies to limit an endpoint's permitted network communication. To build and maintain this control accurately, the Forescout platform must have visibility into both directions of the endpoint's traffic flow. Symmetric traffic visibility allows the appliance to associate the endpoint identity and address information with the complete conversation and apply the relevant ACL behavior consistently for traffic sent by, and returned to, that endpoint.

This requirement is important in a passive monitoring deployment because traffic visibility can be affected by SPAN, TAP, routing, or aggregation design. If only one side of a conversation reaches the appliance, Forescout cannot reliably observe the full communication context needed for endpoint-address ACL enforcement. Administrators should therefore verify that monitored paths provide bidirectional, symmetric visibility before using this type of control action in policy.

Forescout's product documentation and support resources describe deployment planning, traffic visibility, and switch-based enforcement considerations for policy actions. See the Forescout Resources portal and the Forescout Documentation portal for the applicable Platform Administration Guide and Switch Plugin documentation for the deployed version.

QUESTION NO: 3

An organisation is reviewing FLEXX licensing before expanding a Forescout deployment. Which two statements are true? (Choose two)

A. Licensing is centralized and managed by an Enterprise Manager

B. For member appliances, HA and Failover Clustering are part of Resiliency licensing

C. Failover Clustering is used with Enterprise Manager and Remote Module appliances

D. Disaster Recovery is the resiliency feature used for member appliances

E. Each appliance must maintain an unrelated local FLEXX license pool

ANSWER: A B

Explanation:

Licensing is centralized and managed by an Enterprise Manager is correct because FLEXX licensing is administered centrally for the deployment rather than being managed independently on each appliance. **For member appliances, HA and Failover Clustering are part of Resiliency licensing** is also correct.

Failover Clustering is not an Enterprise Manager and Remote Module feature, and Disaster Recovery is not the member-appliance licensing model described for HA and Failover Clustering.

QUESTION NO: 4

A policy identifies corporate Windows endpoints with antivirus definitions that are out of date. The security team wants the policy to correct the condition when possible rather than immediately remove network access. Which action is the best remediation action?

A. Assign to VLAN

B. Start Antivirus update

C. Switch port block

D. Start SecureConnector

E. Endpoint Address ACL

ANSWER: B

Explanation:

Start Antivirus update is correct because it initiates a corrective operation intended to bring the endpoint into compliance. After the endpoint updates its antivirus definitions, Forescout can reevaluate its posture and apply the appropriate compliant-state handling.

Assigning a VLAN or blocking a switch port are network-enforcement actions, not remediation actions. Starting SecureConnector may support later management capabilities but does not directly correct outdated antivirus content.

QUESTION NO: 5

A Change VLAN action is configured in a policy, but no endpoint ports are reassigned. Which two items should be verified as part of the initial switch-action troubleshooting? (Choose two)

A. Verify that the switch model is compatible with the Change VLAN action.

B. Verify that the managing appliance is allowed to make VLAN changes on the switch.

C. Verify that the Enterprise Manager has read-only VLAN access to the switch.

D. Verify that Switch Auto Discovery is enabled for the switch.

E. Verify that only SNMP Get traffic is permitted to the switch.

ANSWER: A B

Explanation:

The **switch model must support the Change VLAN action**, because support is determined at the model and action level. In addition, the **managing appliance must have permission to make VLAN changes**; read-only switch access is insufficient for a write operation.

Switch auto-discovery does not grant permission to modify VLANs, and the Enterprise Manager does not normally perform the member appliance's local switch-management function. SNMP Get access can help retrieve information, but a VLAN change requires the applicable write capability, such as SNMP Set where that method is used.

QUESTION NO: 6

What should be done after the Managed Windows devices are sent to a policy to determine the Windows 10 patch delivery optimization setting?

A. Push out the proper DWORD setting via GPO

B. Non Windows 10 devices must be called out in sub-rules since they will not have the relevant DWORD

C. Manageable Windows devices are not required by this policy

D. Non Windows 10 devices must be called out in sub-rules so that the relevant DWORD value may be changed

E. Write sub-rules to check for each of the DWORD values used in patch delivery optimization

ANSWER: E

Explanation:

Write sub-rules to check for each of the DWORD values used in patch delivery optimization. Delivery Optimization behavior is determined by Windows policy settings, principally the `DODownloadMode` DWORD in the Delivery Optimization policy registry location. A Forescout policy can first scope managed Windows endpoints and then use sub-rules to evaluate the discovered registry value for the applicable delivery mode. This creates a clear, granular view of which endpoints use each configured mode and lets the administrator associate policy actions, reporting, or remediation workflow with the matching condition. Evaluating each relevant DWORD value through distinct sub-rules is especially useful when different device populations have approved but different Delivery Optimization configurations, or when the organization needs to identify endpoints that do not match the expected setting. The approach is a detection and classification step: Forescout determines the endpoint's current state before any corrective process is selected. Microsoft documents Delivery Optimization download modes and their corresponding policy values, including HTTP-only and peer-assisted modes, in its Delivery Optimization reference. For policy construction concepts, Forescout documentation describes how policies and sub-rules provide layered matching criteria for endpoint classification and control. See Microsoft Delivery Optimization reference and Forescout Documentation Portal.

QUESTION NO: 7

When using Remote Inspection for Windows, which of the following properties require fsprocsvc.exe interactive scripting?

A. User Directory Common Name

B. Update Microsoft Vulnerabilities

C. Windows Expected Script Result

D. Antivirus Running

E. Windows Service Running

ANSWER: C

Explanation:

Windows Expected Script Result is the Remote Inspection property that requires `fsprocsvc.exe` interactive scripting. This property evaluates the result returned by a script executed on the Windows endpoint. In Remote Inspection deployments, Forescout uses its endpoint-side process service when an inspection task must run interactively rather than being collected solely through ordinary remote-management queries. The service enables the required script execution in the endpoint context and returns the resulting value to the Forescout platform, where the policy can compare it with the expected result.

This capability is especially important when an organization needs to validate a custom endpoint condition that is not represented by a standard inventory value. For example, a policy can use a script to test a local configuration, inspect an application-specific state, or retrieve a value generated by local command execution, then use the expected script result as a classification or compliance condition. Forescout documentation identifies the process service as a component used for

interactive scripts during Windows Remote Inspection and lists Windows Expected Script Result among the properties that require it. Consult the Forescout Documentation Portal for the applicable HPS Inspection Engine guide and the Forescout Platform overview for product context.

QUESTION NO: 8

Which of the following plugins assists in classification for computer endpoints? (Choose two)

A. Switch

B. HPS Inspection Engine

C. Linux Plugin

D. Advanced Tools

E. DNS Client

ANSWER: B D

Explanation:

HPS Inspection Engine and **Advanced Tools** assist Forescout Platform with computer-endpoint classification. HPS Inspection Engine supplies core inspection and classification capabilities that gather endpoint evidence through active and passive methods. This evidence can include protocol and service information, TCP/IP fingerprinting, banner data, and other observations that let policies identify endpoint type, network function, and relevant characteristics. The classification information is then available to policy conditions and actions, enabling the platform to apply the appropriate controls to discovered devices.

Advanced Tools complements that process by resolving additional endpoint details useful for classification, including operating-system, hardware, vendor, and installed-software characteristics. Enriched properties provide more precise visibility into managed and unmanaged computers and support policy decisions based on the endpoint attributes Forescout discovers. Together, these capabilities are part of the endpoint discovery, assessment, and classification workflow used by the Forescout Platform rather than merely performing network-device administration or DNS resolution. Forescout describes this overall device visibility and control approach on its Forescout Platform product page; product documentation is available through the Forescout documentation portal.

QUESTION NO: 9

An administrator is designing a policy hierarchy for unmanaged IoT devices and managed IT workstations. Which two practices support the recommended policy flow? (Choose two)

A. Modify as little as possible in discovery

B. Flow classified endpoints to an assessment policy

C. Apply broad enforcement actions during initial discovery

D. Use IoT classification primarily to identify endpoint ownership

E. Use IT classification primarily to determine endpoint manageability

ANSWER: A B

Explanation:

Modify as little as possible in discovery is correct because discovery should establish visibility and collect endpoint context without unnecessarily changing endpoint or network behavior. **Flow classified endpoints to an assessment policy** is also correct because assessment should be applied after the endpoint has been placed into an appropriate classification.

IoT classification commonly focuses on manageability, while IT classification commonly indicates ownership. Discovery policies should not normally apply broad enforcement actions before sufficient endpoint context has been established.

QUESTION NO: 10

When creating a new "Send Mail" notification action, which email is used by default?

A. The email configured under Options > General > Mail

B. The email address of the last logged in user

C. The Tech Support email

D. The email that was used when registering the license

E. The email entered in the send mail action on the rule

ANSWER: A

Explanation:

The email configured under Options > General > Mail is used by default. This setting is the appliance-level mail-notification configuration, where administrators define the addresses that should receive Forescout Platform alerts and notifications. When a Send Mail action is created, Forescout uses that centrally configured notification recipient value as the initial/default email destination. This provides consistent notification handling across policies and avoids requiring each policy author to start by re-entering a standard operational recipient address.

The default is associated with the platform’s general mail settings rather than an individual operator session, a licensing workflow, or a support contact. Administrators can still tailor a particular Send Mail action when a policy requires a different recipient or recipient group, but the preconfigured General mail notification address is the baseline value used for a new action. This behavior reflects the distinction between global notification defaults and policy-specific action configuration. Consult the Forescout documentation portal and support site for the version-specific Administration Guide and the Mail and DNS configuration procedure: Forescout Documentation and Forescout Support.