

100% Money Back Guarantee

Vendor: Juniper

Exam Code: JN0-696

Exam Name: Security Support, Professional (JNCSP-SEC)

Version: Demo

QUESTION NO: 1

You are having problems establishing an IPsec tunnel between two SRX Series devices.

What are two explanations for this problem? (Choose two.)

- A. proposal mismatch
- B. antivirus configuration
- C. preshared key mismatch
- D. TCP MSS clamping is disabled

Answer: B,D

QUESTION NO: 2

Two SRX Series devices are having problems establishing an IPsec VPN session. One of the devices has a firewall filter applied to its gateway interface that rejects UDP traffic.

What would resolve the problem?

- A. Disable the IKE Phase 1 part of the session establishment.
- B. Disable the IKE Phase 2 part of the session establishment.
- C. Change the configuration so that session establishment uses TCP.
- D. Edit the firewall filter to allow UDP port 500.

Answer: A

QUESTION NO: 3

Your SRX Series device has the following configuration:

```
user@host> show security policies
```

```
...
```

```
Policy: my-policy, State: enabled, Index: 5, Sequence number: 1
```

```
Source addresses: any
```

Destination addresses: any

Applications: snmp

Action: reject

From zone: trust, To zone: untrust

...

When traffic matches my-policy, you want the device to silently drop the traffic; however, you notice that the device is replying with ICMP unreachable messages instead.

What is causing this behavior?

- A. the snmp application
- B. the reject action
- C. the trust zone
- D. the untrust zone

Answer: C

QUESTION NO: 4

You want to allow remote users using PCs running Windows 7 to access the network using an IPsec VPN. You implement a route-based hub-and-spoke VPN; however, users report that they are not able to access the network.

What is causing this problem?

- A. The remote clients do not have proper licensing.
- B. Hub-and-spoke VPNs cannot be route-based; they must be policy-based.
- C. The remote clients' OS is not supported.
- D. Hub-and-spoke VPNs do not support remote client access; a dynamic VPN must be implemented instead.

Answer: B

QUESTION NO: 5

You notice that the secondary node of a chassis cluster has become disabled.

What caused this behavior?

- A. The fxp0 interface on the secondary device failed.
- B. The control link between the devices failed.
- C. A reth on the secondary device failed.
- D. An IPsec tunnel between the two devices failed.

Answer: D

QUESTION NO: 6

Users at a branch office report that they cannot reach an internal Web server. The users connect through a single SRX Series device to reach the Web server. A security policy has been configured on the device that allows traffic to flow between interfaces in the Trust zone.

What is causing this problem?

- A. The interface on the device that connects to the Web server is not in the Trust zone.
- B. The IPsec VPN connection between the users and the Web server is down.
- C. There is a host inbound traffic configuration problem.
- D. There is an antispam configuration problem.

Answer: C

QUESTION NO: 7

You are asked to troubleshoot a user communication problem. Users connected to the Trust zone cannot communicate with other devices connected to the same zone. These users are able to communicate with other devices in all other zones.

How should you resolve this problem?

- A. You must put each device in a separate subzone to allow internal communication.

- B. You must configure a security policy to allow intrazone communication.
- C. You must enable the allow-internal parameter under the Trust security zone.
- D. You must enable the all parameter for host inbound traffic for the zone.

Answer: B

QUESTION NO: 8

You have implemented AppTrack on your SRX Series device to track YouTube streaming video usage in your network. However, many of the YouTube videos that your users are watching are shorter than five minutes. You notice that the statistics for starting these short YouTube videos are not being recorded by AppTrack.

Which two actions would allow AppTrack to record the statistics for these sessions? (Choose two.)

- A. Change AppTrack to collect session information during shorter intervals.
- B. Change AppTrack to collect session information when the session is first created.
- C. Change AppTrack to collect session information for nested applications only.
- D. Change AppTrack to collect session information for applications only.

Answer: A,B

QUESTION NO: 9

While attempting to set up IDP on an SRX Series device, the IDP attack database fails to download.

What is one reason for this behavior?

- A. The device's Untrust zone to Trust zone security policy does not allow this traffic.
- B. The device's configuration does not include the URL from which to retrieve the attack database.
- C. A firewall filter applied to the loopback interface is preventing the download of the attack database.
- D. The host inbound traffic has not been configured correctly.

Answer: C

QUESTION NO: 10

When attempting to delete IDP policies and configurations from an SRX Series device, a user enters these configuration commands:

Delete security idp

Commit

However, after the commit has completed, the configuration is still present under the [edit security idp] hierarchy.

What should the user do to permanently remove the configuration?

- A. Delete the /var/db/scripts/commit/templates.xsl file and reboot the device.
- B. Delete the [edit security idp] hierarchy, commit the change, and immediately reboot the device.
- C. Stop the idpd process using the set system processes idp-policy disable configuration command, commit the change, delete the [edit security idp] hierarchy, and then commit that change.
- D. Delete the IDP templates commit script from the [edit system scripts commit] hierarchy, delete the [edit security idp] hierarchy, and then commit the change.

Answer: D

QUESTION NO: 11

You recently configured the antivirus feature profile on your Junos device. The security policy is sending traffic for antivirus scanning. However, the traffic is being blocked and you repeatedly receive the system log message that the scan engine is not ready. You must not allow the traffic to be dropped when the scan engine is not ready.

Which action will resolve this problem?

- A. Configure antivirus trickling to prevent the scan engine from timing out.
- B. Configure an antivirus file scanning extension list to reduce the number of files for scanning.
- C. Configure an antivirus fallback option to permit the traffic when the scan engine is not ready.
- D. Configure an antivirus content size limit to minimize the scanning of large files.

Answer: C

QUESTION NO: 12

You are troubleshooting a problem on your Junos device where the antispam SBL server is no longer filtering known spam hosts. You notice that local list antispam filtering is still working for known spam hosts.

What would cause this problem?

- A. You have configured the sbl-default-server parameter in the antispam feature profile.
- B. DNS has stopped working on your Junos device.
- C. The antispam license has expired on your Junos device.
- D. The default spam-action parameter has been set to permit.

Answer: C

QUESTION NO: 13

In preparation for future expansion, a user decides to configure a stand-alone SRX Series device for chassis-clustering mode. The user enters the command set chassis cluster cluster-id 0 node 0 reboot on the device. After the device reboots, the user sees this output:

```
user@host> show chassis cluster status
```

```
error: Chassis cluster is not enabled.
```

```
user@host>
```

The device does not enter chassis-clustering mode.

What is the problem?

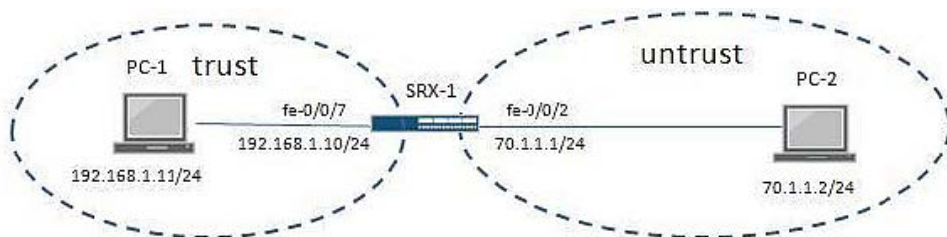
- A. An SRX Series device will not enter chassis-clustering mode unless the fxp0 and fxp1 interfaces are defined in the configuration.

- B.** An SRX Series device will only enter chassis-clustering mode when it finds a peer that is also configured for chassis-clustering mode.
- C.** Cluster ID 0 is not valid for a chassis cluster.
- D.** Node ID 0 is not valid for a chassis cluster.

Answer: C

QUESTION NO: 14

-- Exhibit --



```

user@SRX-1> show security flow session
Session ID: 743, Policy name: allow-internet/4, Timeout: 2, Valid
In: 192.168.1.11/318 --> 70.1.1.2/1717;icmp, If: fe-0/0/7.0, Pkts: 1, Eytes: 84
Out: 70.1.1.2/1717 --> 70.1.1.10/25110;icmp, If: fe-0/0/2.0, Pkts: 0, Eytes: 0

Session ID: 744, Policy name: allow-internet/4, Timeout: 2, Valid
In: 192.168.1.11/319 --> 70.1.1.2/1717;icmp, If: fe-0/0/7.0, Pkts: 1, Eytes: 84
Out: 70.1.1.2/1717 --> 70.1.1.10/12464;icmp, If: fe-0/0/2.0, Pkts: 0, Eytes: 0

Session ID: 745, Policy name: allow-internet/4, Timeout: 4, Valid
In: 192.168.1.11/320 --> 70.1.1.2/1717;icmp, If: fe-0/0/7.0, Pkts: 1, Eytes: 84
Out: 70.1.1.2/1717 --> 70.1.1.10/22227;icmp, If: fe-0/0/2.0, Pkts: 0, Eytes: 0

user@SRX-1> show security policies policy-name allow-internet
From zone: trust, To zone: untrust
Policy: allow-internet, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses: any
Destination addresses: any
Applications: any
Action: permit

root@SRX-1> ping 70.1.1.2
PING 70.1.1.2 (70.1.1.2): 56 data bytes
64 bytes from 70.1.1.2: icmp_seq=0 ttl=64 time=3.176 ms
64 bytes from 70.1.1.2: icmp_seq=1 ttl=64 time=3.261 ms
...

```

-- Exhibit --

Click the Exhibit button.

You are troubleshooting a communication problem between a trust zone and an untrust zone in the network, where PC-1 cannot ping PC-2.

Referring to the exhibit, which configuration change on SRX-1 would resolve this problem?

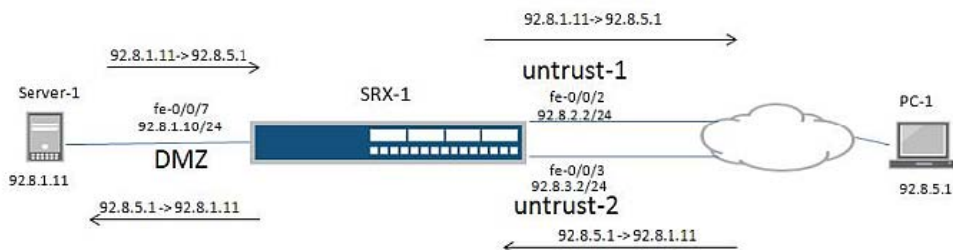
Add a security policy to allow ICMP traffic from the untrust zone to the trust zone.

- A. Configure proxy-arp under the [edit security nat] hierarchy.
- B. Add a security policy to allow ICMP traffic from the trust zone to the untrust zone.
- C. Add an address book entry for address 70.1.1.2.

Answer: B

QUESTION NO: 15

-- Exhibit --



```

user@SRX-1> show security flow session destination-prefix 92.8.1.11
Session ID: 5401, Policy name: dmz-trust-2/7, Timeout: 48, Valid
In: 92.8.5.1/0 --> 92.8.1.11/1950:icmp, If: fe-0/0/3.0, Pkts: 1, Bytes: 84
Out: 92.8.1.11/1950 --> 92.8.5.1/0:icmp, If: fe-0/0/7.0, Pkts: 0, Bytes: 0

user@SRX-1> show route 92.8.5.1
...
92.8.5.1/32 * [Static/5] 00:46:54
    > to 92.8.2.1 via fe-0/0/2.0

user@SRX-1> show log flow-trace
...
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: <92.8.1.11/1937->92.8.5.1/74:1> matched filter pfl:
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: packet [84] ipid = 1287, 842400dle
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: ---- flow_process_pkt: (thd 1): flow_ctxt type 15, common flag 0x0, mbuf
0x42400b00, rtbl_idx = 0
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: Flow process pak fast ifl 73 in ifp fe-0/0/7.0
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: fe-0/0/7.0:92.8.1.11->92.8.5.1, icmp, (0/0)
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: find flow: table 0x4dd0f958, hash 57751(0xffff), sa 92.8.1.11, da 92.8.5.1,
sp 1937, dp 74, proto 1, tok 7
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: flow got session.
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: flow session id 5386
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: route lookup failed: dest-ip 92.8.5.1 orig ifp fe-0/0/3.0 output_ifp fe-
0/0/2.0 fto 0x49b28268 orig-zone 10 out-zone 9 vsd 0
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: packet dropped, pak dropped since re-route failed
Jun 13 08:18:21 08:18:21.620138:CID-0:RT: ---- flow_process_pkt rc 0x7 (fp rc -1)
...
    
```



-- Exhibit --

Click the Exhibit button.

Referring to the exhibit, PC-1 is unable to ping Server-1. Traffic from PC-1 to Server-1 arrives on interface fe-0/0/3 but return traffic from Server-1 to PC-1 should be sent out from interface fe-0/0/2.

What would you change on SRX-1 to resolve this problem?

- A. Configure a security policy to allow traffic from the DMZ zone to the untrust-1 zone.
- B. Configure a security policy to allow traffic from the DMZ zone to the untrust-2 zone.
- C. Move both interface fe-0/0/2 and fe-0/0/3 to the same security zone.
- D. Disable TCP SYN check and TCP sequence check.

Answer: C

QUESTION NO: 16

-- Exhibit --

```
user@host> show security flow session interface ge-0/0/10.0
```

```
Session ID. 29, Policy name: to-infrastructure/4, Timeout: 1250, Valid
```

```
Resource information : FTP ALG, 1, 0
```

```
In: 10.1.1.213/61892 --> 10.2.2.20/21;tcp, If: ge-0/0/8.0, Pkts: 25, Bytes: 1242
```

```
Out: 10.2.2.20/21 --> 10.1.1.213/61892;tcp, If: ge-0/0/10.0, Pkts: 18, Bytes: 1278
```

```
Total sessions: 1
```

```
user@host> show interfaces ge-0/0/10 | match zone
```

```
Security: Zone: infrastructure
```

```
user@host> show interfaces ge-0/0/8 | match zone
```

```
Security: Zone: finance
```

```
user@host> show configuration security policies from-zone infrastructure to-zone finance
```

```
user@host> show log flow-traceoptions
```

```
Jun 13 14:44:01 14:44:01.059151:CID-0:RT:SPU received an event,type 112, common:3
```

Jun 13 14:44:01 14:44:01.059151:CID-0:RT:Rcv packet with rtbl idx 0, cos 0

Jun 13 14:44:01 14:44:01.059151:CID-0:RT:SPU processing spu_flushed_pak, flag: 0x2, mbuf:0x423f6100

Jun 13 14:44:01 14:44:01.060343:CID-0:RT:10.2.2.20/20->10.1.1.213/64313;6> matched filter filter2:

Jun 13 14:44:01 14:44:01.060473:CID-0:RT:packet [64] ipid = 1614, @423fd19c

Jun 13 14:44:01 14:44:01.060473:CID-0:RT:---- flow_process_pkt: (thd 3): flow_ctxt type 15, common flag 0x0, mbuf 0x423fcf80, rtbl_idx = 0

Jun 13 14:44:01 14:44:01.060473:CID-0:RT: flow process pak fast ifl 71 in_ifp ge-0/0/10.0

Jun 13 14:44:01 14:44:01.060473:CID-0:RT: ge-0/0/10.0:10.2.2.20/20->10.1.1.213/64313, tcp, flag 2 syn

Jun 13 14:44:01 14:44:01.060473:CID-0:RT: find flow: table 0x49175b08, hash 34391(0xffff), sa 10.2.2.20, da 10.1.1.213, sp 20, dp 64313, proto 6, tok 8

Jun 13 14:44:01 14:44:01.060473:CID-0:RT: no session found, start first path. in_tunnel - 0, from_cp_flag - 0

Jun 13 14:44:01 14:44:01.060473:CID-0:RT: flow_first_create_session

Jun 13 14:44:01 14:44:01.060473:CID-0:RT:-jsf : preset sess plugin info for session 31

Jun 13 14:44:01 14:44:01.060473:CID-0:RT: Allocating plugin info block for plugin(21)

Jun 13 14:44:01 14:44:01.060473:CID-0:RT:[JSF] set ext handle 0x46389be8 for plugin 21 on session 31

Jun 13 14:44:01 14:44:01.060473:CID-0:RT:asl_usp_get_l3_out_ifp_out_tunnel ASL IPV4 out_ifp = ge-0/0/8.0 for dst:10.1.1.213 in vr_id:0

Jun 13 14:44:01 14:44:01.060473:CID-0:RT:SPU invalid session id 00000000

Jun 13 14:44:01 14:44:01.060473:CID-0:RT: jsf drop pak pid 21, jbuf 0x4fcd7038, release hold 0, sess_id 0

Jun 13 14:44:01 14:44:01.060761:CID-0:RT: After jsf gate hit. sid 0xfb39, pid 0, cookie 0x1f, jbuf 0x15. rc = 1

Jun 13 14:44:01 14:44:01.060761:CID-0:RT:RM populated xlate info for nsp2: 10.1.1.213/64313->10.2.2.20/20out_ifp = ge-0/0/8.0, out_tunnel = 0x0

Jun 13 14:44:01 14:44:01.060761:CID-0:RT: flow_first_in_dst_nat: in 0/10.0>, out 0/8.0> dst_addr 10.1.1.213, sp 20, dp 64313

Jun 13 14:44:01 14:44:01.060761:CID-0:RT: flow_first_in_dst_nat: bypassed by RM

Jun 13 14:44:01 14:44:01.060761:CID-0:RT: flow_first_rule_dst_xlate: bypassed by RM

Jun 13 14:44:01 14:44:01.060761:CID-0:RT: flow_first_routing: bypassed by RM

Jun 13 14:44:01 14:44:01.060761:CID-0:RT: flow_first_policy_search: bypassed by RM

Jun 13 14:44:01 14:44:01.060761:CID-0:RT: flow_first_reverse_mip: bypassed by RM

Jun 13 14:44:01 14:44:01.060761:CID-0:RT: flow_first_src_xlate: bypassed by RM

Jun 13 14:44:01 14:44:01.060761:CID-0:RT: flow_first_get_out_ifp: bypassed by RM

Jun 13 14:44:01 14:44:01.060761:CID-0:RT:is_loop_pak: No loop: on ifp: ge-0/0/8.0, addr: 10.1.1.213, rtt_idx:0

Jun 13 14:44:01 14:44:01.060761:CID-0:RT:[JSF]Normal interest check. regd plugins 18, enabled impl mask 0x0

Jun 13 14:44:01 14:44:01.060761:CID-0:RT:-jsf int check: plugin id 2, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060761:CID-0:RT:-jsf int check: plugin id 3, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060761:CID-0:RT:-jsf int check: plugin id 5, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060761:CID-0:RT:-jsf int check: plugin id 6, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf int check: plugin id 7, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf int check: plugin id 8, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf int check: plugin id 14, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:+++++++jsf_test_plugin_data_evh: 3

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf int check: plugin id 15, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf int check: plugin id 21, svc_req 0x0, impl mask 0x0. rc 3

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf int check: plugin id 22, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf int check: plugin id 25, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf int check: plugin id 26, svc_req 0x0, impl mask 0x0. rc 2

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf int check: plugin id 27, svc_req 0x0, impl mask 0x0. rc 4

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:[JSF]Plugins(0x0, count 0) enabled for session = 4294967296, impli mask(0x0), post_nat cnt 31 svc req(0x0)

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:[JSF]c2s order list:

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: 21

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:[JSF]s2c order list:

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: 21

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: service lookup identified service 79.

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: flow_first_final_check: in 0/10.0>, out 0/8.0>

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:flow_first_complete_session, pak_ptr: 0x48ae5ba0, nsp: 0x4c38e248, in_tunnel: 0x0

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:construct v4 vector for nsp2

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: existing vector list 82-454e5c90.

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: Session (id:31) created for first pak 82

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: flow_first_install_session=====> 0x4c38e248

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: nsp 0x4c38e248, nsp2 0x4c38e2c8

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: make_nsp_ready_no_resolve()

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: route lookup: dest-ip 10.2.2.20 orig ifp ge-0/0/10.0 output_ifp ge-0/0/10.0 orig-zone 8 out-zone 8 vsd 0

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: route to 10.2.2.20

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:Doing jsf sess create notify

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:flow_delete_gate: invoked for gate 0x4c077c24 [id 1000003]

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:gate_start_ageout: ageout started for gate 0x4c077c24

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: jsf sess id ignore. sess 31, pid 21, dir 1, st_buf 0x0.

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: jsf sess id ignore. sess 31, pid 21, dir 2, st_buf 0x0.

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:All plugins have ignored session :31

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: existing vector list 2-454ecbd0.

Jun 13 14:44:01 14:44:01.060975:CID-0:RT: existing vector list 2-454ecbd0.

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:-jsf create notify: plugin id 21. rc 3

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:flow_do_jsf_notify_session_creation(): natp(0x4c38e248): 0 SHORT_CIRCUITED. 0x00000000.

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:no need update ha

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:Installing c2s NP session wing

Jun 13 14:44:01 14:44:01.060975:CID-0:RT:Installing s2c NP session wing

Jun 13 14:44:01 14:44:01.061475:CID-0:RT: flow got session.

Jun 13 14:44:01 14:44:01.061475:CID-0:RT: flow session id 31

Jun 13 14:44:01 14:44:01.061475:CID-0:RT: vector bits 0x2 vector 0x454ecbd0

Jun 13 14:44:01 14:44:01.061475:CID-0:RT: tcp flags 0x2, flag 0x2

Jun 13 14:44:01 14:44:01.061475:CID-0:RT: Got syn, 10.2.2.20(20)->10.1.1.213(64313), nspflag 0x1021, 0x20

Jun 13 14:44:01 14:44:01.061475:CID-0:RT:mbuf 0x423fcf80, exit nh 0xa0010

Jun 13 14:44:01 14:44:01.061475:CID-0:RT: ----- flow_process_pkt rc 0x0 (fp rc 0)

-- Exhibit --

Click the Exhibit button.

While troubleshooting a device, you see that it is permitting packets for which it appears there is no policy.

Using the information in the exhibit, what is causing this behavior?

- A. It is permitted due to an ALG.
- B. It is permitted due to a stale policy.
- C. It is permitted due to a global policy.
- D. It is permitted due to a default permit policy.

Answer: A

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying our product !

- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.