# OVAL for Inter-networking Devices
# Security Automation Developer Days
# July 12, 2012

## Project Martini

Luis Nuñez – Apex Assurance Group

David Solin - jOVAL

Chandrashekhar Basavanna - SecPod

# OVAL for Inter-networking Devices

The OVAL specification currently supports a diverse set of platforms. We see Windows and a variety of UNIX operating systems supported of which there is only one Inter-networking platform. Inter-networking devices are routers and switches that connect the Internet. Currently Cisco is only vendor and platform that is represented in the area of inter-networking devices. In this session we propose a new platform to be supported by the OVAL specification. The session will cover new schema, content and tool (jOVALdi) associated with the new platform. The session will also compare similarities between the Cisco IOS schema and the new platform schema.

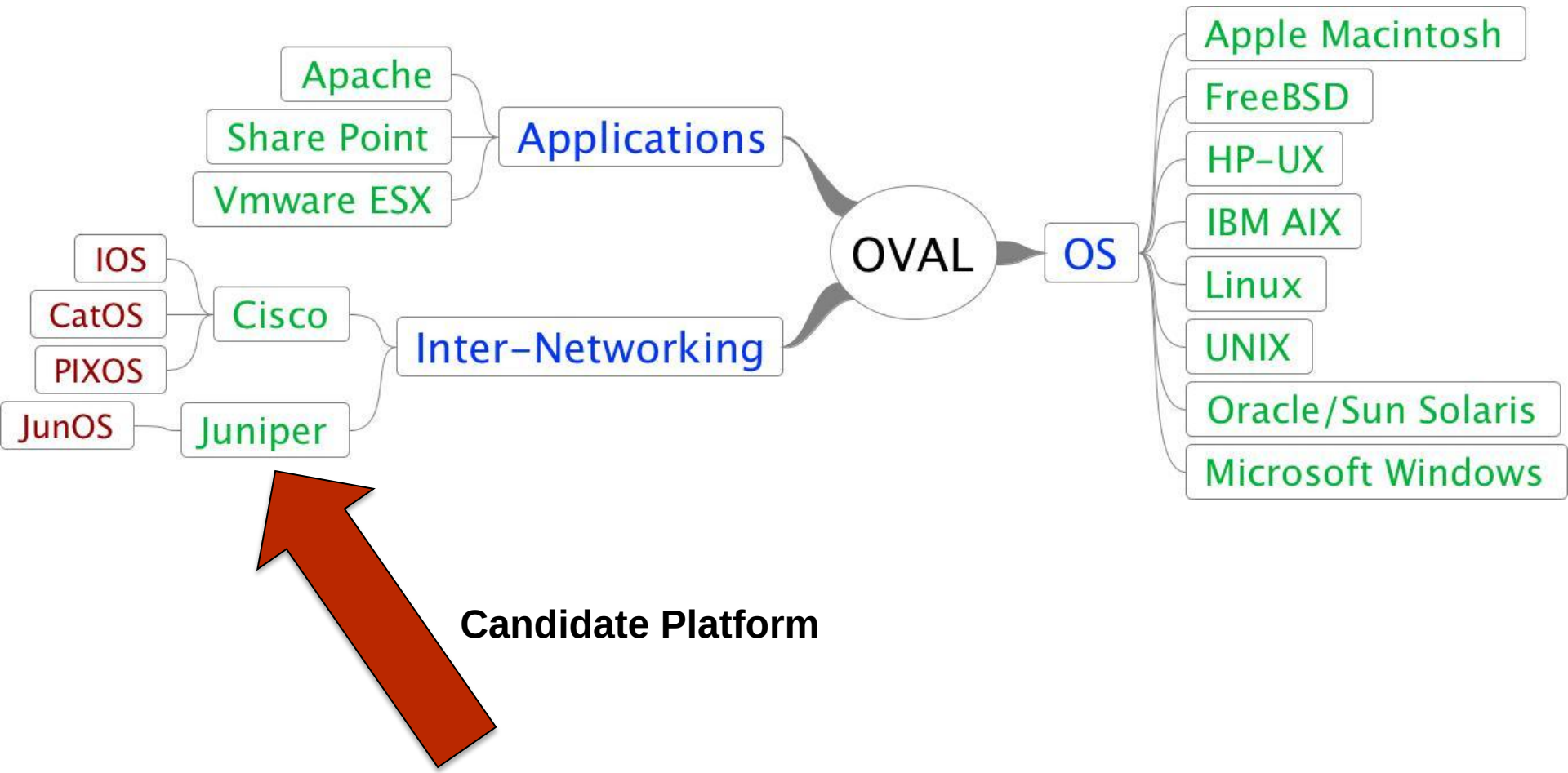
# jOVAL SecPod Apex Assurance

- Collaboration with alignment of interests.
- **Apex Assurance** – Juniper is a good customer to Apex. This was a worth while effort to get Juniper on the SCAP map and also contribute to the community.
- **jOVAL** – Natural to further extend the tool to other networking platforms.
- **SecPod** – Further expand in content capabilities.
- We encourage others to collaborate on common interests.

# Project Martini Goals

- Get Juniper Junos supported in OVAL
- Proof of concept
- “rough consensus and running code”
  - Tool – jOVAL(jovaldi, Xpert)
  - Content OVAL, XCCDF, CCE, CPE
  - Junos OVAL schema
- Acceptance of prototype concept into official OVAL release
- Think big but keep it simple

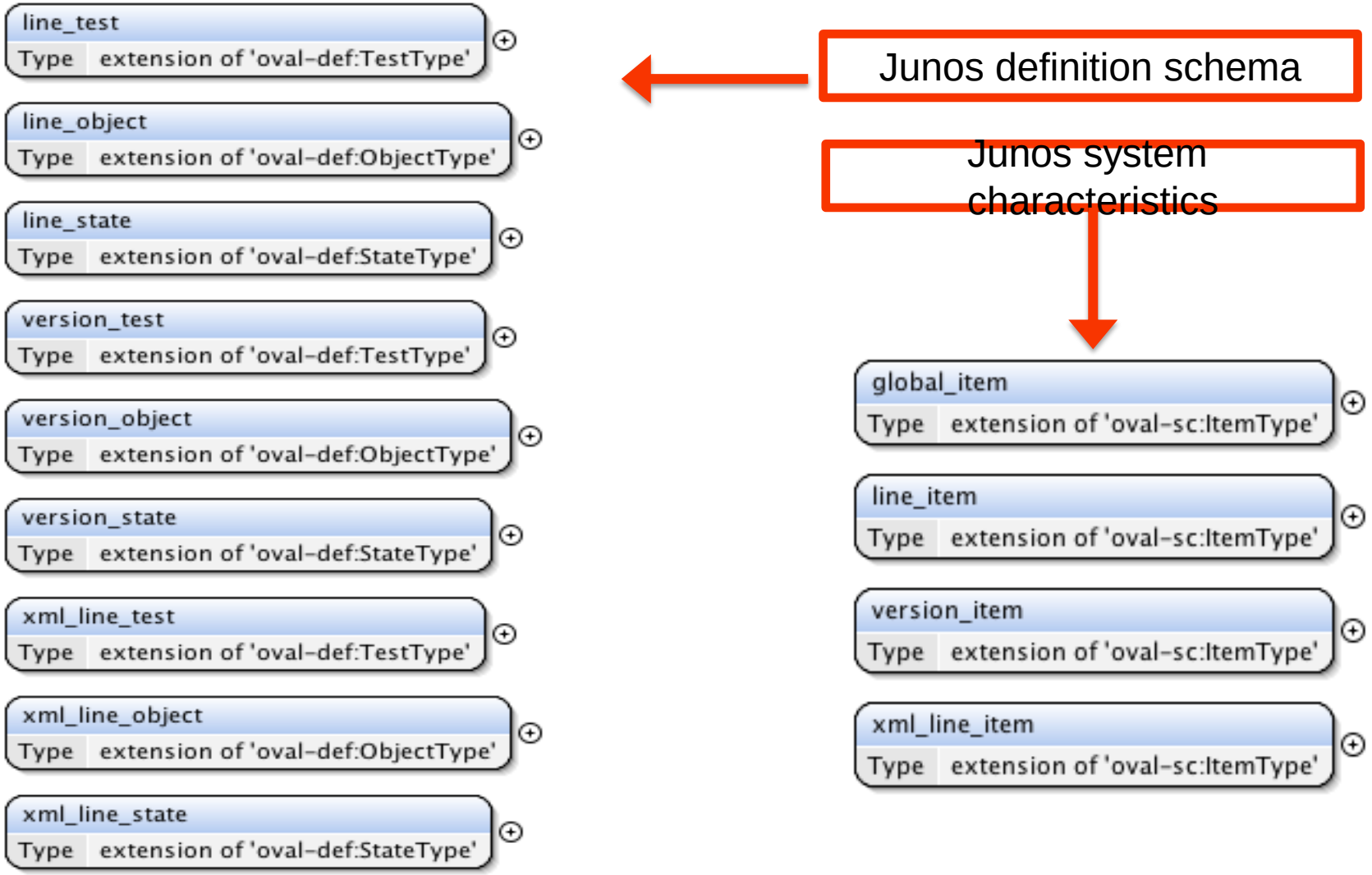
# Current list platforms supported on OVAL



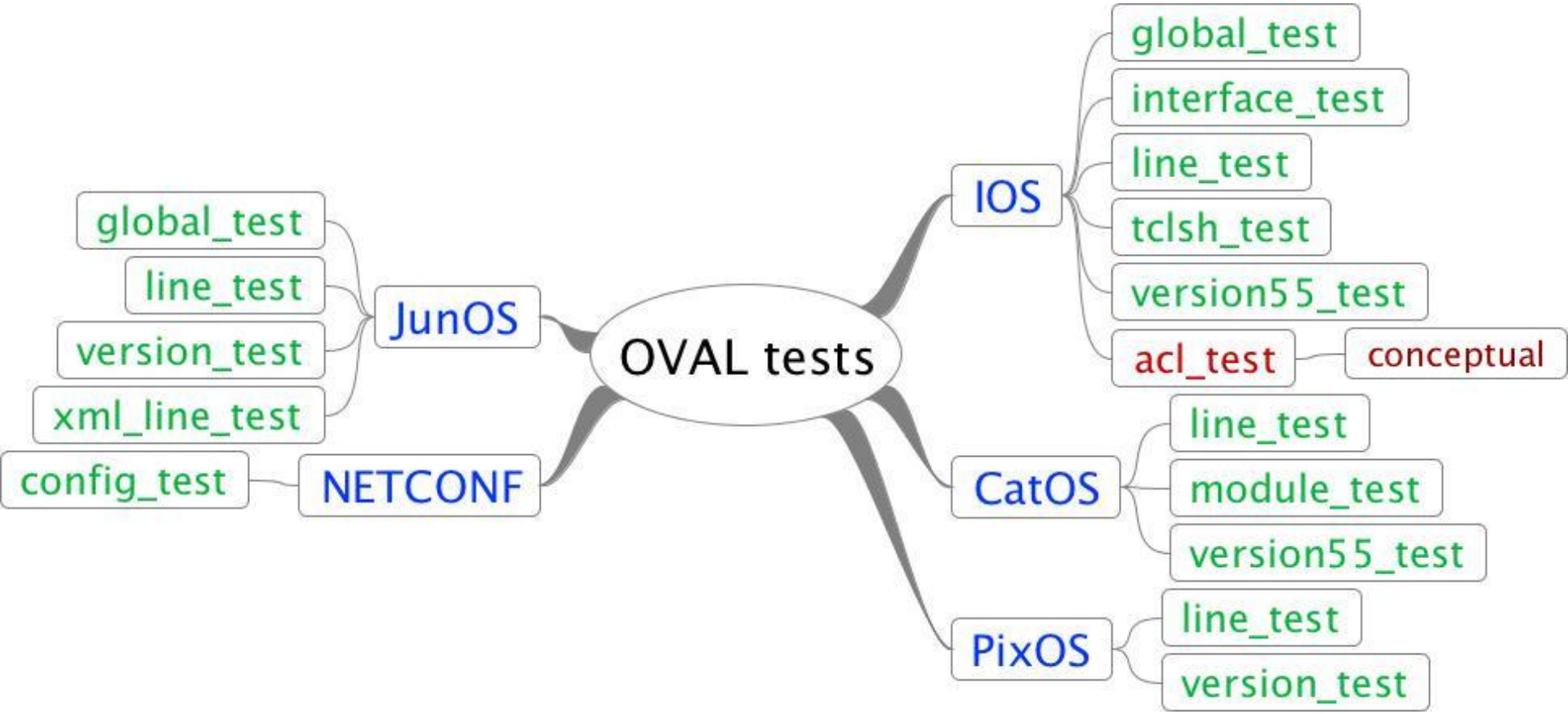
# Ingredients to making this work

- Specification support  for Junos within OVAL
- Content – STIG, SCAP (OVAL, CPE, CCE, XCCDF)
  - SCAP 1.2 data streams
- Tool – jOVAL
  - Xpert
  - Jovaldi

# Juniper Junos OVAL Schema

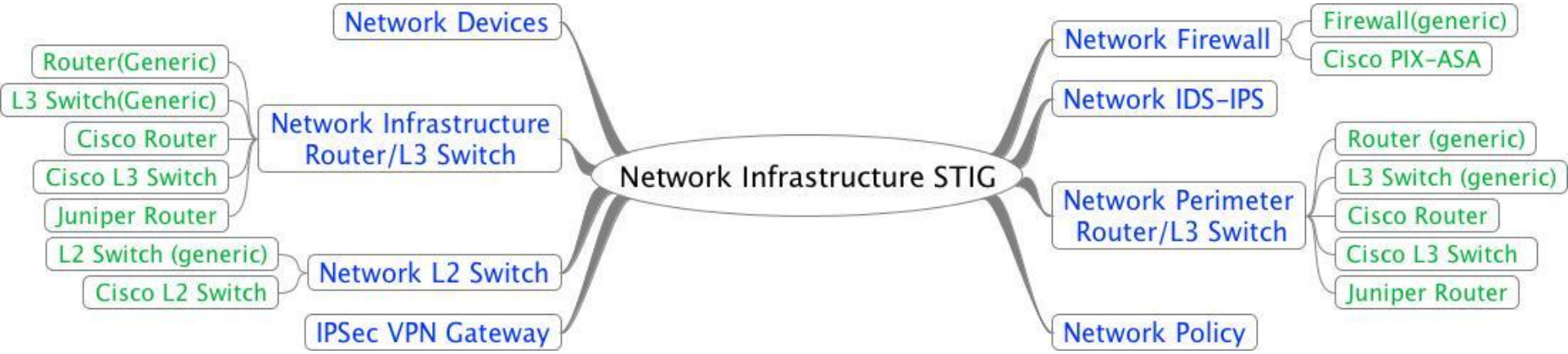


# OVAL tests (Inter-networking devices)



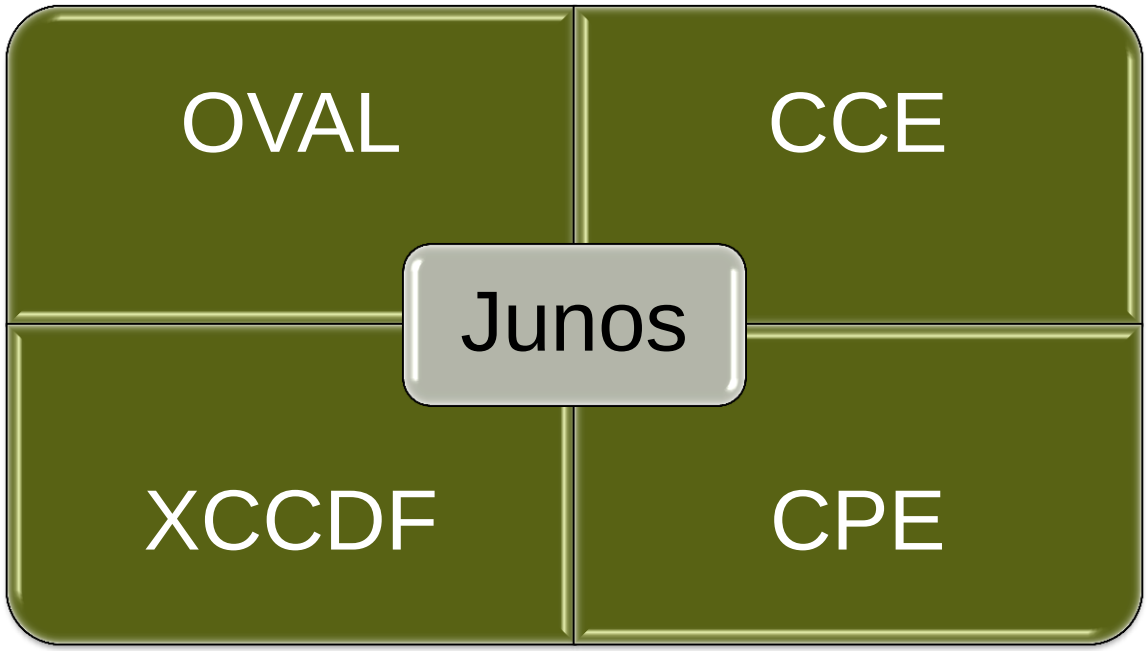
# DISA Network Infrastructure STIG

- Cisco IOS specific checklists (XCCDF)
- Juniper Junos specific checklists (XCCDF)



# Juniper Junos Content – SCAP 1.2 data stream

- sp- junos-cce-xccdf.xml
- sp-junos-cce-oval.xml
- sp-junos-cpe-oval.xml
- sp-junos-cpe-dictionary.xml



# DISA STIG NET0400 test

- STIG ID NET0400 – Interior routing protocols are not authenticated
- Sample Junos CCE
- Junos command line interface (CLI) output
- Curly brace CLI example

```
[edit protocols ospf]
ospf {
    area 0.0.0.0 {
        interface em0.0 {
            authentication {
                md5 1 key "$9$FYPx3tOylMWxdWLkPfQCAxNdV4Z.PQz6Az3vLXN2g69AtIcWLN";
            }
        }
    }
}
```

- set CLI example

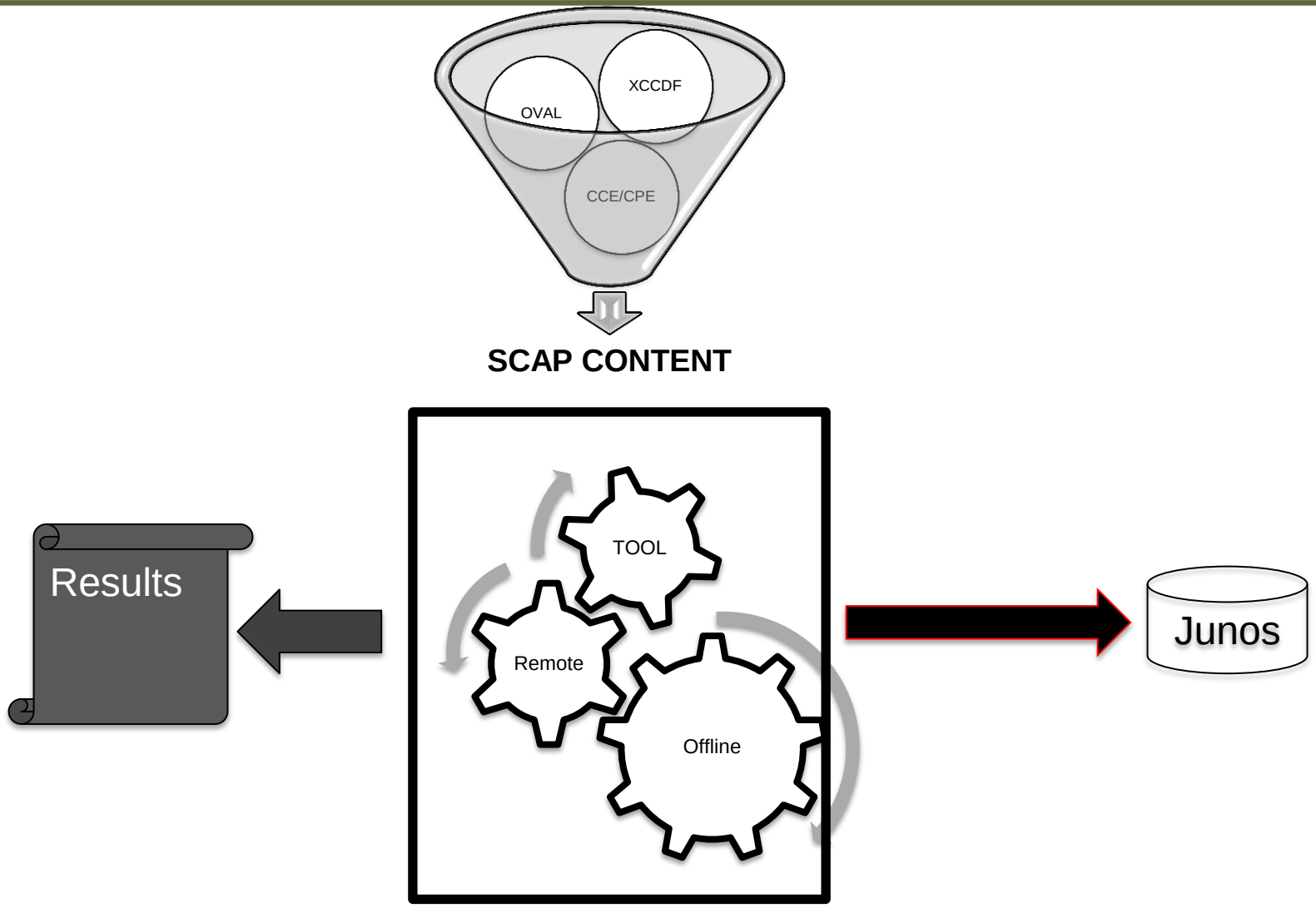
```
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0 authentication md5 1 key
"$9$FYPx3tOylMWxdWLkPfQCAxNdV4Z.PQz6Az3vLXN2g69AtIcWLN"
```

# DISA STIG NET0340 test

- STIG ID NET0340 – Login banner is non-existent or not DOD approved
- Sample Junos CCE
- Simple check
- Variable
- Junos command line interface (CLI) output
- set CLI example

set system login message “test banner page”

# demo



# Demo Content

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

# Challenges and Lessons Learned

- ~~Lack of inter-networking~~ vendors participation in the specifications
- The focus of the specifications on Windows and Linux Operating Systems. Slow adoption to other platforms.
- Incentives to adopt

# 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

# Xpert output transcript

```
>xpert -d def\sp-junos-netconf-datastream-1.1.xml -p xccdf_org.secpod_profile_stig_junos
-plugin remote -config remote-junos.properties -l 1
-------------------------------------------------
XPERT by jOVAL.org
XCCDF Processing Engine and Reporting Tool
Version: 5.10.1.1_Dev
Build date: Fri Jun 22 11:57:19 CDT 2012
Copyright (C) 2012 - jOVAL.org

Plugin: jOVALRemotePlugin by jOVAL.org(TM)
Version: 5.10.1.1_Dev
Copyright (C) 2011, 2012 - jOVAL.org
-------------------------------------------------
```

SCAP 1.2 data stream

XCCDF Profile

Plug options for Remote and offline capabilities

# Xpert output transcript (continued)

Start time: Tue Jun 26 13:07:38 EDT 2012

Loading def\sp-junos-netconf-datastream-1.1.xml

Selected stream scap_org.secpod_datastream_sp-junos-netconf-datastream.zip

Selected benchmark scap_org.secpod_comp_sp-junos-cce-netconf-xccdf.xml

Setting org.joval.ssh.system.SshSession: conn.timeout=3000 [org.joval.intf.ssh.system.ISshSession]

Setting org.joval.ssh.system.SshSession: conn.retries=3 [org.joval.intf.ssh.system.ISshSession]

Setting org.joval.ssh.system.SshSession: attach.log=false [org.joval.intf.ssh.system.ISshSession]

Setting org.joval.ssh.system.SshSession: exec.retries=1 [org.joval.intf.ssh.system.ISshSession]

Setting org.joval.ssh.system.SshSession: debug=false [org.joval.intf.system.IBaseSession]

Setting org.joval.ssh.system.SshSession: read.timeout.small=15000 [org.joval.intf.system.IBaseSession]

Setting org.joval.ssh.system.SshSession: read.timeout.large=900000 [org.joval.intf.system.IBaseSession]

Setting org.joval.ssh.system.SshSession: read.timeout.medium=120000 [org.joval.intf.system.IBaseSession]

Setting org.joval.ssh.system.SshSession: read.timeout.xl=3600000 [org.joval.intf.system.IBaseSession]

Credential set for 172.16.177.25

Auth: Banner Page

# Xpert output transcript (continued)

Established SSH connection to host 172.16.177.25

Starting process: pwd

Starting process: show version

Junos CLI “show version details”

Setting org.joval.os.juniper.system.JunosSession: debug=false [org.joval.intf.system.IBaseSession]

Setting org.joval.os.juniper.system.JunosSession: read.timeout.small=15000 [org.joval.intf.system.IBaseSession]

Setting org.joval.os.juniper.system.JunosSession: read.timeout.large=900000 [org.joval.intf.system.IBaseSession]

Setting org.joval.os.juniper.system.JunosSession: read.timeout.medium=120000 [org.joval.intf.system.IBaseSession]

Setting org.joval.os.juniper.system.JunosSession: read.timeout.xl=3600000 [org.joval.intf.system.IBaseSession]

Credential set for 172.16.177.25

# Xpert output transcript (continued)

There are 4 rules to process for the selected profile

Starting process: request support information

Determining system applicability...

CPE check

Evaluating definition oval:org.secpod.devel.oval:def:10

Evaluating oval:org.secpod.devel.oval:def:10

Evaluating test oval:org.secpod.devel.oval:tst:10

Scanning object oval:org.secpod.devel.oval:obj:10

Scanning object oval:org.secpod.devel.oval:obj:10

NETCONF session ID: 1441

NETCONF session

Passed def oval:org.secpod.devel.oval:def:10

The target system is applicable to the specified XCCDF

# Xpert output transcript (continued)

Creating engine for href sp-junos-cce-netconf-oval.xml
Evaluating OVAL rules
Beginning scan
Evaluating definitions
Evaluating definition oval:org.secpod.devel.oval:def:303
Evaluating oval:org.secpod.devel.oval:def:303
Evaluating definition oval:org.secpod.devel.oval:def:10
Evaluating oval:org.secpod.devel.oval:def:10
Evaluating test oval:org.secpod.devel.oval:tst:10
Scanning object oval:org.secpod.devel.oval:obj:10
Scanning object oval:org.secpod.devel.oval:obj:10
Evaluating test oval:org.secpod.devel.oval:tst:303
Scanning object oval:org.secpod.devel.oval:obj:303
Scanning object oval:org.secpod.devel.oval:obj:303
Evaluating definition oval:org.secpod.devel.oval:def:302
Evaluating oval:org.secpod.devel.oval:def:302
Evaluating test oval:org.secpod.devel.oval:tst:302
Scanning object oval:org.secpod.devel.oval:obj:302
Scanning object oval:org.secpod.devel.oval:obj:302
Evaluating definition oval:org.secpod.devel.oval:def:301
Evaluating oval:org.secpod.devel.oval:def:301
Evaluating test oval:org.secpod.devel.oval:tst:301
Scanning object oval:org.secpod.devel.oval:obj:301
Scanning object oval:org.secpod.devel.oval:obj:301
Evaluating definition oval:org.secpod.devel.oval:def:300
Evaluating oval:org.secpod.devel.oval:def:300
Evaluating test oval:org.secpod.devel.oval:tst:300
Scanning object oval:org.secpod.devel.oval:obj:300
Scanning object oval:org.secpod.devel.oval:obj:300
Scan complete

OVAL checks

# Xpert output transcript (continued)

Completed evaluating definitions

Evaluating SCE rules 


SSH disconnecting from host 172.16.177.25

xccdf_org.secpod_rule_xccdf_netconf_junos_rule_scap_for_internetwork_devices_CCE-JunOS-1001: FAIL

xccdf_org.secpod_rule_xccdf_netconf_junos_rule_scap_for_internetwork_devices_CCE-JunOS-1002: FAIL

xccdf_org.secpod_rule_xccdf_netconf_junos_rule_scap_for_internetwork_devices_CCE-JunOS-1003: FAIL

xccdf_org.secpod_rule_xccdf_netconf_junos_rule_scap_for_internetwork_devices_CCE-JunOS-1004: PASS XCCDF processing complete.

Saving report: .\xccdf-results.xml

Transforming to HTML report: xccdf-result.html

Finished processing XCCDF bundle

# Junos OVAL vulnerability results

**OVAL Definition Results**

True | False | Error | Unknown | Not Applicable | Not Evaluated

| ID | Result | Class | Reference ID | Title |
|---|---|---|---|---|
| oval:org.secpod.devel.oval:def:10 | true | inventory | cpe:/o:juniper:junos | Juniper JUNOS installed |
| oval:org.secpod.devel.oval:def:13 | false | vulnerability | CVE-2009-3485 | Cross-site scripting (XSS) vulnerability in the J-Web interface in Juniper JUNOS 8.5R1.14 and 9.0R1.1 via PATH_INFO |
| oval:org.secpod.devel.oval:def:12 | false | vulnerability | CVE-2009-3487 | Multiple cross-site scripting (XSS) vulnerabilities in the J-Web interface in Juniper JUNOS 8.5R1.14 |
| oval:org.secpod.devel.oval:def:11 | false | vulnerability | CVE-2009-3486 | Multiple cross-site scripting (XSS) vulnerabilities in the J-Web interface in Juniper JUNOS 8.5R1.14 |

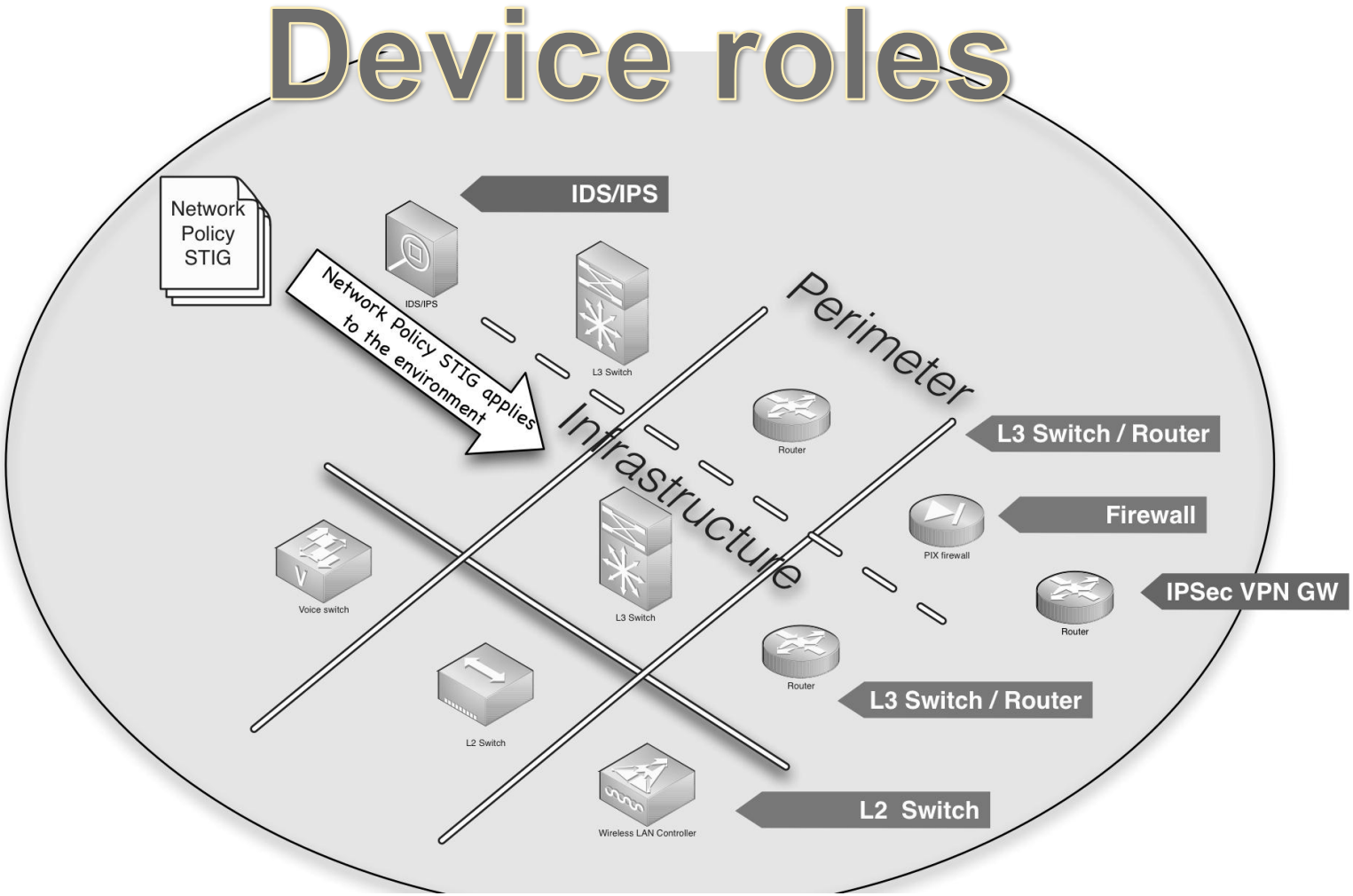
# Xpert Junos STIG XCCDF results

**Benchmark Test Results**

Pass | Fail | Error | Unknown | Not Applicable | Not Checked | Not Selected | Informational | Fixed

| Rule ID | Result | Reference ID | Title |
|---|---|---|---|
| xccdf_org.secpod_rule_xccdf_netconf_junos_rule_scap_for_internetwork_devices_CCE-JunOS-1001 | fail | CCE-JunOS-1001 | NET0400 - Interior routing protocols are not authenticated. |
| xccdf_org.secpod_rule_xccdf_netconf_junos_rule_scap_for_internetwork_devices_CCE-JunOS-1002 | fail | CCE-JunOS-1002 | NET-IPV6-059 - Maximum hop limit is less than 32. |
| xccdf_org.secpod_rule_xccdf_netconf_junos_rule_scap_for_internetwork_devices_CCE-JunOS-1003 | fail | CCE-JunOS-1003 | NET-IPV6-034 - IPv6 Egress Outbound Spoofing Filter |
| xccdf_org.secpod_rule_xccdf_netconf_junos_rule_scap_for_internetwork_devices_CCE-JunOS-1004 | pass | CCE-JunOS-1004 | NET-IPV6-025 - IPv6 Site Local Unicast ADDR must not be defined |

# Network Infrastructure STIG Topology



# Lack of support for Inter-networking devices

- OVAL board members: Tool Vendors, OS Vendors, Others
- No Incentives?
- Is there demand for (OVAL) routers and switches? Yes