1Y0-440 ^{Q&As}

Architecting a Citrix Networking Solution

Pass Citrix 1Y0-440 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/1y0-440.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Citrix Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Scenario: A Citrix Architect has deployed two MPX devices, 12.0.53.13 nc and MPX 11500 models, in high availability (HA) pair for the Workspace labs team. The deployment method is two-arm and the devices are installed behind a CISCO ASA 5585 Firewall. The architect enabled the following features on the NetScaler devices. Content Switching, SSL Offloading, Load Balancing, NetScaler Gateway, Application Firewall in hybrid security and Appflow. All are enabled to send monitoring information to NMAS 12.0.53.13 nc build. The architect is preparing to configure load balancing for Microsoft Exchange 2016 server.

The following requirements were discussed during the implementation:

1.

 All traffic needs to be segregated based on applications, and the fewest number of IP addresses should be utilized during the configuration

2.

 All traffic should be secured and any traffic coming into HTTP should be redirected to HTTPS.

3.

 Single Sign-on should be created for Microsoft Outlook web access (OWA).

4.

 NetScaler should recognize Uniform Resource Identifier (URI) and close the session to NetScaler when users hit the Logoff button in Microsoft Outlook web access.

5.

 Users should be able to authenticate using either user principal name (UPN) or sAMAccountName.

6.

 The Layer 7 monitor should be configured to monitor the Microsoft Outlook web access servers and the monitor probes must be sent on SSL

Which monitor will meet these requirements?

A. add lb monitor mon_rpc HTTP-ECV -send "GET /rpc/healthcheck.htm" recv 200 -LRTM DISABLED

B. add lb monitor mon_rpc HTTP-ECV -send "GET /rpc/healthcheck.htm" recv 200 -LRTM ENABLED

C. add lb monitor mon_rpc HTTP -send "GET /rpc/healthcheck.htm" recv 200 -LRTM DISABLED -secure YES

D. add lb monitor mon_rpc HTTP-ECV -send "GET/rpc/healthcheck.htm" recv 200 -LRTM DISABLED secure YES

Correct Answer: A

QUESTION 2

Scenario: A Citrix Architect needs to assess an existing NetScaler configuration. The customer recently found that certain user groups were receiving access to an internal web server with an authorization configuration that does NOT align with the designed security requirements.

Click the Exhibit button view the configured authorization settings for the web server.

Requirements

- By default, no connection should have access to network resources unless authorized based on the other requirements.
- By default, only connections coming from the internal network (192.168.10.0/24) should be permitted to access the web server.
- The Accountants group is authorized to access URLs with a ".zip" extension; all other users must NOT be authorized for this.
- The Executives group is authorized to access the web server from inside OR outside the internal network.

Configurations

Name	Type	Bind Point	Action	Priority	Associated Policy Expressions
Item 1	Authorization setting	Global	DENY	N/A	N/A
Item 2	Authorization Policy	NetScaler traffic management virtual server	ALLOW	1	Client.IP.SRC.IN_SUBNET (192.168.10.0/24)
Item 3	Authorization Policy	NetScaler traffic management virtual server	DENY	2	HTTP.REQ.URL.SUFFIX.EQ ("zip")
Item 4	Authorization Policy	Accountants Group	ALLOW	1	HTTP.REQ.URL.SUFFIX.EQ ("zip")
Item 5	Authorization Policy	Executives Group	ALLOW	1	Client.IP.SRC.NE (192.168.10.0/24)

Which item should the architect change or remove to align the authorization configuration with the security requirements of the organization?

A. Item 1

B. Item 3

C. Item 4

D. Item 5

E. Item 2

Correct Answer: E

QUESTION 3

Scenario: A Citrix Architect and a team of Workspacelab members have met for a design discussion about the NetScaler Design Project. They captured the following requirements:

1.

 Two pairs of NetScaler MPX appliances will be deployed in the DMZ network and the internal network.

2.

 High availability will be accessible between the pair of NetScaler MPX appliances in the DMZ network.

3.

 Multi-factor authentication must be configured for the NetScaler Gateway virtual server.

4.

 The NetScaler Gateway virtual server is integrated with XenApp/XenDesktop environment.

5.

 Load balancing must be deployed for the users from the workspacelab.com and vendorlab.com

domains.

6.

 The logon page must show the workspacelab logo.

7.

 Certificate verification must be performed to identify and extract the username.

8.

 The client certificate must have UserPrincipalName as a subject.

9.

 All the managed workstations for the workspace users must have a client identifications certificate

installed on it.

10.The workspacelab users connecting from a managed workstation with a client certificate on it should be

authenticated using LDAP. 11.The workspacelab users connecting from a workstation without a client

certificate should be authenticated using LDAP and RADIUS.

12.The vendorlab users should be authenticated using Active Directory Federation Service.

13.The user credentials must NOT be shared between workspacelab and vendorlab.

14.Single Sign-on must be performed between StoreFront and NetScaler Gateway.

15.A domain drop down list must be provided if the user connects to the NetScaler Gateway virtual server

externally.

16.The domain of the user connecting externally must be identified using the domain selected from the

domain drop down list.

On performing the deployment, the architect observes that users are always prompted with two-factor authentication when trying to assess externally from an unmanaged workstation.

Click the exhibit button to view the configuration.

```
> show authentication vserver aaa_dmz_001
      aaa_dmz_001 (192.168.30.131:443) - SSL Type: CONTENT
      State: UP
      Client Idle Timeout: 180 sec
      Down state flush: DISABLED
      Disable Primary Vserver On Down : DISABLED
      Network profile name: ???
      Appflow logging: ENABLED
      Authentication : ON
      Device Certificate Check: ???
      Device Certificate CA List: ???
      CGInfra Homepage Redirect : ???
      Current AAA Sessions: 0
      Total Connected Users: 0
      Dtls : ???       L2Conn: ???
      RDP Server Profile Name: ???
      Max Login Attempts: 0    Failed Login Timeout 0
      Fully qualified domain name: ???
      PCoIP VServer Profile name: ???
      Listen Policy: NONE
      Listen Priority: 0
      IcmpResponse: ???
      RHIstate: ???
      Traffic Domain: 0

1)    LoginSchema Policy Name: LDAP_RADIUS     Priority: 100
      GotoPriority Expression: END

1)    Advanced Authentication Policy Name: cert-upn  Priority: 100
      GotoPriority Expression: NEXT
      NextFactor name: OnlyLDAP
2)    Advanced Authentication Policy Name: No_AUTH   Priority: 110
      GotoPriority Expression: NEXT
      NextFactor name: ldap-radius
3)    Advanced Authentication Policy Name: saml-upn  Priority: 120
      GotoPriority Expressions: NEXT

  Done
```

What should the architect do to correct this configuration?

A. Unbind LoginSchema Policy LDAP_RADIUS from the virtual server.

B. Bind the Portal theme as Domaindropdown.

C. Bind the LoginSchema Policy Domaindropdown to priority 90.

D. Bind the Default LoginSchema Policy as Domaindropdown.

Correct Answer: D

QUESTION 4

Which three methods can a Citrix Architect use to assess the capabilities of a network infrastructure? (Choose three.)

A. Review existing monitoring solutions for periods of latency, lost packets, and insufficient bandwidth.

B. Map the location of the users against the existing network topology.

C. Alter firewall rules of existing network to fit into the new NetScaler Deployment.

D. Examine the topology for single points of failure and potential bottlenecks.

E. Ensure that users and computers are in the correct organizational units (OUs).

Correct Answer: ABD

QUESTION 5

Scenario: A Citrix Architect needs to design a NetScaler deployment in Microsoft Azure. An Active-Passive NetScaler VPX pair will provide load balancing for three distinct web applications. The architect has identified the following requirements:

1.

Minimize deployment costs where possible.

2.

Provide dedicated bandwidth for each web application.

3.

Provide a different public IP address for each web application.

For this deployment, the architect should configure each NetScaler VPX machine to have _____ network interface(s) and configure IP address by using _____. (Choose the correct option to complete the sentence).

A. 4; Port Address Translation

B. 1; Network Address Translation

C. 1; Port Address Translation

D. 2; Network Address Translation

E. 4; Network Address Translation

F. 2; Port Address Translation

Correct Answer: C