

**Exam Code:** 920-232

**Exam Name:** nncss-contivity vpn switch release 5.0

**Vendor:** Nortel

**Version:** DEMO

## Part: A

1: A customer has a Contivity 5000 at a site with two Branch Office tunnel connections. The branch office tunnels use RIP for tunnel endpoint establishment. During setup of the Contivity 5000, the customer setup and enabled Contivity Interface Filters. Shortly afterwards they notice that the Branch Office tunnel has gone down. What is the possible cause of the problem?

- A.The interface filter is set to deny TCP.
- B.The interface filter is set to deny UDP.
- C.The interface filter is set to block the origin IP.
- D.An interface filter and a firewall is turned on at the same time.

**Correct Answers: B**

2: Click the Exhibit button. An administrator is logged into a local Contivity. The Contivity 5.0 event log shown in the exhibit displays the results of a branch office tunnel between a Contivity 5000 and a Contivity 1700. What can be said about the branch office tunnel? (Choose two.)

```
04/07/2003 13:34:18 0 Branch Office [01] IPSEC branch office connection initiated to rem[0.0.0.0-0.0.0.0]@[177.178.1.60] loc[0.0.0.0-0.0.0.0]
04/07/2003 13:34:18 0 Security [11] Session: IPSEC[177.178.1.60] attempting login
04/07/2003 13:34:18 0 Security [01] Session: IPSEC[177.178.1.60] has no active sessions
04/07/2003 13:34:18 0 Security [01] Session: IPSEC[177.178.1.60] Syd-Tok has no active accounts
04/07/2003 13:34:18 0 Security [01] Session: IPSEC[177.178.1.60]181 SHARED-SECRET authenticate attempt...
04/07/2003 13:34:18 0 Security [01] Session: IPSEC[177.178.1.60]181 attempting authentication using LOCAL
04/07/2003 13:34:18 0 Security [11] Session: IPSEC[177.178.1.60]181 authenticated using LOCAL
04/07/2003 13:34:18 0 Security [11] Session: IPSEC[177.178.1.60]181 bound to group /Base/Syd-Tok
04/07/2003 13:34:18 0 Security [01] Session: IPSEC[177.178.1.60]181 using group filter permit all
04/07/2003 13:34:18 0 Security [11] Session: IPSEC[177.178.1.60]181 authorized
04/07/2003 13:34:18 0 Security [11] Session: network IPSEC[0.0.0.0-0.0.0.0] attempting login
04/07/2003 13:34:18 0 ISAKMP [02] ISAKMP SA established with 177.178.1.60
04/07/2003 13:34:18 0 Outbound ESP from 177.178.1.50 to 177.178.1.60 SPI 0x0007512c [03] ESP encap session SPI 0x2c510700 bound to cpu 0
04/07/2003 13:34:18 0 Inbound ESP from 177.178.1.60 to 177.178.1.50 SPI 0x0019e24a [03] ESP decap session SPI 0x4ae21900 bound to cpu 0
04/07/2003 13:34:19 0 Security [01] Session: IPSEC[-]:182 Using gateway input filters 57830d8 46736a8 6e93a10
04/07/2003 13:34:19 0 Security [01] Session: IPSEC[-]:182 returning gateway output filter 5f2e080
04/07/2003 13:34:19 0 Branch Office [00] 5ceb5b8 BranchOfficeCbtCls::RegisterTunnel: rem[0.0.0.0-0.0.0.0]@[177.178.1.60] loc[0.0.0.0-0.0.0.0] overwriting tunnel context [#####] with [57fe780]
04/07/2003 13:34:19 0 ISAKMP [03] Established IPsec SAs with 177.178.1.60:
04/07/2003 13:34:19 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-MD5 outbound SPI 0x7512c
04/07/2003 13:34:19 0 ISAKMP [03] IPcomp LZ5 outbound CPI 0x4fbc
04/07/2003 13:34:19 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-MD5 inbound SPI 0x19e24a
04/07/2003 13:34:19 0 ISAKMP [03] IPcomp LZ5 inbound CPI 0x521c
04/07/2003 13:34:39 0 RTM [10] netw/wite RTM_RouteDef: N 20.4.4.0 M 255.255.255.0 NumNH 1 NH 177.178.1.60 CM 0x5ceb1b0
04/07/2003 13:34:39 0 RTM [00] writeNewEntry: adding new: 20.4.4.0 to 20.4.4.255
```

- A.The tunnel was initiated from the local switch.
- B.The tunnel was initiated from the remote switch.
- C.The tunnel is a peer-to-peer static routing tunnel.
- D.The tunnel is a peer-to-peer dynamic routing tunnel.
- E.Perfect Forward Secrecy is required on one end of the tunnel but not configured.

**Correct Answers: A D**

3: You have been tasked to troubleshoot a customer's Contivity network. You log into the Contivity to view information in the routing table and identify UTUNNEL routes. What does the UTUNNEL status information mean?

- A.access list are enabled
- B.Route Policy Services are enabled
- C.Client Address Redistribution is enabled
- D.the UTUNNEL route is the same as a Static route

**Correct Answers: C**

4: Your company has been using a Contivity 1740 switch running Release 5.0. A telecommuter is reporting that they are receiving an error message when they attempt to connect to the VPN switch. The error message states Remote host not responding . Which situation most accurately describes

the cause of the problem?

- A.The Contivity 1740 user database may have become corrupted.
- B.The users may be using the incorrect version of the Nortel Contivity Extranet Client.
- C.The Contivity 1740 may be configured to ignore requests from a range of IP addresses.
- D.Telecommuters may have enabled a firewall or purchased a broadband router that is blocking port 500.

**Correct Answers: D**

5: A customer has a Contivity 1740 running Release 5.0 at a remote site. The Contivity rebooted from an unknown cause. You are tasked to determine the cause of the reboot on the Contivity. From where would you find information prior to the reset?

- A.check branch office tunnel statistics
- B.check the event log for the information
- C.check the system log to attempt to locate the information
- D.call Nortel Networks Support to have them retrieve the information

**Correct Answers: C**

6: As a support specialist you need a summary of the current state of a Contivity system. What status screen must you access in order to retrieve this information?

- A.Status ---&gt; Report
- B.Status ---&gt; System
- C.Status ---&gt; Statistics
- D.Status ---&gt; Health Check

**Correct Answers: D**

7: Click the Exhibit button. A customer is attempting to bring a tunnel up between a Contivity 2700 and Contivity 2600. They asked the support engineer to interpret the output from the event log. Given the output shown in the exhibit, what is true? (Choose two.)

```
04/07/2003 13:12:52 0 Security [11] Session: IPSEC[177.178.1.60] attempting login
04/07/2003 13:12:52 0 Security [01] Session: IPSEC[177.178.1.60] has no active sessions
04/07/2003 13:12:52 0 Security [01] Session: IPSEC[177.178.1.60] Syd-Tok has no active accounts
04/07/2003 13:12:52 0 ISAKMP [02] Oakley Main Mode proposal accepted from 177.178.1.60
04/07/2003 13:12:52 0 Security [01] Session: IPSEC[177.178.1.60]:162 SHARED-SECRET authenticate attempt...
04/07/2003 13:12:52 0 Security [01] Session: IPSEC[177.178.1.60]:162 attempting authentication using LOCAL
04/07/2003 13:12:52 0 Security [11] Session: IPSEC[177.178.1.60]:162 authenticated using LOCAL
04/07/2003 13:12:52 0 Security [11] Session: IPSEC[177.178.1.60]:162 bound to group /Base/Syd-Tok
04/07/2003 13:12:52 0 Security [01] Session: IPSEC[177.178.1.60]:162 using group filter permit all
04/07/2003 13:12:52 0 Security [11] Session: IPSEC[177.178.1.60]:162 authorized
04/07/2003 13:12:52 0 ISAKMP [02] ISAKMP SA established with 177.178.1.60
04/07/2003 13:12:52 0 Security [11] Session: network IPSEC[20.4.0.255.255.255.0] attempting login
04/07/2003 13:12:52 0 Security [11] Session: network IPSEC[20.4.0.255.255.255.0] logged in from gateway [177.178.1.60]
04/07/2003 13:12:52 0 Outbound ESP from 177.178.1.50 to 177.178.1.60 SPI 0x000cbb14 [03] ESP encap session SPI 0x14bb0c00 bound to cpu 0
04/07/2003 13:12:52 0 Inbound ESP from 177.178.1.60 to 177.178.1.50 SPI 0x0014dcc7 [03] ESP decap session SPI 0xc7dc1400 bound to cpu 0
04/07/2003 13:12:52 0 Security [01] Session: IPSEC[-]:163 Using gateway input filters: 57830d8 46736a8 6e33a10
04/07/2003 13:12:52 0 Security [01] Session: IPSEC[-]:163 returning gateway output filter: 512e080
04/07/2003 13:12:53 0 Branch Office [00] 5d05210 BranchOfficeCtxCls: RegisterTunnel: rem[20.4.0.255.255.255.0]@[177.178.1.60] loc[10.4.0.255.255.255.0] overwriting tunnel context [0] with [571c828]
04/07/2003 13:12:53 0 ISAKMP [03] Established IPsec SAs with 177.178.1.60
04/07/2003 13:12:53 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-MD5 outbound SPI 0xcbb14
04/07/2003 13:12:53 0 ISAKMP [03] IPComp LZS outbound CPI 0xcb7
04/07/2003 13:12:53 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-MD5 inbound SPI 0x14dcc7
04/07/2003 13:12:53 0 ISAKMP [03] IPComp LZS inbound CPI 0xbe4a
```

- A.The tunnel is up and running.
- B.The tunnel was initiated from the local Contivity.
- C.The tunnel was initiated from the remote Contivity.
- D.The phase 1 negotiation failed due to mismatched shared secrets.

**Correct Answers: A C**

8: You have been tasked to install a Contivity 5000 at a customer site. You suspect that the redundant power supply became unseated during shipping. You would like to see a warning message on the Contivity system. Which status screen will show the warning message?

- A. Statistics Screen
- B. Event log Screen
- C. Security Log Screen
- D. Health Check Screen

**Correct Answers: D**

9: You want to check the routing status information for a Contivity 5.0 system. The Contivity is managed using a web browser. What status information can you see from the web browser on the Routing --&gt; OSPF status screen? (Choose four.)

- A. the contents of the LSDB
- B. the list of Neighbors on the Contivity
- C. the summary information on the Contivity
- D. the encryption information on the Contivity
- E. the interface information about OSPF on the Contivity
- F. the information regarding filtered routes on the Contivity

**Correct Answers: A B C E**

10: Click the Exhibit button. Given the Contivity event log shown in the exhibit, why can a branch office tunnel not be established to the Contivity 4600?

```
04/07/2003 14:04:39 0 Branch Office [01] IPSEC branch office connection
initiated to rem[0.0.0.0-0.0.0.0]@[177.178.1.60] loc[0.0.0.0-0.0.0.0]
04/07/2003 14:04:39 0 Security [11] Session: IPSEC[177.178.1.60]
attempting login
04/07/2003 14:04:39 0 Security [01] Session: IPSEC[177.178.1.60] has no
active sessions
04/07/2003 14:04:39 0 Security [01] Session: IPSEC[177.178.1.60] Syd-Tok
has no active accounts
04/07/2003 14:04:39 0 Security [01] Session: IPSEC[177.178.1.60]:186
SHARED-SECRET authenticate attempt...
04/07/2003 14:04:39 0 Security [01] Session: IPSEC[177.178.1.60]:186
attempting authentication using LOCAL
04/07/2003 14:04:39 0 Security [11] Session: IPSEC[177.178.1.60]:186
authenticated using LOCAL
04/07/2003 14:04:39 0 Security [11] Session: IPSEC[177.178.1.60]:186
bound to group /Base/Syd-Tok
04/07/2003 14:04:39 0 Security [01] Session: IPSEC[177.178.1.60]:186
using group filter permit all
04/07/2003 14:04:39 0 Security [11] Session: IPSEC[177.178.1.60]:186
authorized
04/07/2003 14:04:39 0 Security [11] Session: network
IPSEC[0.0.0.0-0.0.0.0] attempting login
04/07/2003 14:04:40 0 ISAKMP [02] ISAKMP SA established with
177.178.1.60
04/07/2003 14:04:40 0 ISAKMP [13] Error notification (No proposal chosen)
received from 177.178.1.60
04/07/2003 14:04:40 0 Security [12] Session: IPSEC[-]:187 logged out
```

- A. The branch office tunnel is undefined on the Contivity.
- B. Filters on the Contivity 4600 are preventing the connection.
- C. There is an encryption type mis-match between the two units.

D.IPsec is NOT enabled on the public interfaces of either the Contivity.

**Correct Answers: C**

11: Click the Exhibit button. A remote user has reported that they cannot login to a Contivity. Given the Contivity 2700 event log shown in the exhibit, what may have caused this problem to occur?

```
03/13/2001 09:28:11 0 Security [13] Session: IPSEC uid invalid -
authentication failed
03/13/2001 09:28:11 0 ISAKMP [13] No proposal chosen in message from
10.0.0.126
03/13/2001 09:28:11 0 ISAKMP [02] Deleting ISAKMP SA with 10.0.0.126
```

A.IPsec is not enabled on the Contivity.

B.There is no active session between the user and the server.

C.There is an encryption type mis-match between the user and server.

D.The user name does not exist in any of the enabled authentication methods on the Contivity.

**Correct Answers: D**

12: A support engineer has configured a DHCP server in a Contivity VPN switch via a Web-based interface. What is the next step in the process for the configuration changes to take place?

A.Restart the DHCP server.

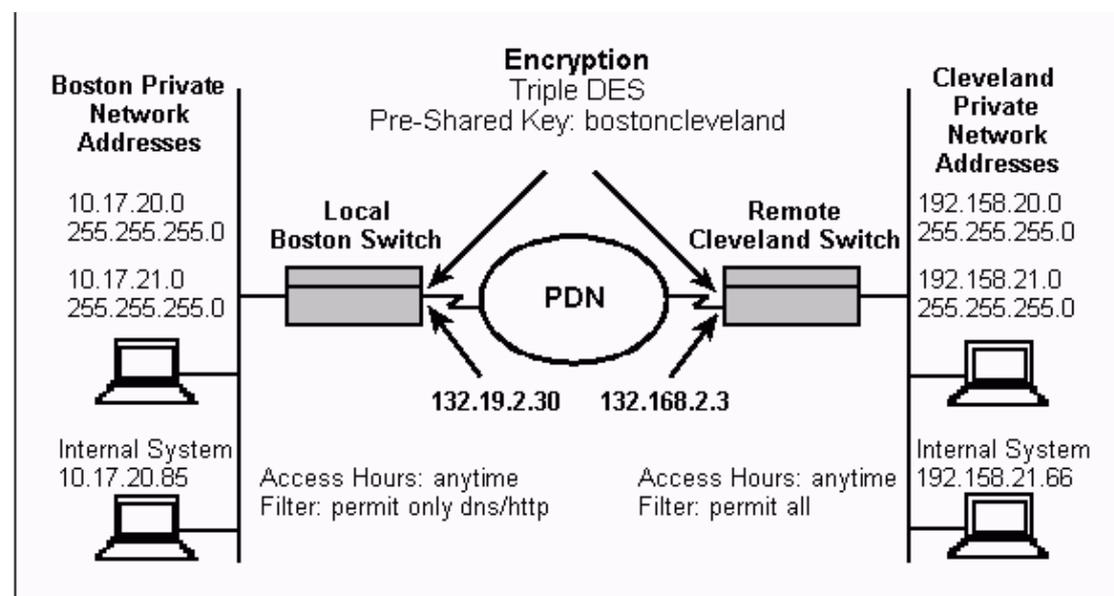
B.Enable the LDAP address pool.

C.Disable the LDAP address pool.

D.No action required: configuration changes are automatic.

**Correct Answers: A**

13: Click the exhibit button. Based on the Contivity 5.0 network in the exhibit, you are tasked to configure OSPF. How many OSPF areas are required to make the branch office configuration work?



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

**Correct Answers: A**

14: A customer has a network consisting of a Contivity 5000 at their corporate site and a mixture of Contivity 1700 and Contivity 2700 systems connected in a full mesh. All are using branch office connections and a static routing scheme. What must you do to ensure network redundancy?

- A.Implement the use of nested tunnels.
- B.Enable branch-to-branch forwarding on the Contivity 5000 switch.
- C.It is not possible to enable branch forwarding with this equipment configuration.
- D.Set up NAT devices at the corporate site and all of the branch office to establish a virtual LAN.

**Correct Answers: B**

15: On a Contivity 5.0 system, which tunneling protocol creates its tunnel between the ISP access concentrator and the client's network server? (Choose two.)

- A.L2F
- B.PPP
- C.L2TP
- D.IPsec
- E.PPTP

**Correct Answers: A C**