Solution ID: **sk39510** Technical Level: **Basic**

Email

How to configure Wireshark to show Check Point FireWall chains in an FW Monitor packet

Product
Other

Version
All

OS
Windows

Platform
Intel/PC

Last Modified
2022-03-24

Solution

As of version 0.10.0, the Wireshark application is able to view Check Point FireWall chains in an FW Monitor packet capture in the same way CPEthereal application can.

Note: The CPEthereal application is no longer developed. Check Point recommends using the latest version of the Wireshark application to analyze FW Monitor packet captures.

Configure the Wireshark application to show the Check Point FireWall chains:

1. Close all instances of Wireshark.

2. Open one instance of Wireshark

4. Go to '`Protocols`' - click '`Ethernet`' - select the box '`Attempt to interpret as FireWall-1 Monitor File`' - click '`Apply`'.

5. Go to '`Appearance`' (in v2.x) / '`User Interface`' (in v1.x) - click '`Columns`' - click '`+`' / '`Add`' button - a new line is added at the bottom of the list:

    - Double-click the title '`New Column`' - assign a name (e.g., *FW-1*)

    - Double-click the type '`Numbers`' - choose '`FW-1 monitor if/direction`'

6. Left-click and hold this new line - drag the line to the desired position (recommended position is between the '`Destination`' and '`Protocol`').

7. Click '`Apply`'.

8. Click '`OK`'.

9. Close Wireshark.

10. Open Wireshark.

You can use these filters in Wireshark to analyze the traffic captured with the FW Monitor tool:

Field Name	Type	Description	Relation operators	Possible values

`fw1.chain`	String	Chain Position	`==`
			`!=`
			`>`
			`<`
			`>=`
			`<=`
			`contains`
			`matches`
				Depends on FW Monitor position during traffic capture.
				
				For a complete list of Check Point kernel chains,
				refer to the output of the '`fw`

`fw1.direction`	String	Direction	`==`
			`!=`
			`>`
			`<`
			`>=`
			`<=`
			`contains`
			`matches`
				`i`
				`I`
				`o`
				`O`

`fw1.interface`	String	Interface	`==`
			`!=`
			`>`
			`<`
			`>=`
			`<=`
			`contains`
			`matches`
				Interface name as configured in the operating system and detected by Check Point kernel - refer to the output of '`fw ctl iflist`' command.

`fw1.type`	Unsigned 16-bit integer	Type	`==`
			`!=`
			`>`
			`<`
			`>=`
			`<=`
				Always `0x0800` (for IP protocol), because Check Point FireWall supports only TCP/IP stack.

`fw1.uuid`	Unsigned 32-bit integer	UUID	`==`
			`!=`
			`>`
			`<`
			`>=`
			`<=`
				Note: this field is irrelevant for analysis.

Example:

```
((fw1.interface == "eth1") and (fw1.direction == "i") and (fw1.chain == "1"))
```

Important Note:

For example, the R80.20 version added new chains - Pre-Outbound VPN Encryption "e", Post-Outbound VPN Encryption "E", Pre-Inbound VPN Decryption "d", Post-Inbound VPN Decryption "D", Pre-QoS "q", and Post-QoS "Q". As of March 2022, Wireshark does not show these chains.

Related Solutions:

- sk30583 - What is FW Monitor?
- sk43076 - How to work with large traffic capture files
- sk39510 - How to configure Wireshark to display Check Point FireWall chains in an FW Monitor packet

Article Properties

Access Level
General

Date Created
2009-04-14

Last Modified
2022-03-24