IPS Troubleshooting

IPS Profile and Detect Mode

When you run the IPS recommended profile, most of the critical and high signatures are in inactive or detect mode.
But still there could be a high cpu performance impact even when you're only in detect mode.

> In prevent mode you kill the connection and you are done.
> In detect mode you have to keep the connection open and keep spending CPU cycles on tracking that traffic.

So detect mode maybe is using higher cpu cycles.

R80.x Performance Tuning Tip - DDOS

See: https://community.checkpoint.com/docs/DOC-3407-r80x-performance-tuning-tip-ddos-fw-sam-vs-fwaccel-dos

R80.10 IPS Best Practices

CP_R80.10_IPS_BestPractices_Guide.pdf

Revision #3
Created 21 October 2020 15:46:56
Updated 27 February 2021 08:28:49