1Y0-440 Q&As

Architecting a Citrix Networking Solution

Pass Citrix 1Y0-440 Exam with 100% Guarantee

QUESTION 1

Scenario: A Citrix Architect is asked by management at the Workslab organization to review their existing configuration and make the necessary upgrades. The architect recommends small changes to the preexisting NetScaler configuration. Currently, the NetScaler MPX devices are configured in a high availability pair, and the outbound traffic is load-balanced between two Internet service providers 9ISPs). However, the failover is NOT happening correctly.

The following requirements were discussed during the design requirements phase:

1.

The return traffic for a specific flow should be routed through the same path while using Link Load Balancing.

2.

The link should fail over if the ISP router is up and intermediary devices to an ISP router are down.

3.

Traffic going through one ISP router should fail over to the secondary ISP, and the traffic should NOT flow through both routers simultaneously.

What should the architect configure with Link Load balancing (LLB) to meet this requirement?

A. Net Profile

B. Mac-based forwarding option enabled.

C. Resilient deployment mode

D. Backup route

Correct Answer: D

QUESTION 2

Scenario: A Citrix Architect has set up NetScaler MPX devices in high availability mode with version

12.0.53.13 nc. These are placed behind a Cisco ASA 5505 Firewall. The Cisco ASA Firewall is configured to block traffic using access control lists. The network address translation (NAT) is also performed on the firewall.

The following requirements were captured by the architect during the discussion held as part of the NetScaler security implementation project with the customer\\'s security team:

The NetScaler MPX device:

1.

should monitor the rate of traffic either on a specific virtual entity or on the device. It should be able to mitigate the attacks from a hostile client sending a flood of requests. The NetScaler device should be able to stop the HTTP, TCP, and DNS based requests.

2.

needs to protect backend servers from overloading.

3.

needs to queue all the incoming requests on the virtual server level instead of the service level.

4.

should provide protection against well-known Windows exploits, virus-infected personal computers, centrally managed automated botnets, compromised webservers, known spammers/hackers, and phishing proxies.

5.

should provide flexibility to enforce the decided level of security check inspections for the requests originating from a specific geolocation database.

6.

should block the traffic based on a pre-determined header length, URL length, and cookie length. The device should ensure that characters such as a single straight quote ("); backslash (\); and semicolon (;) are either blocked, transformed, or dropped while being sent to the backend server.

Which security feature should the architect configure to meet these requirements?

A. Global Server Load balancing with Dynamic RTT

B. Global Server Load Balancing with DNS views

C. Geolocation-based blocking using Application Firewall

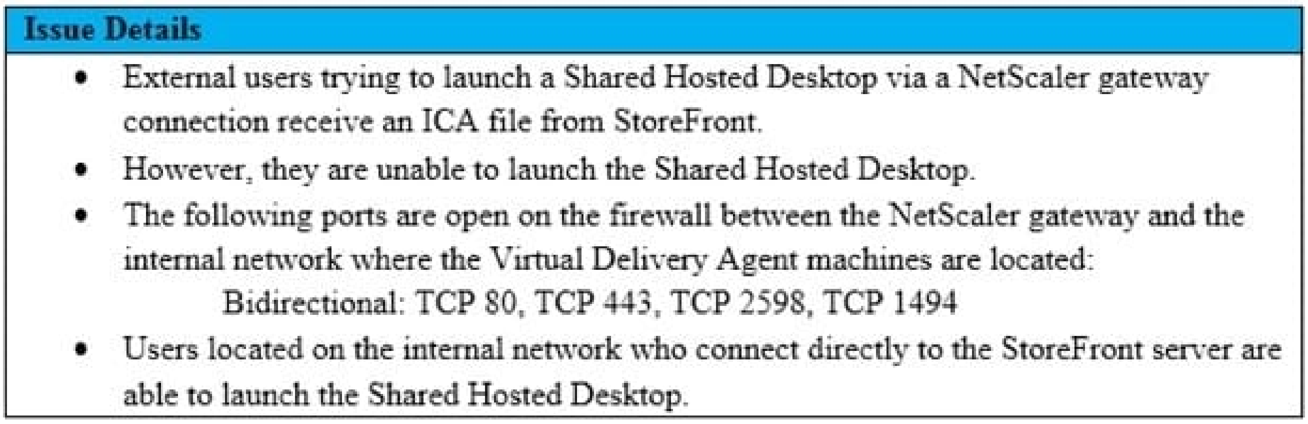
D. geolocation-based blocking using Responder policies

Correct Answer: A

QUESTION 3

Scenario: A Citrix Architect needs to assess a NetScaler Gateway deployment that was recently completed by a customer and is currently in pre-production testing. The NetScaler Gateway needs to use ICA proxy to provide access to a XenApp and XenDesktop environment. During the assessment, the customer informs the architect that users are NOT able to launch published resources using the Gateway virtual server.

Click the Exhibit button to view the troubleshooting details collected by the customer.



Issue Details

- External users trying to launch a Shared Hosted Desktop via a NetScaler gateway connection receive an ICA file from StoreFront.
- However, they are unable to launch the Shared Hosted Desktop.
- The following ports are open on the firewall between the NetScaler gateway and the internal network where the Virtual Delivery Agent machines are located:

  Bidirectional: TCP 80, TCP 443, TCP 2598, TCP 1494
- Users located on the internal network who connect directly to the StoreFront server are able to launch the Shared Hosted Desktop.

What is the cause of this issue?

A. The required ports have NOT been opened on the firewall between the NetScaler gateway and the Virtual Delivery Agent (VDA) machines.

B. The StoreFront URL configured in the NetScaler gateway session profile is incorrect.

C. The Citrix License Server is NOT reachable.

D. The Secure Ticket Authority (STA) servers are load balanced on the NetScaler.

Correct Answer: D

QUESTION 4

For which three reasons should a Citrix Architect perform a capabilities assessment when designing and deploying a new NetScaler in an existing environment? (Choose three.)

A. Understand the skill set of the company.

B. Assess and identify potential risks for the design and build phase.

C. Establish and prioritize the key drivers behind a project.

D. Determine operating systems and application usage.

E. Identify other planned projects and initiatives that must be integrated with the design and build phase.

Correct Answer: BDE

QUESTION 5

Scenario: A Citrix Architect needs to deploy SAML integration between NetScaler (Identity Provider) and ShareFile (Service Provider). The design requirements for SAML setup are as follows:

1.

NetScaler must be deployed as the Identity Provider (IDP).

2.

ShareFile server must be deployed as the SAML Service Provider (SP).

3.

The users in domain workspacelab.com must be able to perform Single Sign-on to ShareFile after authenticating at the NetScaler.

4.

The User ID must be UserPrincipalName.

5.

The User ID and Password must be evaluated by NetScaler against the Active Directory servers SFOADS-001 and SFO-ADS-002.

6.

After successful authentication, NetScaler creates a SAML Assertion and passes it back to ShareFile.

7.

Single Sign-on must be performed.

8.

SHA 1 algorithm must be utilized.

The verification environment details are as follows:

1.

Domain Name: workspacelab.com

2.

NetScaler AAA virtual server URL https://auth.workspacelab.com

3.

ShareFile URL https://sharefile.workspacelab.com

Which SAML IDP action will meet the design requirements?

A. add authentication samlIdPProfile SAMI-IDP -samlSPCertName Cert_1 -samlIdPCertName Cert_2 assertionConsimerServiceURL “https://auth.workspacelab.com/samlIssueName auth.workspacelab.com -signatureAlg RSA-SHA256-digestMethod SHA256-encryptAssertion ON serviceProviderUD sharefile.workspacelad.com

B. add authentication samlIdPProfile SAMI-IDP -samlSPCertName Cert_1 -samlIdPCertName Cert_2 assertionConsimerServiceURL https://sharefile.workspacelab.com/saml/acs” -samlIssuerName sharefile.workspacelab.com -signatureAlg RSA-SHA256 -digestMethod SHA256 -serviceProviderID sharefile.workspacelab.com

C. add authentication samlIdPProfile SAMI-IDP -samlSPCertName Cert_1 -samlIdPCertName Cert_2 assertionConsimerServiceURL https://sharefile.workspacelab.com/saml/acs” -samlIssuerName auth.workspacelab.com

-signatureAlg RSA-SHA1-digestMethod SHA1 -encryptAssertion ON serviceProviderID sharefile.workspacelab.com

D. add authentication samlIdPProfile SAMI-IDP -samISPCertName Cert_1 -samlIdPCertName Cert_2 assertionConsimerServiceURL https://sharefile.workspacelab.com/saml/acs" -samlIssuerName sharefile.workspacelab.com -signatureAlg RSA-SHA1 -digestMethod SHA1 -encryptAssertion ON serviceProviderID sharefile.workspacelab.com

Correct Answer: C