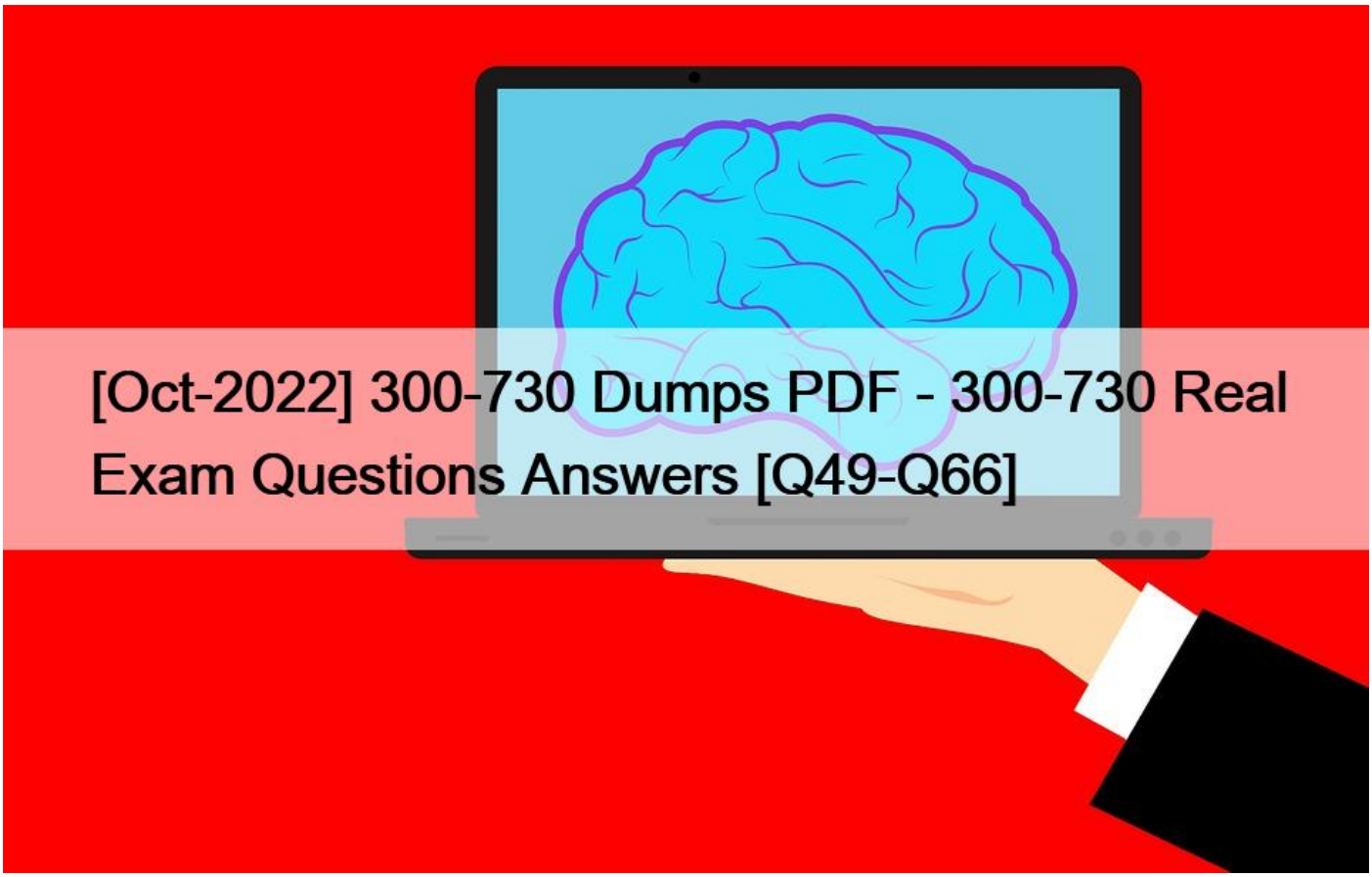
[Oct-2022 300-730 Dumps PDF - 300-730 Real Exam Questions Answers [Q49-Q66



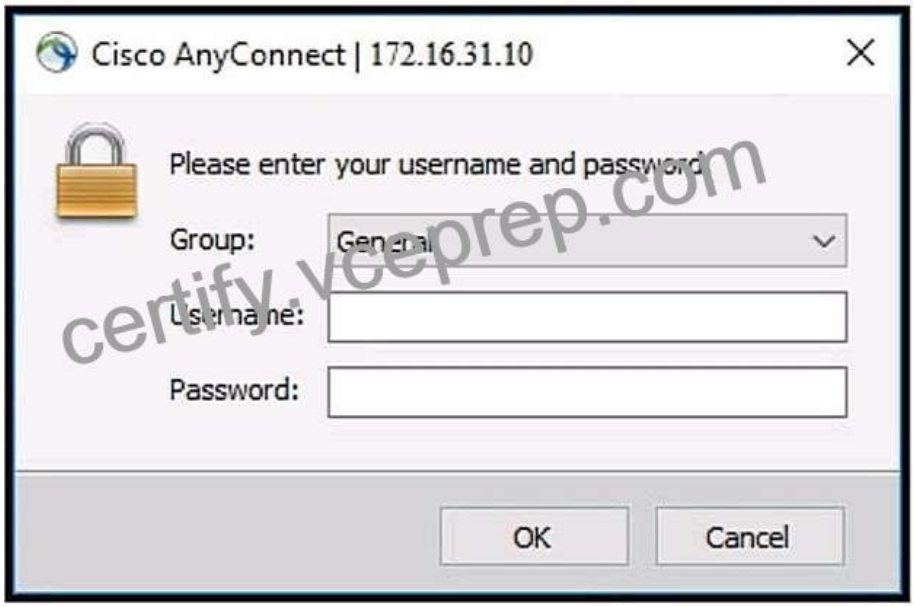
[Oct-2022] 300-730 Dumps PDF - 300-730 Real Exam Questions Answers
300-730 Dumps 100% Pass Guarantee With Latest Demo

Q49. Which command automatically initiates a smart tunnel when a user logs in to the WebVPN portal page?
* auto-upgrade
* auto-connect
* auto-start
* auto-run

Section: Remote access VPNs

Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/webvpn-configure-policy-group.html

Q50.



Refer to the exhibit. Which two commands under the tunnel-group webvpn-attributes result in a Cisco AnyConnect user receiving the AnyConnect prompt in the exhibit? (Choose two.)

* group-url https://172.16.31.10/General enable
* group-policy General internal
* authentication aaa
* authentication certificate
* group-alias General enable

Section: Remote access VPNs

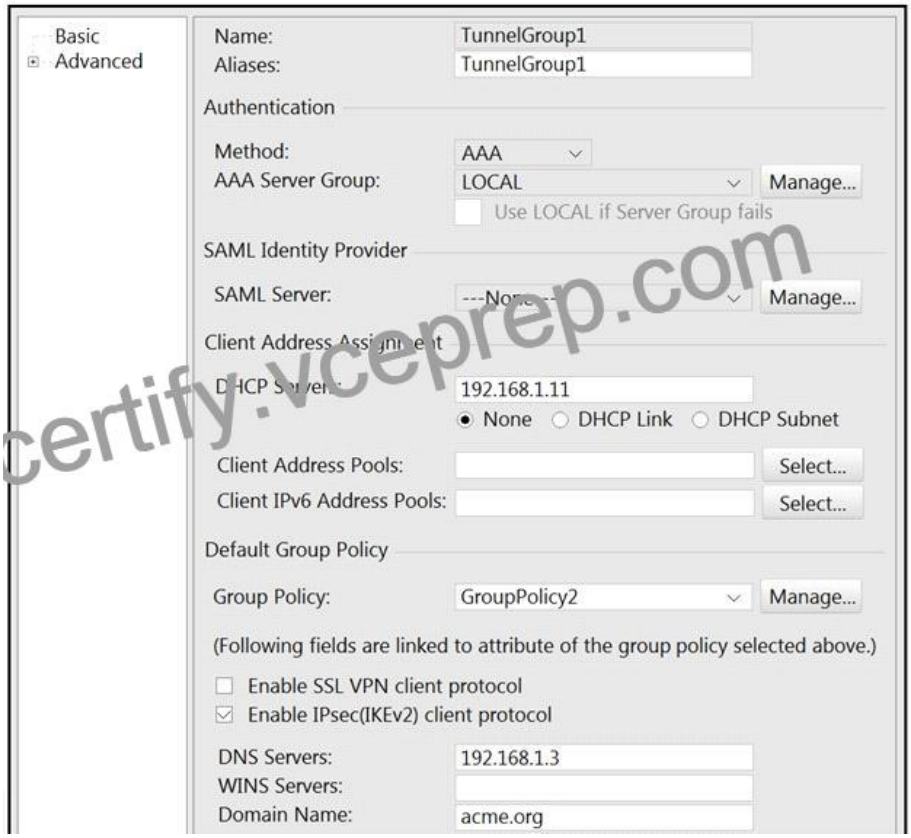
Q51. Refer to the exhibit.

```
webvpn
 port 9443
 enable outside
 dtls port 9443
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.5.03049-webdeploy-k9.pkg 3
 anyconnect profiles vpn_profile_1 disk0:/vpn_profile_1.xml
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
group-policy vpn_policy internal
group-policy vpn_policy attributes
 dns-server value 192.168.1.3
 vpn-tunnel-protocol ssl-client
 address-pools value vpn_pool
```

A network engineer is reconfiguring clientless SSLVPN during a maintenance window, and after testing the new configuration, is

unable to establish the connection. What must be done to remediate this problem?
* Enable client services on the outside interface.
* Enable clientless protocol under the group policy.
* Enable DTLS under the group policy.
* Enable auto sign-on for the user’s IP address.

Q52. 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.

Q53. 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

Q54.

```
ISAKMP: (0):beginning Main Mode exchange
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP: (0):Old State = IKE_I_MM1  New State = IKE_I_MM2
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (0):local preshared key found
ISAKMP: (0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: (0):       encryption AES-CBC
ISAKMP: (0):       keylength of 256
ISAKMP: (0):       hash SHA256
ISAKMP: (0):       default group 14
ISAKMP: (0):       auth pre-share
ISAKMP: (0):       life type in seconds
ISAKMP: (0):       life duration (basic) of 200
ISAKMP: (0):atts are acceptable. Next payload is 0
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM3  New State = IKE_I_MM4
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM4
ISAKMP: (1005):pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
ISAKMP: (1005):retransmitting phase 1 MM_KEY_EXCH...
ISAKMP: (1005):: incrementing error counter on sa, attempt 1 of 5: retransmit phase 1
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
```


Refer to the exhibit. A site-to-site tunnel between two sites is not coming up. Based on the debugs, what is the cause of this issue?

* An authentication failure occurs on the remote peer.
* A certificate fragmentation issue occurs between both sides.
* UDP 4500 traffic from the peer does not reach the router.
* An authentication failure occurs on the router.

Section: Troubleshooting using ASDM and CLI

Q55. 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

Q56. Refer to the exhibit.

```
ip access-list extended CCNP
 permit 192.168.0.10
 permit 192.168.0.11

webvpn gateway SSL_Gateway
 ip address 172.16.0.25 port 443
 ssl trustpoint AnyConnect_Cert
 inservice

webvpn context SSL_Context
 gateway SSL_Gateway

 ssl authenticate verify all
 inservice

 policy group SSL_Policy
   functions svc-enabled
   svc address-pool "ACPool" netmask 255.255.255.0
   svc dns-server primary 192.168.0.100
   svc default-domain cisco.com
 default-group-policy SSL_Policy
```

Cisco AnyConnect must be set up on a router to allow users to access internal servers 192.168.0.10 and 192.168.0.11. All other traffic should go out of the client’s local NIC. Which command accomplishes this configuration?

* svc split include 192.168.0.0 255.255.255.0
* svc split exclude 192.168.0.0 255.255.255.0
* svc split include acl CCNP
* svc split exclude acl CCNP

Q57. Which command automatically initiates a smart tunnel when a user logs in to the WebVPN portal page?
* auto-upgrade
* auto-connect
* auto-start
* auto-run

Q58. Which two features provide headend resiliency for Cisco AnyConnect clients? (Choose two.)
* AnyConnect Auto Reconnect
* AnyConnect Network Access Manager
* AnyConnect Backup Servers
* ASA failover
* AnyConnect Always On

Section: Remote access VPNs

Q59. 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

Q60. Refer to the exhibit.

```
Ciscoasa# sh cap o trace packet-number 4

737 packets captured

     4: 08:19:36.054181    10.99.117.195.56485 > 10.31.124.31.443: $ 3919220036:3919220036(0) win 64240 <mss 1260,nop,wscale 8,nop,nop,sackOK>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
NAT divert to egress interface inside
Untranslate 10.31.124.31/443 to 172.16.0.0/443

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group global_access_1 global
access-list global_access_1 extended permit ip any any
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
Static translate 10.99.117.195/56485 to 10.99.117.195/56485

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:

Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:

Phase: 10
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 123456, packet dispatched to next module

Phase: 13
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.0.0 using egress ifc inside

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow


1 packet shown
```


An SSL client is connecting to an ASA headend. The session fails with the message “Connection attempt has timed out. Please verify Internet connectivity.” Based on how the packet is processed, which phase is causing the failure?

* phase 9: rpf-check
* phase 5: NAT
* phase 4: ACCESS-LIST
* phase 3: UN-NAT

Q61. In order to enable FlexVPN to use a AAA attribute list, which two tasks must be performed? (Choose two.)

* Define the RADIUS server.
* Verify that clients are using the correct authorization policy.
* Define the AAA server.
* Assign the list to an authorization policy.
* Set the maximum segment size.

Q62. Which technology works with IPsec stateful failover?
* GLBR
* HSRP
* GRE
* VRRP

Section: Secure Communications Architectures

Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ ft_vpnha.html#wp1122512

Q63.

```
Spoke1#
     local ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
     remote ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
     #pkts encaps: 200, #pkts encrypt: 200
     #pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 192.168.1.1,
remote crypto endpt.: 192.168.2.1
     inbound esp sas:
     spi: 034B32CA36 (1261619766)
     outbound esp sas:
     spi:0xD601918E (1760427022)

Spoke2#
     local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
     remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
     #pkts encaps: 210, #pkts encrypt: 210,
     #pkts decaps: 200, #pkts decrypt: 200,
local crypto endpt.: 192.168.2.1,
remote crypto endpt.: 192.168.1.1
     inbound esp sas:
     spi: 03D601918E (1760427022)
     outbound esp sas:
     spi: 034BS2CA36 (1261619766)
```


Refer to the exhibit. An engineer is troubleshooting a new GRE over IPsec tunnel. The tunnel is established but the engineer cannot ping from spoke 1 to spoke 2. Which type of traffic is being blocked?
* ESP packets from spoke2 to spoke1
* ISAKMP packets from spoke2 to spoke1
* ESP packets from spoke1 to spoke2
* ISAKMP packets from spoke1 to spoke2

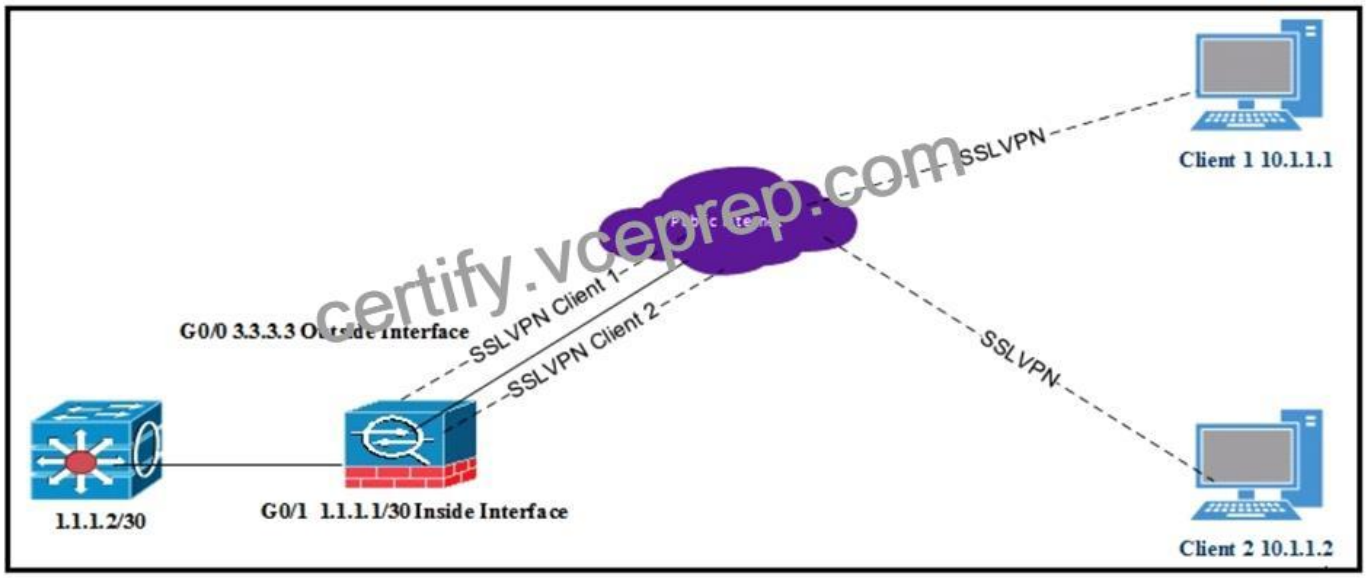
Section: Troubleshooting using ASDM and CLI

Q64. Which technology works with IPsec stateful failover?
* GLBR
* HSRP
* GRE
* VRRP

Q65. Which two features are valid backup options for an IOS FlexVPN client? (Choose two.)
* HSRP stateless failover
* DNS-based hub resolution
* reactivate primary peer

* tunnel pivot
* need distractor

Q66. Refer to the exhibit.



All internal clients behind the ASA are port address translated to the public outside interface that has an IP address of 3.3.3.3. Client 1 and client 2 have established successful SSL VPN connections to the ASA.

What must be implemented so that “3.3.3.3” is returned from a browser search on the IP address?
* Same-security-traffic permit inter-interface under Group Policy
* Exclude Network List Below under Group Policy
* Tunnel All Networks under Group Policy
* Tunnel Network List Below under Group Policy

Prerequisites

The intended audience for this exam is Channel Partners, Network Security Engineers, and CCNP Security Candidates, among others. The Cisco 300-730 test does not have any compulsory requirements. However, the applicants should have knowledge of different Cisco router and firewall command modes. Moreover, it is pretty important to possess expertise in managing Cisco routers and firewalls. In addition, the candidates have to be familiar with the advantages of site-to-site and Remote Access VPN options. They can get and master the necessary skills through completing such courses by Cisco as CCNA and SCOR.

Dumps Real Cisco 300-730 Exam Questions [Updated 2022: https://www.vceprep.com/300-730-latest-vce-prep.html]