Question #1 *Topic 1*

Check Point's self-service knowledge base of technical documents and tools covers everything from articles describing how to fix specific issues, understand error messages and to how to plan and perform product installation and upgrades. This knowledge base is called:

A. SupportCenterBase

B. SecureDocs

C. SupportDocs

D. SecureKnowledge

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

What is the most efficient way to view large fw monitor captures and run filters on the file?

A. snoop

B. CLI

C. CLISH

D. wireshark

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

What is a primary advantage of using the fw monitor tool?

A. It is menu-driven, making it easy to configure

B. It can capture packets in various positions as they move through the firewall

C. It has no negative impact on firewall performance

D. It always captures all packets hitting the physical layer

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

The Check Point FW Monitor tool captures and analyzes incoming packets at multiple points in the traffic inspections. Which of the following is the correct inspection flow for traffic?

A. (i) – pre-inbound, (I) – post-inbound, (o) – pre-outbound, (O) – post-outbound

B. (o) – pre-outbound, (O) – post-inbound, (i) – pre-inbound, (I) – post-inbound

C. (O) – post-outbound, (o) – pre-outbound, (I) – post-inbound, (i) – pre-inbound

D. (I) – pre-inbound, (i) – post-inbound, (O) – pre-outbound, (o) – post-outbound

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Application Control and URL Filtering update files are located in which directory?

A. $CPDIR/appi/update

B. $FWDIR/conf/update

C. $CPDIR/apci/update

D. $FWDIR/appi/update/

Suggested Answer: *D*

Community vote distribution

D (100%)

theindian435 1 month, 2 weeks ago

Selected Answer: D

In CCTA R81.20, page 253, 254

upvoted 2 times

shatterthesilence 2 months, 4 weeks ago

Selected Answer: D

$FWDIR/appi/update/ exists but $CPDIR/appi/update does not

[Expert@gateway:0]# cd $CPDIR/appi/update
-bash: cd: /opt/CPshrd-R81.20/appi/update: No such file or directory
[Expert@gateway:0]# cd $FWDIR/appi/update/
[Expert@gateway:0]# pwd
/opt/CPsuite-R81.20/fw1/appi/update

upvoted 4 times

Question #6 *Topic 1*

As a security administrator/engineer in your company, you have noticed that your HQ Check Point Security Management Server is not receiving logs from your HQ Check Point Gateway/Cluster. To investigate this issue in the command line, you will need to verify which process is running?

A. cpm

B. cpd

C. fwd

D. fwm

Suggested Answer: *C*

Community vote distribution

C (100%)

theindian435 1 month, 2 weeks ago

Selected Answer: C

https://support.checkpoint.com/results/sk/sk97638

upvoted 2 times

Edyspbrazil 2 months, 1 week ago

Selected Answer: C

C is correct. FWD (Firewall Daemon):

Primarily responsible for forwarding logs from Security Gateways to the Security Management Server (SMS) and for certain kernel control commands.

On the gateway, it also acts as a parent process for other security server processes.

upvoted 3 times

Question #7 *Topic 1*

What is the default protection profile for Autonomous Threat Prevention?

A. Perimeter

B. Guest

C. Internal

D. Bypass

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which of the following CLI commands is best to use for getting a quick look at appliance performance Information in Gaia?

A. fw stat

B. fw monitor

C. cpview

D. cphaprob stat

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Running tcpdump causes a significant increase on CPU usage, what other option you should use?

A. fw monitor

B. Wait for out of business hours to do a packet capture

C. cppcap

D. You need to use tcpdump with -e option to decrease the length of packet in captures and it will utilize the less CPU

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

To verify that communication is working between the Security Management Server and the Security Gateway, which service port should be checked?

A. 257

B. 259

C. 18209

D. 19009

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

You were asked to setup a logging for a rule to log a full list of URLs when the rule hits in the Rule Base. How do you accomplish that?

A. Set Extended logging under rule log type

B. Click on the rule, column logging and set "log URL" under application control blade layer

C. All URLs are logged by default

D. For URL logging you need to modify blade settings of URL filtering blade under SmartConsole, Manage&Settings, blades, URL filtering

Suggested Answer: *A*

Community vote distribution

A (100%)

theindian435 1 month, 2 weeks ago

Selected Answer: A

CCTA R81.20, p247: Extended Log : Extended Log provides the same information as the Detailed Log option but also shows a full list of UR Ls and files in the connection or the session. The UR Ls and files show in the lower pane of the Logs view.

upvoted 2 times

freemen810 1 month, 3 weeks ago

Selected Answer: A

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Working-with-logs.htm

upvoted 3 times

Jimbob_101 1 month, 3 weeks ago

Selected Answer: A

From the study guide "Extended Log shows a full list of URLs and files in the connection or the session....."

upvoted 3 times

Question #12 *Topic 1*

How would you check the connection status of a gateway to the Log server?

A. run netstat -anp | grep :257 in CLISH on Log server

B. run netstat -anp | grep :257 in expert mode on Log server

C. run netstat -anp | grep :18187 in expert mode on Log server

D. run netstat -anp | grep :18187 in CLISH on Log server

Suggested Answer: *B*

Community vote distribution

B (100%)

theindian435 1 month, 2 weeks ago

Selected Answer: B

| is not working in clish shell. Correct answer is in Expert

upvoted 1 times

freemen810 1 month, 3 weeks ago

Selected Answer: B

https://support.checkpoint.com/results/sk/sk17745 stated that

FWD_LOG (TCP port 257) is enabled from all Security Gateways to all Security Management Servers.

upvoted 1 times

Jimbob_101 1 month, 3 weeks ago

Selected Answer: B

Expert #netstat -anp | grep :257

upvoted 1 times

Question #13 *Topic 1*

Services with expired licenses and contracts have _____.

A. full functionality for 90 days after they expire

B. full functionality for 45 days after they expire

C. no functionality

D. limited functionality

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

What does the FWD daemon instruct the gateway to do when communication issues between the gateway and SMS/Log Server occurs?

A. It instructs the gateway to continue forwarding logs to SMS/Log Server and the logs with be stored in a holding queue for the server until communication is restored.

B. It instructs the gateway to stop logging until it can restore communication.

C. It instructs the gateway to store logs locally as it continues to try to restore communication.

D. It instructs the gateway to only log a specified number of logs as defined in the Security Policy.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

UserCenter/PartnerMAP access is based on what criteria?

A. The certification level achieved by employees of an organization.

B. User permissions assigned to company contacts.

C. The certification level achieved by the partner.

D. The level of Support purchased by a company manager.

Suggested Answer: *B*

Community vote distribution

B (100%)

theindian435 1 month, 2 weeks ago

Selected Answer: B

CCTA R81.20, p40 - Account Classifications

upvoted 1 times

Jimbob_101 1 month, 3 weeks ago

Selected Answer: B

Access to Check Point's UserCenter and PartnerMAP is primarily determined by the user permissions assigned to company contacts

upvoted 2 times

shatterthesilence 2 months, 4 weeks ago

Selected Answer: B

user center admins control permissions to company contacts to licenser/viewer

upvoted 2 times

Question #16 *Topic 1*

The URL filtering cache limit exceeded. What issues this can cause?

A. When URL filtering cache exceed the limit, it will be disabled temporary to overcome instability of the system

B. RAD process will spawn multiple times to help populate the cache

C. Resource Advisor (RAD) process on the Security Gateway consumes close to 100 percent of the CPU

D. Nothing, the Security Gateway dynamically raise the cache when needed

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

You want to work with a license for your gateway in User Center portal, but all options are greyed out. What is the reason?

A. Your account has classification permission to Viewer

B. Your account has classification permission to Licenser

C. You are not defined as Support Contact

D. Your account does not have any rights

Suggested Answer: *C*

Community vote distribution

A (100%)

theindian435 1 month, 2 weeks ago

Selected Answer: A

CCTA R81.20, page 40

View the products and other users attached to the account: Administrator, Licenser and Viewer
Make changes to licensed products for the account: Administrator, Licenser, but NOT Viewer
Add and remove user and product moves: Administrator, but NOT Licenser and NOT Viewer
Only Support Contact is also not enough to manage licences
also tried through UserCenter

upvoted 4 times

Question #18 *Topic 1*

After manipulating the rulebase and objects with SmartConsole the application crashes and closes immediately. To troubleshoot you will need to review the crash report. In which directory on the host PC will you find this report?

A. <SmartFirewall Directory>\data\crash_report\

B. <SmartConsole Directory>\data\crash_report\

C. <FW1 Directory>\data\crash_report

D. <SmartConsole Directory>\crash_report\data\

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

What are the available types of licenses in Check Point?

A. Evaluation. Perpetual, Trial, Subscription

B. Evaluation, Perpetual, Test, Free

C. Free, Evaluation, Annual, Lifetime

D. Annual, Perpetual, Test, Free

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Customer wants to use autonomous threat prevention. How do you enable it?

A. Enable Autonomous threat prevention on the Security Gateway from the SmartConsole: Gateway and Servers view and enable IPS on the Security Gateway by the command: ips on.

B. Enable Autonomous threat prevention on the Security Gateway from the SmartConsole: Gateway and Servers view, the default profile Strict Security will be selected.

C. Enable Autonomous threat prevention on the Security Gateway from the SmartConsole: Gateway and Servers view, inspection profile is not needed, the Security Gateway will automatically select the best profile according to deployment.

D. Enable Autonomous threat prevention on the Security Gateway from the SmartConsole: Gateway and Servers view, then select inspection profile.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

When managing the disk space for locally stored logs, the Delete threshold for the gateway cannot be more than what percentage of the total disk space?

A. 10%

B. 25%

C. 50%

D. 75%

Suggested Answer: *B*

Community vote distribution

B (100%)

theindian435 1 month, 2 weeks ago

Selected Answer: B

CCTA R81.20, p 201 Important! The delete threshold cannot be more than 25 percent of the disk. Automatically delete logs if less then 12GB are available. It is recommended to delete the old files when disk space is below 15-20 percent.

upvoted 1 times

Jimbob_101 1 month, 3 weeks ago

Selected Answer: B

B is correct - sk98126

upvoted 1 times

Question #22 *Topic 1*

What is the process of intercepting and logging traffic?

A. Debugging

B. Forensics Analysis

C. Logging

D. Packet Capturing

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

For Threat Prevention, which process is enabled when the Policy Conversion process has debug turned on using the INTERNAL_POLICY_LOADING=1 command?

A. fwm

B. cpm

C. solr

D. dlpd

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Which of the following files Is commonly associated with troubleshooting crashes on a system such as SmartConsole?

A. CPMIL dump

B. fw monitor

C. crash dump

D. tcpdump

Suggested Answer: *C*

Community vote distribution

C (100%)

Sai_Vignesh 5 hours, 58 minutes ago

Selected Answer: C

Ruled out the other options because they don't meet the primary requirement. That leaves C.

upvoted 1 times

Question #25 *Topic 1*

After deploying a Hide NAT for a new network, users are unable to access the Internet. What command would you use to check the internal NAT behavior?

A. cp ctl kdebug + xlate xltrc nat

B. fw ctl zdebug + xlate xltrc nat

C. cp ctl zdebug + xlate xltrc nat

D. fw ctl kdebug + xlate xltrc nat

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

You want to print the status of WatchDog-monitored processes. What command best meets your needs?

A. cpwd_admin list

B. tcpdump

C. cppcap

D. cplic print

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Is it possible to analyze ICMP packets with tcpdump?

A. Yes, tcpdump is not limited to tcp specific issues

B. No, use fw monitor instead

C. No, tcpdump works from layer 4. ICMP is located in the network layer (layer 3), therefore is not applicable to this scenario

D. No, since ICMP does not have any source or destination ports, but specification of port numbers is mandatory

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

Which of the following System Monitoring Commands (Linux) shows process resource utilization, as well as CPU and memory utilization?

A. df

B. free

C. ps

D. top

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

In the Security Management Architecture, what port and process SmartConsole uses to communicate with the management server?

A. CPM 19009 and 18191

B. CPM and 18190

C. CPM and 19009

D. FWM and 19009

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

You need to verify the license on Security Gateway. What command you can use from the command line?

A. cplic -l

B. cplic print

C. cplic list

D. sh lic stat

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

Running tcpdump causes a significant increase on CPU usage, what other option you should use?

A. o

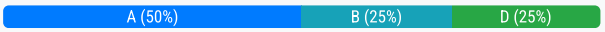
B. O

C. I

D. i

Suggested Answer: *A*

Community vote distribution



theindian435 1 month, 1 week ago

Selected Answer: D

I revised my first post. The correct answer may be D (for -i) to specify a specific interface to limit capture.

upvoted 1 times

theindian435 1 month, 2 weeks ago

Selected Answer: A

WRONG QUESTIONS Also agree and must be cppcap

upvoted 1 times

freemen810 1 month, 3 weeks ago

Selected Answer: B

-o is not valid syntax

upvoted 1 times

Jimbob_101 1 month, 3 weeks ago

Selected Answer: A

None of the above. The answer is cppcap.

upvoted 1 times

Question #32 *Topic 1*

When accessing License Status in Smart Console, what information is available?

A. Blade Name, License Status, Expiration Date, Additional info

B. Expiration Date, Status, SKU, Signature Key

C. Blade Name, Expiration Date, Attached to, Status

D. License Status, Blade Name, Report available, Download

Suggested Answer: *A*

Community vote distribution

A (100%)

theindian435 1 month, 2 weeks ago

Selected Answer: A

CCTA R81.20, LAB 9, p381

upvoted 2 times

Jimbob_101 1 month, 3 weeks ago

Selected Answer: A

Answer is A. I checked in the lab.

upvoted 1 times

Question #33 *Topic 1*

Which command shows the installed licenses and contracts on a Check Point device?

A. cplicenses print -x

B. cplic print -s

C. fwlic print -x

D. cplic print -x

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

You need to capture NAT information into packet capture, what tool is the best suitable for this task?

A. tcpdump

B. fw monitor

C. cppcap

D. fw ctl zdebug + xlate xltrc nat

Suggested Answer: *B*

Community vote distribution

B (100%)

Jimbob_101 1 month, 3 weeks ago

Selected Answer: B

fw monitor shows the NAT taking place and can be viewed in wireshark

upvoted 3 times

Question #35 *Topic 1*

What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

A. .pea

B. .exe

C. .cap

D. .tgz

Suggested Answer: *C*

Community vote distribution

C (100%)

Jimbob_101 1 month, 3 weeks ago

Selected Answer: C

Answer options are wrong, although C is the closest. The answer is .pcap for Wireshark.

upvoted 2 times

Question #36 *Topic 1*

Where can a Check Point customer find information about product licenses they own, download product manuals and get information about product support expiration?

A. Smart Console

B. PartnerMAP portal

C. UserCenter portal

D. In security management server via CLI and executing command cplic print

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

What is the difference between the “Super User” and “Read Write All” SmartConsole permission profiles?

A. “Read Write All” has the extra ability to make changes within the Gaia operating system

B. “Super User” has the extra ability to administer other administrative accounts

C. “Super User” has the extra ability to make changes within the Gaia operating system

D. “Super User” had the extra ability of being able to use the Management API

Suggested Answer: *B*

Community vote distribution

B (100%)

theindian435 1 month, 2 weeks ago

Selected Answer: B

CCTA R81.20, page 224

Super User = Full Read and Write permissions. Has extra ability to administer other administrative accounts.

Read Write All = Full Read and Write permissions.

upvoted 2 times