CHECK POINT
YOU DESERVE THE BEST SECURITY


# HCP parte 2
# Atualizações do HCP
# Analisando alguns testes
# Otimizando Peformance - (SecureXL)

**Documento escrito por: José Irapuan**
**Security Engineering Brazil**
**Data de publicação: 21 de dezembro de 2023**

# Conteúdo



## Ferramentas de análise dos equipamentos Check Point

A Check Point disponibiliza um variedade de ferramentas para **monitoração**, ***debug*** e **suporte**.

Estas ferramentas podem ser utilizadas tanto por seus clientes quanto parceiros para:

- Dimensionamento (sizing) de novos equipamentos;
- Diagnóticos de hardware e software;
- Atualizações (componentes *self-updatable*);
- Troubleshootings mais avançados;
- Análise de performance;
- Monitoração;
- Captura de pacotes;
- entre outras capacidades que ajudam tanto na operação do dia a dia quanto em novos projetos e revisão de ambientes já existentes.

A lista com a descrição e detalhes destas ferramentas pode ser encontrada no **sk97443**.

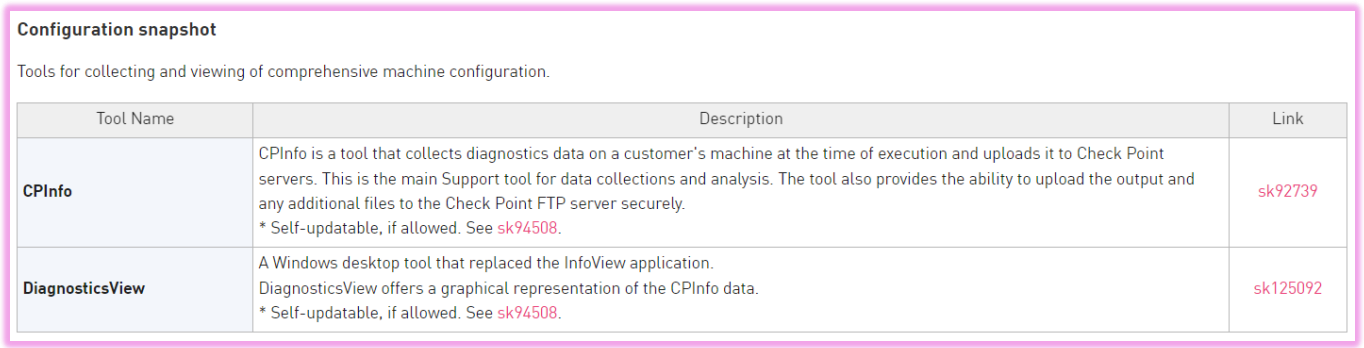

Solution ID: **sk97443** Technical Level: Basic Edit Email Print

Check Point Monitoring, Debug and Support Tools

| Product | Version | Platform | Last Modified |
|---|---|---|---|
| Other | R80 (EOL), R80.10 (EOL), R80.20 (EOL), R80.20.x, R80.20SP (EOL), R80.30 (EOL), R80.30SP (EOL), R80.40, R81, R81.10, R81.10.x, R81.20 | All | 2023-11-23 |

Fig.1 – Ferramentas de Monitoração, Debug e Suporte - sk97443

Uma delas que merece destaque é a CPInfo, pois é bastante conhecida e utilizada por todas as equipes de suporte. Esta ferramenta coleta e analisa dados dos equipamentos e o seu uso é recomendado quando da abertura de chamados no TAC da Check Point.


**Configuration snapshot**

Tools for collecting and viewing of comprehensive machine configuration.

| Tool Name | Description | Link |
|---|---|---|
| **CPInfo** | CPInfo is a tool that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers. This is the main Support tool for data collections and analysis. The tool also provides the ability to upload the output and any additional files to the Check Point FTP server securely.<br>* Self-updatable, if allowed. See sk94508. | sk92739 |
| **DiagnosticsView** | A Windows desktop tool that replaced the InfoView application.<br>DiagnosticsView offers a graphical representation of the CPInfo data.<br>* Self-updatable, if allowed. See sk94508. | sk125092 |

Fig.2 – CPInfo - sk97443 e 92739

## Por que o HCP – parte 2?

Este artigo complementa o documento HCP (HealthCheck Point) escrito por um outro colega da Check Point, que apresenta as características, procedimentos de instalação e o uso inicial de *assessment* do sistema.

Para você que não teve contato ainda com a ferramenta, é importante a leitura desta primeira parte. Contém também um vídeo que ajuda no entendimento. Veja o link (*post*):

**HealthCheck Point (HCP)**
https://community.checkpoint.com/t5/Portugu%C3%AAs/HealthCheck-Point-HCP/m-p/121549#M39

Importante salientar que após 2 (dois) anos a publicação mencionada acima, a ferramenta recebeu diversas novas capacidades, como  por exemplo, testes relacionados a *blade* de *Threat Prevention* e de integridade de interfaces Bond/LACP, dentre tantas outras.

E este incremento de testes demonstra e reforça a utilizazação da ferramenta como um aliado importante na gestão dos equipamentos Check Point.

Através dela é possível ser proativo em ações de melhoria, correção ou mitigação de riscos no ambiente.

E complementando com uma análise mais aprofundada destes parâmetros, tanto físicos quanto de software, estas ações ajudam a otimizar e manter a saúde e a performance da solução.

Portanto, os motivos para a parte 2 são:

1 - Complementar o artigo anterior, mostrando as **atualizações** na ferramenta;

2 – Estabelecer e reforçar **Boas Práticas** de Gestão dos sistemas, provendo relatórios para o devido acompanhamento de melhorias e correções;

3 – **Aprofundar** a análise em alguns parâmetros, explicando detalhadamente o seu funcionamento.

4 – E o principal ponto é **Aprimorar** a **Performance** dos gateways. Este documento servirá como base, para uma série de outros de como o entendimento da tecnologia Check Point pode melhorar o sistema.

## O que é HCP – *parte 2*?

O documento **atualizado** do **HCP** utiliza o **sk171436.**

Mas o **que é** o **HCP**?

O **HCP** é um conjunto de ferramentas **auto-atualizáveis** para:

- ***Tests***: Avalia a saúde e integridade do Sistema (Cluster, gateways, Management systems)
- ***WTS*** (*What's The Story*): Estabelece uma linha do tempo de eventos críticos e informacionais sobre o sistema, que ajudam a entender como determinado problema pode ter ocorrido
- ***Topology***: Visualização da topologia do equipamento (firewall)

Todas as versões Gaia a partir da **R80.10** são **suportadas**

Todas as versões Gaia a partir da R80.10 são suportadas.

## Tests:

Script de diagnóstico que executa um conjunto de testes. São mais de 70 itens analisados.

| Test name |
|---|
| SYSLOG timestamp |
| HTTPD SSL CONF FILE |
| Local Logging |
| Hardware Compatibility |
| Core Dumps |
| Software Version |
| Check Point Processes |
| Disk Space |
| ARP Cache Limit |
| APPI DB status |
| Local Address Port Usage |
| MTU |
| File Descriptors |
| Memory Usage |
| IPv4 forwarding |
| Interface Errors |
| Gaia DB |
| Kernel crash |
| vpnd process running |
| Transceivers Support |
| Soft lockup |
| ARP neighbour table overflow |
| SSD Health |
| Zombie processes |
| Hardware validation |
| Memory Leak Kernel Parameters |
| Dynamic Dispatcher status |
| Pattern Matcher Impact |
| Connection Distribution |
| System stressed |
| User space processes utilization |
| FW and PPACK communication CPAQ failures |
| SecureXL drops |
| CoreXL Affinity |
| FW instances drops |

| Test name |
|---|
| FW queues utilization |
| Traffic distribution |
| Dynamic Balancing |
| Cpu spikes[INFO] |
| IO wait |
| Heavy connections |
| Fragmentation rate |
| FW Connection balancing |
| Multiqueue |
| Network statistics |
| VPN test |
| Dmesg analysis[INFO] |
| Penalty box statistics |
| URL filtering |
| Static affinity |
| Ifconfig validation |
| User space processes affinity check |
| Blocker handlers check |
| Template efficiency |
| Bond - Traffic distribution |
| CPview Diagnostic |
| Connectivity to UC |
| SIC |
| FW Configuration copy File Sanity |
| Implied Rules |
| Global Connection Entries |
| Custom Applications RegEx |
| FW Configuration File Sanity |
| Debug flags - FW |
| Dynamic Objects Database |
| HyperFlow |
| Updatable Objects Package |
| SIM Configuration File Sanity |
| LightSpeed configuration check |
| Debug flags - fwaccel |
| SecureXL status |

Tab.1 – Conjunto de testes – sk171436

Os *Tests* analisam o sistema e podem detectar:

- **Práticas inadequadas** de **configuração** de recursos e do sistema
- **Prever problemas** futuros que podem afetar o sistema
- Problemas antigos que podem **ocorrer novamente**

Provê um relatório abrangente e estruturado de avaliação do sistema:

- Cada um dos testes informa um veredito: **Sucesso**, **Erro** e **Aviso**
- E para aqueles itens com falha, há a descrição detalhada recomendando atividades de correção.

## WTS (What's The Story)

Mostra de forma consolidada:

- Eventos, tanto críticos quanto informativos, ao longo do tempo.
- Combina eventos de vários processos e serviços em uma única linha do tempo
- Útil na solução de problemas (RCA, causa raiz) que afetaram o sistema, mas que não ocorrem mais

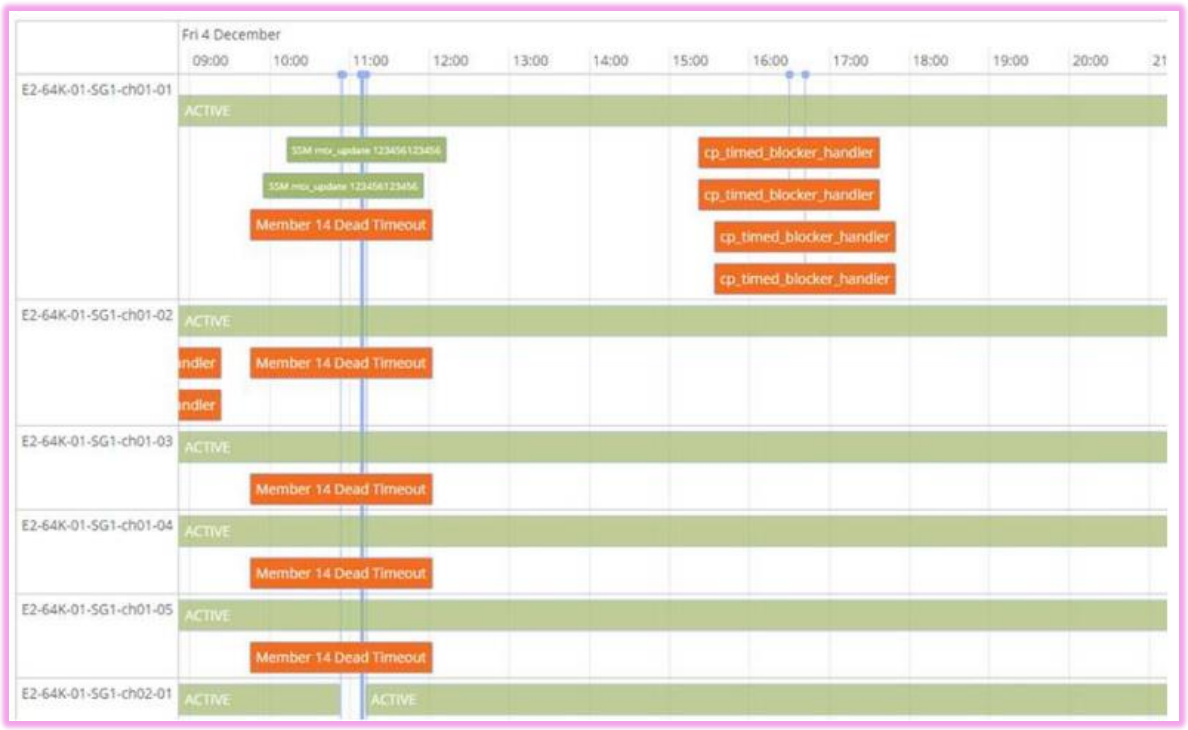



Fig.3 – Eventos na linha do tempo – sk171436

## Topology

Em qualquer momento, seja em fase de planejamento ou de troubleshooting, é importante ter uma visão clara de como o firewall está conectado, interfaces físicas, virtuais e endereçamento IPs.

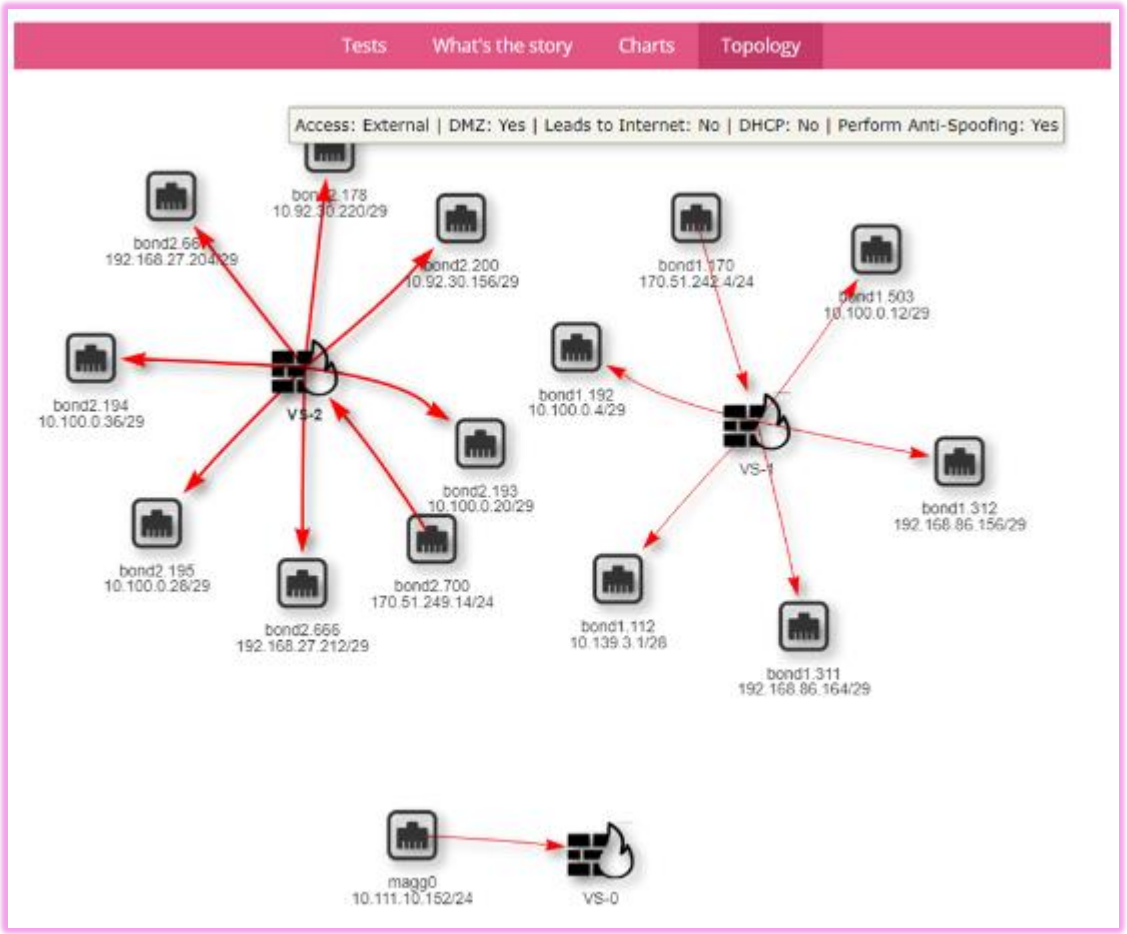



Fig.4 – Topologia – sk171436

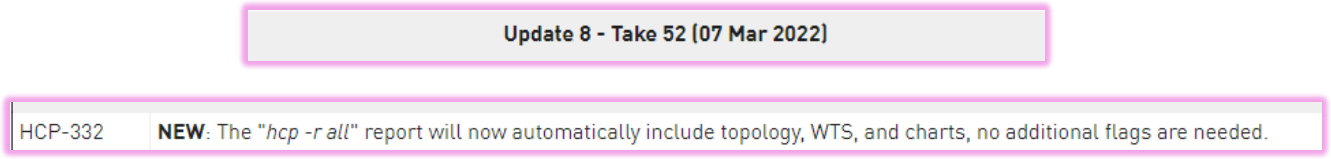
 

## Exemplos de Novas Funcionalidades no HCP

Importante a leitura das novas funcionalidades por atualizacão descritas no sk171436.

Seguem as descrições de 2 (duas) novas capacidades:

- O comando "**#hcp -r all**" inclui automaticamente a Topologia, WTS e os gráficos, sem a necessidade de inclusão de flags adicionais



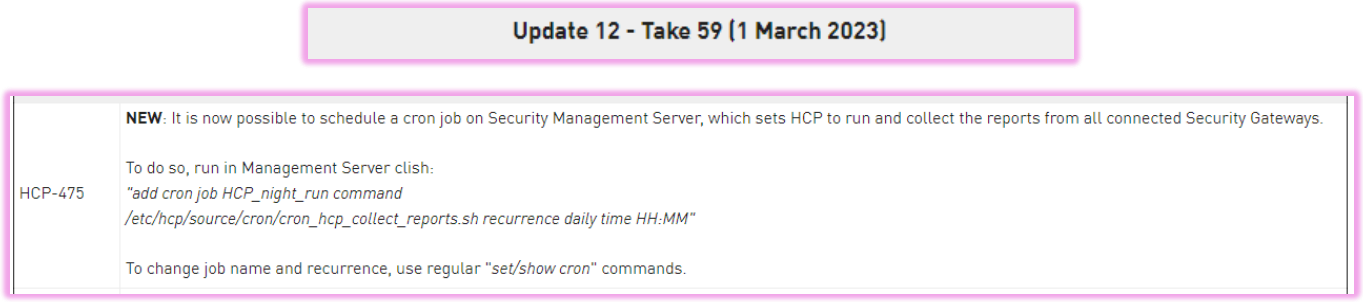
| Update 8 - Take 52 (07 Mar 2022) | |
|---|---|
| HCP-332 | **NEW**: The "*hcp -r all*" report will now automatically include topology, WTS, and charts, no additional flags are needed. |

Fig.5 – Comando HCP simplificado – sk171436

- É possível **automatizar** a execução do HCP para coletar os **relatórios** dos gateways. Deve-se executar o seguinte comando no modo *clish* na *Management Server*:

  "**#add cron job HCP_night_run command**

  **/etc/hcp/source/cron/cron_hcp_collect_reports.sh recurrence daily time HH:MM**"



| Update 12 - Take 59 (1 March 2023) | |
|---|---|
| HCP-475 | **NEW**: It is now possible to schedule a cron job on Security Management Server, which sets HCP to run and collect the reports from all connected Security Gateways.<br><br>To do so, run in Management Server clish:<br>*"add cron job HCP_night_run command*<br>*/etc/hcp/source/cron/cron_hcp_collect_reports.sh recurrence daily time HH:MM"*<br><br>To change job name and recurrence, use regular "*set/show cron*" commands. |

Fig.6 – Execução Automática do HCP – sk171436

## Visualizando os relatórios (Modo 1), executando o HCP diretamente no Gaia

O artigo anterior mostra em detalhes a execução e a visualização de relatórios através da descompactação do aquivo “**/var/log/hcp/last/hcp_last_report.tar.gz”**

## Visualizando os relatórios (Modo 2) através da SmartConsole

A **segunda** forma de **visualização** é através da instalação de uma extensão na SmartConsole.

Requisitos:

- Verificar se os pacotes HCP estão instalados, conforme artigo anterior
- Executar o comando “**#hcp -r all**” ao menos uma vez nos gateways

Acessar a ***Management Server*** e executar:

- “**#service hcp_ext start**”
- “**#hcp --ext-update-reports all**”

Acessar a SmartConsole e clicar em “**Manage&Settings > Preferences**”

Selecionar e clicar em “+” na opção da “SmartConsole Extension”

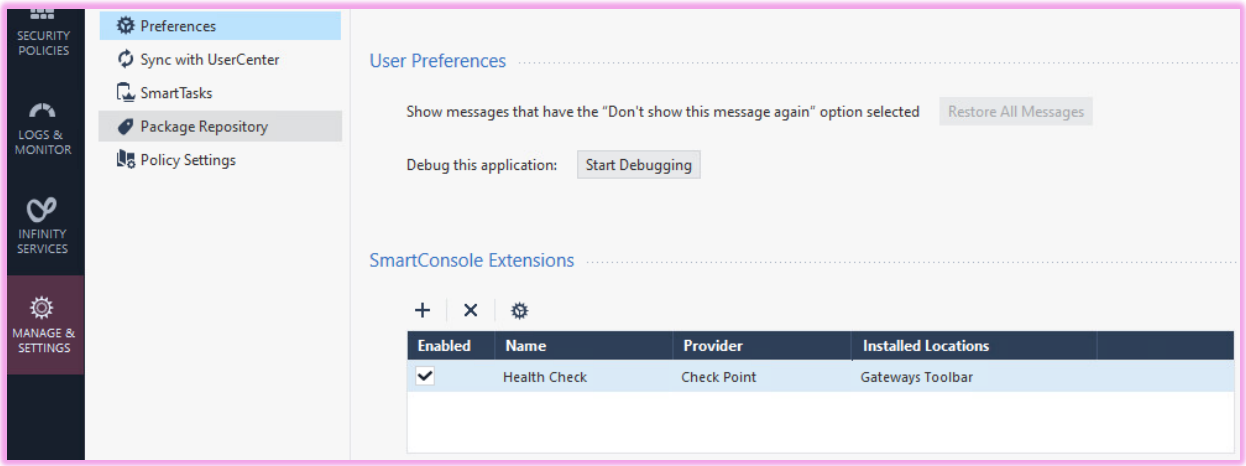



Fig.7 – Adicionando HCP na SmartConsole – sk171436

Insira na janela a seguinte URL:

**“https://<IP da Gerência>/ngm-management-app/hcp/extension.json**”

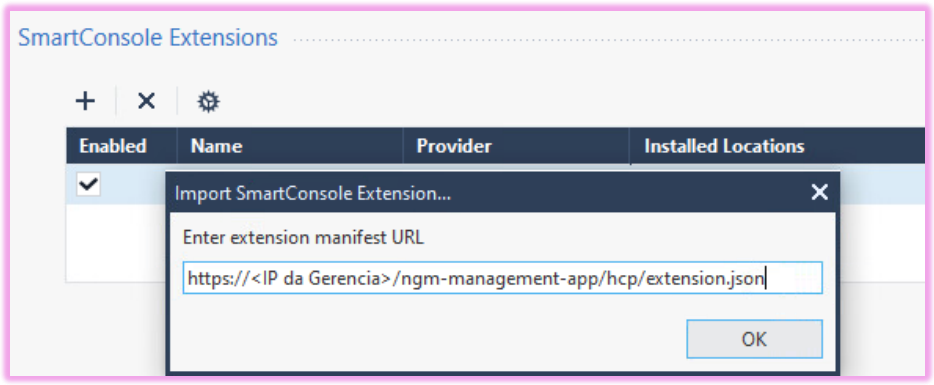



Fig.8 – Adicionando a extensão HCP na SmartConsole – sk171436

## Visualizando os relatórios (Modo 3) através do acesso direto ao gateway

A **terceira** forma de **visualização** é através do acesso direto ao dispositivo.

Acessar o relatório por um browser: “**https://<IP do Gateway >>/hcp”**

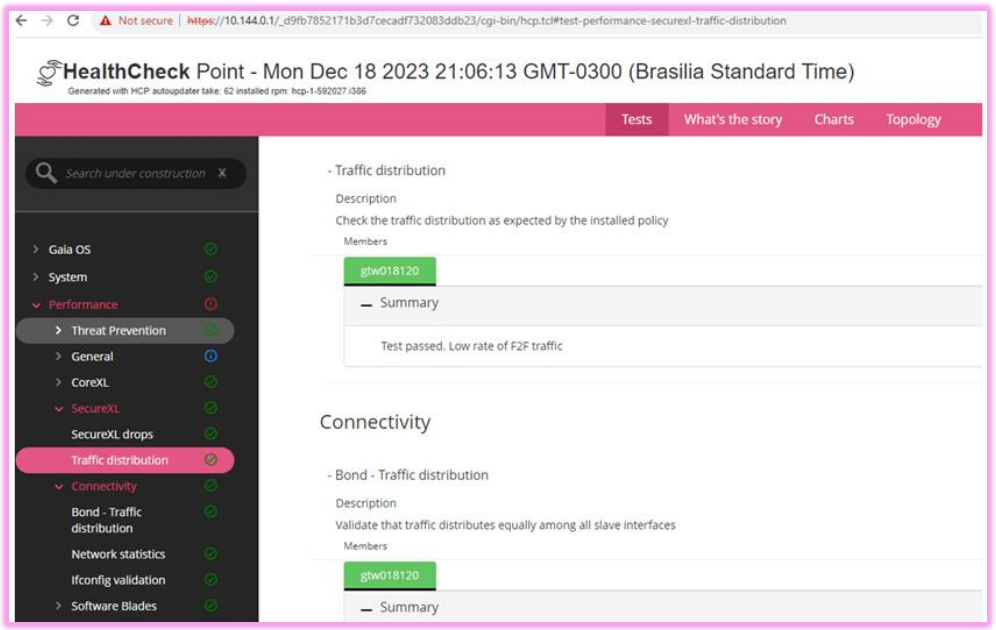



Fig.9 – Acessando relatório HCP diretamente nos equipamentos – sk171436

## Analisando o HCP

## Testes e Veredito

A figura a seguir apresenta alguns parâmetros testados contendo o veredito.

Utilizando uma abordagem *inicial* de focar nos itens com *Status* "***Failed***" ou até mesmo "***Skipped*** (Ignorado)", a ferramenta fornece ações para serem corrigidas e revisadas.

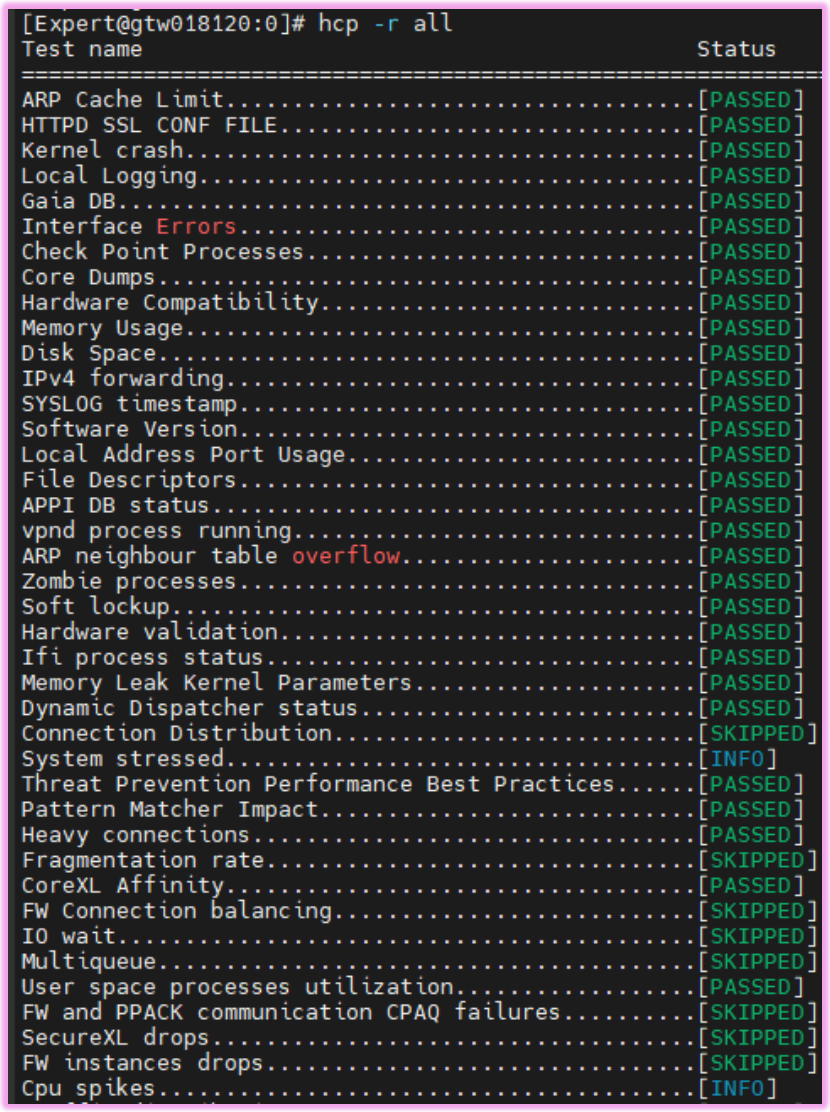



Fig.10 – Amostra de Testes do HCP – sk171436

## Exemplos de Testes - Consumo de espaço em disco

Um exemplo comum, é o consumo excessivo de espaço em disco que pode levar o gateway a apresentar problemas de performance. E a correção é tão simples quanto realizar o backup dos logs e depois a sua retirada, dentre outras ações.

Um dos testes que complementa este item é relacionado ao envio de logs para um “Log Server” e não armazenados localmente.

All file systems are in the right threshold.

| Disk File Systems | | | | |
|---|---|---|---|---|
| Filesystem | Used | Available | Used % | Mounted on |
| /dev/mapper/vg_splat-lv_current | 9.90 GB | 40.07 GB | 20% | / |
| /dev/sda2 | 0.06 GB | 0.21 GB | 24% | /boot |
| /dev/mapper/vg_splat-lv_log | 17.19 GB | 72.80 GB | 20% | /var/log |
| tmpfs | 0.01 GB | 3.76 GB | 1% | /dev/shm |

Fig.11 – Teste de espaço em disco – sk171436

Summary

| Log Servers Connections | | |
|---|---|---|
| IP Address | Description | Status |
| 10.144.0.220 | Log-Server Connected | Connected |

Logs are written to log server

Fig.12 – Teste de envio de logs ao Log Server – sk171436

## Exemplos de Testes - Integridade de Interface Bond

Em outros testes, há necessidade de uma análise mais ampla. E em alguns casos com envolvimento do responsável pelo ambiente.

Por exemplo, o teste a seguir relacionado a Bond, apesar de ser simples, foi ignorado por não encontrar este tipo de interface configurado no sistema.

Cabem algumas perguntas de revisão de *design*:

1 – O ambiente é crítico? Sendo crítico, não seria importante ter redundância de interfaces para um determinado segmento e assim criar um Bond, agregando mais de uma interface física?

2 – A Interface é capaz de suportar uma demanda maior, mesmo que não seja constante?

3 – Existem problemas de lentidão nas aplicações? Há reclamações de usuários em todo final de mês (ou outro período)?

4 – E se por acaso existir uma interface Bond, o tráfego é de fato distribuído em todas elas? Verifiquem a configuração também nas interfaces dos switches diretamente conectados aos gateways.

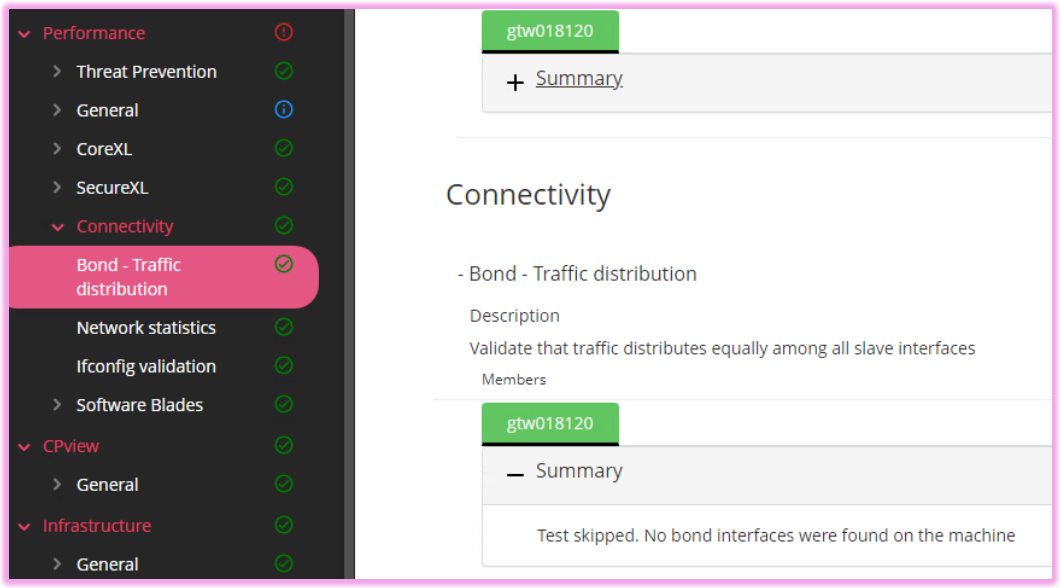



Fig.13 – Teste de Interface Bond - HCP – sk171436

## Exemplos de Testes - Performance das CPUs

O gateway testado apresenta baixo consumo de CPU, tanto para SND quanto para FW (figura 14).

De forma bem resumida:

SND é responsável pelo processamento do tráfego de entrada na interface de rede, distribuindo os pacotes *não acelerados* para as instâncias de FW, e,

FW é responsável pela aplicação da política de segurança ao tráfego.

Observar que o SND também aplica política de segurança quando o SecureXL está habilitado, tema que será aprofundado em um tópico específico deste artigo.

Verificar o **sk98737** para entendimento dos conceitos e detalhes sobre o CoreXL (SND, FW).

Neste exemplo, há um ponto de atenção relacionada a distribuição das instâncias de SNDs e FW. As CPUs 0 e 1 possuem ambas as instâncias SNDs e FW.

Por recomendação, deve-se separar tais instâncias. O **sk98737** mostra detalhes para otimizar performance no uso das CPUs.

— Summary

| CPU Utilization | | | |
|---|---|---|---|
| Test | Expected | Actual | Result |
| FW Average Usage | <70% | 2.5 | Passed |
| SND Average Usage | <70% | 2.5 | Passed |

— Finding #1

**Description**
SNDs and FWs affinity issue
**Suggested Solution**
**Solution #1**
It appears that CPUs {0, 1} have both SND & FW affined to them, please contact TAC for further assistance

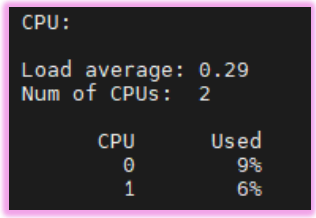
Fig.14 – Teste CPUs, SND e FW - HCP – sk98737

| Number of CPU cores | Default number of CoreXL IPv4 FW instances | Default number of Secure Network Distributors (SNDs) |
|---|---|---|
| 1 | 1<br>Note: CoreXL is disabled | 0<br>Note: CoreXL is disabled |
| 2 | 2 | 2 |
| 4 | 3 | 1 |
| 6 - 20 | [Number of CPU cores] - 2 | 2 |
| More than 20 [1] | [Number of CPU cores] - 4 | 4 |

Fig.15 – Configuração padrão para instâncias SND e FW – CoreXL sk98737

Como se observa na figura a seguir, o equipamento com 2 (duas) CPUs possui SND e FW em ambas CPUs, o que está de acordo com a tabela da figura 15.



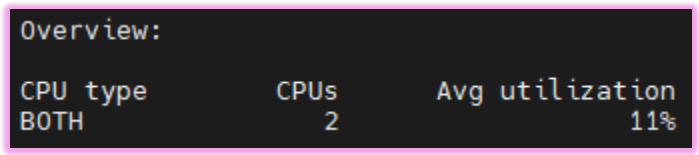




Fig.16 – Distribuição das instâncias SND e FW em um gateway com 2 CPUs

Ao passar para um cenário de maior complexidade, como por exemplo um equipamento com 32 CPUs (figura 17), surge o questionamento – “Como realizar a distribuição e ajustar o processamento ao perfil de trafego?”

Existe uma funcionalidade chamada “***Dynamic Balancing for CoreXL***”, **sk164155** presente desde a versão R80.40, que permite o balanceamento dinâmico das instâncias SNDs e FW, ou seja, altera de forma automática a quantidade de SNDs e FW se ajustando às mudanças de distribuição de tráfego.

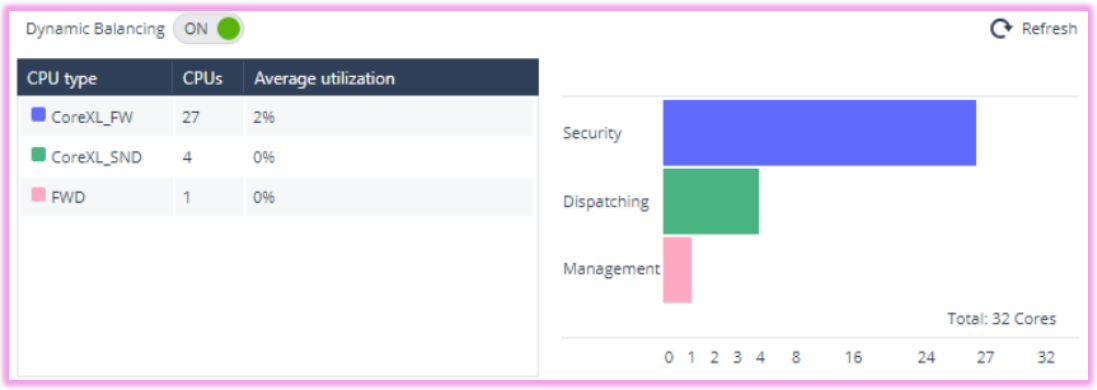



Fig.17 – Distribuição das instâncias SND e FW em um gateway com 32 CPUs - sk164155

Neste mesmo equipamento, há uma CPU dedicada (FWD) para “*Management*” – Gerenciamento. Esta funcionalidade chamada de **MDPS** (Management Data Plane Separation (MDPS) permite isolamento das redes de dados e de gerência, incluindo interfaces, rotas, sockets e processos.

Esta capacidade permite acessar o equipamento em momentos de alto consumo, garantindo a operacionalidade, gerenciamento e coleta de dados.

Existem comandos específicos para configuração que podem encontrados no **sk138672**. Então temos duas otimizações que podem ser utilizadas neste mesmo gateway.

## Otimizando Peformance - (SecureXL)

## Testes do SecureXL

Os testes do HCP mostram alguns resultados sobre o SecureXL (figuras 18 e 19)

Surgem algumas questões:

- O que significa exatamente tráfego “F2F”?
- Existem outros tipos de tráfego, além do “F2F”?
- O teste mostrou status “*Passed*”, por apresentar baixa taxa de tráfego “F2F“. Este valor é absoluto, é baseado em volume (mbps)? É baixo quando comparado com outro tipo de tráfego, ou seja, depende de uma referência? Qual referência?
- O que fazer caso encontremos algum problema?
- Existem Melhores Práticas?

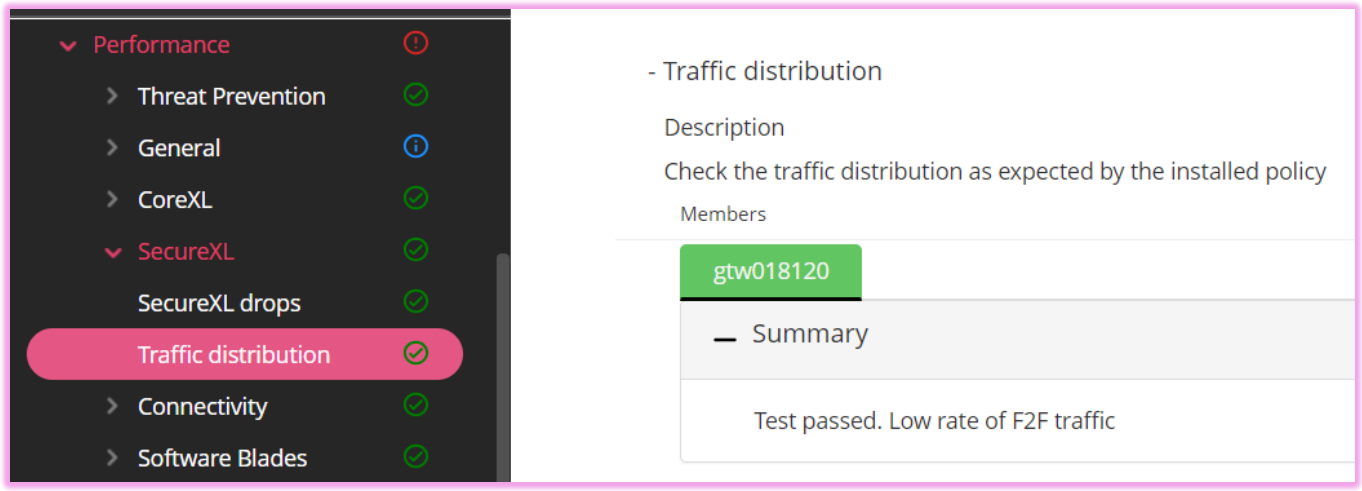



Fig.18 – Teste de SecureXL - Distribuição de tráfego F2F - sk153832

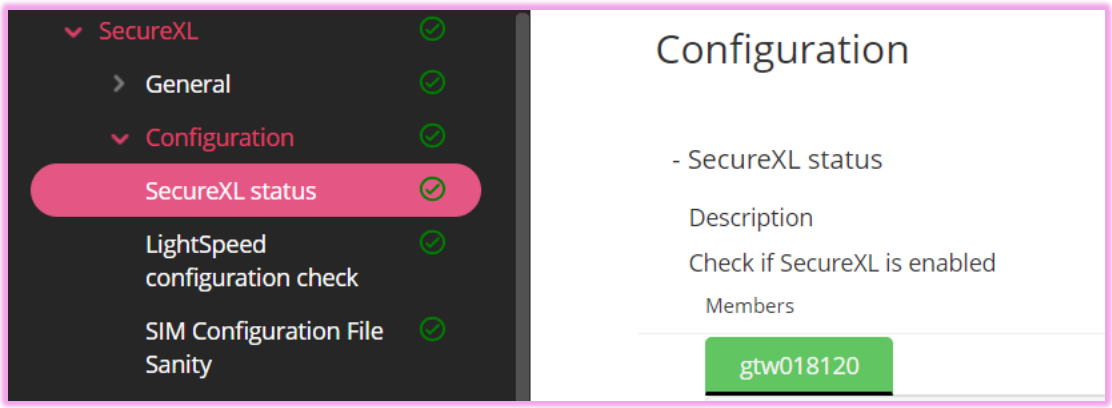



Fig.19 – Teste de status do SecureXL – habilitado - sk153832

## O que é SecureXL?

O SecureXL é uma solução de aceleração de processamento em software instalado nos gateways.

As técnicas implementadas permitem um desempenho da velocidade em “*wire-speed*”.

É suportado nos seguintes sistemas operacionais:

- Gaia OS
- Gaia Embedded OS
- SecurePlatform OS
- SecurePlatform Embedded OS
- IPSO OS
- Crossbeam XOS
- Crossbeam COS

O SecureXL pode ser utilizado com outras funcionalidades de otimização, como:

- CoreXL
- SMT (HyperThreading)
- Multi-Queue
- ClusterXL

Para aumentar a taxa de estabelecimento de conexões, o SecureXL tenta "agrupar" todas as conexões que correspondem a um determinado serviço e cujo único elemento discriminador é a Porta de Origem.

Este tipo de "agrupamento" permite que até mesmo os primeiros pacotes de um *handshake* TCP sejam acelerados. Isto é muito útil para conexões curtas, nas quais a porcentagem de tráfego de *handshake* TCP é muito alta.

Os primeiros pacotes da primeira conexão do mesmo serviço serão encaminhados para o *kernel* do gateway, que então cria um “*template*” da conexão e notificará o mecanismo SecureXL. Quaisquer conexões TCP subsequentes estabelecidas no mesmo serviço (onde apenas a porta de origem é diferente) já serão aceleradas (assim como qualquer outro tráfego).

Então a criação dos “*templates*” é fundamental no processo do SecureXL.

Desta forma, tem-se por exemplo o “*Accept templates*”. Quando uma nova conexão se encaixa no “*Accept template*”, as conexões subsequentes são estabelecidas sem realizar uma correspondência de regras e, portanto, são aceleradas. Atualmente, a aceleração é executada apenas em conexões com a mesma porta de destino (usando * (*wildcards*) para portas de origem).

A figura 20 ajuda a entender o processo de decisões para cada etapa do fluxo de pacotes.

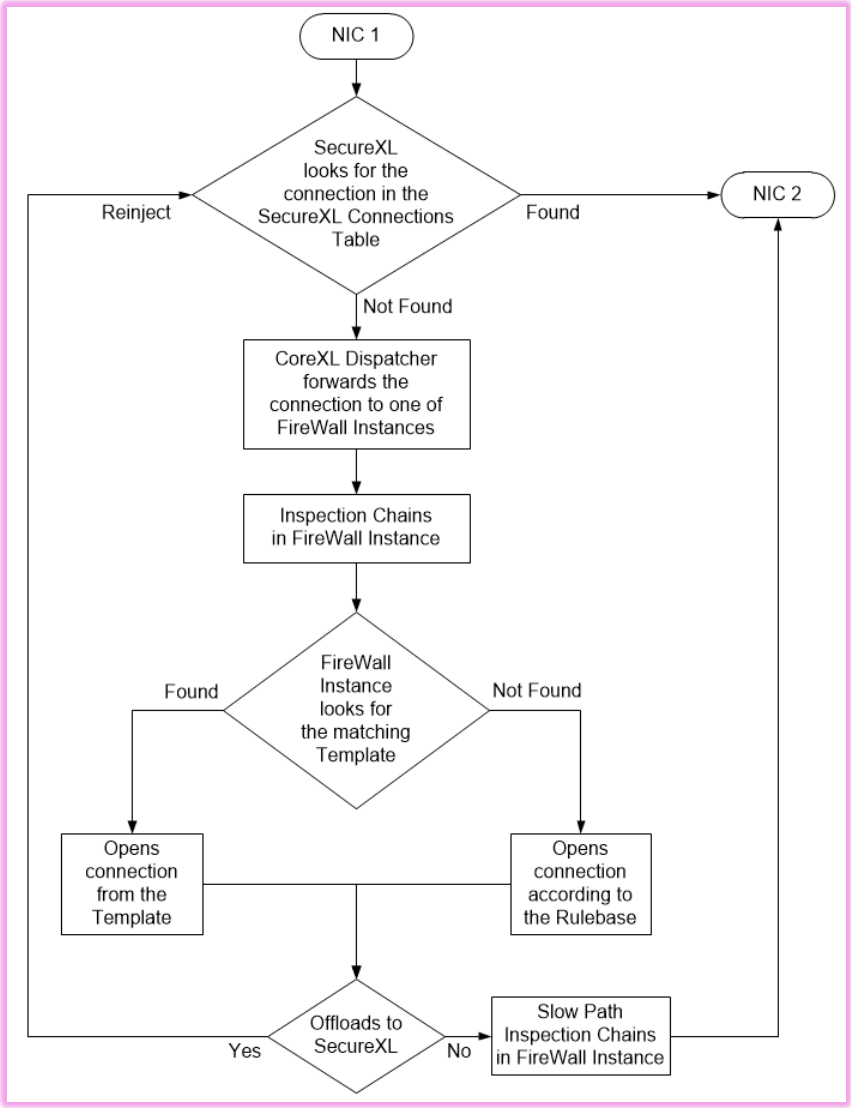



Fig.20 – Fluxo do pacote - SecureXL – habilitado - sk153832

O SecureXL é uma das teconologias inovadoras que juntamente com outras técnicas de aceleração de rede fazem parte do "*Performance Pack*", que é implementado tanto em software quanto em hardware.

O comando abaixo mostra se o "*Performance Pack*" está habilitado, funcionalidades e os "*templates*":

"*#fwaccel stat*"

Se estiver desabilitado, basta:

"*#fwaccel on*"

```
[Expert@gtw018120:0]# fwaccel stat
+-------------------------------------------------------------------------------+
|Id|Name     |Status     |Interfaces              |Features                      |
+-------------------------------------------------------------------------------+
|0 |KPPAK    |enabled    |eth0,eth1               |Acceleration,Cryptography     |
|  |         |           |                        |                              |
|  |         |           |                        |Crypto: Tunnel,UDPEncap,MD5,  |
|  |         |           |                        |SHA1,3DES,DES,AES-128,AES-256,|
|  |         |           |                        |ESP,LinkSelection,DynamicVPN, |
|  |         |           |                        |NatTraversal,AES-XCBC,SHA256, |
|  |         |           |                        |SHA384,SHA512                 |
+-------------------------------------------------------------------------------+

Accept Templates : enabled
Drop Templates   : disabled
NAT Templates    : enabled
LightSpeed Accel : disabled
```

Fig.21 – Status do SecureXL - sk153832

## Trajetos ("*Paths*")

Portanto, ao utilizar "*templates*", "*Performance Pack*" e o CoreXL habilitado tem-se a distribuição de trajetos dos pacotes dentro do processamento do gateway, conforme figura 22.

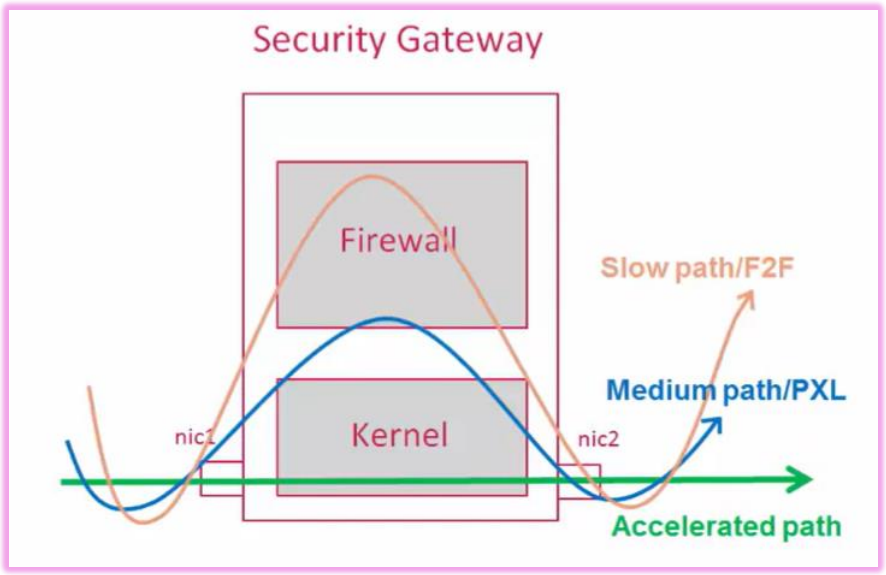



Fig.22 – Trajetos ("*Paths*") do SecureXL - sk153832

Desta forma, tem-se os seguintes "*Paths*" e descrição mais aprofundada do CoreXL:

**"*Accelerated Path (SXL)*"** – o fluxo de pacotes é completamente manipulado pelo mecanismo SecureXL, processado e direcionado para a rede. Utiliza o CoreXL SND.

**"*Medium Path (PXL)*"** – o fluxo de pacotes é manipulado pelo mecanismo SecureXL, exceto para algumas blades. O CoreXL SND envia o pacote para uma das instâncias do CoreXL FW para realizar o processamento.

**"*Firewall path/Slow path (F2F Path)*"** – o fluxo de pacotes é manipulado pelo mecanismo CoreXL FW. Ou seja, o mecanismo SecureXL não consegue processar o pacote (consulte o sk32578 - Mecanismo SecureXL).

**"*SND (Secure Network Distributor)*"** – Distribui as conexões para os CoresXL FW. Também é usado como *buffer* para o processamento dos frames através de "hadware interrupts (IRQ e SoftIRQ) e inspeciona o tráfego, conhecido como *totalmente acelerado* ("*Accelerated Path*", "*SXL Path*").

**"*Firewall Worker Core (FW)*"** – Processa as conexões parcialmente aceleradas ("*PXL – partially-accelerated*") como também aplica as regras. Algumas vezes chamado como "Instance Kernel" ou "Inspect Engine".

## Referências por Trajetos ("*Paths*")

O comando abaixo mostra a distribuição de tráfego para cada um dos "*Path*" em determinado gateway

"*#fwaccel stats -s*"

```
[Expert@gw-3900f9:0]# fwaccel stats -s

Accelerated conns/Total conns : 175/875 (20%)
Accelerated pkts/Total pkts   : 2090/10450 (20%)
F2Fed pkts/Total pkts   : 1045/10450 (10%)
PXL pkts/Total pkts   : 7315/10450 (70%)
QXL pkts/Total pkts   : 0/10450 (0%)
```

Fig.23 – Distribuição das conexões pelos Trajetos ("*Paths*") do SecureXL

Analisando cada item, tem-se a seguinte distribuição:

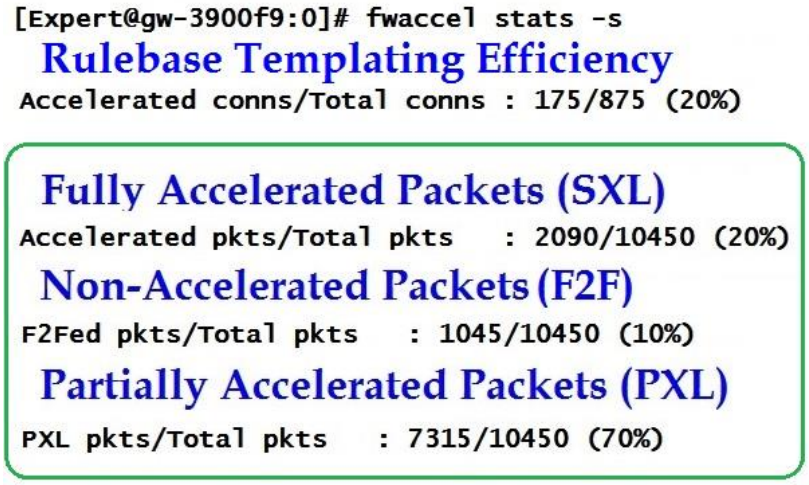



Fig.24 – Identificação dos Trajetos ("*Paths*") do SecureXL

Normalmente pode-se utilizar como *benchmark*, os seguintes percentuais:

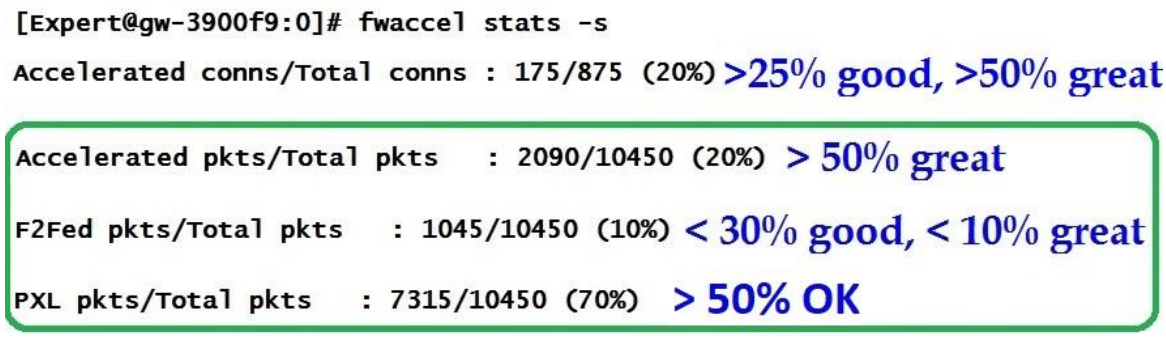



Fig.25 – Referências de Otimização por Trajeto ("*Paths*") do SecureXL

A maior parte do tráfego em um datacenter tende a utilizar *PXL*. E não muito raro encontrar valores acima de 75%.

Portanto, o objetivo de ajuste fino para o SecureXL segue uma ordem de prioridade em termos de aceleração: *SXL > PXL > F2F*. E estes ajustes dependem do perfil e do tipo de tráfego. Por isso é importante entender e analisar o tráfego do ambiente.

E em alguns casos, a aceleração pode ser desabilitada por uma regra que possua um das características relacionadas no sk32578 - SecureXL Mechanism.

O cenário a seguir demonstra como identificar a causa quando a criação do "Accept Template" é desabilitada.

No caso, a regra #2 de firewall desabilita a funcionalidade.

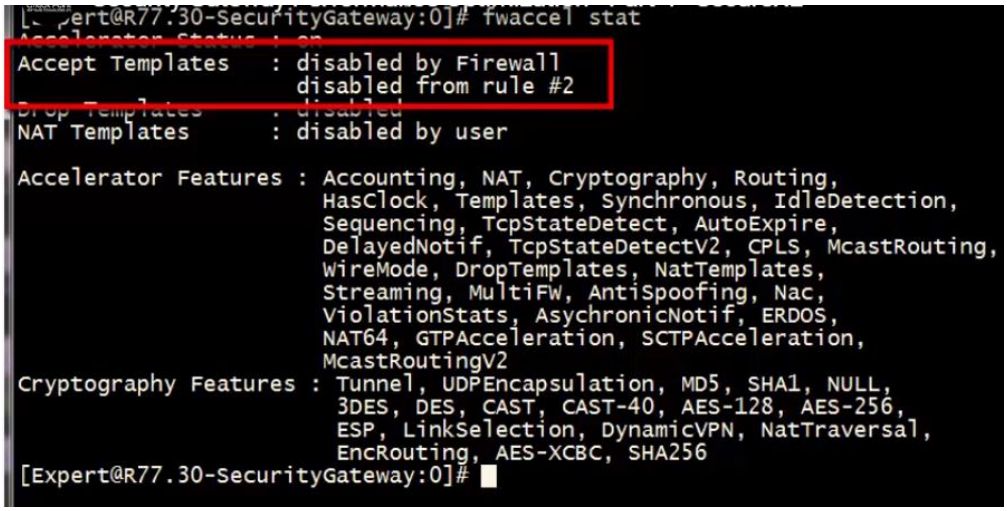



Fig.26 – Aceleração desabilitada por uma regra do Firewall (exemplo)

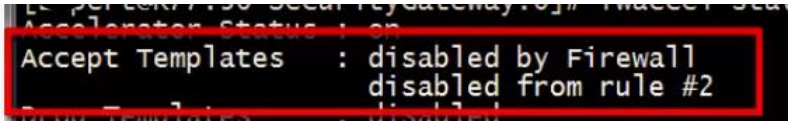



Fig.27 – Regra #2 desabilita aceleração (exemplo)

O próximo passo é analisar a regra #2 do firewall e verificar qual serviço ou condição afeta a performance.

| No. | Hits | Name | Source | Destination | VPN | Service | Action | Track |
|---|---|---|---|---|---|---|---|---|
| 2 | 7 | | Net_192.168.11<br>Net_10.31.31.0 | Any | Any Traffic | DCOM-IRemUn<br>DCOM-System/<br>AD_Dcerpc_sen | accept | Log |

Fig.28 – Regra #2 da política de firewall

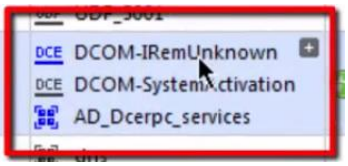



Fig.29 – Serviço DCOM dentro da Regra #2 da política de firewall

O serviço DCOM desabilita "*Accept Templat*e", conforme sk32578.

Desta forma, como ação de otimização e remediação, recomenda-se que todas as regras que podem ser agrupadas dentro de um "template", devam ser colocadas no topo (a menos que viole outras considerações de otimização).

E as regras que não conseguem ser agrupadas devem ser colocadas na base. Neste exemplo, a regra #2 deve ser colocada o mais próximo possível da regra de *cleanup*.

## Sumário

A ferramenta HCP permite ter uma visão sobre a integridade e a performance dos gateways. É possível obter indicadores para a gestão do processo de melhoria contínua, permitindo a implementação das melhores práticas no ambiente.

O aprofundamento na análise destas funcionalidades de otimização Check Point, como o SecureXL, mostra a flexibilidade de ajustes dos gateways de acordo com os perfis de tráfego que podem mudar com certa frequência. Os motivos destas mudanças podem ser os mais diversos, como aquisição ou consolidação de datacenters, mudança de local de trabalho dos profissionais ou mesmo novas aplicações. Como o foco é o ajuste por meio de software, a eficiência na perfomance se sobressai mais ainda, principalmente quando a solução é aplicada em ambientes de cloud, onde o hadware é de responsabilidade do provedor de cloud.

Portanto, ao realizar avaliações constantes no ambiente é possível minimizar riscos, garantir a integridade e uma melhor performance da solução. E os resultados para o usuário podem variar desde uma melhor experiência no uso da aplicação (sem latência), suportar momentos de alto uso (campanhas ou simplesmente atualizações que usam alto volume de tráfego como aquelas realizadas para endpoint) como também obter uma maior capacidade de uso dos equipamentos.

## Referências


sk97443 - Check Point Monitoring, Debug and Support Tools
https://support.checkpoint.com/results/sk/sk97443

sk171436 - HealthCheck Point (HCP) Release Updates
https://support.checkpoint.com/results/sk/sk171436

CheckMates - HealthCheck Point (HCP)
https://community.checkpoint.com/t5/Portugu%C3%AAs/HealthCheck-Point-HCP/m-p/121549#M39

sk153832 - ATRG: SecureXL for R80.20 and higher
https://support.checkpoint.com/results/sk/sk153832

sk32578 - SecureXL Mechanism
https://support.checkpoint.com/results/sk/sk32578

sk98348 - Best Practices - Security Gateway Performance
https://support.checkpoint.com/results/sk/sk98348

sk98737 – ATRG: CoreXL
https://support.checkpoint.com/results/sk/sk98737

Performance Best Practices - Video 4 - SecureXL, Part 1
https://community.checkpoint.com/t5/Check-Point-for-Beginners/Video-4-SecureXL-Part-1/ba-p/88588?cat=1

CheckMates - Performance Optimization Intro West US Introduction Oct 2023
https://community.checkpoint.com/t5/Western-US/Performance-Optimization-Intro-West-US-Introduction-Oct-2023/m-p/194343

CheckMates - TechTalk: Security Gateway Performance Optimization with Tim Hall
https://community.checkpoint.com/t5/General-Topics/TechTalk-Security-Gateway-Performance-Optimization-with-Tim-Hall/m-p/29833