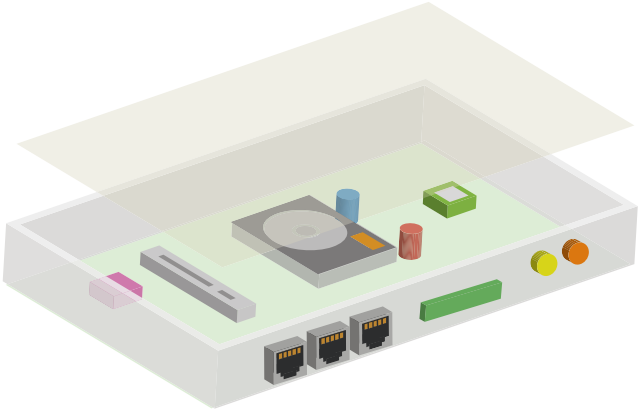
PurpleSynapz™

07 January 2019



FW Health™

For better management of Security Gateways, this report entails all essential information making it easy for security administrators to screen the health status of firewall devices. From memory status and CPU usage to cluster management, nothing has been missed to assist you developing a secured environment.

Client Details:

Purplesynapz Ltd.

Report Generated By:

QOS Technology

Duration of Log capture:

Start Time: Mar-6-12:23:02

End Time: Mar-7-12:18:37

Table of Contents

Section 1: Executive Summary

In the evolving attack surfaces owing to diversifying business delivery channels it is quite evident the Security Gateways capacities may exhaust sooner than the scheduled timelines. Also there is a likelihood of more security controls or greater number of security attributes that may be augmented on the existing Security Gateways and the capacities start to shrink at faster gradient than the expected or experience rate of capacity exhaustion. In either of the situation there is a definite need to get the snapshot of available capacity vis-à-vis consumed resources for any Security Gateway that is far more granular than the real time statistics of CPU & Memory.

If the setup for your organization involves few 10's or few 100's of Security Gateway then the business need goes further to even build a companywide heat map of the appliances/gateways that may be left with zero or less oxygen (available capacity). So the desired tool should also help building a heat map for such gateways while working on complex attributes or variables of capacity analysis.

Last, but not the least your company may want the turnaround time, planning time before going for any technology refresh of the Security Gateways with shrunken capacities. So there is an expectation of tool that may help building these heat maps by employing the automation, thus facilitating the operations' team to generate capacity reports at a click of mouse at any time.

FWHealth is one such tool that addresses these use cases for all the customers that have deployed one or hundreds or thousands of Check Point Security Gateways. FWHealth has two components, Collector & Reporter. The collector instance is an on premise VM that gets installed on any open server that may run the VM and in turn has a TCP/IP connectivity to the management IP addresses of all the Check Point Security Gateways whose real time capacity needs to be reviewed. The 2nd component of FWHealth is the Reporter, that has been hosted in the public cloud infrastructure and you may submit the collector generated file(s) to the cloud and you get this report.

Section 2: Know Your Security Gateway

This section depicts some basic information about Security Gateway and recommendations around hardware, OS and software running in the environment.

2.1 Security Gateway Vital Stats

For effective and smooth security operations, it's extremely fundamental to be cognizant of your Security Gateway, and insights gained through such exposure always aides in better decision making.

Appliance Name	Check Point 5800
Software Version	Gaia R77.30
OS Version	GAIA 64-bit
Host Name	ISP2-FW1

Software Blades	Firewall	IPSec VPN	IPS	Data Loss Prevention	Mobile Access	Identity Awareness	Anti-Virus	URL Filtering	Anti-Spam	Application Control	Anti-Bot	Threat Emulation	Threat Extraction
Purchased	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗
Activated	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Recommendations

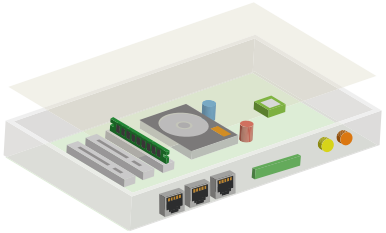
• The current OS installed on the Appliance is running GAIA in 64-bitmode. This hardware has an End of Life date Not announced. The version installed is not the latest version as the current latest version is R80.10 and as per Check Point Best Practice it is recommended to upgrade to the latest version, in order to get the latest features and issues fixed. You are currently using GAIA OS. You are running on a Scalable OS platform.
• These blades namely VPN ,IDENTITYSERVER ,CVPN ,IPS ,URLF ,APPI ,AV ,ANTI_BOT ,ASPM have been purchased but have not been activated on the appliance. In order to get the security cover for the controls provided by these blades, the same should be enabled.

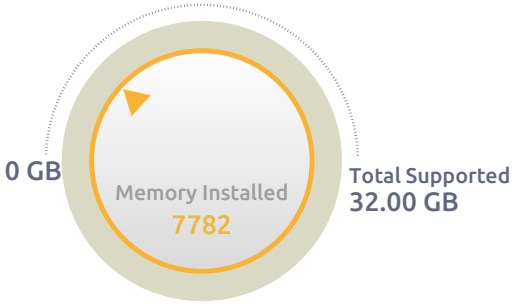
2.2 Security Gateway Internals

2.2.1 Memory

One of the essential component of hardware is memory. It not only governs the connection capacity but also helps in determining the number of users we can secure behind our Security Gateway.

This section delineates about the memory availability of Security Gateway.





Memory Installed vs Total Memory Supported

Occupied	Total no. of Slots
1	4

Total number of Slots occupied by memory modules in Security Gateway hardware

Total number of memory Slots supported by Security Gateway hardware

Recommendations

- The current RAM Installed onto the device is 7782 MB and the device is capable of installing 32768 MB

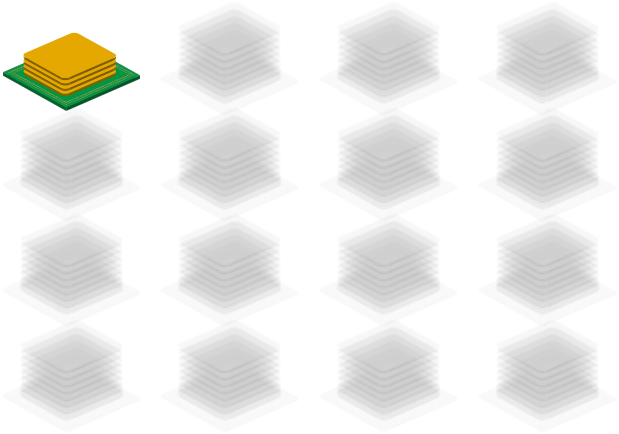
2.2.2 CPU

Another most essential component in our hardware is CPU which governs the throughput we receive from Security Gateway. Better management of CPU ensures better possibility to run more features and proliferate connections per second on any Security Gateway.

Along with the recommendations based on the CPU and core status, this section also focuses on its availability.

Total CPUs	1

Cores Per CPU	4



Section 3: Know Capacity of Your Security Gateway

This section has been assigned for delineating about Security Gateway's capacity and recommendations around hardware upgrade based on its utilization pattern in existing environment.

Why this is important?

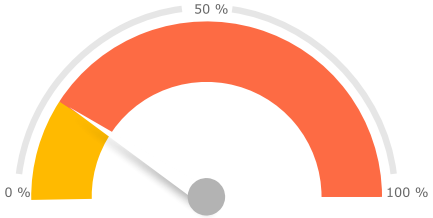
For efficient and seamless security operations, capacity utilization has always remained the most critical element. This information aides security administrators to decide about the optimum capacity and situations when hardware upgrade is required.

3.1 Memory Stats

Memory utilization is critical parameter to look for while planning the capacity of Security Gateway and forms basis for decisions like hardware upgrade and also fine-tuning aspects of configuration.

Memory Utilization

Memory Used vs Total Memory Available.



Memory Used	Total Memory
1.39 GB	7.6 GB

Recommendations

- The current RAM Installed onto the device is 7782 MB and the device is capable of installing 32768 MB
- The memory utilization on the device is 1424MB and the total RAM supported on the device is 32768 MB. The device is using the memory optimally.

3.2 CPU Stats

Apart from assisting to plan capacity utilization, information under this section is extremely critical input for fine-tuning the acceleration techniques like Secure XL & Core XL

Load Average

Average usage of CPU across intervals of 1-5-15 minutes.
It has to be correlated with number of CPU cores available.

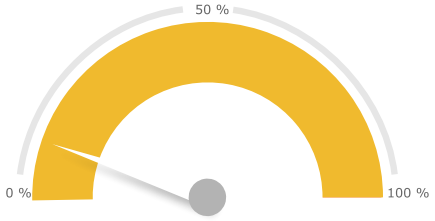
Recommendations

- The System is optimally loaded in the last one minute.
- The System is optimally loaded in the last five minutes.
- The System is optimally loaded in the last fifteen minutes.

3.3 Connection Stats

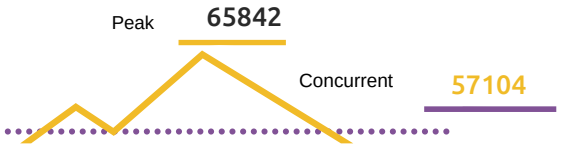
Number of connections Security Gateway is handling signifies the amount of load Security Gateway is inspecting. It is the end result of multiple parameters.

In this section we try to draw 3 dimensional relationships between: Maximum number of connections supported by your Security Gateway, Connection limit configured by your administrator and optimal connection limit your administrator should configure. It also attempts to show a relationship between peak and average connections Security Gateway is processing.



Connection MAP

Optimum	Maximum	Configured
79010.4	759960	759960



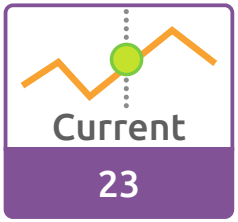
Peak concurrent connection processed by Security Gateway since last reboot. And connections getting processed at the time of capture.

Recommendations

- Peak Connections are optimally configured. The device should be configured with the optimum limit of 79010.4

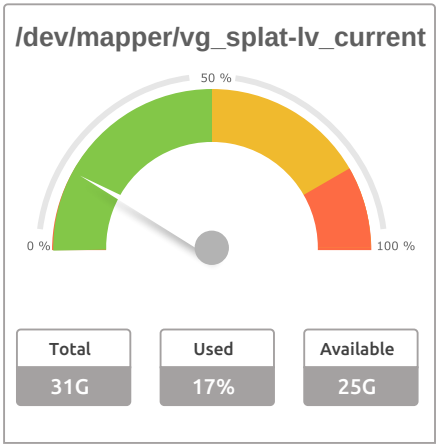
3.4 Network Address Translation (NAT) Stats

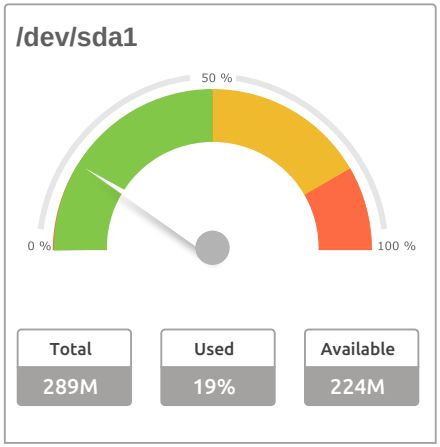
Amount of NATing security sppliance performs directly impacts the performance of the Gateway, making it very critical for administrators to monitor the number of NAT connections appliance is processing. So, in order to dent such difficulty, these insights can help for better security outcome.

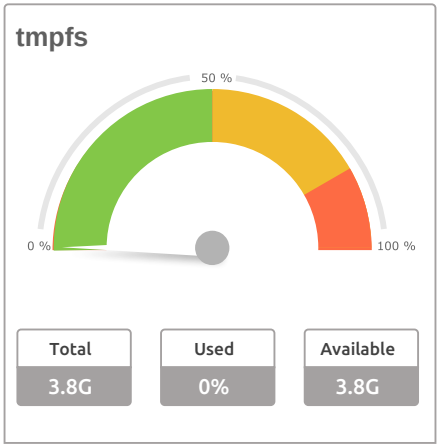


3.5 Hard Disk Utilisation

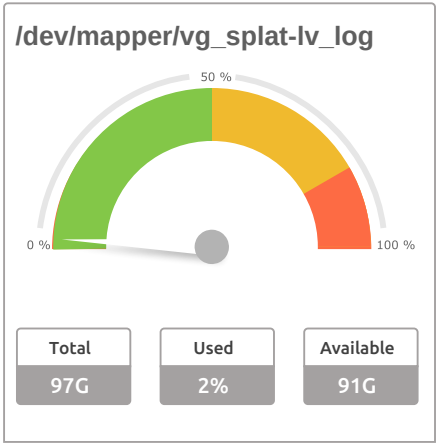
Hard disk utilization is another important parameter which is generally overlooked by many admins. It has been observed that due to some software bug the hard disk utilization may go very high and can impact production.
Also, it has been noticed that firewall admins capture the log files and do not clean the same once the troubleshooting is done. Critical signature updates will fail if hard disk is not maintained properly.







3.5 Hard Disk Utilisation - continued



Recommendations

- Hard Disk Utilization of this gateway is normal.

Section 4: Know Topology of Your Security Gateway

This section has been dedicated to understand the topology of Security Gateway alongside the recommendations around network integration with uplinks and clustering attributable to the interface and cluster design of Security Gateway.

Why this is important?

Layer 2 mismatch is frequently the underlying cause for many unexplained outages within network infrastructure. We are attempting to relate different parameters of interface and measurements to highlight any abnormality which could be a noteworthy reason for any undesirable result.
Clustering configuration is extremely critical to be investigated to guarantee accessibility of your framework at all times. We are trying to highlight health of the cluster by pointing out major parameters used to define behavior of Security Gateway cluster you are running.

4.1 Network interface topology

Interface Outlook

Interface Name	Speed	Duplex	Negotiation
eth8	Unknown!	Unknown! (255)	on
Sync	1000Mb/s	Full	on
eth2-01	Unknown!	Unknown! (255)	on
eth2-03	Unknown!	Unknown! (255)	on
eth2-02	Unknown!	Unknown! (255)	on
eth2-04	Unknown!	Unknown! (255)	on
Mgmt	1000Mb/s	Full	on
eth7	Unknown!	Unknown! (255)	on
eth6	Unknown!	Unknown! (255)	on
eth5	Unknown!	Unknown! (255)	on
eth4	Unknown!	Unknown! (255)	on
eth3	Unknown!	Unknown! (255)	on
eth2	1000Mb/s	Full	on
eth1	1000Mb/s	Full	on

For layer 2 settings of Security Gateway, and to ensure hygiene at its configuration which is often ignored, this section is very helpful.

4.2 Network interface Statistics

Important Layer 2 parameters per interface which defines Layer 2 hygiene of the Security Gateway.

a) Packets : No. of pakets processed by the interface.
b) Errors : No. of errors encountered by the interface.
c) Dropped: No. of packets dropped by the interface
d) Overrun:No. of packets dropped due to overrun

Since last cleared manually or reboot.

	Rx				Tx			
Interface Name	Packets	Errors	Dropped	Overrun	Packets	Errors	Dropped	Overrun
Mgmt	5171849	0	0	0	9050801	0	0	0
Sync	7527164	0	0	0	12838621	0	0	0
eth1	387218410	0	0	0	471194752	0	0	0
eth2	499159228	0	0	0	384394212	0	0	0
lo	32973	0	0	0	32973	0	0	0

Recommendations

- There is no issue on the packets being received on the interfaces - Mgmt, Sync, eth1, eth2, lo
- There is no issue on the packets being transmitted on the interfaces - Mgmt, Sync, eth1, eth2, lo
- Keeping the speed as Auto-negotiation on - on the interface eth8 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth8 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth8 - is either in the shut state or do not have the link connected.
- Keeping the speed as Auto-negotiation on - on the interface Sync keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Keeping the speed as Auto-negotiation on - on the interface eth2-01 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth2-01 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth2-01 - is either in the shut state or do not have the link connected.
- Keeping the speed as Auto-negotiation on - on the interface eth2-03 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth2-03 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth2-03 - is either in the shut state or do not have the link connected.
- Keeping the speed as Auto-negotiation on - on the interface eth2-02 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth2-02 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth2-02 - is either in the shut state or do not have the link connected.
- Keeping the speed as Auto-negotiation on - on the interface eth2-04 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth2-04 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth2-04 - is either in the shut state or do not have the link connected.
- Keeping the speed as Auto-negotiation on - on the interface Mgmt keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Keeping the speed as Auto-negotiation on - on the interface eth7 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth7 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth7 - is either in the shut state or do not have the link connected.
- Keeping the speed as Auto-negotiation on - on the interface eth6 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth6 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth6 - is either in the shut state or do not have the link connected.

Recommendations

- Keeping the speed as Auto-negotiation on - on the interface eth5 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth5 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth5 - is either in the shut state or do not have the link connected.
- Keeping the speed as Auto-negotiation on - on the interface eth4 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth4 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth4 - is either in the shut state or do not have the link connected.
- Keeping the speed as Auto-negotiation on - on the interface eth3 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Duplex:Unknown!--The Interface eth3 is either in the shut state or do not have the link connected.
- Speed:Unknown!--The Interface eth3 - is either in the shut state or do not have the link connected.
- Keeping the speed as Auto-negotiation on - on the interface eth2 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.
- Keeping the speed as Auto-negotiation on - on the interface eth1 keeps a loophole of the interface getting negotiated on lower speeds and half duplex. As part of the best practice, this should be set to off.

4.3 ARP Value

ARP value is extremely critical component when Security Gateway catering to large broadcast domain. This component is often ignored and unexplained in large network deployments.

ARP Used	23	ARP Set	4096

Recommendations

- ARP is being optimally used.

4.4 Security Gateway Cluster

Security Gateways are deployed in clustering to achieve seamless business operations and scalability objective of organization.

This sections depicts the cluster health of Security Gateways based on important parameters.

4.4.1 Cluster Status

Apart from displaying whether cluster is active or passive in its configuration, It also delineates the overall health status of Security Gateway cluster.

Local

Peer

4.4.2 Cluster Interfaces

This section helps in studying the behavior of Interfaces to find out any variance which can be a root cause of any failover and to check whether cluster has failed to function correctly due to interfaces.

Interface Name	Status
eth1	▲
eth2	▲
Sync	▲
Mgmt	▲

Partially Up Up Down

4.4.3 Cluster Processes

This sections helps in better management of cluster by finding out whether any process is involved to dictate the status of cluster and allowing cluster to show any unusual behavior..

Process Name	State
fwd	✓
routed	✓
Filter	✓
Synchronization	✓
Recovery Delay	✓
Interface Active Check	✓
cphad	✓

Recommendations

• High Availability (Active Up) with IGMP Membership
• The Local Cluster member status is normal.
• The Peer Cluster member status is normal.
• eth1 eth2 Sync Mgmt are functioning normally.
• The critical processes fwd, routed, Filter, Synchronization, Recovery Delay, Interface Active Check, cphad required for the cluster are functioning normally.

Okay Problem

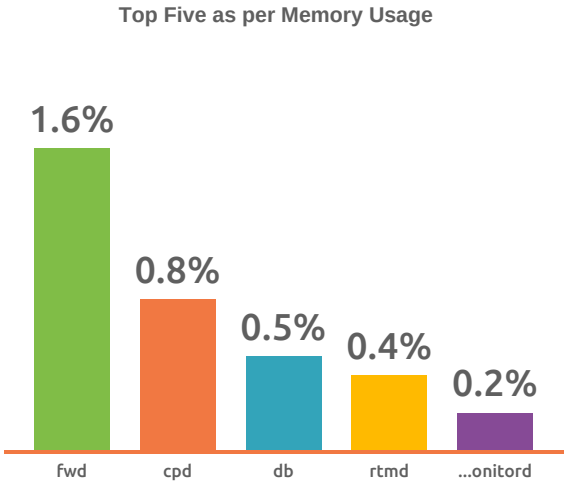
Section 5: Know What is Keeping Your Security Gateway Busy

Aims at depicting which processes are consuming more resources in Security Gateway along with helping to understand traffic profile in an existing setup. .

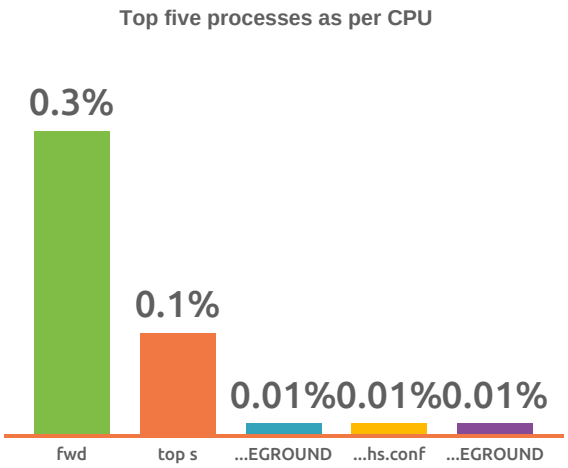
Why this is important?

Understanding how resources are consumed and at which level is extremely important to identify whether load is justified and this information can assist in deciding about any upgrade or fine-tuning of configuration, provided any performance issue is reported. It is also essential to understand traffic profile to size the gateways in refresh cycles.

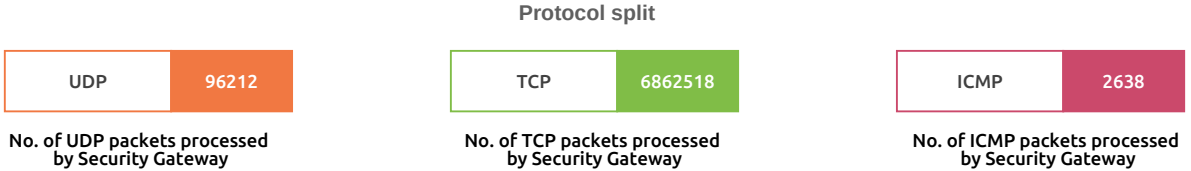
5.1 Processes to Memory Mapping



5.2 Process to CPU Mapping



5.3 Traffic Profile



No. of UDP packets processed by Security Gateway

No. of TCP packets processed by Security Gateway

No. of ICMP packets processed by Security Gateway

Section 6: Know How well Your Security Gateway is Optimized

This section assists in finding out the appropriateness of SecureXL and CoreXL of Security Gateway.

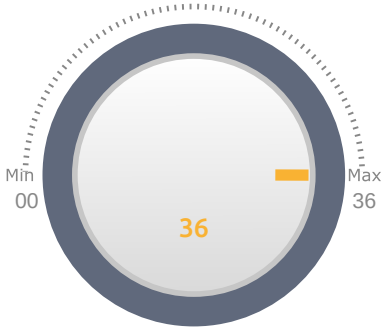
Why this is important?

Secure Xl oversees the acceleration packets processed by firewall engine of your Security Gateway. For optimized utilization of Security Gateway, It is critical to get Secure Xl setup right. We are drawing different correlations to give you the right set of suggestions with respect to Secure XL setup. Process allocation to various CPU cores is governed by cluster. Security Gateway performs multi-functional role when various software blades are enabled and in such scenarios its critical to configure cluster properly which generally gets ignored on a large portion of the events.

6.1 Secure XL Status

This section delineates if Secure XL is enabled in gateway. Enabling Secure Xl is imperative however it is additionally critical to fine tune the rule base for traffic acceleration.

Status



Rule Base - Relationship

Recommendations

- SecureXL as a mechanism allows traffic acceleration by creating the connections and packet templates.

Recommendations

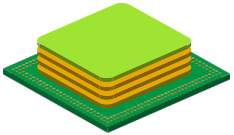
- SecureXl is enabled.
- Drop Templates are Enabled.
- NAT Templates should be enabled to Accelerate the NAT Traffic.
- The device acceleration is optimally configured.

6.2 Core XL Status

Other than finding out whether Core XL is enabled, this section also attempts to provide a better visibility of Security Gateway's status, furthermore correlating various parameters to recognize right CPU spread for your environment.

Status

Secure XL vs Core XL



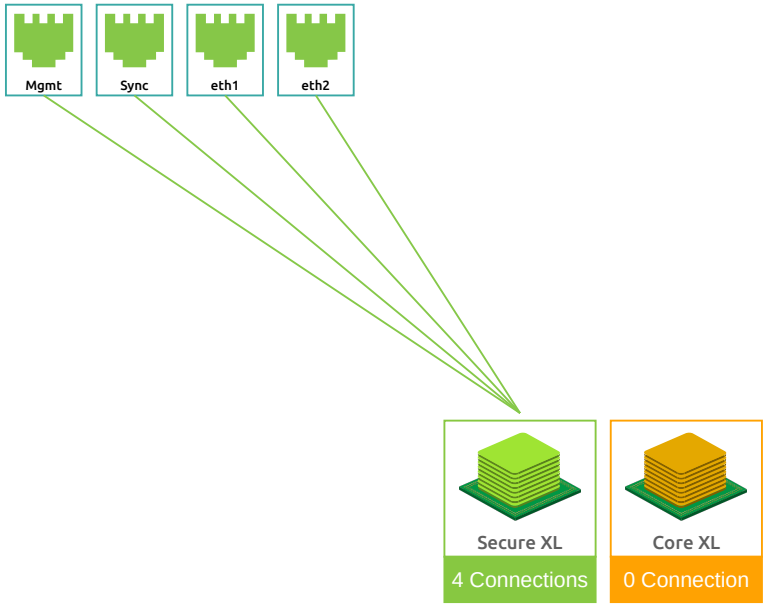
Total Secure XL	1	Total Core XL	3

Recommendations

- Load on CPU with CoreXL: 0.167
- Load on CPU with SecureXL: 0.5

6.3 CPU to Interface Alignment

This segment depicts how different interfaces are assigned to Core XL and Secure XL furthermore providing greater visibility of their allocation which can assist in modifying design and configuration for better security outcomes.



Recommendations

- The interfaces Mgmt, Sync, eth1, eth2 are binded to the SecureXL instances only as per the best practice deployment architecture.

6.4 CPU to Process Alignment

Apart from helping to fine tune design and configuration, this section also depicts how CPU is assigned to various processes and gives better standpoint about how processes are appointed to individual cores.

CPU to Process Alignment

Section 7: Conclusion

This report gives a complete capacity assessment of your Check Point Security Gateway that may have been deployed as Check Point Appliance or as the Software engine on the open server. The report has been prepared by working on variety of attributes beyond the CPU cycles & memory usage and the complex relationships have been assessed that at times are mutually exclusive, like a 'Number of Concurrent Connections' & 'Status of SecureXL' or these may be mutually inclusive, like a 'Status of CoreXL' vis-à-vis 'Status of SecureXL'.

This report has been prepared to give you an automated output which otherwise may only have been possible by hiring the consultant(s) with the diverse technical experience on Check Point Software Technologies' gateways and also having a sufficient exposure on the capacity planning & performance analysis. We believe you will find this report useful and the recommendations section with respect to each attribute will help you plan your security expansion and/or technology refresh more wisely and take decisions based on data & not on the inferential excerpts.