KillTest

質量更高　服務更好



練習題

https://www.killtest.net

一年免費更新服務

Exam : **1Y0-253**

Title : Implementing Citrix NetScaler 10.5 for App and Desktop Solutions

Version : DEMO

1.A Citrix Administrator needs to configure a single virtual server to accept TCP traffic on ports 80, 443 and ports between 10000 and 19999.
Which protocol type should the administrator use to accomplish this task?
A. ANY
B. UDP
C. SSL_TCP
D. SSL_PUSH
Answer: A

2.Which two pieces of information are required to create a virtual server? (Choose two.)
A. Port
B. Protocol
C. Subnet Mask
D. Gateway Address
Answer: A,B

3.Which two items are needed to import an SSL certificate? (Choose two.)
A. A public key
B. A private key
C. A root certificate
D. A server certificate
E. An intermediate certificate
Answer: B,D

4.Scenario: A company requires two-factor authentication using RSA tokens and Active Directory. The Citrix Administrator configured the following two authentication policies with these parameters:
-The policy named RSA_policy is used for RSA token authentication
-The policy named AD_policy is used for Active Directory authentication
What should the administrator do to protect the NetScaler Gateway virtual server from an attack against Active Directory?
A. Bind the RSA_policy in Primary Authentication Policies and bind the AD_policy in Secondary Authentication Policies.
B. Bind the AD_policy in Primary Authentication Policies and bind the RSA_policy in Secondary Authentication Policies.
C. Bind the AD_policy and the RSA_policy in Primary Authentication Policies and set the RSA_policy priority higher than the AD_policy.
D. Bind the AD_policy and the RSA_policy in Primary Authentication Policies and set the AD_policy priority higher than the RSA_policy.
Answer: A

5.Various users report that while accessing the Citrix NetScaler Gateway virtual server they get an error message that the public SSL certificate is NOT trusted.
Which three steps should a Citrix Administrator take on the NetScaler to resolve this issue? (Choose three.)

A. Import the root certificate.
B. Import the intermediate certificate.
C. Download the root certificate from the vendor.
D. Link the root certificate to the intermediate certificate.
E. Download the intermediate certificate from the vendor.
F. Link the intermediate certificate to the existing server certificate.
Answer: B,E,F