Global Information Assurance Certification Paper

AUDITING NOKIA FIREWALL

GSNA Gold Certification

Author: Richard Sokal GSNA, GCIA

Adviser: Dominicus Adriyanto

Accepted: April 24th 2008

Table of Contents

1 Scope of Audit

1.1 Introduction

EastCoast Enterprises, a Fortune 500 company operates numerous externally facing web applications for maintaining the relationships with its agencies, partners and policyholders, and to provide corporate information to the public. Additionally, EastCoast provides Internet access for its employees and visitors, and VPN remote access to internal resources from computers directly attached to the Internet. Internet presence is an undisputed business necessity for EastCoast Enterprises but opens the network to various security risks, originating both externally and internally.

Managing that presence is essential for all EastCoast' operations, however the perception has been that Firewall infrastructure includes components that might be obsolete and proper remediation is due.

1.2 System Characterization

The subjects of this Audit are Nokia IP530 Appliances running Checkpoint Firewall software. The Nokia/Checkpoint firewalls serve as components of the security architecture that protects EastCoast Enterprises' corporate information assets from both external and internal threats.

ECFW1N	
IP Address:	10.10.99.30
Version:	NG with Application Intelligence (R55) HFA_14, Hotfix 463 - Build 009
OS:	IPSO Version: 3.7
ECFW2N	
IP Address:	10.10.99.40
Version:	NG with Application Intelligence (R55) HFA_14, Hotfix 463 - Build 009
OS:	IPSO Version: 3.7
ECFW1H	
IP Address:	10.10.66.231
Version:	NG with Application Intelligence (R55) HFA_14, Hotfix 463 - Build 009
OS:	IPSO Version: 3.7
ECFW2H	
IP Address:	10.10.66.232
Version:	NG with Application Intelligence (R55) HFA_14, Hotfix 463 - Build 009
OS:	IPSO Version: 3.7

ECFW2LQ
IP Address: 10.10.210.71
Version: NG with Application Intelligence (R55) HFA_16, Hotfix 595 - Build 005
OS: IPSO Version: 3.7

ECFW1L
IP Address: 10.10.16.2
Version: NG with Application Intelligence (R55) HFA_14, Hotfix 463 - Build 009
OS: IPSO Version: 3.7

ECFW2L
IP Address: 10.10.16.3
Version: NG with Application Intelligence (R55) HFA_14, Hotfix 463 - Build 009
OS: IPSO Version: 3.7

ECFW2V
IP Address: 10.10.200.75
Version: NGX (R61)
OS: IPSO Version: 4.1

1.3 Area of interest

The scope of the audit was to provide security, performance and capacity review of the Nokia IP530 firewalls, identify areas of concern and provide recommendations for improvement. The audit focuses on the following eight domains:

- Firewall capacity and system assurance examination
- Firewall backup and fault recovery examination
- Firewall change management compliance examination
- Firewall software vulnerability and patch examination
- Firewall operating system vulnerability and patch examination
- Privileged account access control examination

- Firewall rulebase compliance examination
- Firewall rulebase optimization examination

Invasive examination such as Firewall rulebase testing or vulnerability testing is outside the scope.

2 Audit Strategy

2.1 Firewall capacity and system assurance

2.1.1 Risk

To produce expected effect in enforcing authorized access policies, a firewall must examine every individual packet flow traversing through its inspection engines. It must receive, inspect, and re-transmit all network packets in real time, without adding significant delay or worse, dropping connections. The firewall must be able to log those conditions to an external location, secured from unauthorized access, and alert on them based on predefined policy.

A. As CPU approaches 100% utilization packet-loss may occur, impacting performance of existing connections and establishments of new ones.

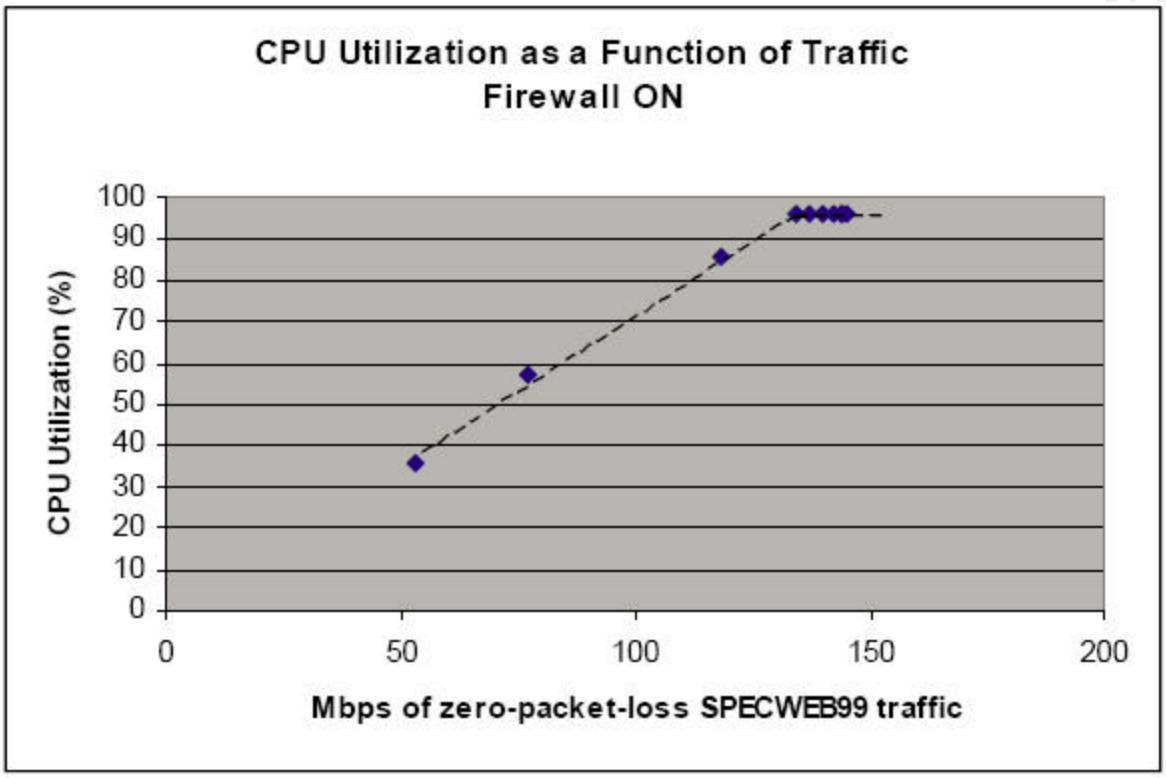


Table 2-1 CPU Utilization as a function of traffic for NOKIA (Ingber, Nokia 2002)

B. As memory approaches 100% utilization establishments of new connections may be impacted.

DRAM	Check Point maximum FW Connections	Maximum connections with Web Intelligence	Hash table size	Memory pool size	Maximum memory pool size
Disk-based IP Security Platforms					
256 MB	36,000		2 MB	48 MB	64 MB
512 MB	135,000	50,000	4 MB	196 MB	256 MB
1 GB	360,000	140,000	8 MB	400 MB	512 MB
2 GB	725,000	325,000	16 MB	800 MB	900 MB

Table 2-2Maximum number of concurrent connections as a function of memory size (Nokia Inc., 2007)

C. Interface throughput is limiting the Firewall performance while the CPU is not fully utilized.

D. System resource problems remain undetected impacting performance and integrity.

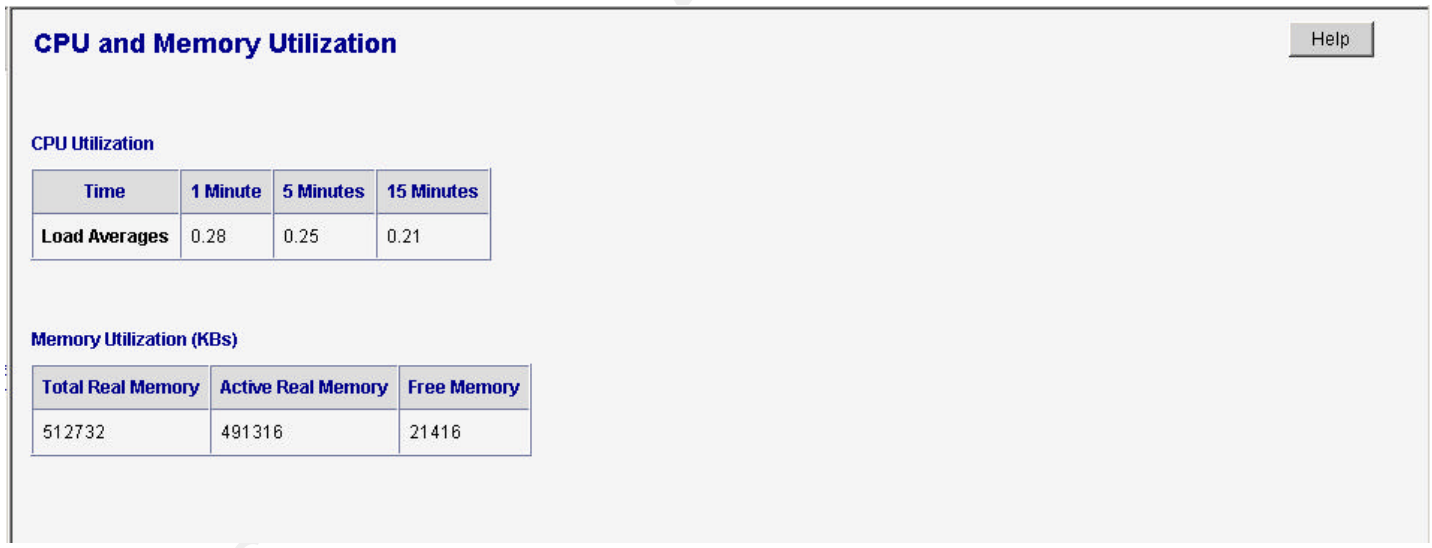
E. System logs unavailable making post-incident investigation difficult.

2.1.2 Checklist

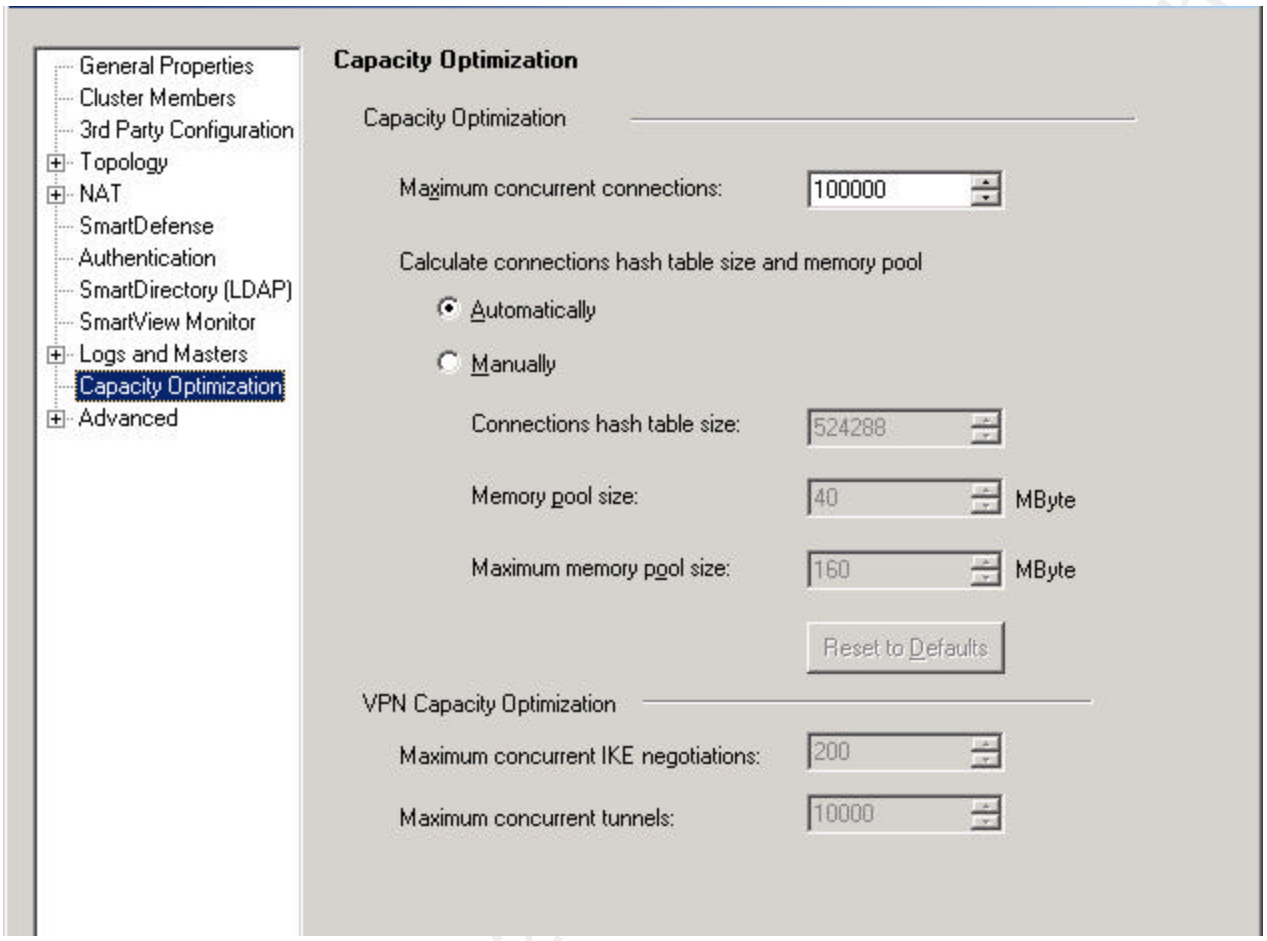
The checklist will include:

a. Current and historical system resource utilization: CPU, Memory, HDD

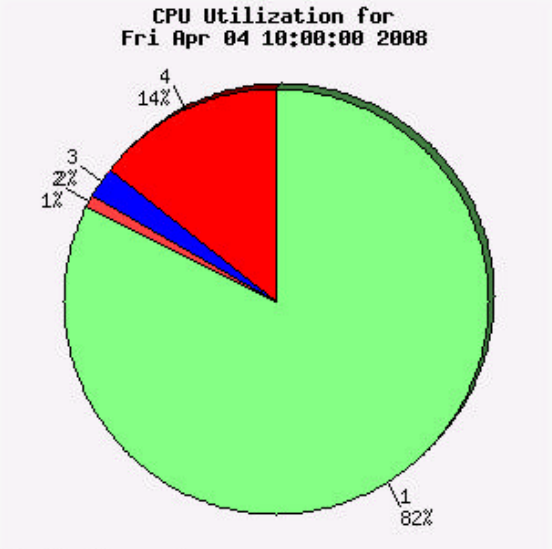
Use Nokia Network Voyager to monitor the Memory and CPU usage. Under the Voyager navigation tree select Monitor-> System Utilization -> CPU-Memory Life Utilization

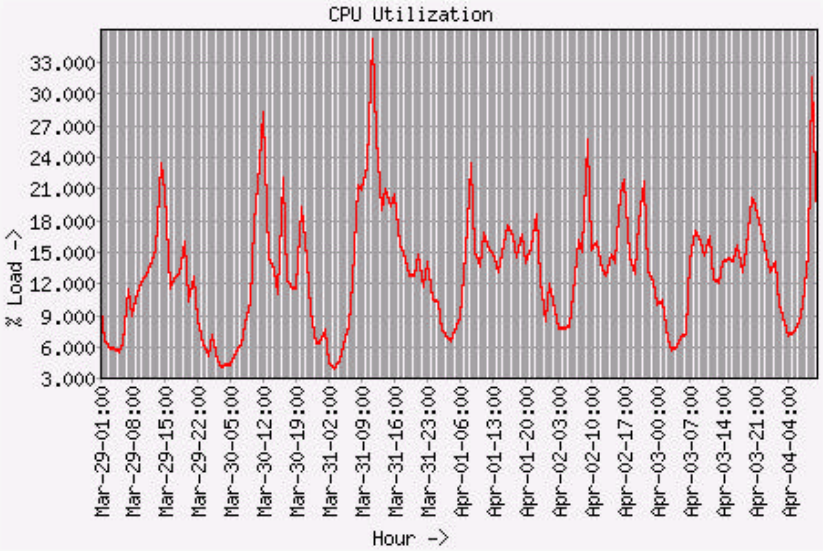


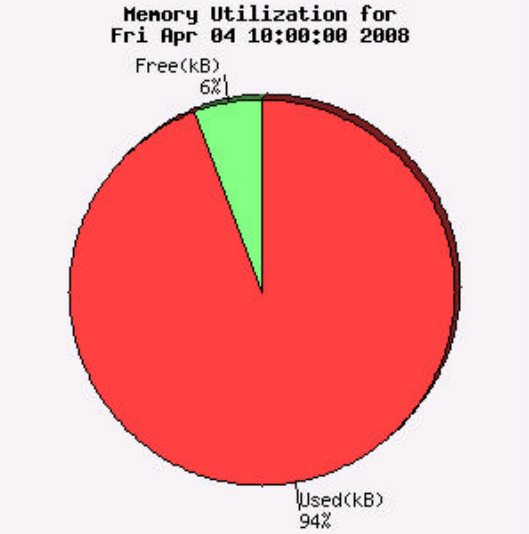
- CPU Load averages of 2 or more indicate that system is under continued heavy load.
- Determine how much total RAM memory the firewall has installed. Refer to Table 2-3 for maximum number of concurrent connections the system can handle. Next, in Check Point Gateway Properties -> Capacity Optimization, check the number of concurrent connections given VPN-1 installation is meant to support. It must be greater than the value obtained in previous step from Table 2-4.

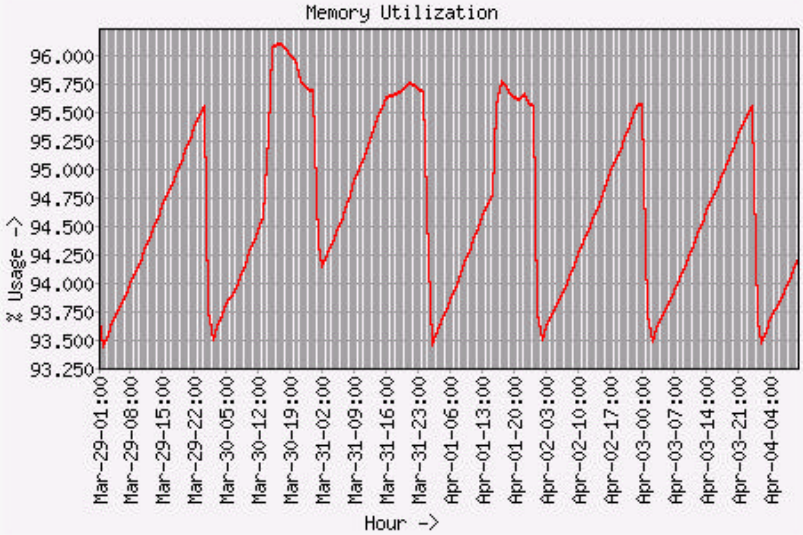


Use Nokia Network Voyager to check the historical CPU and Memory utilization. Under the Voyager navigation tree select Monitor-> Reports -> CPU Utilization Report / Memory Utilization Report





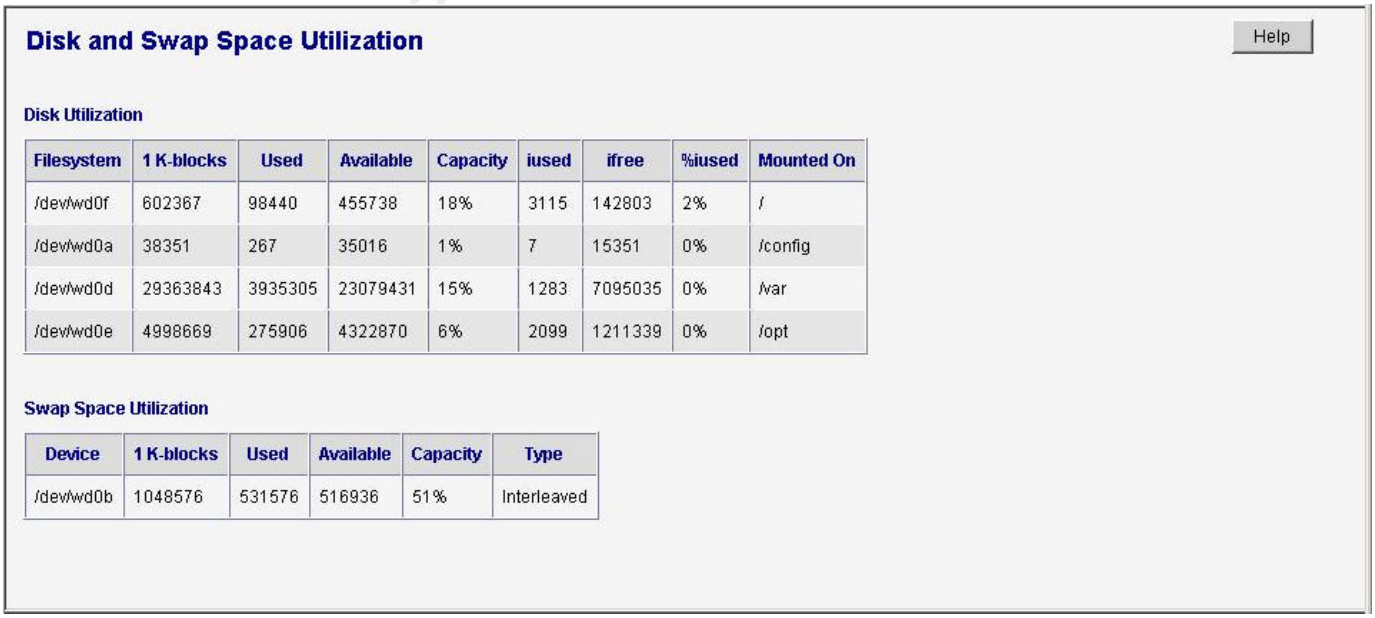




be dropping packets. To verify if that is the case *run ipsctl -a | grep in_qdrop.* Large number of drops (over 1000) may indicate firewall congestion.

```
# ipsctl -a | grep in_qdrop
ifphys:eth-s1p1:errors:in_qdrops = 20304
ifphys:eth-s1p1:errors:in_qdrops = 30033
ifphys:eth-s1p2:errors:in_qdrops = 0
ifphys:eth-s1p2:errors:in_qdrops = 0
ifphys:eth-s1p3:errors:in_qdrops = 0
ifphys:eth-s1p3:errors:in_qdrops = 0
ifphys:eth-s1p4:errors:in_qdrops = 0
ifphys:eth-s1p4:errors:in_qdrops = 0
ifphys:loop0:errors:in_qdrops = 0
ifphys:soverf0:errors:in_qdrops = 0
ifphys:stof0:errors:in_qdrops = 0
ifphys:tun0:errors:in_qdrops = 0
ifphys:eth1:errors:in_qdrops = 0
ifphys:eth1:errors:in_qdrops = 0
ifphys:eth2:errors:in_qdrops = 0
ifphys:eth2:errors:in_qdrops = 0
ifphys:eth3:errors:in_qdrops = 0
ifphys:eth3:errors:in_qdrops = 0
ifphys:eth4:errors:in_qdrops = 0
ifphys:eth4:errors:in_qdrops = 0
```

Use Nokia Network Voyager to check the Disk and Swap Space utilization. Under the Voyager navigation tree select Monitor->System Utilization-> Disk and Swap Space Utilization.



Disk and Swap Space Utilization

Help

Disk Utilization

Filesystem	1 K-blocks	Used	Available	Capacity	iused	ifree	%iused	Mounted On
/dev/wd0f	602367	98440	455738	18%	3115	142803	2%	/
/dev/wd0a	38351	267	35016	1%	7	15351	0%	/config
/dev/wd0d	29363843	3935305	23079431	15%	1283	7095035	0%	/var
/dev/wd0e	4998669	275906	4322870	6%	2099	1211339	0%	/opt

Swap Space Utilization

Device	1 K-blocks	Used	Available	Capacity	Type
/dev/wd0b	1048576	531576	516936	51%	Interleaved

Alternatively use the df –k to retrieve this information via the CLI.

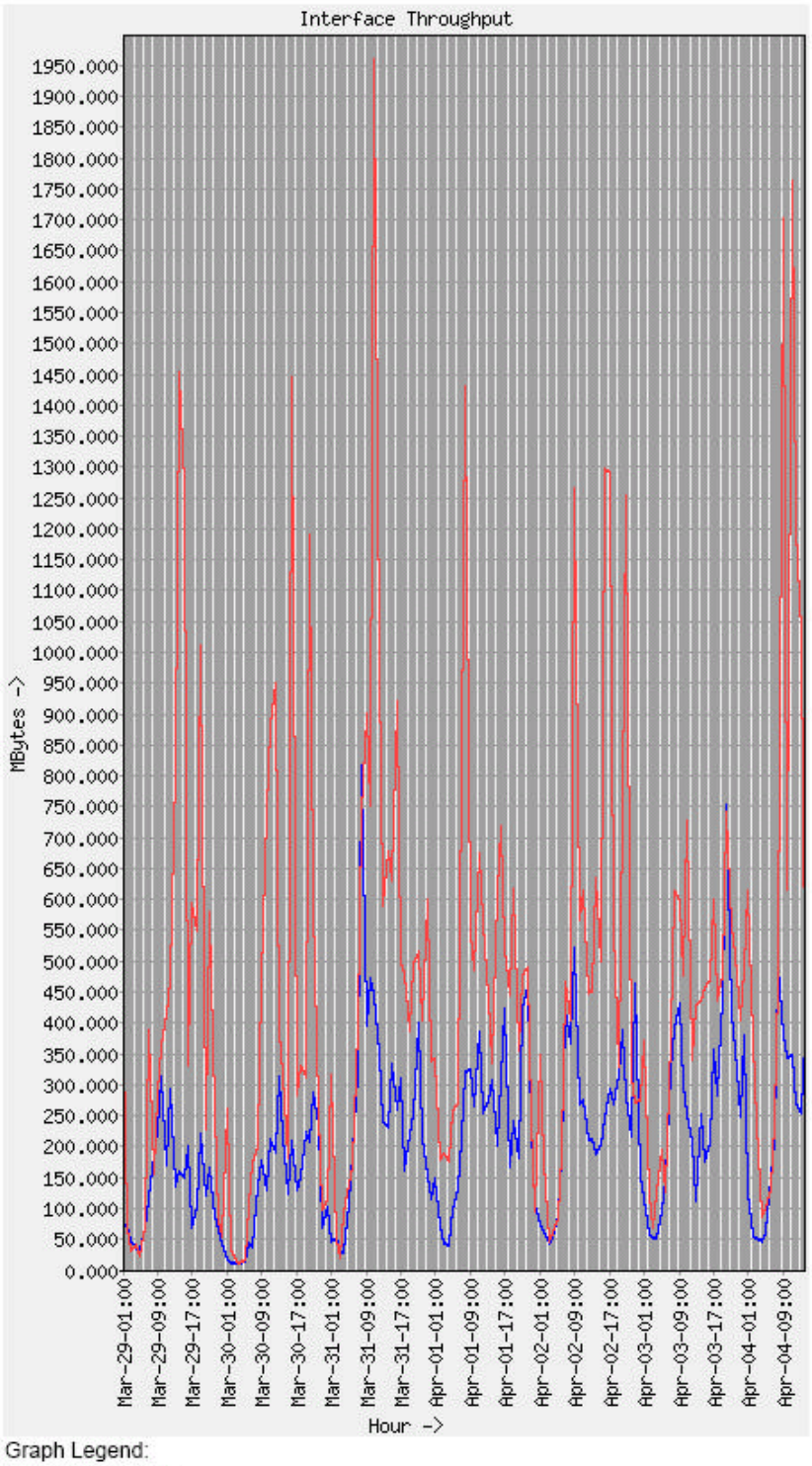
```
# df -k
Filesystem  1K-blocks     Used    Avail Capacity  Mounted on
/dev/wd0f      396952   258326   106870    71%    /
/dev/wd0a       38193      291    34847     1%    /config
/dev/wd0d    14950231  2769691 10984522    20%    /var
/dev/wd0e     2563618   547734  1810795    23%    /opt
#
```

In each case *capacity* should not exceed 80%.

b. Current and historical network bandwidth utilization

Use Nokia Network Voyager to check the network bandwidth utilization. Under the Voyager navigation tree select Monitor->System Utilization-> Interface Throughput Report

Interface Throughput Report



If interface throughput report indicates that any of the interfaces may be under heavy load execute the following to verify if packet loss has been occurring: *ipsctl -a | grep out_qdrops*

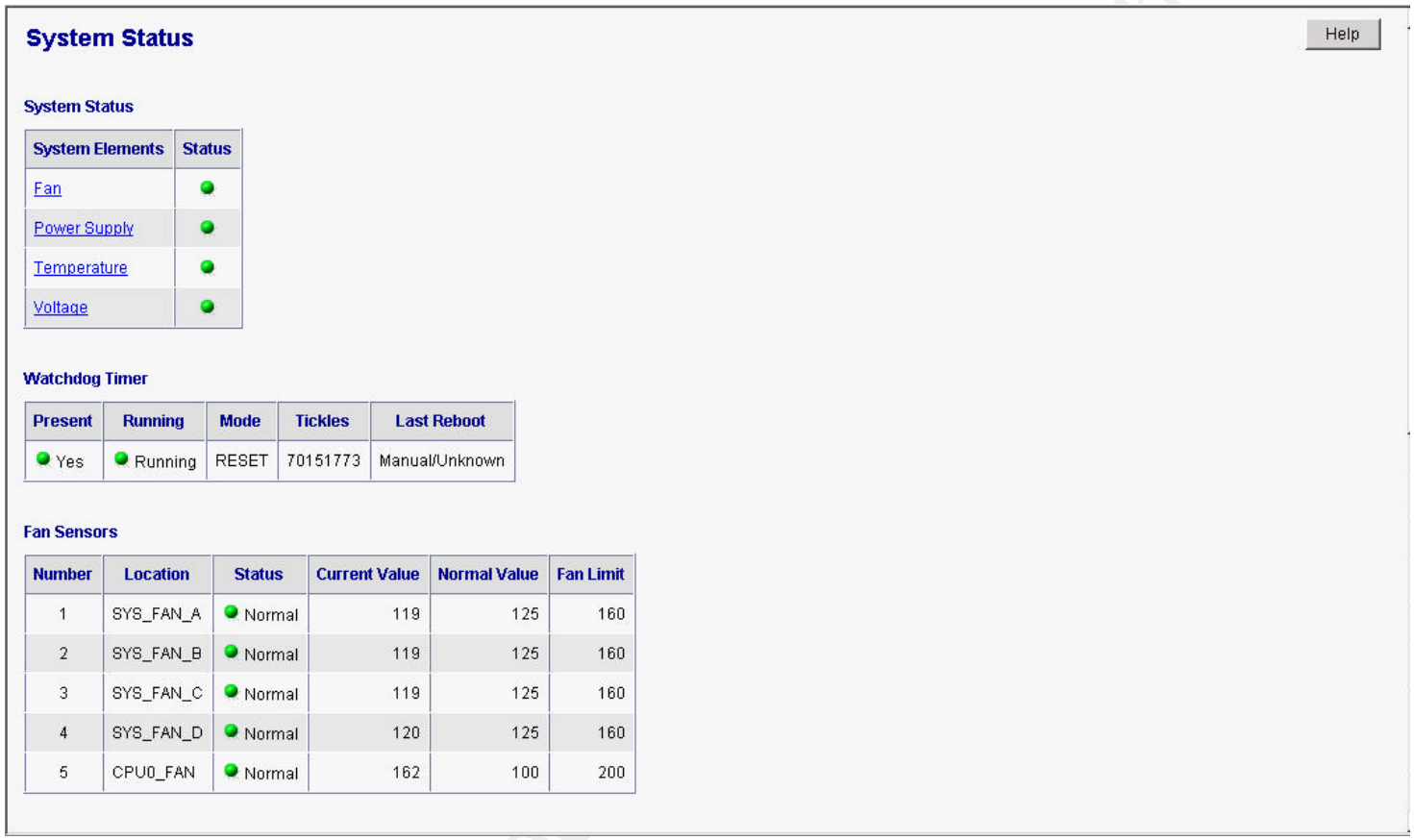
Large number of drops (over 1000) may indicate network interface congestion.

```
# ipsctl -a | grep out_qdrops
ifphys:eth-s1p1:errors:out_qdrops = 2449524
ifphys:eth-s1p1:errors:out_qdrops = 2449524
ifphys:eth-s1p2:errors:out_qdrops = 5364662
ifphys:eth-s1p2:errors:out_qdrops = 5364662
ifphys:eth-s1p3:errors:out_qdrops = 142
ifphys:eth-s1p3:errors:out_qdrops = 142
ifphys:eth-s1p4:errors:out_qdrops = 0
ifphys:eth-s1p4:errors:out_qdrops = 0
ifphys:loop0:errors:out_qdrops = 0
ifphys:soverf0:errors:out_qdrops = 0
ifphys:stof0:errors:out_qdrops = 0
ifphys:tun0:errors:out_qdrops = 0
ifphys:eth1:errors:out_qdrops = 0
ifphys:eth1:errors:out_qdrops = 0
ifphys:eth2:errors:out_qdrops = 0
ifphys:eth2:errors:out_qdrops = 0
ifphys:eth3:errors:out_qdrops = 0
ifphys:eth3:errors:out_qdrops = 0
ifphys:eth4:errors:out_qdrops = 61313
ifphys:eth4:errors:out_qdrops = 61313
```

c. System health and performance monitoring and alerting.

Use Nokia Network Voyager to check the status of various hardware components. Under the Voyager navigation tree select Monitor-> Hardware Monitoring-> System Status

Verify that the status of all listed hardware and environmental components is normal.



System Status

Help

System Status

System Elements	Status
Fan	
Power Supply	
Temperature	
Voltage	

Watchdog Timer

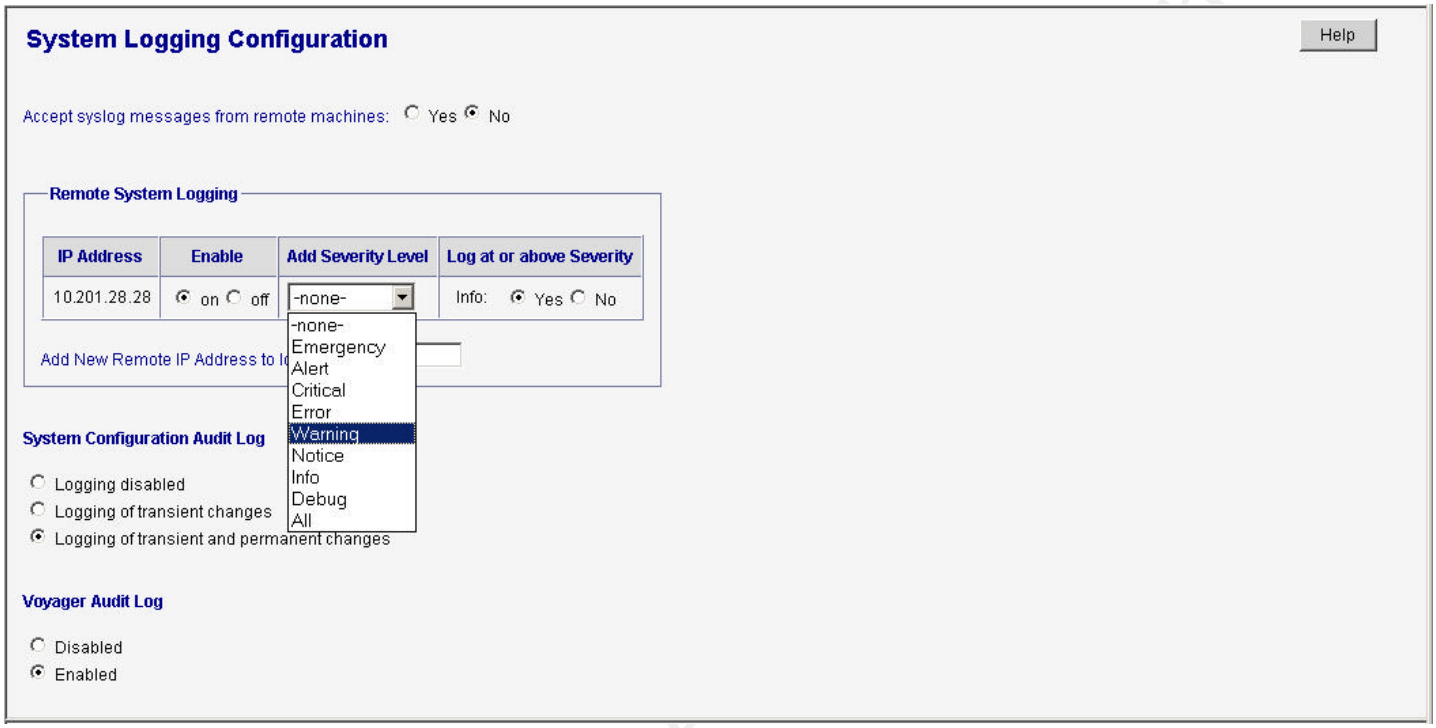
Present	Running	Mode	Tickles	Last Reboot
Yes	Running	RESET	70151773	Manual/Unknown

Fan Sensors

Number	Location	Status	Current Value	Normal Value	Fan Limit
1	SYS_FAN_A	Normal	119	125	160
2	SYS_FAN_B	Normal	119	125	160
3	SYS_FAN_C	Normal	119	125	160
4	SYS_FAN_D	Normal	120	125	160
5	CPU0_FAN	Normal	162	100	200

d. Event logging (audit trail, system log)

Use Nokia Network Voyager to check the Syslog configuration. Under the Voyager navigation tree select Configuration-> System Configuration -> System Logging.



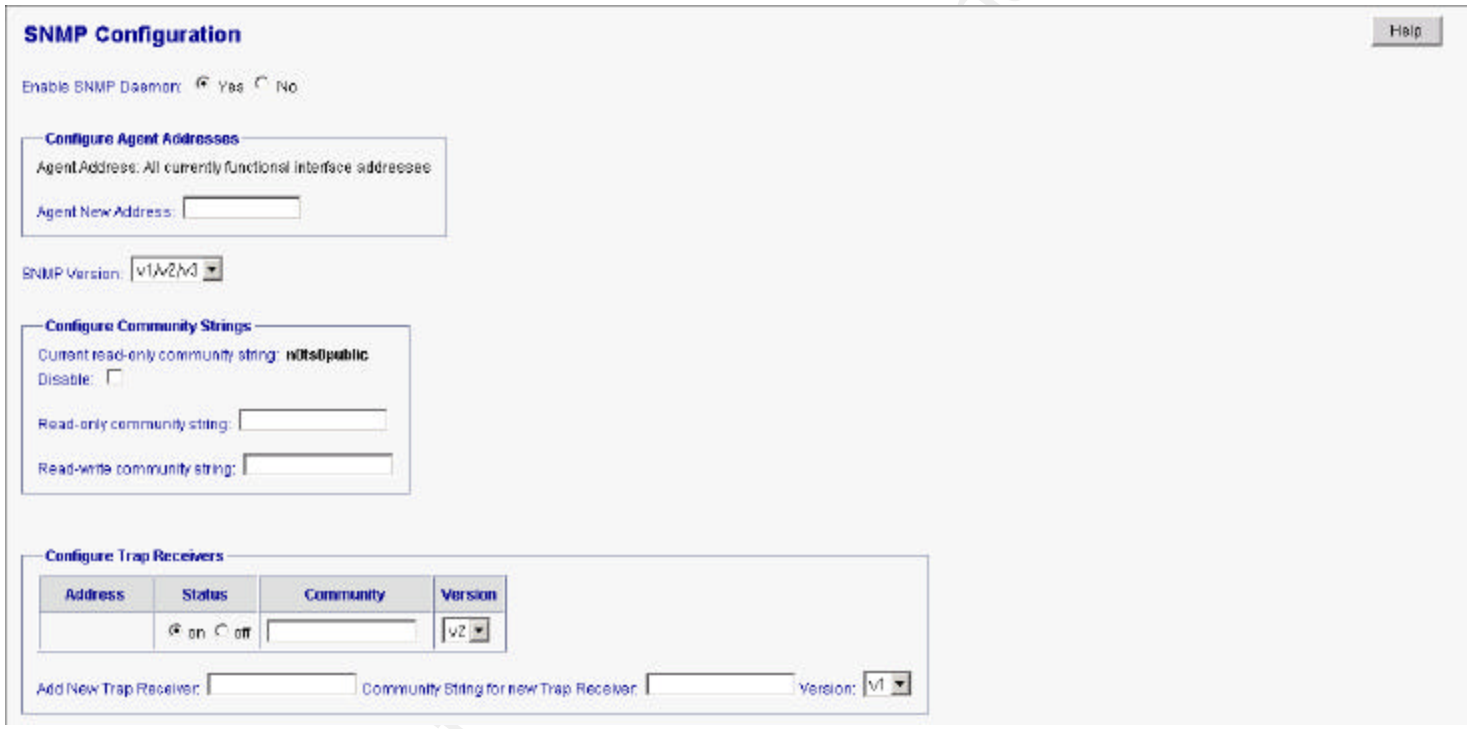
Ensure the System Configuration and Voyager Audit Logs are enabled. A good practice would be to have the severity level set to *Warning* or lower.

e. Critical event notifications (fault management)

Use Nokia Network Voyager to verify the critical event notification is enabled. Under the Voyager navigation tree select Configuration-> System Configuration -> System Failure Notification.

Use Nokia Network Voyager to check the SNMP configuration. Under the Voyager navigation tree select Configuration->System Configuration-> SNMP

Validate the SNMP server settings and community string. Verify that at minimum critical errors, hardware failures and environmental problems are alerted on.



2.2 Firewall backup and fault recovery

2.2.1 Risk

In today's world, more and more mission-critical applications move out on the Internet, therefore providing highly available clustered services becomes increasingly important. Both hardware and software redundancy can be provided by a clustered system as it consists of a number of independent nodes, and each node runs an instance of operating system and application software. Detecting node or daemon failures and reconfiguring the system accordingly achieve high availability, as the remaining nodes in the cluster assume the workload. With stateful failover, a control link is used to replicate the firewall state tables to the peer that is

serving as the standby node. The replication of state information ensures that the standby peer has the necessary information to immediately assume the role of an active peer.

To restore a computer to an operational state following a disaster where the data loss has occurred system backups are neccessary. System backup differs from fault-tolerance approach in the sense that backup systems assume that a fault will cause a data loss event and fault-tolerant systems assume it will not. Backups are commonly the last line of defense against data loss and least convenient to use.

2.2.2 Checklist

a. Firewall high availability (Nokia employs VRRP)

Connect to CLI as a privileged user and inspect the Nokia VRRP configuration and statistics using the *iclid -> show vrrp* utility.

```
FW1>
FW1> sh vrrp

VRRP State
        Flags:  On,LocalReceive
        4 interface enabled
        4 virtual routers configured
                0 in Init state
                0 in Backup state
                4 in Master state
FW1>
FW1>

FW2> sh vrrp

VRRP State
        Flags:  On,LocalReceive
        4 interface enabled
        4 virtual routers configured
                0 in Init state
                4 in Backup state
                0 in Master state
```

Next, inspect the output of *sh vrrp stats* for any errors. During normal operations *Rx Advertisement* or *Tx Advertisement* would be the only statistics with a non-zero value.

```
FW1>
FW1> sh vrrp stat

VRRP Stats
Interface eth3c0
        Rx IP Truncated:        0       Rx Checksum Error:      0
        Rx Unknown Version:     0       Rx Unknown VRID:        0
        Tx IP Truncated:        0
        VRID 100
                Rx Bad TTL:             0       Rx VRRP Truncated:      0
                Rx Auth Mismatch:       0       Rx Auth Failure:        0
                Rx Unknown Auth:        0       Rx Unknown Type:        0
                Rx Bad Advert Intvl:    0       Rx Bad Addr List:       0
                Rx Loopback:            0       Rx Bad Master:          0
                Rx Advertisement:       0       Tx Advertisement        2102126
Interface eth2c0
        Rx IP Truncated:        0       Rx Checksum Error:      0
        Rx Unknown Version:     0       Rx Unknown VRID:        0
        Tx IP Truncated:        0
        VRID 100
                Rx Bad TTL:             0       Rx VRRP Truncated:      0
                Rx Auth Mismatch:       0       Rx Auth Failure:        0
                Rx Unknown Auth:        0       Rx Unknown Type:        0
                Rx Bad Advert Intvl:    0       Rx Bad Addr List:       0
                Rx Loopback:            0       Rx Bad Master:          0
                Rx Advertisement:       0       Tx Advertisement        2102181
Interface eth1c0
        Rx IP Truncated:        0       Rx Checksum Error:      0
        Rx Unknown Version:     0       Rx Unknown VRID:        0
        Tx IP Truncated:        0
        VRID 100
                Rx Bad TTL:             0       Rx VRRP Truncated:      0
                Rx Auth Mismatch:       0       Rx Auth Failure:        0
                Rx Unknown Auth:        0       Rx Unknown Type:        0
                Rx Bad Advert Intvl:    0       Rx Bad Addr List:       0
                Rx Loopback:            0       Rx Bad Master:          0
                Rx Advertisement:       0       Tx Advertisement        2102240
Interface eth-s1p3c0
        Rx IP Truncated:        0       Rx Checksum Error:      0
        Rx Unknown Version:     0       Rx Unknown VRID:        0
        Tx IP Truncated:        0
        VRID 100
                Rx Bad TTL:             0       Rx VRRP Truncated:      0
                Rx Auth Mismatch:       0       Rx Auth Failure:        0
                Rx Unknown Auth:        0       Rx Unknown Type:        0
                Rx Bad Advert Intvl:    0       Rx Bad Addr List:       0
                Rx Loopback:            0       Rx Bad Master:          0
                Rx Advertisement:       0       Tx Advertisement        15940312
Interface eth-s1p2c0
        Rx IP Truncated:        0       Rx Checksum Error:      0
        Rx Unknown Version:     0       Rx Unknown VRID:        0
        Tx IP Truncated:        0
```

```
        VRID 100
                Rx Bad TTL:             0       Rx VRRP Truncated:      0
                Rx Auth Mismatch:       0       Rx Auth Failure:        0
                Rx Unknown Auth:        0       Rx Unknown Type:        0
                Rx Bad Advert Intvl:    0       Rx Bad Addr List:       0
                Rx Loopback:            0       Rx Bad Master:          0
                Rx Advertisement:       0       Tx Advertisement        2102290
Interface eth-s1p1c0
        Rx IP Truncated:        0       Rx Checksum Error:      0
        Rx Unknown Version:     0       Rx Unknown VRID:        0
        Tx IP Truncated:        0
        VRID 100
                Rx Bad TTL:             0       Rx VRRP Truncated:      0
                Rx Auth Mismatch:       0       Rx Auth Failure:        0
                Rx Unknown Auth:        0       Rx Unknown Type:        0
                Rx Bad Advert Intvl:    0       Rx Bad Addr List:       0
                Rx Loopback:            0       Rx Bad Master:          0
                Rx Advertisement:       0       Tx Advertisement        2102461
```

Finally, to verify the HA link status use the *cphaprob state* Checkpoint command. The following are examples of successful (A) and failing (B) state synchronization links.

```
A.

# cphaprob state

Cluster Mode:   Sync only (OPSEC))

Number     Unique Address  Firewall State (*)

1          192.168.252.2   Active
2 (local)  192.168.252.1   Active

(*) FW-1 monitors only the sync operation and the security policy
#


B.

# cphaprob state

Cluster Mode:   Sync only (IPSO cluster)

Number     Unique Address  Firewall State (*)

1          192.168.252.1   down
2 (local)  192.168.252.2   down
```

```
(*) In IP Clustering FW-1 also monitors the cluster status
    In VRRP you should use Nokia's monitoring tool to get the cluster status

#
```

b. Firewall stateful failover (transparent recovery)

Checkpoint software introduces stateful failover by employing the Cluster XL state synchronization.

Use Checkpoint SmartView Monitor to inspect the ClusterXL status. Go to SmartView Monitor->Gateway Status->Firewalls->ClusterXL .

Successfully established state synchronization would manifest itself as follows:

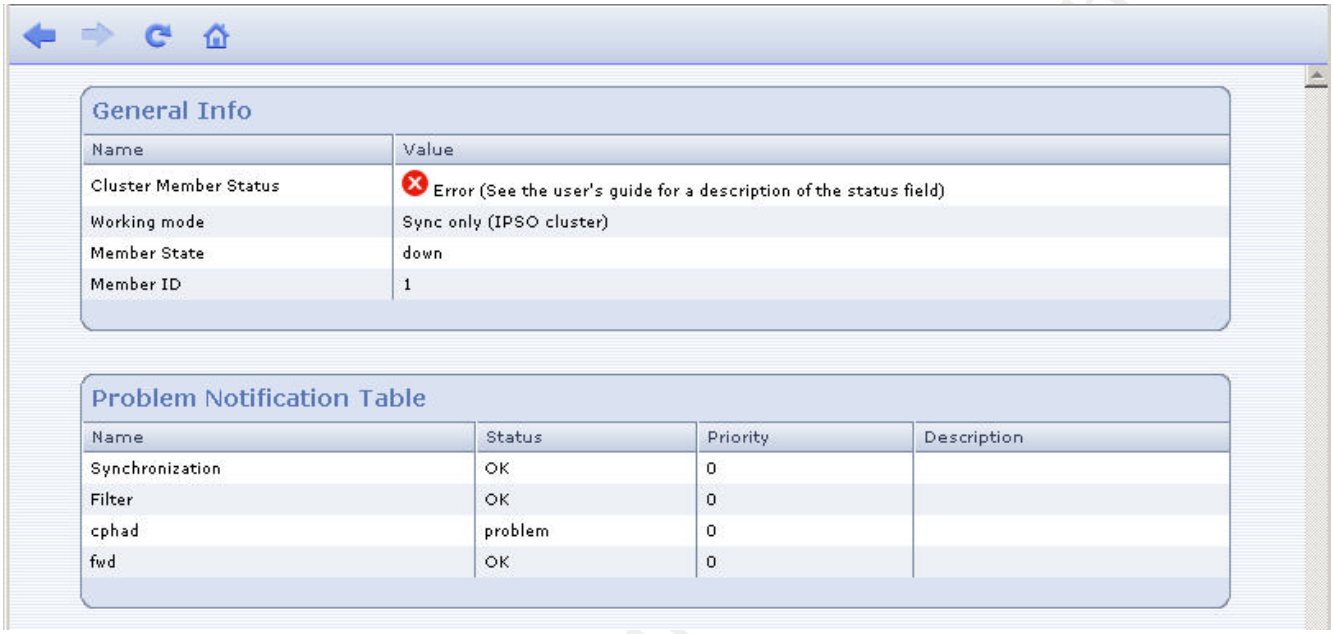
General Info

Name	Value
Cluster Member Status	OK
Working mode	Sync only (IPSO cluster)
Member State	active
Member ID	2

Problem Notification Table

Name	Status	Priority	Description
Synchronization	OK	0	
Filter	OK	0	
cphad	OK	0	
fwd	OK	0	

The following is an example of a synchronization link failure.



General Info

Name	Value
Cluster Member Status	Error (See the user's guide for a description of the status field)
Working mode	Sync only (IPSO cluster)
Member State	down
Member ID	1

Problem Notification Table

Name	Status	Priority	Description
Synchronization	OK	0	
Filter	OK	0	
cphad	problem	0	
fwd	OK	0	

Alternatively, via the CLI the following system commands can be used:

cphaprob

verify status of the synchronization channel: *sync(secured)*, *broadcast* and the *virtual cluster interfaces*

fw tab -t connections –s

verify the state table is synchronized, the numbers should not differ substantially between the nodes in a cluster

The following is an example of stateful synchronization check using the CLI.

```
# cphaprob -a if

eth-s1p3c0      non sync(non secured)
eth-s1p1c0      non sync(non secured)
eth-s1p2c0      non sync(non secured)
eth4c0          sync(secured), broadcast
eth2c0          non sync(non secured)
eth3c0          non sync(non secured)
```

```
eth1c0          non sync(non secured)

Virtual cluster interfaces: 6

eth-s1p3c0      10.21.5.1
eth-s1p1c0      10.21.6.1
eth-s1p2c0      10.21.7.1
eth2c0          10.200.16.1
eth3c0          10.20.16.1
eth1c0          10.21.7.1
#


# fw tab -t connections –s

HOST                 NAME                          ID #VALS #PEAK #SLINKS
localhost            connections                 8158  3911 19941   11730
#

# fw tab -t connections –s


HOST                 NAME                          ID #VALS #PEAK #SLINKS
localhost            connections                 8158  3947 19920   11839
#
```

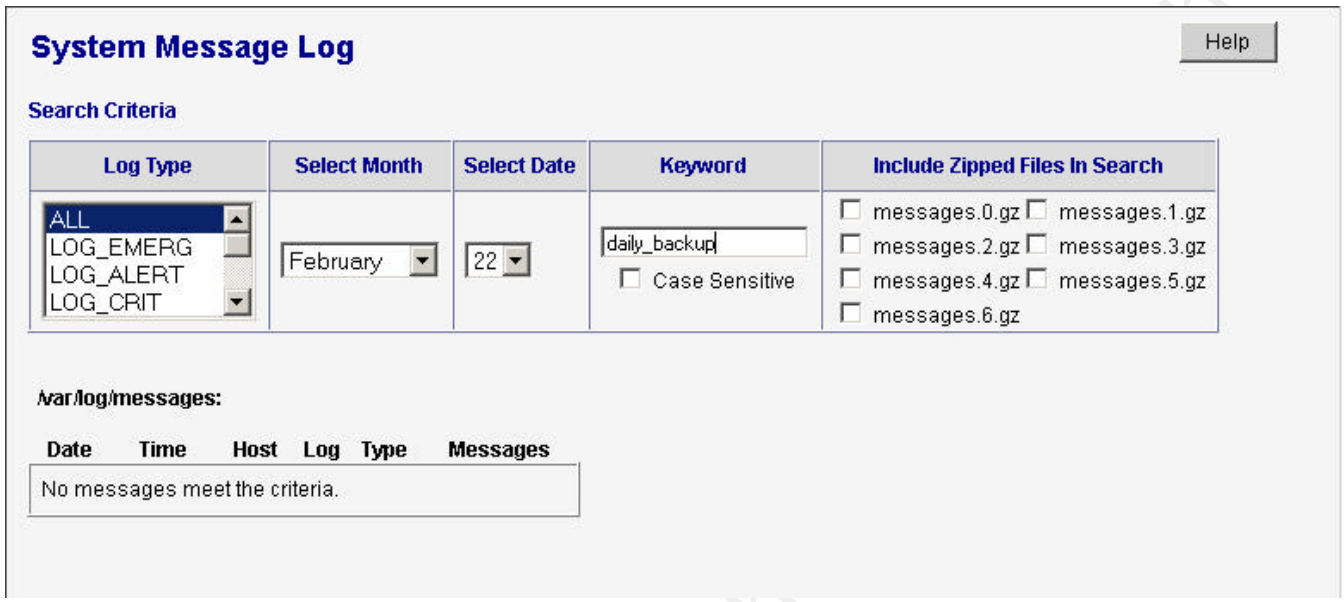
c. Firewall backup process validation

Use Nokia Network Voyager to verify the backup process configuration and scheduling. Under the Voyager navigation tree select Configuration-> System Configuration ->Backup and Restore Configuration

Ensure that at minimum the backup of Ipsec files, cron files in /var/cron/ and config files in /config/ directory are enabled and the frequency is set to 'weekly'. Manual backup may supplement this schedule in scope and frequency, i.e. following a major system update.

Use Nokia Network Voyager to verify the backup process has been successful. Under the Voyager navigation tree select Monitor-> System Logs ->System Message Log.

Search for the name of the backup file.



Interview with the firewall administrator regarding this and other backup processes that might be running on the firewall in question.

What directories are being backed up?

How frequently?

How often are the backups tested?

Are the backups encrypted?

Ipsec files, cron files in /var/cron/ and config files in /config/ directory should be backed daily, tested at least monthly and encrypted at all times to assure the confidentiality in case of tape loss.

2.3 Firewall change management compliance

2.3.1 Policy

EastCoast Enterprises has implemented the following Change Management Policy:

Overview: *To properly control all business application/system changes to the EastCoast Production environment.*

Purpose: *To define the actions necessary for discussing, monitoring, reporting, and approving production changes.*

Scope: *An approved Change Track ticket is required for all modifications to production applications and supporting infrastructure. No change shall be made to production resources without explicit, documented approval within the Change Track System.*

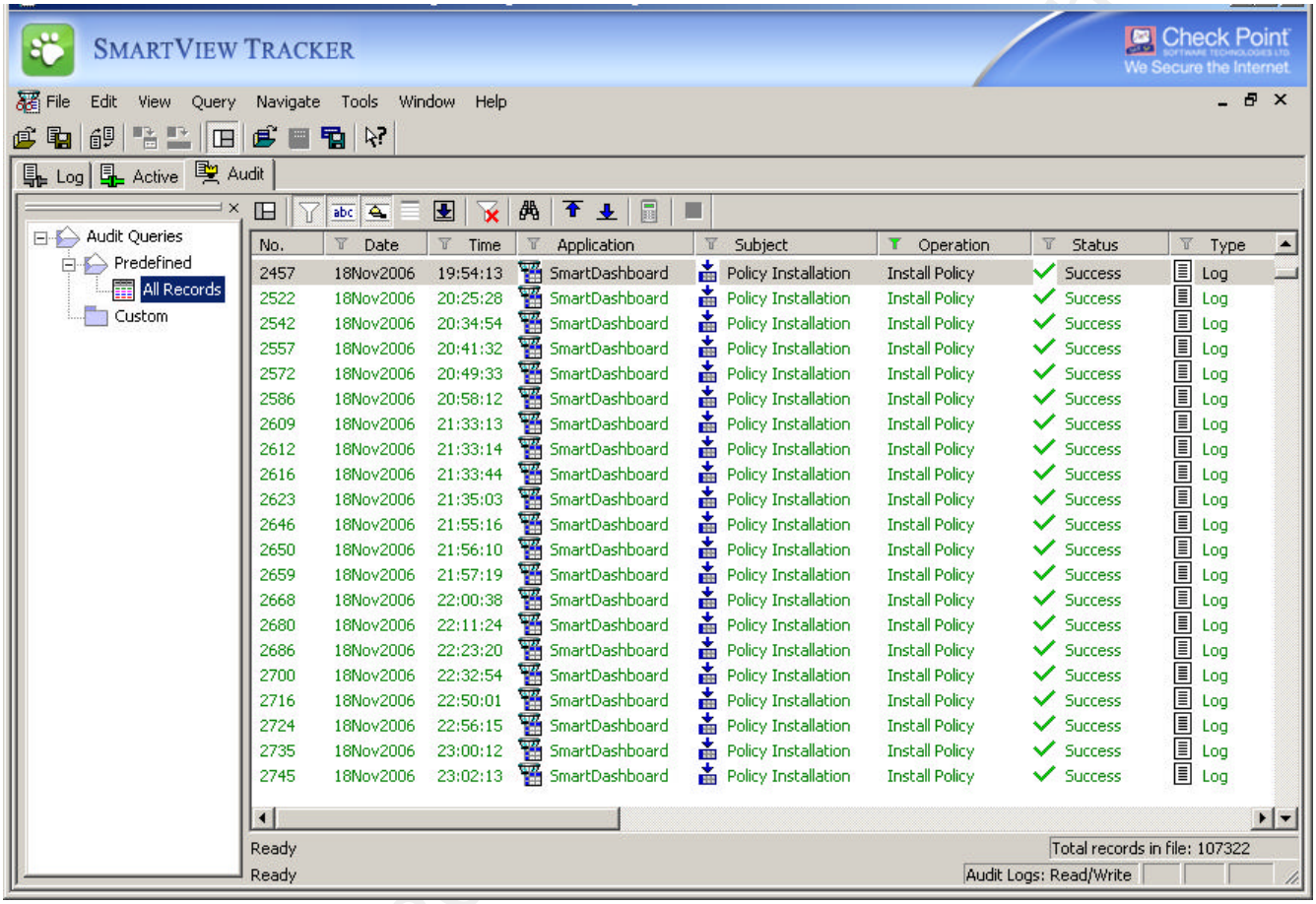
Compliance: *Adherence to this policy is not optional and will be included in the employee's overall performance management objectives. It is expected that this policy be treated as any other corporate policy.*

2.3.2 Checklist

The checklist will include:

a. Firewall audit trail inspection

Use Checkpoint SmartView Tracker to produce a list of changes implemented within the given time range. Search for operation "Install Policy". Verify that each firewall policy install can be matched to an approved Change Track ticket.



2.4 Firewall software vulnerability and patch management

2.4.1 Risk

In order to assure the availability and integrity of the firewalls and avoid the risk of a security exposure they must be subject to vulnerability examination on an ongoing basis. There are a number of reasons why is it important for these checks to be performed regularly:

A. Software defects - Firewall systems are prone to software flows and the risk increases with complexity of the code. A great deal of those defects will be security related. If maliciously exploited the organization can suffer a security breach or denial of service leading to damaging business consequences.

B. Configuration errors - Firewalls routinely require configuration changes such as the addition of

new rules, objects and services or a functionality enhancement. These modifications may be unintentionally misconfigured, causing unforeseen system behavior or side effects such as unauthorized system access.

C. System maintenance - During the operational life of a firewall software new features will need to be added, patches applied and other regular maintenance performed. If such changes are not tested thoroughly can leave loopholes in the firewall's performance, which, if exploited, can result in business, financial or legal loss.

2.4.2 Checklist

The checklist will include:

a. Network services' enumeration

Use the UNIX *netstat –an* command to evaluate network services and their respective communication ports in LISTENING or ESTABLISHED state.

According to Checkpoint Solution ID: sk9408 the list below details the common ports used by Check Point Next Generation. Everything else should have well defined purpose and corresponding documentation.

1. TCP 18211 (FW1_ica_push): The Check Point Daemon (CPD) process, running on the FireWall module, listens on TCP port 18211 for certificate creation and for the "push" of the certificate to the FireWall module from the management module.

2. TCP 18210 (FW1_ica_pull): The CPD process, on the management module, is listening on TCP port 18210 for certificates to be "pulled" by a FireWall module from a management module.

3. TCP 18186 (FW1_omi-sic): This TCP port is used for Secure Internal Communications (SIC) between OPSEC certified products and a NG FireWall module.

4. TCP 18191 (CPD): This TCP port is used by the CPD process for communications such as policy installation, certificate revocation, and status queries.

5. TCP 18190 (CPMI): This TCP port is used by the FireWall Management process (FWM) to listen for NG Management Clients attempting to connect to the management module.

6. TCP 18192 (CPD_amon): This TCP port is used by the CPD process FireWall Application Monitoring.

7. TCP 257 (FW1_log): This TCP port is used for logging purposes

b. Firewall software version and patch level inspection

Check Point recommends that the latest hotfix acumulators be installed in order to stay current with the latest software and security updates. Latest HFAs can be obtained from

http://www.checkpoint.com/downloads/latest/hfa/index.html

Table 2-5 presents latest hotfix acumulator as of Oct 2007.

Product	VPN-1 Power/UTM
Version	NGX R65
Platform	IPSO
Release	R65_HFA_02
Filename	VPN-1_R65_HFA_02_wrapper.ipso.tgz
Size	80.21MB
MD5 Checksum	874b55b4fad98849bd7480c196a6da71
Date Published	21-Oct-2007

Table 2-5 Latest Hotfix Accumulators (HFAs). (Checkpoint, 2007)

Use the *fw ver* CLI Checkpoint command to evauate current HFA/version level.

```
# fw ver
This is Check Point VPN-1(TM) & FireWall-1(R) NG with Application Intelligence (R55) for
IPSO 3.8 - Build 584
#
```

2.5 Firewall operating system vulnerability and patch management

2.5.1 Risk

The outlined in Chapter 4 risks apply to the underlying operating systems, therefore similar checks will be performed.

2.5.2 Checklist

The checklist will include:

a. Continuation of network services' evaluation at the OS level

b. Firewall OS software version and patch level inspection

Use the *unix -a* Nokia IPSO command to evauate the current version level.

```
# uname -a
IPSO FW1 3.8.1-BUILD033 releng 1519  05.01.2005-224100 i386
#
```

Nokia has issued *Security and Mobile Connectivity Products Policy for Product End of Sale and End of Maintenance.*

The following tables provide information on compatibility with Checkpoint software and support status for Nokia IP security platforms during the final limited support period, ending in 2010 (End of Life – EOL, End of Sale – EOS, End of Contract Support – EOCS, Active).

Nokia IPSO Version	FCS or Build	Nokia IPSO Support Status	Projected EOL Date [1]
3.4	4A	EOL	EOL
	9		
3.4.1	5	EOL	EOL
	5a		
	10		
	11, 12, 15, 16, 21		
3.4.2	3	EOL	EOL
3.5 [2]	3	EOL	EOL
	6, 7		
	8		
	10, 14, 15, 17, 18, 19, 22, 23, 24		
3.5.1 [2][3]	2, 6, 7, 8, 10, 11, 12	EOL	EOL
3.6	3, 4, 6, 7, 13, 14, 17, 18	EOL	EOL
3.7	023, 026, 027, 029, 031	EOL	EOL
	032, 034, 035, 036, 039, 041, 044, 048, 049		
3.7.1	004, 007, 010, 012, 013, 016, 020, 024, 025	EOL	EOL
3.7.89	004, 008	EOS	April 25, 2008
3.7.90	006	EOS	January 12, 2009
3.7.99 [4]		EOS	June 17, 2008
3.8	031, 034, 039, 045, 049, 051, 055, 058, 059, 061	EOS	December 7, 2007
3.8.1	028, 029 [5], 033, 035, 038, 044, 045, 048	EOS	June 17, 2008
3.9 [6]	035, 037, 041, 045, 052, 056, 065, 068	EOS	October 21, 2008
3.9 [7]	45c	EOS	October 21, 2008
3.9.90 [8]	019	EOS	
3.9.91 [9]	014	EOS	
3.9.92 [10]	005, 008	Active	
4.0	023, 030, 040, 041, 045, 048	EOS	February 9, 2009
4.0.1	008, 010, 011	EOS	April 24, 2009
4.1 [11]	013, 016, 019, 022, 025, 028, 033, 035	EOS	January 31, 2010
4.1 [12]	20c	EOS	January 31, 2010
4.2	029, 031, 038, 041, 042_HF002, 042_HF003, 051_HFA02, 051A04 [13], 069	Active	

Table 2-6 The versions of the Nokia IPSO operating system, their current support status, and the projected end-of-maintenance and end-of-life dates. (Nokia Inc., 2007)

IP Security Platforms					
IP30	EOL	11/30/2003	2/28/2005	2/28/2005	1.0
IP40	EOS	9/30/2006	9/30/2008	9/30/2008	1.0
IP45	EOS	6/30/2007	6/30/2009	6/30/2009	3.5
IP51	EOCS	12/31/2002	12/31/2005	12/31/2007	1.1
IP55	EOL	8/01/2001	8/01/2001	8/01/2001	NA
IP60	Active				7.0
IP71	EOCS	11/30/2002	11/30/2005	11/30/2007	1.0
IP110	EOL	4/30/2002	4/30/2005	4/30/2007	3.3
IP120	EOCS	12/31/2003	12/31/2006	12/31/2008	3.4
IP130	EOS	12/31/2005	12/31/2008	12/31/2010	3.7
IP260	Active				3.8.1
IP265	Active		6/30/2010	6/30/2012	3.8.1
IP290	Active				4.2 Build 038
IP330	EOS	9/30/2003	9/30/2008	9/30/2008	3.3
IP350	EOS	11/30/2006(1)	11/30/2011	11/30/2011	3.5.1 or 3.7 (3.6 not supported)
IP355	EOS	11/30/2006(1)	11/30/2011	11/30/2011	3.9 Build 037
IP380	EOS	11/30/2006(1)	11/30/2011	11/30/2011	3.5.1 or 3.7 (3.6 not supported)
IP385	EOS	11/30/2006(1)	11/30/2011	11/30/2011	3.9 Build 037
IP390	Active				4.1
IP400	EOL	1998	6/29/2001	6/29/2003	NA
IP410	EOL	1999	3/31/2005	3/31/2007	3.3
IP440	EOL	3/31/2002	3/31/2005	3/31/2007	3.3
AV445	EOL	12/31/2002	1/31/2003	1/31/2003	NA
IP530	EOS	3/31/2005	3/31/2010	3/31/2010	3.3.1
IP560	Active				4.0.1
IP650	EOS	4/30/2003	4/30/2008	4/30/2008	3.3
IP690	Active				4.2 Build 041
IP710	EOS	4/30/2006	4/30/2011	4/30/2011	3.5
IP740	EOS	6/30/2005	6/30/2010	6/30/2010	3.4.1
IP1220	Active				3.7.1 Build 016(3)
IP1260	Active				3.7(3)
IP2250	EOS	5/31/2006	(2)		3.8 Build 034
IP2255	Active				4.1
IP2450	Active				4.2 Build 069

Table 2-7 The support status for the Nokia IP Security appliances. (Nokia Inc., 2007)

Nokia IPSO Version	FCS or Build	Compatible Check Point Software Version(s)
3.4	4A	4.1 SP4, SP4 HF, SP5
	9	4.1 SP4, SP4 HF, SP5, SP5a, SP6
3.4.1	5	4.1 SP5
	5a	4.1 SP5a, 4.1 SP6
	10	4.1 SP5a
	11, 12, 15, 16, 21	4.1 SP5a, SP6
3.4.2	3	NG FP1
3.5	3	4.1 SP5a, NG FP2
	6, 7	4.1 SP5a, SP6; NG FP2
	8	4.1 SP5a, SP6, NG FP2, FP3 VSX 1.0; GX 1.5
	10, 14, 15, 17, 18, 19, 22, 23, 24	4.1 SP5a, SP6; NG FP2, FP3; VSX 1.0; GX 1.5, 1.5 HS1, 2.0
3.5.1 (1)	2, 6, 7, 8, 10, 11, 12	NG FP2, FP3
3.6	3, 4, 6, 7, 13, 14, 17, 18	NG FP2 (2), FP3
3.7	023, 026, 027, 029, 031	NG FP3 HF2, NG AI (3) R54
	032, 034, 035, 036, 039, 041, 044, 048, 049	NG FP3 HF2,NG AI (3) R54,NG AI R55,NG AI R55W,GX 2.5 (4)
3.7.1	004, 007, 010, 012, 013, 016, 020, 024, 025	NG FP3 HF2,NG AI (3) R54,NG AI R55,NG AI R55W,GX 2.5 (4)
3.7.89	004, 008	VPN-1 VSX NG AI Release 2
3.7.90	006	VPN-1 VSX NG AI Release 2.1N (4)
3.7.99 (5)		NG FP2
3.8	031, 034, 039, 045, 049, 051, 055, 058, 059, 061	NG AI R55 for Nokia IPSO 3.8 (6)
3.8.1	028, 029, 033, 035, 038, 044, 045, 048	NG AI R55 for Nokia IPSO 3.8 (6)
3.9 (7)	035, 037, 041, 045, 052, 056, 065, 068	NG AI R55,NGX R60,NGX R61,NGX R62,GX NGX,IPv6 Pack
3.9 (8)	45c	NGX R60
3.9.90	019	VPN-1 VSX NG AI Release 2.2N (9)
3.9.91	014	VPN-1 VSX NG AI Release 2.3N (10)
3.9.92	005, 008	VPN-1 VSX NG AI Release 2.3N (11)
4.0	023, 030, 040, 041, 045, 048	NGX R60,NGX R61,GX NGX,IPv6 Pack
4.0.1	008, 010, 011	NGX R60, NGX R61
4.1 (12)	013, 016, 019, 022, 025, 028, 033, 035	NGX R60,NGX R61,NGX R62,NGX R65(FW Only)(15),FW-1 GX 4.0
4.1 (13)	20c	NGX R60
4.2	029, 031, 038, 041, 042_HF002, 042_HF003, 051_HFA02, 051A04(16), 069	NGX R62,NGX R65(FW & UTM)(15),FW-1 GX 4.0 (14)

Table 2-8 The versions of the Nokia IPSO operating system and compatible Check Point applications. (Nokia Inc., 2007)

2.6 Privileged account access control

2.6.1 Risk

As organizations face the challenge of keeping control over their network resources in response to endlessly developing security threats, system administrators must maintain computer security, while allowing user productivity. The solution must be able to sustain an attack and assure data confidentiality, integrity, and availability.

Because of its sensitive role, a firewall system should be carefully administered, with permissions delegated carefully. This section describes administration considerations and provides a checklist on how to administer a firewall in a secure manner.

2.6.2 Checklist

The checklist will include:

a. Presence of login warning banner.

Warning banners are implemented to provide legal protection. There are several issues that the banner should address; therefore its content should be established in conjunction with the company's legal staff.

b. Remote administration restricted to particular hosts.

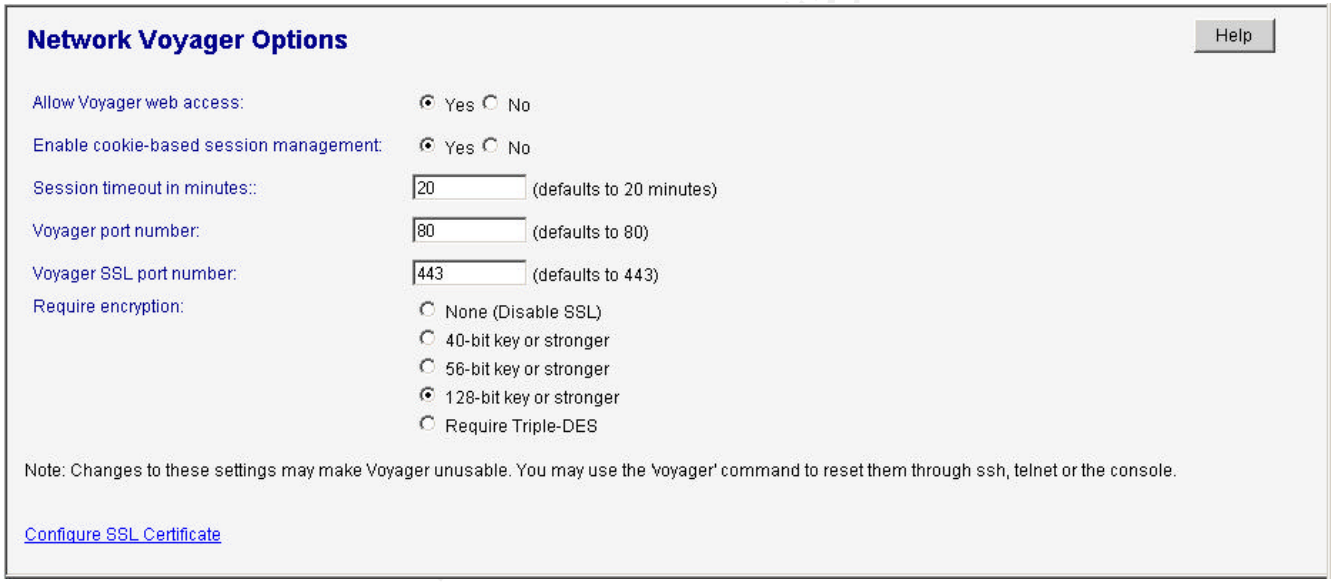
In case of Nokia firewall this is done via the Checkpoint policy. Verify that appropriate firewall rule is in effect. Evaluate all rules with the destination of the Firewall object in question. Only high-security secure protocols such as SSHv2 or HTTPS (+128 bit encryption) should be allowed.

c. Remote administration encrypted and authenticated.

Nokia leaves the Voyager remote console encryption as an optional feature. This checklist will ensure all the administrator's activity is confidential.

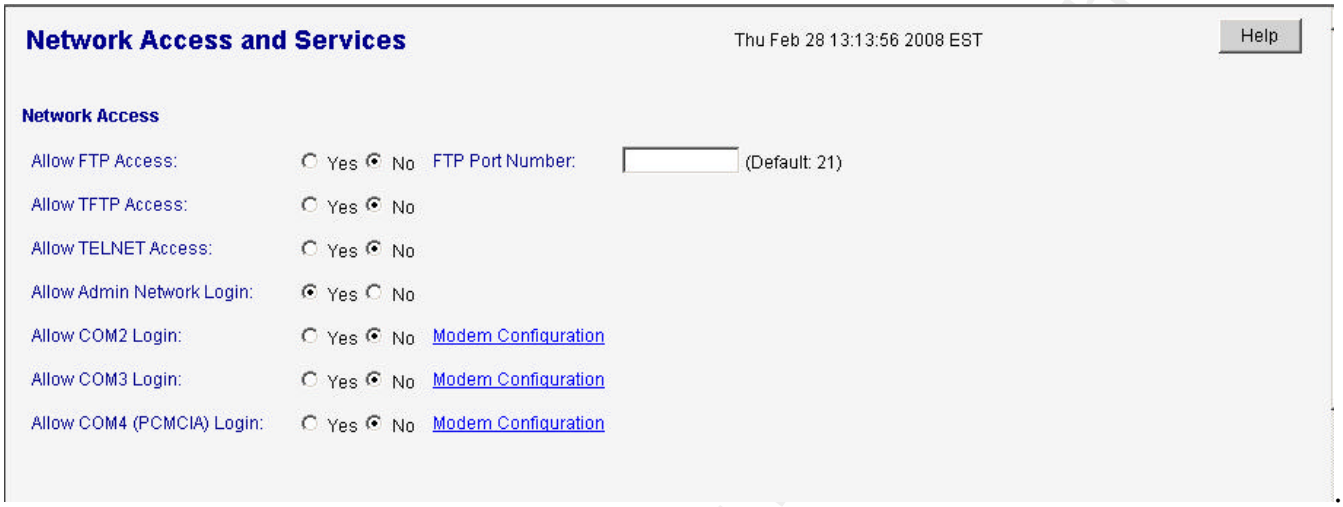
Under the Voyager navigation tree select Configuration->Security and Access-> Voyager Web Access-> Network Voyager Options.

The encryption level must be set to 128-bit key or stronger.



Next, under the Voyager navigation tree select Configuration->Security and Access-> Network Access and Services

Verify that insecure, poorly authenticated, clear-text protocols such as FTP, Telnet and TFTP are not enabled.



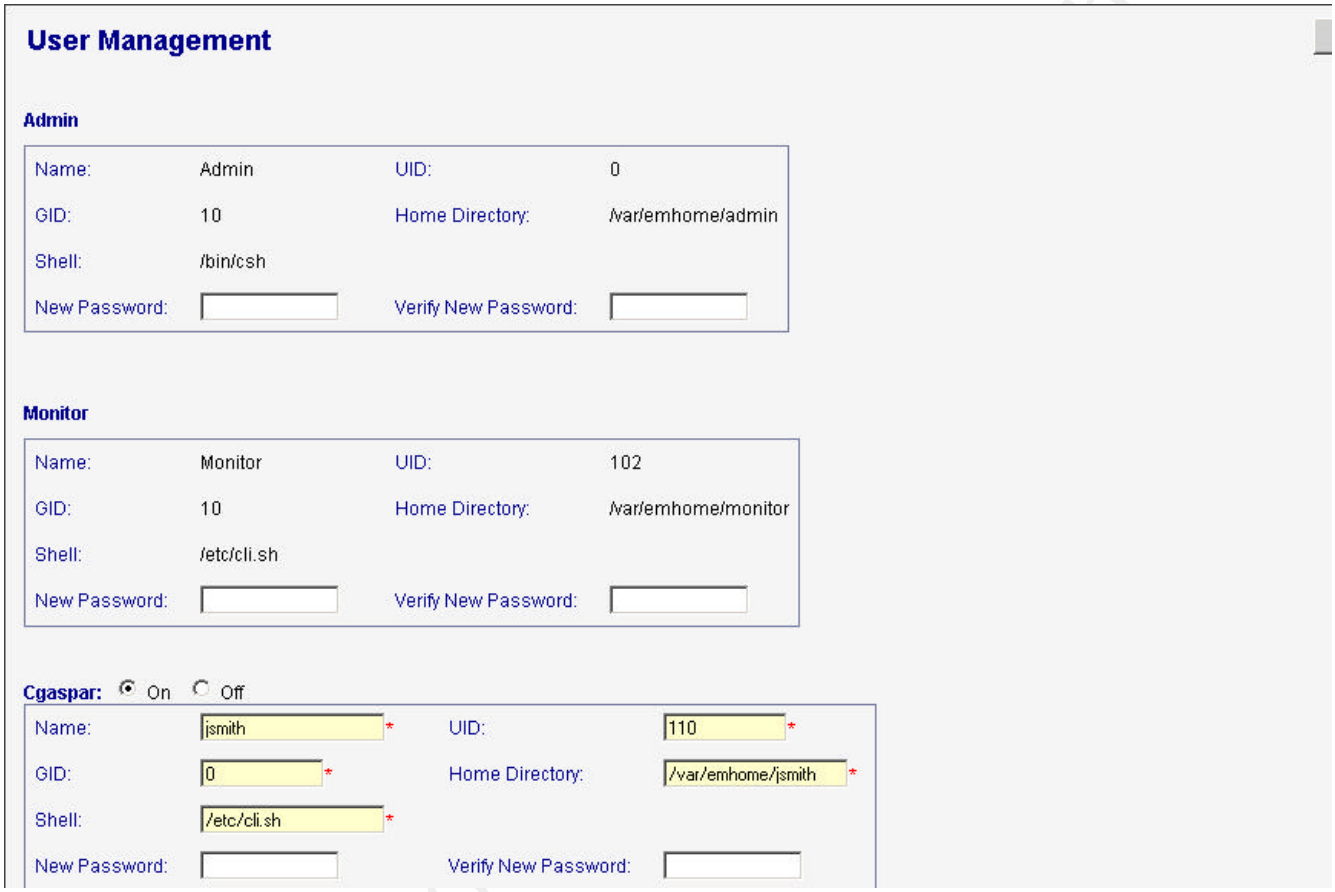
Finally, in the home directories, review the hidden startup files. The *.rhosts* file opens a non-authenticated access to the corresponding account over the network, therefore should not be found in any of the Nokia home directories.

```
# ls -al
drwxr-xr-x   3 root  wheel       512 Mar  3 14:14 .
drwxr-xr-x  25 root  wheel       512 Jun  8  2007 ..
-rw-------   1 root  wheel      5028 Jul 11  2007 .clish_history
-rwxr-xr-x   1 root  wheel      1039 May  1  2005 .cshrc
-rw-------   1 root  wheel      5340 Feb 29 17:26 .history
-rw-rw-r--   1 root  wheel       498 Feb 10  2007 .iclid_history
-rwxr-xr-x   1 root  wheel       114 May  1  2005 .login
-rwxr-xr-x   1 root  wheel       573 May  1  2005 .profile
drwxrwxr-x   2 root  wheel       512 May 25  2005 bin
-rw-rw-r--   1 root  wheel       985 Mar  3 14:14 .rhosts
```

d. Unique administrative accounts in use

Shared accounts compromise the accountability on the system therefore should not be used. Since users' activity is logged with a numeric user-id, each user needs to be associated with unique id number.

Under the Voyager navigation tree select Configuration->Security and Access-> Users Management



e. Password file analysis.

Each user account entry in the Nokia password file should consist of 7 colon-separated fields

Accountname:encrypted_password:user-id:group-id:comment:home directory:shell

An asterisk should be seen in place of the encrypted password. That means the encrypted password is stored in /etc/shadow which can only be accessed by root, whereas the /etc/passwd must be readable by all users. If the password field is blank the corresponding account has no password. No account should be left without password. That includes system accounts such as daemon, monitor which otherwise can be abused. The guest account should not be available, altogether.

The following is an example of Nokia */etc/passwd* file.

```
#vi /etc/passwd

root:*:0:0:Root:/var/admin:/bin/csh
admin:*:0:0:Admin:/var/admin:/bin/csh
monitor:*:102:10:Monitor:/var/monitor:/bin/csh
nobody:*:65534:65534:Unprivileged user:/nonexistent:/nonexistent
jsmith:*:110:20:jsmith:/var/jsmith:/bin/csh
test:*:0:0:Test:/var/test:/bin/csh
```

2.7 Firewall rulebase compliance

2.7.1 Risk

The protection that a firewall can provide is only as good as the policy it is configured to enforce. Corporate firewalls are often enforcing rule sets that do not comply with industry well-established best practices.

2.7.2 Checklist

The checklist will include an examination of the following:

a. Firewall rule base complexity

This may appear subjective initially, however as a common source of configuration errors should be looked at in more detail. Are the rules redundant or obsolete? Is the number of rules excessive? Can the rules be consolidated? Is the purpose of the rule obvious? Is the corresponding documentation sufficient? These are examples of the common sense questions that need to be answered.

b. Configuration errors

Is the rule precisely defined or due to it broad definition "back-door" connections to the firewall or unwanted traffic into the internal network may be allowed?

c. Implicit rules

In addition to the access rules defined with in the policy firewalls often allow automatic creation of implicit rules. The problem with implicit rule is that for given service they allow broad access to/from any IP address. In most cases they should be eliminated and replaced with explicit policy rules.

d. Vulnerable services

Certain communication protocols with inherent security risks such as NetBios, RPC and TFTP should be blocked by the firewall policy. A good source of Information Security vulnerabilities can be http://www.securityfocus.com/ and http://nvd.mist.gov

e. "Any" rules

A special consideration has to be given to the "Any" rules. "Any" covers Inside, DMZ and the Internet. This may not be apparent while such rule is implemented, therefore remains a common firewall configuration error.

f. Anti-spoofing enabled on all interfaces

Verify that private (RFC 1918) addresses are not accepted on any public interface. These are:

```
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 - 192.168.255.255
```

Verify that loopback, reserved or zero (RFC 1700) addresses are not accepted on any interface. These are:

```
127.0.0.0 - 127.255.255.255
240.0.0.0 - 255.255.255.255
0.0.0.0 - 0.255.255.255
```

g. Verify the rule set structure. The following order is an example of best practice approach.

1. 'Drop' rules for malicious/suspicious traffic – logged and alerted (abnormal, not compliant traffic)
2. Firewall stealth rules - the stealth rule matches packets destined to the firewall.
3. 'permit' rules for expected irrelevant high volume traffic – not logged (VRRP, other talkative protocols)
4. Global Network 'permit' rules (DNS, NTP etc.)
5. Application specific rules (HTTP, FTP, SMTP etc.)
6. Administrative access rules (SSH, SNMP etc.)
7. 'Drop' and log everything else.

2.8 Firewall rulebase optimization

2.8.1 Risk

As the firewall operations team processes hundreds of change requests, and the corporate security objectives mature over time, the underlying rule base that contains the firewall policy becomes extremely large and complex, with many of the rules and objects that may be outdated and not in use anymore. These obsolete rules create a potential security hole and should be removed.

With every new connection, the Firewall sequentially examines the rule base, looking for the first exact match. As the rule base increases in size, the performance of the Firewall becomes inevitably impaired. Processing a larger rule base, the inspection engine must scan more entries in order to match a new packet flow with the correct rule. This activity can degrade Firewall response time and throughput. Moreover, the larger the rule set the more time and system resources are required to validate, compile and deploy the firewall policy. The rule order should be inspected on an ongoing basis and adjusted so that most used rules are located higher in the rulebase. Finally, logging as one of the factors causing high CPU utilization should be turned off for connections

that do not require tracking.

2.8.2 Checklist

Eventia Reporter (component of Checkpoint Smart Center Suite) or a third party firewall analyzer should be employed to obtain statistics on object and rule usage. The results will be divided into the following four categories.

a. Obsolete rules and objects

- may be eliminated upon investigation

b. High frequency rules

- may be moved to the top of the policy

c. Low frequency rules

- may be moved down

d. Rules with no tracking

- ascertain if tracking is required

3 Audit Report

3.1 Management Summary

The purpose of this project was to assess the current state of EastCoast Enterprises' Nokia firewall infrastructure. The assessments efforts focused specifically on capacity, performance and security of the IP530

firewall models. Although, the recommendations are aimed at leveraging existing security technologies and integrating them into stronger overall architecture, to address critical weaknesses, the recommendations will require investments in new infrastructure components.

The recommendations are summarized as follows:

A. Bring all firewalls to a common patch level. Stay current with the latest software and security updates.

B. Develop Firewall performance monitoring, alerting and reporting capability.

C. Improve Firewall critical event monitoring, alerting and logging.

D. Review and evaluate backup processes.

E. Remove single point of failures in firewall deployments.

F. Review and evaluate firewall rule sets.

G. Implement legal warning banners on all security devices.

H. Reassure that Change Management processes and Shared Account Usage policies are followed

I. Plan for End Of Life Nokia firewall replacement.

3.2 Detailed Findings and Recommendations

A. FIREWALL CAPACITY AND SYSTEM ASSURANCE EXAMINATION

3.2.1.1 Current and historical system resource utilization: CPU, Memory, Disks

During this examination it has been revealed that ECFW1N, ECFW2N, ECFW2H, ECFW1L and ECFW2L

were constantly reporting 100% CPU utilization. That was seen using both the NOKIA CPU Monitor (Figure 3-1 ECFW1N CPU Utilization) and the Nokia internal statistics (vmstat). It has been determined that the packets drop does not occur and that the root cause is not related to the volume of traffic traversing through the firewalls. It appears to be related to a malfunctioning VRRP process. Further investigation to identify and eradicate the root cause is strongly recommended.

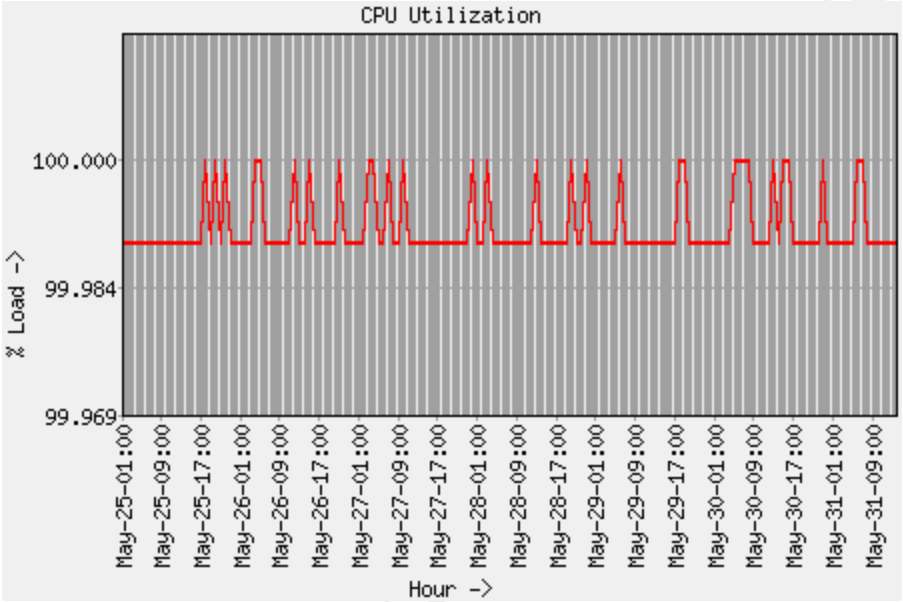


Figure 3-2 ECFW1N CPU Utilization

3.2.1.2 Current and historical network bandwidth utilization

Although network monitoring and reporting feature is enabled, it does not appear to be functional. For example, the DMZ interface is reporting 0 packet output rate. Adequate traffic monitoring, shaping and reporting can be accomplished by investing in third party infrastructure components.

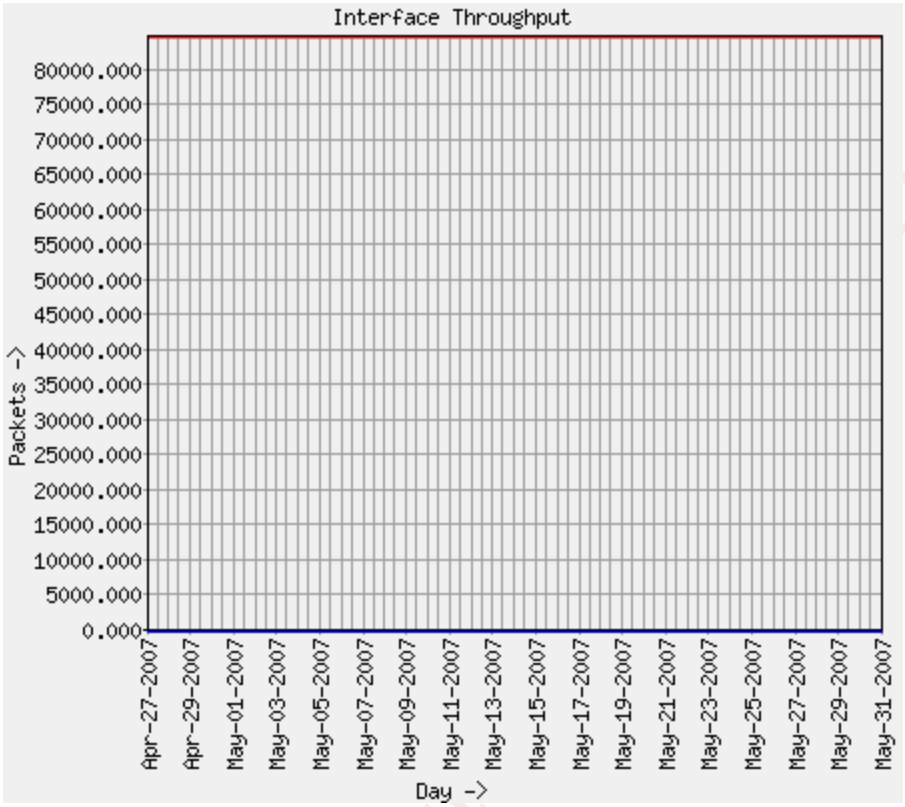


Figure 3-3 Packet Throughput for interface DMZ

3.2.1.3 System health and performance monitoring/alerting

The following findings have been revealed.

A. The native email based critical event notifications (fault management) is not enabled.

B. SNMP Traps have been configured as shown in Table 3-1

It is recommended that

A. The email based critical event notifications be considered

B. The following SNMP traps be enabled:

1. Cold Start traps
2. LinkUp/linkDown traps
3. System Power Supply Failure trap
4. System Over Temperature trap
5. System Fan Failure trap
6. System Disk Failure trap

ColdStart traps:	enabled
LinkUp/linkDown traps:	enabled
Authentication traps:	disabled
VRRP Trap New Master traps:	disabled
VRRP Trap Authentication Failure traps:	disabled
System Trap Configuration Change traps:	disabled
System Trap Configuration File Change traps:	disabled
System Trap Configuration Save Change traps:	disabled
System Trap Low Disk Space traps:	disabled
System Trap No Disk Space traps:	disabled
System Disk Failure trap:	disabled
System Trap Disk Mirror Set Create trap:	disabled
System Trap Disk Mirror Set Delete trap:	disabled
System Trap Disk Mirror Sync Success trap:	disabled
System Trap Disk Mirror Sync Failure trap:	disabled
Cluster Member Reject trap:	disabled
Cluster Member Join trap:	disabled
Cluster Member Left trap:	disabled

Cluster NewMaster trap:	disabled
Cluster Protocol Interface Change trap:	disabled
System Power Supply Failure trap:	disabled
System Over Temperature trap	disabled
System Fan Failure trap:	disabled
Trap PDU Agent Address:	
System location:	ECFW2H - HEC data center
System contact:	

Table 3-1 SNMP trap configuration

3.2.1.4 Event logging.

Although Local System Log is enabled, it has been revealed that Audit Trail and Remote logging via Syslog are not currently in use.

The recommendation will include enabling Audit Trail and Remote logging via Syslog.

Table 3-2 Findings' Summary

	ECFW1N	ECFW2N	ECFW1H	ECFW2H	ECFW2LQ	ECFW1L	ECFW2L	ECFW2V
CPU	✗	✗	✓	✗	✓	✗	✗	✓
RAM	✓	✓	✓	✓	✓	✓	✓	✓
HDD	✓	✓	✓	✓	✓	✓	✓	✓
Network Utilization	✗	✗	✗	✗	✗	✗	✗	✗
System Performance Monitoring/Alerting	✗	✗	✗	✗	✗	✗	✗	✗
Event Logging	✗	✗	✗	✗	✗	✗	✗	✗
Admin Audit Trail	✗	✗	✗	✗	✗	✗	✗	✗
Critical Event Alert.	✗	✗	✗	✗	✗	✗	✗	✗

B. FIREWALL BACKUP AND FAULT RECOVERY EXAMINATION

The EastCoast Security Operations team addresses the firewall high availability considerations by implementing the Nokia VRRP protocol. Stateful failover has been accomplished by introducing the Checkpoint State Synchronization. The VRRP and state synchronization configuration and status appear correct. Firewall failover test is outside of the scope of this assessment.

The Checkpoint Management Center is the central depository for the Nokia firewall policies. It is a distributed system residing in multiple locations (Boston, MA and Philadelphia, PA) in High Availability mode with automatic state synchronization. Although, all the firewall polices are successfully backed up to the corporate storage manager via the Checkpoint Management Server, each of the Nokia firewalls has a unique system configuration that are not automatically backed up. Manual backups have been performed in the past; they are not current, however.

Table 3-3 Findings' Summary

	ECFW1N	ECFW2N	ECFW1H	ECFW2H	ECFW2LQ	ECFW1L	ECFW2L	ECFW2V
Firewall high availability	✔	✔	✔	✔	✘	✔	✔	✔
Firewall statefull failover	✔	✔	✔	✔	✘	✔	✔	✔
Firewall backup process validation	✘	✘	✘	✘	✘	✘	✘	✘

C. FIREWALL CHANGE MANAGEMENT COMPLIANCE EXAMINATION

The Checkpoint Smart View Tracker audit log for the month of May 2007 has been examined. The findings are as follows:

Table 3-4 Findings' Summary

Number	Date	Time	Operation	Status	Performed On	Chng Track #	CM Compliance
45093	3-May-07	19:46:50	Install Policy	Success	ECFWL_POLICY	PLN0323438	✔
45064	3-May-07	18:38:25	Install Policy	Success	ECFWH_POLICY	Not found	✘
45078	3-May-07	19:37:00	Install Policy	Success	ECFWH_POLICY	PLN032438	✔
45099	3-May-07	19:51:17	Install Policy	Success	ECFWN_POLICY	PLN034538	✔
46195	10-May-07	17:28:39	Install Policy	Success	ECFWL_POLICY	Not found	✘

46300	10-May-07	20:24:38	Install Policy	Success	ECFWH_POLICY	PLN033281	✔
47461	17-May-07	18:06:04	Install Policy	Success	ECFWH_POLICY	EBR032344	✔
48632	24-May-07	19:05:52	Install Policy	Success	ECFWL_POLICY	Not found	✘

D. FIREWALL SOFTWARE VULNERABILITY AND PATCH EXAMINATION

During this phase of the IP530 security assesment it has been revealed that each of the firewalls was missing important software updates. Check Point recommends that the latest HFA be installed in order to stay current with the latest software and security updates.

Table 3-5 shows some of the problems identified and corrected by Checkpoint since the release of the currently installed HFA_14.

Table 3-5 Findings' Summary

HFA	Description	Installed On
R55_18-19	FireWall-1: Miscellaneous FWD stability has improved and it is no longer core dumped.	Gateway
R55_18-29	ClusterXL: General The cphamcset process has been enhanced.	Gateway
R55_17-25	FireWall Improved memory allocation. The following message was displayed fwhandle_pool_add: Table kbufs - All available pools exhausted when a structure required for the infrastructure could not be found on account of the memory allocation.	Gateway
R55_15-4	VPN-1 When authenticating users and installing a	Enforcement Module

	Security Policy simultaneously, vpnd may show signs of instability.	
R55_15-13	FireWall-1 The IPSO OS has severe performance issues when a packet with source IP address 0.0.0.0 generated by FireWall-1, passes through FireWall-1 to IPSO OS. These packets should be blocked in the function that passes the packets to the IP stack.	Nokia Enforcement Module (IPSO)
R55_15-16	FireWall-1: Security Servers Improved stability of fwd file descriptors.	Enforcement Module
R55_15-19	FireWall-1: Stateful Inspection IDs of inspect handlers may change dynamically as a result of SmartCenter server upgrade or SmartDefense update. Keep connections or load proof handler connections may then hold inspect handlers ids that are no longer relevant, (for instance they may run other inspect handlers!). This may result in some system instability.	Enforcement Module
R55_15-13	FireWall-1 The IPSO OS has severe performance issues when a packet with source IP address 0.0.0.0 generated by FireWall-1, passes through FireWall-1 to IPSO OS. These packets should be blocked in the function that passes the packets to the IP stack.	Nokia Enforcement Module (IPSO)

Table 3-6 presents detailed findings and recommendations for each IP530 appliance.

Table 3-6 Findings' Summary

	ECFW1N	ECFW2N	ECFW1H	ECFW2H	ECFW2LQ	ECFW1L	ECFW2L	ECFW2V
A. Current state								
Overall compliance	✕	✕	✕	✕	✕	✕	✕	✕
Version	NG R55	NG R55	NG R55	NG R55	NG R55	NG R55	NG R55	NGX R61
HFA	HFA 14	HFA 14	HFA 14	HFA 14	HFA 16	HFA 14	HFA 14	-
Hotfix	463	463	463	463	595	463	463	-
Build	008	008	008	008	006	008	008	207
B.								
Current HFA/ date of release	HFA 19 22-Feb-07	HFA 19 22-Feb-07	HFA 19 22-Feb-07	HFA 19 22-Feb-07	HFA 19 22-Feb-07	HFA 19 22-Feb-07	HFA 19 22-Feb-07	HFA 01 25-Oct-06
Missing HFA's (number of issues addressed)	HFA 19 (37) HFA 18 (32) HFA 17 (36) HFA 16 (21) HFA 15 (26)	HFA 19 (37) HFA 18 (32) HFA 17 (36) HFA 16 (21) HFA 15 (26)	HFA 19 (37) HFA 18 (32) HFA 17 (36) HFA 16 (21) HFA 15 (26)	HFA 19 (37) HFA 18 (32) HFA 17 (36) HFA 16 (21) HFA 15 (26)	HFA 19 (37) HFA 18 (32) HFA 17 (36)	HFA 19 (37) HFA 18 (32) HFA 17 (36) HFA 16 (21) HFA 15 (26)	HFA 19 (37) HFA 18 (32) HFA 17 (36) HFA 16 (21) HFA 15 (26)	HFA 01 (19)
C. Recommendation								
Short term								
HFA	**HFA 19**	**HFA 19**	**HFA 19**	**HFA 19**	**HFA 19**	**HFA 19**	**HFA 19**	**HFA 01**
Long term								
Version	**NGX R62**	**NGX R62**	**NGX R62**	**NGX R62**	**NGX R62**	**NGX R62**	**NGX R62**	**NGX R62**
HFA	**latest available**	**latest available**	**latest available**	**latest available**	**latest available**	**latest available**	**latest available**	**latest available**

E. FIREWALL OPERATING SYSTEM VULNERABILITY AND PATCH EXAMINATION

The following table lists the NOKIA support status for the IP Security appliances.

Platform/Product	Status	EOS Date	EOCS Date	EOL Date	Minimum OS Version
IP530	EOS	3/31/2005	3/31/2010	3/31/2010	3.3.1

The following table lists the versions of the Nokia IPSO operating system, their current support status, and the projected end-of-maintenance and end-of-life dates.

Nokia IPSO Version	FCS or Build	Nokia IPSO Support Status	Projected EOL Date
3.7.1	004, 007, 010, 012, 013, 016, 020, 024, 025	EOL	May 24, 2007
4.1	013, 016, 019, 022, 025, 028, 030	EOS	January 31, 2010
4.2	029, 031, 038	Active	

The following table lists the compatible versions of the Nokia IPSO operating system and the Check Point applications.

Nokia IPSO Version	FCS or Build	Compatible Check Point Software Version(s)
3.7.1	004, 007, 010, 012, 013, 016, 020, 024, 025	NG FP3 HF2, NG AI R54, NG AI R55, NG AI R55W, GX 2.5
4.1	013, 016, 019, 022, 025, 028, 030	NGX R60, NGX R61, NGX R62
4.2	029, 031, 038	NGX R62, FW-1 GX 4.0

The following table presents the results of the Nokia IP530 software examination.

Except the recently deployed ECFW2V all the Nokia appliances as of May 2007 run an outdated version of IPSO. Although version 4.1 may be considered, an upgrade to 4.2 is recommended.

Table 3-7 Findings' Summary

	ECFW1N	ECFW2N	ECFW1H	ECFW2H	ECFW2LQ	ECFW1L	ECFW2L	ECFW2V
Current state								
Compliance	✗	✗	✗	✗	✗	✗	✗	✓
OS Software	IPSO	IPSO	IPSO	IPSO	IPSO	IPSO	IPSO	IPSO
Version	3.7.1	3.7.1	3.7.1	3.7.1	3.7.1	3.7.1	3.7.1	4.1
Build	020	020	020	020	020	020	020	017
Recommendation:								
Version	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2
Build	038	038	038	038	038	038	038	038

F. PRIVILEGED ACCOUNT ACCESS CONTROL EXAMINATION

The following privileged accounts have been identified:

Table 3-8 Privileged accounts

ACCOUNT	AUTHENTICATION	OWNERSHIP
admin	Local password	Shared
audit	Local password	Shared
callan	SecurID	Personal

jsmith	SecurID	Personal
blinda	Local password	Personal
appears	SecurID	Personal
wimallu	SecurID	Personal
rlakos	SecurID	Personal
mbrown	SecurID	Personal

Table 3-9 Shared account usage shows the usage of shared account during the Month of May 2007.

Table 3-9 Shared account usage

Number	Date	Time	Subject	Administrator	General Information
44581	1-May-07	8:24:11	Administrator Login	admin	Authentication method: Internal Password
45236	4-May-07	11:38:57	Administrator Login	admin	Authentication method: Internal Password
45270	4-May-07	13:53:15	Administrator Login	admin	Authentication method: Internal Password
45284	4-May-07	15:28:44	Administrator Login	admin	Authentication method: Internal Password
45311	4-May-07	20:01:18	Administrator Login	admin	Authentication method: Internal Password
47510	17-May-07	19:35:15	Administrator Login	admin	Authentication method: Internal Password
48070	21-May-07	14:03:49	Administrator Login	admin	Authentication method: Internal Password
48332	23-May-07	12:01:12	Administrator Login	admin	Authentication method: Internal Password
48725	25-May-07	9:26:14	Administrator Login	admin	Authentication method: Internal Password

With the exception of the above, unique privileged accounts are used (only shared are shown). Firewall rules have been implemented to restrict access to a set of administrative subnets only. This sensitive communication is encrypted with HTTPS or Checkpoint proprietary SIC protocol. It is strongly recommended that a legal warning banner be presented before access to any EastCoast Enterprises security device is granted.

The following is an example of such banner:

********** *WARNING* **********

You have accessed a private computer system. This system is for authorized use

only and user activities may be monitored and recorded by company personnel.

Unauthorized access to or use of this system is strictly prohibited and

constitutes a violation of federal, criminal, and civil laws. Violators may

be subject to employment termination and prosecuted to the fullest extent of

the law. By logging in you certify that you have read and understood these

terms and that you are authorized to access and use the system.

****

Table 3-10 Findings' Summary

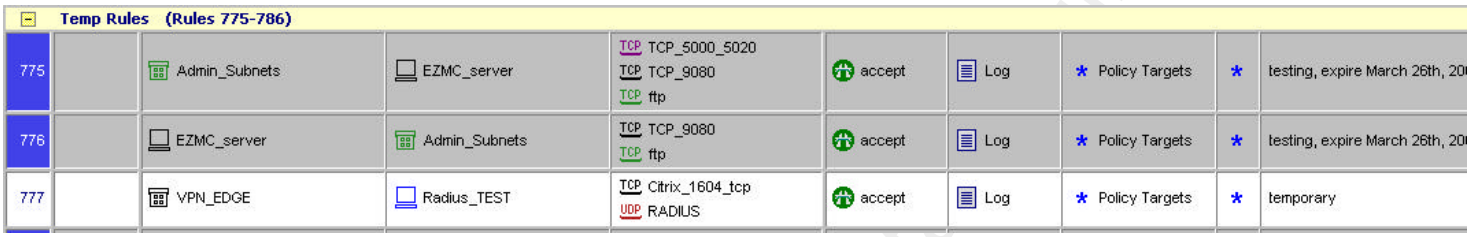
	ECFW1N	ECFW2N	ECFW1H	ECFW2H	ECFW2LQ	ECFW1L	ECFW2L	ECFW2V
Legal warning	✗	✗	✗	✗	✗	✗	✗	✗
Admin ACL	✔	✔	✔	✔	✔	✔	✔	✔
Encrypted communication	✔	✔	✔	✔	✔	✔	✔	✔
Unique admin accounts	✔	✔	✔	✔	✔	✔	✔	✔
Password file analysis	✔	✔	✔	✔	✔	✔	✔	✔

G. FIREWALL RULEBASE COMPLIANCE EXAMINATION

The following findings were revealed while reviewing the firewall rules:

a. Rule base complexity

Firewall rule base complexity examination uncovered two issues. The rule sets on some of the firewalls are overgrown, thus very difficult to manage (i.e. ECFWN_POLICY: 743 rules). The rule sets may contain obsolete or malformed rules [Figure 3-4], which could lead to a successful exploit.

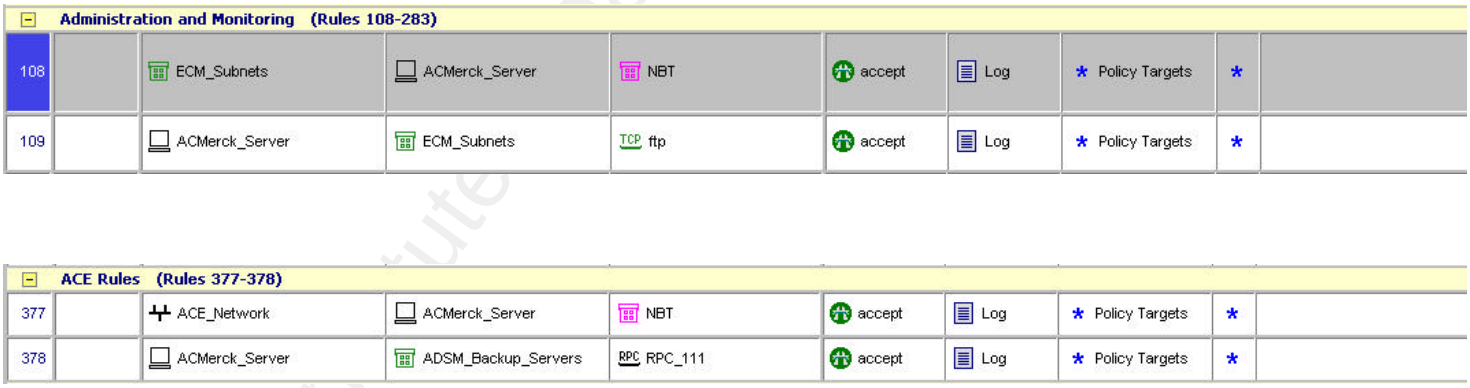


Temp Rules (Rules 775-786)									
775		Admin_Subnets	EZMC_server	TCP_5000_5020 TCP_9080 ftp	accept	Log	* Policy Targets	*	testing, expire March 26th, 20
776		EZMC_server	Admin_Subnets	TCP_9080 ftp	accept	Log	* Policy Targets	*	testing, expire March 26th, 20
777		VPN_EDGE	Radius_TEST	Citrix_1604_tcp RADIUS	accept	Log	* Policy Targets	*	temporary

Figure 3-4 ECFWN_POLICY excerpt – obsolete, malformed rules

b. Vulnerable services.

Services such as NetBIOS, RPC, telnet and ftp are in use. Moreover NetBIOS ports are open from an un-trusted network to the Internal Domain Controllers.



Administration and Monitoring (Rules 108-283)									
108		ECM_Subnets	ACMerck_Server	NBT	accept	Log	* Policy Targets	*	
109		ACMerck_Server	ECM_Subnets	ftp	accept	Log	* Policy Targets	*	

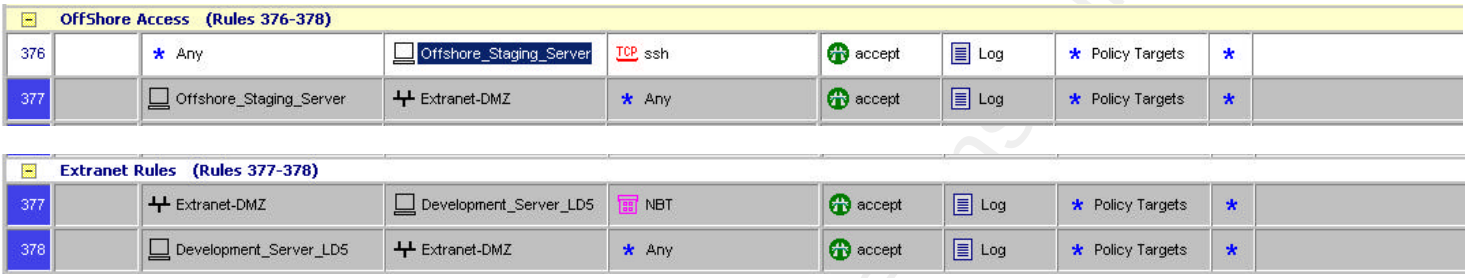
ACE Rules (Rules 377-378)									
377		ACE_Network	ACMerck_Server	NBT	accept	Log	* Policy Targets	*	
378		ACMerck_Server	ADSM_Backup_Servers	RPC_111	accept	Log	* Policy Targets	*	

Figure 3-5 ECFWH_POLICY excerpt – NetBIOS, RPC, FTP

c. "Any" Rules

"Any" rules appear to be commonly in use. For Example in Rule #376 the apparent objective was to provide access from EastCoast's hosts located on various DMZs to a group of hosts on the Internal networks and NOT from the Internet. It has also been uncovered that "Any" service is commonly in use. "Any" includes

numerous high-risk services including RPC and NetBIOS, therefore should be avoided and in most cases it is not necessary.



OffShore Access (Rules 376-378)								
376		* Any	Offshore_Staging_Server	TCP ssh	accept	Log	* Policy Targets	*
377		Offshore_Staging_Server	Extranet-DMZ	* Any	accept	Log	* Policy Targets	*

Extranet Rules (Rules 377-378)								
377		Extranet-DMZ	Development_Server_LD5	NBT	accept	Log	* Policy Targets	*
378		Development_Server_LD5	Extranet-DMZ	* Any	accept	Log	* Policy Targets	*

Figure 3-6 ECFWL_POLICY excerpt – 'ANY' rules

d. Rule sets structure

In general, a proper rule order is being followed, however there are exceptions such as ECFWN_POLICY, where the stealth rule has been omitted. It is recommended that all the firewall policies be reviewed on an ongoing basis with a strong focus on maintaining a proper rule sets structure.

H. FIREWALL RULEBASE OPTIMIZATION EXAMINATION

Eventia Reporter was used to provide the following statistics. As the Eventia System was still in the deployment phase, not all the statistics were available at the time of the examination.

The analysis of the ECFWV_POLICY statistics reveals that 63.94% of total policy scans resulted in matching rule #92 (out of 140). Respectively rule #67 (out of 148) of the ECFWL_POLICY matched 29.26% of all policy scans.

Further rule set review is highly recommended. By optimizing the rule order significant performance gain can be obtained.

Additionally, existence of rules with no matching connection has been uncovered. It is recommended that these be investigated carefully. They may be candidates for removal, but it is worth to note that this behavior may be resulting from the nature of the application the rule is meant to support.

Table 3-11 Matched Logged Rules (Policy: ECFWV_POLICY)

Top Matched Logged Rules (Policy: ECFWV_POLICY)		
Rule Number in Current Policy	**Number of Connections**	% of Total Connections
92	4,459,645	63.94%
139	937,217	13.44%
Implied	790,872	11.34%
12	507,851	7.28%
126	197,821	2.84%
90	27,582	0.40%
59	14,684	0.21%
93	13,378	0.19%
40	11,809	0.17%
129	9,410	0.13%
9	1,605	0.02%
1	1,094	0.02%
132	294	0.00%
88	291	0.00%
42	213	0.00%
47	148	0.00%
55	147	0.00%
92*	139	0.00%
5	133	0.00%
131	87	0.00%
Others (9)	253	0.00%
Total (29)	6,974,673	100.00%
Average	240,506	3.45%

Table 3-12 Top Matched Logged Rules (Policy: ECFWL_POLICY)

Top Matched Logged Rules (Policy: ECFWL_POLICY)		
Rule Number in Current Policy	Number of Connections [Thousands]	% of Total Connections
67*	10,555.03	29.26%

34*	6,396.36	17.73%
73*	3,693.24	10.24%
39*	3,434.58	9.52%
42*	1,888.82	5.24%
51*	1,774.88	4.92%
89*	1,672.61	4.64%
25*	1,447.38	4.01%
147*	1,376.72	3.82%
148*	861.85	2.39%
121*	597.64	1.66%
76*	588.55	1.63%
11*	359.79	1.00%
24*	270.03	0.75%
85*	199.52	0.55%
78*	139.30	0.39%
5*	123.58	0.34%
37*	109.53	0.30%
88*	99.72	0.28%
72*	86.00	0.24%
Others (43)	402.14	1.11%
Total (63)	36,077.25	100.00%
Average	572.65	1.59%

4 Conclusion

Firewalls, along with other perimeter security solutions control access to critical resources and services so that only legitimate users and information can pass trough the network, according to a predefined policy. If not adequately controlled, enterprise networks are increasingly vulnerable to security threats.

EastCoast makes extensive use of firewalls along its perceived network perimeter. The IT staff implements firewall pairs at all Internets access points as well as at the entry points for financial data feeds and business partner connections. Firewalls are not used for boundary control within the network, however. The current state of EastCoast's firewall performance, recoverability, capacity and security was assessed and compared against existing policies or industry best practices, in those areas where internal policies were not available. This Nokia IP530 Assessment provides EastCoast Enterprises with information to defy potential attacks and intrusions. The assessment allows EastCoast Enterprises to identify vulnerabilities, provides guidelines to

correct the vulnerabilities, and to ensure the company achieves the expected results in protecting its resources by continuing to invest in Nokia based firewall technology while the replacement platform is being selected.

5 References

Ingber, Ed (2002). Using CPU Utilization Instrumentation In IPSO

EastCoast Enterprises, (2007). Production Change Management Policies & Procedures

Nokia Inc., (2007). Nokia IP Security Platform Performance Best Practices. White Paper.

Nokia Inc., (2007). IP Security Platforms. Network Security. https://support.nokia.com/home/static/productsSupported_smc.htm#top

Check Point Software Technologies Ltd., (2007). Solution ID: sk9408, Common ports used by Check Point Next Generation (NG). https://supportcenter.checkpoint.com

Check Point Software Technologies Ltd., (21-Oct-2007). Latest Hotfix Accumulators (HFAs). Retrieved February 29, 2008, Web site: http://www.checkpoint.com/downloads/latest/hfa/index.html