

# SECURE ENTERPRISE BRANCH SOLUTIONS WITH NFX AND AUTOMATION

Oliver Schuermann and Todd Walker

# LEGAL DISCLAIMER

This statement of direction sets forth Juniper Networks' current intention and is subject to change at any time without notice. No purchases are contingent upon Juniper Networks delivering any feature or functionality depicted in this presentation.

This presentation contains proprietary roadmap information and should not be discussed or shared without a signed non-disclosure agreement (NDA).

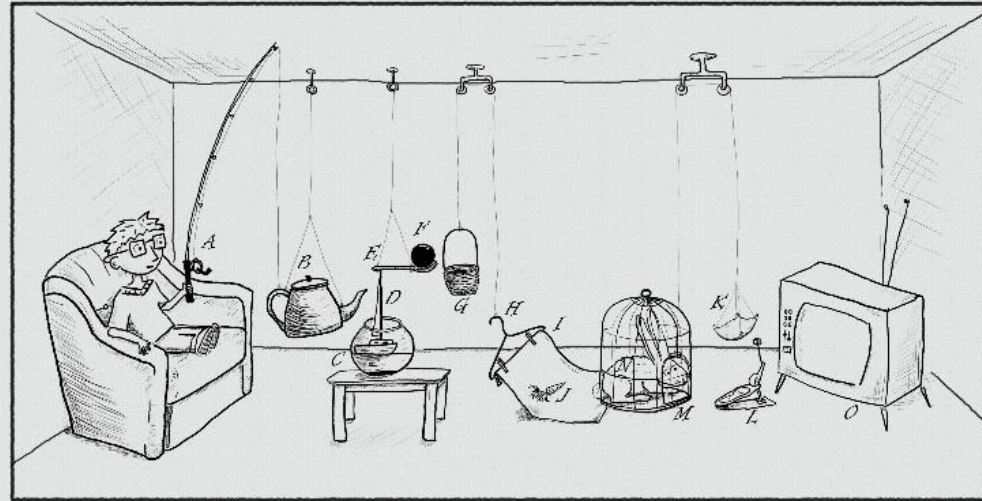
# TAKEAWAYS: WHAT YOU WILL GET WHILE YOU ARE HERE

- Evolution of Branch Architectures
- Intro to the NFX Platform
- Deployment Methods
- SD-WAN Market
- Management Integration
- NFX Deep Dive

# WE HAVE BEEN DEPLOYING BRANCHES FOR YEARS...

*Invention of the week - no. 55*

*The Remote Control*



Boy sitting on couch reels in fishing rod (A) causing kettle (B) to tilt and pour water into fish bowl (C). As water level rises, toy yacht (D) floats higher and tilts spoon (E) causing ball (F) to roll into basket (G). As basket drops to floor, coat hanger (H) rises making towel (I) stretch tight and baby carrot (J) is launched through the air. As carrot lands in napkin (K), it falls gently onto bass drum pedal (L) and causes door of rabbit cage (M) to open. Rabbit (N) comes out of cage to eat carrot and stops on bass drum pedal causing pedal to strike the power button on television (O) allowing boy to enjoy the show.

# BRANCH MARKET OVERVIEW

## Branches include Company-owned and Franchise locations such as:

- Banking, Insurance, Financial
- Retail and Restaurant Chains
- Medical Offices
- Education
- Satellite Campuses
- Others

## Complexities on the Rise

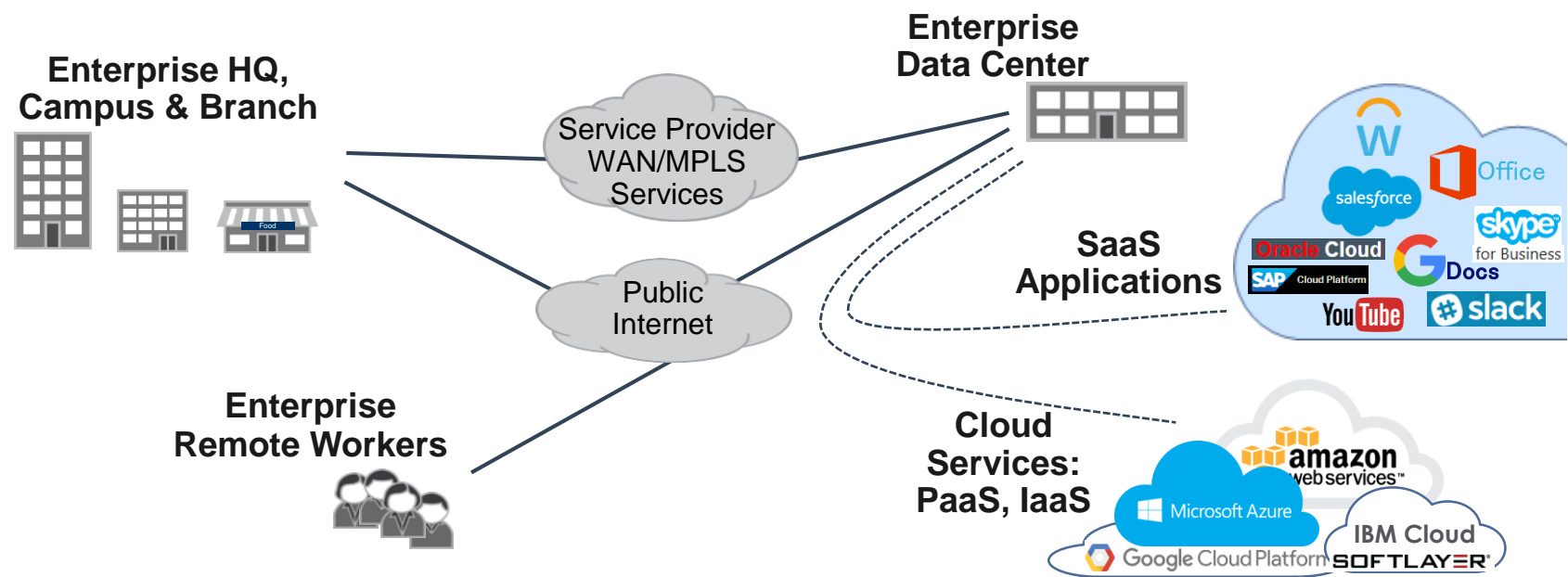
- Improve Application Performance
- Increase Security
- Onsite Partner Services / Kiosks
- Systems Dependent on Bandwidth
- Continue to reduce costs



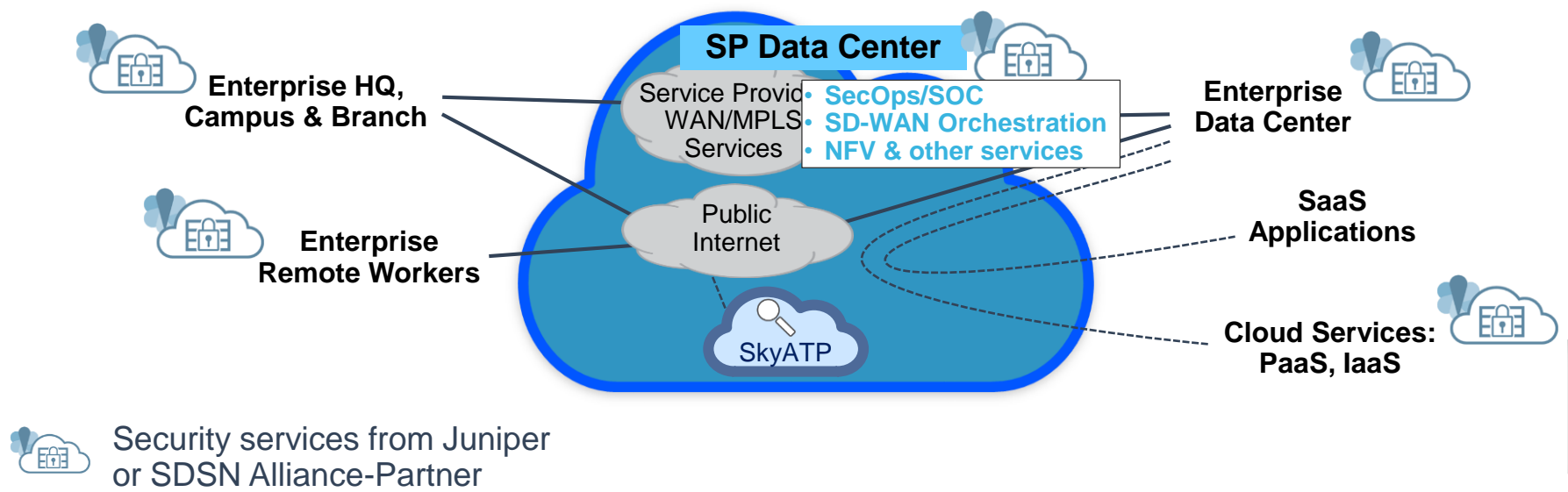
## Technology Drivers (High-Level)

- Consolidation of Services
- Reduce Number of Branch Touches
- Platform Longevity
- Cheaper Bandwidth
- Security

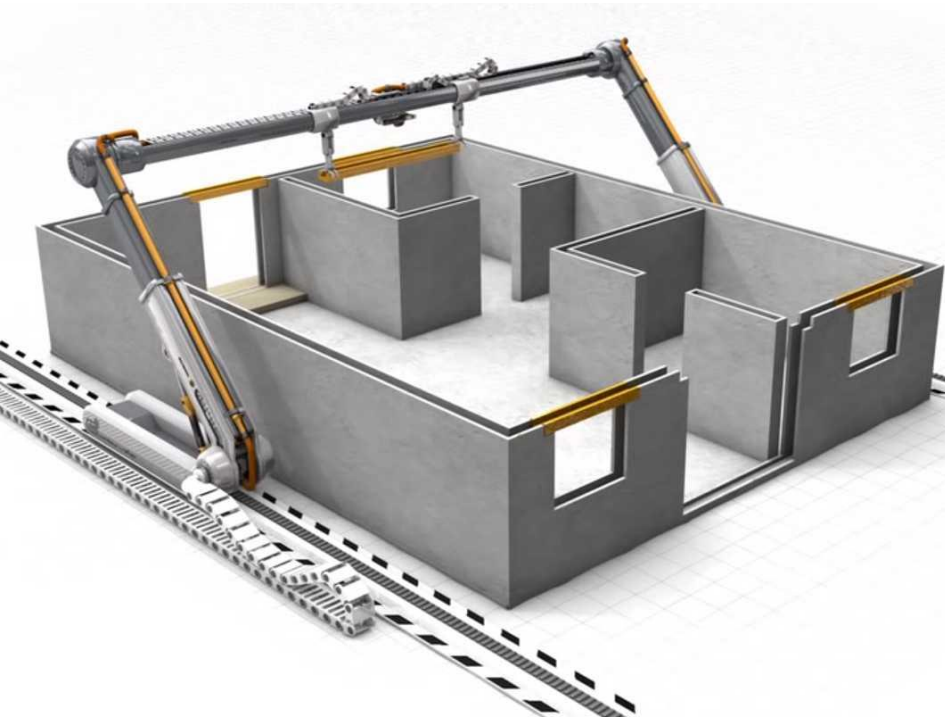
# ENTERPRISE ARCHITECTURE – OVERVIEW



# MSSP: MANAGED SECURITY, SECURE SD-WAN SERVICES



# CREATING VALUE BY INTEGRATED SETUPS



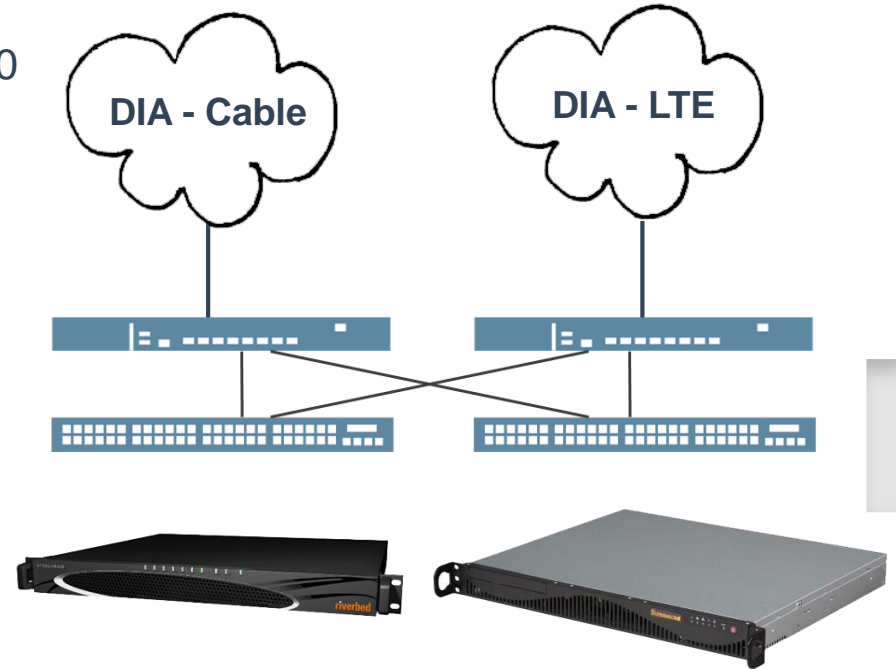
- Deploying more than just CPE
- Integration with other IT systems
- Creating longevity
- Service consolidation
- Reducing or eliminating truck rolls
- Reduction in Circuit costs (SD-WAN)
- Cloud Managed



# ADDRESSING BRANCH CHALLENGES THE OLD WAY

## Issues:

- 👉 Each Truck Roll costs \$700 Domestic & \$2100 International
- 👍 WAN Acceleration reduces Circuit costs (Primarily Internationally)
- 👍 Need to have addition function to PXE boot Registers
- 👎 Cloud based management
- 👍 DevOps Deployments



# CHANGING THE GAME IN THE BRANCH

## Deploying more than just CPE – Large Retail Example

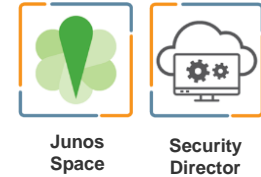
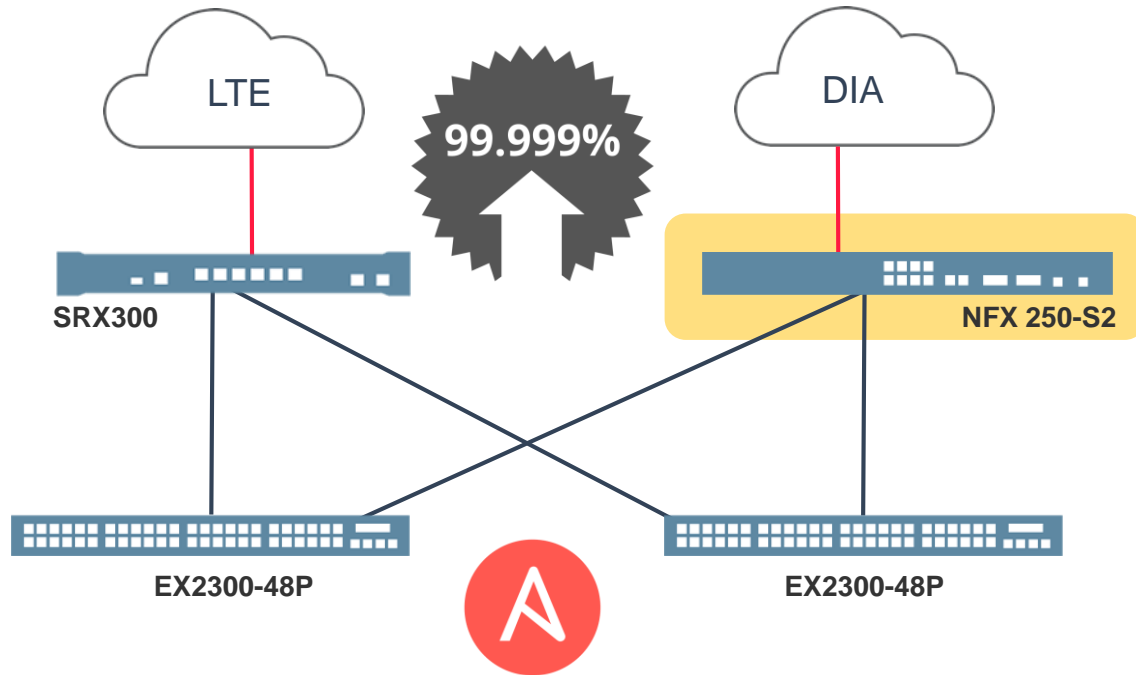
### Issues:

- 👍 Each Truck Roll costs \$700 Domestic & \$2100 International
- 👍 WAN Acceleration reduces Circuit costs (Primarily Internationally)
- 👍 Need to have addition function to PXE boot Registers
- 👍 Cloud based management
- 👍 DevOps Deployments



# CHANGING THE GAME IN THE BRANCH

Deploying more than just CPE – Large Retail Example



# REDUCING OR ELIMINATING TRUCK ROLLS

Some customers indifferent about initial deployment

~~ZTP (PXE Boot) Relies on DHCP~~

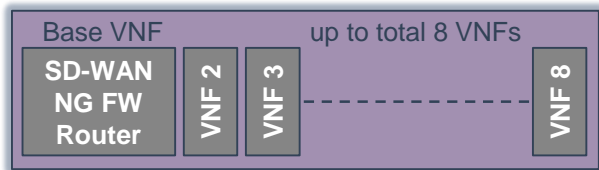
~~USB Boot?~~



# REDUCTION IN CIRCUIT COSTS (SD-WAN)

## Enterprise SD-WAN

### NFX



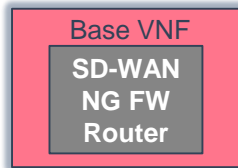
- **Up to total 8 VNFs**
- Multi-vendor VNF support
- Base VNF includes 3 equivalent VNFs & license options:
  - SD-WAN
  - NG FW
  - Router
- Pricing bundles for additional VNFs
- Provides most Value & Capability

Sell at a Premium

Full  
Capability

## Quick-Start SD-WAN

### Branch SRX



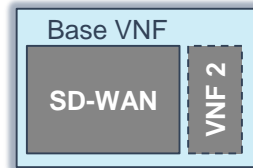
- **Supports 3 equivalent VNFs**
- Base VNF includes 3 license options
- Quick-Start Low-Cost PAYG
- SD-WAN entry point
- Zero-Touch Provisioning option
- Option to deploy with NFXs
- Lowest cost option
- Std SRX price structure
- SD-WAN license per device

Competitive Pricing

Low-Cost  
Quick-Start

## Competitors

### Basic vCPE



- **One or Two VNFs**
- No multi-vendor VNF support
- Base VNF supports SD-WAN only
- Still requires additional CPE to support minimum functions:
  - NG FW
  - Router / Switch
- Multiple Network managers

Additional Costs & Complexity

Hidden  
Costs

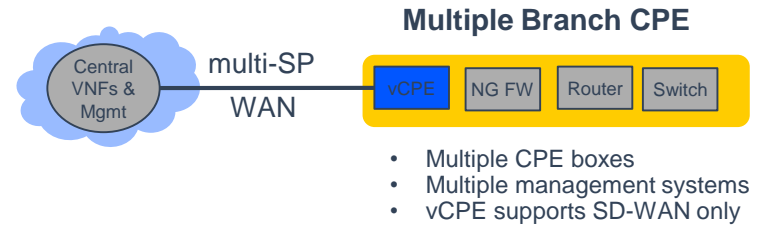
# JUNIPER VS COMPETITORS

## Quick Start SRX vs vCPE + Central VNFs

### Typical Competitor Solution

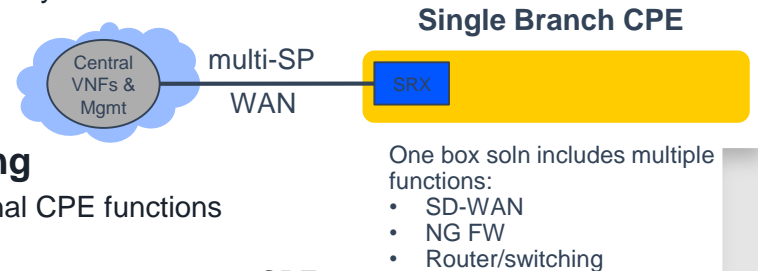
Vendors include: VeloCloud, Versa, Viptela (Cisco), Meraki (Cisco)

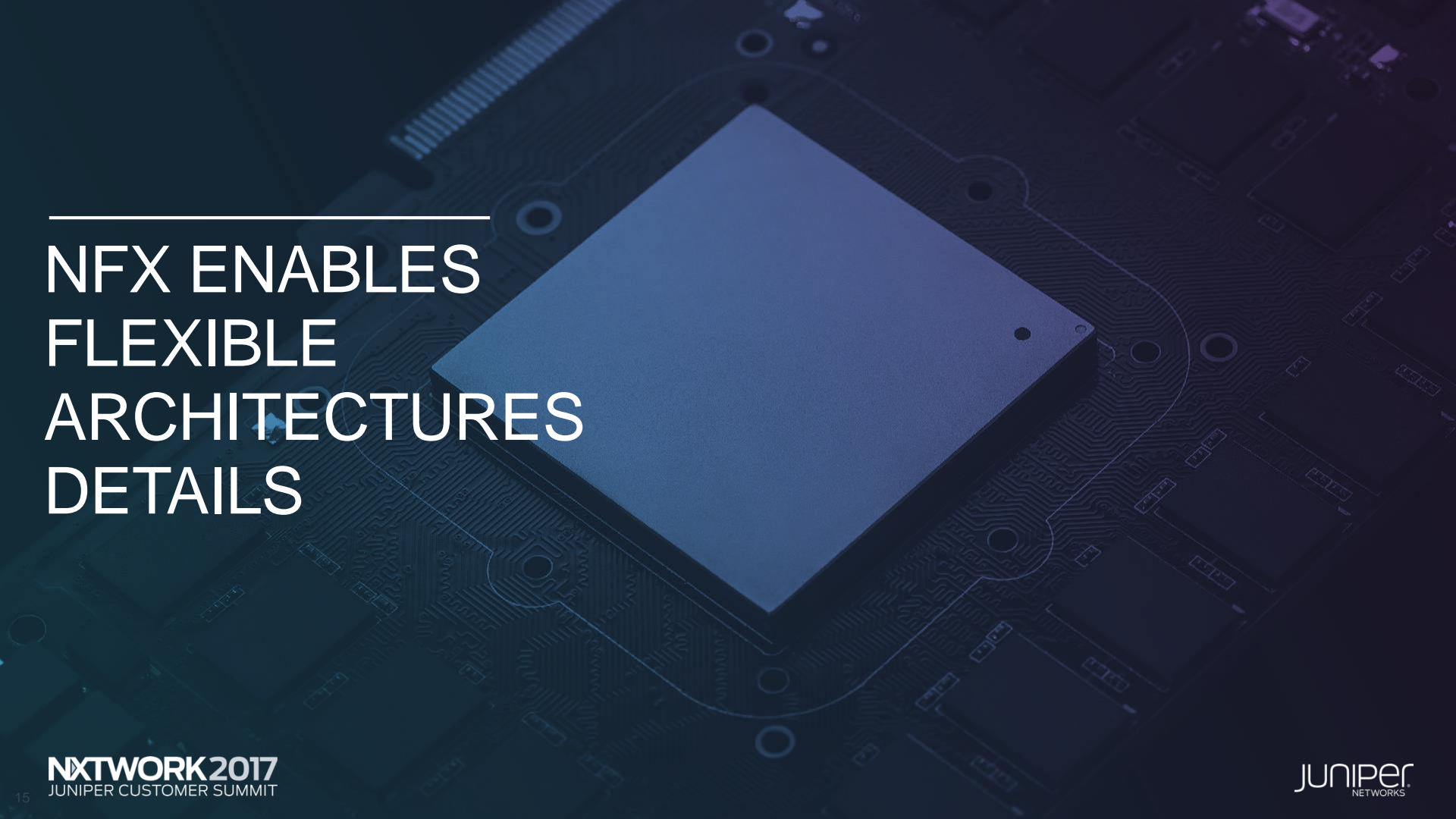
- Offer low-cost (<US\$500) virtual CPE with minimum functions – typically SD-WAN only
- VNF's are located in cloud
- Adds an additional CPE box at branch, and does not replace existing firewalls and routers
- Does not support advanced routing options such as BGP – often preferred by customers
- Does not integrate the management of all branch-located CPE devices
- vCPE does not support multi-vendor VNFs



### Juniper Solution – sell additional value for similar pricing

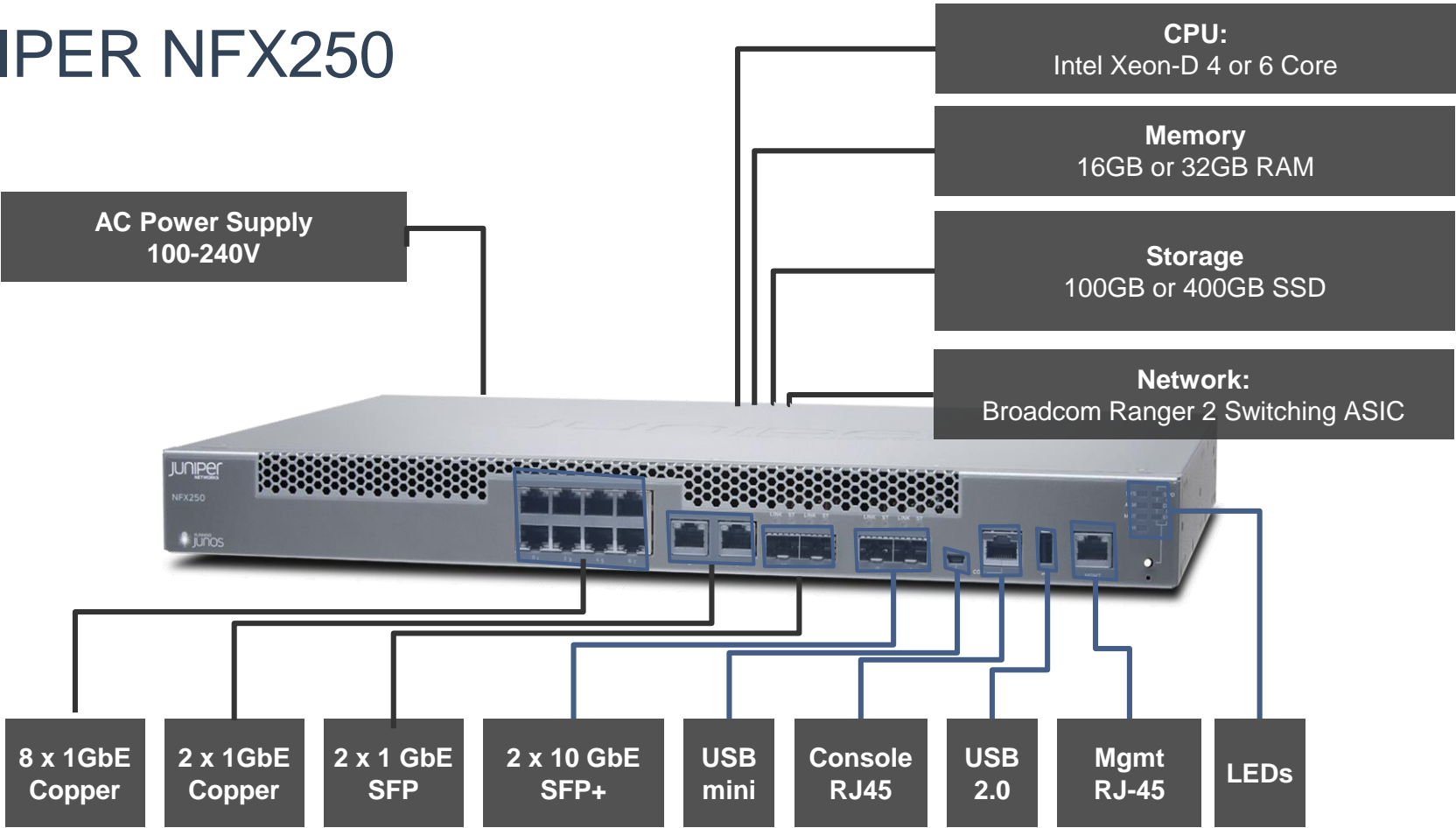
- Juniper Quick-Start SRX option provides similar price-points with additional CPE functions including: NG FW and Router and BGP options
- Provides a one box solution & can replace existing CPE with integrated management across CPE functions.
- Retains benefit of additional VNF flexibility by supporting centralized cloud VNFs
- Allows introduction of NFX and mix/match of SRX/NFX depending on branch requirements
- Allows re-use of existing SRX deployments and avoids wholesale WAN changes
- Subscription option can replicate virtual CPE & cloud vendor solutions – if needed





# NFX ENABLES FLEXIBLE ARCHITECTURES DETAILS

# JUNIPER NFX250





# NFX250 – A HIGH LEVEL

## Linux Server

- KVM Hypervisor
- Wind River Linux
- Junos Device Manager

## Ethernet Switch

- Ranger-2 ASIC (Same ASIC as EX2300)
- 2x10G + 12x1G
- Junos (QFX like)

## Internal Server Interconnection

- 2 x 10G Links





# KEY COMPONENTS

## Junos Device Manager (JDM)

- A Junos like CLI on top of Wind River Linux
- Implemented in container
- Configurations converted to Linux commands and pushed down

## Junos Control Plane (JCP)

- True Junos (BSD)
- Manages switching ASIC and front panel ports

## vSRX

- Not required but usually implemented

# WHY THIS MATTERS

Convergence of enterprise grade switching, server grade compute and leading virtualization technologies

Provides flexibility for customer

- May have Juniper logo on outside but can be anything inside
- Can add/delete/swap VNF vendors relatively easily (compared to truck rolls)
- Device consolidation

Think outside the of the network

- Most retail / small branch have a local server infrastructure
- Build business cases on total consolidation of all services

# WHAT YOU NEED TO KNOW

The NFX does not run:

- Contrail vRouter
- OpenStack
- Containers (although Docker is installed and used for system services)

## Juniper VNFs

- vSRX - tested and supported
- vRR - tested and supported
- vMX - Work underway to get an MX image that will run on NFX



# IMPORTANT SERVER

Memory Huge Pages  
CPU Allocation  
Networking Options

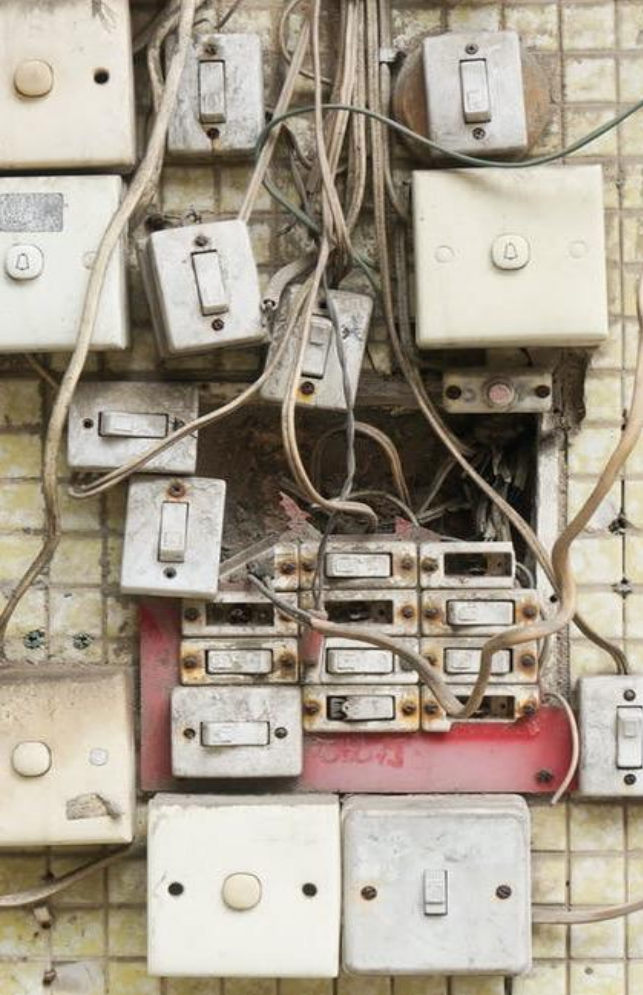
# MEMORY - HUGE PAGES

- Memory is fragmented in pages similar to sectors on disks
- Default page size 4KB in Linux
- For 32GB system this yields 8M pages
- Smaller pages yields better memory utilization but more fragmentation (and more memory burned for page table maintenance)
- Pages can be fragmented and swapped to disk as needed
- Huge pages allocates larger chunks of memory. On NFX either 2M or 1G are available
- With new versions of DPDK, 1G page size is required
- When assigning to a VM, can specify that the pages cannot be swapped

# CPU PINNING

- Linux has a sophisticated scheduler that schedules thread to run on available CPU cores
- Normally this is desirable but with low latency VNFs, switching cores can add jitter
- To avoid switching cores, VMs can be pinned to specific cores
- Most server grade CPUs from Intel support hyper-threading which allocates two virtual CPUs per physical core
- CPU layout can be obtained in multiple ways but at the hypervisor shell: 'virsh capabilities' provides easily consumable information (in XML)





# VM NETWORK INTERFACES

## Para-virtualized driver (Virtio)

- Widely deployed, supported in NFX250
- Excellent compatibility
- Decent performance

## SR-IOV

- Fairly widely deployed, supported in NFX250
- Best performance as the VM directly drives a slice of the hardware
- VM must have drivers to support physical hardware



# EXAMPLE CONFIG – STARTING AN SRX

## Starting a VNF via CLI

```
set virtual-network-functions vsrx image /var/third-party/images/vsrx.qcow2
set virtual-network-functions vsrx memory size 4194304
set virtual-network-functions vsrx memory features hugepages page-size 1024
set virtual-network-functions vsrx virtual-cpu 0 physical-cpu 5
set virtual-network-functions vsrx virtual-cpu 1 physical-cpu 11
set virtual-network-functions vsrx virtual-cpu count 2
set virtual-network-functions vsrx virtual-cpu features hardware-virtualization
set virtual-network-functions vsrx interfaces eth2 mapping hsxe0 virtual-function
set virtual-network-functions vsrx interfaces eth3 mapping hsxe1 virtual-function
set virtual-network-functions vsrx interfaces eth4 mapping vlan mode access
set virtual-network-functions vsrx interfaces eth4 mapping vlan members Transit-
LAN
```

# INIT-DESCRIPTOR

If the JDM CLI doesn't provide all of the functionality needed to start a VM, you can use a libvirt XML definition document

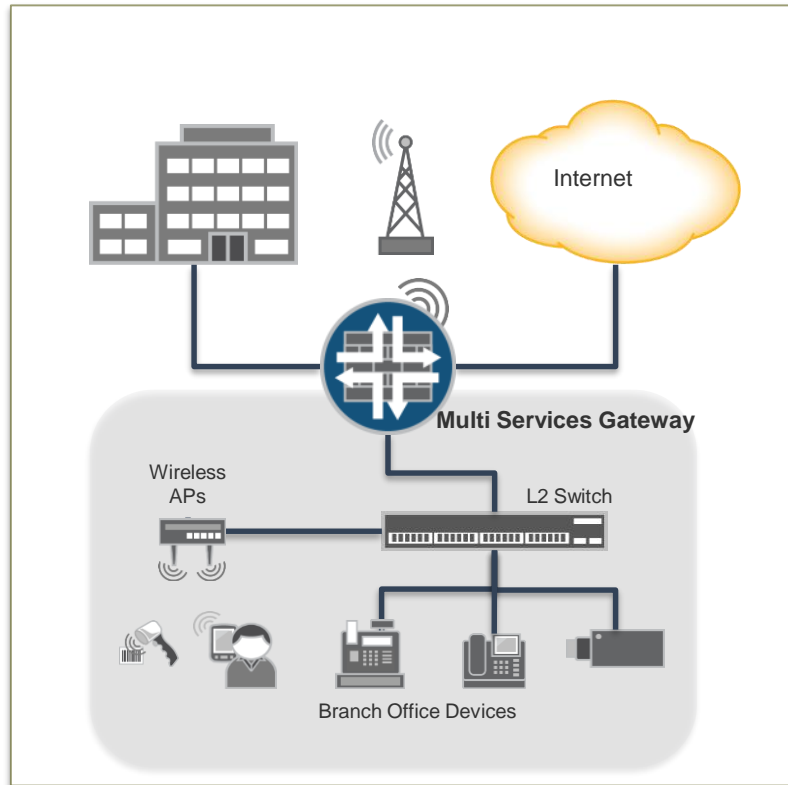
Reasons you might want to do this:

- Need to have more specific control of networking (disable TCP optimization)
- Might need to configure devices JDM doesn't expose
- Docs at: <https://libvirt.org/formatdomain.html>

CLI:

```
set virtual-network-functions suse init-descriptor /var/third-party/images/suse.xml
```

# BRANCH SECURITY



- Firewall (PCI, Non-PCI, etc.)
- Advanced Security Services
- IPsec
- Advanced routing
- Local Internet breakout
- Guest wireless

Solution: Implement SRX as a VNF

# BRANCH/WAN DISRUPTION AND TRANSFORMATION

## User Experience



On-Demand  
Self Service



Visibility  
and Control



Open,  
Flexible Choice

## Cloud/Connectivity



Application  
Aware WAN



Hybrid WAN  
Flexibility



Centralized  
Policy Control

## Business



Reduced  
Capex/Opex

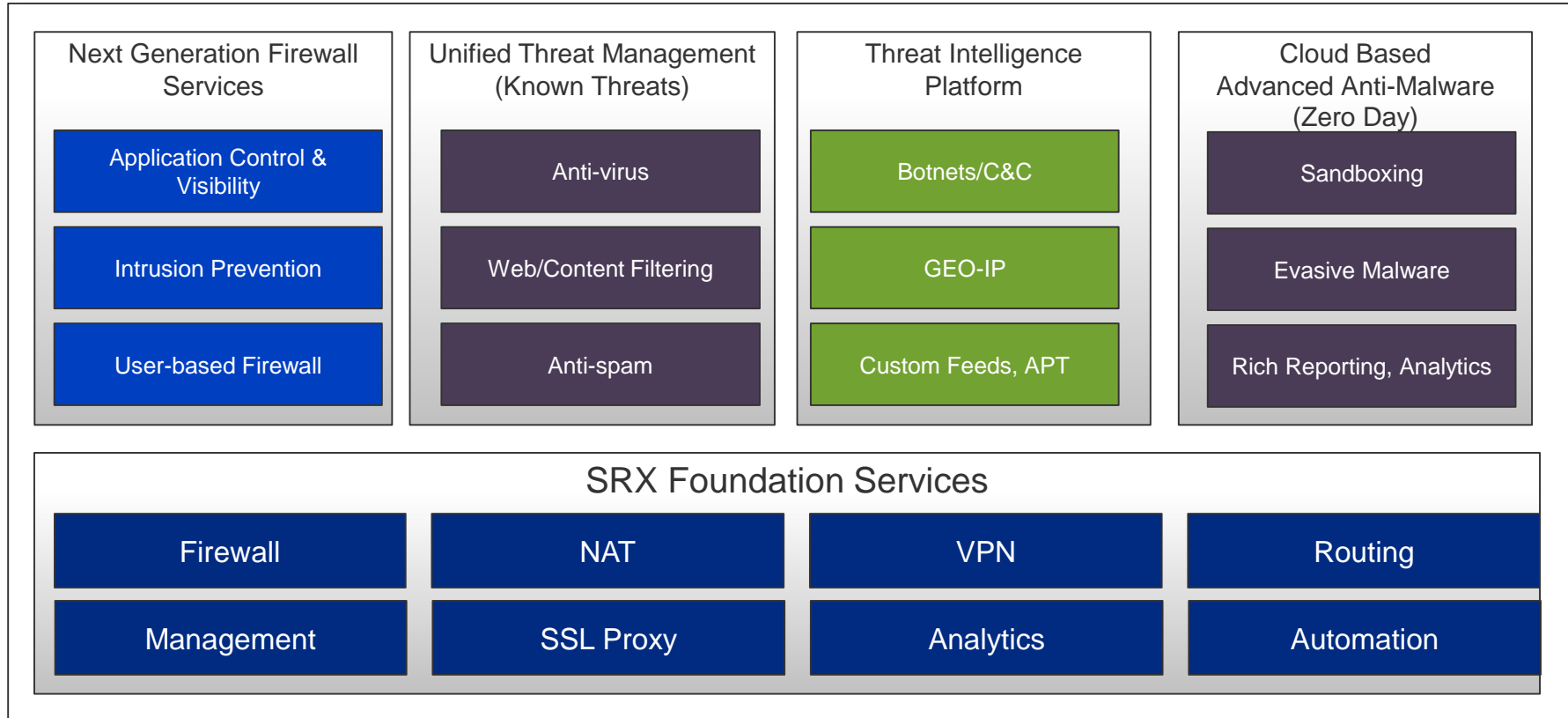


Service Agility  
& DevOps

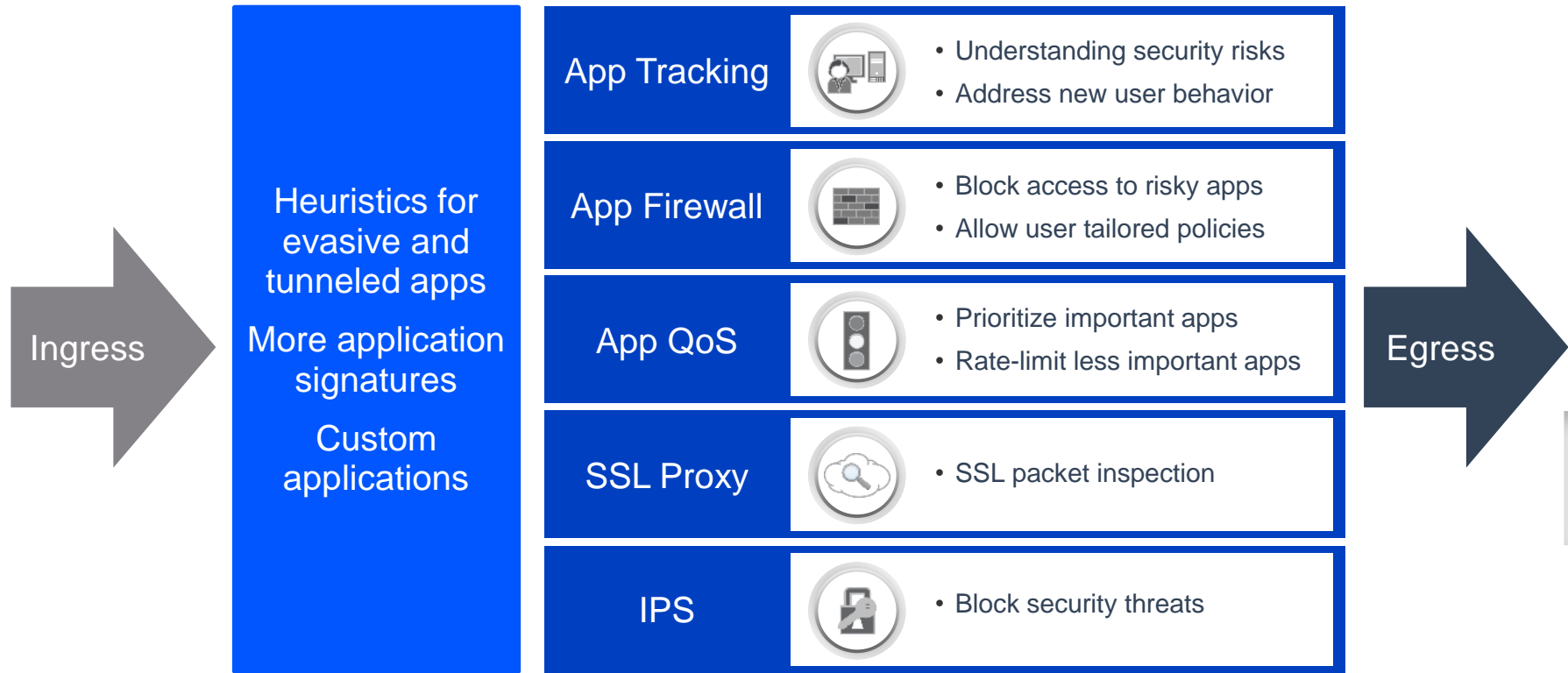


Pay-As-You-Grow  
Biz Model

# JUNIPER SECURITY SERVICES OVERVIEW



# APPLICATION VISIBILITY AND CONTROL





# MANAGEMENT INTEGRATION

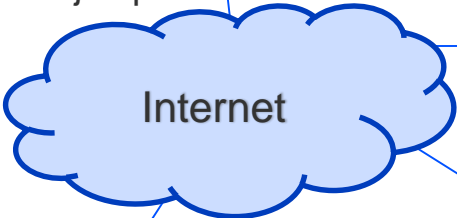
# PHONE HOME

## Enterprise Remote Branch / Campus



SRX / NFX

**1** Upon initial boot-up, Device's Phone-Home contacts `redirect.juniper.net`

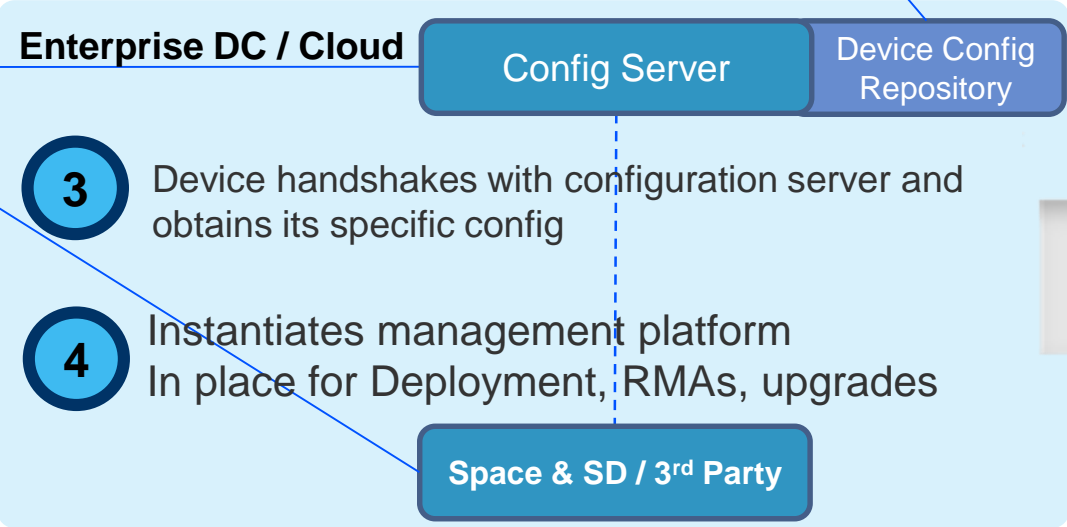


`redirect.juniper.net`

**2** `redirect.juniper.net` passes the address of customer configuration server to the Device

**0** Device configurations are generated

**0.1** Authentication for installations

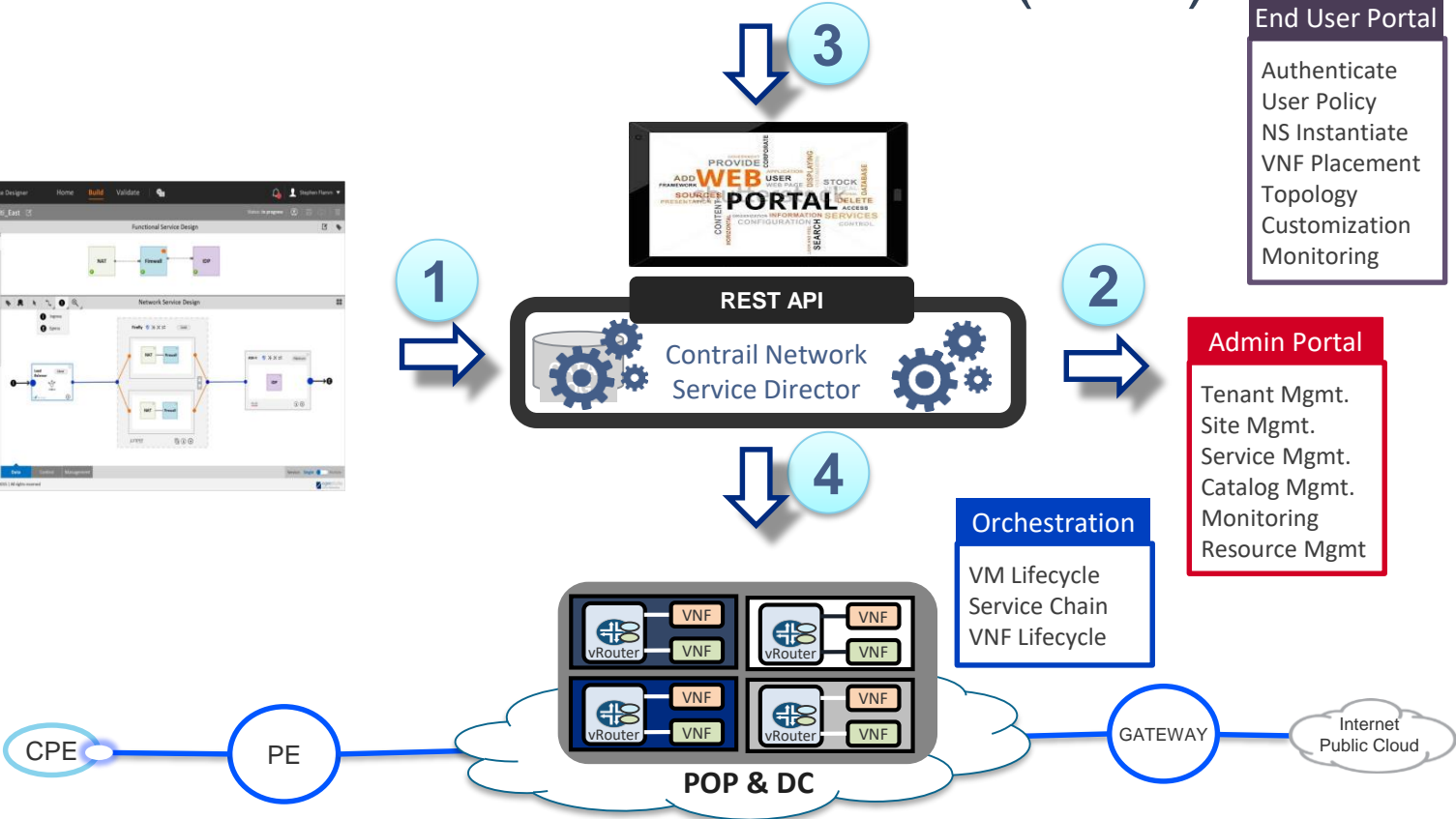
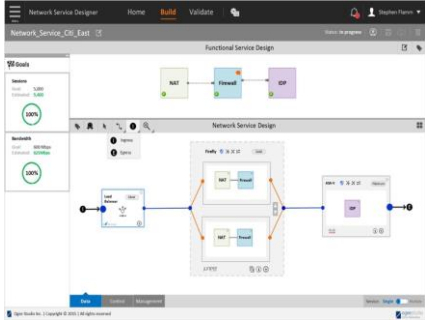




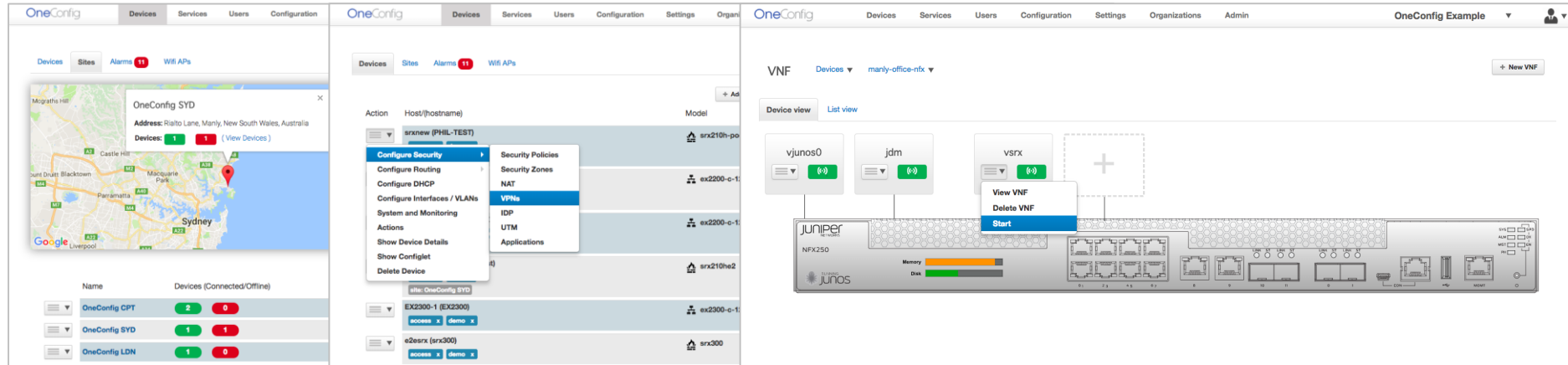
# CONTRAIL SERVICE ORCHESTRATOR (CSO)

Designer

VNF Onboard  
VNF Flavor  
VNF Descriptor  
NS Design  
Service Graph  
NS Descriptor  
Service Config  
Service Template  
Share Resources  
Access Control



# CLOUD BASED MANAGEMENT FOR JUNIPER



- Centralized visibility and control
- Delivered as a service, nothing to install or maintain
- Detailed security reports
- Aerohive integration for AP visibility
- Supports EX, SRX, vSRX and NFX
- 2FA, IPsec VPNs
- Advanced Policy-Based Routing
- Zero Touch Provisioning for rapid deployment

# CLOUD MANAGEMENT

OneConfig

Devices

Users


Configuration

Settings

Organizations

Admin






















OneConfig ▾

 ▾

## Devices

Alarms ▾



 Download

| Action  | Host (hostname)                 | Description/IP address                      | Model   | Status   |
|---|---------------------------------|---|---|--|
|  ▾ | srxnew (BUFU1)                  | Home Security 1<br>IP: 124.170.242.186      |  srx210h-poe       | Online    |
|  ▾ | exnew (EX2200-1-NEW)            | Office Access Switch<br>IP: 124.170.242.186 |  ex2200-c-12t-2g   | Online    |
|  ▾ | EX2200-C-12P (EX2200-C-12P-new) | Basement switch 1<br>IP: 124.170.242.186    |  ex2200-c-12p-2g   | Online    |
|  ▾ | evaltest1 (LAB-SRX2_test)       | IP: 124.170.242.186                         |  srx210he2         | Online   |
|  ▾ | vSRX1 (vSRX)                    | IP: 124.170.242.186                         |  firefly-perimeter | Online    |
|  ▾ | EX2300-1 (EX2300)               | IP: 124.170.242.186                         |  ex2300-c-12t      | Online    |
|  ▾ | BuffaloTest (SRXbuffalo)        | IP unknown                                  |  srx300            | Offline   |

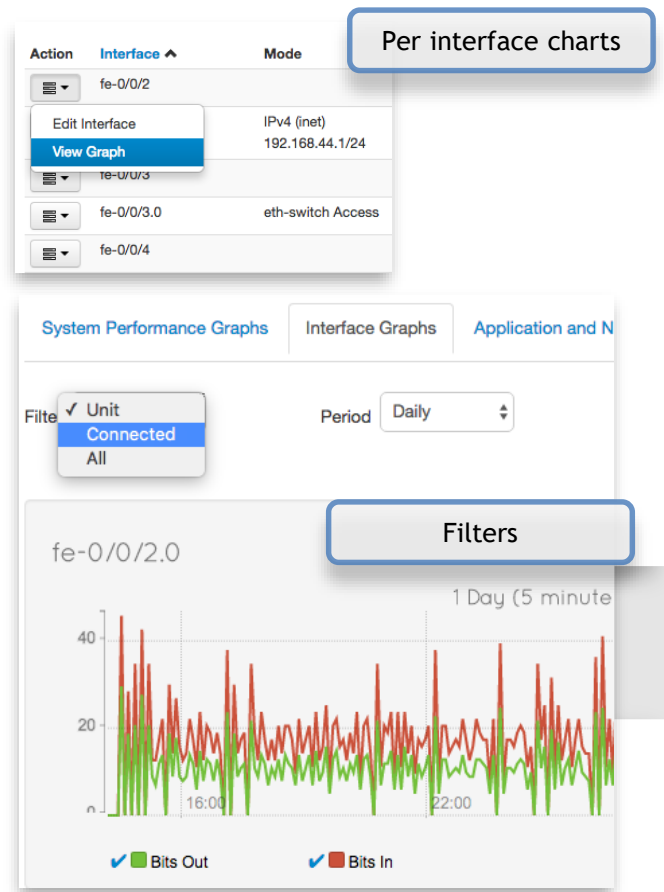
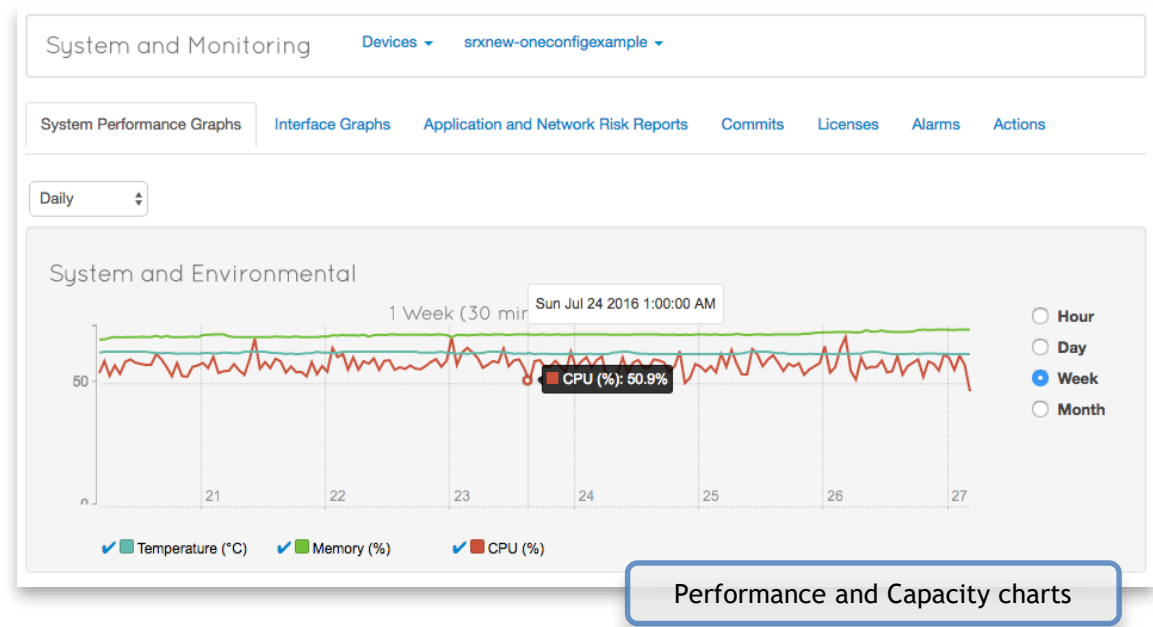
+ Add device

# CLOUD MANAGEMENT

VNF Devices ▾ nfx-jdm-miomaxtest ▾ + New VNF

| Action   | ID | Name     | State    | Liveliness         |
|--|----|----------|----------|--------------------|
|     | 4  | vjunos0  | running  | <span>Alive</span> |
|     | 22 | vsrx     | running  | <span>Down</span>  |
|     | 29 | ubuntu   | running  | <span>Alive</span> |
| <div><div>View VNF</div><div>Delete VNF</div><div>Restart</div><div>Stop</div></div> |    | riverbed | shut off | <span>Down</span>  |
|  |    | jdm      | running  | <span>Alive</span> |

# CLOUD MANAGEMENT



# CLOUD MANAGEMENT – SINGLE PANE



OneConfig

DevicesServicesUsersConfigurationSettingsOrganizationsAdmin

miomaxtest

DevicesSitesAlarms8Wifi APs1

Wifi Access Points

Search

| Action      | Host Name   | Model  | Associated Device | Associated Site | Active Clients | Connected   |
|-------------|-------------|--------|-------------------|-----------------|----------------|-------------|
| <div></div> | AH-0ad540   | AP_122 |                   | dublin oh       | 6              | <div></div> |
| <div></div> | AH-0ad680   | AP_122 | ex2200-1          |                 | 1              | <div></div> |
| <div></div> | SIM-2112A3  | AP_250 |                   |                 | 0              | <div></div> |
| <div></div> | AH-060a40   | AP_122 |                   |                 | 0              | <div></div> |
| <div></div> | Hoover-BSMT | AP_122 |                   |                 | 9              | <div></div> |

Wifi Access Point Clients

Search

| Status      | Health      | Connection Type | Host Name                | Connection Status | IP Address    | MAC Address  | OS Type                    | Usage   | VLAN | SSID          |
|-------------|-------------|-----------------|--------------------------|-------------------|---------------|--------------|----------------------------|---------|------|---------------|
| <div></div> | <div></div> | WIRELESS        | Jeremys-iPhone           | CONNECTED         | 192.168.1.205 | CC2DB782F33A | Apple iPod, iPhone or iPad | 645 KB  | 1    | cadenza-guest |
| <div></div> | <div></div> | WIRELESS        | LAPTOP-35KUGSBL          | CONNECTED         | 192.168.1.209 | 1C4D70213C2F | Windows 8/10               | 0 Bytes | 1    | cadenza-guest |
| <div></div> | <div></div> | WIRELESS        | iPhone                   | CONNECTED         | 192.168.1.211 | 80ED2C85F902 | Apple iPod, iPhone or iPad | 0 Bytes | 1    | cadenza-guest |
| <div></div> | <div></div> | WIRELESS        | 2017-MBP                 | CONNECTED         | 192.168.1.210 | DCA904785F48 | Mac OS X                   | 0 Bytes | 1    | cadenza-guest |
| <div></div> | <div></div> | WIRELESS        | android-485f5e4cae30689d | CONNECTED         | 192.168.1.207 | 98F1704D252D | Generic Android            | 192 KB  | 1    | cadenza-guest |

OneConfig

HomePrivacyTermsSecurityFaqFeaturesContact

Copyright 2012 - 2017 OneConfig Pty Ltd Version: 1.54.0

# CLOUD MANAGEMENT – SINGLE PANE



| OneConfig   |                           |            |                   |              |              |              |
|---|---------------------------|------------|-------------------|--------------|--------------|--------------|
| Devices Services Users Configuration Settings Organizations Admin |                           |            |                   |              |              |              |
| Wifi Access Point Clients   |                           |            |                   |              |              |              |
| Status  |                           |            |                   |              |              |              |
| Health  | Connection Type           | Host Name  | Connection Status | IP Address   | MAC Address  |              |
| ●   | Connected:                | ●          | d8a2411914816     | CONNECTED    | 10.10.10.100 | 182195F87F6F |
| ●   | Client Health: 100 %      | ●          | 863e9f5a8f918     | CONNECTED    | 10.10.10.165 | DCCF96378CD7 |
| ●   | Network Health: 100 %     | ●          | f5e4cae30689d     | CONNECTED    | 10.10.10.105 | 98F1704D252D |
| ●   | Radio Health: 100 %       | ●          | 1c3fe805e6c2c     | CONNECTED    | 10.10.10.99  | 28565A691BFD |
| ●   | Application Health: 100 % |            |                   |              |              |              |
| ●   | WIRELESS                  | Elis-ipod  | CONNECTED         | 10.10.10.206 | 00C610EBD658 |              |
| ●   | WIRELESS                  | Chromecast | CONNECTED         | 10.10.10.69  | 546009129110 |              |

---

# GETTING STARTED



# WHERE TO GET STARTED/RESOURCES

## Resources

- NFX: <https://www.juniper.net/us/en/products-services/sdn/nfx250>
- vSRX: <https://www.juniper.net/us/en/products-services/security/srx-series/vsrx/>
- CSO: <https://www.juniper.net/us/en/products-services/sdn/.../contrail-service-orchestration/>
- One Config: [www.OneConfig.com](http://www.OneConfig.com)

## Where to get Started

- Juniper Account Team for a demo
- Juniper Partner demo and solutions
- OneConfig (OneConfig.com)



# TAKEAWAYS: WHAT YOU GOT WHILE YOU WERE HERE

- Evolution of Branch Architectures
- Intro to the NFX Platform
- Deployment Methods
- SD-WAN Market
- Management Integration
- NFX Deep Dive



# Q&A

# Thank you



<http://forums.juniper.net/>

@JunosAutomation  
#JKitty



<http://www.facebook.com/JuniperNetworks>



<http://www.juniper.net/youtube>



<http://twitter.com/#!/junipernetworks>



<http://www.linkedin.com/company/juniper-networks>



<https://github.com/Juniper>

@ATL\_Oliver