Check Point
SOFTWARE TECHNOLOGIES LTD.

CLOUD • MOBILE • THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT
PROFESSIONAL SERVICES
Consult • Design • Deploy • Operate • Optimize

CHECK POINT GATEWAY HEALTH CHECK REPORT

Prepared for	**By**	**Date**
<Customer ACME>	**<PS Consultant>**	**<Date>**

Table of Contents

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.

Hardware	Name	Cluster	Version	Jumbo
VMware Virtual Platform	**fw1-management**		R80.10	Take 91
VMware Virtual Platform	**FW1**	Cluster1	R80.10	Take 112
VMware Virtual Platform	**FW2**	Cluster1	R80.10	Take 112
Check Point 23800	**vsx-1**	VSXCluster2	R80.10	Take 103
Check Point 23800	**vsx-2**	VSXCluster2	R80.10	Take 103

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):

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

Each recommendation is rated as follows:

❌	Serious - Needs immediate attention
⚠	Attention - Needs attention
✓	Good - No need for any action
ℹ	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.

License	3 out of 27 licenses are expired.
Contract	14 out of 51 contracts are expired.

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.

	Status	Count	Percent	Remediation
Total Network Objects	✓	4638	100%	
Unused Network Objects	✗	966	20.83%	Consider deleting these objects.
Duplicate Network Objects	✗	3162	68.18%	Consider deleting copies.
Nested Network Objects	✓	41	0.88%	
Total Services Objects	✓	1283	100%	
Unused Services Objects	✗	208	16.21%	Consider deleting these objects.
Nested Services Objects	!	26	2.03%	

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

Unassigned Policies

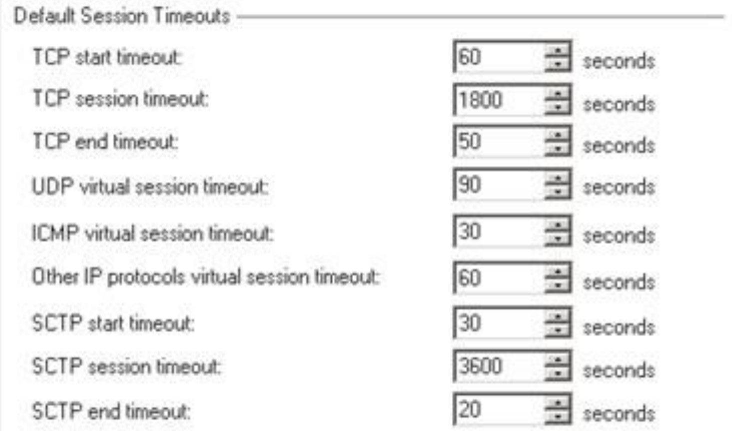
Removing the unassigned policies eliminates the possibility for human error but more importantly, increases the amount of unused objects and allowed a greater potential for object database cleanup.

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.

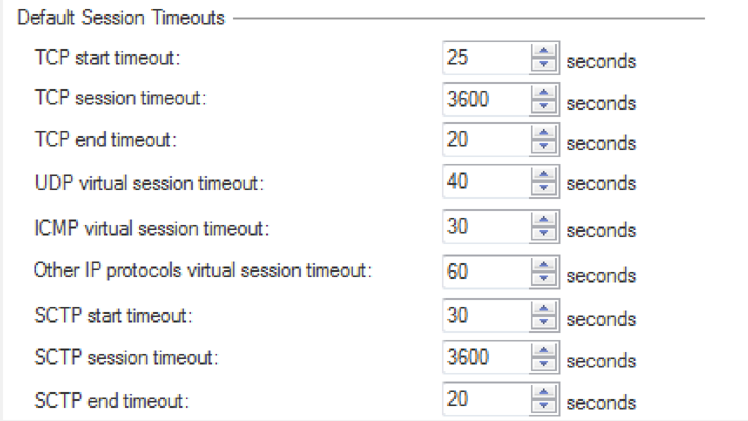
<customer> Values



Default Session Timeouts

TCP start timeout:	60	seconds
TCP session timeout:	1800	seconds
TCP end timeout:	50	seconds
UDP virtual session timeout:	90	seconds
ICMP virtual session timeout:	30	seconds
Other IP protocols virtual session timeout:	60	seconds
SCTP start timeout:	30	seconds
SCTP session timeout:	3600	seconds
SCTP end timeout:	20	seconds

Default Values



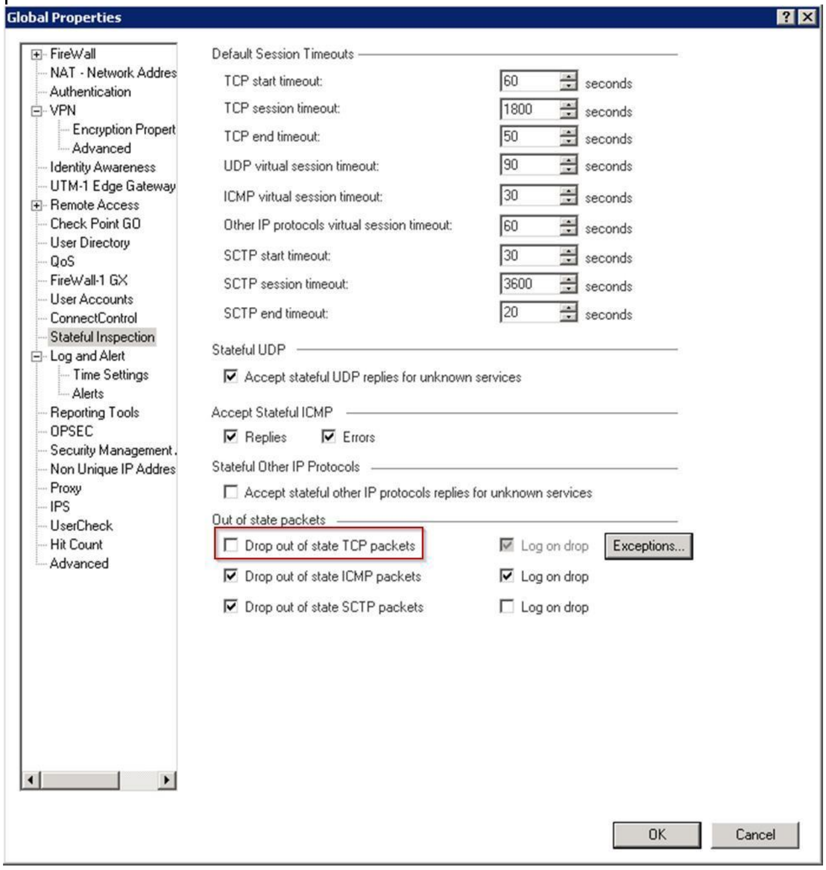
Default Session Timeouts

TCP start timeout:	25	seconds
TCP session timeout:	3600	seconds
TCP end timeout:	20	seconds
UDP virtual session timeout:	40	seconds
ICMP virtual session timeout:	30	seconds
Other IP protocols virtual session timeout:	60	seconds
SCTP start timeout:	30	seconds
SCTP session timeout:	3600	seconds
SCTP end timeout:	20	seconds

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.



Default Session Timeouts

TCP start timeout:	60	seconds
TCP session timeout:	1800	seconds
TCP end timeout:	50	seconds
UDP virtual session timeout:	90	seconds
ICMP virtual session timeout:	30	seconds
Other IP protocols virtual session timeout:	60	seconds
SCTP start timeout:	30	seconds
SCTP session timeout:	3600	seconds
SCTP end timeout:	20	seconds

Stateful UDP

☑ Accept stateful UDP replies for unknown services

Accept Stateful ICMP

☑ Replies ☑ Errors

Stateful Other IP Protocols

☐ Accept stateful other IP protocols replies for unknown services

Out of state packets

☐ Drop out of state TCP packets ☑ Log on drop Exceptions...

☑ Drop out of state ICMP packets ☑ Log on drop

☑ Drop out of state SCTP packets ☐ Log on drop

Disk Usage

Log directory at 85% usage:

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

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_8_5_2018_15_06_migrate_export_out.tgz
/var/log/CPbackup/backups/04-09-18_fw_migate-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_FULL.tgz
/var/log/dump/usermode/fwm.4293.core.gz
```

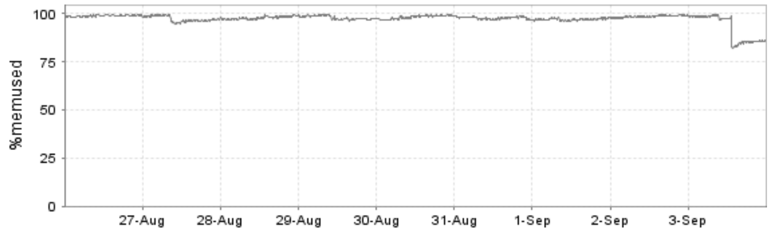
Memory Usage

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

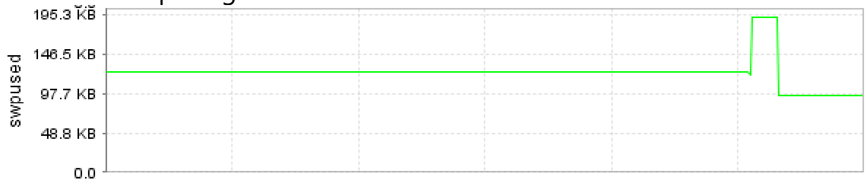
Current usage:

	total	used	free	shared	buffers	cached
Mem:	32823288	31546036	1277252	0	1078096	11319580
-/+ buffers/cache:		19148360	13674928			
Swap:	33551744	120	33551624			
Total:	66375032	31546156	34828876			

Historical data:



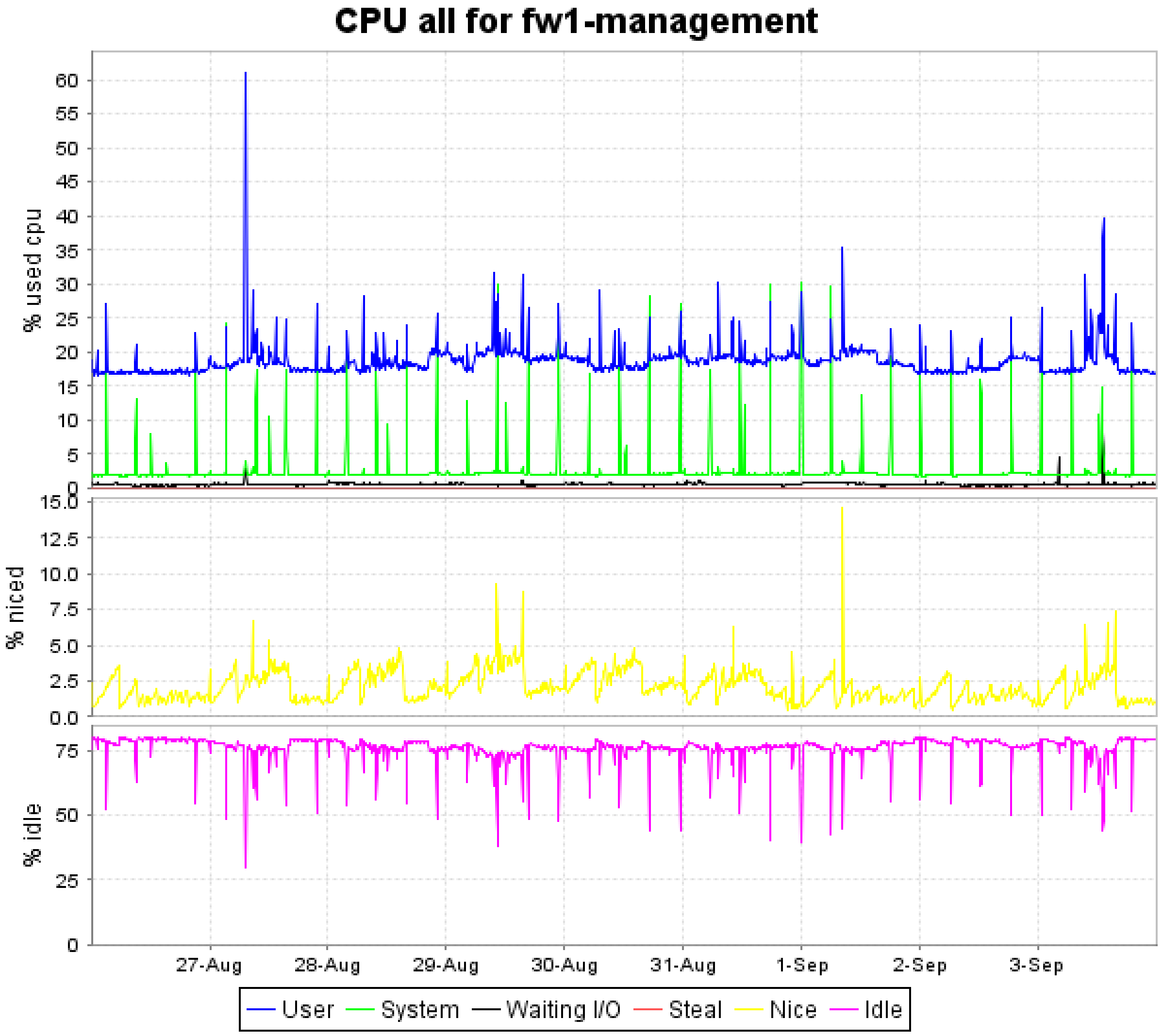
Historical swap usage:



Memory usage should be monitored and increased if required.

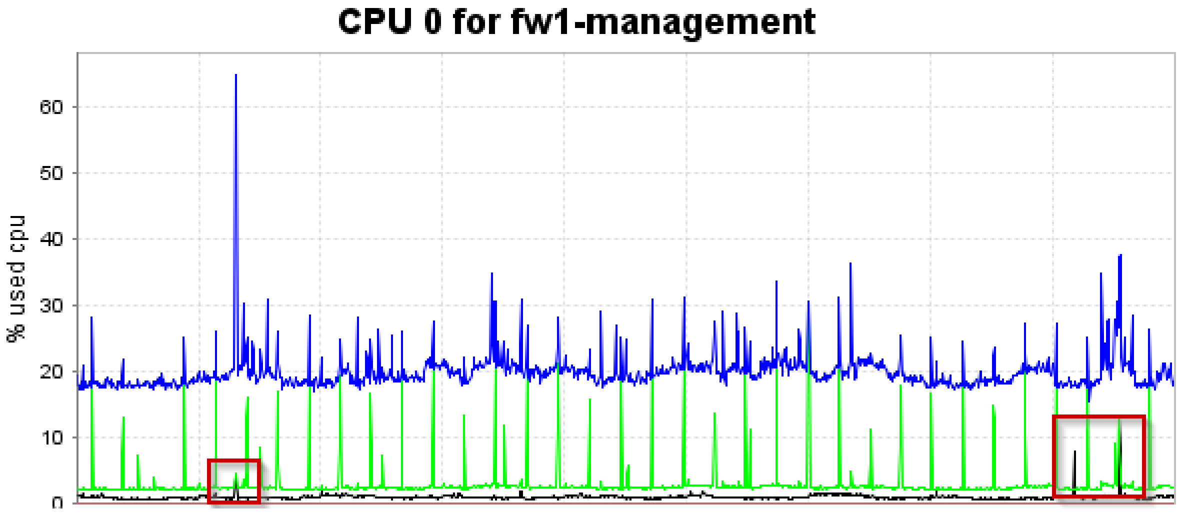
CPU Usage

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

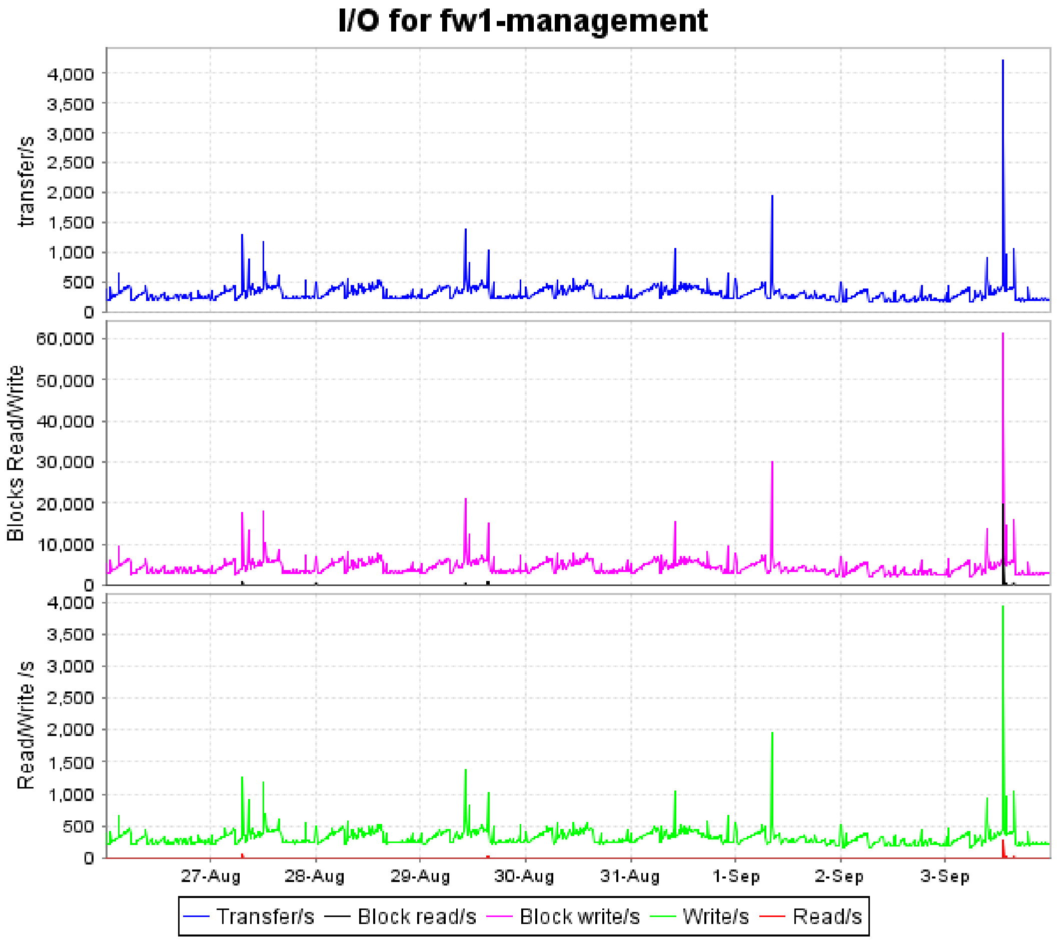


IO Wait

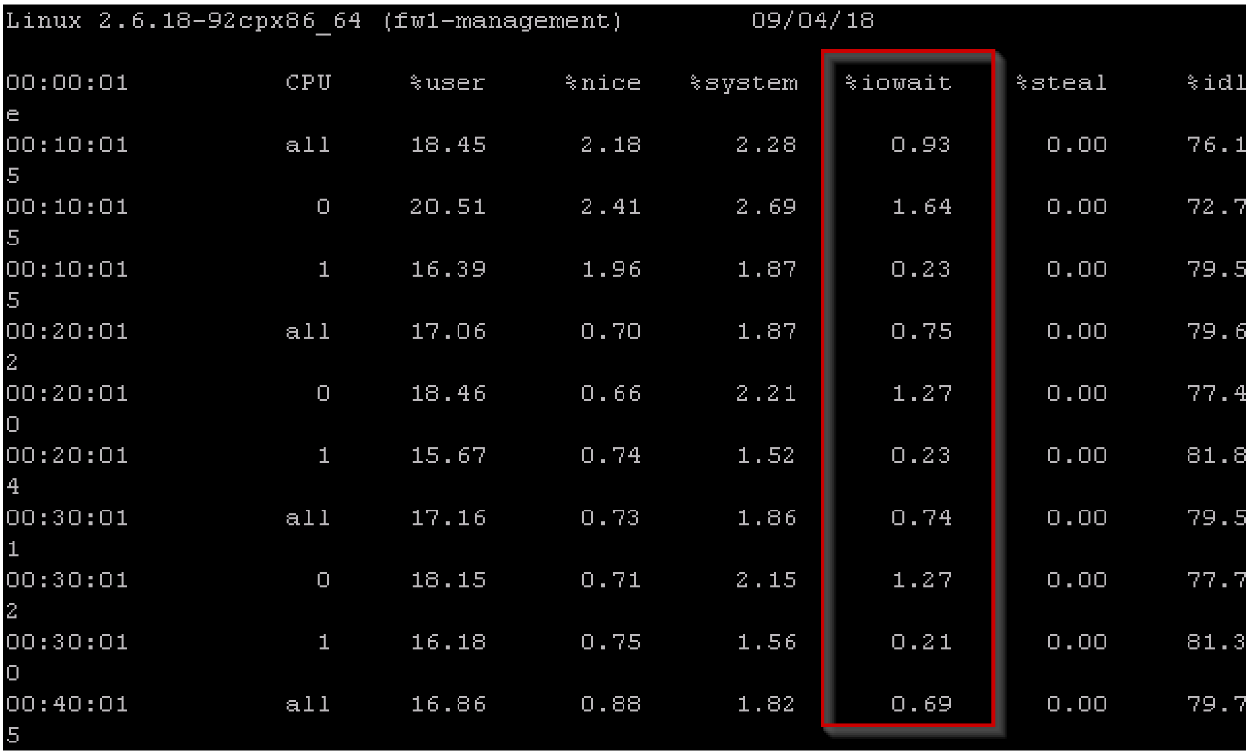
There is a constant amount of IOWait. The IOWait on a VM environment is typically due to Disk IO on a shared infrastructure with the combination of Check Point logging/indexing.



The IO correlates with the disk read/writes.



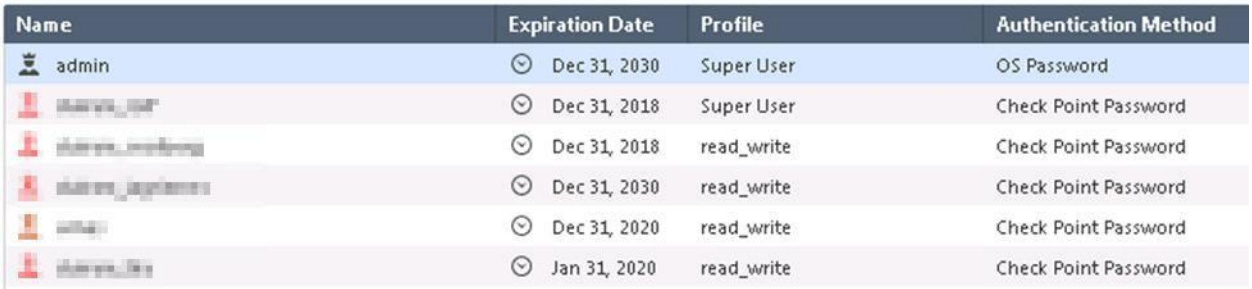
In general use, IOwait is low but consistent and should be monitored.


```
Linux 2.6.18-92cpx86_64 (fw1-management)          09/04/18

00:00:01           CPU     %user     %nice   %system   %iowait    %steal     %idl
e
00:10:01           all     18.45      2.18      2.28      0.93      0.00     76.1
5
00:10:01             0     20.51      2.41      2.69      1.64      0.00     72.7
5
00:10:01             1     16.39      1.96      1.87      0.23      0.00     79.5
5
00:20:01           all     17.06      0.70      1.87      0.75      0.00     79.6
2
00:20:01             0     18.46      0.66      2.21      1.27      0.00     77.4
0
00:20:01             1     15.67      0.74      1.52      0.23      0.00     81.8
4
00:30:01           all     17.16      0.73      1.86      0.74      0.00     79.5
1
00:30:01             0     18.15      0.71      2.15      1.27      0.00     77.7
2
00:30:01             1     16.18      0.75      1.56      0.21      0.00     81.3
0
00:40:01           all     16.86      0.88      1.82      0.69      0.00     79.7
5
```

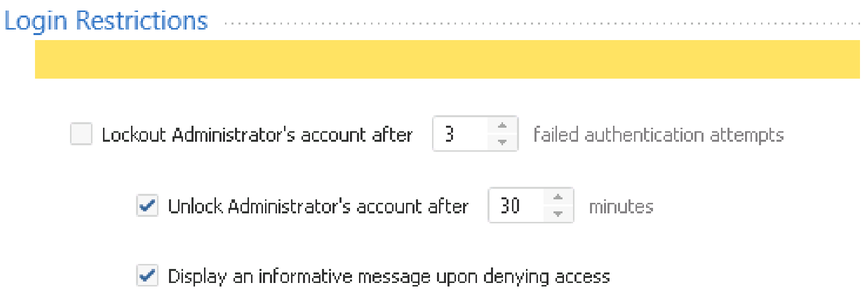
Local Users

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.



Name	Expiration Date	Profile	Authentication Method
admin	Dec 31, 2030	Super User	OS Password
[redacted]	Dec 31, 2018	Super User	Check Point Password
[redacted]	Dec 31, 2018	read_write	Check Point Password
[redacted]	Dec 31, 2030	read_write	Check Point Password
[redacted]	Dec 31, 2020	read_write	Check Point Password
[redacted]	Jan 31, 2020	read_write	Check Point Password

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 3 failed authentication attempts

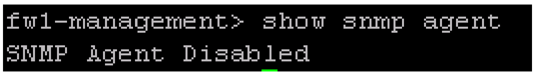
☑ Unlock Administrator's account after 30 minutes

☑ 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

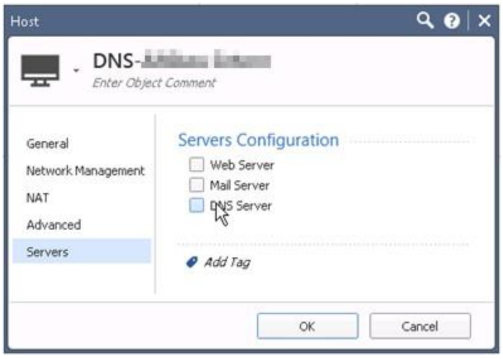
SNMP is used to monitor the system and identify any potential issues. SNMP agent is disabled.



```
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.



Servers Configuration

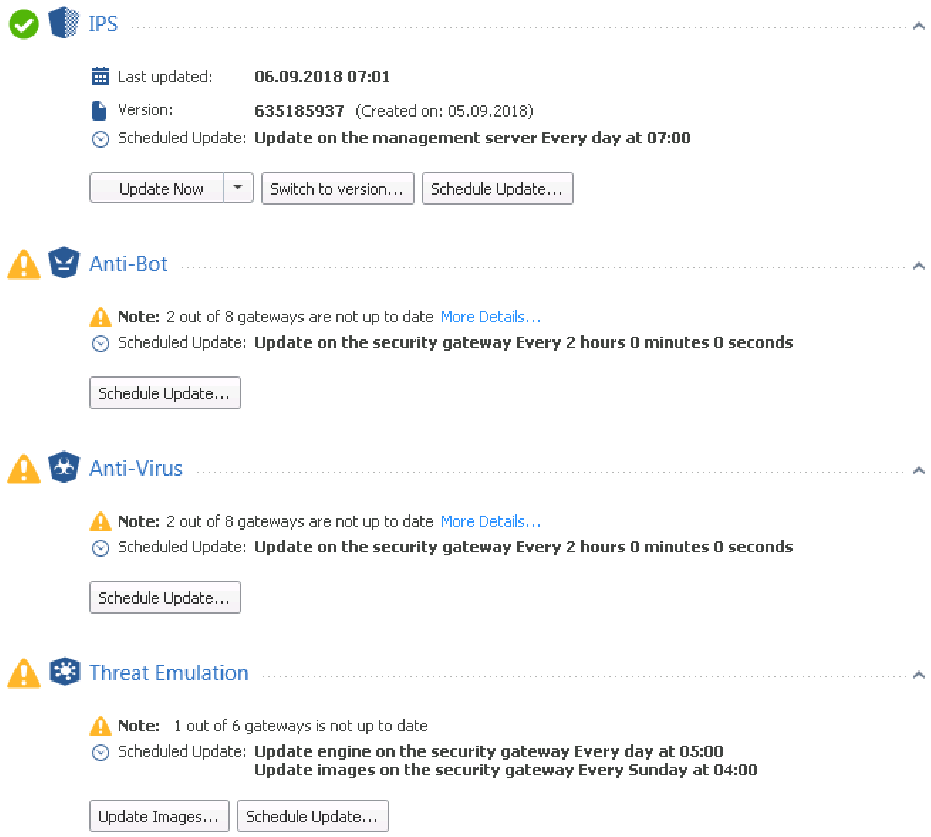
□ Web Server

□ Mail Server

□ DNS Server

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.



✓ IPS

Last updated: 06.09.2018 07:01
Version: 635185937 (Created on: 05.09.2018)
Scheduled Update: Update on the management server Every day at 07:00

⚠ Anti-Bot

⚠ Note: 2 out of 8 gateways are not up to date More Details...
Scheduled Update: Update on the security gateway Every 2 hours 0 minutes 0 seconds

⚠ Anti-Virus

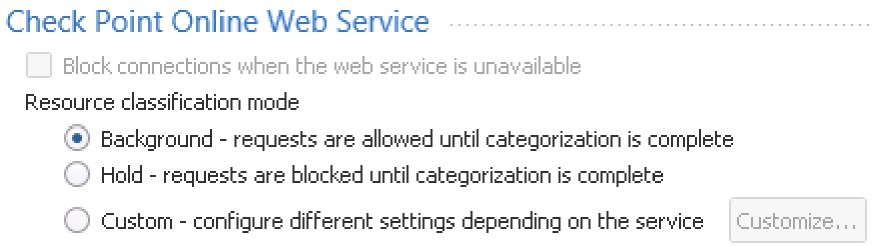
⚠ Note: 2 out of 8 gateways are not up to date More Details...
Scheduled Update: Update on the security gateway Every 2 hours 0 minutes 0 seconds

⚠ Threat Emulation

⚠ Note: 1 out of 6 gateways is not up to date
Scheduled Update: Update engine on the security gateway Every day at 05:00
Update images on the security gateway Every Sunday at 04:00

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

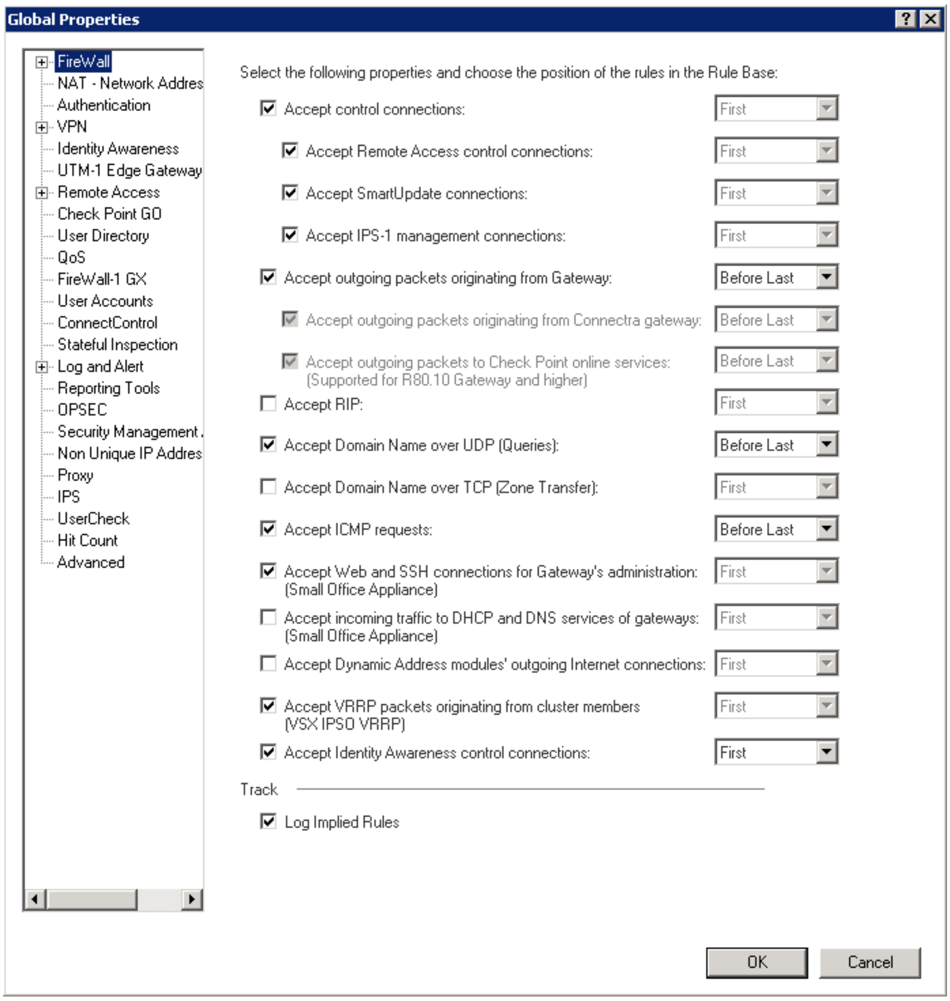
Resource classification mode

● 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.



Global Properties

- FireWall
- NAT - Network Addres
- Authentication
- VPN
- Identity Awareness
- UTM-1 Edge Gateway
- Remote Access
- Check Point GO
- User Directory
- QoS
- FireWall-1 GX
- User Accounts
- ConnectControl
- Stateful Inspection
- Log and Alert
- Reporting Tools
- OPSEC
- Security Management
- Non Unique IP Addres
- Proxy
- IPS
- UserCheck
- Hit Count
- Advanced

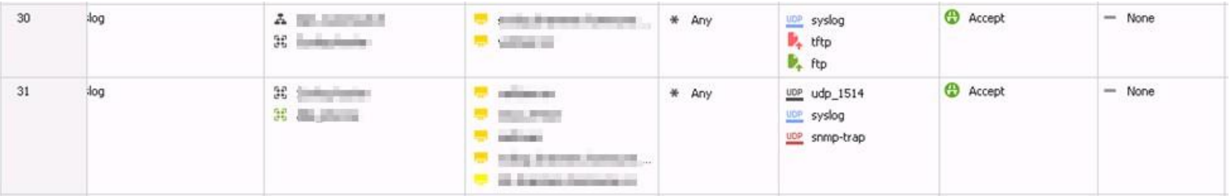
Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept control connections:	First
☑ Accept Remote Access control connections:	First
☑ Accept SmartUpdate connections:	First
☑ Accept IPS-1 management connections:	First
☑ Accept outgoing packets originating from Gateway:	Before Last
☑ Accept outgoing packets originating from Connectra gateway:	Before Last
☑ Accept outgoing packets to Check Point online services: (Supported for R80.10 Gateway and higher)	Before Last
☐ Accept RIP:	First
☑ Accept Domain Name over UDP (Queries):	Before Last
☐ Accept Domain Name over TCP (Zone Transfer):	First
☑ Accept ICMP requests:	Before Last
☑ Accept Web and SSH connections for Gateway's administration: (Small Office Appliance)	First
☐ Accept incoming traffic to DHCP and DNS services of gateways: (Small Office Appliance)	First
☐ Accept Dynamic Address modules' outgoing Internet connections:	First
☑ Accept VRRP packets originating from cluster members (VSX IPSO VRRP)	First
☑ Accept Identity Awareness control connections:	First

Track

☑ Log Implied Rules

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 cant be the case:

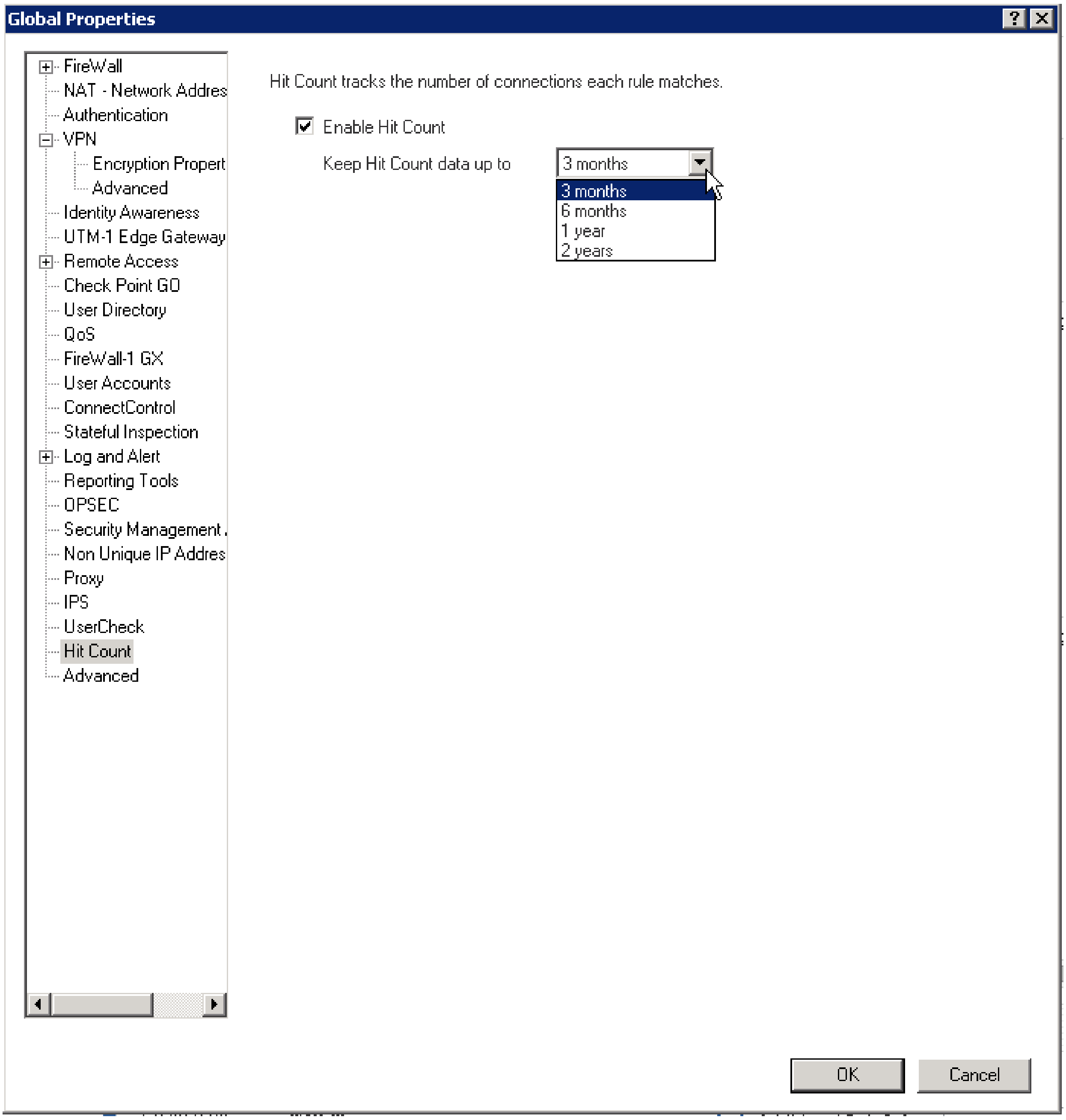


30	log	[redacted] [redacted]	[redacted] [redacted]	✱ Any	syslog tftp ftp	Accept	— None
31	log	[redacted] [redacted]	[redacted] [redacted] [redacted] [redacted] [redacted]	✱ Any	udp_1514 syslog snmp-trap	Accept	— None

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

Hit Count tracks the number of connections each rule matches.

☑ Enable Hit Count

Keep Hit Count data up to: 3 months

Cluster1 Cluster Review

The following findings have been identified on the R80.10 VSec cluster:

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

Each recommendation is rated as follows:

✗	Serious - Needs immediate attention
⚠	Attention - Needs attention
✓	Good - No need for any action
ℹ	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

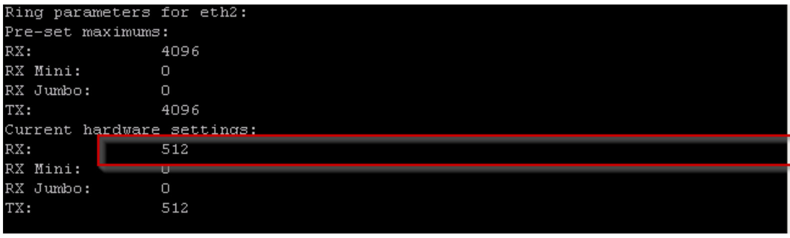
AAA is used to authorize, authenticate and account user access. Only local user accounts are configured on the gateway:

```
RADIUS:  [DISABLED]
TACACS:  [DISABLED]
```

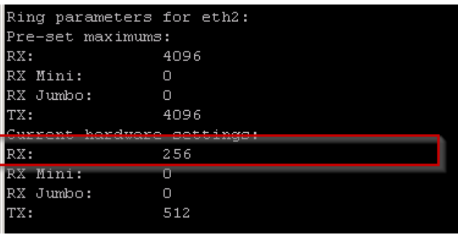
AAA is used to determine who actually is logging onto the gateway and their access revoked when removed from the company/Active Directory.

Interface Buffers

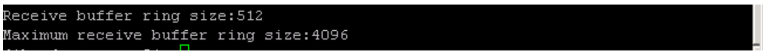
The RX interface buffer between cluster members do not match:



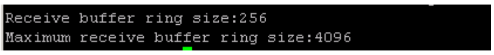
```
Ring parameters for eth2:
Pre-set maximums:
RX:             4096
RX Mini:        0
RX Jumbo:       0
TX:             4096
Current hardware settings:
RX:             512
RX Mini:        0
RX Jumbo:       0
TX:             512
```



```
Ring parameters for eth2:
Pre-set maximums:
RX:             4096
RX Mini:        0
RX Jumbo:       0
TX:             4096
Current hardware settings:
RX:             256
RX Mini:        0
RX Jumbo:       0
TX:             512
```



```
Receive buffer ring size:512
Maximum receive buffer ring size:4096
```



```
Receive buffer ring size:256
Maximum receive buffer ring size:4096
```

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 "ync"
[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_2];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

Number     Unique Address  Assigned Load   State

1 (local)  172.20.250.2    100%            Active
2          172.20.250.3    0%              Standby

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

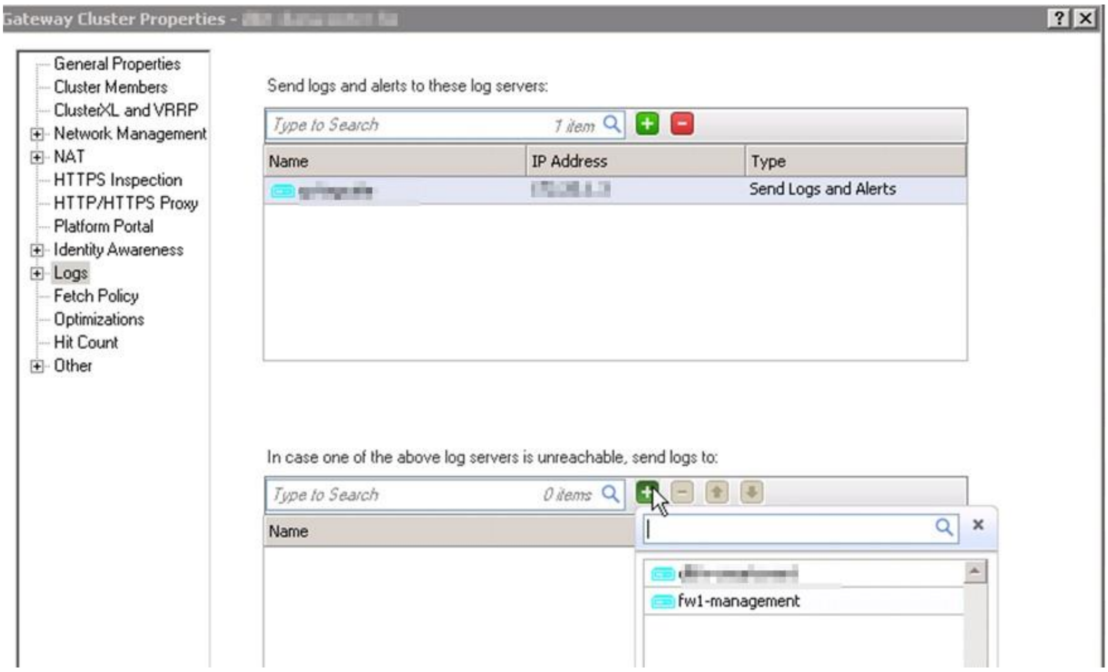
It appears an interface went down:

```
[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.



Gateway Cluster Properties - [redacted]

Send logs and alerts to these log servers:

Name	IP Address	Type
[redacted]	[redacted]	Send Logs and Alerts

In case one of the above log servers is unreachable, send logs to:

[redacted]
fw1-management

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).

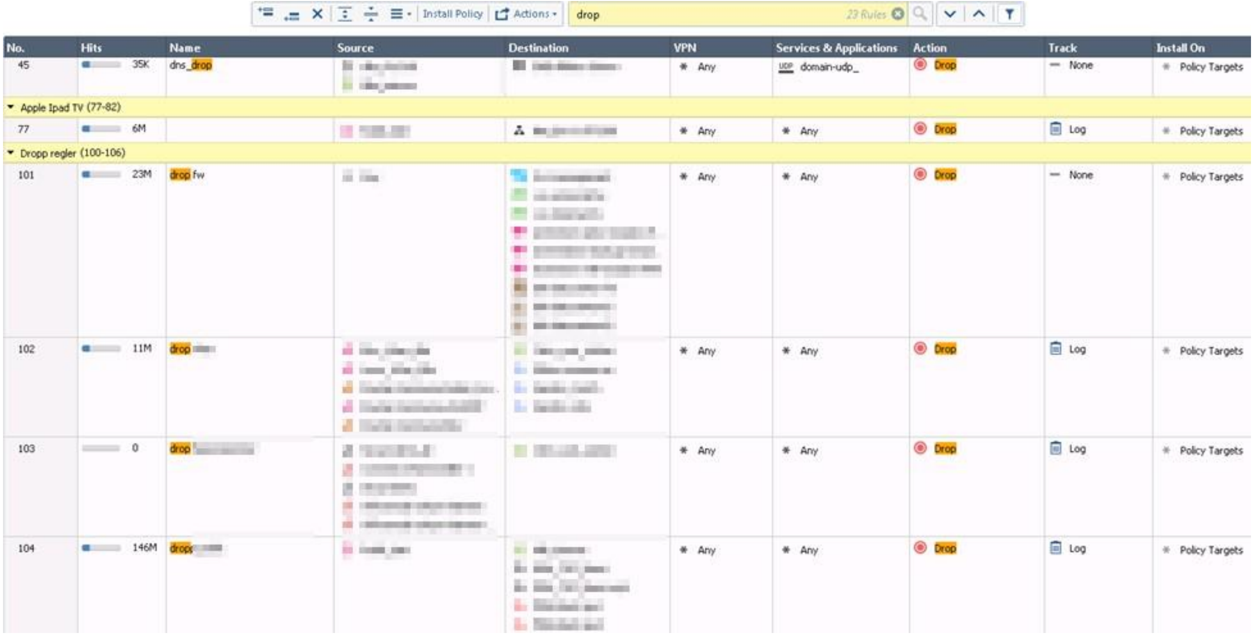
Check Point recommend to configure Anti-Spoofing correctly.

```
[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-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.1101 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth2.1104 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.3 interface is not protected by the anti-spoofin
g feature.
[fw4_0];FW-1: Warning: The eth4.220 interface is not protected by the anti-spoof
ing feature.
[fw4_0];FW-1: Warning: The eth1.381 interface is not protected by the anti-spoof
ing feature.
[fw4_0];FW-1: Warning: The eth1.1105 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.2 interface is not protected by the anti-spoofin
g feature.
[fw4_0];FW-1: Warning: The eth2.1103 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.1100 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth2.4 interface is not protected by the anti-spoofin
g feature.
[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-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.1101 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth2.1104 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.3 interface is not protected by the anti-spoofin
g feature.
[fw4_0];FW-1: Warning: The eth4.220 interface is not protected by the anti-spoof
ing feature.
[fw4_0];FW-1: Warning: The eth1.381 interface is not protected by the anti-spoof
ing feature.
[fw4_0];FW-1: Warning: The eth1.1105 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.2 interface is not protected by the anti-spoofin
g feature.
[fw4_0];FW-1: Warning: The eth2.1103 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.1100 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth2.4 interface is not protected by the anti-spoofin
g feature.
[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-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.1101 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth2.1104 interface is not protected by the anti-spoo
fing feature.
[fw4_0];FW-1: Warning: The eth1.3 interface is not protected by the anti-spoofin
g feature.
[fw4_0];FW-1: Warning: The eth4.220 interface is not protected by the anti-spoof
ing feature.
[fw4_0];FW-1: Warning: The eth1.381 interface is not protected by the anti-spoof
ing feature.
[fw4_0];FW-1: Warning: The eth1.1105 interface is not protected by the anti-spoo
fing feature.
```

Drop Templates

There are a lot drop rules in the policy with high connection hits. Enabling Drop templates would improve acceleration statistics, 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.

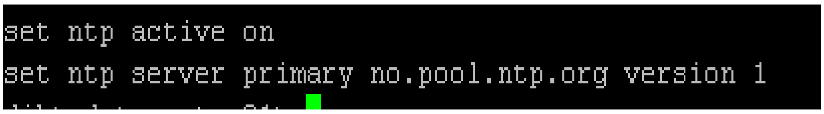
```
[Expert@FW1:0]# fw stat -l
HOST        IF      POLICY            DATE                   TOTAL     REJECT  DROP ACCEPT    LOG
localhost >eth0 Standard_Policy  4Sep2018 14:04:07 :  33107622       0   8733 33098889 1050642
localhost <eth0 Standard_Policy  4Sep2018 14:04:07 :  66705190       0     0 66705190    129
localhost >eth2 Standard_Policy  4Sep2018 14:04:07 :         2      0      2      0      2
localhost >eth3 Standard_Policy 4Sep2018 14:04:07 :     79428      0      0  79428      0
localhost <eth3 Standard_Policy 4Sep2018 14:04:07 :     79428      0      0  79428      1
localhost >eth2.1102 Standard_Policy  4Sep2018 14:04:07 :  30961618    0 1506281 29455337 1370017
localhost <eth2.1102 Standard_Policy  4Sep2018 14:04:07 :  393685690  0     10 393685680   2329
localhost >eth1.1101 Standard_Policy  4Sep2018 14:04:07 :  69660874    0 1890450 67770424 1855277
localhost <eth1.1101 Standard_Policy  4Sep2018 14:04:07 :  34318436    0      0 34318436      0
localhost >eth1.383 Standard_Policy  4Sep2018 14:04:07 :     678      0     17    661  90784
localhost <eth1.383 Standard_Policy  4Sep2018 14:04:07 :     784      0      0    784      0
localhost >eth2.1104 Standard_Policy  4Sep2018 14:04:07 :  3614476      0 1771278 1843198 2011710
localhost <eth2.1104 Standard_Policy  4Sep2018 14:04:07 :  683430      0      0 683430     10
localhost >eth1.3 Standard_Policy  4Sep2018 14:04:07 :  319287      0   1485 317802  10292
localhost <eth1.3 Standard_Policy  4Sep2018 14:04:07 :  4770118      0      0 4770118      0
localhost >eth4.220 Standard_Policy  4Sep2018 14:04:07 :  482899151      0 9593529 473305622
11925898
localhost <eth4.220 Standard_Policy  4Sep2018 14:04:07 :  334253693      0      0 334253693   4835
localhost >eth1.381 Standard_Policy  4Sep2018 14:04:07 :  313769      0 31892 281877  79702
localhost <eth1.381 Standard_Policy 4Sep2018 14:04:07 :   242813      0      0 242813      0
localhost >eth1.384 Standard_Policy 4Sep2018 14:04:07 :   269018      0     85 268933     99
localhost <eth1.384 Standard_Policy 4Sep2018 14:04:07 :   255359      0      0 255359      0
localhost >eth1.1105 Standard_Policy  4Sep2018 14:04:07 :  120657284      0 3895776 116761508
4056457
localhost <eth1.1105 Standard_Policy  4Sep2018 14:04:07 :  94408310      0      0 94408310    297
localhost >eth1.2 Standard_Policy  4Sep2018 14:04:07 :  12369679      0 834655 11535024 1551993
localhost <eth1.2 Standard_Policy  4Sep2018 14:04:07 :  16549407      0      0 16549407      1
localhost >eth1.7 Standard_Policy  4Sep2018 14:04:07 :   29252      0  24533   4719  25989
localhost <eth1.7 Standard_Policy  4Sep2018 14:04:07 :    2032      0      0   2032      0
localhost >eth1.382 Standard_Policy  4Sep2018 14:04:07 :   90448      0   4678  85770 109278
localhost <eth1.382 Standard_Policy  4Sep2018 14:04:07 :   69547      0      0  69547      0
localhost >eth1.6 Standard_Policy  4Sep2018 14:04:07 :   70026      0  35050  34976 126459
localhost <eth1.6 Standard_Policy  4Sep2018 14:04:07 :   24972      0      0  24972      0
localhost >eth2.1103 Standard_Policy  4Sep2018 14:04:07 :  456559      0  56282 400277  74268
localhost <eth2.1103 Standard_Policy  4Sep2018 14:04:07 :  517609      0      0 517609      0
localhost >eth1.1100 Standard_Policy  4Sep2018 14:04:07 :  490204651      0 720192 489484459
11646193
localhost <eth1.1100 Standard_Policy  4Sep2018 14:04:07 :  244667349      0     28 244667321   4075
localhost >eth1.5 Standard_Policy  4Sep2018 14:04:07 :   75015      0  57656  17359  40059
localhost <eth1.5 Standard_Policy  4Sep2018 14:04:07 :   21747      0      0  21747      0
localhost >eth2.4 Standard_Policy  4Sep2018 14:04:07 :  315851      0 122120 193731 119691
localhost <eth2.4 Standard_Policy  4Sep2018 14:04:07 :  196279      0      0 196279      0
localhost >eth1.380 Standard_Policy  4Sep2018 14:04:07 :  2326391      0 2297403 28988 2297421
localhost <eth1.380 Standard_Policy  4Sep2018 14:04:07 :   28154      0      0  28154      0
```



No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
45	35K	dns_drop	[redacted]	[redacted]	Any	domain-udp_	Drop	None	Policy Targets
Apple Ipad TV (77-82)									
77	6M		[redacted]	[redacted]	Any	Any	Drop	Log	Policy Targets
Dropp regler (100-106)									
101	23M	drop fw	[redacted]	[redacted]	Any	Any	Drop	None	Policy Targets
102	11M	drop [redacted]	[redacted]	[redacted]	Any	Any	Drop	Log	Policy Targets
103	0	drop [redacted]	[redacted]	[redacted]	Any	Any	Drop	Log	Policy Targets
104	146M	drop [redacted]	[redacted]	[redacted]	Any	Any	Drop	Log	Policy Targets

NTP

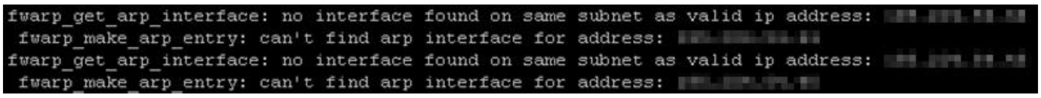
NTP versions 1-3 are no longer maintained, so any security flaws uncovered are not patched and remain dangerously exploitable. There are many NTP exploits so using the latest version is highly recommended:



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

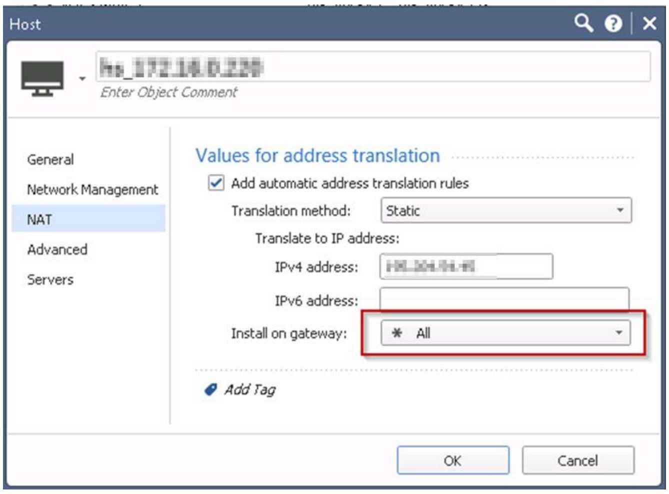
ARP

$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: [redacted]
 fwarp_make_arp_entry: can't find arp interface for address: [redacted]
fwarp_get_arp_interface: no interface found on same subnet as valid ip address: [redacted]
 fwarp_make_arp_entry: can't find arp interface for address: [redacted]
```

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



[redacted]

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

Translation method: Static

Translate to IP address:

IPv4 address: [redacted]

IPv6 address:

Install on gateway: All

Stealth

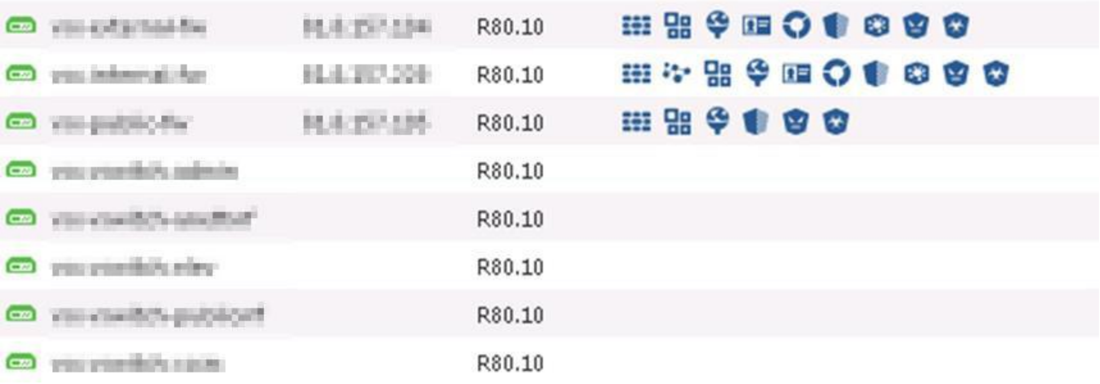
A “stealth” rule should be added as one of the very top rules stating:

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:



[redacted]	[redacted]	R80.10
[redacted]	[redacted]	R80.10
[redacted]	[redacted]	R80.10
[redacted]		R80.10
[redacted]		R80.10
[redacted]		R80.10
[redacted]		R80.10
[redacted]		R80.10

VS0

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

VS1 – vs-xxxa

Topic	Status	Recommendations
IPS Profile	⚠	No scope defined.
Application Control Policy	⚠	Overhead due to configuration.
Policy Types	ℹ	
NAT Connections	ℹ	
Internet Connectivity	✗	Failed to connect to URL.
Misplaced Rules	⚠	Performance can be improved by moving rules within the policy.
Fragments	⚠	Determine source of fragments.
Stealth	✗	Missing.

VS2 – vs-xxxb

Topic	Status	Recommendations
Application Control Policy	⚠	Overhead due to configuration.
Policy Types	ℹ	
Old UDP Session	⚠	High amount of packets being dropped due to expired session.
Misplaced Rules	✗	Security concern.
NAT Connections	ℹ	
Fragments	⚠	Determine source of fragments.
Stealth	✗	Missing.

VS8 – vs-xxxc

Topic	Status	Recommendations
ALL	✗	No policy installed.

Each recommendation is rated as follows:

✗	Serious - Needs immediate attention
⚠	Attention - Needs attention
✓	Good - No need for any action
ℹ	Informational

VS0

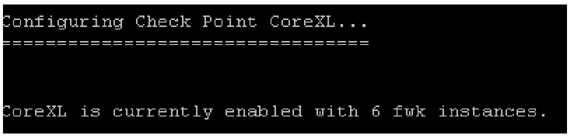
Hotfix

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 fwk 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#8#BUNDLE_R80_10_JUMBO_HF#103/Check_Point_R80
_10_JUMBO_HF_Bundle_T103_sk116380_FULL.tgz
730M /var/log/opt/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_134845_2.log
2.0G  /var/log/opt/CPsuite-R80/fw1/CTX/CTX00001/2018-06-14_105259_1.log
985M /var/log/opt/CPsuite-R80/fw1/CTX/CTX00001/2018-06-15_000000.log
1.5G  /opt/CPUserCheckPortal/CTX/CTX00001/log/error_log
```

```
Big Files:
515M
      /var/log/CPda/repository/CheckPoint#CPUpdates#All#6.0#4#8#BUNDLE_R80_10_JUMBO_HF#103/Check_Poi
nt_R80_10_JUMBO_HF_Bundle_T103_sk116380_FULL.tgz
2.0G  /var/log/opt/CPsuite-R80/fw1/CTX/CTX00002/2018-06-14_140408_3.log
917M  /var/log/opt/CPsuite-R80/fw1/CTX/CTX00002/2018-06-14_000000.log
2.0G  /var/log/opt/CPsuite-R80/fw1/CTX/CTX00002/2018-06-14_115824_2.log
2.0G /var/log/opt/CPsuite-R80/fw1/CTX/CTX00002/2018-06-14_100114_1.log
844M  /var/log/dump/usermode/temain.16109.core.gz
```

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
```

```
Usermode Cores:
-rw-r--r-- 1 admin root 124589091 Sep  2 09:43 fwk2_4.23114.core.gz
-rw-r--r-- 1 admin root 884717619 Aug 24 13:52 temain.16109.core.gz
```

The system should be monitored and TAC incident raised once coredump is created.

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

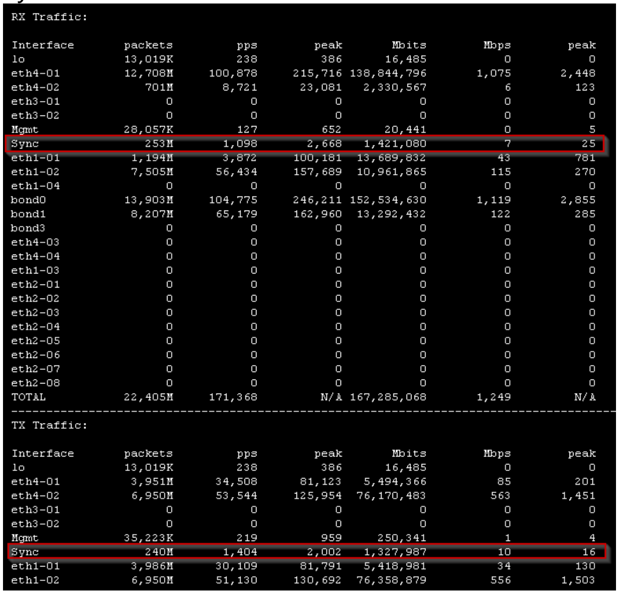
The customer mentioned they have occasional Sync issues they cant explain. As the System was recently rebooted we don't have many Sync errors to investigate:

```
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:



```
RX Traffic:

Interface      packets       pps      peak       Mbits      Mbps      peak
lo             13,019K       238       386      16,485         0         0
eth4-01        12,708M   100,878   215,716 138,844,796     1,075     2,448
eth4-02           701M     8,721    23,081   2,330,567         6       123
eth3-01              0         0         0           0         0         0
eth3-02              0         0         0           0         0         0
Mgmt           28,057K       127       652      20,441         0         5
Sync              253M     1,098     2,668   1,421,080         7        25
eth1-01         1,194M     3,872   100,181  13,689,832        43       781
eth1-02         7,505M    56,434   157,689  10,961,865       115       270
eth1-04              0         0         0           0         0         0
bond0          13,903M   104,775   246,211 152,534,630     1,119     2,855
bond1           8,207M    65,179   162,960  13,292,432       122       285
bond3                0         0         0           0         0         0
eth4-03              0         0         0           0         0         0
eth4-04              0         0         0           0         0         0
eth1-03              0         0         0           0         0         0
eth2-01              0         0         0           0         0         0
eth2-02              0         0         0           0         0         0
eth2-03              0         0         0           0         0         0
eth2-04              0         0         0           0         0         0
eth2-05              0         0         0           0         0         0
eth2-06              0         0         0           0         0         0
eth2-07              0         0         0           0         0         0
eth2-08              0         0         0           0         0         0
TOTAL          22,405M   171,368       N/A 167,285,068     1,249       N/A
------------------------------------------------------------------------------
TX Traffic:

Interface      packets       pps      peak       Mbits      Mbps      peak
lo             13,019K       238       386      16,485         0         0
eth4-01         3,951M    34,508    81,123   5,494,366        85       201
eth4-02         6,950M    53,544   125,954  76,170,483       563     1,451
eth3-01              0         0         0           0         0         0
eth3-02              0         0         0           0         0         0
Mgmt           35,223K       219       959     250,341         1         4
Sync              240M     1,404     2,002   1,327,987        10        16
eth1-01         3,986M    30,109    81,791   5,418,981        34       130
eth1-02         6,950M    51,130   130,692  76,358,879       556     1,503
```

But we do see a minimal out of RX-Drp and RX-Ovr on the Sync interface:

```
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
Mgmt       1500   0 27904899      0      0      0 34969843      0      0      0 BMRU
Sync       1500   0 252316994      0     83     83 238780989      0      0      0 BMRU
bond0      1500   0 13745610464     27      0      0 7845031952      0      0      0 BMmRU
bond1      1500   0 8114082557      0      0      0 13742926331      0      0      0 BMmRU
bond3      1500   0        0      0      0      0        0      0      0      0 BMmU
eth1-01    1500   0 1185476048     27      0      0 3941005823      0      0      0 BMsRU
eth1-02    1500   0 7421066192      0      0      0 6875710596      0      0      0 BMsRU
eth1-04    1500   0        0      0      0      0        0      0      0      0 BMRU
eth3-01    1500   0        0      0      0      0        0      0      0      0 BMsU
eth3-02    1500   0        0      0      0      0        0      0      0      0 BMsU
eth4-01    1500   0 12560138864      0      0      0 3904028261      0      0      0 BMsRU
eth4-02    1500   0 693017000           0      0 6867218841      0      0      0 BMsRU
lo        16436   0 12840407      0      0      0 12840407      0      0      0 LRU
```

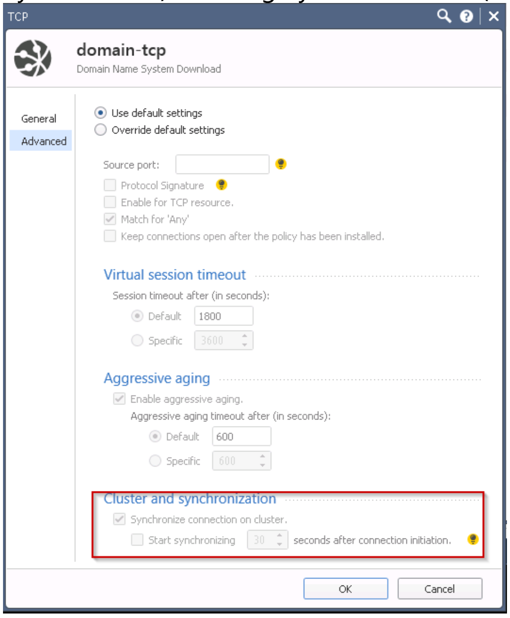
- **"The "RX-OK/ERR/DRP/OVR" columns** give statistics about the packets that have been received by the interface so far. "OK" stands for "correctly received", "ERR" for "received but with incorrect checksum" (happens when the connection is bad), "DRP" for "dropped because my receive buffer was too full" (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).



TCP

domain-tcp
Domain Name System Download

● Use default settings
○ Override default settings

Source port:
□ Protocol Signature
□ Enable for TCP resource.
☑ Match for 'Any'
□ Keep connections open after the policy has been installed.

Virtual session timeout

Session timeout after (in seconds):
● Default 1800
○ Specific 3600

Aggressive aging

☑ Enable aggressive aging.
Aggressive aging timeout after (in seconds):
● Default 600
○ Specific 600

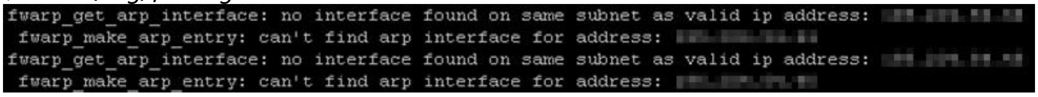
Cluster and synchronization

☑ Synchronize connection on cluster.
□ Start synchronizing 30 seconds after connection initiation.

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

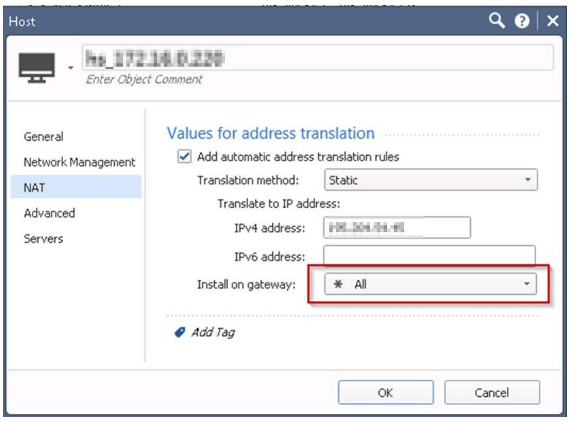
ARP

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



```
fwarp_get_arp_interface: no interface found on same subnet as valid ip address: [redacted]
 fwarp_make_arp_entry: can't find arp interface for address: [redacted]
fwarp_get_arp_interface: no interface found on same subnet as valid ip address: [redacted]
 fwarp_make_arp_entry: can't find arp interface for address: [redacted]
```

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



Host

[redacted]

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

Translation method: Static

Translate to IP address:

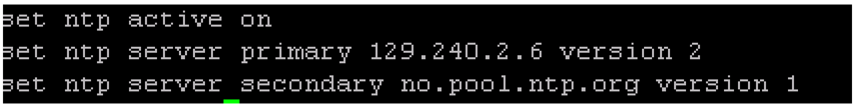
IPv4 address: [redacted]

IPv6 address:

Install on gateway: ✱ All

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

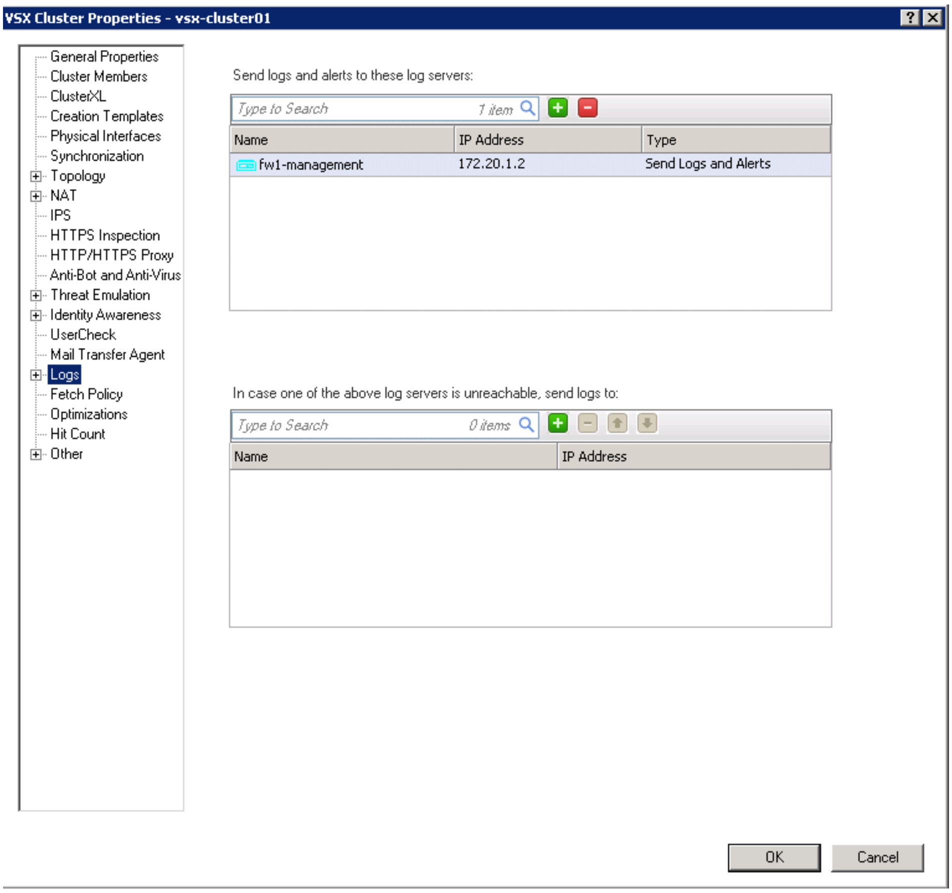
Note: This is not relevant for VS0 as CoreXL should be disabled. This is regarding user mode CoreXL instances across the system for VS instances.

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:



VSX Cluster Properties - vsx-cluster01

Send logs and alerts to these log servers:

Type to Search 1 item

Name	IP Address	Type
fw1-management	172.20.1.2	Send Logs and Alerts

In case one of the above log servers is unreachable, send logs to:

Type to Search 0 items

Name	IP Address

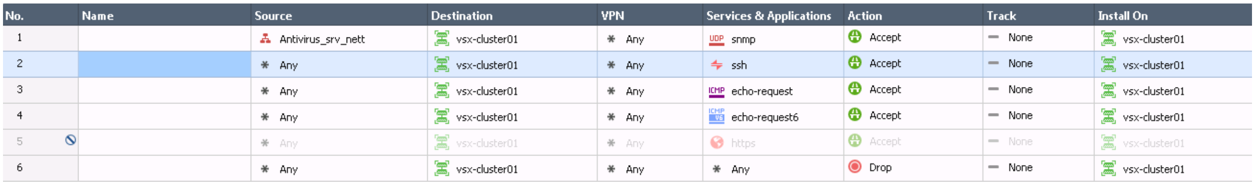
Stealth

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.

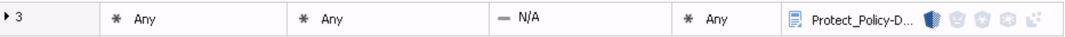


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		Antivirus_srv_nett	vsx-cluster01	Any	UDP snmp	Accept	None	vsx-cluster01
2		Any	vsx-cluster01	Any	ssh	Accept	None	vsx-cluster01
3		Any	vsx-cluster01	Any	ICMP echo-request	Accept	None	vsx-cluster01
4		Any	vsx-cluster01	Any	ICMP V6 echo-request6	Accept	None	vsx-cluster01
5 ⦸		Any	vsx-cluster01	Any	https	Accept	None	vsx-cluster01
6		Any	vsx-cluster01	Any	Any	Drop	None	vsx-cluster01

VS1 – vs-xxxa

IPS Profile

The IPS profile does not have a scope defined:



▸ 3	Any	Any	N/A	Any	Protect_Policy-D...

Consultant Report

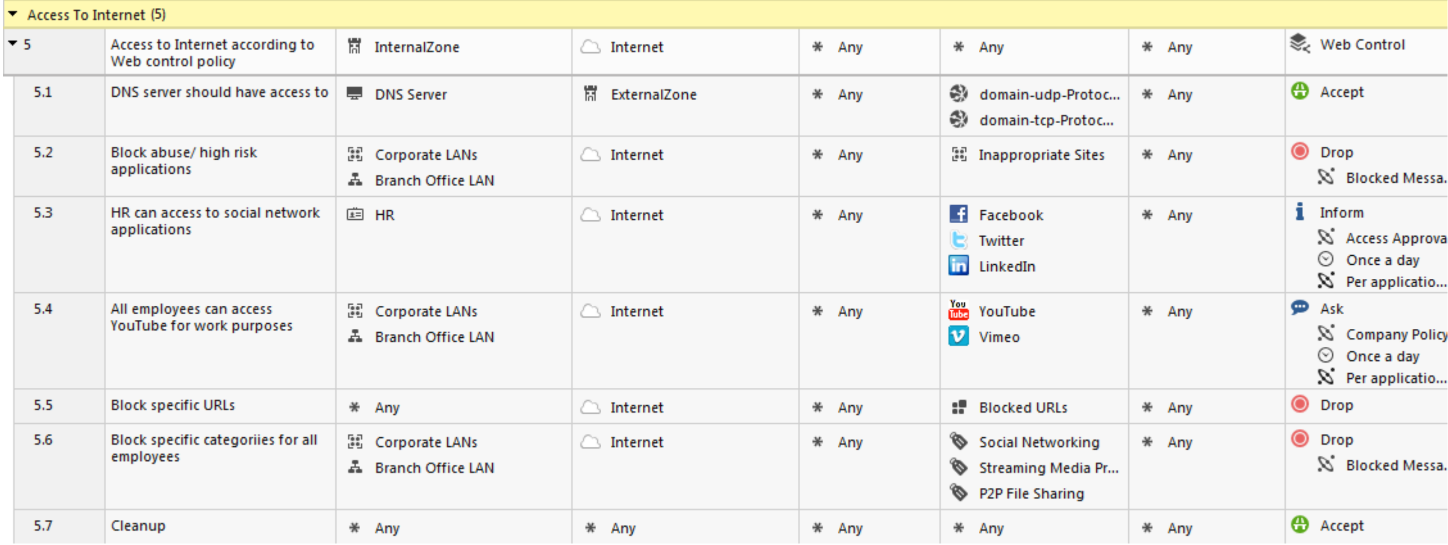
Application Control Policy

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.

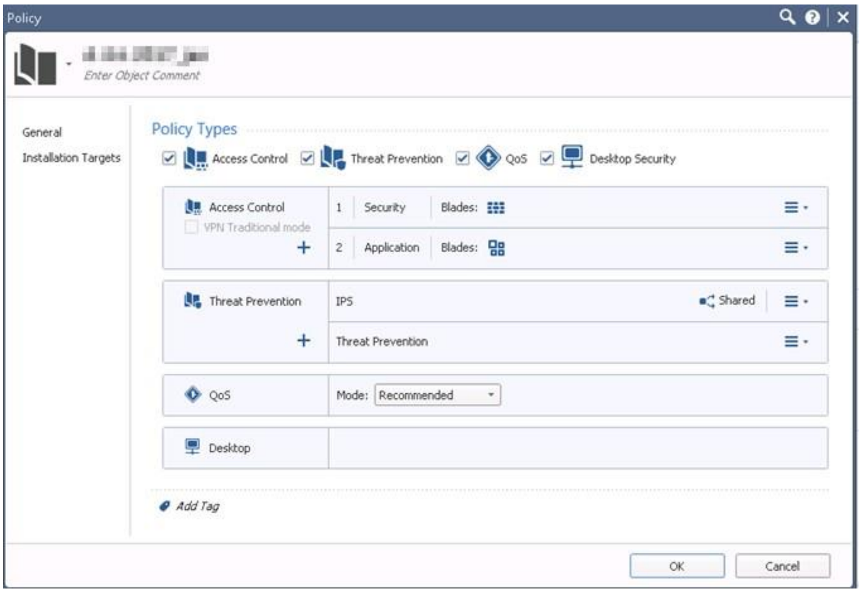


▾ Access To Internet (5)

▾ 5	Access to Internet according to Web control policy	InternalZone	Internet	Any	Any	Any	Web Control
5.1	DNS server should have access to	DNS Server	ExternalZone	Any	domain-udp-Protoc... domain-tcp-Protoc...	Any	Accept
5.2	Block abuse/ high risk applications	Corporate LANs Branch Office LAN	Internet	Any	Inappropriate Sites	Any	Drop Blocked Messa.
5.3	HR can access to social network applications	HR	Internet	Any	Facebook Twitter LinkedIn	Any	Inform Access Approva Once a day Per applicatio...
5.4	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN	Internet	Any	YouTube Vimeo	Any	Ask Company Policy Once a day Per applicatio...
5.5	Block specific URLs	Any	Internet	Any	Blocked URLs	Any	Drop
5.6	Block specific categoriies for all employees	Corporate LANs Branch Office LAN	Internet	Any	Social Networking Streaming Media Pr... P2P File Sharing	Any	Drop Blocked Messa.
5.7	Cleanup	Any	Any	Any	Any	Any	Accept

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.



Policy

[redacted]
Enter Object Comment

General
Installation Targets

Policy Types

☑ Access Control ☑ Threat Prevention ☑ QoS ☑ Desktop Security

Access Control □ VPN Traditional mode	1	Security	Blades:
	2	Application	Blades:
Threat Prevention	IPS		Shared
	Threat Prevention		
QoS	Mode: Recommended		
Desktop			

Consultant Report

NAT Connections

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

```
Accelerated Path------------------------------------------------------------
C total conns                     65328    C templates                     305
C TCP conns                       56772    C delayed TCP conns             865
C non TCP conns                    8556    C delayed nonTCP con              0
conns from templates             811402    temporary conns               57855
nat conns                       4002483    dropped packets               10692
```

```
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-xxxa (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-xxxb (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-xxxa (ID 1).
[Expert@vsx-2:1]# curl_cli -k -Is https://updates.checkpoint.com| head -1

[Expert@vsx-2:1]# vsenv 2
Context is set to Virtual Device vsx-2_vs-xxxb (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 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 271  |    592425|
|Rule 266  |     73581|
|Rule 269  |     73570|
|Rule 291  |     56397|
|Rule 297  |     50555|
-----------------------
```

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:
        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-xxxb

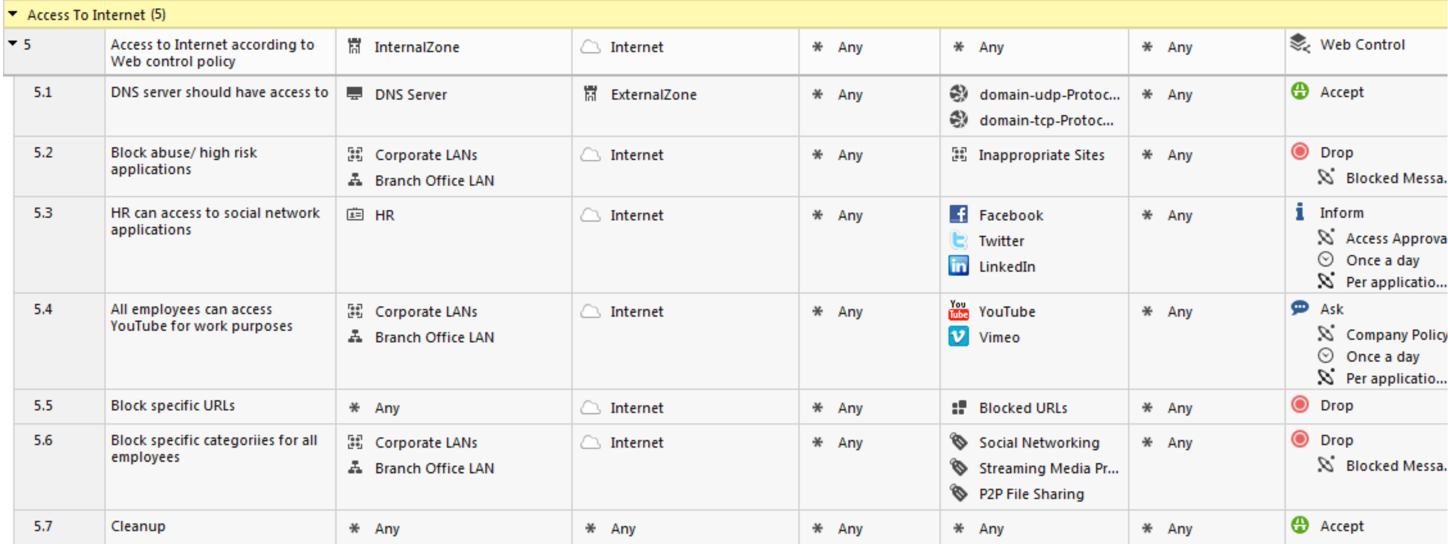
Application Control Policy

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.

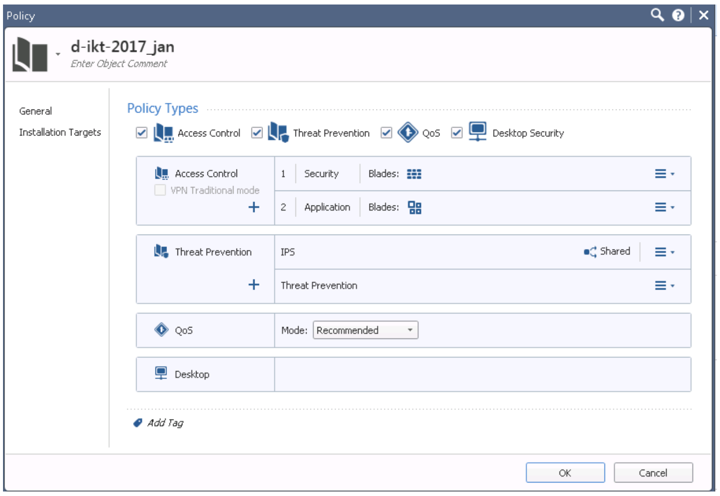


▾ Access To Internet (5)

▾ 5	Access to Internet according to Web control policy	InternalZone	Internet	Any	Any	Any	Web Control
5.1	DNS server should have access to	DNS Server	ExternalZone	Any	domain-udp-Protoc... domain-tcp-Protoc...	Any	Accept
5.2	Block abuse/ high risk applications	Corporate LANs Branch Office LAN	Internet	Any	Inappropriate Sites	Any	Drop Blocked Messa...
5.3	HR can access to social network applications	HR	Internet	Any	Facebook Twitter LinkedIn	Any	Inform Access Approva... Once a day Per applicatio...
5.4	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN	Internet	Any	YouTube Vimeo	Any	Ask Company Policy Once a day Per applicatio...
5.5	Block specific URLs	Any	Internet	Any	Blocked URLs	Any	Drop
5.6	Block specific categoriies for all employees	Corporate LANs Branch Office LAN	Internet	Any	Social Networking Streaming Media Pr... P2P File Sharing	Any	Drop Blocked Messa...
5.7	Cleanup	Any	Any	Any	Any	Any	Accept

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.



Policy

d-ikt-2017_jan

Enter Object Comment

General
Installation Targets

Policy Types

☑ Access Control ☑ Threat Prevention ☑ QoS ☑ Desktop Security

Access Control
□ VPN Traditional mode
1 Security Blades:
2 Application Blades:

Threat Prevention
IPS Shared
Threat Prevention

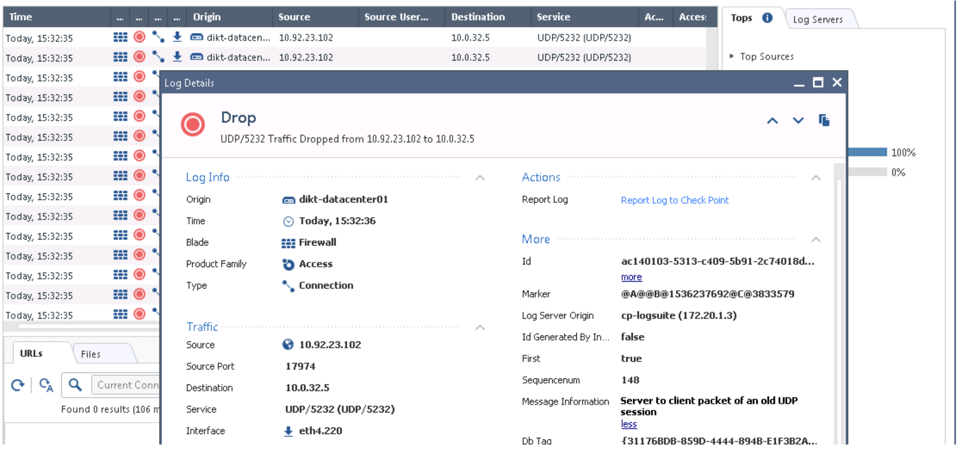
QoS Mode: Recommended

Desktop

Add Tag

Old UDP Sessions

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



```
Time              Origin          Source        Source User...  Destination  Service               Ac...  Acces:
Today, 15:32:35   dikt-datacen... 10.92.23.102                  10.0.32.5    UDP/5232 (UDP/5232)
Today, 15:32:35   dikt-datacen... 10.92.23.102                  10.0.32.5    UDP/5232 (UDP/5232)
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
Today, 15:32:35
```

Log Details

Drop
UDP/5232 Traffic Dropped from 10.92.23.102 to 10.0.32.5

Log Info

Origin	dikt-datacenter01
Time	Today, 15:32:36
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	10.92.23.102
Source Port	17974
Destination	10.0.32.5
Service	UDP/5232 (UDP/5232)
Interface	eth4.220

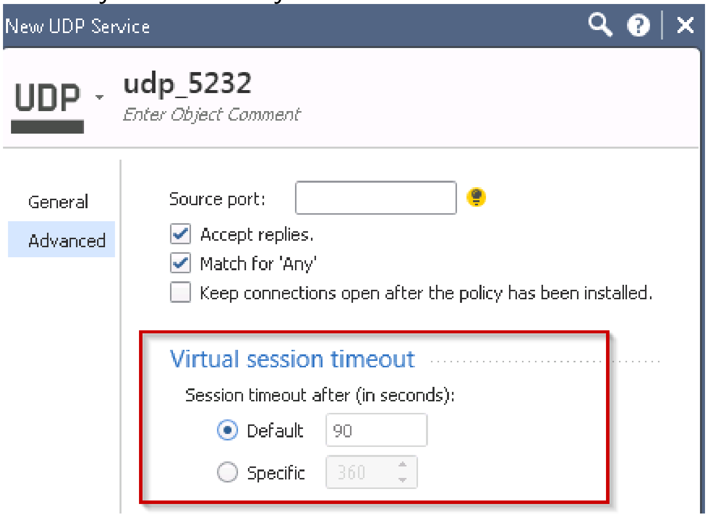
Actions

Report Log	Report Log to Check Point

More

Id	ac140103-5313-c409-5b91-2c74018d... more
Marker	@A@@B@1536237692@C@3833579
Log Server Origin	cp-logsuite (172.20.1.3)
Id Generated By In...	false
First	true
Sequencenum	148
Message Information	Server to client packet of an old UDP session less
Db Tag	{31176BDB-859D-4444-894B-E1F3B2A...

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



New UDP Service

UDP udp_5232
Enter Object Comment

Source port:

☑ Accept replies.
☑ Match for 'Any'
☐ Keep connections open after the policy has been installed.

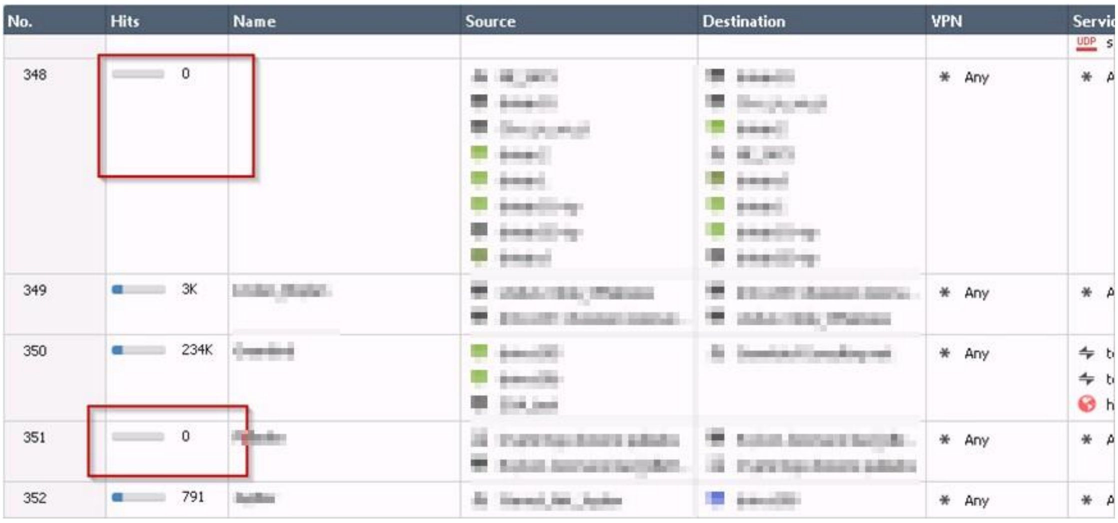
Virtual session timeout
Session timeout after (in seconds):
● Default 90
○ Specific 360

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:

```
Top Rule Hits
--------------------------------
|rule index|rule count|
--------------------------------
|Rule 121  |      22676|
|Rule 247  |          2|
--------------------------------
```

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.



No.	Hits	Name	Source	Destination	VPN	Servi
348	0		[redacted]	[redacted]	Any	A
349	3K	[redacted]	[redacted]	[redacted]	Any	A
350	234K	[redacted]	[redacted]	[redacted]	Any	t t h
351	0	[redacted]	[redacted]	[redacted]	Any	A
352	791	[redacted]	[redacted]	[redacted]	Any	A

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:

```
Accelerated Path-------------------------------------------------------------------------------
accel packets                535738514    accel bytes                 657880315079
conns created                  8473750    conns deleted                    1544490
C total conns                   110187    C templates                           25
C TCP conns                     106320    C delayed TCP conns                  141
C non TCP conns                   3867    C delayed nonTCP con                   0
conns from templates             60646    temporary conns                    84551
nat conns                      8371478    dropped packets                     6458
```

```
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 overtime.

```
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-xxxc

ALL

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

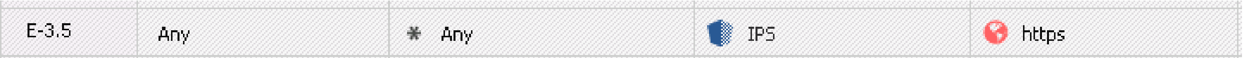
The VS instance is out of scope of the audit.

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:



E-3.5	Any	* Any	IPS	https

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: ______________________	By: ______________________
Authorized Customer Representative	Check Point Professional Services Representative
Date: ______________________	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

Please contact us for any 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