



Cisco IT Network Management

NSO Use Cases

Andrea Di Lecce, Technical Program Manager, Cisco IT

Brandon Black, NSO Developer & DevOps Engineer, Cisco IT

Madalina Ana, Technical Program Manager, Cisco IT

November, 2017

NSO Business Benefits

Security



Simplify Everything

- Employee Services
- Customer/Partner Services
- IT as a Service



Extend the Cloud

- Global Cloud Strategy
- Fast(er) Applications
- Application Centric Infrastructure



Insightful Data

- Connected Install Base
- Connected Renewals
- Quality



Operational Excellence

- Quality
- Cost
- Resiliency
- Security



Culture

- Talent Cloud
- People Deal/Strategy
- Best Place to Work

Continuous Delivery

Improve User Experience, Deliver Services Faster	Plug-and-Play Provisioning – Remote Office, Other	Control, Maintain and Update Network Configuration	Reduce Incidents and Support Cases, Save Engineering Time	Develop Full-Stack Engineers
--	---	--	---	------------------------------

Cisco IT Main Use Cases



Lab Automated Provisioning & Management



Lab ACL Configuration Service Management



PnP Remote Worker Device Configuration



Branch Office Configuration Standard Management



TrustSec Audit and Deployment



QoS Configuration Service Management



Other Service Management



Ad-Hoc Automation for One-Off Requirements

Cisco IT – Home Office (Cisco Virtual Office)

Madalina Ana

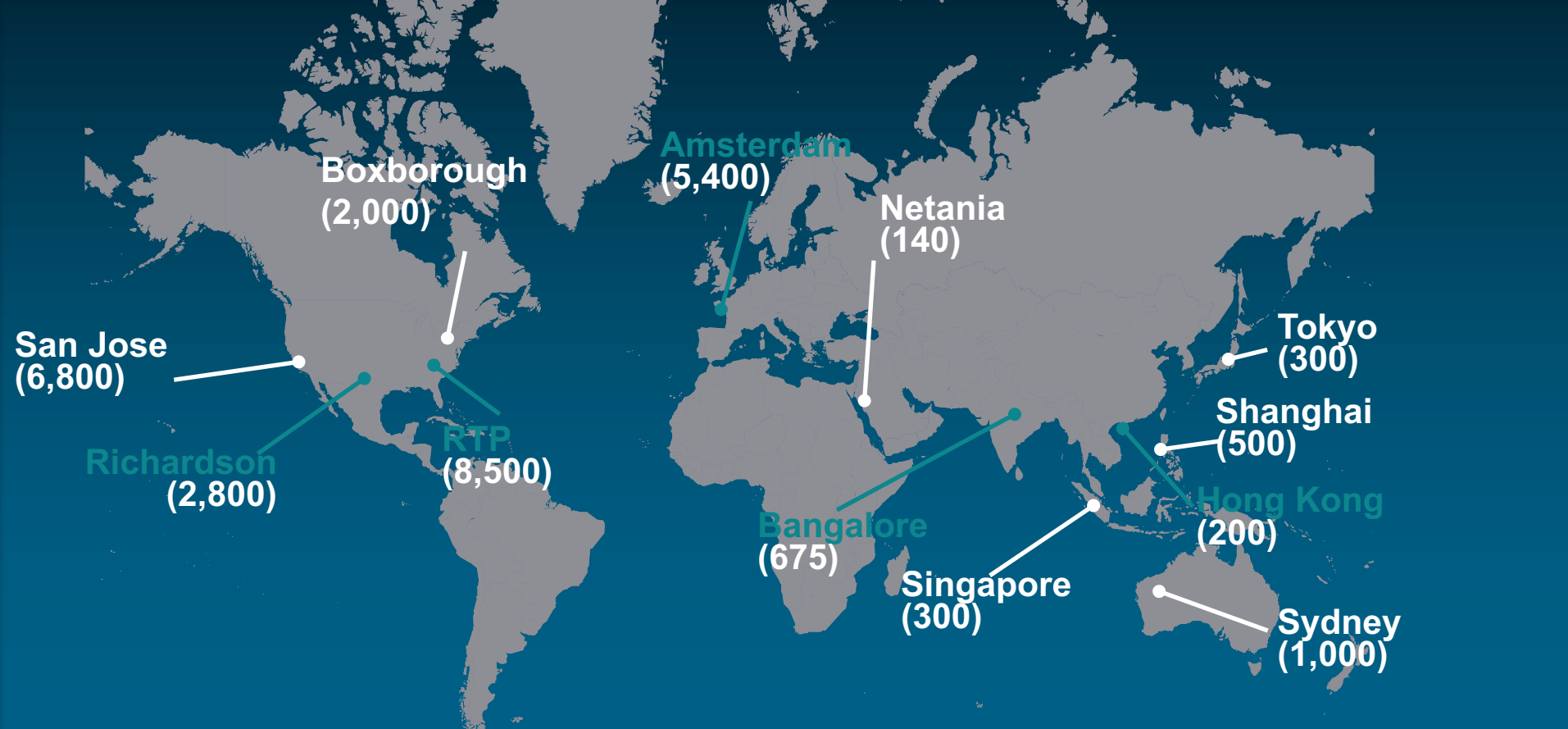
Use Case: NSO for CVO

Remotely manage configuration for:

- ~30k CVOs spoke routers
- ~30k APs

NSO leveraged for:

- CVO Provisioning
- CVO Configuration Compliance
- rollout large changes with relative ease (IPv6)



NSO Automation Processes

Day 0

**Service
Ordering
and Shipping
Process**

deploy most basic configuration for device to connect to network

Day 1

**Service
Provisioning
Process**

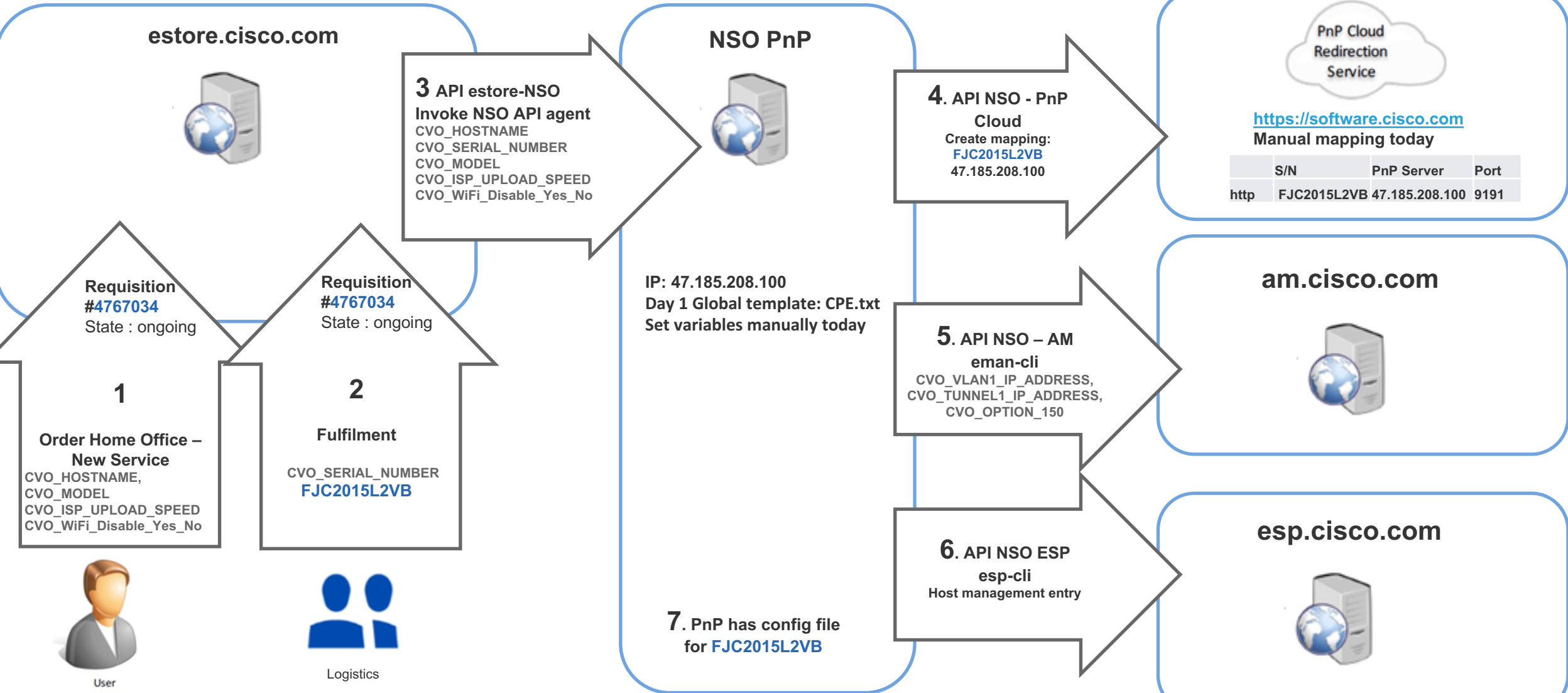
provision complete configuration based on SN# using PnP cloud

Day 2

**Service
Compliance
Process**

ongoing configuration compliance

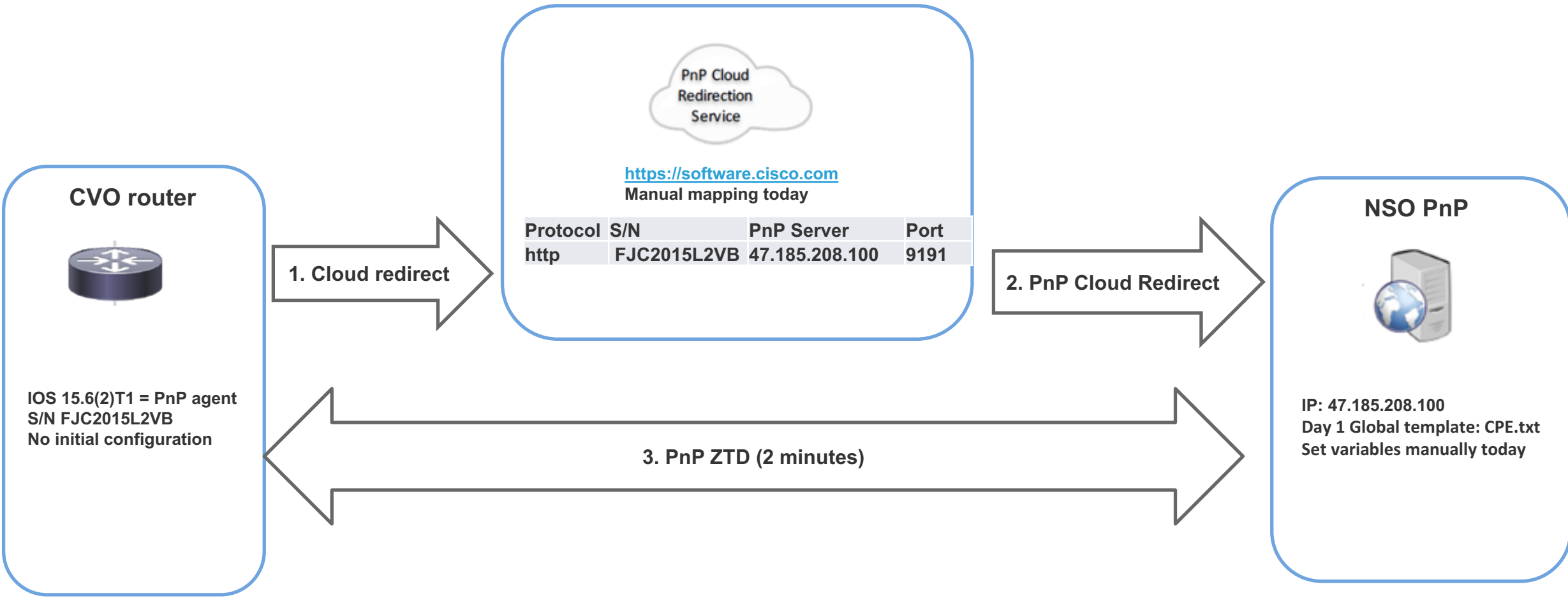
Day 0 provisioning using NSO PnP



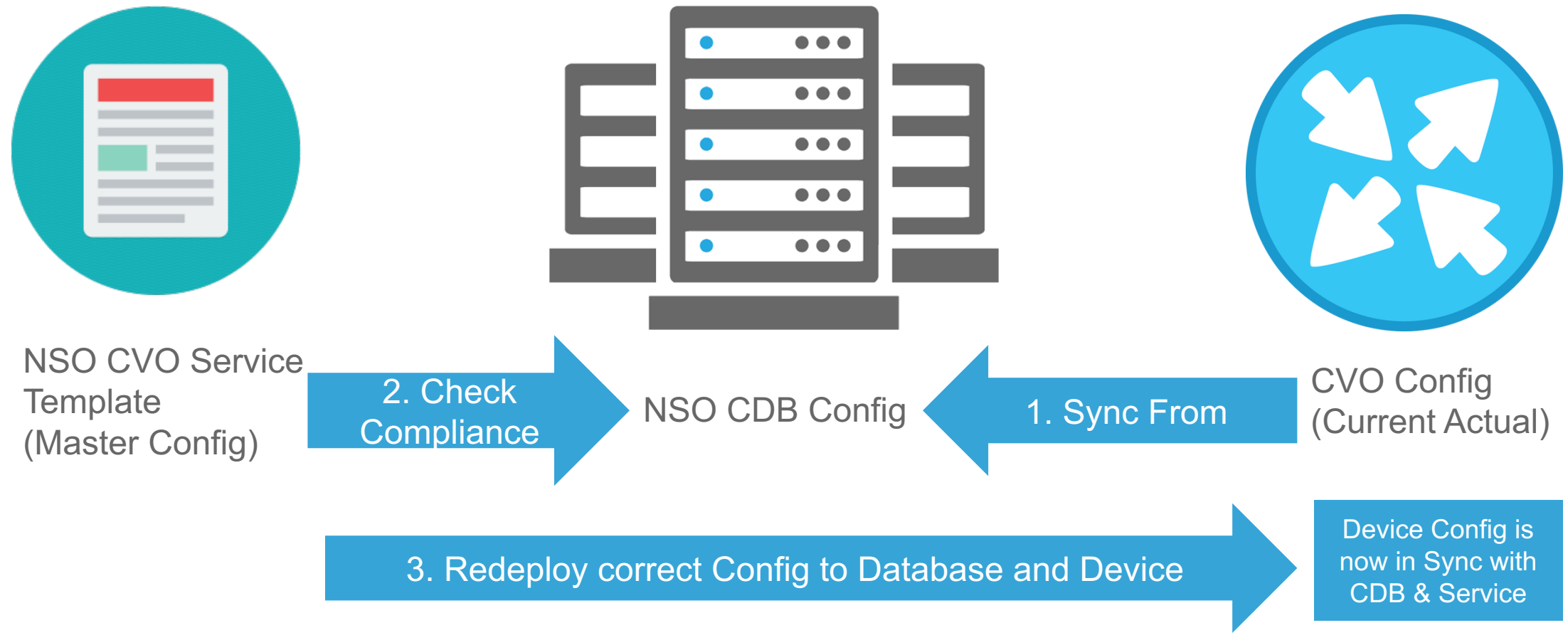
Requisition #4767034
State : Complete
After shipment received



Day 1 provisioning using NSO PnP



Day 2 Process – Service Compliance



Day 2 Process - Service Compliance - deep dive



NSO CVO Service Yang model

```
leaf nwaddr {  
    tailf:info "Network Address registered in EMAN for the CVO";  
    type inet:ipv4-address;  
}
```

NSO CVO Service XML Template

```
<ext-named-acl>  
<name>TRUST_ACL_1</name>  
<ext-access-list-rule insert="first">  
    <rule>permit icmp 10.0.2.0 0.0.0.255 {/nwaddr} 0.0.0.15</rule>  
</ext-access-list-rule>  
<ext-access-list-rule insert="after" value="permit icmp 10.0.2.0 0.0.0.255 {/nwaddr} 0.0.0.15">  
    <rule>permit tcp any any established</rule>  
</ext-access-list-rule>  
<ext-access-list-rule insert="after" value="permit tcp any any established">  
    <rule>deny ip 10.0.2.0 0.0.0.255 {/nwaddr} 0.0.0.15</rule>  
</ext-access-list-rule>  
<ext-access-list-rule insert="after" value="deny ip 10.0.2.0 0.0.0.255 {/nwaddr} 0.0.0.15">  
    <rule>permit ip any any</rule>  
</ext-access-list-rule>  
</ext-named-acl>
```

2. Check Compliance

NSO CDB
Config

1. Sync
From

CVO Config

```
ip access-list extended TRUST_ACL_1  
permit icmp 10.0.2.0 0.0.0.255 10.56.253.48 0.0.0.15  
permit tcp any any established  
deny ip 10.0.2.0 0.0.0.255 10.27.68.208 0.0.0.15  
permit ip any any  
exit
```

Compliance Report

http://nwsnsocvodev-1:8080/compliance-reports/report_9_jakerby_1_2016-11-17T13:6:29:0.html

```
ext-named-acl TRUST_ACL_1 {  
+     # after ext-access-list-rule "permit tcp any any established"  
+     ext-access-list-rule "deny ip 10.0.2.0 0.0.0.255 10.56.253.48 0.0.0.15";  
+     ext-access-list-rule "permit ip any any";  
-     ext-access-list-rule "permit ip any any";  
}
```

3. Redeploy correct Config to NSO CDB and Device

Device Config is now in
Sync with CDB & Service

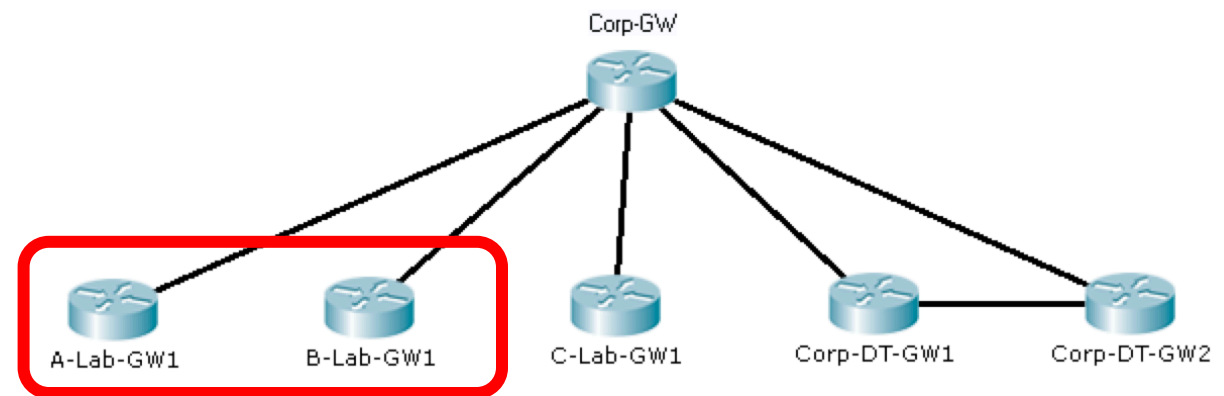
Lab Gateways - ACL Enforcement

Brandon Black

Cisco IT – ACL Enforcement

Cisco IT – ACL Enforcement Use Case

- Cisco IT provides secured network connectivity through 500 + Lab GWs
- Security enforced via uplink ACLs
- ACL to control network traffic from labs to corporate network
- Highly important for compliance and security
- Protects the production environment
- Gives engineers the control of Lab traffic



NSO Development

- Solution was to develop a small ACL enforcement service
- Separate scripts were used to determine correct interfaces
- Interface mapping service instances created via python
- NSO Compliance Reporting for auditing
- Service Re-deploy for remediation



Deployment Challenges

Challenges:

- Performance for re-deploys against separate service instances
- Transactionality and considerations (commit-queues)
- Handling device failure (TCAM Utilization)
- Device discovery and additions

Project Status

- 100% ACL Compliance of ACL application globally
- Monthly auditing of global devices
- Considerations for cross-service usage and service chaining

100

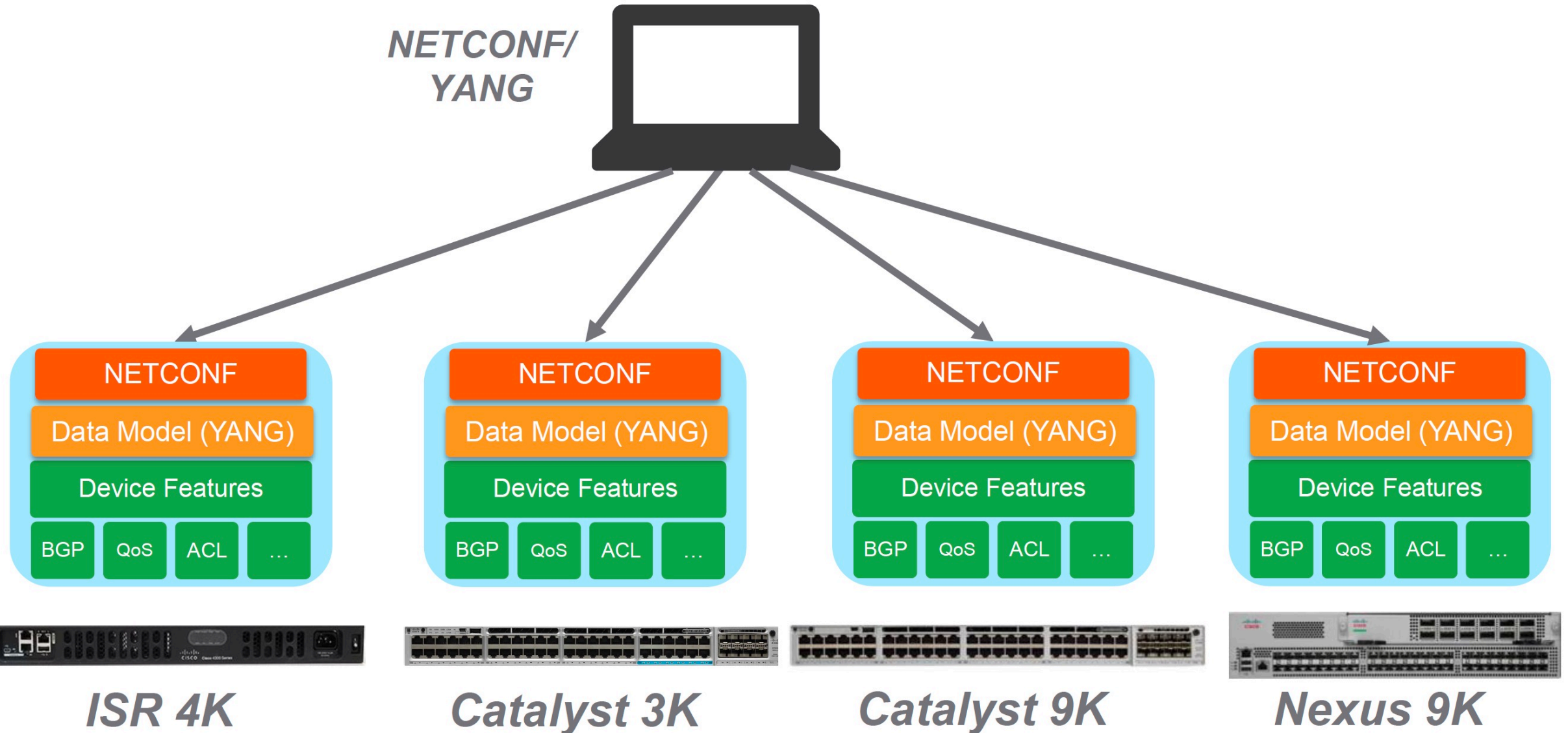
Thank you



The Industry's Broadest Multivendor Support with Over 100 Supported NEDs—Customization Available



Consistency across Cisco platforms



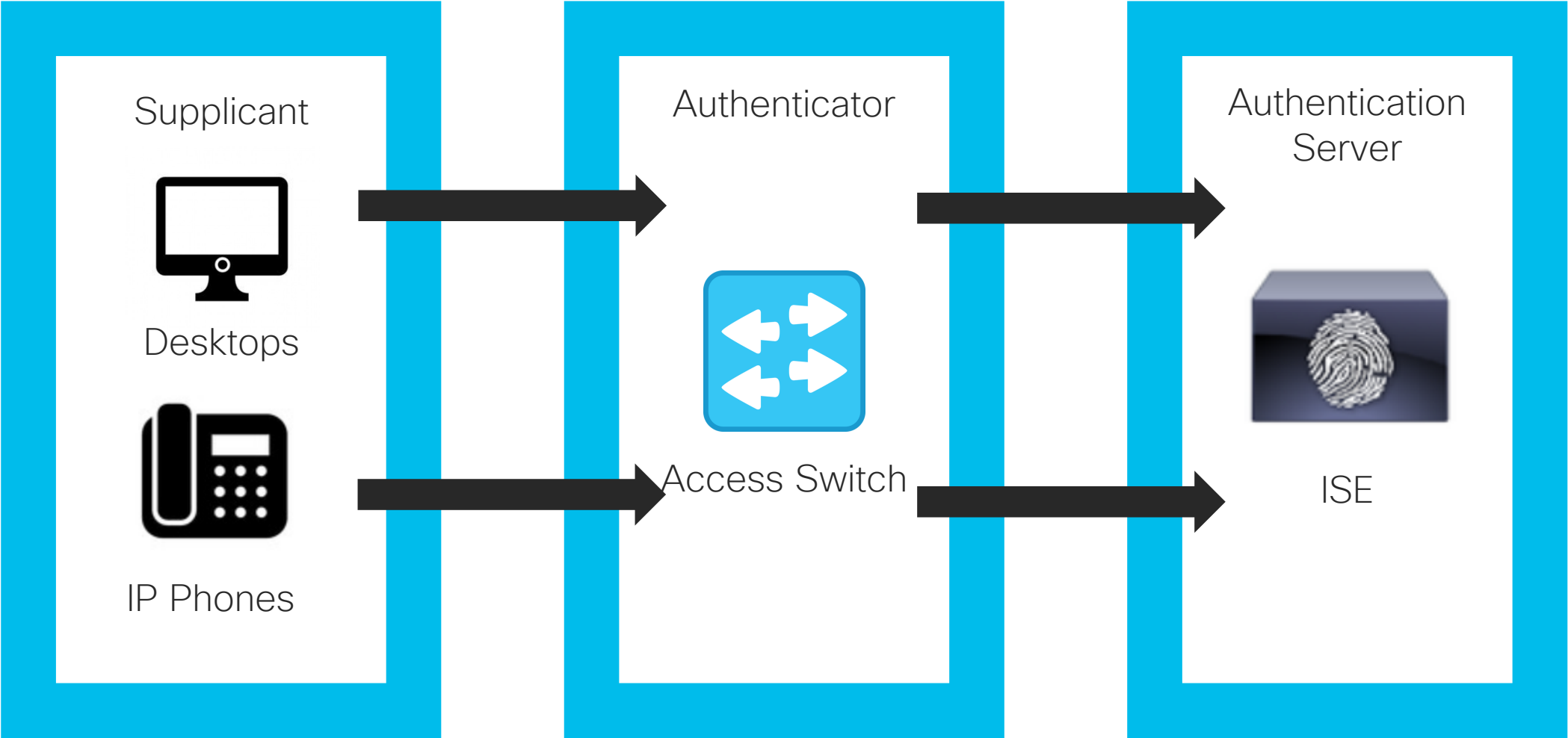
ISR 4K

Catalyst 3K

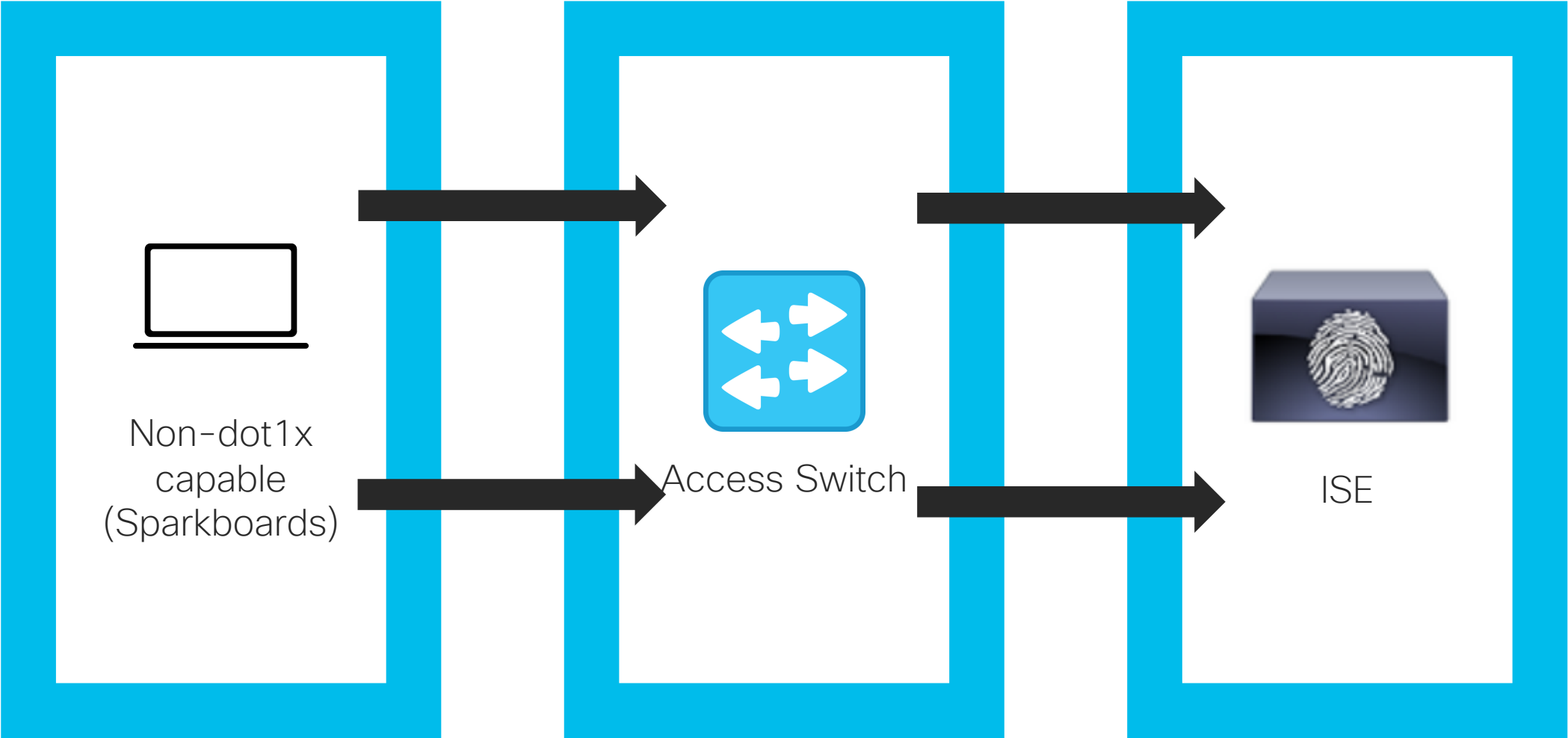
Catalyst 9K

Nexus 9K

Authentication Method 1: 802.1x

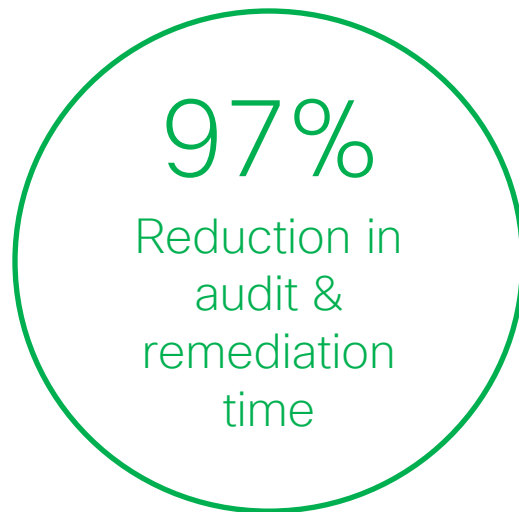


Authentication Method 2: MAB



Example: Lab ACL Configuration Service Management

The team wrote a service automation which determines the lab uplink interfaces, and audits if the IPv4 and IPv6 ACLs are not configured on those interfaces. Remediation automation was run during a change window.



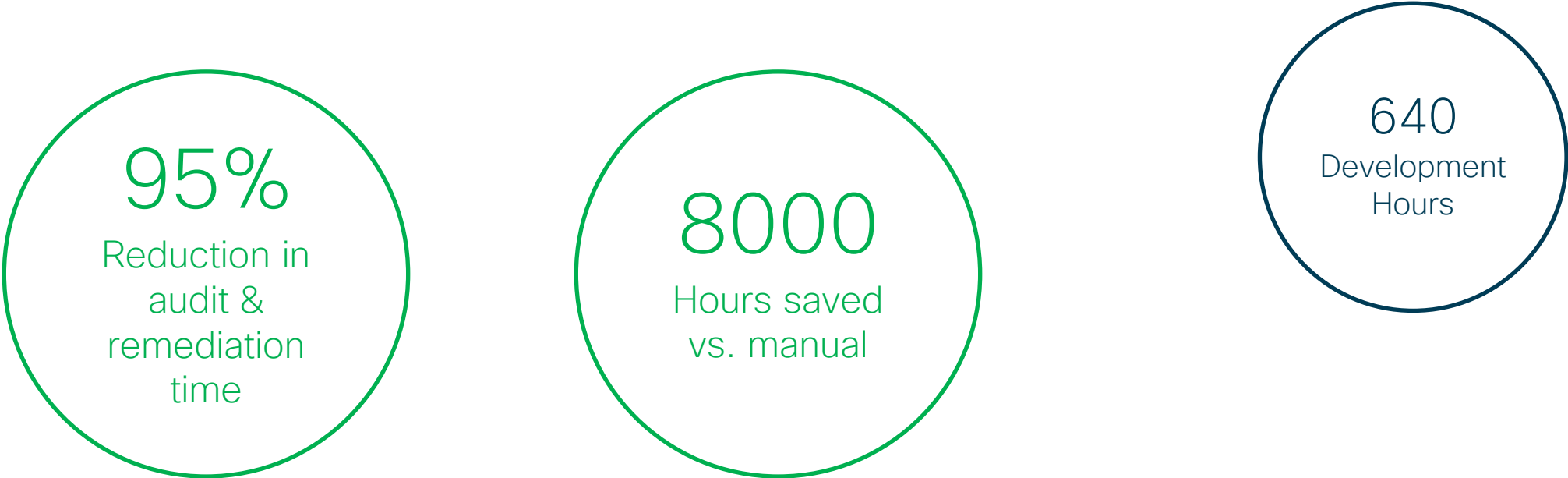
Handoff to Production in progress



Regular audit & remediation cadence will **avoid high-priority P1/P2 issues** in future

Example: TrustSec Audit and Deployment

Audit and remediate 802.1x configuration across the enterprise; deploy TrustSec service end-to-end.



- ★ This effort would not be realistically possible without automation due to massive scope
- ★ End-to-end TrustSec configuration ensures security of wired ports enterprise-wide