DOS & DDOS Prevention, Mitigation

Preface

Since R80.20 DOS/DDOS Prevention changed in Check Point.
The following is a summary how you can setup and mitigate DOS & DDOS attacks.

SYN Defender since R80.20

Important changes in IPS "SYN Attack" (SYN Defender) protection for R80.20 and above

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120476

How to configure Rate Limiting rules for DoS Mitigation (R80.20 and newer)

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112454

Mitigation

How to configure Security Gateway to detect and prevent port scan

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk110873&partition=Advanced&product=Security

How to create and view Suspicious Activity Monitoring (SAM) Rules

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112061

Best practice

- Set "Host Scan" and "Sweep Scan" in IPS Policy to "User Alert 1".
- In Global Settings on Smartcenter at "User Alert 1" 120 seconds blocking of source ip run via script

```
sam_alert -t 120 -I -src
```

Revision #4
Created 21 October 2020 14:45:29
Updated 21 October 2020 15:53:38