



**Vendor:** Check Point

**Exam Code:** 156-115.77

**Exam Name:** Check Point Certified Security Maste

**Version:** DEMO

### 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 260 bytes
[FWM 4929 2012145344]@standalone[4 Aug 11:10:56] cpsec_send_sset: session=0x0b589f18, id=2, last=1, set=
(userc2
```

©2014 Check Point Software Technologies Ltd. 2

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?

©2014 CheckPoint Software Technologies Ltd. 3

- A. loglist
- B. tablist
- C. fw\_x\_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 are trying to troubleshoot a NAT issue on your network, and you use a kernel debug to verify a connection is correctly translated to its NAT address. What flags should you use for the kernel debug?

- A. fw ctl debug -m fw + conn drop nat vm xlate xltrc
- B. fw ctl debug -m fw + conn drop ld
- C. fw ctl debug -m nat + conn drop nat xlate xltrc
- D. fw ctl debug -m nat + conn drop fw xlate xltrc

**Answer: A**

#### QUESTION 10

Since switching your network to ISP redundancy you find that your outgoing static NAT connections are failing. You use the command \_\_\_\_\_ to debug the issue.

- A. fwaccel stats misp
- B. fw ctl pstat
- C. fw ctl debug -m fw + nat drop
- D. fw tab -t fw\_x\_alloc -x

**Answer: C**

**QUESTION 11**

Remote VPN clients can initiate connections with internal hosts, but internal hosts are unable to initiate connections with the remote VPN clients, even though the policy is configured to allow it. You think that this is caused by NAT. What command can you run to see if NAT is occurring on a packet?

- A. fw tab -t fw\_x\_alloc -x
- B. fw ctl pstat
- C. fwaccel stats misp
- D. fw ctl debug -m fw + conn drop packet xlate xltrc nat

**Answer: D**

**QUESTION 12**

Where in a fw monitor output would you see source address translation occur in cases of automatic Hide NAT?

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

**Answer: C**

**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**

## Thank You for Trying Our Product

### Braindump2go Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives<sup>®</sup>

**10% Discount Coupon Code: BDN2014**