



**Exam Code:** 1Y0-700

**Exam Name:** Citrix Application Firewall 8.0: Administration  
Exam

**Vendor:** Citrix

**Version:** DEMO

## Part: A

1: An administrator is considering adding an Application Firewall deployment to an environment that contains two network firewalls, a public network and a private network. Where should the administrator place the Application Firewall?

- A. In the DMZ
- B. Behind the private network
- C. In front of the public network
- D. In front of the two network firewalls

**Correct Answers: A**

2: The positive security model as applied in the Application Firewall can protect against \_\_\_\_\_ and \_\_\_\_\_ attacks. (Choose the two options that best complete the sentence.)

- A. worms
- B. viruses
- C. zero day
- D. layer 3 network
- E. application layer

**Correct Answers: C E**

3: Scenario: A banking company has decided to deploy an Application Firewall in their network environment, which already has two third-party load balancers. The Application Firewall deployment will be used to inspect approximately 400 Mb/sec of traffic. How should an administrator deploy the system in this environment?

- A. As a module on a NetScaler appliance
- B. As a standalone Application Firewall appliance
- C. As a module on a NetScaler High Availability pair
- D. As a cluster of standalone Application Firewall appliances

**Correct Answers: D**

4: Scenario: A busy web application (400 Mb/sec) for an ecommerce company includes pictures of items for sale that are displayed to shoppers with text descriptions, an input field to accept customer reviews, a shopping cart and an encrypted billing page for credit cards. Many more customers browse than buy. An administrator needs to create profiles for this web application on the Application Firewall. How many profiles should an administrator configure for this web application for security with maximum performance?

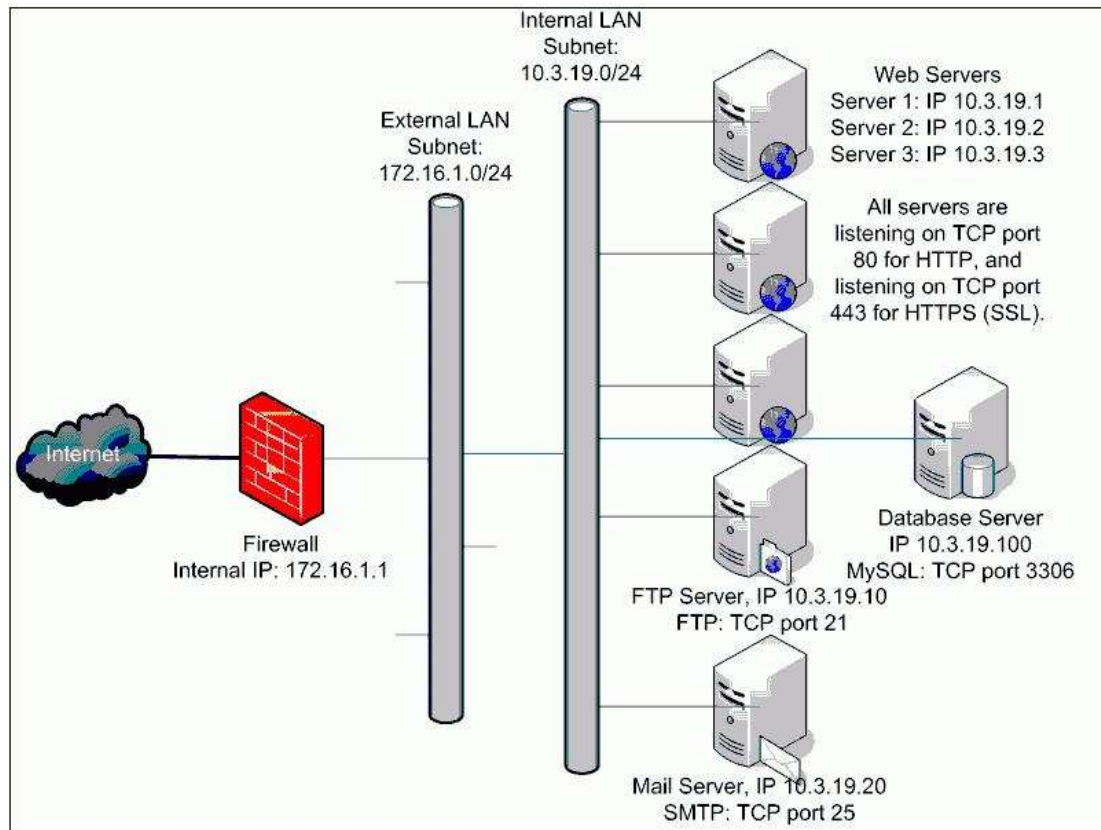
- A. One, an advanced profile for the reviews and billing pages
- B. Two, a basic profile for the reviews page and an advanced profile for the billing page
- C. Three, a basic profile for browsing and separate advanced profiles for the reviews and the billing pages
- D. Four, separate basic profiles for the images and text, and separate advanced profiles for the reviews and the billing pages

**Correct Answers: B**

5: An administrator is deploying a standalone Application Firewall in the network environment depicted in the exhibit.

Click the Exhibit button to view the network diagram.

What should the VIP address range be for the Application Firewall in this environment?



- A.1.1.100.0/24
- B.10.3.19.0/24
- C.172.16.1.0/24
- D.10.3.19.100/124

**Correct Answers: C**

6: Scenario: The manufacturing department of a global biomedical company uses a web application to access manufacturing ratios and QA testing results from external plants that manufacture the biomedical devices. All the information for all the plants is stored in a data warehouse based on a Microsoft SQL server and accessed from the web application by running reports. Users receive instructions through a popup and then select the specific data for a report through a series of dynamically-generated drop-down menus populated from the Microsoft SQL database. Because the company is global, the web application also has language options that the user can select for the report to be delivered in.

Which part of the application can access sensitive data in this scenario?

- A.The popup
- B.The language options
- C.The resultant URL for a report

D.The drop-down menus for the report details

**Correct Answers: D**

7: Scenario: A media corporation has a website where viewers can read articles on current topics and stream videos of daily newscasts. The streaming videos are provided by IPTV, a streaming media application utilizing UDP. The company decides to add an Application Firewall to their network deployment to protect their site from hackers. To determine how many devices are necessary, the administrator must determine which traffic requires protection.

Which content data type(s) does the Application Firewall need to inspect in this environment?

A.Text/html

B.Images and text/html

C.UDP packets and text

D.Text/html, UDP packets and images

**Correct Answers: A**

8: The positive security model works with Application Firewall by \_\_\_\_\_. (Choose a phrase to complete this statement correctly.)

A.protecting web servers based on learning

B.protecting web servers based on signatures

C.only allowing traffic that matches approved patterns

D.allowing traffic that does not match blocked patterns

**Correct Answers: C**

9: Scenario: A banking company is planning on deploying an Application Firewall in their network environment. The company will need to use SSL, plans on using Advanced profiles, and requires redundancy in their network. The web servers never serve more than 300 Mb/sec of traffic. How should an administrator deploy the Application Firewall in this environment?

A.As a standalone appliance

B.As a module on a NetScaler

C.As a cluster of standalone appliances

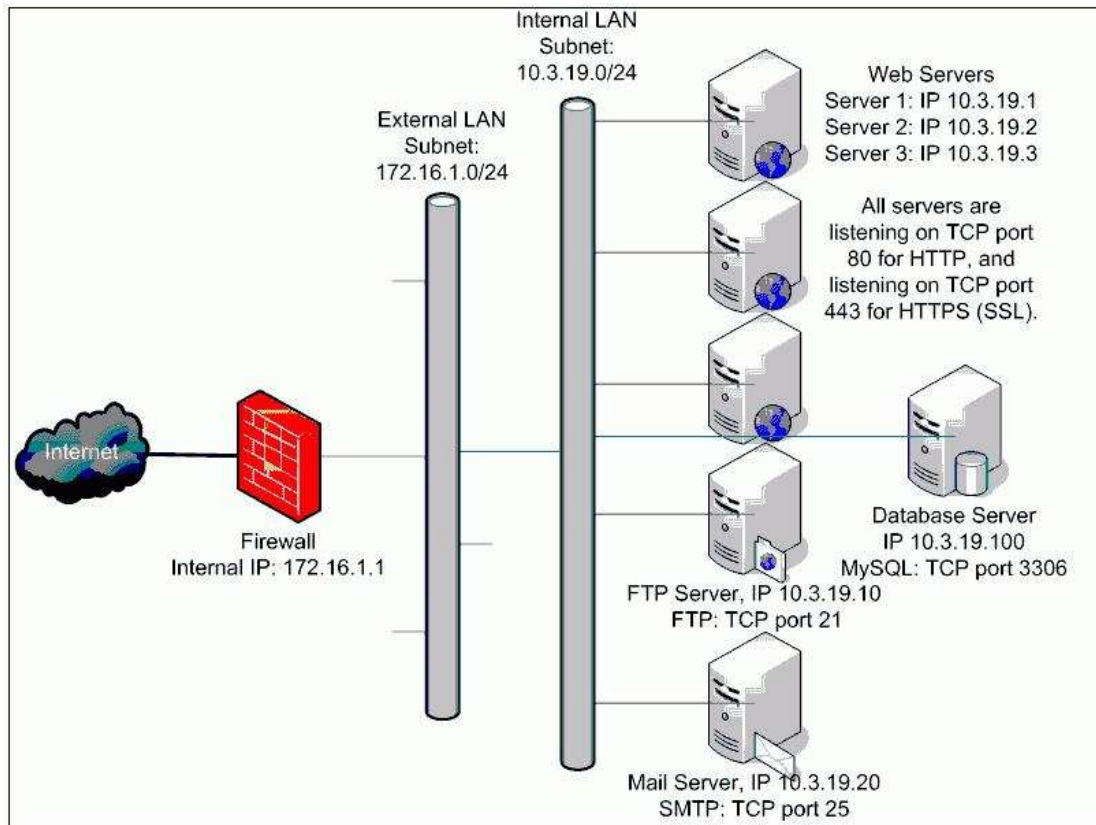
D.As a module on a NetScaler High Availability pair

**Correct Answers: D**

10: An administrator is deploying a standalone Application Firewall in the network environment depicted in the exhibit.

Click the Exhibit button to view the network diagram.

What should the NSIP address of the Application Firewall be in this environment?



- A.10.3.19.0
- B.172.16.1.1
- C.172.16.1.2
- D.10.3.19.254

**Correct Answers: C**

11: Scenario: The IT Manager of a popular social networking website has decided to deploy at least one Application Firewall to protect the millions of users that regularly log on to the website. The social networking site allows members to post group messages, email personal messages and blogs as well as maintain a personal page with pictures, messages and backgrounds created with HTML code. An administrator is tasked with determining the content type of the data that will be passing through the Application Firewall to determine how many devices are necessary. Which web application traffic and content data type(s) need to be inspected by the Application Firewall in this environment?

- A.HTTP traffic with GIF content data types
- B.HTTP traffic with text/html and text/javascript content data types
- C.All TCP and UDP traffic with text/html and GIF content data types
- D.All TCP traffic with text/html, POP3 and NNTP content data types

**Correct Answers: B**

12: Scenario: An online auctioning site has a web application that allows users to post their own items, including images and text. Users are permitted to animate their sites with Javascript. Auctioneers and shoppers must create an account and log in to be able to view any items. The web application creates session IDs at each login to keep track of shoppers and their carts and to

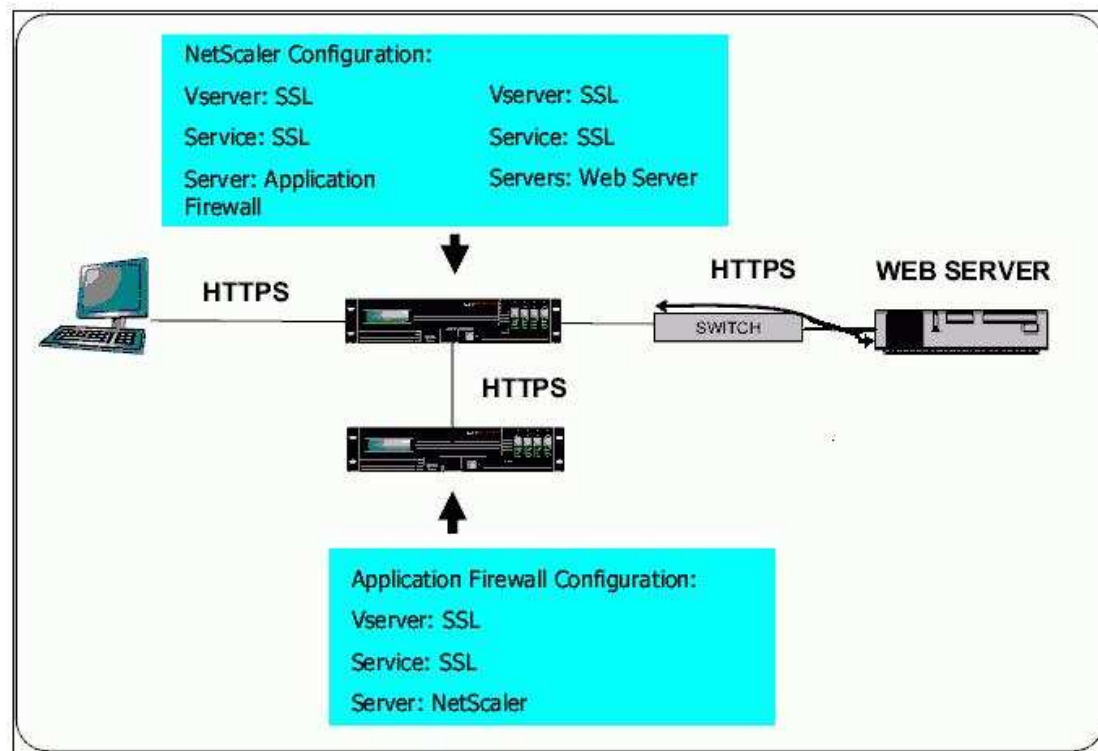
generate suggestions for similar purchases.

Which three parts of the application can be exploited to access sensitive data? (Choose three.)

- A.The text
- B.The login
- C.The images
- D.The Javascript
- E.The session IDs

**Correct Answers: B D E**

13: How many SSL termination points exist in the attached exhibit?



- A.1
- B.2
- C.3
- D.4

**Correct Answers: D**

14: Scenario: A company's corporate security policy requires that web servers be protected with end-to-end SSL encryption. An administrator is configuring SSL in an environment with a load balancer and a standalone Application Firewall deployment to meet the corporate security policy. At a minimum, which two SSL termination points are necessary for this environment? (Choose two.)

- A.at the web server
- B.on the load balancer
- C.on the network firewall
- D.at the Application Firewall

**Correct Answers: A D**

15: An administrator is creating and uploading an SSL certificate for a production environment. For added security, the administrator plans on encrypting the SSL key generated using the DES algorithm. What should the administrator generate to accomplish this?

- A.A self-signed certificate with DER as the keyform
- B.A self-signed certificate with PEM as the keyform
- C.A certificate signing request with DER as the keyform
- D.A certificate signing request with PEM as the keyform

**Correct Answers: D**

16: Scenario: An administrator is configuring an Application Firewall to protect a critical company web application and will be using many of the protections including Cookie Consistency. The company security policy requires that no information about which servers, services or firewalls being used is available through web traffic. The administrator needs to modify the Application Firewall default cookie so that it does not have "citrix" in it. How can the administrator change the name of the Application Firewall session cookie?

- A.Through Engine Settings
- B.In the settings tab of the basic profile
- C.In the settings tab of the advanced profile
- D.By modifying the policy bound to the web application's profile

**Correct Answers: A**

17: Scenario: An administrator is configuring the initial settings for a standalone Application Firewall in an environment with web servers that receive encrypted and non-encrypted traffic. Server1 with IP address 10.10.10.1 and Server2 with IP address 10.10.10.2 receive the non-encrypted traffic, and Server3 with IP address 10.10.10.3 receives the encrypted traffic. The administrator has already configured the servers.

Which two sets of steps should the administrator take to configure virtual servers (vservers) and services through the name-based approach to meet the deployment needs of this environment? (Choose two.)

- A.Add a vserver labeled vs1 of type HTTP and bind it to services sv1 and sv2, and a vserver labeled vs2 of type SSL and bind it to service sv3.
- B.Add a service labeled sv1 and bind it to Server1, a service labeled sv2 and bind it to Server2, and a service labeled sv3 and bind it to Server3.
- C.Add a service labeled sv1 and bind it to 10.10.10.1, a service labeled sv2 and bind it to 10.10.10.2, and a service labeled sv3 and bind it to 10.10.10.3.
- D.Add a vserver labeled vs1 of type HTTP and bind it to service sv1, a vserver labeled vs2 of type HTTP and bind it to service sv2, and a vserver labeled vs3 of type SSL and bind it to service sv3.

**Correct Answers: B D**

18: An administrator needs to configure a standalone Application Firewall to receive encrypted traffic and verify that the back-end servers receive clear text traffic. Which type of virtual server deployment should the administrator deploy for this environment?

- A.SSL
- B.TCP
- C.HTTP
- D.SSL and SSL\_TCP
- E.SSL, SSL\_TCP, and HTTP

**Correct Answers: A**

19: Scenario: An Internet-based company running an online blogging site is preparing to open a new section of the site for auctioning items and for adding encryption to the entire site. The company just purchased a standalone Application Firewall and plans to use the system to avoid increasing the CPU utilization due to SSL encryption and decryption that the web servers would otherwise incur. An administrator has already created the necessary certificate and key pairs. Which three entities should an administrator create for this scenario? (Choose three.)

- A.A virtual server of type SSL for the web servers
- B.A virtual server of type HTTP for the web servers
- C.Server objects that point to the back-end web servers
- D.Services of type SSL associated with the web servers
- E.Services of type HTTP associated with the web servers

**Correct Answers: A C E**

20: Which step must an administrator take when a server certificate is signed by an intermediate certificate authority?

- A.Copy the intermediate certificate into the same file as the server certificate, placing it in the file after the server certificate.
- B.Copy the intermediate certificate into the same file as the server certificate, placing it in the file before the server certificate.
- C.Copy the intermediate certificate into the same file as the root certificate, placing it in the file after the private key of the server.
- D.Copy the intermediate certificate into the same file as the root certificate, placing it in the file before the private key of the server.

**Correct Answers: A**