Question #1 *Topic 1*

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

A. CPM and 18190

B. FWM and 19009

C. CPM and 19009

D. CPM 19009 and 18191

Suggested Answer: *C*

Community vote distribution

C (100%)

Sartarus 1 week, 4 days ago

Selected Answer: C

C is correct

upvoted 1 times

edwardT3ach 1 month ago

Selected Answer: C

CPM process and Port 19009 used for remote communication with SmartConsole

CCTE R81.20 textbook pg 100

upvoted 1 times

keikei1228 2 months ago

Selected Answer: C

The correct answer is:

C. CPM and 19009

- SmartConsole connects to the CPM (Check Point Management) process on the Security Management Server.
- The communication occurs over TCP port 19009.

upvoted 1 times

Question #2 *Topic 1*

The Check Point Watch Daemon (CPWD) monitors critical Check Point processes, terminating them or restarting them as needed to maintain consistent, stable operating conditions. When checking the status/output of CPWD you are able to see some columns like APP, PID, STAT, START, etc. What is the column “STAT” used for?

A. Shows the status of the monitored process

B. Shows how many times the WatchDog started the monitored process

C. Shows the WatchDog name of the monitored process

D. Shows what monitoring method WatchDog is using to track the process

Suggested Answer: *A*

Community vote distribution

A (100%)

⊟ **Sartarus** 1 week, 4 days ago

Selected Answer: A

A is correct

upvoted 1 times

⊟ **edwardT3ach** 1 month ago

Selected Answer: A

Ans is A

CCTE textbook R81.20 pg 153

upvoted 1 times

Question #3 *Topic 1*

Which of the following commands can be used to see the list of processes monitored by the Watch Dog process?

A. cpstat fw -f watchdog

B. fw ctl get str watchdog

C. cpwd_admin list

D. ps -ef | grep watchd

Suggested Answer: *C*

Community vote distribution

C (100%)

Sartarus 1 week, 4 days ago

Selected Answer: C

C is correct

upvoted 1 times

Question #4 *Topic 1*

You run cpwd_admin list on a Security Gateway and notice that the CPM process is not listed. Select best answer?

A. The output is different between gateway and Management server.

B. CPM is not running and can’t be monitored by watch dog.

C. If you want to monitor CPM you have to manually add it to watch dog.

D. CPM is not there because it has own monitoring system. Only lower processes are monitored by watch dog.

Suggested Answer: *A*

Community vote distribution

A (100%)

Sartarus 1 week, 4 days ago

Selected Answer: A

CPM is a Management proccess, by elimination is A

upvoted 1 times

jrugel 2 months, 3 weeks ago

Selected Answer: A

CPM is a management proccess

upvoted 2 times

Question #5 *Topic 1*

What process monitors, terminates, and restarts critical Check Point processes as necessary?

A. CPM

B. FWD

C. CPWD

D. FWM

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **Sartarus** 1 week, 4 days ago

Selected Answer: C

C : CCTE R81.10 page 347

upvoted 1 times

Question #6 *Topic 1*

You found out that $FWDIR/log/fw.log is constantly growing in size at a Security Gateway, what is the reason?

A. TCP state logging is enabled

B. It’s not a problem the gateway is logging connections and also sessions

C. fw.log can grow when GW does not have space in logging directory

D. The GW is logging locally

Suggested Answer: *D*

Community vote distribution

D (100%)

Sartarus 1 week, 4 days ago

Selected Answer: D

D : CCTE R81.10 page 51

upvoted 1 times

Question #7 *Topic 1*

What tool would you run to diagnose logging and indexing?

A. run cpm_doctor.sh

B. cpstat mg -f log_server

C. run diagnostic view

D. run doctor-log.sh

Suggested Answer: *D*

Community vote distribution

D (100%)

edwardT3ach 1 month ago

Selected Answer: D

Ans D is correct

CCTE textbook R81.20 Pg 203

upvoted 1 times

Question #8 *Topic 1*

Where will the usermode core files located?

A. $FWDIR/var/log/dump/usermode

B. /var/suroot

C. /var/log/dump/usermode

D. $CPDIR/var/log/dump/usermode

Suggested Answer: *C*

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

Question #9 *Topic 1*

When a user space process or program suddenly crashes, what type of file is created for analysis?

A. core dump

B. kernel_memory_dump.dbg

C. core analyzer

D. coredebug

Suggested Answer: *A*

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

Question #10 Topic 1

You receive reports from multiple users that they cannot browse. Upon further discovery you identify that Identity Awareness cannot identify the users properly and apply the configured Access Roles. What commands you can use to troubleshoot all identity collectors and identity providers from the command line?

A. on the gateway: pdp debug set IDC all IDP all

B. on the gateway: pdp debug set AD all and IDC all

C. on the management: pdp debug on IDC all

D. on the management: pdp debug set all

Suggested Answer: *A*

Community vote distribution

A (100%)

keikei1228 2 months ago

Selected Answer: A

The correct answer is:
A. on the gateway: pdp debug set IDC all IDP all

The correct command to troubleshoot all identity collectors and identity providers from the command line on the gateway is:
# pdp debug set idc all idp all
idc = Identity Collector
idp = Identity Provider

upvoted 1 times

Question #11 *Topic 1*

When a User process or program suddenly crashes, a core dump is often used to examine the problem. Which command is used to enable the core-dumping via GAIA clish?

A. set core-dump enable

B. set core-dump total

C. set user-dump enable

D. set core-dump per_process

Suggested Answer: *A*

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

Question #12 *Topic 1*

What is the best way to resolve an issue caused by a frozen process?

A. Power off the machine

B. Restart the process

C. Reboot the machine

D. Kill the process

Suggested Answer: *B*

Community vote distribution

C (67%) B (33%)

keikei1228 2 months ago

Selected Answer: B

The correct answer is:
B. Restart the process

When dealing with a frozen (hung) process, the best practice is to:
Restart the affected process, especially if it's a known Check Point daemon (e.g., FWD, CPM, HTTPD).

This method:
- Minimizes disruption to other services
- Resolves the issue cleanly
- Preserves system uptime

upvoted 1 times

Secentity 2 months, 2 weeks ago

Selected Answer: C

As per study material easiest option is reboot of machine

upvoted 2 times

Question #13 *Topic 1*

What is NOT monitored as a PNOTE by ClusterXL?

A. ted

B. Policy

C. RouteD

D. vpnd

Suggested Answer: *B*

Community vote distribution

A (40%) D (40%) B (20%)

alumast 1 month ago

The correct answer is:
D. vpnd

In the ClusterXL Administrator Guide of R81.20 you can see the Critical Devices (pnotes) and their states on the Cluster Member (see "Viewing Critical Devices" on page 264)

ted: Monitors the Threat Emulation process called ted.
Policy: Monitors if the Security Policy is installed.
routed: Monitors the Gaia process called routed.
vpnd: This item is NOT listed as a Critical Device (pnote).

upvoted 1 times

edwardT3ach 1 month ago

Selected Answer: D

VPND seems to be the correct answer.
R81.20 ClusterXL admin guide pg 264-266

upvoted 1 times

922f9b2 1 month, 3 weeks ago

Selected Answer: D

I was mistaken...double checked, its actually vpnd.

upvoted 1 times

922f9b2 1 month, 3 weeks ago

Selected Answer: A

A is 100% the right answer.

upvoted 2 times

keikei1228 2 months ago

Selected Answer: B

The correct answer is:
B. Policy

In Check Point ClusterXL, a PNOTE (Problem Notification) is a mechanism that monitors critical processes and components.
If any monitored item fails, it can trigger a failover to the standby cluster member.

While policy installation and status are tracked in logs and SmartConsole, it is not monitored as a PNOTE by ClusterXL. Policy status does not directly trigger a cluster failover.

ted: Monitors the Threat Emulation Software Blade and is a PNOTE.
RouteD: Monitors the dynamic routing daemon and is a PNOTE.
vpnd: Is not typically listed as a PNOTE in ClusterXL documentation.
Policy: There is no PNOTE called "Policy" in ClusterXL.

upvoted 1 times

⊟ 👤 **922f9b2** 1 month, 3 weeks ago

thats incorrect, check the cluster lab

upvoted 1 times

Question #14 *Topic 1*

What is NOT a benefit of the ‘fw ctl zdebug’ command?

A. Automatically allocate a 1MB buffer

B. Collect debug messages from the kernel

C. Cannot be used to debug additional modules

D. Clean the buffer

Suggested Answer: *C*

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

Question #15 *Topic 1*

Which command is used to write a kernel debug to a file?

A. fw ctl kdebug -T -l > debug.txt

B. fw ctl debug -S -t > debug.txt

C. fw ctl kdebug -T -f > debug.txt

D. fw ctl debut -T -f > debug.txt

Suggested Answer: *C*

Community vote distribution

C (100%)

keikei1228 2 months ago

Selected Answer: C

The correct answer is:
C. fw ctl kdebug -T -f > debug.txt

To write kernel debug output to a file, you use:
fw ctl kdebug -T -f > debug.txt
-T → Adds timestamps to each debug line
-f → Follows the output in real time (like tail -f)
> → Redirects output to a file (in this case, debug.txt)

upvoted 1 times

Question #16 *Topic 1*

What is the buffer size set by the fw ctl zdebug command?

A. 8GB

B. 1 MB

C. 1 GB

D. 8 MB

Suggested Answer: *B*

Community vote distribution

B (100%)

keikei1228 2 months ago

Selected Answer: B

The correct answer is:

B. 1 MB

The "fw ctl zdebug" command is a shorthand for kernel debugging in Check Point, and it sets the debug buffer size to 1 MB by default.

upvoted 1 times

Question #17 *Topic 1*

You are seeing output from the previous kernel debug. What command should you use to avoid that?

A. fw ctl clean buffer = 0

B. fw ctl debug 0

C. fw ctl zdebug disable

D. fw ctl debug = 0

Suggested Answer: *B*

Community vote distribution

B (100%)

keikei1228 2 months ago

Selected Answer: B

The correct answer is:

B. fw ctl debug 0

This command resets all debug flags and enables only the default debug flags in all kernel modules. It also clears the debug buffer, so you will not see output from previous kernel debug sessions.

upvoted 1 times

Question #18 *Topic 1*

During firewall kernel debug with fw ctl zdebug you received less information that expected. You noticed that a lot of messages were lost since the time the debug was started. What should you do to resolve this issue?

A. Increase debug buffer; Use fw ctl debug -buf 32768

B. Redirect debug output to file; Use fw ctl debug-o ./debug.elg

C. Redirect debug output to file; Use fw ctl zdebug -o ./debug.elg

D. Increase debug buffer; Use fw ctl zdebug -buf 32768

Suggested Answer: *A*

Community vote distribution

A (33%) D (33%) C (33%)

TemiEkum 1 week, 2 days ago

Selected Answer: C

When using fw ctl zdebug, it's common to lose messages if there's a high volume of kernel debug output. This tool prints output directly to the screen in real-time, so messages can be dropped if the terminal or shell can't process them fast enough.

To prevent this, you should redirect the output to a file using the -o option. This captures all debug data, ensuring nothing is missed even under heavy load.

Why the others are incorrect:
A. fw ctl debug -buf 32768:
This applies to fw ctl debug, not zdebug. zdebug works differently and doesn't use this buffer setting.

B. fw ctl debug -o ./debug.elg:
Again, this is for fw ctl debug, not fw ctl zdebug.

D. fw ctl zdebug -buf 32768:
fw ctl zdebug does not support the -buf option. It's not a valid parameter.
upvoted 1 times

922f9b2 1 month, 3 weeks ago

Selected Answer: D

its actually D, if you read the question CAREFULLY :)
upvoted 1 times

keikei1228 2 months ago

Selected Answer: A

The correct answer is:
A. Increase debug buffer; Use fw ctl debug -buf 32768

- The "fw ctl zdebug" command is a shorthand for quickly enabling kernel debug flags and outputs directly to the console, but it uses a small buffer (by default, 1MB). If you are losing messages, it is likely because the buffer is too small and overflows.

- To resolve this, you should increase the kernel debug buffer size before starting the debug. The correct command to do this is:
fw ctl debug -buf 32768
This sets the buffer size to 32MB, which helps prevent message loss during high-volume debugging.
upvoted 1 times

Question #19 *Topic 1*

What is the benefit of fw ctl debug over fw ctl zdebug?

A. There is no difference. Both are used for debugging kernel

B. You don’t need timestamps

C. It allows you to debug multiple modules at the same time

D. You only need 1MB buffer

Suggested Answer: *C*

Community vote distribution

C (100%)

keikei1228 2 months ago

Selected Answer: C

The correct answer is:
C. It allows you to debug multiple modules at the same time

- "fw ctl debug" is a more advanced and flexible tool for kernel debugging. It allows you to enable debug flags for multiple kernel modules simultaneously, control the buffer size, output to files, and more.
- "fw ctl zdebug" is a shorthand command that quickly sets kernel debug flags (mainly for the "fw" module) and outputs to the console with a default buffer of 1MB. It is mainly used for quick, on-the-fly troubleshooting and is less flexible.

upvoted 1 times

Question #20 *Topic 1*

The Check Point Firewall Kernel is the core component of the Gaia operating system and an integral part of the traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for troubleshooting packet drops and other kernel activities while using minimal resources (1 MB buffer)?

A. fw ctl zdebug

B. fwk ctl debug

C. fw debug ctl

D. fw ctl debug/kdebug

Suggested Answer: *A*

Community vote distribution

A (100%)

keikei1228 2 months ago

Selected Answer: A

The correct answer is:
A. fw ctl zdebug

The fw ctl zdebug command is designed specifically for:
- Lightweight, real-time kernel debugging
- Uses a fixed 1 MB buffer
- Ideal for quickly troubleshooting issues like packet drops, NAT issues, or connection handling
- Requires no prior flag configuration

upvoted 1 times

Question #21

Topic 1

You need to monitor traffic pre-inbound and before the VPN-module in a security gateway. How would you achieve this using fw monitor?

A. fw monitor -p all

B. fw monitor -pi -vpn

C. fw monitor -pi +vpn

D. fw monitor-pl +vpn

Suggested Answer: *C*

Community vote distribution

C (60%) B (40%)

edwardT3ach 2 weeks, 1 day ago

Selected Answer: C

The Correct answer is C CCSE Guide page 275

upvoted 1 times

alumast 1 month ago

Selected Answer: B

The correct answer is:

B. fw monitor -pi -vpn

The –pi means Pre-Inbound (in chain).

The -vpn means - (minus sign) specifies before the given module (vpn).

upvoted 1 times

922f9b2 1 month, 3 weeks ago

Selected Answer: B

Its actually B, because -vpn means BEFORE vpn occurs.

upvoted 1 times

keikei1228 2 months ago

Selected Answer: C

The correct answer is:

C. fw monitor -pi +vpn

In Check Point, the fw monitor tool captures packets as they pass through various inspection points in the kernel. The common inspection points are:

i – Pre-inbound (before Security Policy)

I – Post-inbound (after Policy, before forwarding)

o – Pre-outbound

O – Post-outbound

If you want to capture pre-inbound traffic before it enters the VPN module, you must:

Include "-pi" to capture pre-inbound

Include "+vpn" to capture before VPN decryption occurs

upvoted 2 times

Question #22 *Topic 1*

You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore, you need to add a timestamp to the kernel debug and write the output to a file. What is the correct syntax for this?

A. fw ctl debug -T -f > filename.debug

B. fw ctl kdebug -T -f -o filename.debug

C. fw ctl kdebug -T > filename.debug

D. fw ctl kdebug -T -f > filename.debug

Suggested Answer: *B*

Community vote distribution

B (50%) D (50%)

edwardT3ach 2 weeks, 4 days ago

Selected Answer: D

answer is D

upvoted 1 times

922f9b2 1 month, 3 weeks ago

Selected Answer: D

It is D, for sure

upvoted 2 times

keikei1228 2 months ago

Selected Answer: B

Correct answer is:

B. fw ctl kdebug -T -f -o filename.debug

- The command runs the debug and uses the shell's redirection (>) to write the output to the specified file. After stopping the debug, these files are merged and then output to the screen (and thus to your file).

- The "-o" flag tells the kernel debug process to write output directly to the specified file. Ensures you get the debug output in your file as the debug runs, not just after it stops.

Note: Use "-o" for long-term, reliable debugging.

upvoted 3 times

Question #23 *Topic 1*

What is the correct syntax to set all debug flags for Unified Policy related issues?

A. fw ctl kdebug -m UP all

B. fw ctl debug -m UP all

C. fw ctl debug -m up all

D. fw ctl debug -m fw all

Suggested Answer: *B*

Community vote distribution

B (100%)

922f9b2 1 month, 3 weeks ago

Selected Answer: B

ran it in the lab, it is B

upvoted 1 times

keikei1228 2 months ago

Selected Answer: B

fw ctl debug -m <module> all sets all debug flags for the specified module.

For Unified Policy, the correct module name is UP (uppercase).

upvoted 1 times

Question #24 *Topic 1*

What is the shorthand reference for a classification object?

A. classobj

B. CLOB

C. COBJ

D. class.obj

Suggested Answer: *C*

Community vote distribution

B (67%) C (33%)

Abrieg 1 month ago

Selected Answer: C

In Check Point, the shorthand reference for a classification object is COBJ. This prefix is used internally to identify classification objects in the system.

upvoted 1 times

keikei1228 2 months ago

Selected Answer: B

Correct answer: B. CLOB

In Check Point architecture, a classification object is referred to as a CLOB (Classification Object).

upvoted 1 times

0cddb14 2 months, 1 week ago

Selected Answer: B

CLOB is the abbreviation of Classification Object, which is used to refer to the object generated during the packet classification stage (Classification OBject)

upvoted 1 times

Question #25

Topic 1

The Unified Access Control policy eliminates the need to maintain policies for different access control features. However, you need to start a general debug of the Unified Policy with all flags turned on. Which of the following is the correct syntax?

A. fw ctl debug -m UP all

B. fw ctl debug -m UP + all flags

C. fw ctl kdebug -m UP all

D. fwm ctl debug -m UP all

Suggested Answer: *A*

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

Question #26 *Topic 1*

The FileApp parser in the Content Awareness engine does not extract text from which of the following file types?

A. Microsoft Office Excel files

B. Microsoft Office PowerPoint files

C. Microsoft Office .docx files

D. PDF’s

Suggested Answer: *D*

Community vote distribution

B (67%) D (33%)

922f9b2 1 month, 3 weeks ago

Selected Answer: B

its actually B

upvoted 2 times

keikei1228 2 months ago

Selected Answer: D

Correct answer: D. PDF’s

The FileApp parser in Check Point's Content Awareness engine supports text extraction from:

- Microsoft Office 2007+ files (.docx, .xlsx, .pptx)
- Text files
- Archives like .zip and .gzip

However, PDF files are not supported for text extraction. The engine can recognize the file type but cannot extract or inspect text content from PDFs.

upvoted 1 times

Question #27 *Topic 1*

In Check Point's Packet Processing Infrastructure, what is the role of Observers?

A. Observers attach object IDs to traffic

B. They store Rule Base matching state related information

C. Observers monitor the state of Check Point gateways and report it to the security manager

D. Observers decide whether or not to publish a CLOB to the Security Policy

Suggested Answer: *D*

Community vote distribution

D (60%) B (20%) A (20%)

Abrieg 1 month ago

Selected Answer: A

n Check Point's packet processing infrastructure, Observers are responsible for attaching object IDs to traffic and storing Rule Base matching state information. They also monitor the state of Check Point gateways and report this information to the security manager. Furthermore, Observers determine whether to publish a CLOB (Check Point Large Object) to the Security Policy based on the observed state of the traffic and its associated connection.

upvoted 1 times

keikei1228 1 month, 2 weeks ago

Selected Answer: D

Observers are responsible for refining and classifying CLOBs, which are then used to enhance the accuracy of the Security Policy. They play a key role in the Publisher-Observer system by deciding whether or not to publish a CLOB to the Security Policy.

upvoted 1 times

keikei1228 2 months ago

Selected Answer: B

The correct answer is:
B. They store Rule Base matching state related information

Explanation:
In Check Point's Unified Policy (UP) infrastructure, Observers are components that collect and store classification objects (CLOBs) for further classification refinement. They are responsible for maintaining the state of rule base matching and classification objects during a connection or transaction. Observers do not attach object IDs to traffic (that's the role of Classifiers), nor do they monitor gateway health or decide on publishing CLOBs to the policy.

Reference:
"Observers CLOBS are distributed to a Publisher-Observer system (via the Manager). The Transaction is a Publisher. The Observer is a unit collecting CLOBs for classification refinement (e.g: CLOB dependency)."
— ATRG: Unified Policy (sk120964)

upvoted 1 times

eww_cybr 2 months, 2 weeks ago

Selected Answer: D

Observer
The Observer decides if enough information is known to publish a CLOB to the security policy. CLOBs are observed in the context of their transaction and the connection that the transaction belongs to. The Observer may request more CLOBs for a dedicated packet from the Classifier or decides that it has sufficient information about the packet to execute the rule base on the CLOB, e.g. if a file type is needed for Content Awareness and the gateway hasn't yet received the S2C response containing the file. Executing the rule base on a CLOB is called "publishing a CLOB". The Observer may wait to receive more CLOBs that belong to the same transaction before publishing the CLOBs.

upvoted 1 times

Secentity 2 months, 3 weeks ago

Selected Answer: D

CCTE R81.20, p318: Observers decide whether to publish a CLOB to the rulebase. More CLOBs can be requested from the Classifier if the Observer needs additional information for a particular packet. The Observer publishes the CLOB and subsequent packets to the rulebase.

upvoted 1 times

Question #28 *Topic 1*

What is the kernel process for Content Awareness that collects the data from the contexts received from the CMI and decides if the file is matched by a data type?

A. cntawmod

B. cntmgr

C. dlpda

D. dlpu

Suggested Answer: *A*

Community vote distribution

C (67%) A (33%)

Abrieg 1 month ago

Selected Answer: A

cntawmod is the kernel module for Content Awareness.
It collects data from the CMI (Context Management Infrastructure) and evaluates whether a file matches a defined data type.
It operates within the kernel space to enforce content inspection policies.
The other options refer to user-space processes or components related to DLP (Data Loss Prevention), not the Content Awareness kernel module.

upvoted 1 times

keikei1228 2 months ago

Selected Answer: C

The correct answer is:
C. dlpda

The dlpda process is responsible for collecting data from the contexts created by the FileApp parser (as received from the CMI) and deciding if the file matches a defined Data Type in Content Awareness. When a file is matched, the dlpda process notifies the Unified Rulebase (UP) and triggers rulebase execution.
- dlpda = Data Loss Prevention Daemon for Content Awareness (CTNT)
- cntawmod and cntmgr are not Check Point kernel processes related to Content Awareness.
- dlpu is a process in DLP (Data Loss Prevention), but not specifically for Content Awareness context matching.

upvoted 1 times

Secentity 2 months, 3 weeks ago

Selected Answer: C

The Content Awareness DLPDA process collects the data from those
contexts and decides if the file is matched by a data type

upvoted 1 times

Question #29 *Topic 1*

The packet processing infrastructure consists of 4 components. Which component contains the CLOB, the object that contains information about the packet that is needed to make security decisions?

A. Manager

B. Classifiers

C. Handlers

D. Observers

Suggested Answer: *C*

Community vote distribution

B (100%)

CChristos 1 month, 2 weeks ago

Selected Answer: B

Classifier - When the “first packet” rule base check is complete Classifiers initiate streaming for subsequent packets in the session. The “first packet” rule base check identifies a list of rules that possibly may match and a list of classifier objects (CLOBs) that are required to complete the rule base matching process. The Classifier reads this list and generates the required CLOBs to complete the rule base matching. Each Classifier App executes on the packet and tells the result of the CLOB to the UP Manager. The CMI then tells the Protocol Parser to enable streaming.

upvoted 1 times

keikei1228 2 months ago

Selected Answer: B

Correct answer: B. Classifiers

In Check Point’s packet processing infrastructure, the Classifier component is responsible for:
- Creating and managing CLOBs (Classification Objects)
- Analyzing traffic and attaching CLOBs that describe key attributes (e.g., application, user, file type)

These CLOBs are then used by the Manager and other components to make security decisions based on policy.

upvoted 1 times

eww_cybr 2 months, 2 weeks ago

Selected Answer: B

Unified Policy (UP) Infrastructure Components

UP Manager of the UP infrastructure
Classifier creates classifier objects (CLOBs) to match against the UP policy
Observer decides if enough is known in the CLOB to check it against the rule base
Column based rule base enforcement matches CLOBs against the policy
Handle stores the rule base execution state

upvoted 2 times

Question #30 *Topic 1*

Which of the following is a component of the Context Management Infrastructure used to collect signatures in user space from multiple sources, such as Application Control and IPS, and compiles them together into unified Pattern Matchers?

A. Context Loader

B. PSL - Passive Signature Loader

C. cpas

D. CMI Loader

Suggested Answer: *D*

Community vote distribution

D (100%)

edwardT3ach 1 month ago

Selected Answer: D

CCTE pg 314

Ans is CMI Loader

upvoted 1 times

922f9b2 1 month, 3 weeks ago

Selected Answer: D

I would agree its D.

upvoted 1 times

keikei1228 2 months ago

Selected Answer: D

The correct answer is:

D. CMI Loader

- The CMI Loader (Context Management Infrastructure Loader) is responsible for collecting signatures in user space from multiple sources, such as Application Control, IPS, Content Awareness, etc., and compiling them together into unified Pattern Matchers (PM) for each context (e.g., URL, Host header, etc.).
- This process is a key part of the Context Management Infrastructure (CMI) in Check Point architecture.

upvoted 1 times

Question #31 *Topic 1*

Which of these packet processing components stores Rule Base matching state-related information?

A. Classifiers

B. Manager

C. Handlers

D. Observers

Suggested Answer: *C*

Community vote distribution

C (75%) B (25%)

Abrieg 1 month ago

Selected Answer: B

In Check Point's Packet Processing Infrastructure (PPI):

The Manager component is responsible for storing Rule Base matching state-related information.
It tracks the state of connections and maintains contextual data needed for consistent and accurate policy enforcement across packets in a session.
This makes Manager the correct choice for handling state-related rule base matching data.

upvoted 1 times

eww_cybr 2 months, 2 weeks ago

Selected Answer: C

Handle
Each connection may consist of several transactions. Each transaction has a Handle. Each Handle contains a list of published CLOBs. The Handle holds the state of the security policy matching process. The Handle infrastructure component stores the rule base matching state related information.

upvoted 3 times