

[New 300-209 Dumps Braindump2go 300-209 PDF Dumps and 300-209 Exam Questions 384Q Free Offered][349-359]

2018/September Braindump2go 300-209 Exam Dumps with PDF and VCE New Updated Today! Following are some new 300-209 Real Exam Questions:1. |2018 Latest 300-209 Exam Dumps (PDF & VCE) 384Q&As

Download: <https://www.braindump2go.com/300-209.html>2. |2018 Latest 300-209 Exam Questions & Answers

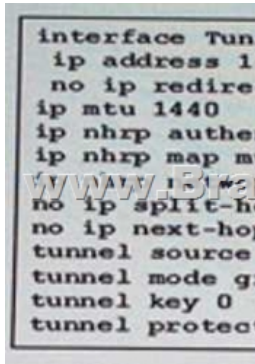
Download: <https://drive.google.com/drive/folders/0B75b5xYLjSSNRkY3M21SbTdTNDg?usp=sharing>
QUESTION 349A customer has two ASAs configured in high availability and is experiencing connection drops that require re-establishment each time failover occurs. Which type of failover has been implemented?
A. Stateless
B. routed
C. trans parent
D. stateful
Answer: D
QUESTION 350In a new DMVPN deployment, phase 1 completes successfully. However, phase 2 experiences issues. Which troubleshooting step is valid in this situation?
A. Temporarily remove encryption to check if the GRE tunnel is working.
B. Verify IP routing between the external IPs of the two peers is correct.
C. Remove NHRP configuration and reset the tunnels.
D. Ensure that the nodes use the same authentication method.
Answer: A
QUESTION 351An engineer is configuring clientless SSL VPN. The finance department has a database server that only they should access, but the sales department can currently access it. The finance and the sales departments are configured as separate group-policies. Which option must be added to the configuration to make sure the users in the sales department cannot access the finance department server?
A. Web type ACL
B. Port forwarding
C. Tunnel group lock
D. VPN filter ACL
Answer: C
QUESTION 352Refer to the Exhibit. All internal clients behind the ASA are port address translated to the public outside interface, which has an IP address of 3.3.3.3. Client 1 and Client 2 have established successful SSL VPN connections to the ASA. However, when either client performs a browser search on their IP address, it shows up as 3.3.3.3.



Why is this happening when both clients have a direct connection to the local internet service provider?
A. Same-security-traffic permit inter-interface has not been configured.
B. Tunnel All Networks is configured under Group Policy.
C. Exclude Network List Below is configured under Group Policy.
D. Tunnel Network List Below is configured under Group Policy.
Answer: B
QUESTION 353Refer to the Exhibit. Users at each end of this VPN tunnel cannot communicate with each other. Which cause of this behavior is true?



A. The Diffie-Hellman groups configured are different.
B. The pre shared key does not match.
C. Phase 1 is not completed and troubleshooting is required.
D. The issue occurs in phase 2 of the tunnel.
Answer: C
QUESTION 354An engineer is defining ECC variables and has set the input_mode set to B. Which statement is true?
A. DTMF voice is accepted.
B. Get Digits are written to the CEDC.
C. Mixed mode input is not accepted.
D. An ASR is not being used.
Answer: A
QUESTION 355Refer to the Exhibit. An engineer must implement DMVPN phase 2 and two conclusions can be made from the configuration? (Choose two.)



A. Spoke-to-spoke communication is allowed. B. Next-hop-self is required. C. EIGRP neighbor adjacency will fail. D. EIGRP route redistribution is not allowed. E. EIGRP used as the dynamic routing protocol. **Answer: A** QUESTION 356 An engineer wants to ensure that Diffie-Helman keys are re-generated upon a phase-2 rekey. What option can be configured to allow this? A. Aggressive mode B. Dead-peer detection C. Main mode D. Perfect-forward secrecy **Answer: D** QUESTION 357 Which two options are features of Cisco GET VPN? (Choose two.) A. Allows for optimal routing B. provides point to point IPsec SAC. Provides encryption for MPLS D. uses public Internet E. uses MORE **Answer: AC** QUESTION 358 Refer to the Exhibit. Which statement about this output is true?

```
Router#show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA

IPv6 Crypto IKEv2 SA

Tunnel-id  Ivrf/ivrf          Status
1          none/none                READY
Local 2001:DB8:123:2::2/500
Remote 2001:DB8:123:1::2/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: RSA,
Auth verify: RSA
Life/Active Time: 86400/17811 sec
Local spi: 60269648713C7FAB Remote spi: 282FE0B3B5C99A2B
Local id: 2001:DB8:123:2::2 Remote id: 2001:DB8:123:1::2
Local req msg id: 8 Remote req msg id: 8
Local next msg id: 8 Remote next msg id: 8
Local req queued: 8 Remote req queued: 8
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

A. Identity between endpoints is verified using a certificate authority. B. The tunnel is not functional because NAT-T is not configured. C. This router has sent the first packet to establish the Flex VPN tunnel. D. The remote device encrypts IKEv2 packets using key "282FE0B3B5C99A2B". **Answer: C** QUESTION 359 Refer to the Exhibit. A network security engineer is troubleshooting intermittent connectivity issues across a tunnel. Based on the output from the show crypto ipsec sa command, which cause is most likely?

```
Router#show crypto ipsec security-assoc lifetime
Security association lifetime: 4608000 kilobytes/3600 seconds

Router# show crypto ipsec sa
interface: Ethernet0/1
Crypto map tag: vpn, local addr. 10.10.250.250
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.10.250.250/255.255.255.255/47/0)
current peer: 10.10.250.250/500
PERMIT, flags={origin,is_acl}
#pkts encaps: 5961, #pkts encrypt: 5961, #pkts decrypt: 5961
#pkts decaps: 5961, #pkts decrypt: 5961, #pkts verify: 5961
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decomp. failed: 0
#send errors 1, #recv errors 0
local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.10.250.250
path mtu 1500, via mtu 1500
inbound esp sas:
spi: 0x4579534B(1165587771)
transform: esp-3des esp-md5-hmac ,
in use settings = (Tunnel, )
slot: 0, conn id: 2600, flow id: 1, crypto map: vpn
sa timing: remaining key lifetime (k/seq): (4506885/3581)
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x8E1CB88A(2384246650)
transform: esp-3des esp-md5-hmac ,
in use settings = (Tunnel, )
slot: 0, conn id: 2601, flow id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/seq): (4506885/3581)
IV size: 8 bytes
replay detection support: Y
```

A. ISAKMP and/or IP sec may be bouncing up and down. B. The security association lifetimes are set to default values. C. Return traffic is not coming back from the other end of the tunnel. D. Traffic may flow in only one direction across this tunnel. **Answer: B** !!!RECOMMEND!!! | 2018 Latest 300-209 Exam Dumps (PDF & VCE) 384Q&As
Download: <https://www.braindump2go.com/300-209.html> | 2018 Latest 300-209 Study Guide Video: YouTube Video: [YouTube.com/watch?v=IHRU47HQXac](https://www.youtube.com/watch?v=IHRU47HQXac)