

PULP AND PAPER SOUTHERN AFRICA LIMITED (PTY) LTD IT SERVICE MANAGEMENT REPORT

REPORTING MONTH: FEBRUARY 2019

Prepared for Service Desk by:

Keeren Mansingh

Service Assurance Analyst

Contents

Executive summary.....	3
Report criteria.....	4
Exception Report.....	6
Problematic lines for the month – low availability.....	6
Bandwidth Utilisation – High Usage.....	6
Teraco Hosting.....	7
Enterprise security management.....	8
Ten recommended steps to help secure your Network.....	8
Service availability of the Firewall VM.....	8
Health overview.....	8
Summary of Network Security.....	9
Events, Incidents and Problem Management.....	12
Priority Matrix.....	12
Classification of events, incidents and problems logged.....	13
Service improvement.....	14
Fail-over testing.....	14
Action points.....	15
Conclusion.....	16
Annexure A: WAN Diagram.....	17

Executive summary

During the reporting month of February 2019, the Service Desk connect links and the Service Desk core infrastructure that forms part of the Pulp and Paper Southern Africa (Pty) Ltd WAN infrastructure was stable with no major incidents reported.




Fibre breaks and equipment faults were responsible for the reduced availability of the Venus and Helvetia sites.

We are pleased to report that the overall SLA was achieved for all core services.

Report criteria

The following criteria have been outlined in the service level agreement and forms the basis of the report.







Service	Description	Service Level – expectation	SLA met
MPLS – Primary	Availability for the month for each primary site	Availability: 99.8%	
MPLS – Secondary	Availability for the month for each primary site	Availability: 99 %	
Internet access	Download speeds to be measured and reported on	Bandwidth to reflect service billed with 0 discrepancies Availability: 99.95% RTT 33 ms Packet loss: 0.75%	
Hosting	Power	Availability: 100%	
Hosting	Datacentre availability	Availability: 99.999% RTT 35 ms Packet loss: 0.75%	
Firewall	Service availability of firewall devices	Uptime: 99.8%	
Incident management	Priority 1	98% of calls for the reporting month to be resolved within 4 business elapsed hours of the call being logged	
Incident management	Priority 2	98% of calls for the reporting month to be responded to within 4 business hours of the call being logged 98% of calls for the reporting month to be resolved within 8 business hours of the call being logged	

Service	Description	Service Level – expectation	SLA met
Incident management	Priority 3	<p>96% of calls for the reporting month to be responded to within 8 business hours of the call being logged</p> <p>96% of calls for the reporting month to be resolved within 24 business hours of the call being logged</p>	
Change management	All changes	90% of all changes must be successfully implemented the first time – during the reporting month	
Capacity management	Monitoring	Less than 1% of outages due to inadequate proactive monitoring – during the reporting month	

Exception Report

Problematic lines for the month – low availability

Refer to Annexure A for the WAN diagram

Site	Pulp and Paper Site Priority Status	Link Affected	SLA target	Availability	SLA met	Reason
Venus	Secondary	Single Link	99%	87.22%		Customer premises equipment , fibre break.
Helvetia	Secondary	Single Link	99%	86.21%		Link Flaps
High Flats	Secondary	Single Link	99%	87.09%		Link Flap
Driehoek	High Priority	Primary	99%	99.19%		
Ngodwana Mill	Business Critical	Primary	99%	99.99%		
Rosebank	Business Critical	Secondary	99%	92.23%		Fibre Break

Comments:

- On the 05/02/2019 there was an outage after a storm that affected all Mpumalanga sites. The root cause of the outage was due to a faulty 10GB port on a switch caused by the storm on the upstream provider's equipment.
- On the 25/02/2019 head office experienced a fibre break on their secondary link. The site was fully operational on the primary link. Overall SLA has been met.
- The height of the mast at the High Flats site needs to be increased to improve line of sight with the upstream provider's tower. Pulp and Paper is aware of this and arrangements are being made to increase the height of the mast.







Bandwidth Utilisation – High Usage

Comments:

- There have been no reported sites reaching maximum bandwidth thresholds for the month.

Teraco Hosting

Health overview

Service	Average Latency Target	Average Latency	SLA Met	Average Packet Loss Target	Average Packet loss	SLA Met
Check Point	33 ms	6.3 ms		0.75%	0.27%	
Teraco - DC6 - N12-15	33 ms	2.33 ms		0.75%	0.32%	
Teraco - Router	33 ms	1.08 ms		0.75%	0.21%	

Enterprise security management

Below are ten recommended steps to help secure your network. The steps provided below is not a complete list of actions, but a starting point with some of the most critical and proactive means to build on your internal IT security policy.

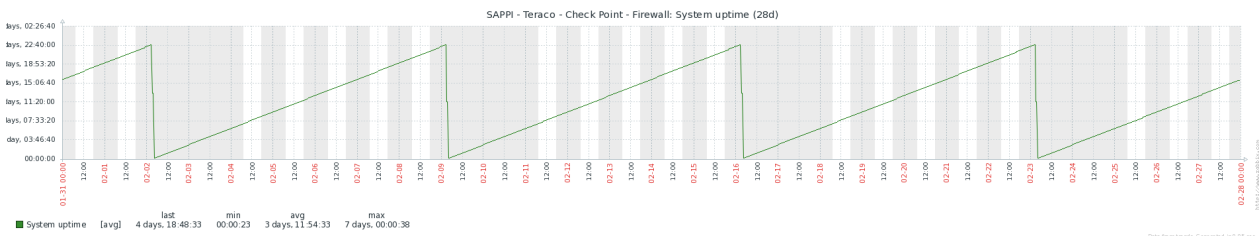
Ten recommended steps to help secure your Network

- 1) Inventory of authorised and unauthorised devices.
- 2) Inventory of authorised and unauthorised software.
- 3) Secure configurations for hardware and software
- 4) Controlled Use of administrative privileges.
- 5) Malware Defences
- 6) Limitation and control of network Ports and Secure configurations for network devices
- 7) Data recovery cabability
- 8) Wireless access control
- 9) Account monitoring and control
- 10) Incident response and management

Service availability of the Firewall VM

Service availability of firewall devices	Allowable downtime ranges between 6-7.5 hours per month, based on the number of days in a calendar month
--	--

Health overview



Period – 1 February (00:00) –28 February (23.59) 2019

Comments:

The Check Point VM is restarted weekly to clear reserved memory that isn't entirely released when connections expire.

Summary of Network Security

 **245** Critical Attack Types
Not prevented by policy

 **321** Infected Hosts
With bots



















Top applications/sites(top30)

Application / Site	Category	Risk Level	Sources	Traffic
Unauthenticated Sites	Custom Application/Site	3 Medium	7766 Sources	15.6TB
Whitelisted Sites	Custom Application/Site	3 Medium	8085 Sources	781.5GB
WhatsApp Messenger	Instant Messaging	2 Low	3765 Sources	644.8GB
Windows Update	Software Update	1 Very Low	5491 Sources	604.6GB
App Store	Search Engines / Portals	1 Very Low	858 Sources	400.5GB
Dropbox	File Storage and Sharing	4 High	568 Sources	162.2GB
Microsoft Office-update	Business / Economy	1 Very Low	357 Sources	34.6GB
Autodiscover	Email	1 Very Low	3942 Sources	24.8GB
Facebook-chat	Instant Messaging	2 Low	2310 Sources	23.9GB
WhatsApp Messenger-file transfer	Media Sharing	3 Medium	1725 Sources	20.8GB
Xbox Live	Games	2 Low	1086 Sources	12.3GB
Cornerstone	Business / Economy	2 Low	427 Sources	11.3GB
Spotify	Media Streams	2 Low	26 Sources	10.6GB
Microsoft Services	Web Services Provider	2 Low	3725 Sources	5.5GB
	Computers / Internet	2 Low	2162 Sources	3.2GB
Apple Software Update	Software Update	1 Very Low	1566 Sources	8.2GB
Microsoft Power BI-web	Business / Economy	2 Low	103 Sources	4.5GB
WhatsApp Messenger-web/PC	Instant Messaging	2 Low	288 Sources	4.0GB
Office365-Outlook-web	Email	1 Very Low	954 Sources	3.8GB
Giphy	Media Sharing	2 Low	146 Sources	3.3GB
Microsoft Store	Computers / Internet	2 Low	3837 Sources	3.2GB
rsync	Network Utilities	3 Medium	30 Sources	2.2GB
Office365-Delve	Business / Economy	2 Low	956 Sources	2.2GB
Facebook-file sharing	File Storage and Sharing	3 Medium	365 Sources	1.9GB
TED	Education	2 Low	30 Sources	1.5GB
Google Maps	Search Engines / Portals	2 Low	2725 Sources	1.3GB
Optimizely	Computers / Internet	2 Low	2436 Sources	1.0GB
Office365-Outlook	Email	1 Very Low	3143 Sources	876.4MB
WeTransfer-download	File Storage and Sharing	3 Medium	5 Sources	789.6MB

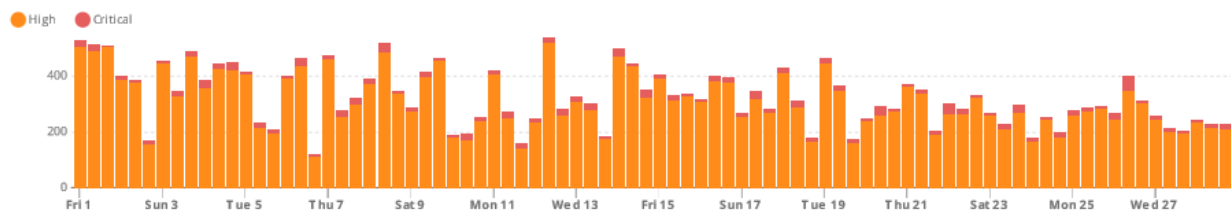
Cloud Based Web applications (top 20)

Application Name	Traffic Total Bytes
Dropbox	162.2GB
Cornerstone	11.3GB
Microsoft Power BI-web	4.5GB
Office365-Outlook-web	3.8GB
Office365-Outlook	876.4MB
Skype for Business (Lync)	50.8MB
SharePoint-online	48.2MB
LastPass	36.8MB
PingOne	9.7MB
Wunderlist	5.6MB
Microsoft OneDrive-web	5.5MB
FreshBooks	4.9MB
Freshdesk	2.4MB
Apple News	2.3MB
Reamaze	877.6KB
Amazon EC2	622.4KB
Dropbox paper	621.0KB
Google Apps	620.5KB
Office365	51.6KB
LivePerson	41.0KB
Total: 21 Applications	182.9GB

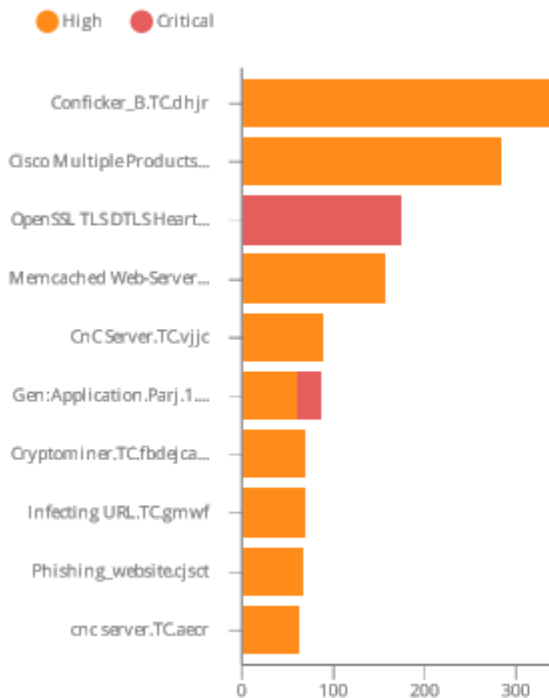
Top High Risk Applications (top 10 apps per category)

Application Category	Application Name	Source	Application Risk*	Traffic
File Storage and Sharing	Dropbox	 168.155.31.4  168.155.31.23  168.155.31.98  168.155.36.20  168.155.40.3 563 more Sources	 High	162.2GB
		Total: 1 Application	4 High	162.2GB
Browser Plugin	LastPass	 168.155.30.23  168.155.30.117  168.155.31.11  168.155.188.149  168-155-224-41.connect.za.sappi.com (168.155... 54 more Sources	 High	36.8MB
		Total: 1 Application	4 High	36.8MB
Anonymizer	UC browser	 168.155.251.129  192.168.8.122  192.168.8.147  192.168.8.152  192.168.8.157 7 more Sources	 Critical	1.7MB
		Total: 1 Application	5 Critical	1.7MB
Total: 3 Categories	3 Applications	624 Sources	5 Critical	162.3GB

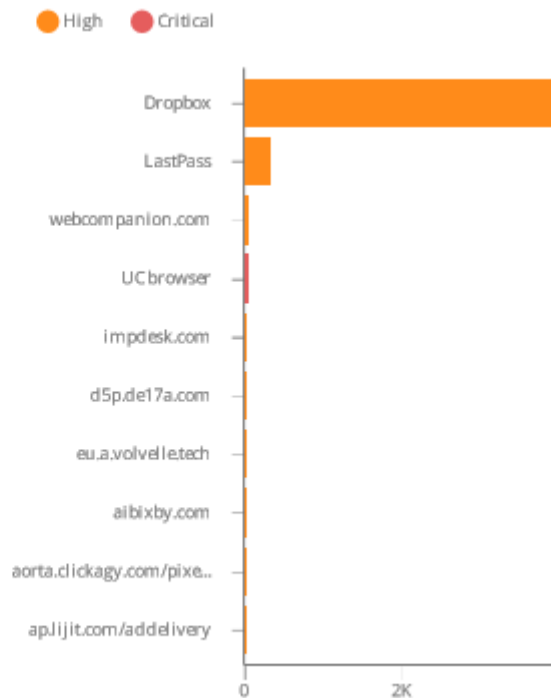
Top Security Incidents



Important Attacks Not Prevented



Allowed High Risk Applications



C

Comments:

The key findings above do not signify all current threats identified on the network, but instead represent a high-level view extracted from the comprehensive logs available from the Check Point Smart Console, at the time of compiling this report.

A drilled down view can be obtained by logging a ticket with our service desk or viewing the live logs found on the Check Point smart console. Service Desk can be consulted for further analysis of the finding, of this report and current live logs.

Recommendation

Enable query logging on Active Directory DNS servers and correlate these to Anti-Bot logs available via the Check Point firewall. The origin for these requests is presumed to be infected workstations with malware, which should be identified and cleaned.

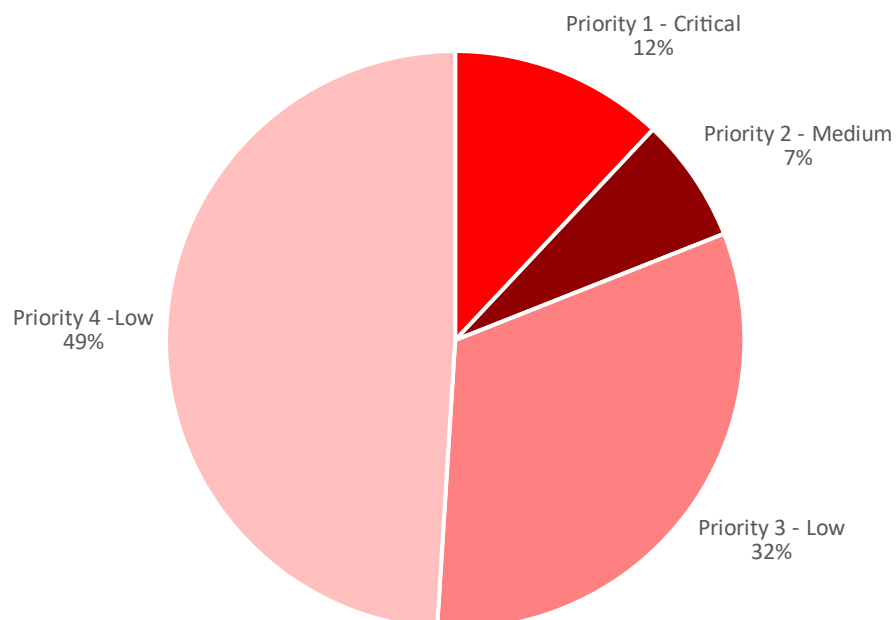
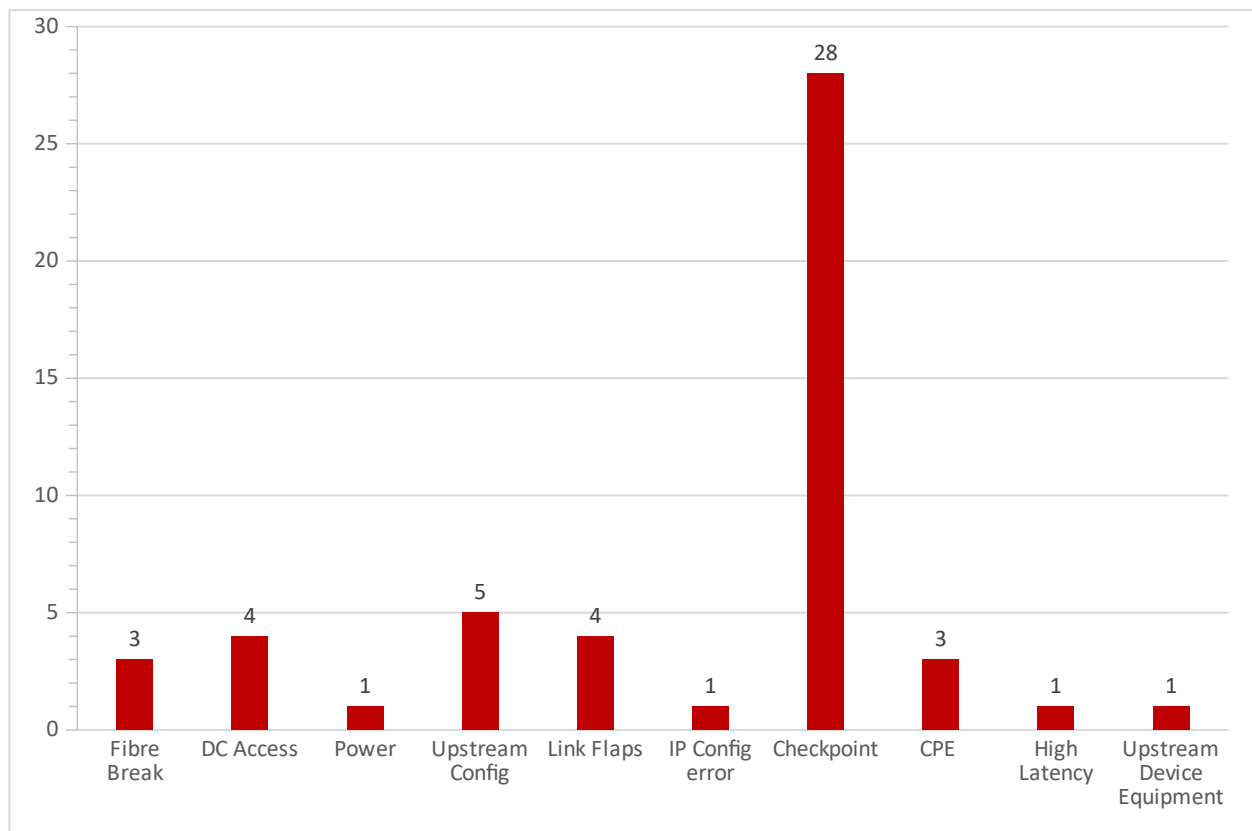
We would like to open a discussion into Pulp and Paper's strategy to mitigate these risks when they are highlighted in the forthcoming reports and notifications from Service Desk.

Events, Incidents and Problem Management

Priority Matrix

Service Desk Priority Matrix	Pulp and Paper Priority Matrix	Mean Time for Response (MTFR)		Mean Time to Restore (MTTR)		SLA Met
		Office Hours	After Hours	Office Hours	After Hours	
Priority 5 – Very High	Priority 1 – Negotiated	2 hours	4 hours	12 hours	16 hours	
Priority 4 – High	Priority 2– Medium/Normal	4 hours	8 hours	16 hours	20 hours	
Priority 3 – Medium/Normal	Priority 3 – Medium/Normal	6 hours		20 hours		
Priority 2– Medium/Normal	Priority 2– Medium/Normal	8 hours		24 hours		
Priority 1 – Negotiated	Priority 1 – Negotiated	12 hours		48 hours		

Classification of events, incidents and problems logged



Service improvement

Suggestions to improve the ticket logging process and the information provided has been submitted to Pulp and Paper. We now receive most logged tickets with their priority to the business, however there is still room for improvement and we are in contact with Pulp and Paper's IT team to expand on this initiative

Further discussions and correspondence to improve all aspects, regarding the logging process and the response of our service desk engineers is currently being monitored. Follow-up's on logged incidents with a phone call is a practise we making mandatory for agents to adhere to.

Service Desk is committed to the ongoing improvement of all our services and product offerings. We would, therefore, welcome and appreciate any feedback Pulp and Paper may have to make improvements to our services.

Fail-over testing

Fail-over testing at head office was conducted on the 08/03/2019. The fail-over testing for all three links was successful. The Technical Account Manager and the Network Operations team are liaising with the Service Manager and the Pulp and Paper help desk to arrange the next business critical site to be tested.

Action points

Task	Scope	Update	Status
1. Failover testing	Link Fail-over to be conducted periodically over the year with priority testing on the Critical and Priority Sites.	Fail-over test done on the 08/03/2019 for the head-office site was successful. Next site to be tested is to be confirmed by Barbara.	In Progress
2. ConnectWise portal access	Access to views of tickets logged with Service Desk	Draft process to implement is in the planning phase.	In Progress
3. Check Point Performance	Monitor performance over January/February 2019.	Follow-up on feedback from Pulp and Paper's IT Team.	In Progress
4. Change Management	The process to track and monitor Check Point change requests.	An initiative to align Service Management Services and Pulp and Paper's fault and incident logging process is in progress.	In Progress

Conclusion

In summary, the network infrastructure was stable with minimal downtime to core services.

Service Desk does not actively monitor and investigate threats entering your network from entry points outside of our direct control. Due to the sheer volume of reported incidents and resources required for this exercise, logged security events will require active investigation and reduction from your IT team. Service Desk is, however, available to consult with the team to improve security or provide support on incidents logged with our service desk via our standard support process.

Service Desk will endeavour to improve our service to achieve and exceed the required SLA, where we have fallen short.

On behalf of the Service Desk team, we like to thank Pulp and Paper for allowing us to be a significant component of their IT infrastructure. We look forward to working with you as a valuable client of Service Desk to improve service at all levels within our direct control.

Annexure A: WAN Diagram