[Feb 10, 2024 Lesson Brilliant PDF for the 300-730 Tests Free Updated Today [Q45-Q65

[Feb 10, 2024] Lesson Brilliant PDF for the 300-730 Tests Free Updated Today
Get New 2024 Valid Practice CCNP Security 300-730 Q&A - Testing Engine

Career Bonuses

After taking the Cisco 300-730 test along with the core exam, the candidates can earn the CCNP Security certification. The specialists with this certificate have a wide range of career opportunities to explore. Various organizations are looking to hire the reliable security professionals to protect their enterprises from cyber threats. Some of the positions that the individuals with this certification can take up include an IT Network Specialist, an IT Security Consultant, a Cybersecurity Specialist, a Network Security Specialist, an Infrastructure Engineer, a Network Engineer, a Network Administrator, and a Network Engineer, among others. The average remuneration outlook for the certificate holders is $100,000 per annum.

QUESTION 45

What are two purposes of the key server in Cisco IOS GETVPN? (Choose two.)
* to download encryption keys
* to maintain encryption policies

* to distribute routing information
* to encrypt data traffic
* to authenticate group members

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-GETVPNDesignGuide-AUG14.pdf

QUESTION 46

A network engineer has set up a FlexVPN server to terminate multiple FlexVPN clients. The VPN tunnels are established without issue. However, when a Change of Authorization is issued by the RADIUS server, the FlexVPN server does not update the authorization of connected FlexVPN clients. Which action resolves this issue?

* Add the aaa server radius dynamic-author command on the FlexVPN clients.
* Fix the RADIUS key mismatch between the RADIUS server and FlexVPN server.
* Add the aaa server radius dynamic-author command on the FlexVPN server.
* Fix the RADIUS key mismatch between the RADIUS server and FlexVPN clients.

QUESTION 47

Which configuration construct must be used in a FlexVPN tunnel?

* EAP configuration
* multipoint GRE tunnel interface
* IKEv1 policy
* IKEv2 profile

The correct answer is D.

IKEv2 profile. A FlexVPN tunnel requires an IKEv2 profile to define the parameters for the IKEv2 negotiation and the IPsec security association. The IKEv2 profile references the IKEv2 keyring, the authentication method, the identity of the peers, and other options. The IKEv2 profile is then applied to a virtual tunnel interface (VTI) or a dynamic virtual tunnel interface (DVTI) to protect the tunnel with IPsec12. An EAP configuration is used for authentication with Extensible Authentication Protocol (EAP), which is optional for FlexVPN3. A multipoint GRE tunnel interface is used for DMVPN, not FlexVPN. An IKEv1 policy is used for IKEv1, not IKEv2, which is the protocol for FlexVPN.

QUESTION 48

Which IKE identity does an IOS/IOS-XE headend expect to receive if an IPsec Cisco AnyConnect client uses default settings?

* *$SecureMobilityClient$*
* *$AnyConnectClient$*
* *$RemoteAccessVpnClient$*
* *$DfltlkeldentityS*

QUESTION 49

What are two advantages of using GETVPN to traverse over the network between corporate offices? (Choose two.)

* It has unique session keys for improved security.
* It supports multicast.
* It has QoS support.
* It is a highly scalable any to any mesh topology.
* It supports a hub-and-spoke topology.

QUESTION 50

Which command identifies a Cisco AnyConnect profile that was uploaded to the flash of an IOS router?
* svc import profile SSL_profile flash:simos-profile.xml
* anyconnect profile SSL_profile flash:simos-profile.xml
* crypto vpn anyconnect profile SSL_profile flash:simos-profile.xml
* webvpn import profile SSL_profile flash:simos-profile.xml

QUESTION 51

Which method dynamically installs the network routes for remote tunnel endpoints?
* policy-based routing
* CEF
* reverse route injection
* route filtering

Reference:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/12-4t/sec-vpn-availability-12-4t-book/sec-rev-rte-inject.html>

QUESTION 52

Refer to the exhibit.

```
tunnel-group client general-attributes
address-pool MYPOOL
authentication-server-group RADIUS
tunnel-group client ipsec-attributes
pre-shared-key test123
```


Which type of VPN is used?
* GETVPN
* clientless SSL VPN
* Cisco Easy VPN
* Cisco AnyConnect SSL VPN

https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn-config/vpn-easyvpn.html

QUESTION 53

Refer to the exhibit.

XML profile


```
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
```

The customer must launch Cisco AnyConnect in the RDP machine. Which IOS configuration accomplishes this task?

A.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
  svc platform win seq 1
  policy group PolicyGroup1
   functions svc-enabled
```

B.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
browser-attribute import flash:RDP.xml
```

C.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc profile Profile1
```

D.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc module RDP
```


* Option A
* Option B
* Option C
* Option D

QUESTION 54

A network engineer is implementing a FlexVPN tunnel between two Cisco IOS routers. The FlexVPN tunnels will terminate on encrypted traffic on an interface configured with an IP MTU of 1500, and the company has a security policy to drop fragmented traffic coming into or leaving the network. The tunnel will be used to transfer TFTP data between users and internal servers. When the TFTP traffic is not traversing a VPN, it can have a maximum IP packet size of 1500. Assuming the encrypted payload will add 90 bytes, which configuration allows TFTP traffic to traverse the FlexVPN tunnel without being dropped?

* Set the tunnel IP MTU to 1500.
* Set the tunnel tcp adjust-mss to 1460.
* Set the tunnel IP MTU to 1400.
* Set the tunnel tcp adjust-mss to 1360.

QUESTION 55

```
HUB configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 1 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 2 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local pre-shared-key flexvpn
 authentication remote rsa-sig
 pki trustpoint CA
aaa authorization group cert list default default
virtual-template 1
```


Refer to the exhibit. What is a result of this configuration?

* Spoke 1 fails the authentication because the authentication methods are incorrect.
* Spoke 2 passes the authentication to the hub and successfully proceeds to phase 2.
* Spoke 2 fails the authentication because the remote authentication method is incorrect.
* Spoke 1 passes the authentication to the hub and successfully proceeds to phase 2.

Section: Troubleshooting using ASDM and CLI

QUESTION 56

An engineer must investigate a connectivity issue and decides to use the packet capture feature on Cisco FTD. The goal is to see the real packet going through the Cisco FTD device and see Snort detection actions as a part of the output. After the capture-traffic command is issued, only the packets are displayed. Which action resolves this issue?

* Specify the trace using the -T option after the capture-traffic command
* Perform the trace within the Cisco FMC GUI instead of the Cisco FMC CLI
* Use the verbose option as a part of the capture-traffic command

* Use the capture command and specify the trace option to get the required information

B) Performing the trace within the Cisco FMC GUI instead of the Cisco FMC CLI is not a valid option, because the FMC GUI does not support packet capture or tracing on the FTD device. You can only use the FMC GUI to view and export captures that are taken on the FTD CLI1.

C) Using the verbose option as a part of the capture-traffic command is not a valid option, because there is no verbose option for this command. The verbose option is only available for the capture command, which is used to capture packets on the LINA engine domain of the FTD device1.

D) Using the capture command and specifying the trace option to get the required information is not a valid option, because the capture command does not have a trace option. The capture command allows you to capture packets on the LINA engine domain of the FTD device, but it does not show the Snort detection actions. The trace option is only available for the packet-tracer command, which is used to simulate a packet going through the FTD device and show its processing steps1.

Explanation:

The correct answer is A.

Specify the trace using the -T option after the capture-traffic command. According to the document Use Firepower Threat Defense Captures and Packet Tracer, the capture-traffic command allows you to capture packets on the Snort engine domain of the FTD device. However, by default, it only shows the packet headers and does not include the Snort detection actions. To see the Snort detection actions, you need to use the -T option, which enables tracing. For example:

capture-traffic -T

This will show the packet headers along with the Snort verdicts, such as allow, block, or replace. You can also use other options to filter or save the capture output1.

QUESTION 57

Which feature allows the ASA to handle nonstandard applications and web resources so that they display correctly over a clientless SSL VPN connection?

* single sign-on
* Smart Tunnel
* WebType ACL
* plug-ins

Reference:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ vpn_clientless_ssl.html#29951

QUESTION 58

Over the weekend, an administrator upgraded the Cisco ASA image on the firewalls and noticed that users cannot connect to the headquarters site using Cisco AnyConnect. What is the solution for this issue?

* Upgrade the Cisco AnyConnect client version to be compatible with the Cisco ASA software image.
* Upgrade the Cisco AnyConnect Network Access module to be compatible with the Cisco ASA software image.
* Upgrade the Cisco AnyConnect client driver to be compatible with the Cisco ASA software image.
* Upgrade the Cisco AnyConnect Start Before Logon module to be compatible with the Cisco ASA software image.

https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asa-vpn-compatibility.html#Cisco_Reference.dita_60cec583-01b8-4cb2-a6e3-2fe87a6b0f82

QUESTION 59

Cisco AnyConnect clients need to transfer large files over the VPN sessions. Which protocol provides the best throughput?
* SSL/TLS
* L2TP
* DTLS
* IPsec IKEv1
Section: Secure Communications Architectures

QUESTION 60

Which parameter is initially used to elect the primary key server from a group of key servers?
* code version
* highest IP address
* highest-priority value
* lowest IP address
Reference:

https://www.cisco.com/c/en/us/products/collateral/security/group-encrypted-transport-vpn/ deployment_guide_c07_554713.html

QUESTION 61

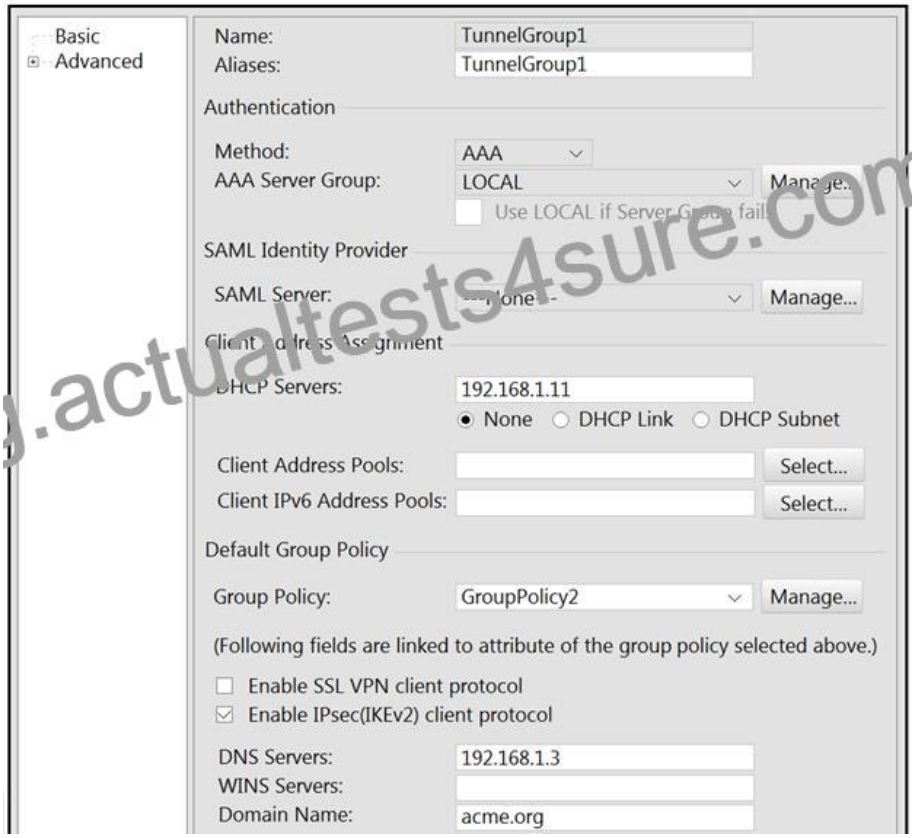
What is a requirement for smart tunnels to function properly?
* Java or ActiveX must be enabled on the client machine.
* Applications must be UDP.
* Stateful failover must not be configured.
* The user on the client machine must have admin access.

QUESTION 62

Which feature of GETVPN is a limitation of DMVPN and FlexVPN?
* sequence numbers that enable scalable replay checking
* enabled use of ESP or AH
* design for use over public or private WAN
* no requirement for an overlay routing protocol
one benefit of GET VPN is Simplified network design due to leveraging of native routing infrastructure (no overlay routing protocol needed) f mismatch is causing the problem with the IPsec VPN

QUESTION 63

Refer to the exhibit.



A network engineer is configuring a remote access SSLVPN and is unable to complete the connection using local credentials. What must be done to remediate this problem?

* Enable the client protocol in the Cisco AnyConnect profile.
* Configure a AAA server group to authenticate the client.
* Change the authentication method to local.
* Configure the group policy to force local authentication.

QUESTION 64

Which two types of web resources or protocols are enabled by default on the Cisco ASA Clientless SSL VPN portal? (Choose two.)

* HTTP
* ICA (Citrix)
* VNC
* RDP
* CIFS

HTTP (Hypertext Transfer Protocol) is used for transferring web resources, such as web pages and HTML documents, across the internet. CIFS (Common Internet File System) is used for sharing files and printers between computers on a network. ICA (Citrix), VNC (Virtual Network Computing), and RDP (Remote Desktop Protocol) are not enabled by default on the Cisco ASA Clientless SSL VPN portal.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/vpn/asa-94-vpn-config/webvpn-configure-gateway.html

QUESTION 65

Which VPN does VPN load balancing on the ASA support?

* VTI
* IPsec site-to-site tunnels
* L2TP over IPsec
* Cisco AnyConnect

To pass the Cisco 300-730 exam, candidates must have a thorough understanding of VPN technologies, protocols, and security policies. They must also have hands-on experience in implementing and maintaining VPN solutions using different technologies and deployment models. 300-730 exam format consists of multiple-choice questions, drag and drop, and simulation-based questions.

300-730 Dumps PDF - 100% Passing Guarantee: https://www.actualtests4sure.com/300-730-test-questions.html]