



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.passapply.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 needs to configure a full VPN session profile to meet the following requirements:

1.
Users should be able to send the traffic only for the allowed networks through the VPN tunnel.
2.
Only the DNS requests ending with the configured DNS suffix workspacelab.com must be sent to NetScaler Gateway.
3.
If the DNS query does NOT contain a domain name, then DNS requests must be sent to NetScaler gateway.

Which settings will meet these requirements?

- A. Split Tunnel to OFF, Split DNS Both
- B. Split Tunnel to ON, Split DNS Local
- C. Split Tunnel to OFF, Split DNS Remote
- D. Split Tunnel to ON, Split DNS Remote

Correct Answer: B

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 web servers, 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

A Citrix Architect needs to configure advanced features of NetScaler by using StyleBooks as a resource in the Heat service.

What is the correct sequence of tasks to be completed for configuring NetScaler using the Heat stack?

- A. 1. Install NetScaler Bundle for OpenStack

2.

Deploy the Heat stack

3.

Register OpenStack with NMAP

4.

Add NetScaler instances (Optional)

5.

Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource

6.



Create service packages (Add OpenStack tenants)

B. 1. Install NetScaler Bundle for OpenStack

2.

Register OpenStack with NMAS

3.

Add NetScaler instances (Optional)

4.

Create service packages (Add OpenStack tenants)

5.

Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource

6.

Deploy the Heat stack

C. 1. Install NetScaler Bundle for OpenStack

2.

Add NetScaler instances (Optional)

3.

Create service packages (Add OpenStack tenants)

4.

Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource

5.

Register OpenStack with NMAS

6.

Deploy the Heat stack

D. 1. Install NetScaler Bundle for OpenStack

2.

Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource

3.

Register OpenStack with NMAS

4.



Deploy the Heat stack

5.

Add NetScaler instances (Optional)

6.

Create service packages (Add OpenStack tenants)

Correct Answer: D

Reference: https://docs.citrix.com/en-us/netscaler-mas/12/integrating-netscaler-mas-with-openstackplatform/integrating_netscaler_mas_with_openstack_heat_services.html

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 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

[Latest 1Y0-440 Dumps](#)

[1Y0-440 VCE Dumps](#)

[1Y0-440 Study Guide](#)