SCAP and the Network Configuration Protocol (NETCONF)
Security Automation Developer Days
July 12, 2012

Luis Nuñez – Apex Assurance Group

David Solin - jOVAL

Chandrashekhar Basavanna - SecPod

SCAP and NETCONF

Further expanding the discussion on inter-networking devices (Routers and Switches) the NETCONF protocol will be discussed. NETCONF is a open standard protocol supported by major inter-networking vendors. This session looks to leveraging the NETCONF schema to retrieve the configuration files from inter-networking devices. This session will cover issues and challenges related to:

- Security Automation and inter-networking devices.
- Access methods to retrieve and process device configuration settings.

NETCONF

- RFC 6241 Network Configuration Protocol

"The Network Configuration Protocol (NETCONF) defined in this document provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages. The NETCONF protocol operations are realized as remote procedure calls (RPCs)."

http://tools.ietf.org/html/rfc6241

- RFC 6242 Using the NETCONF protocol over Secure Shell (SSH)

http://tools.ietf.org/html/rfc6242

Why NETCONF for SCAP?

- Leverage existing mechanisms such as NETCONF, SNMP, etc…
- By design NETCONF is geared for configuration management
- XML based messages and XML based configuration (Xpath)

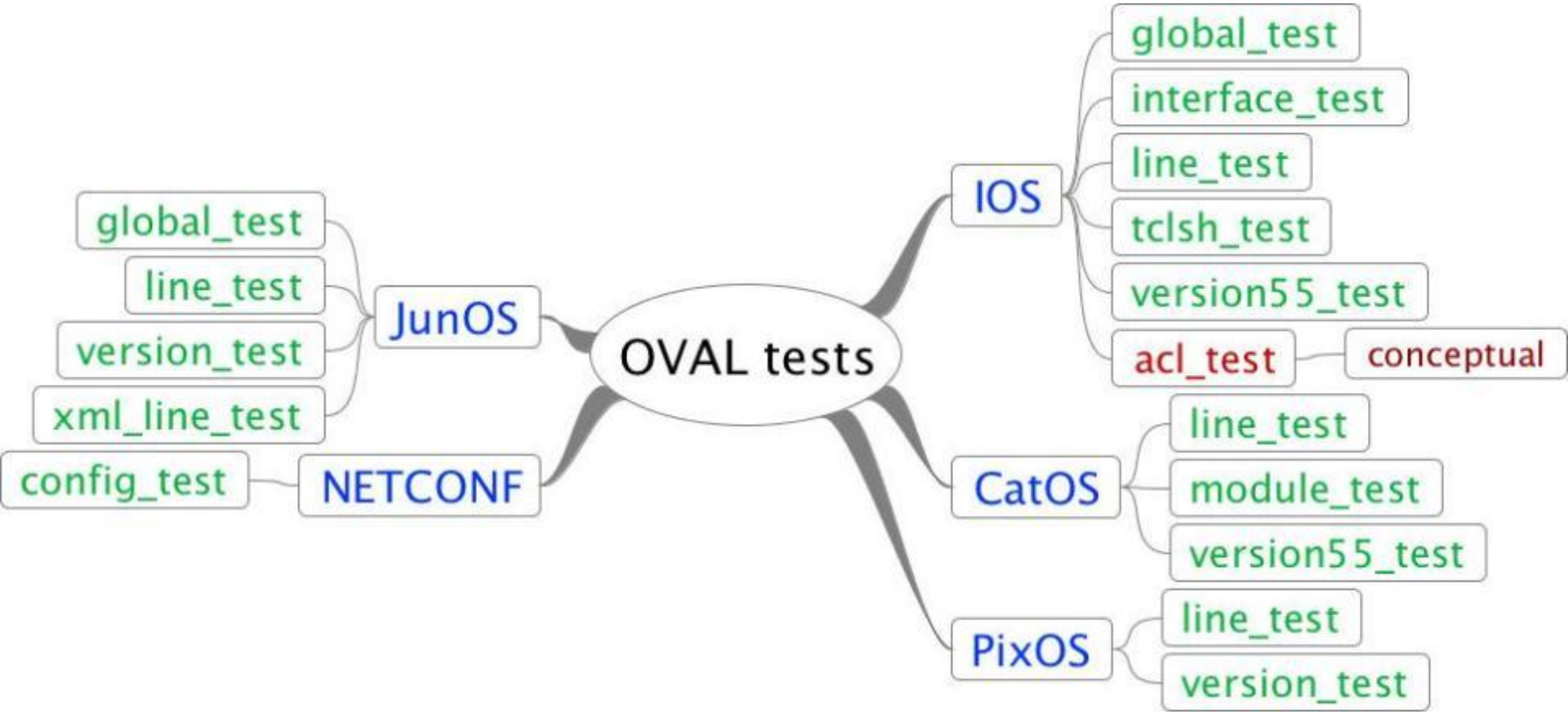
NETCONF capabilities

- Client server RPC based communications
- Request types:
  - <get> configuration and state data
  - <get-config> configuration and state data
  - <edit-config> edit operations conducted on the device
  - <copy-config> create or replace configuration operation
  - <delete-config> delete configuration operation
  - <lock> lock configuration operation to session
  - <unlock> release configuration operation
  - <close-session> graceful session termination
  - <kill-session> Force session termination

NETCONF capabilities

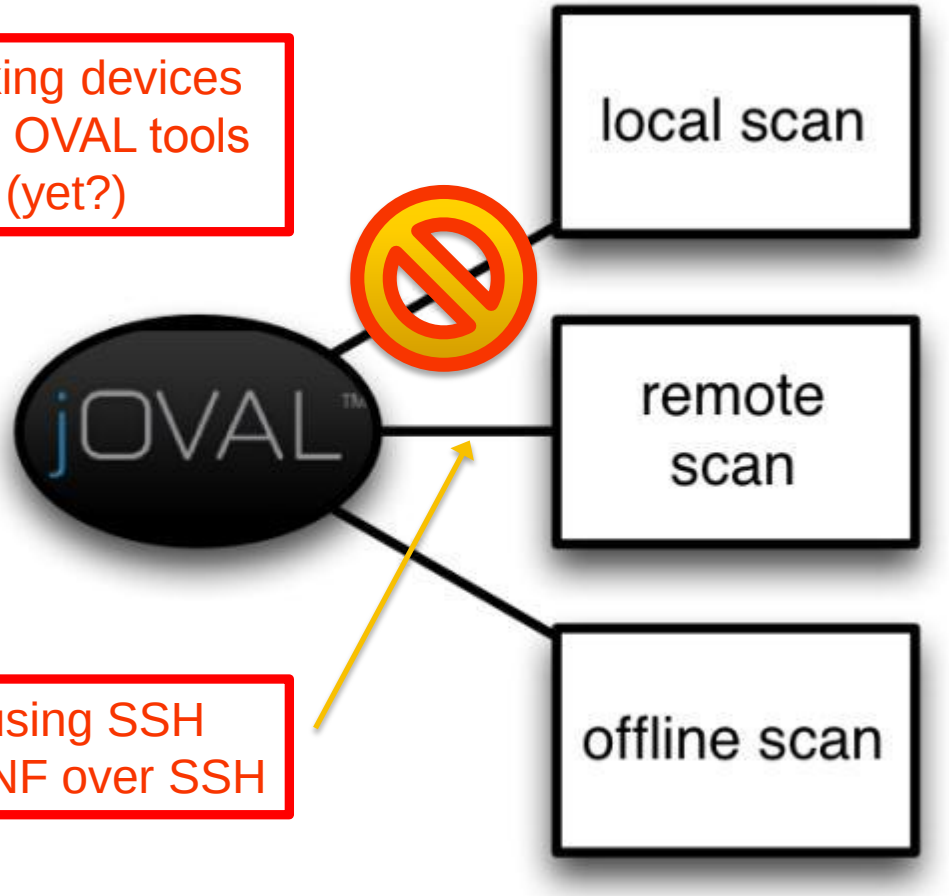
- XML Subtree Filter
- NETCONF sessions
- YANG data models
- SSH 2.0, BEEP, HTTP, TLS
- Vendors that support NETCONF
  - Cisco, Juniper, Brocade …

OVAL tests (Inter-networking devices)



Scanning methods

Inter-networking devices don't support OVAL tools to run locally (yet?)



Connection using SSH and NETCONF over SSH

Demo Content

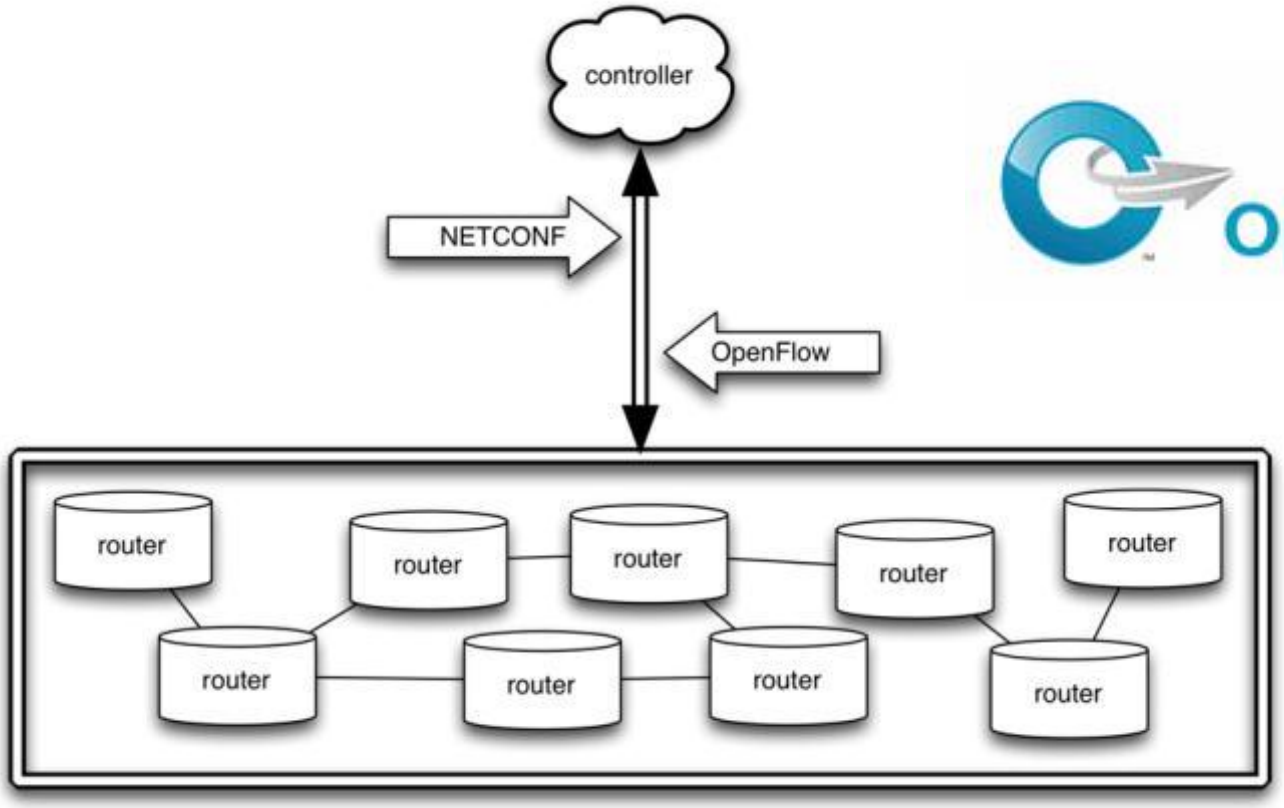
- OVAL NETCONF schema
- OVAL definition
- XCCDF – based on DISA STIG
- CPE
- CCE

NETCONF and Remediation

- Leverage existing protocols suited for remediation
- Remedial aspects of NETCONF
- NETCONF is a protocol that can commit and roll-back changes to configurations
- Ideal for configuration remediation? < thoughts?

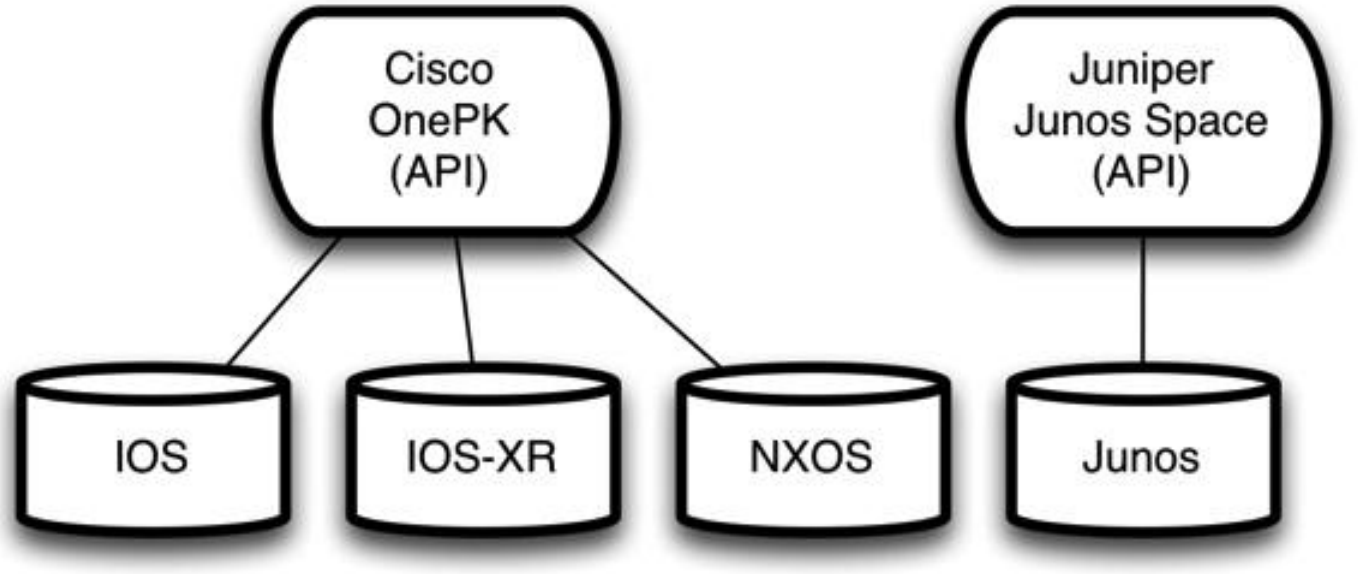
Software Defined Networks (SDN)

- NETCONF is part of the OF-Config 1.1 specification (opennetworking.org)
- Raging debate in the inter-networking industry
- SDN based on OpenFlow protocol (not to be confused with Netflow)
- SDN is about programmability of the inter-networking devices

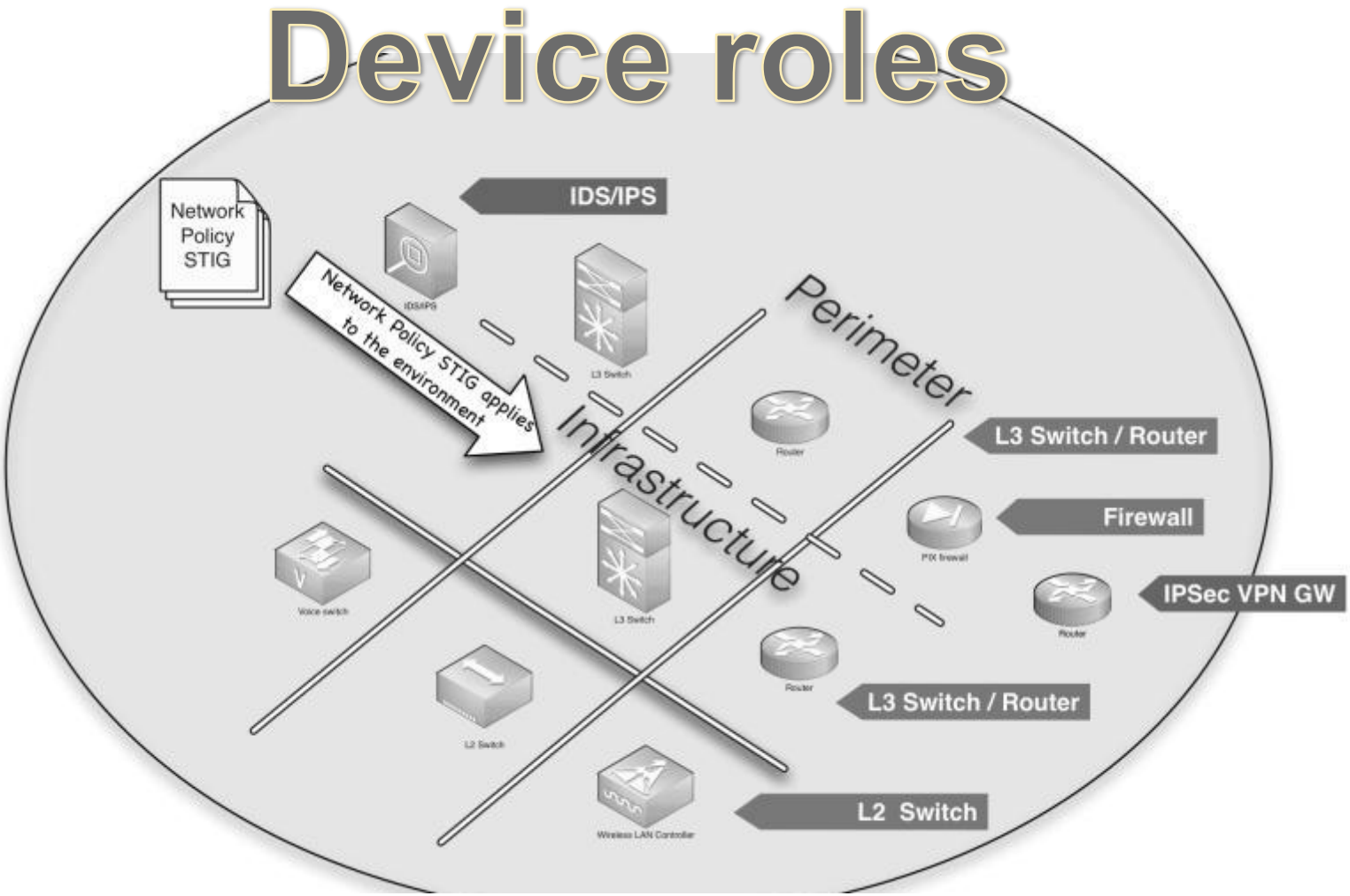


Programmable Networks

- Juniper Junos Space
- Cisco OnePK
- API into programing networks



Network Infrastructure STIG Topology



Thanks

Reference

- www.apexassurance.com
- www.joval.org
  - Tool download http://joval.org/download/mitre
- www.secpod.com
  - Content download http://scaprepo.com/
- Junos STIG reference
  - http://www.c3isecurity.com/home/junos-hardening