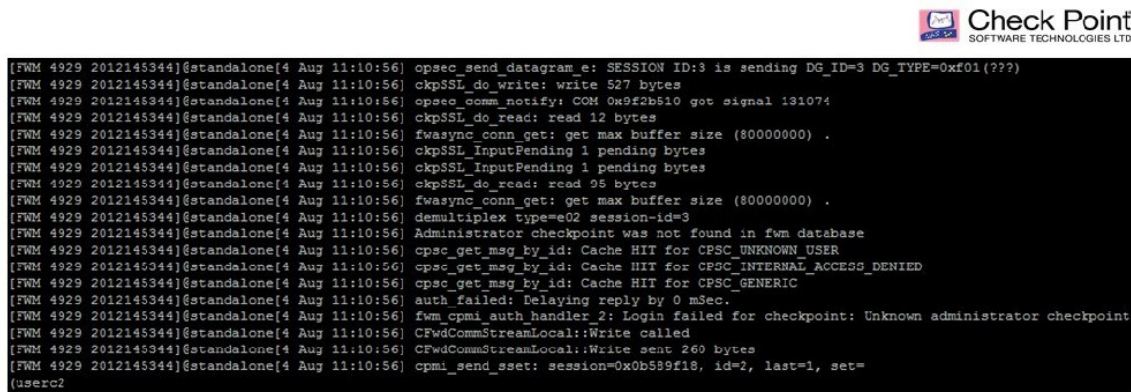


- **Vendor: Check Point**
- **Exam Code: 156-115.77**
- **Exam Name: Check Point Certified Security Master**
- **Question 1 – Question 40**

[Visit PassLeader and Download Full Version 156-115.77 Exam Dumps](#)

QUESTION 1

The user tried to connect in SmartDashboard and did not work. You started a FWM debug and receive the logs below:



```
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] opsec_send_datagram e: SESSION ID:3 is sending DG_ID=3 DG_TYPE=0xf01(???)
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] ckpSSL_do write: write 527 bytes
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] opsec_comm_notify: COM 0x9f2b510 got signal 131074
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] ckpSSL_do read: read 12 bytes
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] fwasync_conn_get: get max buffer size (80000000) .
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] ckpSSL_inputPending 1 pending bytes
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] ckpSSL_inputPending 1 pending bytes
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] ckpSSL_do read: read 95 bytes
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] fwasync_conn_get: get max buffer size (80000000) .
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] demultiplex type=e02 session-id=3
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] Administrator checkpoint was not found in fwm database
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] cpsec_get_msg_by_id: Cache HIT for CPSEC_UNKNOWN_USER
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] cpsec_get_msg_by_id: Cache HIT for CPSEC_INTERNAL_ACCESS_DENIED
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] cpsec_get_msg_by_id: Cache HIT for CPSEC_GENERIC
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] auth failed: Delaying reply by 0 msec.
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] fwm_cpsec_auth_handler 2: Login failed for checkpoint: Unknown administrator checkpoint
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] CFwdCommStreamLocal::Write called
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] CFwdCommStreamLocal::Write sent 269 bytes
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] cpml_send_sset: session=0x0b589f18, id=2, last=1, set=
(userc2
```

What is the error cause?

- A. IP not defined in \$FWDIR/conf/gui-clients
- B. Wrong user and password
- C. Wrong password
- D. Wrong user

Answer: D

QUESTION 2

When troubleshooting and trying to understand which chain is causing a problem on the Security Gateway, you should use the command:

- A. fw ctl zdebug drop
- B. fw tab -t connections
- C. fw monitor -e "accept;" -p all
- D. fw ctl chain

Answer: C

QUESTION 3

Which process should you debug when SmartDashboard authentication is rejected?

- A. fwm
- B. cpd
- C. fwd
- D. DAService

Answer: A

QUESTION 4

A fwm debug provides the following output. What prevents the customer from logging into SmartDashboard?



```

FWM 3103 1951651808@manager [2 Aug 23:03:17] fwasync_conn_get: get max buffer size (1048576) .
FWM 3103 1951651808@manager [2 Aug 23:03:17] sic_server_sst_sic_type_str: 61 security tyoe is cpmi.
FWM 3103 1951651808@manager [2 Aug 23:03:17] policy_query: src : cn=cp_mgmt,ou=srvmgmt..f2kd31 dst : CN=gui_client
FWM 3103 1951651808@manager [2 Aug 23:03:17] gui_connection_sic_plugin: gui client sic name on connection 61.
FWM 3103 1951651808@manager [2 Aug 23:03:17] call_handlers_list: conversion success
FWM 3103 1951651808@manager [2 Aug 23:03:17] PM_session_init: given session 1(cn=cp_mgmt,ou=srvmgmt..f2kd31;IP=192.168.220.113,CN=gui_client;18190;cpmi).
FWM 3103 1951651808@manager [2 Aug 23:03:17] PM_policy_query: input session 1(cn=cp_mgmt,ou=srvmgmt..f2kd31;IP=192.168.220.113,CN=gui_client;18190;cpmi).
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] sicobj_resolve_by_opsec: No object found with SIC name 'IP=192.168.220.113,CN=gui_client'
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] Login failed: 192.168.220.113 is not allowed for remote login
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwm_log: Login failed from IP=192.168.220.113,CN=gui_client: unauthorized client.
Sun Aug 3 02:03:17 2014 (GMT): reject client IP=192.168.220.113,CN=gui_client
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwnetobj_gettoysicname: table_chosen_get_with_param(ETABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113,CN=gui_client)
rc) returned NULL.
FWM 3103 1951651808@manager [2 Aug 23:03:17] PM_policy_query: rule not found.
FWM 3103 1951651808@manager [2 Aug 23:03:17] PM_policy_query: finished successfully, 1st method = deny
FWM 3103 1951651808@manager [2 Aug 23:03:17] fwasync_conn_get: get max buffer size (1048576) .

```

- A. There are not any policy to login in SmartDashboard
- B. FWM process is crashed and returned null to access
- C. User and password are incorrect
- D. IP not defined in \$FWDIR/conf/gui-clients

Answer: D

QUESTION 5

When performing a fwm debug, to which directory are the logs written?

- A. \$FWDIR/log
- B. \$FWDIR/log/fwm.elg
- C. \$FWDIR/conf/fwm.elg
- D. \$CPDIR/log/fwm.elg

Answer: B

QUESTION 6

You are attempting to establish an FTP session between your computer and a remote server, but it is not being completed successfully. You think the issue may be due to IPS. Viewing SmartView Tracker shows no drops. How would you confirm if the traffic is actually being dropped by the gateway?

- A. Search the connections table for that connection.
- B. Run a fw monitor packet capture on the gateway.
- C. Look in SmartView Monitor for that connection to see why it's being dropped.

D. Run fw ctl zdebug drop on the gateway.

Answer: D

QUESTION 7

The fw tab -t _____ command displays the NAT table.

- A. loglist
- B. tablist
- C. fwx_alloc
- D. conns

Answer: C

QUESTION 8

While troubleshooting a DHCP relay issue, you run a fw ctl zdebug drop and see the following output:

```
;[cpu_1];[fw_0];fw_log_drop: Packet proto=17 10.216.14.108:67 > 172.31.2.1:67 dropped by  
fw_handle_first_packet Reason: fwconn_init_links (INBOUND) failed;
```

Where 10.216.14.108 is the IP address of the DHCP server and 172.31.2.1 is the VIP of the Cluster. What is the most likely cause of this drop?

- A. An inbound collision due to a connections table check on pre-existing connections.
- B. An outbound collision due to a Rule Base check, and dropped by incorrectly configuring DHCP in the firewall policy.
- C. A link collision due to more than one NAT symbolic link being created for outgoing connections to the DHCP server.
- D. A link collision due to more than one NAT symbolic link being created for connections returning from the DHCP server back to the VIP of the Cluster.

Answer: D

QUESTION 9

You need to completely reboot the Operating System after making which of the following changes on the Security Gateway? (i.e. the command cprestart is not sufficient.)

1. Adding a hot-swappable NIC to the Operating System for the first time.
2. Uninstalling the R75 Power/UTM package.
3. Installing the R75 Power/UTM package.
4. Re-establishing SIC to the Security Management Server.
5. Doubling the maximum number of connections accepted by the Security Gateway.

- A. 2, 3 only
- B. 3 only
- C. 3, 4, and 5 only
- D. 1, 2, 3, 4, and 5

Answer: A

QUESTION 10

The Security Gateway is installed on SecurePlatform R77. The default port for the Web User Interface is _____.

- A. TCP 443
- B. TCP 4433
- C. TCP 18211
- D. TCP 257

Answer: A

QUESTION 11

You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the

authentication credentials. What must happen after authentication that allows the client to connect to the Security Gateway's VPN domain?

- A. Active-X must be allowed on the client.
- B. The SNX client application must be installed on the client.
- C. SNX modifies the routing table to forward VPN traffic to the Security Gateway.
- D. An office mode address must be obtained by the client.

Answer: C

QUESTION 12

Your primary Security Gateway runs on SecurePlatform. What is the easiest way to back up your Security Gateway R77 configuration, including routing and network configuration files?

- A. Using the native SecurePlatform backup utility from command line or in the Web based user interface.
- B. Copying the directories \$FWDIR/conf and \$FWDIR/lib to another location.
- C. Using the command upgrade_export.
- D. Run the pre_upgrade_verifier and save the .tgz file to the directory /temp.

Answer: A

QUESTION 13

Where in a fw monitor output would you see destination address translation occur in cases of inbound automatic static NAT?

- A. Static NAT does not adjust the destination IP
- B. Between the "i" and "I"
- C. Between the "I" and "o"
- D. Between the "o" and "O"

Answer: B

QUESTION 14

Which flag in the fw monitor command is used to print the position of the kernel chain?

- A. -all
- B. -k
- C. -c
- D. -p

Answer: D

QUESTION 15

Server A is subject to automatically static NAT and also resides on a network which is subject to automatic Hide NAT. With regards to address translation what will happen when Server A initiates outbound communication?

- A. This will cause a policy verification error.
- B. This is called hairpin NAT, the traffic will return to the server.
- C. The static NAT will take precedence.
- D. The Hide NAT will take precedence.

Answer: C

QUESTION 16

In your SecurePlatform configuration you need to set up a manual static NAT entry. After creating the proper NAT rule what step needs to be completed?

- A. Edit or create the file local.arp.
- B. No further actions are required.
- C. Edit or create the file discntd.if.
- D. Edit the file netconf.conf.

Answer: A

QUESTION 17

How do you set up Port Address Translation?

- A. Since Hide NAT changes to random high ports it is by definition PAT (Port Address Translation).
- B. Create a manual NAT rule and specify the source and destination ports.
- C. Edit the service in SmartDashboard, click on the NAT tab and specify the translated port.
- D. Port Address Translation is not support in Check Point environment.

Answer: B

QUESTION 18

You have set up a manual NAT rule, however fw monitor shows you that the device still uses the automatic Hide NAT rule. How should you correct this?

- A. Move your manual NAT rule above the automatic NAT rule.
- B. In Global Properties > NAT ensure that server side NAT is enabled.
- C. Set the following fwx_alloc_man kernel parameter to 1.
- D. In Global Properties > NAT ensure that Merge Automatic to Manual NAT is selected.

Answer: A

QUESTION 19

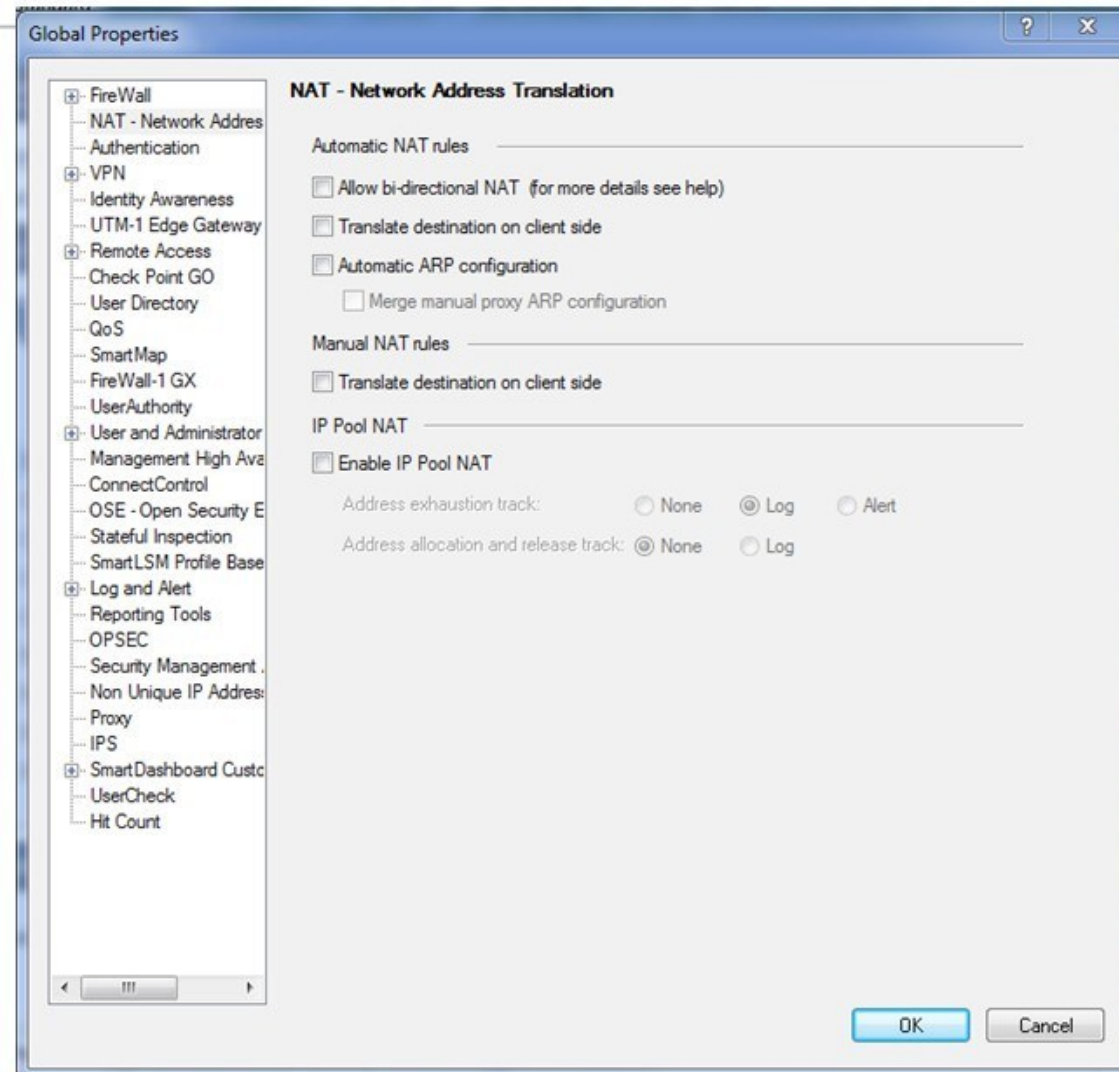
Since R76 GAiA, what is the method for configuring proxy ARP entries for manual NAT rules?

- A. WebUI or add proxy ARP ... commands via CLISH
- B. SmartView Tracker
- C. local.arp file
- D. SmartDashboard

Answer: A

QUESTION 20

Tom has a Web server for which he has created a manual NAT rule. The rule is not working. He tries to initiate a connection from the external network to a DMZ server using the public IP which the firewall translates to the actual IP of the server. He analyzes the captured packets using Wireshark and observes that the destination IP is being changed as required by the firewall but does not see the packet leave the internal interface. Which box in Global Properties should be checked?



- A. Automatic NAT rules > Allow bi-directional NAT
- B. Automatic NAT rules > Automatic ARP Configuration
- C. Automatic NAT rules > Translate destination on client side
- D. Manual NAT rules > Translate destination on client side

Answer: D

QUESTION 21

Tom is troubleshooting NAT issues using fw monitor and Wireshark. He tries to initiate a connection from the external network to a DMZ server using the public IP which the firewall translates to the actual IP of the server. He analyzes the captured packets using Wireshark and observes that the destination IP is being changed as required by the firewall but does not see the packet leave the external interface. What could be the reason?

- A. The translation might be happening on the client side and the packet is being routed by the OS back to the external interface.
- B. The translation might be happening on the server side and the packet is being routed by OS back to the external interface.
- C. Packet is dropped by the firewall.

D. After the translation, the packet is dropped by the Anti-Spoofing Protection.

Answer: B

QUESTION 22

Which FW-1 kernel flags should be used to properly debug and troubleshoot NAT issues?

- A. nat, route, conn, fwd, zeco, err
- B. nat, xlate, fwd, vm, ld, chain
- C. nat, xltrc, xlate, drop, conn, vm
- D. nat, drop, conn, xlate, filter, ioctl

Answer: C

QUESTION 23

Which file should be edited to modify ClusterXL VIP Hide NAT rules, and where?

- A. \$FWDIR/lib/base.def on the cluster members
- B. \$FWDIR/lib/table.def on the SMC
- C. \$FWDIR/lib/table.def on the cluster members
- D. \$FWDIR/lib/base.def on the SMC

Answer: B

QUESTION 24

When viewing a NAT Table, What represents the second hexadecimal number of the 6-tuple:

- A. Source port
- B. Protocol
- C. Source IP
- D. Destination port

Answer: C

QUESTION 25

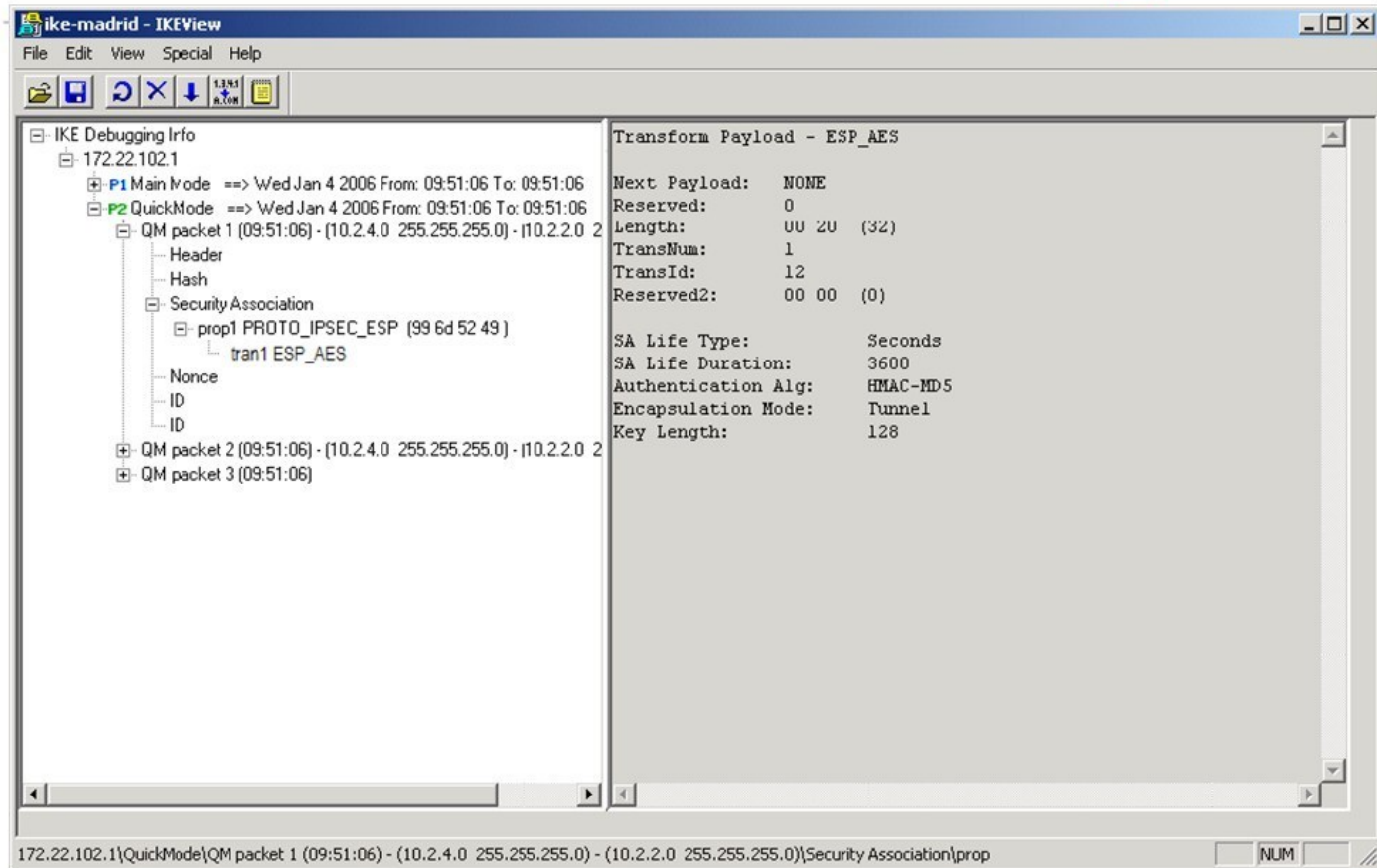
By default, the size of the fwx_alloc table is:

- A. 65535
- B. 65536
- C. 25000
- D. 1024

Answer: C

QUESTION 26

Given the screen configuration shown, the failure's probable cause is:



- A. Packet 1 Proposes SA life Type , Sa Life Duration, Authentication and Encapsulation Algorithm.
- B. Packet 1 proposes a symmetrical key.
- C. Packet 1 proposes a subnet and host ID, an encryption and hash algorithm.
- D. Packet 1 proposes either a subnet or host ID, an encryption and hash algorithm, and ID data.

Answer: D

QUESTION 27

Ann wants to hide FTP traffic behind the virtual IP of her cluster. Where is the relevant file table.def located to make this modification?

- A. \$FWDIR/log/table.def
- B. \$FWDIR/conf/table.def
- C. \$FWDIR/bin/table.def
- D. \$FWDIR/lib/table.def

Answer: D

QUESTION 28

While troubleshooting a connectivity issue with an internal web server, you know that packets are getting to the upstream router, but when you run a tcpdump on the external interface of the gateway, the only traffic you observe is ARP requests coming from the upstream router. Does the problem lie on the Check Point Gateway?

- A. Yes This could be due to a misconfigured route on the firewall.
- B. No This is a layer 2 connectivity issue and has nothing to do with the firewall.
- C. No The firewall is not dropping the traffic, therefore the problem does not lie with the firewall.

D. Yes This could be due to a misconfigured Static NAT in the firewall policy.

Answer: D

QUESTION 29

In a production environment, your gateway is configured to apply a Hide NAT for all internal traffic destined to the Internet. However, you are setting up a VPN tunnel with a remote gateway, and you are concerned about the encryption domain that you need to define on the remote gateway. Does the remote gateway need to include your production gateway's external IP in its encryption domain?

- A. No all packets destined through a VPN will leave with original source and destination packets without translation.
- B. No all packets destined to go through the VPN tunnel will have the payload encapsulated in an ESP packet and after decryption at the remote site, will have the same internal source and destination IP addresses.
- C. Yes all packets destined to go through the VPN tunnel will have the payload encapsulated in an ESP packet and after decryption at the remote site, the packet will contain the source IP of the Gateway because of Hide NAT.
- D. Yes The gateway will apply the Hide NAT for this VPN traffic.

Answer: B

QUESTION 30

The "Hide internal networks behind the Gateway's external IP" option is selected. What defines what traffic will be NATted?

- A. The Firewall policy of the gateway
- B. The network objects configured for the network
- C. The VPN encryption domain of the gateway object
- D. The topology configuration of the gateway object

Answer: D

QUESTION 31

With the default ClusterXL settings what will be the state of an active gateway upon using the command ClusterXL_admin up?

- A. Ready
- B. Down
- C. Standby
- D. Active

Answer: C

QUESTION 32

Which command should you use to stop kernel module debugging (excluding SecureXL)?

- A. fw ctl debug 0
- B. fw ctl zdebug - all
- C. fw debug fwd off; vpn debug off
- D. fw debug fwd off

Answer: A

QUESTION 33

Which command should you run to debug the VPN-1 kernel module?

- A. fw debug vpn on
- B. vpn debug on TDERROR_ALL_ALL=5
- C. fw ctl zdebug crypt kbuf

D. fw ctl debug -m VPN all

Answer: D

QUESTION 34

Which command can be used to see all active modules on the Security Gateway:

- A. fw ctl zdebug drop
- B. fw ctl debug -h
- C. fw ctl chain
- D. fw ctl debug -m

Answer: C

QUESTION 35

In some situations, switches may not play nicely with a Check Point Cluster and it is necessary to change from multicast to broadcast. What command should you invoke to correct the issue?

- A. set ccp broadcast
- B. cphaconf set_ccp broadcast
- C. cpha_conf set ccp broadcast
- D. This can only be changed via GuiDbEdit.

Answer: B

QUESTION 36

Which of the following commands shows the high watermark threshold for triggering the cluster under load mechanism in R77?

- A. fw ctl get int fwha_cul_mechanism_enable
- B. fw ctl get int fwha_cul_cluster_short_timeout
- C. fw ctl get int fwha_cul_member_cpu_load_limit
- D. fw ctl get int fwha_cul_policy_freeze_event_timeout_millise

Answer: C

QUESTION 37

What mechanism solves asymmetric routing issues in a load sharing cluster?

- A. Flush and ACK
- B. Stateful Inspection
- C. SYN Defender
- D. State Synchronization

Answer: A

QUESTION 38

When you have edited the local.arp configuration, to support a manual NAT, what must be done to ensure proxy arps for both manual and automatic NAT rules function?

- A. In Global Properties > NAT tree select Merge manual proxy ARP configuration check box
- B. Run the command fw ctl ARP a on the gateway
- C. In Global Properties > NAT tree select Translate on client side check box
- D. Create and run a script to forward changes to the local.arp tables of your gateway

Answer: A

QUESTION 39

Which command clears all the connection table entries on a Security Gateway?

- A. fw tab t connetion u
- B. fw ctl tab t connetions u
- C. fw tab t connetion -s
- D. fw tab t connections -x

Answer: D

QUESTION 40

How can you see a dropped connection and the cause from the kernel?

- A. fw zdebug drop
- B. fw ctl debug drop on
- C. fw debug drop on
- D. fw ctl zdebug drop

Answer: D

[Visit PassLeader and Download Full Version 156-115.77 Exam Dumps](#)