Eskom	TENDER SCOPE OF WORK

Description of Request	Network Performance Monitoring - Adding of Smart Nodes to existing TAP Aggregation devices 1. Purchase of additional Smart Nodes to TAP Aggregation devices 2. Support Maintenance and Licensing 3. Commission of new Smart Nodes 4. Training of 5 people

1. High level background

Eskom needs and integrated system, instead of multiple legacy point products, simplifying operational workflows, speeding up incident management and issue resolution as well as reducing capex and opex costs.

The current TAP aggregation solution at Eskom allows for adding Smart Nodes that can perform advanced services such as full packet capture and analytics. Service Nodes can be introduced to the fabric for advanced packet handling, such as deduplication, packet slicing, packet masking, header stripping, regular expression matching and Netflow generation. The solution allows the adding of an Analytics Node to help security and network operations teams visualize traffic flows, identify root causes of outages, latency, or security issues. Recorder Nodes can also be included and integrated with the Analytics Node for full packet capture recording and replay.

By adding the about smart nodes will help Eskom to gain pervasive visibility into our network by creating a monitoring fabric that allows us to:

- Pre-process or filter the traffic for what Eskom tools are looking for, making them more accurate.
- Perform advanced services like deduplication and 1:1 Netflow generation, making Eskom tools more accurate and making them more cost effective by removing un-needed packets.
- Save a copy of the production network traffic flows to a network DVR (Recorder Node) for later replay.
- Use analytics for network troubleshooting, security incident response and security threat hunting.

By adding these Smart Nodes the TAP aggregation solution will help Eskom to eliminate silos of tools throughout the organization by delivering filtered network traffic to a centralized set of tools. This makes the observability of the Eskom network more accurate and more cost effective.

By adding the Analytics Node, will allow Eskom visibility, network troubleshooting, capacity planning, Machine Learning and Application Dependency Mapping. The Analytics Node need to provide a set of dashboards with visualizations that can be customized to fit Eskom needs. Thus, allowing ingest Netflow traffic directly from the production network.

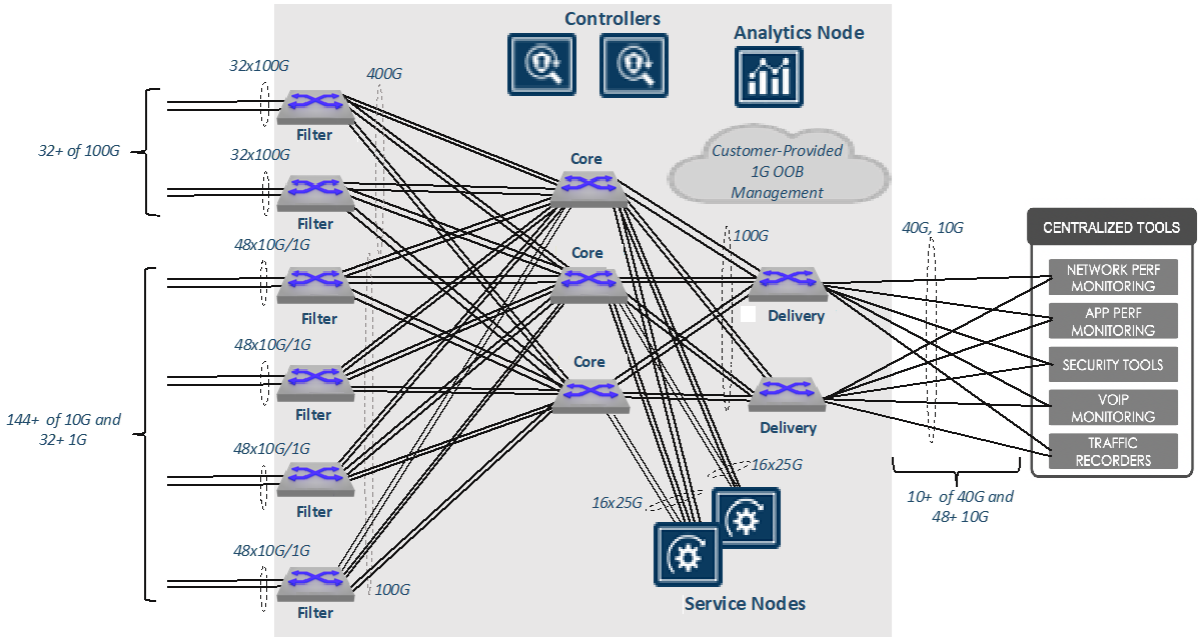
The Analytics Node will allow Eskom to learn what the network is doing:

- Visibility of the unknown should be identified and be easily visible.
- Get automatic alerts when anomalies are detected.
- Map the connections between applications on the Eskom network.

By adding the Recorder Node to perform full packet capture, query and replay. Queries can then use the index SSD to find the packets that we are interested in, and then the Recorder Node can reach into the packet storage to retrieve the packets. The Recorder Nodes to scale-out, the Controller can then search all RN's based on our query and return a single result. The Recorder Node should have the capability to support off-appliance storage by using methods such as NFS mount to other environments.

The proposed solution should provide a single pane of glass by adding the service node, analytics and recorder node. An example of a proposed architecture solution illustrated in the next figure 1.

Figure 1. Proposed smart nodes added to the existing 2-Tier that can grow to a 3-Tier TAP aggregator's deployment at Eskom



In this proposed architecture, the Controllers provide centralized management of the complete monitoring fabric, including the fabric switches and Smart Nodes.

- The Service Node provides advanced services including deduplication, packet slicing and more
- The Analytics Node provides flow and control plane visibility with enriched meta data
- The Filter fabric switches provide connectivity of tap/span ports from the production network

- The Delivery fabric switches provide connectivity to tools
- The Core fabric switches provide connectivity between Filter, Delivery and Smart Nodes

As needs grow over time, additional Filter fabric switches can be added to connect additional.

- 1/10/25/40/100G tap/span ports. Additional Delivery fabric switches can be added to connect more 1/10/25/40/100G interfaces to tools
- Additional Core fabric switches can be added to provide the backplane for the monitoring fabric
- Additional Service Nodes and Analytics Nodes can be added as capacity needs increase

Summary of Key Features required

Key features of the Monitoring Fabric include:

- Single pane of glass management via Controllers
  - Provides an easy-to-use network observatory using GUI or CLI
  - Eliminate box-by-box configuration and management

- Gain pervasive visibility
  - Any-to-any connection of tap/span ports to tools
  - Provide Monitoring as a Service
  - Filter traffic for what your tools are looking for
  - Perform advanced services like deduplication and 1:1 IPFIX generation
  - Capture full packets and replay with easy-to-use workflow
  - Gain visibility for network flows and control plane traffic

- Controllers
  - Auto-discovery of monitoring fabric components
  - Auto-provisions the entire path for forwarding traffic
  - Resiliency of paths

- Scale-out architecture
  - Current three TAP aggregators, which can grow to a 3-tier topology
  - Eliminate tool silos by delivering tap/span across multiple sites to a centralized tool set
  - Support for 1/10/25/40/50/100G connectivity for tap/span and tools
  - Support for multiple 400G links for monitoring fabric backplane

- Programmatic REST API
  - Dynamic configuration changes
  - Tool integration
  - Monitoring fabric automation

- Advanced services with optional Service Node
  - Multiple services per appliance with no additional licenses
  - Centrally managed by Controller
  - Deduplication

  - 1:1 Netflow generation
  - 1:1 IPFIX generation
  - Header strip, packet slice, pattern drop, pattern match, mask
  - TCP Analysis, timestamp, UDP replication

- Scale-out as needed by adding additional Service Nodes
  - Full packet capture and replay with optional Recorder Node
  - Hardware appliance with native 192TB packet and 7.6TB index storage
  - Scale-out as needed by adding additional Recorder Nodes
  - Get single result when querying across multiple Recorder Nodes
  - Centrally managed by Controller
  - Easy to use for query/replay
  - Integration with Analytics Node
  - Integration and automation with REST API

- Analytics with optional Analytics Node
  - Hardware appliance provides network visibility and flow collection
  - Network troubleshooting
  - Capacity planning
  - Security incident response
  - Security threat hunting
  - Access to Recorder Node full packets
  - Machine learning
  - Automatic alerting when anomalies are detected
  - Application Dependency Mapping
  - Integration and automation with REST API

2. Scope of work/Business requirements

2.1. Provide detailed description and volumes of the product/service requested:

The current TAP aggregation solution at Eskom allows for adding of Smart Nodes.

Scope of work will include:

The purchase of the following Smart Nodes
- Purchase of one (1) Service Node
- Purchase of one (1) Analytics Node
- Purchase of one (1) Recorder Node

Purchase of cables and SFP+
- 10GbaseCopper with SFP+, with a quantity of six (6)
- 25Gbe SFP 25, with a quantity of two (2)

Purchase OEM services to commission afterhours, the three new Smart Nodes at Megawatt Park and handover to Eskom.

2.2. Maintenance and Support:

The proposed solution should be covered by a 5 Year Maintenance and support contract, 24x7 OEM support with Next Business Day (NBD) hardware replacement.

2.3. Training/Transfer of skills: During handover, transfer of skills and knowledge on new equipment should be provided. OEM online training for 5-day training for five (5) Eskom staff personal on the proposed solution. (Monitoring specialist training – expert level)

3. Service Level Agreement requirements

- 24 x 7 x 365 SLA with the OEM basis with the following components.
  - Global Technical Assistance Centre (TAC)
  - OEM online resources
  - Worldwide hardware replacement
  - Hardware Replacement Next Business Day - Onsite installation for advance replacement hardware, performed by an onsite engineer for next business day
- Hardware support, receive proactive notifications about known hardware issues.
- The ability to log a call with the OEM and get 24 x 7 x 365 remote support.
- OEM online resources, to be able to access various resources online anytime. To include:
  - Software Downloads: Unlimited access to the software download section where you can obtain new software maintenance releases, as well as new feature releases
  - Notification Service: Proactive notifications for known software and hardware issues, including security vulnerabilities, allowing you to take action before encountering any known issues
  - Release Recommendations: Access to software release recommendations for help in picking the most appropriate software version for your environment.
  - Bug Portal Access: Access to the OEM Bug Portal for reviewing known caveats and associated details
  - Online Case Management: Customer Portal to create new cases, provide updates, and upload necessary files in a secure manner

4. Approvals:

End user / requestor:	**Name:**	Danie Kleinhans
	Designation:	Senior Advisor Infrastructure Operations
	Date:	17 March 2023
	Signature:	

Eskom	TENDER SCOPE OF WORK

Senior Manager:	**Name:**	Tebogo Makhwelo
	Designation:	Senior Manager IT Infrastructure
	Date:	27/06/2023
	Signature: