

Checkpoint

Exam 156-115.77

Check Point Certified Security Master

Version: 6.1

[Total Questions: 295]

Topic break down

Topic	No. of Questions
Topic 1: Chain Modules	28
Topic 2: NAT	25
Topic 3: ClusterXL	35
Topic 4: VPN Troubleshooting	27
Topic 5: SecureXL Acceleration debugging	24
Topic 6: Hardware Optimization	33
Topic 7: Software Tuning	16
Topic 8: Enable CoreXL	16
Topic 9: IPS	30
Topic 10: IPV6	15
Topic 11: Advanced VPN	46

Topic 1, Chain Modules**Question No : 1 - (Topic 1)**

You are running a debugging session and you have set the debug environment to TDERROR_ALL_ALL=5 using the command export TDERROR_ALL_ALL=5. How do you return the debug value to defaults?

- A. fw ctl debug 0x1ffffe0
- B. fw debug 0x1ffffe0
- C. export TDERROR_ALL_ALL
- D. unset TDERROR_ALL_ALL

Answer: D

Question No : 2 - (Topic 1)

The command that lists the firewall kernel modules on a Security Gateway is:

- A. fw list kernel modules
- B. fw ctl kernel chain
- C. fw ctl debug -m
- D. fw list modules

Answer: C

Question No : 3 - (Topic 1)

When finished running a debug on the Management Server using the command fw debug fwm on how do you turn this debug off?

- A. fwm debug off
- B. fw ctl debug off
- C. fw debug off
- D. fw debug fwm off

Answer: D

Question No : 4 - (Topic 1)

What command would you use to view which debugs are set in your current working environment?

- A. "env" and "fw ctl debug"
- B. "cat /proc/etc"
- C. "fw ctl debug all"
- D. "export"

Answer: A

Question No : 5 - (Topic 1)

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

```

fwm 3503 1951651808@manager [2 Aug 23:03:17] fwasync_conn_get: get max buffer size (1048576)
fwm 3503 1951651808@manager [2 Aug 23:03:17] sic_server_set_sic_type_str: 01 security type is cpml
fwm 3503 1951651808@manager [2 Aug 23:03:17] policy_query: src : cn=cp_mgmt, o=srvmgmt, f2kd31 dst : CN=Gui_client
fwm 3503 1951651808@manager [2 Aug 23:03:17] gui_connection_sic_plugins: gui client sic name on connection 01.
fwm 3503 1951651808@manager [2 Aug 23:03:17] call_handlers_list: conversion success.
fwm 3503 1951651808@manager [2 Aug 23:03:17] pm_session_init: given session I(cn=cp_mgmt, o=srvmgmt, f2kd31; IP=192.168.220.113, CN=Gui_client; 18190; cpml).
fwm 3503 1951651808@manager [2 Aug 23:03:17] pm_policy_query: input session I(cn=cp_mgmt, o=srvmgmt, f2kd31; IP=192.168.220.113, CN=Gui_client; 18190; cpml).
fwm 3503 1951651808@manager [2 Aug 23:03:17] fwnetobj_getbysicname: table_chosen_get_with_param(eTABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113, CN=Gui_client)
returned NULL.
fwm 3503 1951651808@manager [2 Aug 23:03:17] fwnetobj_getbysicname: table_chosen_get_with_param(eTABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113, CN=Gui_client)
returned NULL.
fwm 3503 1951651808@manager [2 Aug 23:03:17] fwnetobj_getbysicname: table_chosen_get_with_param(eTABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113, CN=Gui_client)
returned NULL.
fwm 3503 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'
returned NULL.
fwm 3503 1951651808@manager [2 Aug 23:03:17] fwnetobj_getbysicname: table_chosen_get_with_param(eTABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113, CN=Gui_client)
returned NULL.
fwm 3503 1951651808@manager [2 Aug 23:03:17] fwnetobj_getbysicname: table_chosen_get_with_param(eTABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113, CN=Gui_client)
returned NULL.
fwm 3503 1951651808@manager [2 Aug 23:03:17] fwnetobj_getbysicname: table_chosen_get_with_param(eTABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113, CN=Gui_client)
returned NULL.
fwm 3503 1951651808@manager [2 Aug 23:03:17] fwnetobj_getbysicname: table_chosen_get_with_param(eTABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113, CN=Gui_client)
returned NULL.
Login failed: 192.168.220.113 is not allowed for remote login
Sun Aug 3 02:03:17 2014 (GMT): reject client IP=192.168.220.113,CN=Gui_client
fwm 3503 1951651808@manager [2 Aug 23:03:17] fwnetobj_getbysicname: table_chosen_get_with_param(eTABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113, CN=Gui_client)
returned NULL.
fwm 3503 1951651808@manager [2 Aug 23:03:17] fwnetobj_getbysicname: table_chosen_get_with_param(eTABLE_NETWORK_OBJECTS, is_obj_sic_name, IP=192.168.220.113, CN=Gui_client)
returned NULL.
fwm 3503 1951651808@manager [2 Aug 23:03:17] pm_policy_query: rule not found.
fwm 3503 1951651808@manager [2 Aug 23:03:17] pm_policy_query: finished successfully, 1st method = deny
fwm 3503 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 No : 6 - (Topic 1)

What does the IP Options Strip represent under the fw chain output?

- A. IP Options Strip is not a valid fw chain output.

- B. The IP Options Strip removes the IP header of the packet prior to be passed to the other kernel functions.
- C. The IP Options Strip copies the header details to forward the details for further IPS inspections.
- D. IP Options Strip is only used when VPN is involved.

Answer: B

Question No : 7 - (Topic 1)

What command would give you a summary of all the tables available to the firewall kernel?

- A. fw tab
- B. fw tab -s
- C. fw tab -h
- D. fw tab -o

Answer: B

Question No : 8 - (Topic 1)

What command would you use for a packet capture on an absolute position for TCP streaming (out) 1ffffe0

- A. fw ctl chain -po 1ffffe0 -o monitor.out
- B. fw monitor -po -0x1ffffe0 -o monitor.out
- C. fw monitor -e 0x1ffffe0 -o monitor.out
- D. fw monitor -pr 1ffffe0 -o monitor.out

Answer: B

Question No : 9 - (Topic 1)

The command fw ctl kdebug <params> is used to:

- A. list enabled debug parameters.
- B. read the kernel debug buffer to obtain debug messages.
- C. enable kernel debugging.
- D. select specific kernel modules for debugging.

Answer: B

Question No : 10 - (Topic 1)

True or False: Software blades perform their inspection primarily through the kernel chain modules.

- A. False. Software blades do not pass through the chain modules.
- B. True. Many software blades have their own dedicated kernel chain module for inspection.
- C. True. All software blades are inspected by the IP Options chain module.
- D. True. Most software blades are inspected by the TCP streaming or Passive Streaming chain module.

Answer: B

Question No : 11 - (Topic 1)

Which of the following items is NOT part of the columns of the chain modules?

- A. Inbound/Outbound chain
- B. Function Pointer
- C. Chain position
- D. Module location

Answer: A

Question No : 12 - (Topic 1)

What causes the SIP Early NAT chain module to appear in the chain?

- A. The SIP traffic is trying to pass through the firewall.
- B. SIP is configured in IPS.
- C. A VOIP domain is configured.
- D. The default SIP service is used in the Rule Base.

Answer: D

Question No : 13 - (Topic 1)

For URL Filtering in the Cloud in R75 and above, what table is used to contain the URL Filtering cache values?

- A. urlf_blade_on_gw
- B. urlf_cache_tbl
- C. urlf_cache_table
- D. url_scheme_tab

Answer: C

Question No : 14 - (Topic 1)

Which process should you debug when SmartDashboard authentication is rejected?

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

Answer: A

Question No : 15 - (Topic 1)

Compare these two images to establish which blade/feature was disabled on the firewall.



Before

```
[Expert@fw1:0]# fw ctl chain
in chain (16):
0: -7f800000 (c26a9c70) (ffffffff) IP Options Strip (in) (ipopt_strip)
1: - 20000000 (c183b020) (00000003) vpn decrypt (vps)
2: - 1fffff8 (c184e080) (00000001) l2tp inbound (l2tp)
3: - 1fffff6 (c26ab420) (00000001) Stateless verifications (in) (asm)
4: - 1fffff2 (c1862a60) (00000003) vpn tagging inbound (tagging)
5: - 1fffff0 (c1838700) (00000003) vpn decrypt verify (vpn_ver)
6: - 10000000 (c2728940) (00000003) SecureXL conn sync (secxl_sync)
7: 0 (c2654220) (00000001) fw VM inbound (fw)
8: 1 (c26cb2b0) (00000002) wire VM inbound (wire_vm)
9: 20000000 (c1839b90) (00000003) vpn policy inbound (vpn_pol)
10: 10000000 (c272e640) (00000003) SecureXL inbound (secxl)
11: 7f600000 (c269f2b0) (00000003) fw SCV inbound (scv)
12: 7f730000 (c2835210) (00000001) passive streaming (in) (pass_str)
13: 7f750000 (c2a2b3f0) (00000001) TCP streaming (in) (cpas)
14: 7f800000 (c26aa010) (ffffffff) IP Options Restore (in) (ipopt_res)
15: 7fb00000 (c2db29f0) (00000001) HA Forwarding (ha_for)
out chain (14):
0: -7f800000 (c26a9c70) (ffffffff) IP Options Strip (out) (ipopt_strip)
1: - 1fffff8 (c1837fc0) (00000003) vpn nat outbound (vpn_nat)
2: - 1fffff0 (c2a2b270) (00000001) TCP streaming (out) (cpas)
3: - 1fffff5 (c2835210) (00000001) passive streaming (out) (pass_str)
4: - 1ff00000 (c1862a60) (00000003) vpn tagging outbound (tagging)
5: - 1f000000 (c26ab420) (00000001) Stateless verifications (out) (asm)
6: 0 (c2654220) (00000001) fw VM outbound (fw)
7: 1 (c26cb2b0) (00000002) wire VM outbound (wire_vm)
8: 20000000 (c1838e10) (00000003) vpn policy outbound (vpn_pol)
9: 10000000 (c272e640) (00000003) SecureXL outbound (secxl)
10: 1fffff0 (c1846c30) (00000003) l2tp outbound (l2tp)
11: 20000000 (c183ba60) (00000003) vpn encrypt (vpn)
12: 7f700000 (c2a2d840) (00000001) TCP streaming post VM (cpas)
13: 7f800000 (c26aa010) (ffffffff) IP Options Restore (out) (ipopt_res)
```

After

```
[Expert@fw1:0]# fw ctl chain
in chain (11):
0: -7f800000 (c26a9c70) (ffffffff) IP Options Strip (in) (ipopt_strip)
1: - 1fffff6 (c26ab420) (00000001) Stateless verifications (in) (asm)
2: - 10000000 (c2728940) (00000003) SecureXL conn sync (secxl_sync)
3: 0 (c2654220) (00000001) fw VM inbound (fw)
4: 1 (c26cb2b0) (00000002) wire VM inbound (wire_vm)
5: 10000000 (c272e640) (00000003) SecureXL inbound (secxl)
6: 7f600000 (c269f2b0) (00000001) fw SCV inbound (scv)
7: 7f730000 (c2835210) (00000001) passive streaming (in) (pass_str)
8: 7f750000 (c2a2b3f0) (00000001) TCP streaming (in) (cpas)
9: 7f800000 (c26aa010) (ffffffff) IP Options Restore (in) (ipopt_res)
10: 7fb00000 (c2db29f0) (00000001) HA Forwarding (ha_for)
out chain (9):
0: -7f800000 (c26a9c70) (ffffffff) IP Options Strip (out) (ipopt_strip)
1: - 1fffff0 (c2a2b270) (00000001) TCP streaming (out) (cpas)
2: - 1fffff5 (c2835210) (00000001) passive streaming (out) (pass_str)
3: - 1f000000 (c26ab420) (00000001) Stateless verifications (out) (asm)
4: 0 (c2654220) (00000001) fw VM outbound (fw)
5: 1 (c26cb2b0) (00000002) wire VM outbound (wire_vm)
6: 10000000 (c272e640) (00000003) SecureXL outbound (secxl)
7: 7f700000 (c2a2d840) (00000001) TCP streaming post VM (cpas)
8: 7f800000 (c26aa010) (ffffffff) IP Options Restore (out) (ipopt_res)
```

- A. IPS
- B. VPN
- C. NAT
- D. L2TP

Answer: B

Question No : 16 - (Topic 1)

John is a Security Administrator of a Check Point platform. He has a mis-configuration issue that points to the Rule Base. To obtain information about the issue, John runs the command:

- A. fw debug fw on and checks the file fwm.elg.
- B. fw kdebug fwm on and checks the file fwm.elg.
- C. fw debug fwm on and checks the file fwm.elg.
- D. fw kdebug fwm on and checks the file fw.elg.

Answer: C

Question No : 17 - (Topic 1)

When using the command fw monitor, what command ensures the capture is accurate?

- A. export TDERROR_ALL_ALL=5
- B. fwaccel off
- C. fwaccel on
- D. fw accel off

Answer: B

Explanation:

C102 - Chain Modules

Question No : 18 - (Topic 1)

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 No : 19 - (Topic 1)

Which commands will properly set the debug level to maximum and then run a policy install in debug mode for the policy Standard on gateway A-GW from an R77 GAIa Management Server?

- A. setenv TDERROR_ALL_ALL=5fwm -d load A-GW Standard
- B. setenv TDERROR_ALL_ALL=5fwm -d load Standard A-GW
- C. export TDERROR_ALL_ALL=5fwm -d load Standard A-GW
- D. export TDERROR_ALL_ALL=5fwm -d load A-GW Standard

Answer: C

Question No : 20 - (Topic 1)

The command _____ shows which firewall chain modules are active on a gateway.

- A. fw stat
- B. fw ctl debug
- C. fw ctl chain
- D. fw ctl multik stat

Answer: C

Question No : 21 - (Topic 1)

The command fw monitor -p all displays what type of information?

- A. It captures all points of the chain as the packet goes through the firewall kernel.
- B. This is not a valid command.

- C. The -p is used to resolve MAC address in the firewall capture.
- D. It does a firewall monitor capture on all interfaces.

Answer: A

Question No : 22 - (Topic 1)

Which directory below contains the URL Filtering engine update info? Here you can also go to see the status of the URL Filtering and Application Control updates.

- A. \$FWDIR/urlf/update
- B. \$FWDIR/appi/update
- C. \$FWDIR/appi/urlf
- D. \$FWDIR/update/appi

Answer: B

Question No : 23 - (Topic 1)

When you perform an install database, the status window is filled with large amounts of text. What could be the cause?

- A. There is an active fw monitor running.
- B. There is an environment variable of TDERROR_ALL_ALL set on the gateway.
- C. There is an active debug on the SmartConsole.
- D. There is an active debug on the FWM process.

Answer: D

Question No : 24 - (Topic 1)

Which of the following BEST describes the command fw ctl chain function?

- A. View how CoreXL is distributing traffic among the firewall kernel instances.
- B. View established connections in the connections table.
- C. View the inbound and outbound kernel modules and the order in which they are applied.
- D. Determine if VPN Security Associations are being established.

Answer: C