

Exam Code: 920-449

Exam Name: nncse contivity security

Vendor: Nortel

Version: DEMO

Part: A

1: A Contivity configuration has two private interfaces (LAN 0 and LAN 1) and one public interface (LAN 3) with Application servers residing on LAN 0. An administrator needs to create a default rule in order to allow users from LAN 1 and tunneled users from LAN 3 to access the application servers in LAN 0. What would be the most secure interface classification for the source interface?

- A.Any
- B.Trusted
- C.Tunnel: Any
- D.LAN 1 and LAN 3

Correct Answers: B

2: A technician is setting up a rule base for a Contivity Stateful Firewall configuration. The technician plans to enable a Lockdown rule. What will be the impact of this rule?

- A.non-tunneled traffic will be blocked
- B.access to the firewall will be blocked
- C.outgoing traffic through the firewall will be blocked
- D.incoming traffic through the firewall will be blocked

Correct Answers: B

3: A company has a main office and three branch offices. Each branch office has a branch office tunnel (BOT) connection to the main office. The following conditions exist: - Contivity firewall is disabled but each BOT has a default setting of ermit all?tunnel filter configured under the group profile. - Contivity firewall is disabled but each BOT has a default setting of ?ermit all?tunnel filter configured under the group profile. - The company has their own internal/private DNS server which resides in the main office. - Contivity from each branch offices is acting as DNS proxy. - Workstations from the branch offices are pointing to their local Contivity as the default gateway and DNS server. All workstations from the branch offices can reach all devices in the main office via IP address but cannot reach them through DNS names. What is the most likely cause of the problem?

- A.The access control of ermit all?given to the BOT group is enough to allow DNS to pass through the tunnel so the DNS server could be The access control of ?ermit all?given to the BOT group is enough to allow DNS to pass through the tunnel so the DNS server could be down.
- B.DNS server is up but main office's Contivity has DNS setting unchecked under the allow management traffic for remote servers portion of the permit all rule.
- C.DNS server is up but branch offices' Contivity has DNS setting unchecked under the allow management traffic for remote servers portion of the permit all rule.
- D.Main office's Contivity has DNS setting checked under the allow management traffic for remote servers portion of the permit all rule but DNS server could be down.

Correct Answers: C

4: Contivity Stateful Firewall has been enabled on a customer's Contivity system. The customer wants to extend user authentication on traffic between branch office connections in their VPN

environment and a technician has set up Firewall User Authentication (FWUA). How will this affect system users?

- A. Users will now have transparent access to the Contivity Stateful Firewall.
- B. Users will be automatically authenticated for internal authorization services such as LDAP.
- C. Users will be automatically authenticated for external authorization services such as RADIUS.
- D. Users will be required to log into the Contivity Stateful Firewall before they are granted network access.

Correct Answers: D

5: A Contivity has two private interfaces (LAN and DMZ) and one public interfaces (INT). Workstation1 with an IP address of 10.10.10.1/24 is in the network that is directly attached to the private interface LAN. Workstation2 with an IP address of 20.20.20.1/24 is in the network that is directly attached to private interface DMZ. The requirement is to block only traffic from workstation1 to workstation2 using interface filters to be applied to the private interface DMZ. Select the most appropriate filter action, direction, and address for the access control filter.

- A. Filter action = Deny ; Direction = Inbound ; Address = 20.20.20.1
- B. Filter action = Deny ; Direction = Inbound ; Address = 10.10.10.1
- C. Filter action = Deny ; Direction = Outbound ; Address = 10.10.10.1
- D. Filter action = Deny ; Direction = Outbound ; Address = 20.20.20.1

Correct Answers: C

6: Company A and Company B established a branch office tunnel connection using Contivity v4.8 with the following setup: Company A - private interface (LAN A) has an IP address of 192.168.3.1/24 Company A - FTP server with IP address 192.168.3.3/24 which resides in LAN A Company B - private interface (LAN B) has an IP address of 192.168.30.2/24 The security policy allows users from LAN B to access Company A's FTP server to download files with no other access to the rest of Company A's network. In Company A's Contivity Stateful Firewall configuration, what would be the most likely default rule?

- A. Source interface = LAN B ; Destination Interface = LAN A ; Source = 192.168.30.0/24 ; Destination = 192.168.3.3/24 ; Service = FTP ; Action = Allow
- B. Source interface = LAN B ; Destination Interface = Trusted ; Source = 192.168.30.0/24 ; Destination = 192.168.3.3/24 ; Service = FTP ; Action = Allow
- C. Source interface = Tunnel: Any ; Destination Interface = LAN A ; Source = 192.168.30.0/24 ; Destination = 192.168.3.3/24 ; Service = FTP ; Action = Allow
- D. Source interface = Branch Tunnel: Any ; Destination Interface = Trusted ; Source = 192.168.30.0/24 ; Destination = 192.168.3.3/24 ; Service = FTP ; Action = Allow

Correct Answers: D

7: A Contivity has a private interface (LAN) and a public interface (DMZ). Workstation1 with an IP address of 10.10.10.1/24 is in the network that is directly attached to the private interface LAN. Workstation2 with an IP address of 20.20.20.1/24 is in the network that is directly attached to public interface DMZ. The requirement is to block only traffic from workstation1 to workstation2 using interface filters applied to the private interface LAN. Select the most appropriate filter action, direction, and address for the access control filter.

- A.Filter action = Deny ; Direction = Inbound ; Address = 20.20.20.1
- B.Filter action = Deny ; Direction = Inbound ; Address = 10.10.10.1
- C.Filter action = Deny ; Direction = Outbound ; Address = 20.20.20.1
- D.Filter action = Deny ; Direction = Outbound ; Address = 10.10.10.1

Correct Answers: A

8: A technician is debugging a problem on a Contivity system and has input Override rules to be in effect during this time. Which statement best describes how the Override rules will function?

- A.will be processed first
- B.will override all rules in the policy
- C.will override the rest of the rules described later in the policy
- D.will apply only to the specific interface identified in the override rule

Correct Answers: C

9: A customer's Contivity system is currently supporting a network of tunneled and non-tunneled traffic. Assume Contivity Stateful Firewall has just been enabled but no specific rules have been configured. How will the tunneled and non-tunneled traffic be handled?

- A.Tunneled and non-tunneled traffic is allowed until rules restricting specific traffic are established.
- B.Tunneled traffic is allowed but non-tunneled traffic is disallowed until rules allowing for specific traffic are established
- C.Non-tunneled traffic is allowed but tunneled traffic is disallowed until rules allowing for specific traffic are established.
- D.Tunnels can be established, but all data traffic is disallowed from passing through the CES until rules allowing for specific traffic are established.

Correct Answers: D

10: A company has a Contivity v4.8 configured with branch office tunnel connections under /Base/Partners group for all of its business partners. User tunnel access is also provided for all employees and partners. The Contivity has two private interfaces (LAN and DMZ) and one public interface. Application servers reside in the DMZ. The following rules are in effect: Interface specific rule 1 : Source interface rule = LAN ; Source interface = LAN ; Destination interface = DMZ ; Source = Any ; Destination = Any ; Service = Any ; Action = Allow Default rule 1 : Source interface = Trusted ; Destination Interface = Trusted ; Source = Any ; Destination = Any ; Service = Any ; Action = Allow The company's security policy dictates that only local users and remote users through a branch office tunnel can access application servers in the DMZ. However, even users via user tunnel connection also appear to have access to the application servers in the DMZ. How can the rules be changed to resolve the problem?

- A.Interface specific rule 1 is correct but the source interface for default rule 1 is wrong and should be changed to Branch Tunnel: Any.
- B.Default rule 1 is correct but the source interface for interface specific rule 1 is wrong and should be changed to Branch Tunnel: Any.
- C.Interface specific rule 1 is correct but the source interface for default rule 1 is wrong and should be changed to Branch Tunnel:/Base/Partners.

D.Default rule 1 is correct but the source interface for interface specific rule 1 is wrong and should be changed to Branch Tunnel:/Base/Partners.

Correct Answers: A