# Table of Contents

**TABLE OF CONTENTS** ........................................................................................................... 2  
**EXECUTIVE SUMMARY** ...................................................................................................... 4  
  Network Diagram .................................................................................................................. 4  
**MANAGEMENT REVIEW** ................................................................................................... 5  
  Hotfix ....................................................................................................................................... 6  
  Licenses and Contracts .......................................................................................................... 6  
  Object Database ....................................................................................................................... 6  
  Unassigned Policies .............................................................................................................. 6  
  Session Timeouts ................................................................................................................... 7  
  Out of State ............................................................................................................................ 7  
  Disk Usage ............................................................................................................................... 8  
  Memory Usage ....................................................................................................................... 8  
  CPU Usage ............................................................................................................................... 9  
  IO Wait ..................................................................................................................................... 9  
  Local Users ............................................................................................................................ 11  
  SNMP ...................................................................................................................................... 11  
  IPS - Server Configuration ..................................................................................................... 11  
  Blade Updates ....................................................................................................................... 12  
  Online Web Services - Threat Prevention ............................................................................ 12  
  Implied Rules .......................................................................................................................... 13  
  Hit Count Database ............................................................................................................... 14  
**CLUSTER1 CLUSTER REVIEW** .......................................................................................... 15  
  Hotfix ....................................................................................................................................... 16  
  NAT Cache .............................................................................................................................. 16  
  Misplaced Rules ..................................................................................................................... 16  
  VOIP ....................................................................................................................................... 16  
  Snapshot/Backup .................................................................................................................... 17  
  AAA ........................................................................................................................................ 17  
  Interface Buffers .................................................................................................................... 17  
  Fragments ............................................................................................................................... 17  
  Sync ........................................................................................................................................ 18  
  Zombie Processes .................................................................................................................. 18  
  Weak Ciphers ........................................................................................................................ 18  
  SNMP Version ....................................................................................................................... 19  
  HA State .................................................................................................................................. 19  
  Logging ................................................................................................................................... 19  
  Anti-Spoofing ........................................................................................................................ 20  
  Drop Templates ..................................................................................................................... 21  
  NTP .......................................................................................................................................... 22  
  ARP ......................................................................................................................................... 22  
  Stealth ..................................................................................................................................... 23  
**VSXCLUSTER2 CLUSTER REVIEW** ....................................................................................... 24  
**VS0** ...................................................................................................................................... 26  
  Hotfix ....................................................................................................................................... 26  
  CoreXL .................................................................................................................................... 26  
  NAT ......................................................................................................................................... 26  
  SNMP Version ........................................................................................................................ 26

Consultant Report

© 2019 Check Point Software Technologies Ltd. All rights reserved. | Classification: [Customer Confidential] — For customer use only | Page | 2
SNMP Mode .................................................................................................................. 27
Disk Usage .................................................................................................................. 27
Core Dumps .................................................................................................................. 27
AAA ............................................................................................................................. 27
Weak Ciphers .............................................................................................................. 28
Sync .............................................................................................................................. 28
ARP .............................................................................................................................. 29
NTP .................................................................................................................................. 30
Resource - CoreXL ..................................................................................................... 30
Logging .......................................................................................................................... 30
Stealth ........................................................................................................................... 31

VS1 – VS-XXA ............................................................................................................ 31
IPS Profile .................................................................................................................... 31
Application Control Policy .......................................................................................... 32
Policy Types ................................................................................................................ 32
NAT Connections ....................................................................................................... 33
Internet Connectivity .................................................................................................. 33
Misplaced Rules .......................................................................................................... 34
Fragments ..................................................................................................................... 34
Stealth .......................................................................................................................... 34

VS2 – VS-XXB ............................................................................................................ 35
Application Control Policy .......................................................................................... 35
Policy Types ................................................................................................................ 35
Old UDP Sessions ....................................................................................................... 36
Misplaced Rules .......................................................................................................... 36
NAT Connections ....................................................................................................... 37
Fragments ..................................................................................................................... 37
Stealth .......................................................................................................................... 38

VS8 – VS-XXC ............................................................................................................ 38
All ................................................................................................................................... 38

Consultant Overview .................................................................................................. 39
Disclaimer ..................................................................................................................... 40

Post Project Contact Information .............................................................................. 40
Executive Summary

Check Point Professional Services have been engaged to run a Health Check to ensure the following devices are installed to Check Point best practices and optimized.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Name</th>
<th>Cluster</th>
<th>Version</th>
<th>Jumbo</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Virtual Platform</td>
<td>fw1-management</td>
<td>Cluster1</td>
<td>R80.10</td>
<td>Take 91</td>
</tr>
<tr>
<td>VMware Virtual Platform</td>
<td>FW1</td>
<td>Cluster1</td>
<td>R80.10</td>
<td>Take 112</td>
</tr>
<tr>
<td>VMware Virtual Platform</td>
<td>FW2</td>
<td>Cluster1</td>
<td>R80.10</td>
<td>Take 112</td>
</tr>
<tr>
<td>Check Point 23800</td>
<td>vsx-1</td>
<td>VSXCluster2</td>
<td>R80.10</td>
<td>Take 103</td>
</tr>
<tr>
<td>Check Point 23800</td>
<td>vsx-2</td>
<td>VSXCluster2</td>
<td>R80.10</td>
<td>Take 103</td>
</tr>
</tbody>
</table>

The Health Check includes Summary Reports, Health Check Reports and any supporting documentation. This Consultant Report will summarize the findings and highlight any concerns or recommendations.

<customer> have also requested a review on network design.

Network Diagram
<removed>
Management Review

The following findings have been identified on the R80.10 Security Management Server (fw1-management):

<table>
<thead>
<tr>
<th>Topic</th>
<th>Status</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotfix</td>
<td>✗</td>
<td>Old version of JHF installed with known issues.</td>
</tr>
<tr>
<td>Licenses &amp; Contracts</td>
<td>⚠</td>
<td>Number of expired licenses and contracts.</td>
</tr>
<tr>
<td>Object Database</td>
<td>✗</td>
<td>High amount of unused and duplicate objects.</td>
</tr>
<tr>
<td>Unassigned Policies</td>
<td>✗</td>
<td>50% of policies are unassigned + increasing object count.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>⚠</td>
<td>Default values increased.</td>
</tr>
<tr>
<td>Out of State</td>
<td>✗</td>
<td>TCP out of state allowed. Security concern.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>⚠</td>
<td>85% disk usage.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>i</td>
<td>Swapping.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IO Wait</td>
<td>i</td>
<td>Above expected value.</td>
</tr>
<tr>
<td>Local Users</td>
<td>✗</td>
<td>Improvement to prevent unauthorized access.</td>
</tr>
<tr>
<td>SNMP</td>
<td>✗</td>
<td>Disabled.</td>
</tr>
<tr>
<td>IPS – Server Config</td>
<td>⚠</td>
<td>Servers not defined.</td>
</tr>
<tr>
<td>Blade Updates</td>
<td>⚠</td>
<td>Incorrect warnings.</td>
</tr>
<tr>
<td>Online Web Service</td>
<td>✗</td>
<td>Set to Background.</td>
</tr>
<tr>
<td>Implied Rules</td>
<td>⚠</td>
<td>Logging implied rules.</td>
</tr>
<tr>
<td>Hit Count Database</td>
<td>⚠</td>
<td>Many unused rules.</td>
</tr>
</tbody>
</table>

Each recommendation is rated as follows:

- Serious - Needs immediate attention
- Attention - Needs attention
- Good - No need for any action
- Informational
Hotfix

**R80.10 Jumbo Hotfix Accumulator** is an accumulation of stability and quality fixes resolving multiple issues in different products.

A backup taken from the installed take 91 will not restore correctly. Sk123352

Recommended to install the latest jumbo to enhance feature set and improve stability.

Note: the latest Jumbo includes an updated SmartConsole. Post install of the Jumbo ensure that the latest SmartConsole is installed on all GUI clients.

Licenses and Contracts

The license repository contains a number of expired licenses and contracts.

<table>
<thead>
<tr>
<th>License</th>
<th>3 out of 27 licenses are expired.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract</td>
<td>14 out of 51 contracts are expired.</td>
</tr>
</tbody>
</table>

Object Database

The environment has a high number of duplicate and unused objects. The high number of duplicate objects is a concern; on policy push all used objects are verified. Remediating the duplicate objects would greatly improve policy push times.

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
<th>Percent</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Network Objects</td>
<td>✓4638</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Unused Network Objects</td>
<td>✗966</td>
<td>20.83%</td>
<td>Consider deleting these objects.</td>
</tr>
<tr>
<td>Duplicate Network Objects</td>
<td>✗3162</td>
<td>68.18%</td>
<td>Consider deleting copies.</td>
</tr>
<tr>
<td>Nested Network Objects</td>
<td>✓41</td>
<td>0.88%</td>
<td></td>
</tr>
<tr>
<td>Total Services Objects</td>
<td>✓1283</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Unused Services Objects</td>
<td>✗208</td>
<td>16.21%</td>
<td>Consider deleting these objects.</td>
</tr>
<tr>
<td>Nested Services Objects</td>
<td>✗26</td>
<td>2.03%</td>
<td></td>
</tr>
</tbody>
</table>

A separate object report will be provided to identify duplicate and unused objects.

Unassigned Policies

Removing the unassigned policies eliminates the possibility for human error but more importantly, increases the amount of unused objects and allowed a greater potential for object database cleanup.

| Policies Assigned | 5 out of 10 policies are not assigned. |
Session Timeouts
The default timeouts have been changed. Extending the session timeouts increase the gateway connection table utilizing additional memory.

<table>
<thead>
<tr>
<th>&lt;customer&gt; Values</th>
<th>Default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Session Timeouts</td>
<td>TCP start timeout:</td>
</tr>
<tr>
<td>TCP start timeout:</td>
<td>TCP session timeout:</td>
</tr>
<tr>
<td>TCP session timeout:</td>
<td>TCP end timeout:</td>
</tr>
<tr>
<td>TCP end timeout:</td>
<td>UDP virtual session timeout:</td>
</tr>
<tr>
<td>UDP virtual session timeout:</td>
<td>ICMP virtual session timeout:</td>
</tr>
<tr>
<td>ICMP virtual session timeout:</td>
<td>Other IP protocols virtual session timeout:</td>
</tr>
<tr>
<td>Other IP protocols virtual session timeout:</td>
<td>SCTP start timeout:</td>
</tr>
<tr>
<td>SCTP start timeout:</td>
<td>SCTP session timeout:</td>
</tr>
<tr>
<td>SCTP session timeout:</td>
<td>SCTP end timeout:</td>
</tr>
</tbody>
</table>

Out of State
TCP out of state packets are allowed for all gateways. Allowing out of state packets allows the potential of a Denial of Service attack to all protected servers.

Highly recommended to prevent out of state packets; especially as the reviewed gateways are on the internet perimeter.
Disk Usage
Log directory at 85% usage:

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Type</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/mapper/vg_splat-lv_current</td>
<td>ext3</td>
<td>47G</td>
<td>16G</td>
<td>29G</td>
<td>37%</td>
<td>/</td>
</tr>
<tr>
<td>proc</td>
<td>proc</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>/proc</td>
</tr>
<tr>
<td>sysfs</td>
<td>sysfs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>/sys</td>
</tr>
<tr>
<td>devpts</td>
<td>devpts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>/dev/pts</td>
</tr>
<tr>
<td>/dev/sda1</td>
<td>ext3</td>
<td>289M</td>
<td>24M</td>
<td>251M</td>
<td>9%</td>
<td>/boot</td>
</tr>
<tr>
<td>tmpfs</td>
<td>tmpfs</td>
<td>16G</td>
<td>4.0K</td>
<td>16G</td>
<td>1%</td>
<td>/dev/shm</td>
</tr>
<tr>
<td>/dev/mapper/vg_splat-lv_log</td>
<td>ext3</td>
<td>97G</td>
<td>78G</td>
<td>15G</td>
<td>85%</td>
<td>/var/log</td>
</tr>
<tr>
<td>none</td>
<td>binfmt_misc</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>/proc/sys/fs/binfmt_misc</td>
</tr>
</tbody>
</table>

There are some large files that could be removed to increase available space:

```
[Expert@fw1-management:0]# find / -size +500M
/home/admin/fw1-management_3_9_2018_13_07_migrate_export_out.tgz
/home/admin/fw1-management_3_5_2018_15_06_migrate_export_out.tgz
/var/log/CPbackup/backups/04-09-18_fw_migrate-export.tgz
/var/log/CPda/repository/CheckPoint#CPUpdates#All#6.0#4#8#BUNDLE_R80_10_JUMBO_HF#91/Check_Point_R80_10_JUMBO_HF_Bundle_T91_sk116380_FUL.tgz
/var/log/dump/usermode/fwm.4293.core.gz
```

Memory Usage
The system currently has sufficient memory; but prior to the 3rd September memory usage was at around 100%.

Current usage:

<table>
<thead>
<tr>
<th></th>
<th>total</th>
<th>used</th>
<th>free</th>
<th>shared</th>
<th>buffers</th>
<th>cached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mem:</td>
<td>32823288</td>
<td>31546036</td>
<td>1277252</td>
<td>0</td>
<td>1078096</td>
<td>11319580</td>
</tr>
<tr>
<td>+/- buffers/cache:</td>
<td>19148360</td>
<td>13674928</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Swap:</td>
<td>33551744</td>
<td>120</td>
<td>33551624</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total:</td>
<td>66375032</td>
<td>31546156</td>
<td>34828876</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Historical data:

![Graph showing memory usage over time]

Historical swap usage:

![Graph showing swap usage over time]

Memory usage should be monitored and increased if required.
**CPU Usage**

CPU usage is within acceptable values, but as it's a VM an additional CPU or two would improve the user experience.

![CPU Usage Graph](image)

**IO Wait**

There is a constant amount of IOWait. The IOWait on a VM environment is typically due to Disk IO on a shared infrastructure with the combination of Check Point logging/indexing.

![IO Wait Graph](image)
The IO correlates with the disk read/writes.

**I/O for fw1-management**

In general use, IOwait is low but consistent and should be monitored.

```
Linux 2.6.18-92cpx36_64 (fw1-management) 09/04/18
00:00:01 CPU %user %nice %system %iowait %steal %idle
00:10:01 all 18.45 2.18 2.23 0.03 0.00 76.1
00:10:01 0 20.51 2.41 2.69 1.54 0.00 72.7
00:10:01 1 15.39 1.96 1.87 0.23 0.00 79.5
00:20:01 all 17.06 0.70 1.87 0.75 0.00 79.6
00:20:01 0 18.46 0.66 2.21 1.27 0.00 77.6
00:20:01 1 15.67 0.74 1.52 0.23 0.00 81.8
00:30:01 all 17.16 0.73 1.86 0.74 0.00 79.5
00:30:01 0 18.15 0.71 2.15 1.27 0.00 77.7
00:30:01 1 16.18 0.75 1.56 0.21 0.00 81.3
00:40:01 all 15.86 0.88 1.82 0.69 0.00 79.7
```
Local Users
Both CLI and SmartConsole have users defined with local accounts only. It is recommended to configure AAA; so when users leave the company and removed from Active Directory they are automatically restricted access.

<table>
<thead>
<tr>
<th>Name</th>
<th>Expiration Date</th>
<th>Profile</th>
<th>Authentication Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Dec 31, 2030</td>
<td>Super User</td>
<td>OS Password</td>
</tr>
<tr>
<td>username_1</td>
<td>Dec 31, 2018</td>
<td>read_write</td>
<td>Check Point Password</td>
</tr>
<tr>
<td>username_2</td>
<td>Dec 31, 2030</td>
<td>read_write</td>
<td>Check Point Password</td>
</tr>
<tr>
<td>username_3</td>
<td>Jan 31, 2020</td>
<td>read_write</td>
<td>Check Point Password</td>
</tr>
</tbody>
</table>

It would also be recommended to enable a lockout policy on both CLI and GUI to prevent any Brute Force Authentication attacks.

**Login Restrictions**

- [ ] Lockout Administrator's account after [ ] failed authentication attempts
- [ ] Unlock Administrator's account after [ ] minutes
- [ ] Display an informative message upon denying access

If/when AAA is configured, it is normal practice to have one local account in the case when the AAA servers are not accessible. In SmartEvent I would recommend to create an alert (email, SNMP or SMS) whenever the local account is used so that the password can be changed.

SNMP
SNMP is used to monitor the system and identify any potential issues. SNMP agent is disabled.

```
fw1-management> show snmp agent
SNMP Agent Disabled
```

IPS - Server Configuration
Some IPS protections are only applied against defined servers. Web, Mail and DNS servers need to be defined in the host objects for these IPS protections to take effect.
**Blade Updates**

The management is incorrectly stating that’s blades are not up to date on the gateways. Install the latest Jumbo on all devices and install the latest SmartConsole to remediate the cosmetic issue.

---

**Online Web Services – Threat Prevention**

Threat Prevention blade connections are allowed until they are categorized:

- **Check Point Online Web Service**
  - Block connections when the web service is unavailable
  - Resource classification mode
    - Background - requests are allowed until categorization is complete
    - Hold - requests are blocked until categorization is complete
    - Custom - configure different settings depending on the service

This is the default setting.
Implied Rules

Logging implied rules is recommended only to troubleshoot connectivity or VPN issues as it adds overhead to the gateway and management.

In some environments its required to log all rules for auditing purposes; but in this environment we can see many rules not being logged so this can't be the case:
**Hit Count Database**

There are many rules that have not been hit in the last 3 months. Only required access to be allowed through the gateway; if the rule is not in use then it is not required.

It is recommended to remove unused rules. If you require increasing the time recorded in the Hit Count database then this can be achieved in Global properties:

![Global Properties](image)

Erik: The `Hit Count Database` report highlights the insignificance of certain rules that haven't been accessed in the last three months. It advocates for the removal of these unused rules to streamline access. Implementing this change in the `Global Properties` can significantly enhance efficiency.

Erik: To achieve this, one must clear the `Hit Count Database` by adjusting the recording period in the `Global Properties`. This involves checking the `Enable Hit Count` box and selecting an extended period for data retention.
Cluster1 Cluster Review
The following findings have been identified on the R80.10 VSec cluster:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Status</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotfix</td>
<td>✗</td>
<td>Gateway vulnerability to be remediated with latest JHF.</td>
</tr>
<tr>
<td>NAT Cache</td>
<td>🔄</td>
<td>Performance can be improved by moving rules within the policy.</td>
</tr>
<tr>
<td>Misplaced Rules</td>
<td>🔄⚠️</td>
<td>Performance can be improved by moving rules within the policy.</td>
</tr>
<tr>
<td>VOIP</td>
<td>🔄⚠️</td>
<td>Firewall Early NAT chain enabled but no VOIP traffic passing gateway.</td>
</tr>
<tr>
<td>Snapshot/Backup</td>
<td>⚠️</td>
<td>No backups scheduled.</td>
</tr>
<tr>
<td>AAA</td>
<td>⚠️</td>
<td>Local accounts only defined.</td>
</tr>
<tr>
<td>Interface buffers</td>
<td>✗</td>
<td>Inconsistent values set.</td>
</tr>
<tr>
<td>Fragments</td>
<td>☢️</td>
<td>Determine source of fragments.</td>
</tr>
<tr>
<td>Sync</td>
<td>✗</td>
<td>Sync issues detected.</td>
</tr>
<tr>
<td>Zombie Processes</td>
<td>✗</td>
<td>5 zombie processes detected.</td>
</tr>
<tr>
<td>Weak Ciphers</td>
<td>⚠️</td>
<td>Default ciphers configured.</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>⚠️</td>
<td>Insecure version of SNMP configured.</td>
</tr>
<tr>
<td>HA State</td>
<td>⚠️</td>
<td>Recent change of state.</td>
</tr>
<tr>
<td>Logging</td>
<td>⚠️</td>
<td>Non-resilient logging.</td>
</tr>
<tr>
<td>Anti-Spoofing</td>
<td>✗</td>
<td>Not configured correctly.</td>
</tr>
<tr>
<td>Drop Templates</td>
<td>⚠️</td>
<td>Optimization possible.</td>
</tr>
<tr>
<td>NTP</td>
<td>✗</td>
<td>Version configured open to exploit.</td>
</tr>
<tr>
<td>ARP</td>
<td>⚠️</td>
<td>sk18463</td>
</tr>
<tr>
<td>Stealth</td>
<td>✗</td>
<td>Missing.</td>
</tr>
</tbody>
</table>

Each recommendation is rated as follows:

- ✗ Serious - Needs immediate attention
- ⚠️ Attention - Needs attention
- ✔️ Good - No need for any action
- ❓ Informational
Hotfix
R80.10 Jumbo Hotfix Accumulator is an accumulation of stability and quality fixes resolving multiple issues in different products.

The latest Jumbo (T142) remediates the security gateway from the SegmentSmack vulnerability (sk134253). Recommended to install the latest jumbo to enhance feature set and improve stability.

NAT Cache
NAT Cache limit has exceeded. This will not cause any problems, as these connections will be matched against the NAT rules instead of the NAT cache table.

NAT Statistics:-------------------------
Current NAT Cache:   [30000]
Peak NAT Cache:       [30000]

Please refer to sk21834 - How to modify values of properties related to NAT cache table “fwx_do_nat_cache”

Misplaced Rules
This output if from the current connection table; so only accurate for the time of investigation. It is recommended to review the policy and move rules with the highest hit count as far to the top of the policy as possible.

Top Rule Hits
-------------------------
|rule index|rule count|
-------------------------
|Rule 28   | 163696407|
|Rule 44   | 152628839|
|Rule 271  |  82327028|
|Rule 46   |  34211047|
|Rule 130  |  17375433|
-------------------------

VOIP
Firewall “fw early SIP nat” is enabled (triggered by specific VOIP services in rulebase) while there were no entries in the VOIP tables.

In case the VOIP calls are not encrypted and should be inspected the tables should have some values. In case the VOIP is encrypted or not in use then it is recommended to disable the chain since it may cause interruptions and improve gateway performance.

Current state:
-------------------------
Firewall Early NAT Chain:   [TRUE]
SIP Registered phones:   [0]
SIP Calls:               [0]
H323 Registered phones:  [0]
H323 Calls:             [0]
MGCP Registered Phones:  [0]
MGCP Calls:             [0]

Please refer to sk65072 - How to disable ‘fw early SIP nat’ chain / SIP inspection
Snapshot/Backup
There are no Snapshots, Backups or Scheduled Backups on the system.

As these gateways are running on VMware the backups could be handled via external software.

AAA
AAA is used to authorize, authenticate and account user access. Only local user accounts are configured on the gateway:

<table>
<thead>
<tr>
<th>RADIUS: [DISABLED]</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS: [DISABLED]</td>
</tr>
</tbody>
</table>

AAA is used to determine who actually is logging onto the gateway and their access revoked when removed from the company/Active Directory.

Interface Buffers
The RX interface buffer between cluster members do not match:

<table>
<thead>
<tr>
<th>Received parameters for eth1:</th>
<th>Received parameters for eth2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-set minimum:</td>
<td>Pre-set minimum:</td>
</tr>
<tr>
<td>RX: 4096</td>
<td>RX: 4096</td>
</tr>
<tr>
<td>RX Min: 0</td>
<td>RX Min: 0</td>
</tr>
<tr>
<td>RX Jumbo: 0</td>
<td>RX Jumbo: 0</td>
</tr>
<tr>
<td>RX: 4096</td>
<td>RX: 4096</td>
</tr>
<tr>
<td>Current hardware settings:</td>
<td>Current hardware settings:</td>
</tr>
<tr>
<td>RX: 512</td>
<td>RX: 256</td>
</tr>
<tr>
<td>RX Min: 0</td>
<td>RX Min: 0</td>
</tr>
<tr>
<td>RX Jumbo: 0</td>
<td>RX Jumbo: 0</td>
</tr>
<tr>
<td>RX: 512</td>
<td>TX: 512</td>
</tr>
</tbody>
</table>

Fragments:
There are a high number of fragments on the firewall:

Expired - denotes how many fragments were expired when the firewall failed to reassemble them within in a 1 second (default, but configurable) time frame or when due to memory exhaustion, they could not be kept in memory anymore.
Failures - denotes the number of fragmented packets that were received that could not be successfully re-assembled.

It is important to verify this counters are not increasing overtime.

Fragments:
23500346 fragments, 9121282 packets, 548 expired, 0 short, 0 large, 0 duplicates, 0 failures

Fragments are expected on the external/internet interface; but fragments on the internal interfaces could indicate an issue with the internal network infrastructure. Recommended to follow sk65852 to confirm the source of fragmented packets.
Sync

[[!] 135 drops caused by network occurred
[!] Sync retransmissions were detected (Sent: 12 , Receive: 754)
[-] 11 average missing updates per request
[!] Sync lost events were detected (Timeout events: 3 , Sync Lost events: 111)

[[!] 1673 drops caused by network occurred
[-] 322 events of Sync Overload occurred
[!] Sync retransmissions were detected (Sent: 754 , Receive: 12 )
[-] 2 average missing updates per request
[!] Sync lost events were detected (Timeout events: 3 , Sync Lost events: 116)

[Expert@FW2:0]# dmesg | egrep -i "sync"
[fw4_0];FW-1: State synchronization is in risk. Please examine your synchronization network to avoid further problems!
[fw4_1];FW-1: fwldbcast_recv: delta sync connection with member 0 was lost and regained.616 updates were lost.
[fw4_0];FW-1: State synchronization is in risk. Please examine your synchronization network to avoid further problems!
[fw4_1];FW-1: fwldbcast_recv: delta sync connection with member 0 was lost and regained.1323 updates were lost.
[fw4_0];FW-1: State synchronization is in risk. Please examine your synchronization network to avoid further problems!
[fw4_1];FW-1: fwldbcast_recv: delta sync connection with member 0 was lost and regained.527 updates were lost.

For more information on Sync:
- sk34476: Explanation of Sync section in the output of fw ctl pstat command
- sk34475: ClusterXL Sync Statistics - output of `cphaprob syncstat` command

To troubleshoot Sync issues use:
- sk37029: Full Synchronization issues on cluster member
- sk37030: Debugging Full Synchronization in ClusterXL

For more information on redundant sync configurations:
- sk92804: Sync Redundancy in ClusterXL

Zombie Processes
There are 5 Zombie processes. Zombie process from a script created by user/<customer>.

5 zombie processes found.
PID COMMAND
14951 [helse.sh] <defunct>
19254 [helse.sh] <defunct>
21801 [helse.sh] <defunct>
27404 [helse.sh] <defunct>
30971 [helse.sh] <defunct>

Weak Ciphers
Week Ciphers are allowed to and through the gateway (sk113114, sk106031, sk107166). If in a PCI environment then they need to be hard disabled, if not then they can be prevented in security and IPS policy.
SNMP Version
It is recommended to configure SNMP v3 only as previous versions are deemed insecure.

```
FW2> show configuration snmp
set snmp mode default
set snmp agent on
set snmp agent-version any
```

HA State
While investigating I noticed there was a recent change of state (Sep 4 09:04:33 2018).

```
[Expert@FW1:0]# cphaprob stat
Cluster Mode: High Availability (Primary Up) with IGMP Membership

<table>
<thead>
<tr>
<th>Number</th>
<th>Unique Address</th>
<th>Assigned Load</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (local)</td>
<td>172.20.250.2</td>
<td>100%</td>
<td>Active</td>
</tr>
<tr>
<td>2</td>
<td>172.20.250.3</td>
<td>0%</td>
<td>Standby</td>
</tr>
</tbody>
</table>

Local member is in current state since Tue Sep 4 09:04:33 2018
```

It appears an interface went down:

```
[fw4_1];fwha_report_id_problem_status: Try to update state to DOWN due to pnote Interface Active Check (desc interface is down, member 2 (172.20.250.3) reports more interfaces up)
fw4_1];fwha_report_id_problem_status: Try to update state to ACTIVE due to pnote Problem Notification (desc routed)
```

Recommend to monitor and investigate when/if happens again.

Logging
Logs are set to only be sent to a single log server. In the instance where the logserver is not reachable the configuration could be set to send logs to the management rather than log locally.
Anti-Spoofing
Anti-spoofing is the first line of defense from unauthorized access attempts and ensure the firewall policy is correctly applied as Check Point enforce a policy based security policy (rather than zone-based).

Check Point recommend to configure Anti-Spoofing correctly.

```
[fw4_0];FW-1: Warning: The eth0 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth2.1102 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth1.1101 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth2.1104 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth1.3 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth4.220 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth1.1100 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth1.1105 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth1.2 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth2.1103 interface is not protected by the anti-spoofing feature.
[fw4_0];FW-1: Warning: The eth1.1101 interface is not protected by the anti-spoofing feature.
```
Drop Templates

There are a lot drop rules in the policy with high connection hits. Enabling Drop templates would improve the gateway performance and connection latency, but the gateway doesn't currently have a performance issue and does not need the optimization; but the option is available.

```plaintext
<table>
<thead>
<tr>
<th>Localhost</th>
<th>IP</th>
<th>Policy</th>
<th>Date</th>
<th>Total</th>
<th>Reject</th>
<th>Drop</th>
<th>Accept</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost</td>
<td>&gt;eth0</td>
<td>Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>33107622</td>
<td>0   8733</td>
<td>33098889</td>
<td>1050642</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth0</td>
<td>Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>66705190</td>
<td>0   66705190</td>
<td>129</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth2</td>
<td>Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth3</td>
<td>Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>79428</td>
<td>0</td>
<td>79428</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth3</td>
<td>Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>79428</td>
<td>0</td>
<td>79428</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth2.1102 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>30961618</td>
<td>0</td>
<td>1506281</td>
<td>29455337</td>
<td>1370017</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth2.1102 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>393685690</td>
<td>0</td>
<td>10   393685680</td>
<td>2329</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.1101 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>69660874</td>
<td>1890450</td>
<td>67770424</td>
<td>1855277</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.1101 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>34318436</td>
<td>0</td>
<td>34318436</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.383 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>678</td>
<td>0   17</td>
<td>661</td>
<td>90784</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.383 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>784</td>
<td>0</td>
<td>784</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth2.1104 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>3614476</td>
<td>0</td>
<td>1771278</td>
<td>1843198</td>
<td>2011710</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth2.1104 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>683430</td>
<td>0</td>
<td>683430</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.3 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>319287</td>
<td>0</td>
<td>1485</td>
<td>317802</td>
<td>10292</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.3 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>4770118</td>
<td>0</td>
<td>4770118</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth4.220 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>482899151</td>
<td>0</td>
<td>9593529</td>
<td>473305622</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth4.220 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>334253693</td>
<td>0</td>
<td>334253693</td>
<td>4835</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.381 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>313769</td>
<td>0</td>
<td>31892</td>
<td>281877</td>
<td>79702</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.381 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>242813</td>
<td>0</td>
<td>242813</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.384 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>269018</td>
<td>85</td>
<td>269018</td>
<td>99</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.384 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>255359</td>
<td>0</td>
<td>255359</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.1105 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>120657284</td>
<td>0</td>
<td>3895776</td>
<td>116761508</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.1105 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>94408310</td>
<td>0</td>
<td>94408310</td>
<td>297</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.2 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>12369679</td>
<td>0</td>
<td>834655</td>
<td>11535024</td>
<td>1551993</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.2 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>16549407</td>
<td>0</td>
<td>16549407</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.7 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>29252</td>
<td>24553</td>
<td>4719</td>
<td>25989</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.7 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>2032</td>
<td>0</td>
<td>2032</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.382 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>90448</td>
<td>0</td>
<td>4678</td>
<td>85770</td>
<td>109278</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.382 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>69547</td>
<td>0</td>
<td>69547</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.6 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>70026</td>
<td>0</td>
<td>35050</td>
<td>34976</td>
<td>126459</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.6 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>24972</td>
<td>0</td>
<td>24972</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth2.1103 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>456559</td>
<td>0</td>
<td>56282</td>
<td>400277</td>
<td>74268</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth2.1103 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>517609</td>
<td>0</td>
<td>517609</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.1100 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>490204651</td>
<td>0</td>
<td>720192</td>
<td>489484459</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.1100 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>244667349</td>
<td>0</td>
<td>244667321</td>
<td>4075</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.5 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>75015</td>
<td>0</td>
<td>57656</td>
<td>17359</td>
<td>40059</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.5 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>21747</td>
<td>0</td>
<td>21747</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth2.4 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>315851</td>
<td>0</td>
<td>122120</td>
<td>193731</td>
<td>119691</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth2.4 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>196279</td>
<td>0</td>
<td>196279</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&gt;eth1.380 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>2326391</td>
<td>0</td>
<td>2297403</td>
<td>28988</td>
<td>2297421</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>&lt;eth1.380 Standard_Policy</td>
<td>4Sep2018 14:04:07</td>
<td>28154</td>
<td>0</td>
<td>28154</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**NTP**

NTP versions 1-3 are no longer maintained, so any security flaws uncovered are not patched and remain dangerously exploitable. There are many NTP exploits so using the latest version is highly recommended:

```
set ntp active on
set ntp server primary no.pool.ntp.org version 1
```

**ARP**

$FWDIR/log/fwd.elg is full of ARP entries as below:

```
fwarp_get_arp_interface: no interface found on same subnet as valid ip address:
fwarp_make_arp_entry: can't find arp interface for address: 9.9.9.9 1.1.1.1
fwarp_get_arp_interface: no interface found on same subnet as valid ip address: 2.2.2.2 1.1.1.1
fwarp_make_arp_entry: can't find arp interface for address: 2.2.2.2 1.1.1.1
```

These errors are because Auto Static NAT's are in the policy but assigned to all gateways:
Stealth
A “stealth” rule should be added as one of the very top rules stating:

Source: Any
Destination: Gateway
Service: Any
Action: Drop

This is to ensure the gateway is hidden to unauthorized systems and access restricted.
VSXCluster2 Cluster Review

The following findings have been identified on the R80.10 VSX cluster. The following VS instances are configured on VSXCluster2:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Status</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotfix</td>
<td>✗</td>
<td>Gateway vulnerability to be remediated with latest JHF.</td>
</tr>
<tr>
<td>CoreXL</td>
<td>✗</td>
<td>CoreXL should not be enabled on VS0.</td>
</tr>
<tr>
<td>NAT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP Version</td>
<td>✗</td>
<td>Insecure version of SNMP configured.</td>
</tr>
<tr>
<td>SNMP Mode</td>
<td></td>
<td>Default mode set.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>!</td>
<td>Many large files that could be removed.</td>
</tr>
<tr>
<td>Core Dumps</td>
<td>!</td>
<td>Old core dumps on system.</td>
</tr>
<tr>
<td>AAA</td>
<td></td>
<td>Local accounts only defined.</td>
</tr>
<tr>
<td>Weak Ciphers</td>
<td>!</td>
<td>Default ciphers configured.</td>
</tr>
<tr>
<td>Sync</td>
<td>!</td>
<td>Sync Issues detected.</td>
</tr>
<tr>
<td>ARP</td>
<td>✗</td>
<td>sk18463</td>
</tr>
<tr>
<td>NTP</td>
<td>✗</td>
<td>Version configured open to exploit.</td>
</tr>
<tr>
<td>Resource - CoreXL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td>!</td>
<td>Non-resilient logging.</td>
</tr>
<tr>
<td>Stealth</td>
<td>✗</td>
<td>Missing.</td>
</tr>
</tbody>
</table>

Date: May 19, 2019
### VS1 – vs-xxxxa

<table>
<thead>
<tr>
<th>Topic</th>
<th>Status</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Profile</td>
<td>![Icon]</td>
<td>No scope defined.</td>
</tr>
<tr>
<td>Application Control Policy</td>
<td>![Icon]</td>
<td>Overhead due to configuration.</td>
</tr>
<tr>
<td>Policy Types</td>
<td>![Icon]</td>
<td></td>
</tr>
<tr>
<td>NAT Connections</td>
<td>![Icon]</td>
<td></td>
</tr>
<tr>
<td>Internet Connectivity</td>
<td>![Icon]</td>
<td>Failed to connect to URL.</td>
</tr>
<tr>
<td>Misplaced Rules</td>
<td>![Icon]</td>
<td>Performance can be improved by moving rules within the policy.</td>
</tr>
<tr>
<td>Fragments</td>
<td>![Icon]</td>
<td>Determine source of fragments.</td>
</tr>
<tr>
<td>Stealth</td>
<td>![Icon]</td>
<td>Missing.</td>
</tr>
</tbody>
</table>

### VS2 – vs-xxxxb

<table>
<thead>
<tr>
<th>Topic</th>
<th>Status</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Control Policy</td>
<td>![Icon]</td>
<td>Overhead due to configuration.</td>
</tr>
<tr>
<td>Policy Types</td>
<td>![Icon]</td>
<td></td>
</tr>
<tr>
<td>Old UDP Session</td>
<td>![Icon]</td>
<td>High amount of packets being dropped due to expired session.</td>
</tr>
<tr>
<td>Misplaced Rules</td>
<td>![Icon]</td>
<td>Security concern.</td>
</tr>
<tr>
<td>NAT Connections</td>
<td>![Icon]</td>
<td></td>
</tr>
<tr>
<td>Fragments</td>
<td>![Icon]</td>
<td>Determine source of fragments.</td>
</tr>
<tr>
<td>Stealth</td>
<td>![Icon]</td>
<td>Missing.</td>
</tr>
</tbody>
</table>

### VS8 – vs-xxxxc

<table>
<thead>
<tr>
<th>Topic</th>
<th>Status</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>![Icon]</td>
<td>No policy installed.</td>
</tr>
</tbody>
</table>

Each recommendation is rated as follows:

- **![Icon]** - Serious - Needs immediate attention
- **![Icon]** - Attention - Needs attention
- **![Icon]** - Good - No need for any action
- **![Icon]** - Informational
VS0

Hotfix

R80.10 Jumbo Hotfix Accumulator is an accumulation of stability and quality fixes resolving multiple issues in different products.

The latest Jumbo (T142) remediates the security gateway from the SegmentSmack vulnerability (sk134253). Recommended to install the latest jumbo to enhance feature set and improve stability.

CoreXL

VS0 should not have CoreXL enabled:

```
Configuring Check Point CoreXL...
-----------------------------------
CoreXL is currently enabled with 6 fwx instances.
```

VS instances run in user mode and use the first available resource to best utilize CPU usage.

Enabling CoreXL on VS 0 has created instances running in kernel mode (taking preference over usermode processes) and reserving system resource per instance.

Check point recommend disabling CoreXL on VS 0 during a scheduled change window.

NAT

Dynamic NAT port allocation (sk103656, sk69480) have been enabled to presumably remediate a previous NAT issue.

```
fwkern.conf:
===============
cat /opt/CPsuite-R80/fw1/boot/modules/fwkern.conf
fwha_enable_state_machine_by_vs=1
fwx_high_port_quota=600
fwx_low_port_quota=60
fwx_nat_dynamic_port_allocation=1
fwx_nat_dynamic_high_port_allocation_size=300
```

Values look incorrectly set and hence why CoreXL was enabled on VS0 to make the solution work:

Set the value of `fwx_nat_dynamic_high_port_allocation_size` to a lower value, starting at `800 / (Number of CoreXL FW instances)`, and possibly as low as `500 / (Number of CoreXL FW instances)`.

Note: The lower the value, the higher the performance requirement.

SNMP Version

It is recommended to configure SNMP v3 only as previous versions are deemed insecure.

```
FW2> show configuration snmp
set snmp mode default
set snmp agent on
set snmp agent-version any
```
SNMP Mode
SNMP mode is default, which means only VS 0 is monitored. It is recommended to VS mode as it's a VSX
cluster, which then allows monitoring of all VS instances.

> set snmp mode vs

Disk Usage
There are no issues with disk usage but some cleanup is possible:

Big Files:
511M /var/log/dump/usermode/fwk1_5.24369.core.gz
11G /var/log/CPbackup/backups/backup_vsx-1.customer.org_14_Jun_2018_19_50.tgz
515M /var/log/CPda/repository/CheckPoint#CPUpdates#All#6.0#4#R80_10_JUMBO_HF#103/Check_Point_R80
10_JUMBO_HF_Bundle_T103_sk116380_FULL.tgz
730M /var/log/CPsuite-R80/fw1/CTX/CTX00001/2018-04-25_000000.log741M /var/log/opt/CPsuite-
R80/fw1/CTX/CTX00001/2018-06-13_000000.log
2.0G /var/log/opt/CPsuite-R80/fw1/CTX/CTX00001/2018-06-14_134852_2.log
2.0G /var/log/opt/CPsuite-R80/fw1/CTX/CTX00001/2018-06-14_105259_1.log
985M /var/log/dump/usermode/temain.16109.core.gz
1.5G /var/log/opt/CPsuite-R80/fw1/CTX/CTX00001/2018-06-14_100114_1.log

Core dumps
The system has a number of old coredumps relating to Firewall, Identity Awareness and Threat Emulation.

Usermode Cores:
-rw-r--r-- 1 admin root 535681519 Aug 31 16:45 fwk1_5.24369.core.gz
-rw-r--r-- 1 admin root 325065113 Aug 28 13:55 pdpd.2349.core.gz

AAA
AAA is used to authorize, authenticate and account user access. Only local user accounts are configured on
the gateway:

RADIUS: [DISABLED]
TACACS: [DISABLED]

AAA is used to determine who actually is logging onto the gateway and their access revoked when removed
from the company/Active Directory.
Weak Ciphers

Week Ciphers are allowed to and through the gateway (sk113114, sk106031, sk107166). If in a PCI environment then they need to be hard disabled, if not then they can be prevented in security and IPS policy.

Sync

The customer mentioned they have occasional Sync issues they cant explain. As the System was recently rebooted we don’t have many Sync errors to investigate:

```
reboot system boot 2.6.18-92cpx86_6 Sun Sep  2 09:41 (1+00:55)
```

But we do see a high delay in Sync traffic. As per sk34476, max delay above 34 indicates an overload of Sync traffic:

```
Sync packets received:
total : 8825353, were queued : 10, dropped by net : 4
retrans reqs : 0, received 1635124 acks
retrans reqs for illegal seq : 0
dropped updates as a result of sync overload: 0
 Callback statistics: handled 1620344 cb, average delay : 1, max delay : 46
```

Sync interfaces do not have excessive amount of traffic:

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>MTU</th>
<th>RX-OK</th>
<th>RX-ERR</th>
<th>RX-DRP</th>
<th>RX-OVR</th>
<th>TX-OK</th>
<th>TX-ERR</th>
<th>TX-DRP</th>
<th>TX-OVR</th>
<th>Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt</td>
<td>1500</td>
<td>27904899</td>
<td>0</td>
<td>0</td>
<td>34969843</td>
<td>0</td>
<td>0</td>
<td>BMRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sync</td>
<td>1500</td>
<td>25316594</td>
<td>0</td>
<td>83</td>
<td>238780989</td>
<td>0</td>
<td>0</td>
<td>BMRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bond0</td>
<td>1500</td>
<td>13745610464</td>
<td>27</td>
<td>0</td>
<td>7845031952</td>
<td>0</td>
<td>0</td>
<td>BMmRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bond1</td>
<td>1500</td>
<td>8114082557</td>
<td>0</td>
<td>0</td>
<td>13742926331</td>
<td>0</td>
<td>0</td>
<td>BMmRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bond3</td>
<td>1500</td>
<td>1256013864</td>
<td>0</td>
<td>0</td>
<td>3941005823</td>
<td>0</td>
<td>0</td>
<td>BMmRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth1-01</td>
<td>1500</td>
<td>7421066192</td>
<td>0</td>
<td>0</td>
<td>6875710596</td>
<td>0</td>
<td>0</td>
<td>BMmRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth1-04</td>
<td>1500</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>BMmRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth3-01</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>BMmRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth3-02</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>BMmRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth4-01</td>
<td>1500</td>
<td>1256013864</td>
<td>0</td>
<td>0</td>
<td>3940428261</td>
<td>0</td>
<td>0</td>
<td>BMmRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth4-02</td>
<td>1500</td>
<td>6930170000</td>
<td>0</td>
<td>0</td>
<td>6867238841</td>
<td>0</td>
<td>0</td>
<td>BMmRU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo</td>
<td>16436</td>
<td>12840407</td>
<td>0</td>
<td>0</td>
<td>12840407</td>
<td>0</td>
<td>0</td>
<td>LRU</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

But we do see a minimal out of RX-Drp and RX-Ovr on the Sync interface:
“The “RX-OK/ERR/DRP/OVR” columns give statistics about the packets that have been received by the interface so far. “OK” stands for “correctly received”, “ERR” for “received but with incorrect checksum” (happens when the connection is bad), “DRP” for “dropped because my receive buffer was too full” (happens when too many packets are received in a very short interval), and “OVR” for “dropped because the kernel couldn’t get to it in time” (if this happens, your computer was really busy).

The customer confirmed that the gateways are directly connected, which eliminates the possibility of network traffic collisions.

The statistics indicate an overload of the Sync interface, but the amount of traffic does not warrant the errors.

I would recommend to:
- Remediate CoreXL misconfiguration
- Install latest JHF
- Replace Sync cable
- Either remove Synchronization or delay Synchronization (closed connections are then not synchronized) from highly used services (DNS, HTTP etc).

If the issue persists after making the advised changes then raise a call with TAC to investigate further.

**ARP**

$FWDIR/log/fwd.elg is full of ARP entries as below:

These errors are because Auto Static NAT’s are in the policy but assigned to all gateways:
NTP

NTP versions 1-3 are no longer maintained, so any security flaws uncovered are not patched and remain dangerously exploitable. There are many NTP exploits so using the latest version is highly recommended:

```
set ntp active on
set ntp server primary 129.240.2.6 version 2
set ntp server secondary no.pool.ntp.org version 1
```

Resource - CoreXL

Note: This is not relevant for VS0 as CoreXL should be disabled. This is regarding user mode CoreXL instances across the system for VS instances.

There are 44 cores assigned for CoreXL use. Utilization potential is approx. x 1.5, so we have 66 CoreXL instances possible to be shared between all VS instances.

Currently the maximum CoreXL instances per VS instance is 10. In R80.20 the maximum will be increased to 32.

Logging

Logs are set to only be sent to “fw1-management”. In the instance where “fw1-management” is not reachable the configuration could be set to send logs to the dedicated log server:
Stealth

A “stealth” rule should be added as one of the very top rules stating:

Source: Any
Destination : Gateway
Service: Any
Action: Drop

This is to ensure the gateway is hidden to unauthorized systems and access restricted.

Note: Access to VS0 is not restricted and not logged.

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service &amp; Applications</th>
<th>Action</th>
<th>Dir</th>
<th>Rate</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>In</td>
<td>Any</td>
<td>None</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>In</td>
<td>Any</td>
<td>vs(vsla01)</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>In</td>
<td>Any</td>
<td>vs(vsla01)</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>In</td>
<td>Any</td>
<td>vs(vsla01)</td>
</tr>
<tr>
<td>5</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>In</td>
<td>Any</td>
<td>vs(vsla01)</td>
</tr>
</tbody>
</table>

VS1 – vs-xxxxa

IPS Profile

The IPS profile does not have a scope defined:
**Application Control Policy**

The configuration of the Application Control policy could be improved; the current legacy configuration means that traffic must traverse two policies.

Migrating to a unified policy limits the load on the gateway and simplifies administration.

Another improvement could be to utilize the R80 enhancements and use Layers in the security Policy. Currently traffic must traverse the Security Policy and then the Application Control policy.

Using the below example, applications are defined for traffic destined to the internet. Traffic not destined to the internet would skip rule 5; ultimately reducing the load on the gateway.

### Policy Types

QoS and Desktop Security Types are enabled and in view, as they are not in use I would recommend to remove them from view to eliminate any confusion.
NAT Connections
There are a high number of NAT connections in the accelerated path on this VS instance:

<table>
<thead>
<tr>
<th>Accelerated Path</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>C total conns</td>
<td>65328</td>
</tr>
<tr>
<td>C TCP conns</td>
<td>56772</td>
</tr>
<tr>
<td>C non TCP conns</td>
<td>8556</td>
</tr>
<tr>
<td>conns from templates</td>
<td>811402</td>
</tr>
<tr>
<td>nat conns</td>
<td>4002483</td>
</tr>
</tbody>
</table>

NAT:
230105859/0 forw, 313362402/0 bckw, 532861116 tcpudp, 1632606 icmp, 72158072-55441915 alloc

Enabling NAT templating may improve performance/overhead:

NAT Templates Status: [DISABLED]

Please refer to NAT Template limitations: sk71200

Internet Connectivity
All VS instances (active or Standby) can connect to a public URL, except for vsx-2:1 (VS1).

```
[Expert@vsx-1:0]# curl_cli -k -Is https://updates.checkpoint.com| head -1
HTTP/1.1 200 OK
[Expert@vsx-1:0]# vsenv 1
Context is set to Virtual Device vsx-1_vs-xxxx (ID 1).
[Expert@vsx-1:1]# curl_cli -k -Is https://updates.checkpoint.com| head -1
HTTP/1.1 200 OK
[Expert@vsx-1:1]# vsenv 2
Context is set to Virtual Device vsx-1_vs-xxxxb (ID 2).
[Expert@vsx-1:2]# curl_cli -k -Is https://updates.checkpoint.com| head -1
HTTP/1.1 200 OK

[Expert@vsx-2:0]# curl_cli -k -Is https://updates.checkpoint.com| head -1
HTTP/1.1 200 OK
[Expert@vsx-2:0]# vsenv 1
Context is set to Virtual Device vsx-2_vs-xxxx (ID 1).
[Expert@vsx-2:1]# curl_cli -k -Is https://updates.checkpoint.com| head -1
HTTP/1.1 200 OK
[Expert@vsx-2:1]# vsenv 2
Context is set to Virtual Device vsx-2_vs-xxxxb (ID 2).
[Expert@vsx-2:2]# curl_cli -k -Is https://updates.checkpoint.com| head -1
HTTP/1.1 200 OK

vsx-2:1 also cant ping:

[Expert@vsx-2:1]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 2999ms
```

Further investigation is required.
Misplaced Rules
This output is from the current connection table; so only accurate for the time of investigation. It is recommended to review the policy and move rules with the highest hit count as far to the top of the policy as possible.

<table>
<thead>
<tr>
<th>Top Rule Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule index</td>
</tr>
<tr>
<td>Rule 271</td>
</tr>
<tr>
<td>Rule 266</td>
</tr>
<tr>
<td>Rule 269</td>
</tr>
<tr>
<td>Rule 291</td>
</tr>
<tr>
<td>Rule 297</td>
</tr>
</tbody>
</table>

Fragments
There are a high number of fragments on the firewall:

*Expired* - denotes how many fragments were expired when the firewall failed to reassemble them within a 1 second (default, but configurable) time frame or when due to memory exhaustion, they could not be kept in memory anymore.

*Failures* - denotes the number of fragmented packets that were received that could not be successfully re-assembled.

It is important to verify this counters are not increasing overtime.

| Fragments: |
| 22022324 fragments, 9082432 packets, 33 expired, 0 short, 0 large, 0 duplicates, 380 failures |

Fragments are expected on the external/internet interface; but fragments on the internal interfaces could indicate an issue with the internal network infrastructure. Recommended to follow sk65852 to confirm the source of fragmented packets.

Stealth
A “stealth” rule should be added as one of the very top rules stating:

Source: Any
Destination: Gateway
Service: Any
Action: Drop

This is to ensure the gateway is hidden to unauthorized systems and access restricted.
VS2 – vs-xxxxb

**Application Control Policy**
The configuration of the Application Control policy could be improved; the current legacy configuration means that traffic must traverse two policies.

Migrating to a unified policy limits the load on the gateway and simplifies administration.

Another improvement could be to utilize the R80 enhancements and use Layers in the security Policy. Currently traffic must traverse the Security Policy and then the Application Control policy.

Using the below example, applications are defined for traffic destined to the internet. Traffic not destined to the internet would skip rule 5; ultimately reducing the load on the gateway.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Access to Internet</th>
<th>Action 1</th>
<th>Action 2</th>
<th>Action 3</th>
<th>Action 4</th>
<th>Action 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Access to Internet</td>
<td>Internalzones</td>
<td>Internet</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>5.1</td>
<td>DNS server</td>
<td>DNS Server</td>
<td>Internalzones</td>
<td>Internet</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>5.2</td>
<td>Block abuse/High risk applications</td>
<td>Corporate LAN</td>
<td>Internet</td>
<td>Any</td>
<td>Any</td>
<td>Inappropriate Sites</td>
</tr>
<tr>
<td>5.3</td>
<td>HR has access to social networking applications</td>
<td>HR</td>
<td>Internet</td>
<td>Any</td>
<td>Facebook</td>
<td>LinkedIn</td>
</tr>
<tr>
<td>5.4</td>
<td>All employees can access YouTube for work purposes</td>
<td>Corporate LAN</td>
<td>Internet</td>
<td>Any</td>
<td>YouTube</td>
<td>Vimeo</td>
</tr>
<tr>
<td>5.5</td>
<td>Block specific URLs</td>
<td>Any</td>
<td>Internet</td>
<td>Any</td>
<td>Blocked URLs</td>
<td></td>
</tr>
<tr>
<td>5.6</td>
<td>Block specific categories for all employees</td>
<td>Corporate LAN</td>
<td>Internet</td>
<td>Any</td>
<td>Social Networking</td>
<td></td>
</tr>
<tr>
<td>5.7</td>
<td>Cleanup</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
</tr>
</tbody>
</table>

**Policy Types**
QoS and Desktop Security Types are enabled and in view, as they are not in use I would recommend to remove them from view to eliminate any confusion.
Old UDP Sessions

There are a high amount of drops due to old UDP session packets for service UDP5232:

Instead of globally increasing the UDP timeout, create a new UDP service for the connection and amend the timeout just for that object:

Misplaced Rules

The concern on this output is not the placement of rules, but more that in the current connection table there are only two rules in use:

Each rule in the policy is access to the clients network. There are hundreds of rules but only 2 in use (currently, at point of review) and many rules with no hits in the policy.
It is highly recommended to remove unused rules to ensure only required access is allowed.

**NAT Connections**

There are a high number of NAT connections in the accelerated path on this VS instance:

<table>
<thead>
<tr>
<th>Accelerated Path</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>accel packets</td>
<td>535738514</td>
<td>accel bytes</td>
</tr>
<tr>
<td>conns created</td>
<td>8473750</td>
<td>conns deleted</td>
</tr>
<tr>
<td>total conns</td>
<td>110187</td>
<td>C templates</td>
</tr>
<tr>
<td>TCP conns</td>
<td>106320</td>
<td>delayed TCP conns</td>
</tr>
<tr>
<td>non TCP conns</td>
<td>3867</td>
<td>delayed nonTCP con</td>
</tr>
<tr>
<td>conns from templates</td>
<td>60646</td>
<td>temporary conns</td>
</tr>
<tr>
<td>nat conns</td>
<td>8371478</td>
<td>dropped packets</td>
</tr>
</tbody>
</table>

**NAT:**

241995072/0 forw, 343359487/0 bckw, 555683990 tcpudp, 1246490 icmp, 77800827-60949157 alloc

Enabling NAT templating may improve performance/overhead:

NAT Templates Status: [DISABLED]

Please refer to NAT Template limitations: sk71200

**Fragments**

There are a high number of fragments on the firewall:

*Expired* - denotes how many fragments were expired when the firewall failed to reassemble them within in a 1 second (default, but configurable) time frame or when due to memory exhaustion, they could not be kept in memory anymore.

*Failures* - denotes the number of fragmented packets that were received that could not be successfully re-assembled.

It is important to verify this counters are not increasing over time.

Fragments:

19544439 fragments, 3362819 packets, 24140 expired, 0 short, 0 large, 13 duplicates, 0 failures
Fragments are expected on the external/internet interface; but fragments on the internal interfaces could indicate an issue with the internal network infrastructure. Recommended to follow sk65852 to confirm the source of fragmented packets.

**Stealth**

A “stealth” rule should be added as one of the very top rules stating:

- **Source**: Any
- **Destination**: Gateway
- **Service**: Any
- **Action**: Drop

This is to ensure the gateway is hidden to unauthorized systems and access restricted.

**VS8 – vs-xxxxc**

**ALL**

The vs-xxxxc VS instance does not have a policy installed, so many errors including; no NA, initial policy assigned, no CoreXL instances etc.

The VS instance is out of scope of the audit.
Consultant Overview

The main concern in the environment is security; due to gateways susceptible to SegmentSmack vulnerability, no stealth rules, insecure versions of SNMP and NTP in use, many rules defined that are not in use/required, access to VS 0 not logged and open to “Any” source, non-resilient logging/auditing, no AAA to determine who accessed the system etc (as highlighted in this document).

On the plus side, the systems are not under any particular load. Check Point PS would recommend to utilize this resource to enable HTTPS Inspection to enhance the perimeters security.

HTTPS traffic is increasing being used on the Internet (approx. 40-60% of internet traffic) which an exception has currently been added to not inspect any HTTPS traffic against IPS protections. Instead of ignoring this traffic PS recommend to secure it:

<table>
<thead>
<tr>
<th>E-1.5</th>
<th>Any</th>
<th># Any</th>
<th>IPS</th>
<th>http</th>
</tr>
</thead>
</table>

Overall, the systems are performing well and have the resources to enable further blades/features to improve securing the environment; but there are some identified issues that should be remediated as soon as possible to improve stability and security.
Disclaimer

The Customer hereby attests and acknowledges that the Check Point Professional Services Engineer has completed the project work described above. This work meets the requirements specified by the Customer and has been completed to the satisfaction of the Customer.

By: 
Authorized Customer Representative

Date: 

By: 
Check Point Professional Services Representative

Date: 

Post Project Contact Information

Technical Issues
Check Point Software offers a wide variety of additional Assistance methods for their customers. Check Point Software offers direct customer support though our Worldwide Technical Assistance Centers for customers who purchase a support contract. Customers may also purchase follow-up telephone support assistance from Professional Services. Alternatively, a customer may work with a local Check Point reseller for support.

Check Point Professional Services
We offer follow-up telephone support at the rate of $800 per ½ day. Please contact us for this or any other future Professional Services project needs.
http://www.checkpoint.com/professional-services-escalation-matrix/

Check Point Technical Support
Our Worldwide Technical Assistance Centers are available to assist you 24x7.

Americas: 972-444-6600
International (Non-US): +972-3-6115100
E-mail: support@ts.checkpoint.com
Web: http://support.checkpoint.com
Please provide your organization’s support number when contacting Technical Services.

Check Point Sales
To find a Check Point Reseller:
Phone: 1-800-429-4391
E-mail: sales@checkpoint.com
Web: http://www.checkpoint.com/sales/index.html