Automated WAN Solutions

Juniper Paragon Automation 2.0

Vijendra Singh,Reseller at Juniper Networks

JUNIPER NETWORKS | Driven by Experience™

Juniper Paragon Evolution & Offerings

Juniper Paragon

Cloud-Native
Open, DevOps

NEW

Paragon Automation (PA 2.0)

+ Use-case based
+ Easy button (UX/UI)
+ Intent-driven
+ AI/ML enabled
+ API First

2024

Paragon Planner  Paragon Pathfinder

Paragon Active Assurance  Paragon Insights

Paragon Applications (1.0)

+ Active Assurance
+ Closed loop
+ Cloud-native Applications

2020


Healthbot


Northstar

Standalone products
Industry best SDN Controller
Multi-vendor

2017

EXPERIENCE-FIRST NETWORKING

Juniper Paragon

Juniper Networks

Paragon Automation – FRS use case features

Juniper Paragon

1 Base Use-Case (mandatory)

Device Onboarding	Device Management	Observability	Trust
Guided onboarding workflow	Inventory management	Up to 71 KPIs monitored	Trust score
Infrastructure intent plan	Software management	Device KPIs	Compliance (CIS level 1 & 2)
Physical installation assistance	Configuration management	Interface KPIs	Vulnerability SIRT
Device profiles	Backup & Restore	Routing KPIs	Vulnerability Proactive Bug notifications
Interface profiles	License management	Graphing & Drill-in	Integrity Software EOL
Configuration of Device & Network	Alarm collection	Alerts	Integrity Hardware EOL
Assurance Trust, Active Assurance, Device health	Syslog collection	Notifications (webhook, email)	

S-PA-PLATFORM-S-1
S-PA-PLATFORM-S-3
S-PA-PLATFORM-S-5
S-PA-BASE-100-S-1
S-PA-BASE-100-S-3
S-PA-BASE-100-S-5
S-PA-BASE-400-S-1
S-PA-BASE-400-S-3
S-PA-BASE-400-S-5

Phase 1 SKUs Orderable NOW

3 USE CASES

#2 Active Assurance
#3 Service Orchestration

Active Assurance	Service Orchestration
Test & Monitors	*Customizable Service Designs*
Test Agents (list & drill-in)	*Customer Management*
Results (list and dril—in)	*Service Management*
Test Agent on ACX and as a Container	*Order Management*
RPM support	*Resource Management*
	L2, L3-VPN Model
	Assurance part of workflows

S-PA-ASSR-100-S-1
S-PA-ASSR-100-S-3
S-PA-ASSR-100-S-5

S-PA-ORCH-100-S-1
S-PA-ORCH-100-S-3
S-PA-ORCH-100-S-5

JUNIPER NETWORKS

Paragon Automation 2.0 BoM Example

Single use-case, both 100G & 400G bandwidth

Example:

Service Orchestration use case, 3-year term, 25x100G + 5x400G licensed bandwidth on network devices

SKU	Description	Unit Qty
S-PA-ORCH-100-S-3	Paragon Automation Service Orchestration Use Case: 100G BW - Subscription 3Y	25
S-PA-ORCH-400-S-3	Paragon Automation Service Orchestration Use Case: 400G BW - Subscription 3Y	5
S-PA-PLATFORM-S-3	Paragon Automation On Prem Platform license – Subscription 3Y	1
S-PA-BASE-100-S-3	Paragon Automation Base Use Case Package: Device Onboarding and management, Observability, Trust and compliance verification – 100G BW license - Subscription 3Y	25
S-PA-BASE-400-S-3	Paragon Automation Base Use Case Package: Device Onboarding and management, Observability, Trust and compliance verification – 400G BW license - Subscription 3Y	5

User input in configurator tool

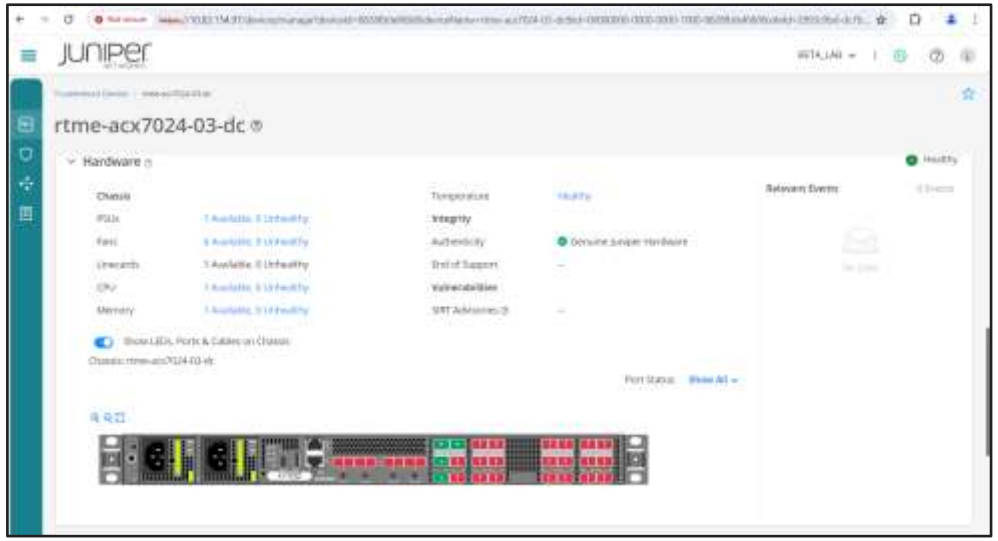
Matching Base and Platform SKU gets added automatically to BoM by configurator tool

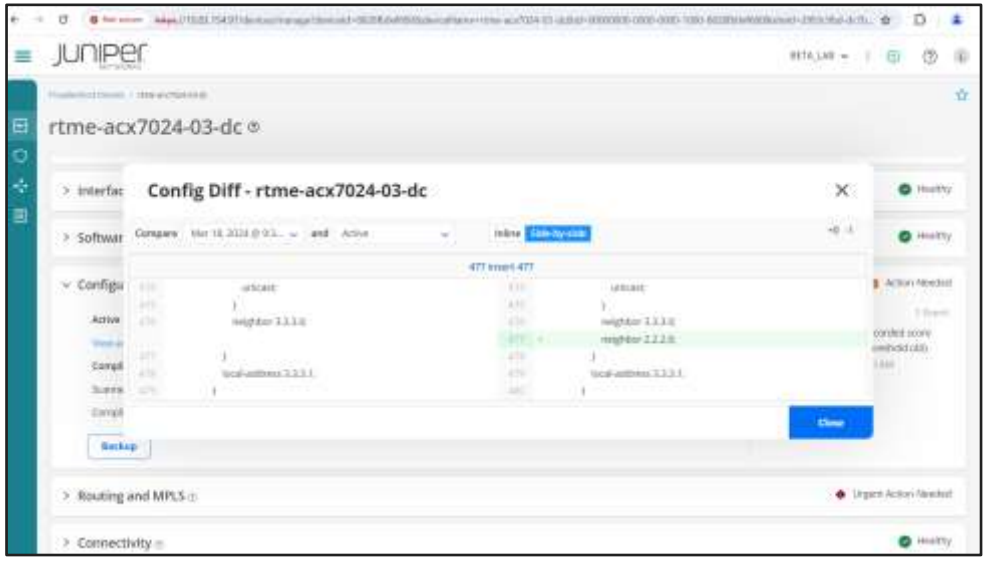
Network Observability

FRS

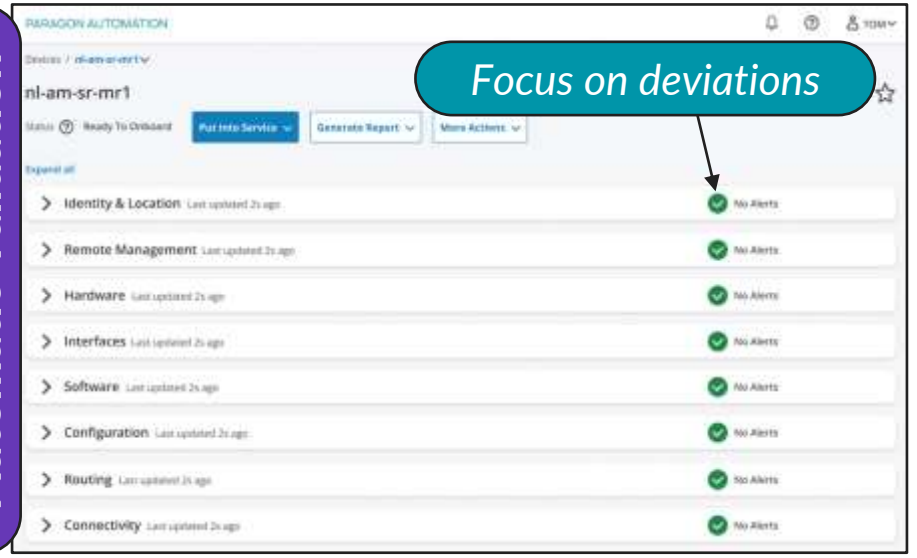
Observe various network KPIs based on Telemetry, Active Assurance, Topology.

- *CPU and memory utilization, fans, and PSUs*
- *Available physical interfaces, operational status, input and output traffic*
- *Information on the SIRT advisories*
- *Location, version, and compliance*
- *Device connectivity health and data*
- *Routing protocols, and health information related to BGP, OSPF, IS-IS, RSVP, LSP, and LDP neighbors*





Automatic Validation



JUNIPER NETWORKS

FRS

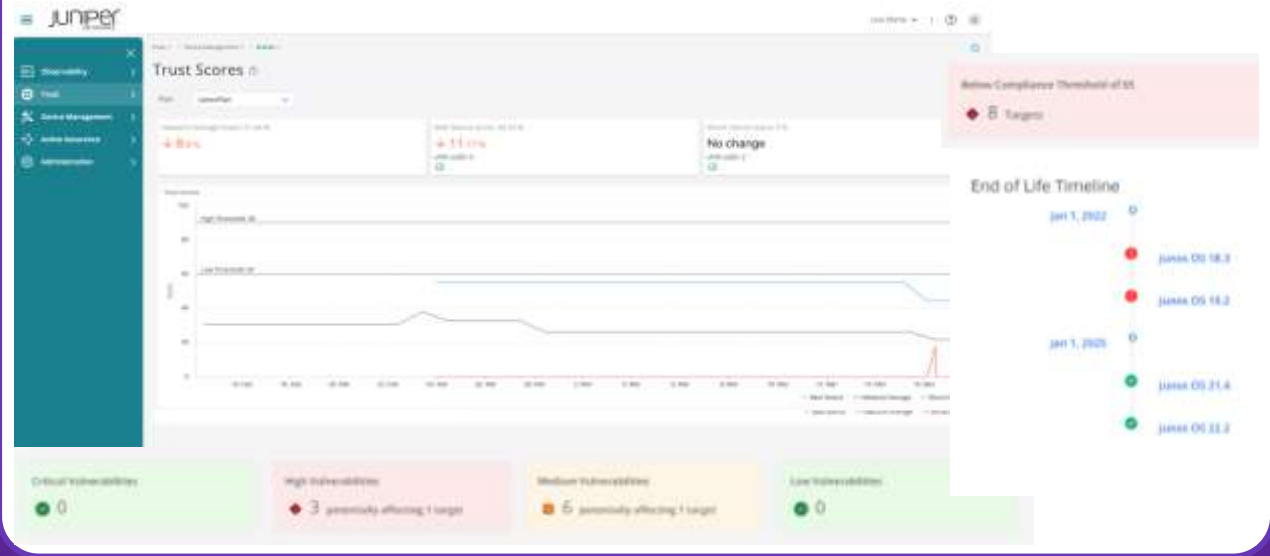
Trust and compliance

Confirm and quantify trust in the network.

PROBLEM

- *Difficult to ensure best practices for zero trust hardening of configuration compliance and integrity across the network.*
- *Cumbersome and effort intensive to track existing and new vulnerabilities and assessing network susceptibility.*
- *Complex to analyze and track EOL cycles on many different device types and software versions running in the network.*

Solution Snapshot



SOLUTION

- *Monitor network infrastructure to measure trust posture and level of risk of impairments.*
- *Enforce trustworthiness and compliance on a per-device basis through configuration hardening.*
- *Verify integrity of hardware, OS and software packages.*

Proven Benefits

- *Increased confidence in your network.*
- *Reduced risks of vulnerabilities.*
- *Reduced OPEX through automation.*

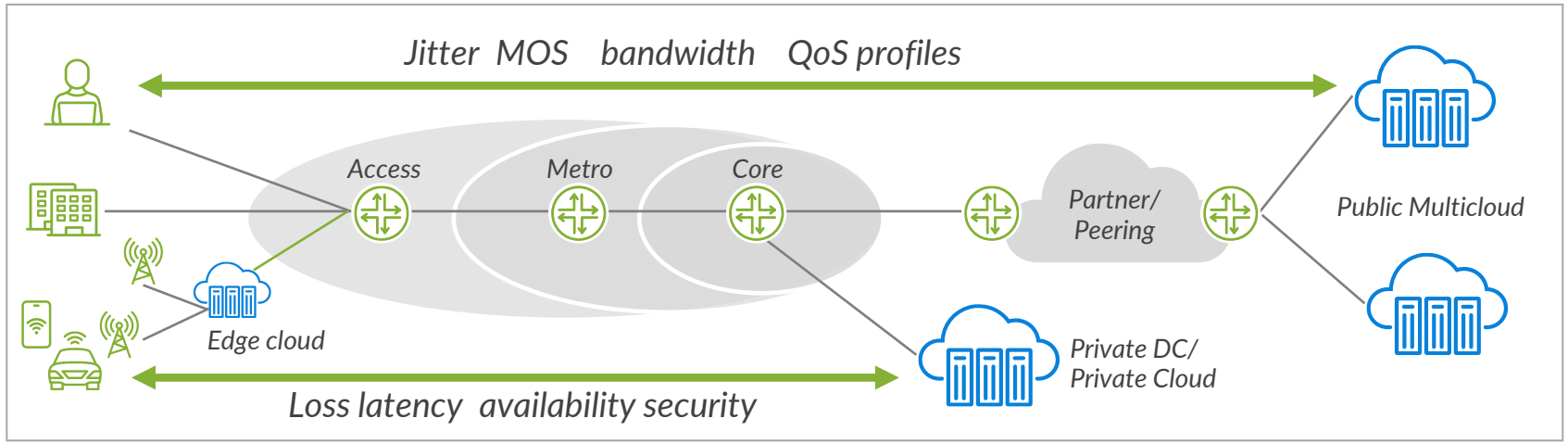
Why Paragon?

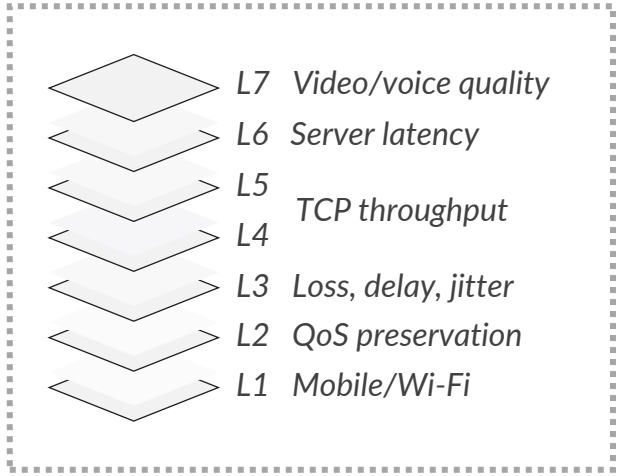
- *Verifies, attests and quantifies the trust aspects of the network, making it easier for network operations teams to run trustworthy networks.*

FRS

Active Assurance

Active data-plane measurements





- **Measure what matters, directly on the data plane.**
- **Generate synthetic traffic like an end-user.**

You cannot improve what you do not measure

JUNIPER NETWORKS

Service Orchestration

JUNIPER NETWORKS

Intent-based service orchestration

ORCHESTRATE

FRS

Automate provisioning of network services based on service intent.

PROBLEM

- *Operators need to differentiate on quality and make sure the network can guarantee service levels proposed to customers.*
- *Network services take weeks to roll out.*
- *Frequent CRUD operations results in stale configuration with no means to ensure config sanity.*

SOLUTION

- *End-to-end service provisioning driven by quality intent.*
- *Low-cost, simplified, automated model-based provisioning.*
- *Multi-vendor device mapping support with YANG-based standard interface.*
- *Built-in service quality testing with Active Assurance.*
- *Ensure config sanity during CRUD operations.*

Solution Snapshot

Built-in Service Models

L2 VPN

L3 VPN

Etc.

Proven Benefits

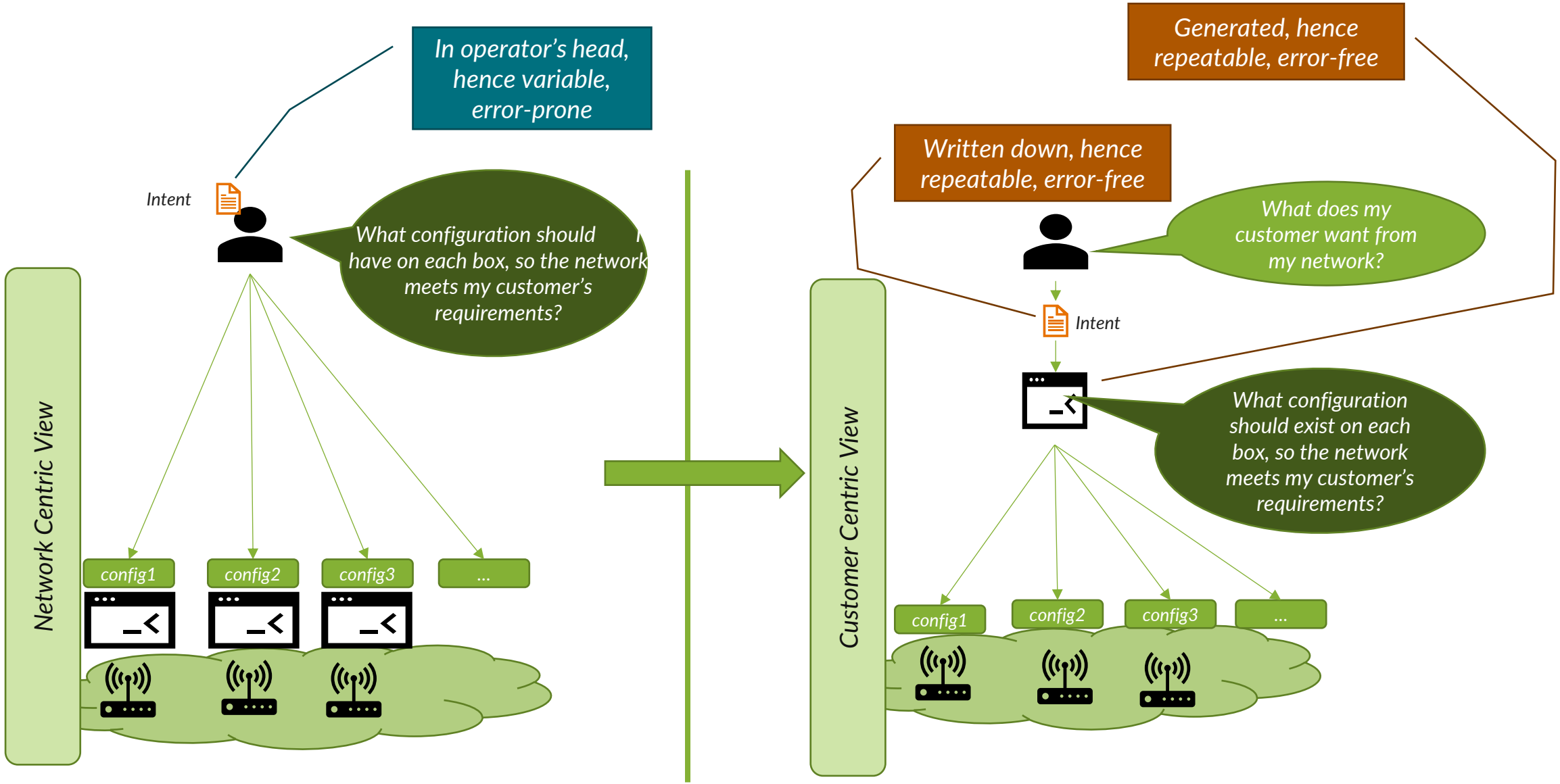
- *Accelerates time-to-revenue.*
- *Lowers OPEX by automating multiple config tasks.*
- *Provides network-level service visibility.*
- *Reduces failed service delivery rates.*

Why Paragon?

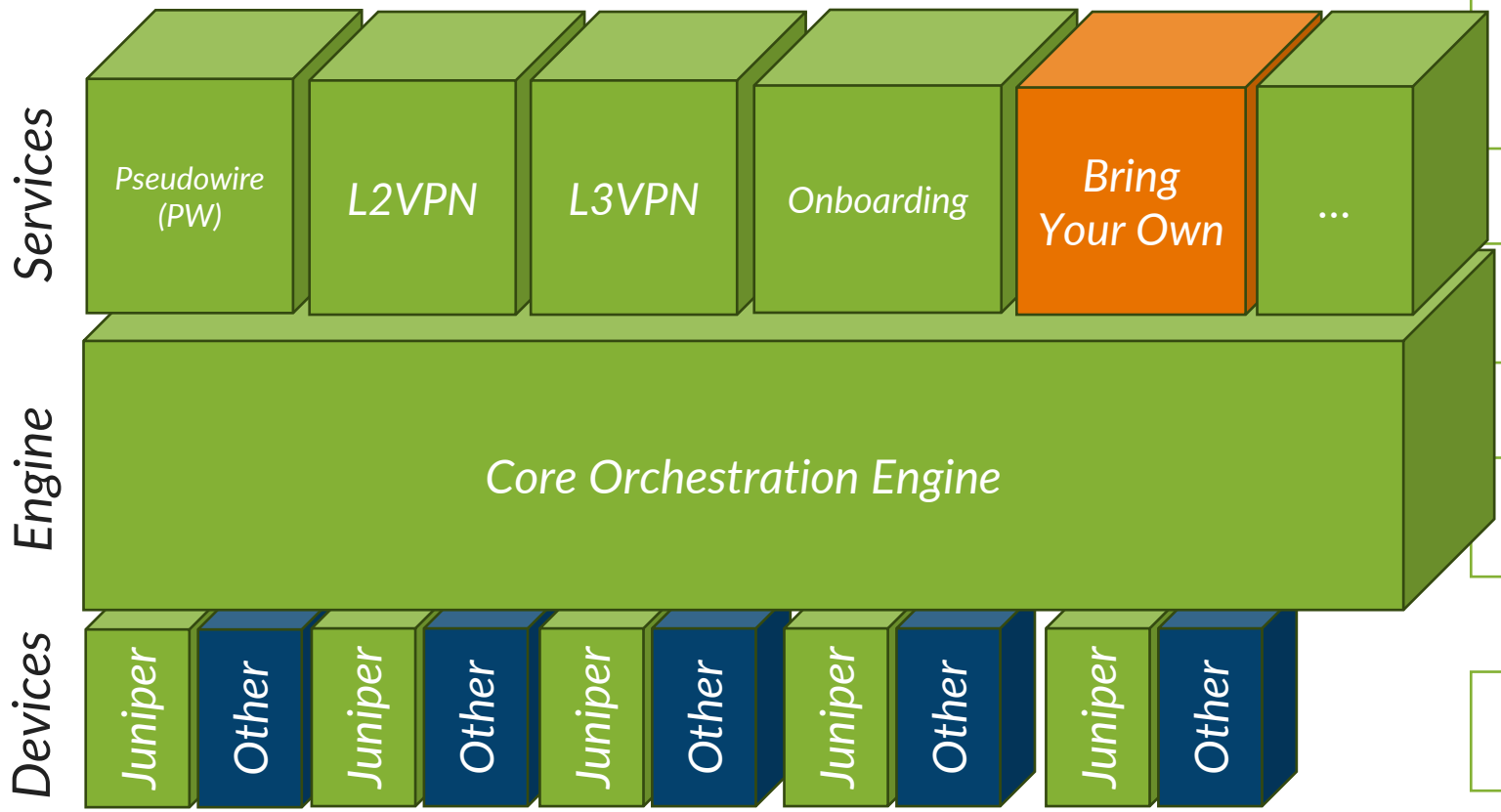
- *Enables YANG model-driven service provisioning within minutes.*
- *Provides the complete service lifecycle automation for multi-vendor infrastructure along w/ service compliance.*
- *One vendor for automated service activation and testing, with active testing and monitoring built-in.*

JUNIPER NETWORKS

Intent Based



Model Driven Architecture



- *Services are user-defined*
  - *Will ship with commonly used services that the user can **customize**.*
- *Services are developed using high level languages (YANG, JQ, Jinja, etc…)*
- *L3VPN was the first service developed*
- *Adding L2VPN & Onboarding services needed no change to the core engine*

Assurance KPIs L3VPN & L2VPN

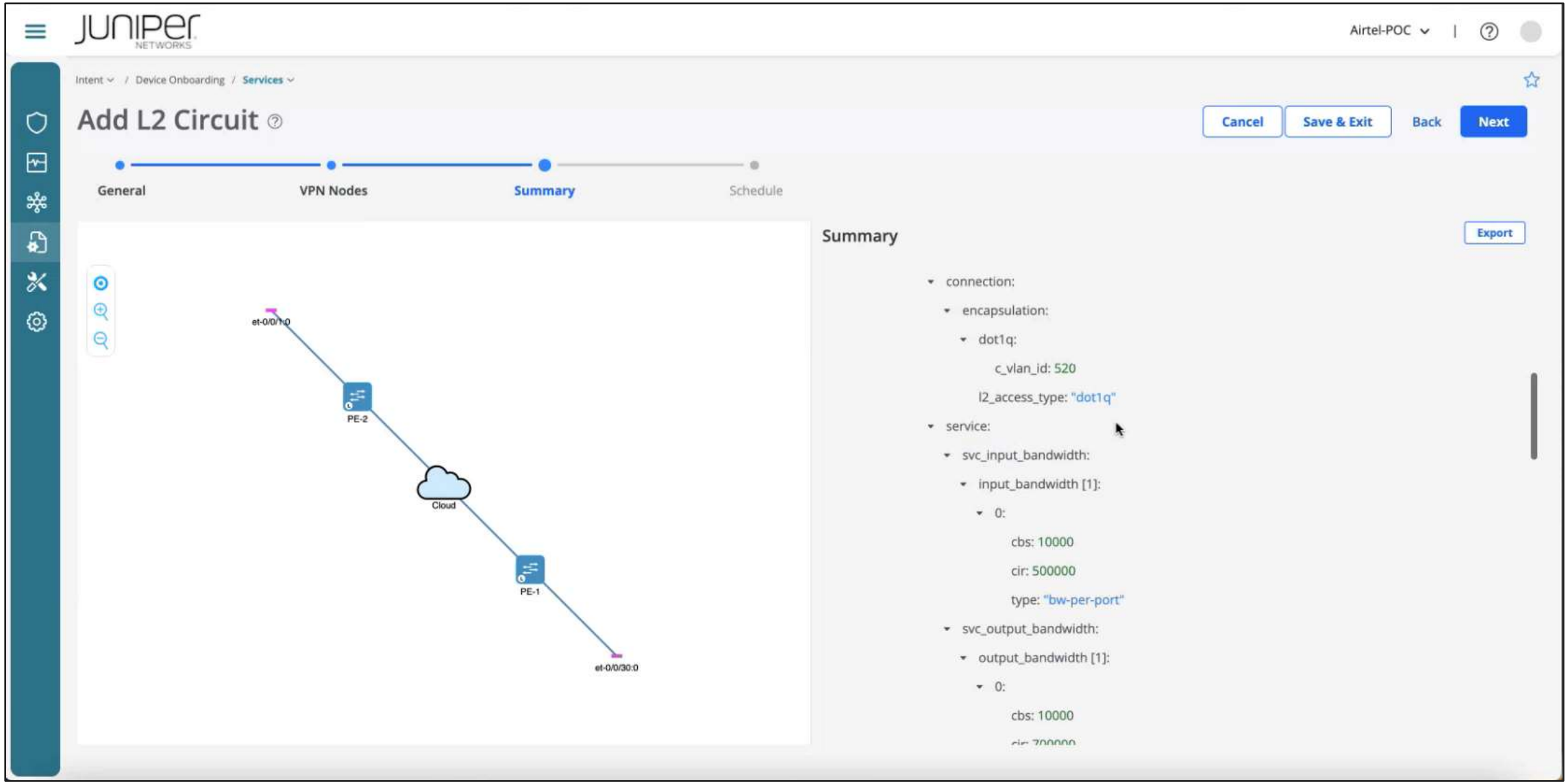
Day 1

L3VPN - Detail	Frequency
IFD - validate that all interfaces state(s) are as expected	60s
IFD - validate that the interface does not flap	60s
IFD - input errors	60s
IFD - output errors	60s
IFD - input traffic monitoring	60s
IFD - output traffic monitoring	60s
IFL - validate that all interfaces state(s) are as expected	60s
BGP - validate that all neighbour state(s) are as expected	60s
OSPF - validate that all ospf neighbour state(s) are as expected	60s
OSPF - detect that no ospf (extensive) flaps are occurring	60s
OSPF - validate that the expected number or OSPF nodes and adjacencies are visible, expected number should be “learned” based on the number of nodes and adjacencies over a learning period for a device that has been on-boarded for more than the learning period or from data from other similar devices in the same network for newly on-boarded devices. (if available) validate that there are no statistics that are unexpected (e.g., frame discards, frame errors, TLV discards & unknown TLVs)	60s
BFD - validate that all session state(s) are as expected	180s
L3VPN BGP - Network health status i.e. Links and neighbors sessions of service	65s
L3VPN OSPF - Network health status i.e. Links and neighbors sessions of service	65s
L3VPN Static - Network health status i.e. Links and neighbors sessions of service	65s

L2VPN - Detail	Frequency
IFD - validate that all interfaces state(s) are as expected	60s
IFD - validate that the interface does not flap	60s
IFD - input errors	60s
IFD - output errors	60s
IFD - input traffic monitoring	60s
IFD - output traffic monitoring	60s
IFL - validate that all interfaces state(s) are as expected	60s
LFM OAM - validate that no alarms related to links	180s
LLDP - validate that all neighbor state(s) are as expected	60s
Validate that all expected l2circuit connections are up	180s
Validate that all expected PWs are up	180s
L2Ckt - Network health status i.e. links, lfm, lldp and pw of a service/vpn	185s

L2 Circuit Overview

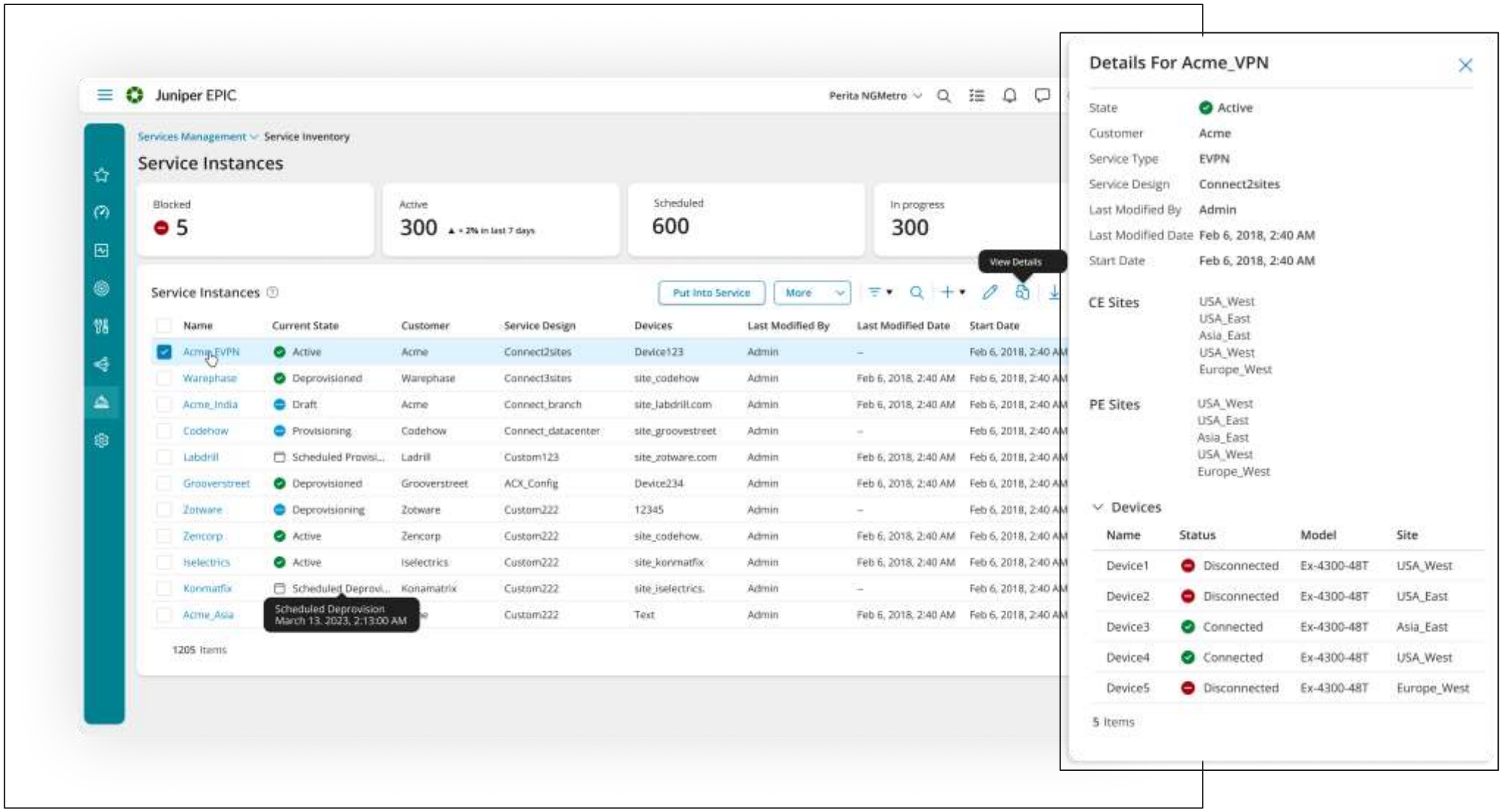
Day 1

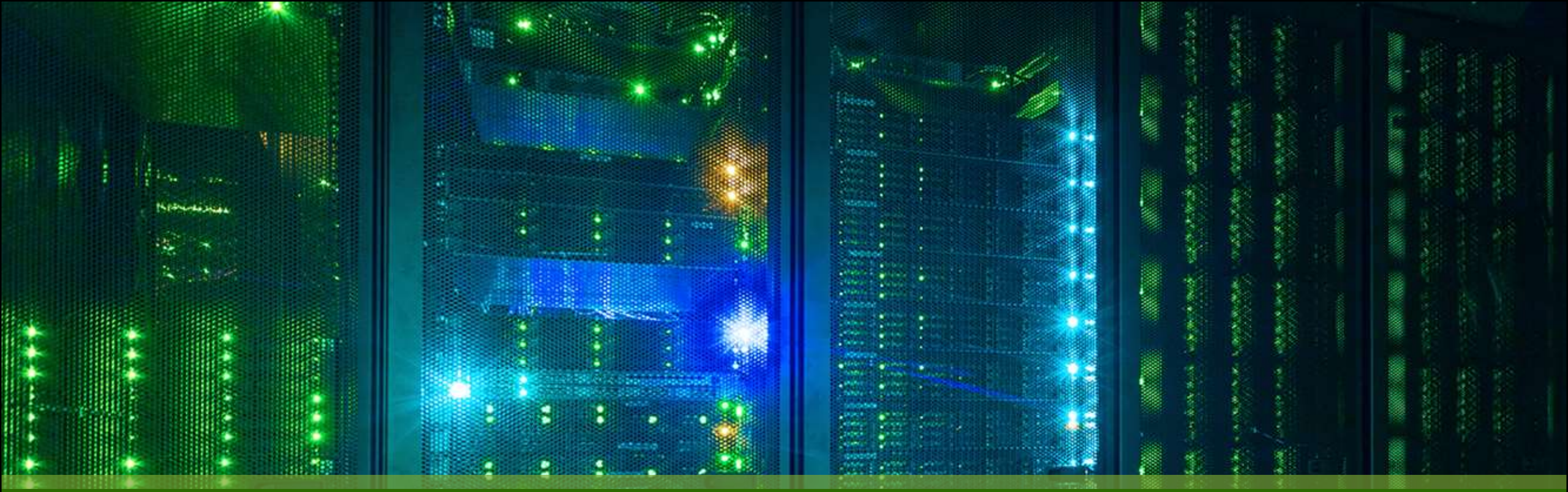


JUNIPER NETWORKS

Service Instances Inventory

Day 1





Thank you

JUNIPER NETWORKS