

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	24
debugging	
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)



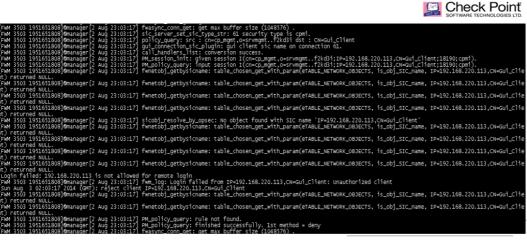
What command would you use to view which debugs are set in your current working environment?

- 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?



©2014 Check Point Software Technologies Ltd.

- 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

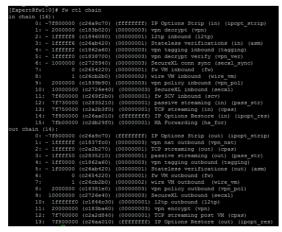
Answer: A

Question No: 15 - (Topic 1)

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



Before



After

[Expert@fw1:0] # fw o	tl chain		
in chain (11):			
0: -7f800000	(c26a9c70)	(ffffffff)	IP Options Strip (in) (ipopt_strip)
1: - 1ffffff6	(c26ab420)	(00000001)	Stateless verifications (in) (asm)
2: - 1000000	(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	(c2726e40)	(00000003)	SecureXL inbound (secx1)
6: 7f600000	(c269f2b0)	(00000001)	fw SCV inbound (scv)
7: 7f730000	(c2835210)	(00000001)	passive streaming (in) (pass_str)
			TCP streaming (in) (cpas)
9: 7f800000	(c26aa010)	(ffffffff)	IP Options Restore (in) (ipopt_res)
10: 7fb0000	0 (c2db29f0)	(00000001) HA Forwarding (ha_for)
out chain (9):			
0: -7f800000	(c26a9c70)	(ffffffff)	IP Options Strip (out) (ipopt_strip)
1: - 1ffffff0	(c2a2b270)	(00000001)	TCP streaming (out) (cpas)
2: - 1ffff50	(c2835210)	(00000001)	passive streaming (out) (pass_str)
3: - 1f00000	(c26ab420)	(00000001)	Stateless verifications (out) (asm)
			fw VM outbound (fw)
			wire VM outbound (wire_vm)
			SecureXL outbound (secx1)
			TCP streaming post VM (cpas)
8: 7f800000	(c26aa010)	(ffffffff)	IP Options Restore (out) (ipopt_res)

©2014 Check Point Software Technologies Ltd.



- 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:

C1O2 - 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)
QUOULIOII	110 . 20	(IOPIOI)

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