Deploying Enterprise Scale User Firewall and Device Identity

Harry Cornwell

Technical Marketing Engineer--Security

NXTWORK2017
JUNIPER CUSTOMER SUMMIT

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.

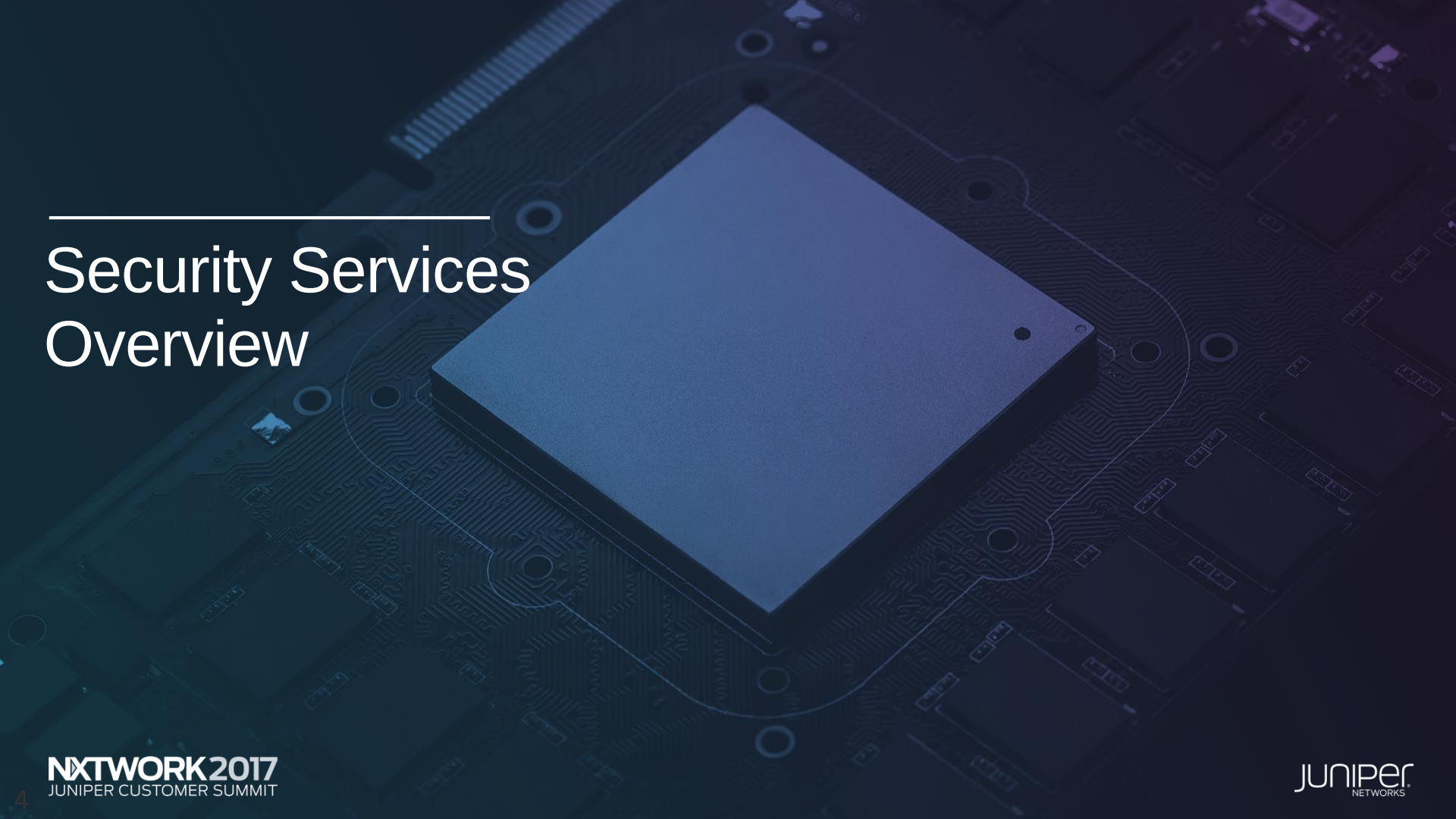
This presentation contains proprietary roadmap information and should not be discussed or shared without a signed non-disclosure agreement (NDA).

Juniper Networks

Agenda

- Security Services Overview
- The Evolution of Security Policy
- Defining Context Aware Firewall
- Existing UserFW
- Juniper Identity Management Service (JIMS)
- Demo
- Summary
- Q&A

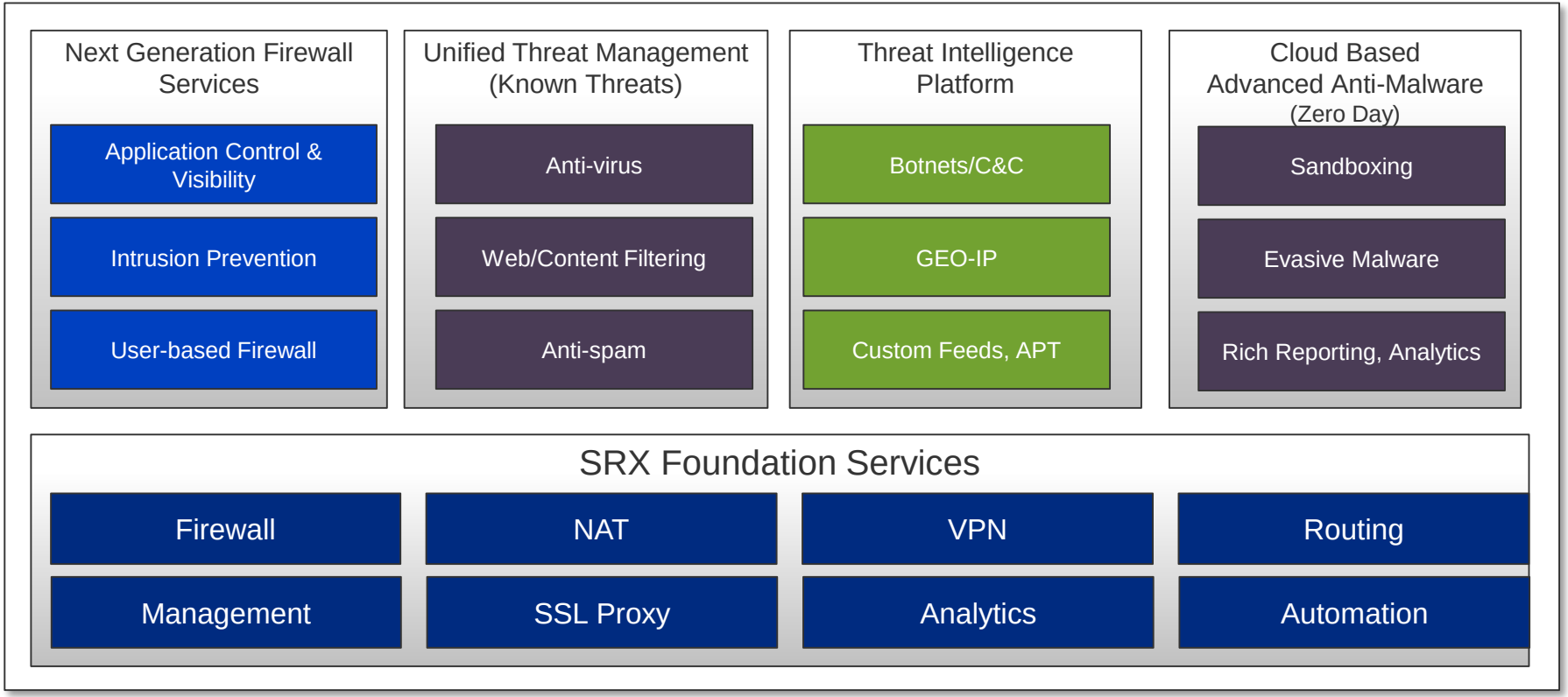
Security Services Overview



SRX Layered L7 Security: Defense in Depth

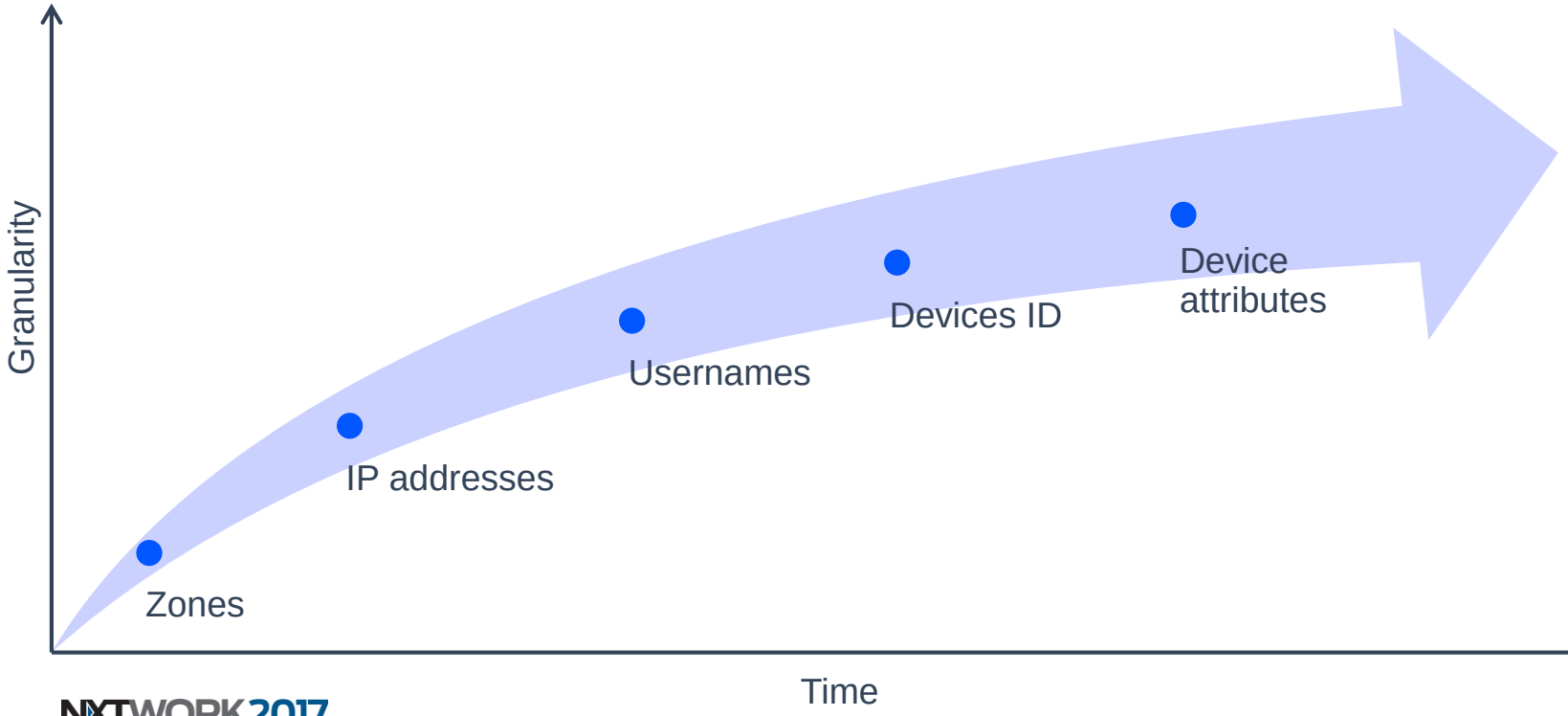
Enhanced Web Filtering		Block access to unapproved sites Real time threat score for each URL
Antivirus (known and unknown)		Stops known and unknown viruses, file-based trojans or spread of spyware, adware, keyloggers
IPS		IDP detects/stops Worms, Trojans, exploits, shellcode, Scans
SSL Proxy		Inspect Encrypted Traffic
AppSecure		Application level visibility and classification Application security policies tied to user roles
Core Security with User Role FW		Firewall, VPN, NAT, UserID tied to FW policies Allows UserID to apply to all L7 Security

Juniper Security Services Overview



The Evolution of Security Policy

Security Policy Evolution



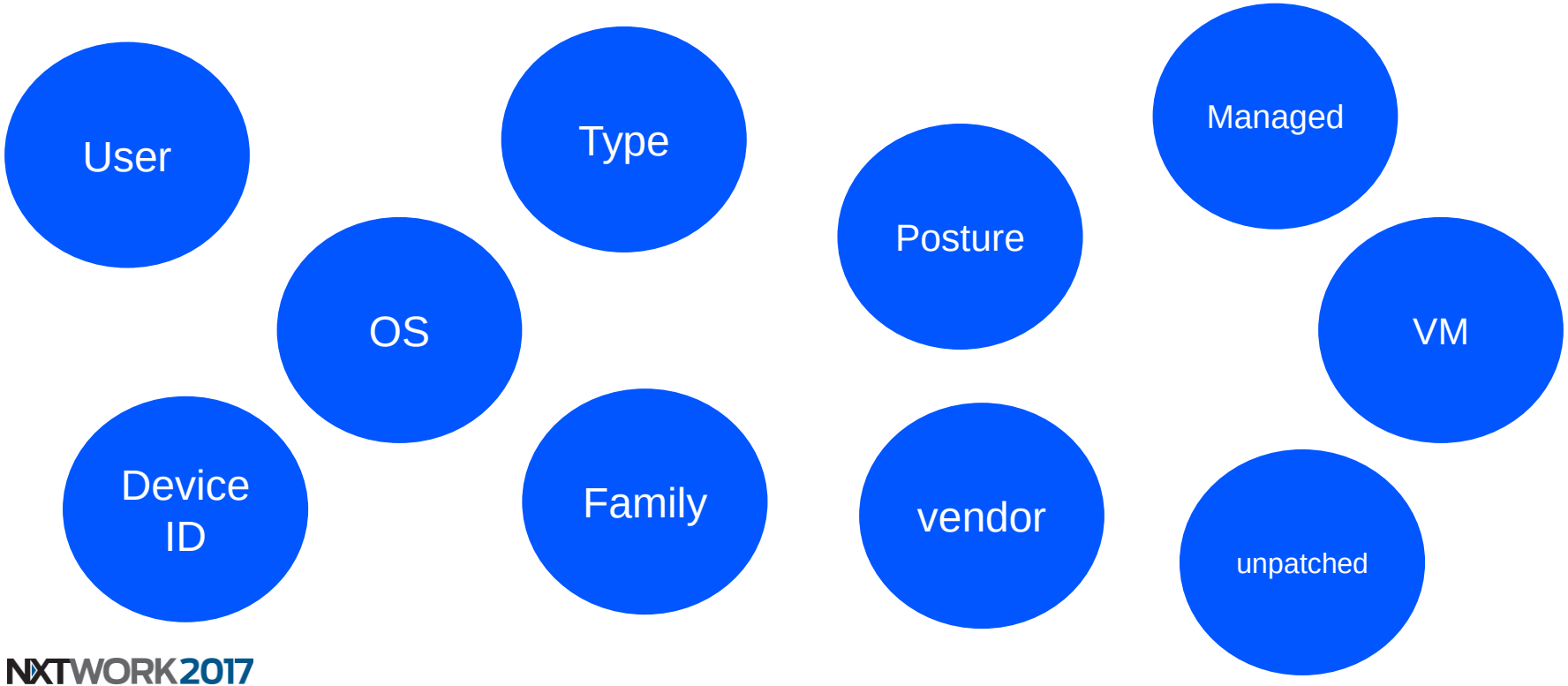
It is no longer only about users..

Context Aware Firewall

What is a Context Aware Firewall?

- Richer Firewall Security Policy
- Leverage User ***and/or*** Device context (on top of IP addresses/zones)
- Flexible attributes for each endpoint
  - Predefined attributes (id, os, category, vendor..)
  - Custom attributes (anything!!)
- Apply security services in a granular way
- Visibility
- Enforcement

Multi-dimension Security Policy



Existing User FW

Options previously available on SRX

	Integrated User FW	• DC polling • Passive authentication • Best effort	• Client probing • Captive portal • No agent
Pulse Secure	Pulse Policy Secure	• Pull user info from Pulse • Deterministic • Captive portal	• Endpoint assessment • Agent / Agentless • Security Threat Correlation
aruba	ClearPass	• CPPM push to SRX • SRX pull from CPPM • Deterministic	• Security Threat Correlation

The dilemma: Simplicity versus Security!

Device/User Firewall

- NGFW capabilities
- Passive authentication (best effort)
- Firewall enforced
- No agents (802.1x supplicant)
- Provides visibility & enforcement
- Captive Portal fallback
- Layer 3 to 7

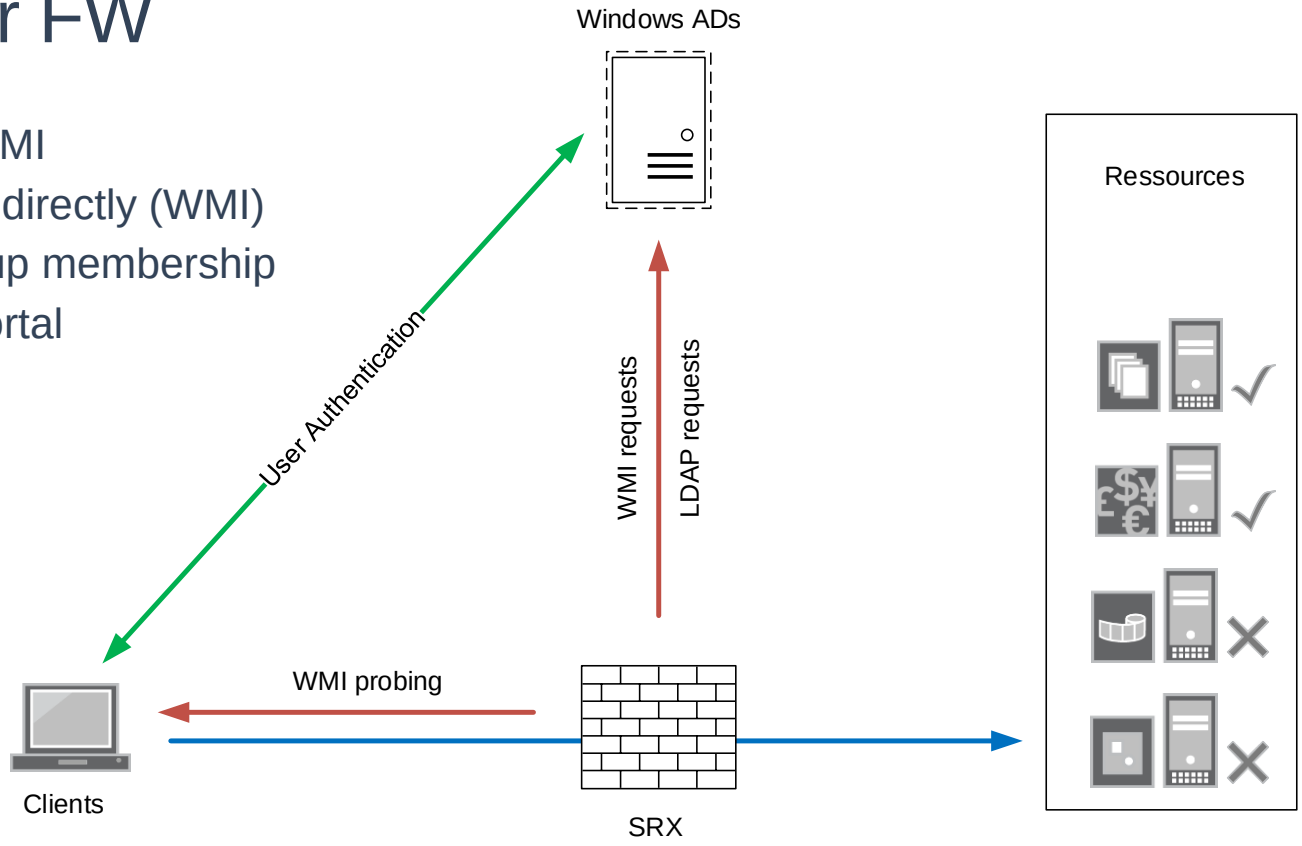
Network Access Control

- End-to-end security
- Deterministic (active authentication)
- Enforced at access & firewall
- SRX + NAC (Aruba CPPM, Pulse..)
- Security conscious environments
- Layer 2 to 7

Integrated User FW

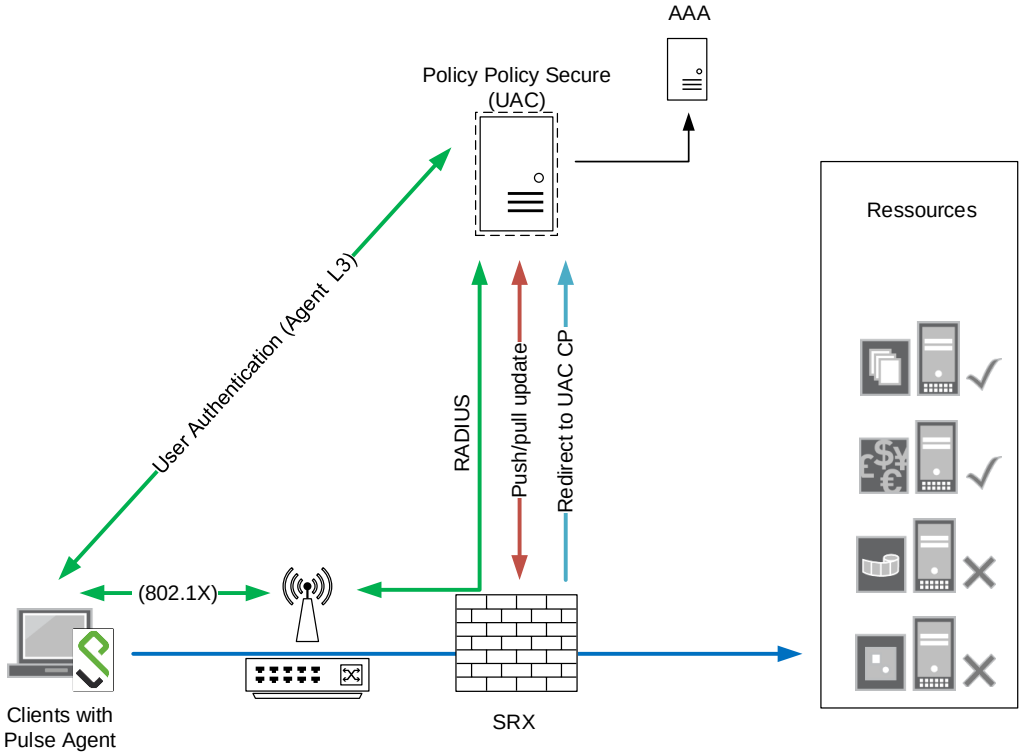
- SRX polls AD using WMI
- SRX probes the client directly (WMI)
- LDAP lookups for group membership
- Fallback to Captive Portal
  - HTTPS/HTTP

- Scalability, up to:
  - 2 Domains
  - 10 DCs
  - 100K users



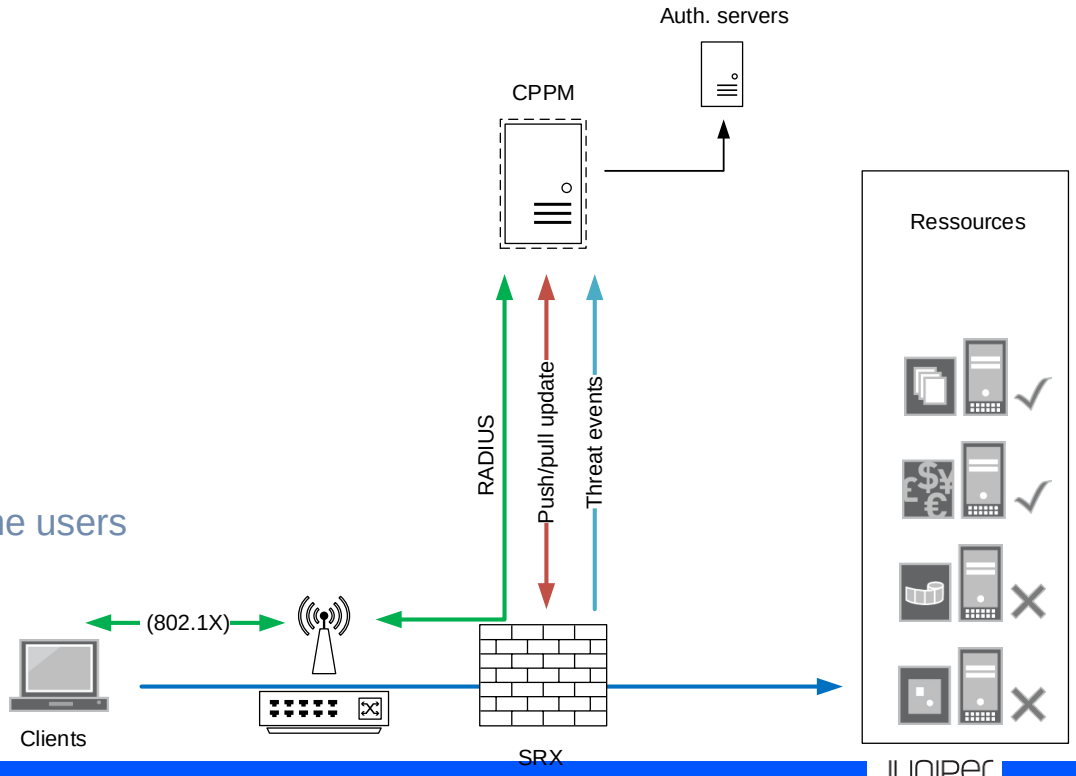
Pulse Policy Secure Integration

- Agent or agentless
- Clients authenticate with:
  - L2 - 802.1x (EAP)
  - L3 – HTTPS (Agent)
- UAC pushes username/IP/roles to the SRX
- SRX enforces user policies
- If a user is unknown, SRX can redirect the user to a captive portal hosted by UAC



ClearPass Policy Manager Integration

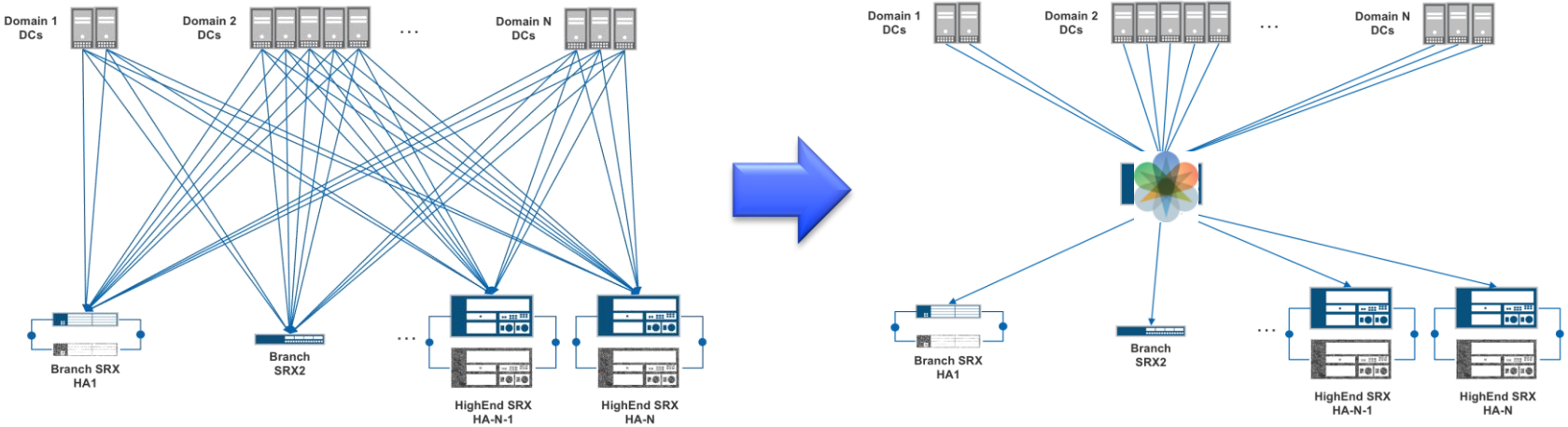
- 802.1x based (wire/wireless)
- Bi-directional communication
  - CPPM pushes to SRX
  - SRX pulls from CPPM
- Coordinate Threat Control
  - SRX send threat events to CPPM
  - CPPM send CoA to take action on the users



Juniper Identity Management Service (JIMS)

Why JIMS?

- Solving the N:M full matrix issue for User FW

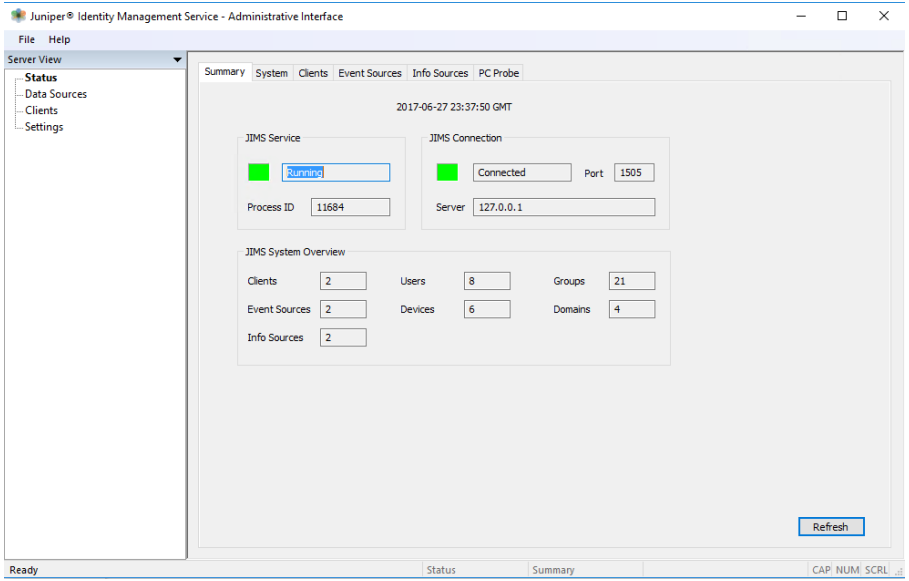


Juniper Identity Management Service

- A Windows based agent for collecting Users and Devices data
- Available for free
- Highly scalable (Up to 100 DC and 25 domains)
  - 1 a single agent can query multiple domains !
- High performance
- Backward compatible with legacy SRX Hardware (12.3 code base)
- Enhanced interface for new hardware (15.1 code base)
- Constantly tracks Active Directory for user and group changes
- Global Filters

Juniper Identity Management Service

- Easy to install, easy to configure.. Wait for the demo !

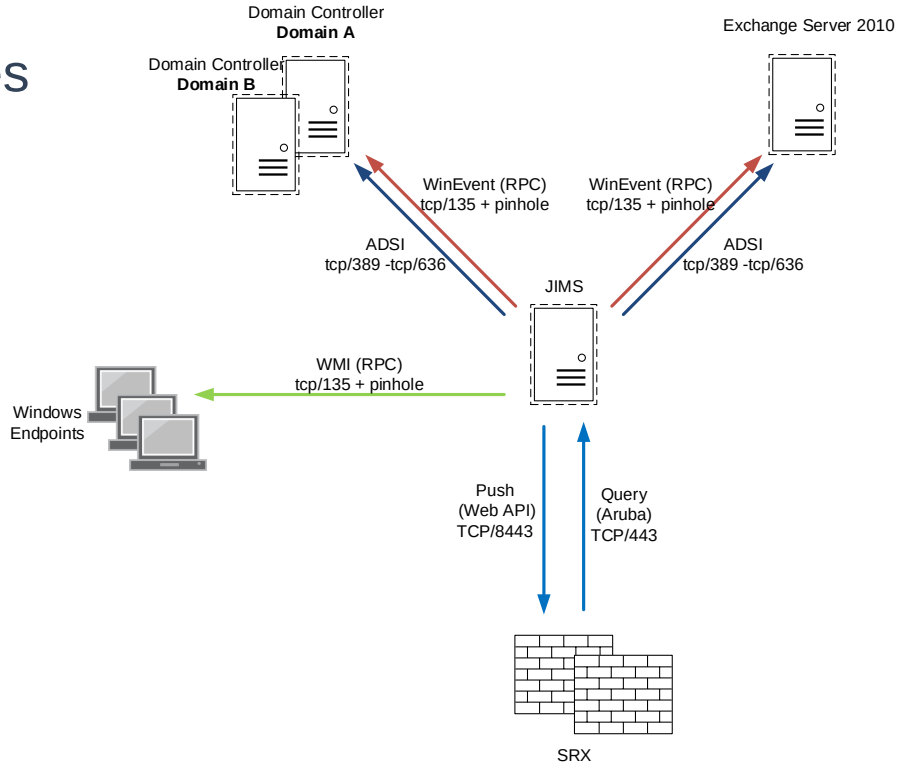


Data Collection mechanisms

- Windows Event API to collect events (versus WMI)
  - Low resources usage
  - Low network bandwidth usage
- ADSI API to collect user's attributes and groups
  - Faster than LDAP
- WMI to probe endpoints
  - Up 10 credential sets.
  - Triggered at the end of the session timeout (configurable)
  - Triggered if no information about a specific IP address

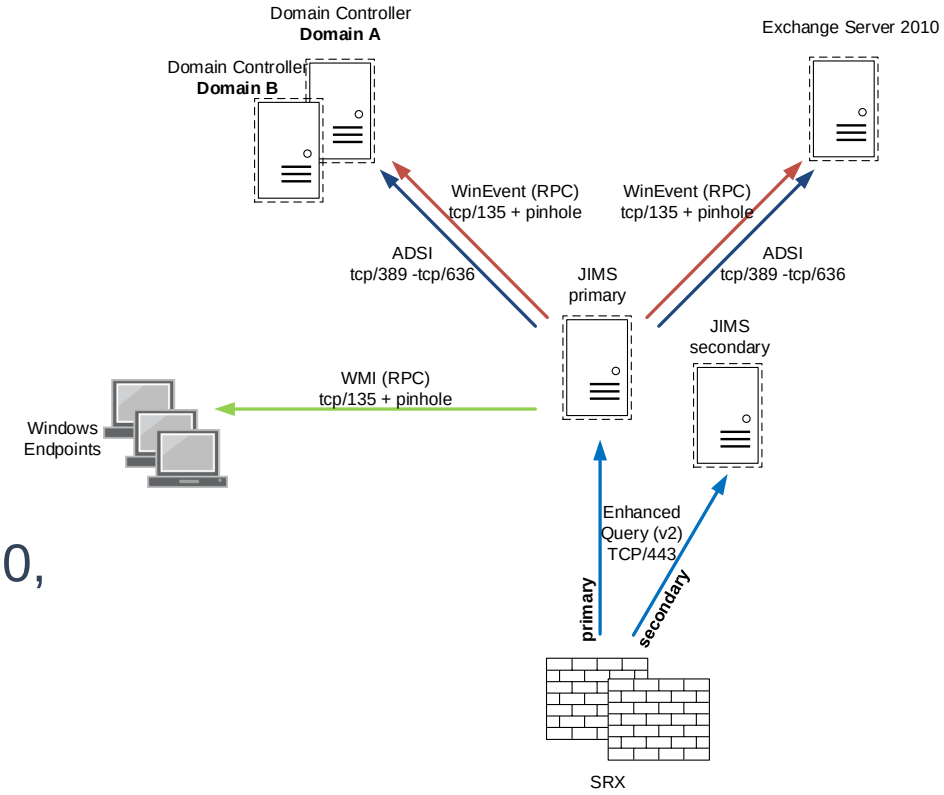
Legacy SRX Backward Compatibility (12.3X48)

- Leverage existing SRX capabilities to support legacy hardware
  - JIMS -> SRX (Web API)
  - SRX -> JIMS (Aruba Query)
- Support on 12.3X48-D45+
- SRX1x0, SRX2xx, SRX550, SRX650, SRX1400, SRX3K, SXR5K (RE1)

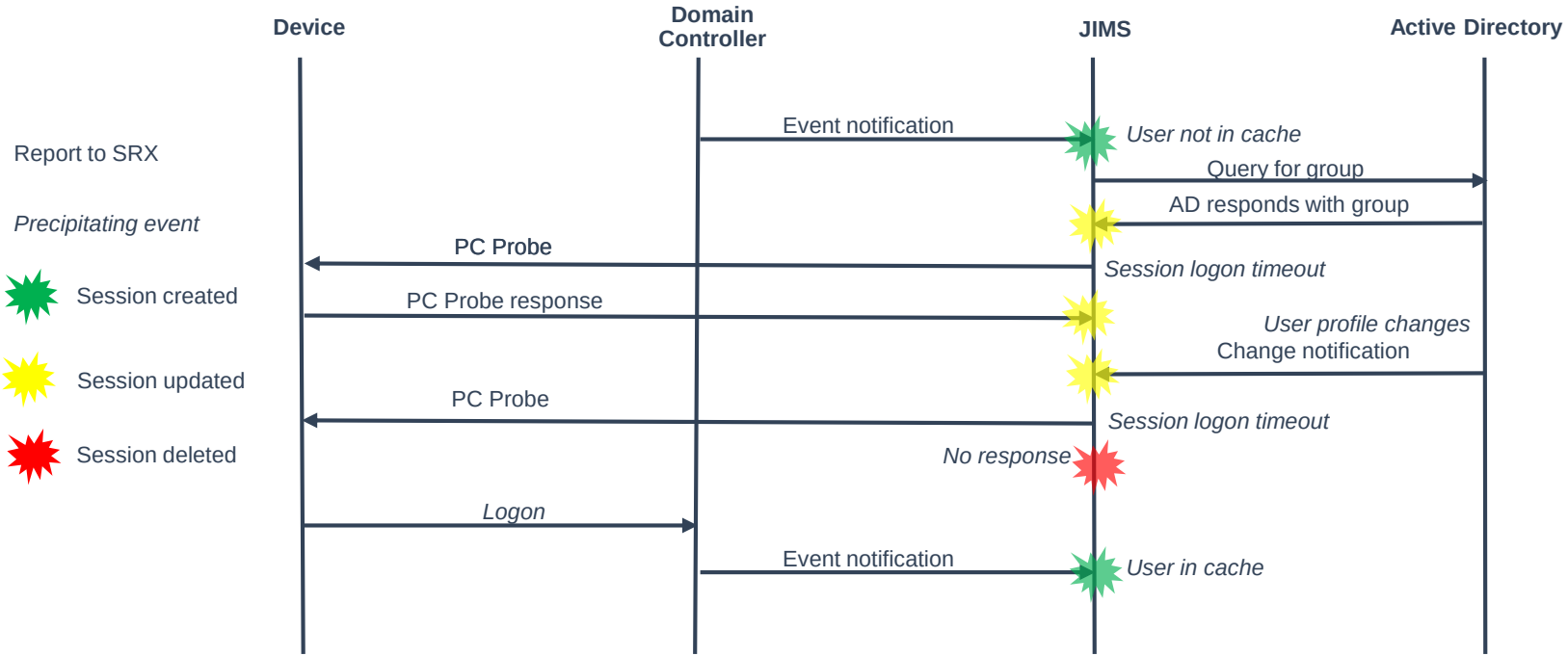


Advanced Query Mode

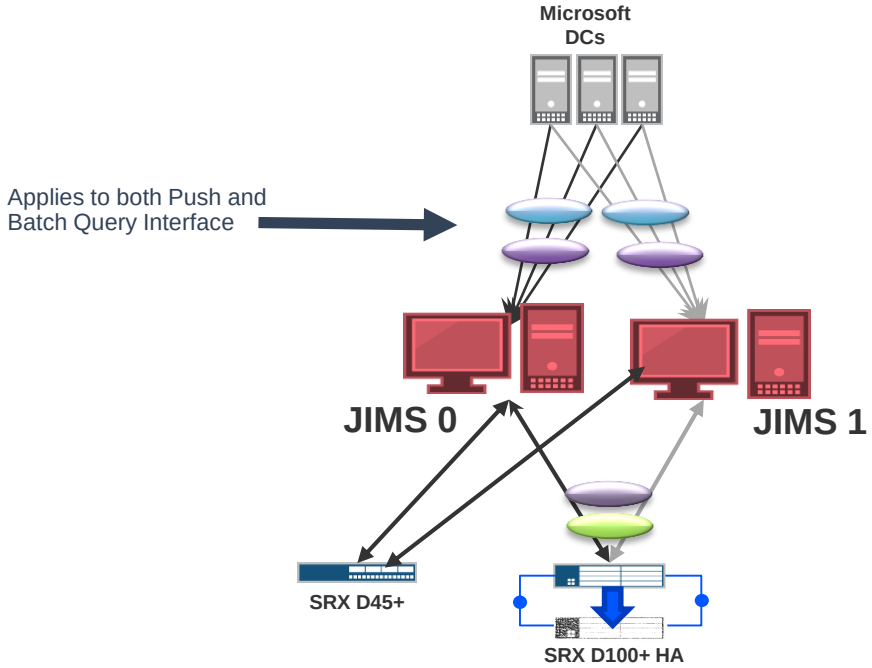
- Pull mode only (batch)
- IP Query
- High Availability support
- Advanced filters
- Device info support
- Support on 15.1X49-D100+
- vSRX, SRX300 Series, SRX1500, SRX4K, SRX5K (RE2)



Session Report Generation

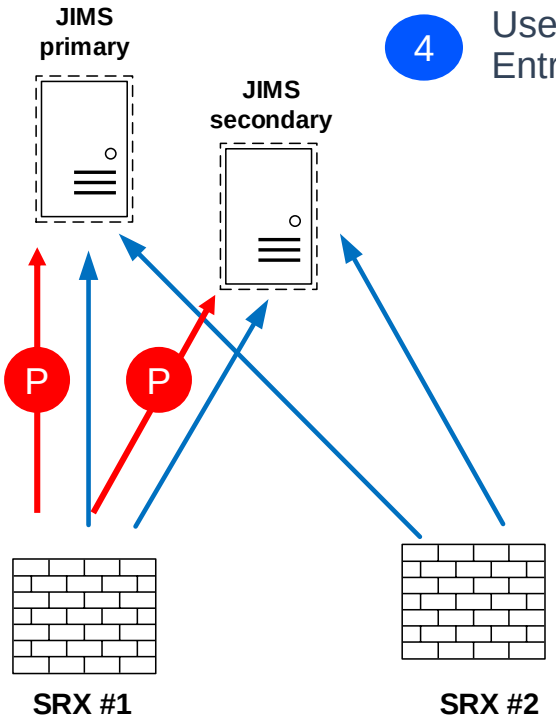


JIMS – Redundancy & Filtering



- Global IP filter
- Global Group filter
- SRX-configured IP filter
- SRX-configured Domain filter

Captive Portal Local Authentication Sharing



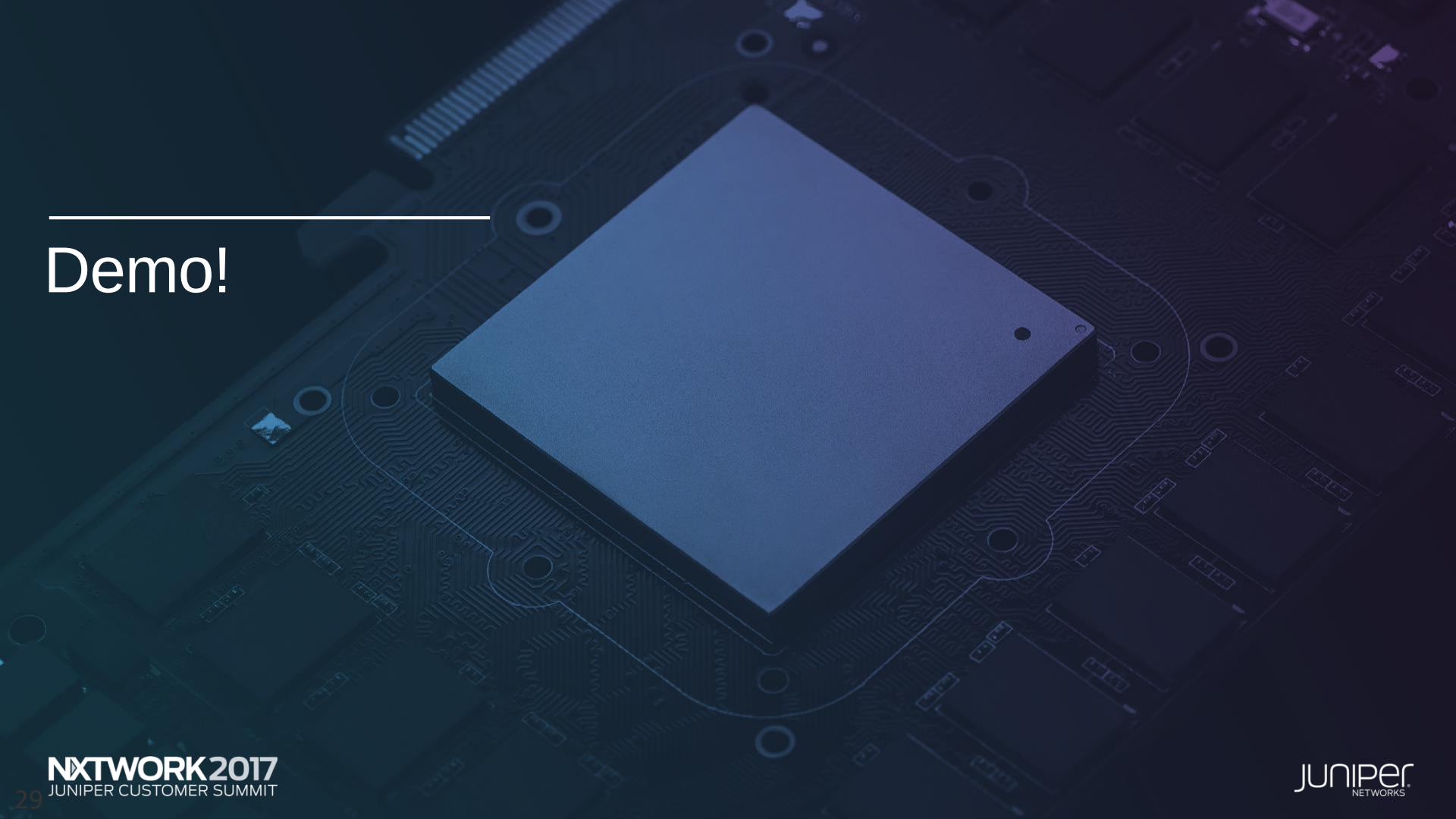
1 User fallback to Captive Portal

2 User authenticate successfully

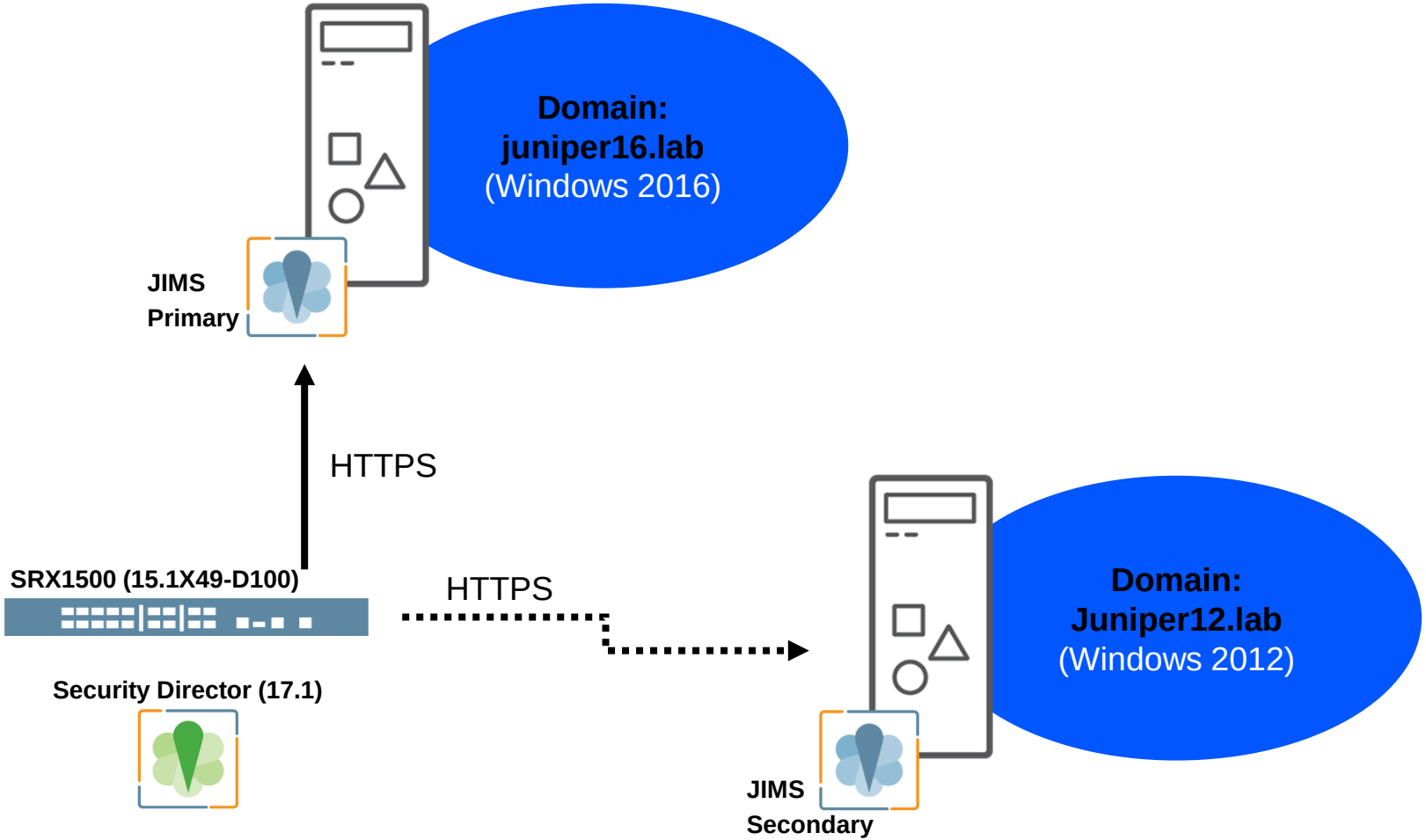
3 IP, User and Dain pushes to JIMS (red)

4 User/Group lookup Entry is cached

5 SRX gets the report



Demo!


Domain:
juniper16.lab
(Windows 2016)
JIMS
Primary
HTTPS
SRX1500 (15.1X49-D100)
HTTPS
Security Director (17.1)
Domain:
Juniper12.lab
(Windows 2012)
JIMS
Secondary

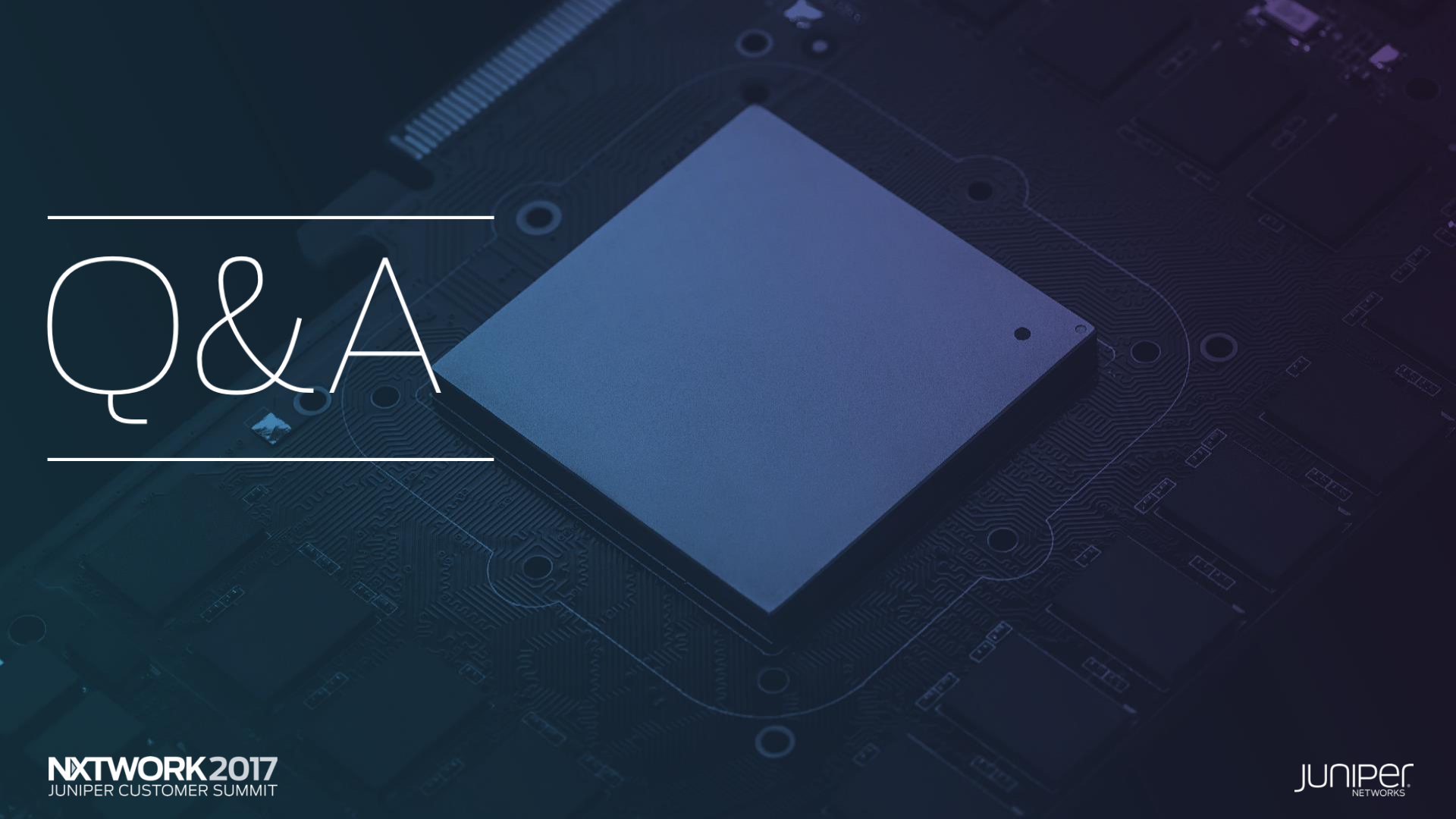
Summary

Takeaways

- Easy to install, easy to setup
- Highly scalable solution
- Does not require one agent per domain
- Visibility & enforcement based on users and devices
- Rich ecosystem: Leverage the right solution for the right need !

Additional resources

- Download available on www.juniper.net
- JIMS Information
  - http://www.juniper.net/us/en/products-services/security/jims/
- JIMS Data Sheet
  - http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000618-en.pdf
- Security Director Information
  - https://www.juniper.net/us/en/products-services/security/security-director/


Q&A


JUNIPER
NETWORKS
THANK YOU!
NXTWORK2017
JUNIPER CUSTOMER SUMMIT