

SCAP for Inter-networking devices

Luis Nuñez

7th Annual IT Security Automation
Conference 2011

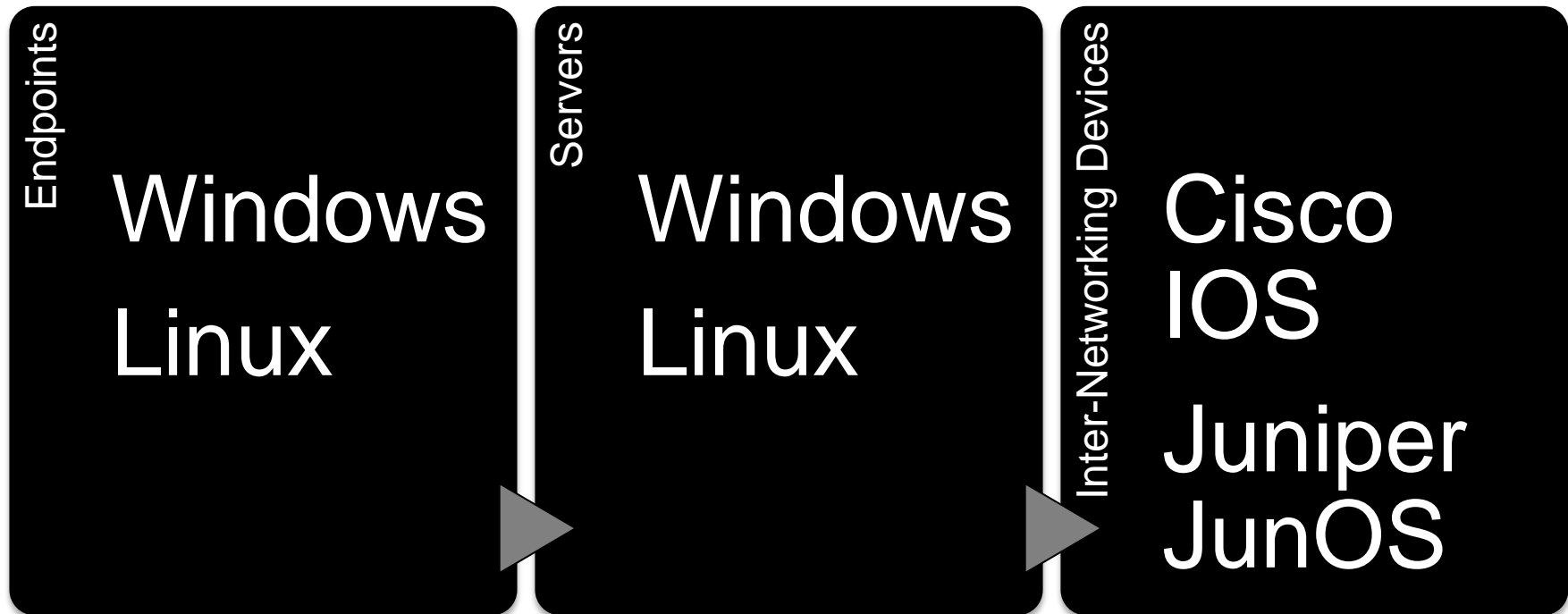
SCAP for Inter-networking devices

Survey on SCAP for inter-networking devices such as routers and switches. The critical infrastructure and enterprise networks today are built on routers and switches to transport communications to endpoints and beyond. SCAP expansion into discovering and interrogating inter-networking devices fits into this continuous monitoring paradigm. The presentation will cover traditional SCAP methods used to probe devices and will discuss other methods. The presentation will also will explore current and future SCAP capabilities for inter-networking devices.

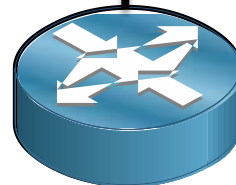
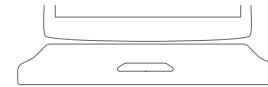
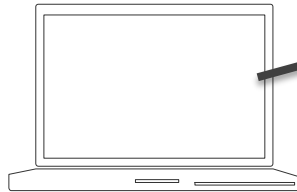
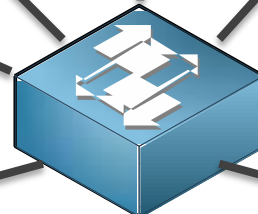
Apex Assurance Group

- Product Security Assurance
- FIPS-140
- Common Criteria
- DoD Information Assurance (IA)
- Security Technical Implementation Guide (STIG)
- Security Content Automation Protocol (SCAP)

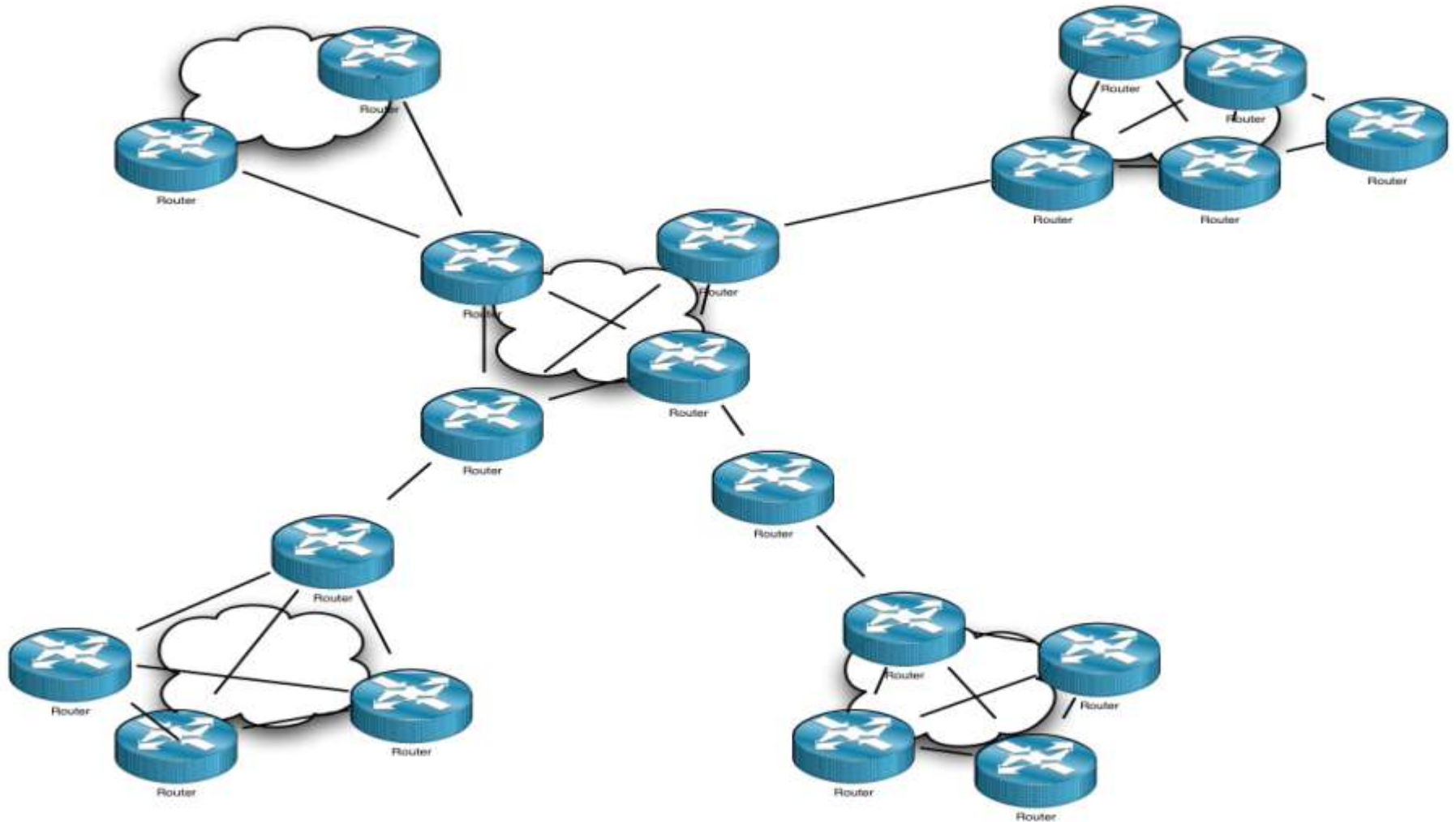
SCAP



Endpoints

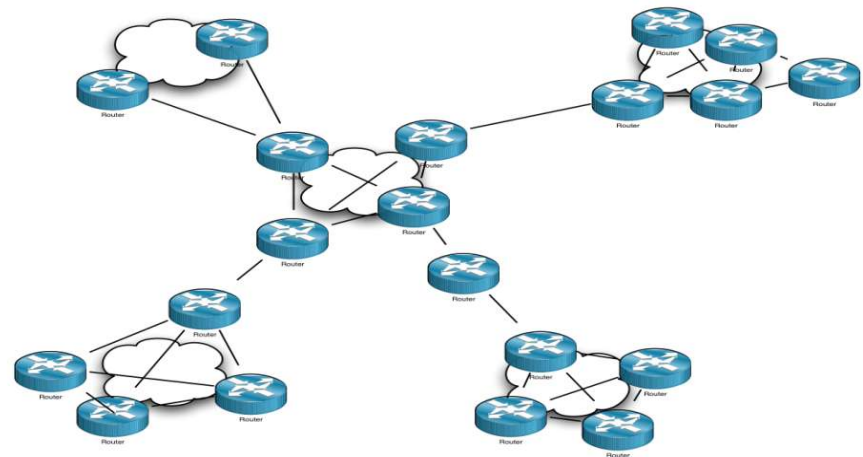
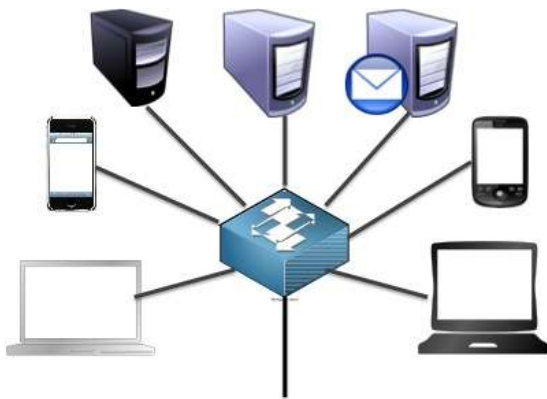


The Network Infrastructure



Differences: endpoints and Inter-Networking devices

- Data flows through and transits Inter-networking devices.
- Router/Switch config usually static.
- Inter-networking devices
 - Intermediary/transit devices
 - The network is the information highway for the endpoints



Why SCAP for inter-networking devices

- Anyone can write scripts to check the system?
 - RAT Perl script
 - TCL
- DISA STIG/XCCDF
- Leverage existing standards for consistent authoritative results

2 SCAP use cases

- Configuration Hygiene
 - Security Best practices (STIG)
 - Cisco IOS Check-list
 - Juniper JUNOS Check-list
- Vulnerability Check
 - IOS OVAL content

Cisco IOS OVAL content

Total: 137 definitions

1 2 3 Next >

Last >>

Definition Id	Class	Title	Last Modified ▼	Ref-Id
oval:org.mitre.oval:def:12043	V	Cisco IOS Software Mobile IP and Mobile IPv6	2010-11-17	CVE-2009-0634
oval:org.mitre.oval:def:12290	V	Cisco IOS Mobile IP NAT and IPv6	2010-11-17	CVE-2009-0633
oval:org.mitre.oval:def:5075	V	Cisco IOS Session Initiation Protocol (SIP) Packet Code Execution Vulnerability	2010-07-16	CVE-2007-4295
oval:org.mitre.oval:def:6087	V	Cisco IOS Processing SSL Packet Vulnerability	2010-07-16	CVE-2008-3798
oval:org.mitre.oval:def:5889	V	Cisco IOS Session Initiation Protocol Denial of Service Vulnerability	2010-07-16	CVE-2008-3802
oval:org.mitre.oval:def:6047	V	Cisco IOS Session Initiation Protocol Denial of Service Vulnerability	2010-07-16	CVE-2008-3801
oval:org.mitre.oval:def:5927	V	Cisco IOS Session Initiation Protocol Denial of Service Vulnerability	2010-07-16	CVE-2008-3799
oval:org.mitre.oval:def:5785	V	Multiple Vendors Net-SNMPv3 Hash Message Authentication Code Design Error Vulnerability	2010-07-16	CVE-2008-0960
oval:org.mitre.oval:def:6086	V	Cisco IOS Session Initiation Protocol Denial of Service Vulnerability	2010-06-02	CVE-2008-3800
oval:org.mitre.oval:def:6058	V	Cisco IOS IPS Denial of Service Vulnerability	2010-06-02	CVE-2008-2739
oval:org.mitre.oval:def:5858	V	Cisco IOS Fragmented Packet IPS Evasion Vulnerability	2010-05-26	CVE-2007-0917
oval:org.mitre.oval:def:5138	V	Cisco IOS Device SIP Support DoS Vulnerability	2010-05-26	CVE-2007-0648
oval:org.mitre.oval:def:5781	V	Cisco IOS Session Initiation Protocol (SIP) Packet DoS Vulnerability	2010-05-26	CVE-2007-4292
oval:org.mitre.oval:def:5851	V	Cisco IOS Session Initiation Protocol (SIP) Packet Arbitrary Code Execution Vulnerability	2010-05-26	CVE-2007-4294
oval:org.mitre.oval:def:5188	V	Cisco 7600, Catalyst 6000 and 6500 Network Analysis Module SNMP Message Spoofing Vulnerability	2010-05-26	CVE-2007-1257
oval:org.mitre.oval:def:5910	V	Cisco 10000, uBR10012, uBR7200 Series Devices IPC Vulnerability	2010-05-26	CVE-2008-3805
oval:org.mitre.oval:def:7254	V	Cisco IOS zone based sip inspection vulnerability	2010-05-13	CVE-2009-2867

JunOS Network Time Protocol (NTP) hardening

- CCE example related to STIG

```
system {  
    ntp {  
        authentication-key [key-id] type md5 value "[pass-  
phrase]";  
        trusted-key [key-id];  
        /* Allow NTP to sync if server clock is  
        significantly different than local clock */  
        boot-server 192.0.2.1;  
        /* NTP server to sync to */  
        server 192.0.2.1;  
        server 192.0.2.2 key [key-id] prefer;  
    }  
}
```

CCI/STIG NET0813

CCE

CCE

CCE

*Sample from team cymru

Cisco IOS Network Time Protocol hardening

- CCE example related to STIG

CCI/STIG
NET0813

```
!enable NTP authentication
```

CCE

```
ntp authenticate
```

```
ntp authentication-key [key-id] md5 [hash]
```

CCE

```
ntp trusted-key [key-id]
```

```
ntp peer [peer_address] key [key-id]
```

CCE

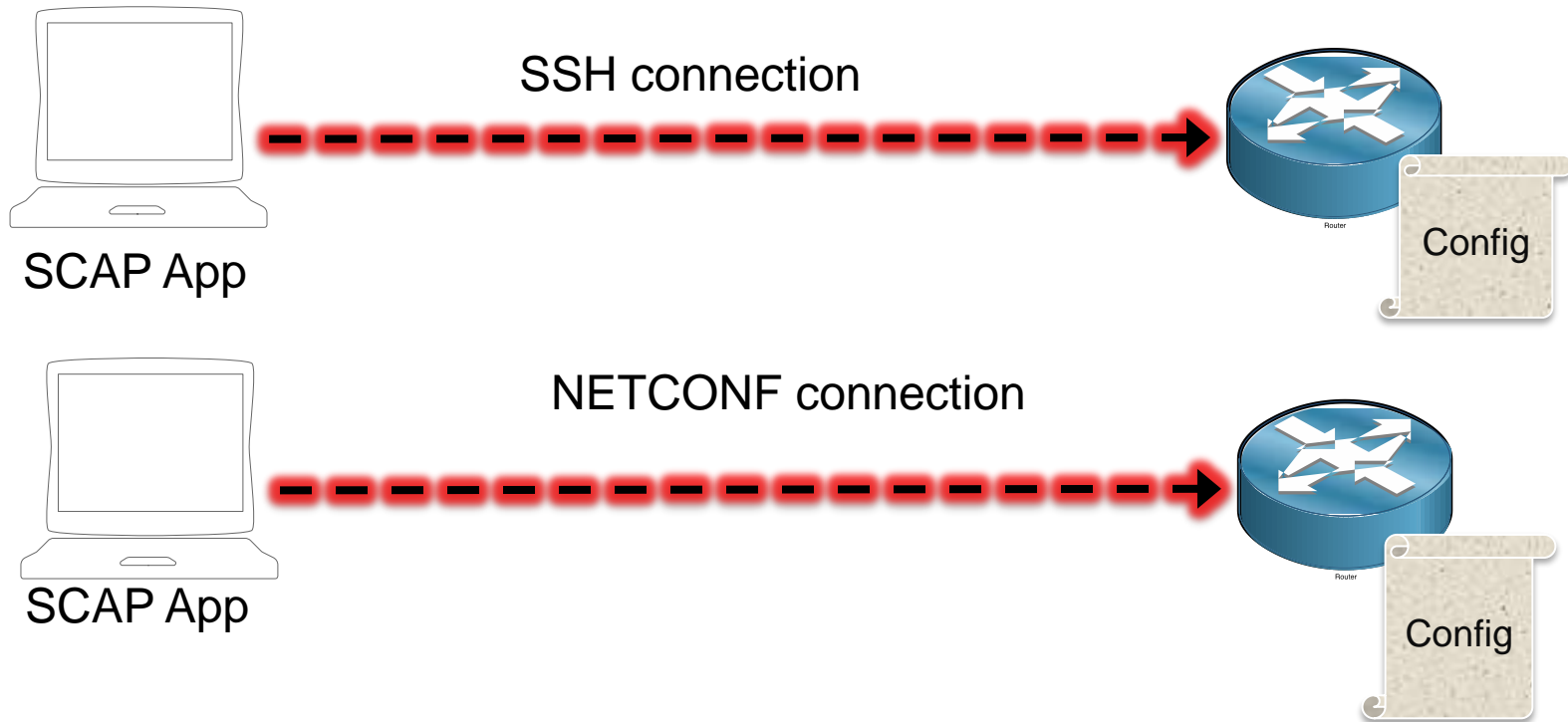
```
ntp server [server_address] key [key-id]
```

*Sample from team cymru

Device access methods

- SSH
- NETCONF
- SNMP
- RESTful

Direct connect Methods



NETCONF

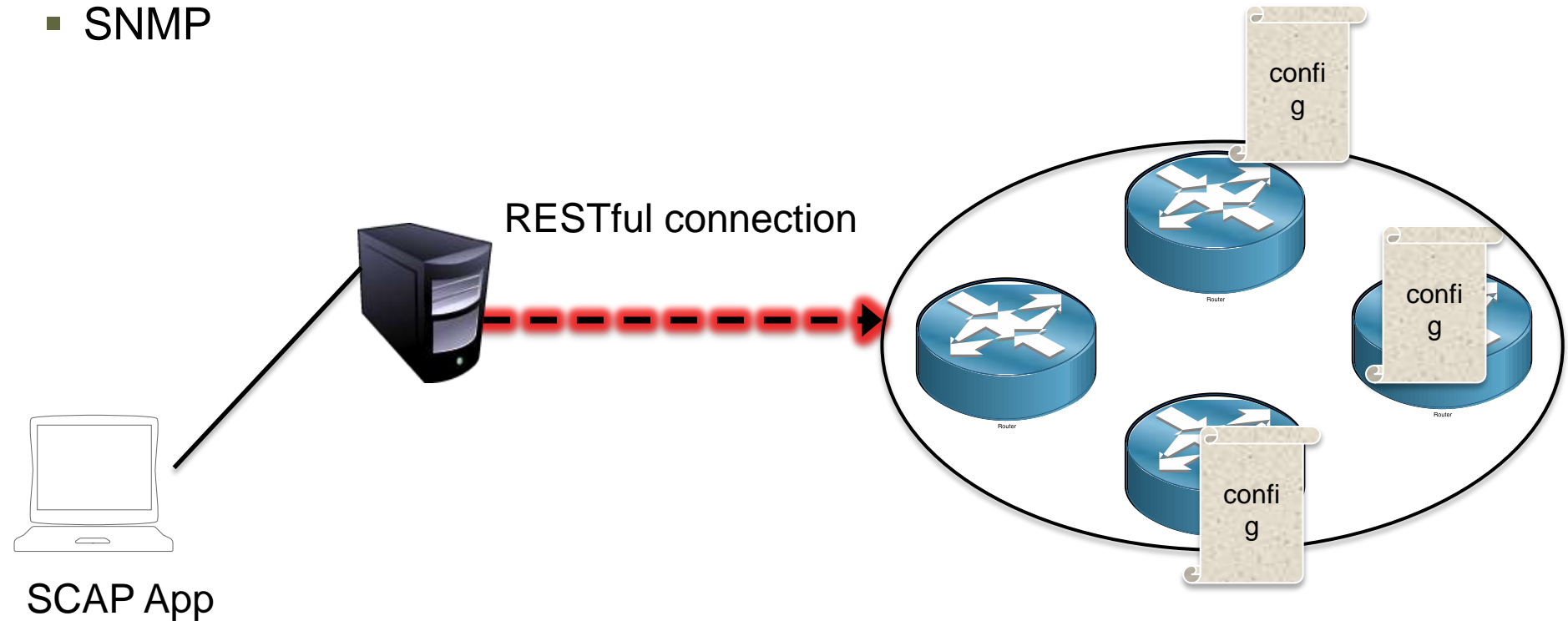
- RFC 6241 Network Configuration Protocol

“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>

Leverage existing network management tools

- RESTful HTTP based
- JunOS Spaces
- SNMP



- Online and offline OVAL analysis
- online direct connection and probe of the device
- offline parsing of system config and state information
- Leveraging existing network management systems for system information
- On box agents
 - Cisco IOS TLC parser
 - Cisco Embedded Event Manager (EEM)

Challenges

- Content contribution
- Vendor participation
- Network device role
 - Edge Router/Filter Router/L3/L2/Purpose device (Voice GW)
- Virtualization
- IOS CPE
- OVAL test content for Inter-networking devices

Future

- EMAP - Events of interests from a network perspective
- Trusted Computing Group –Trusted Network Connect and SCAP
- TMSAD Trust Model for Security Automation Data
 - <http://csrc.nist.gov/publications/nistir/ir7802/NISTIR-7802.pdf>
- SCAP for NIAP Common Criteria Protection Profile



Luis Nuñez

lnunez@apexassurance.com

lnunez@c3isecurity.com

www.apexassurance.com

Cisco IOS Tips

- `show running-config` – outputs the current running configuration (in memory)
- `show startup-config` – outputs the last saved configuration
- `show running-config all` – outputs all configuration include some defaults
- `show tech-support` – outputs vital statics
- `show version`

Cisco IOS show version

```
splinter1#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9-M), Version 15.0(1)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Thu 28-Oct-10 17:09 by prod_rel_team
```

```
ROM: System Bootstrap, Version 12.3(8r)T7, RELEASE SOFTWARE (fc1)
```

```
splinter1 uptime is 12 weeks, 6 days, 3 hours, 13 minutes
```

```
System returned to ROM by power-on
```

```
System image file is "flash:c2800nm-adventerprisek9-mz.150-1.M4"
```

```
Last reload type: Normal Reload
```

```
Cisco 2851 (revision 53.51) with 509952K/14336K bytes of memory.
```

```
Processor board ID FTX0925A1BF
```

```
2 Gigabit Ethernet interfaces
```

```
1 Virtual Private Network (VPN) Module
```

```
DRAM configuration is 64 bits wide with parity enabled.
```

```
239K bytes of non-volatile configuration memory.
```

```
62720K bytes of ATA CompactFlash (Read/Write)
```

```
License Info:
```

```
License UDI:
```

```
-----
Device#      PID          SN
-----
*0           CISCO2851    FTX0925A1BF
```

```
Configuration register is 0x2102
```

Last IOS configuration change

```
Router# show run
Building configuration...
!
! Last configuration change at 20:40:41 GMT Nov 2 2011 by lnunez
!
Version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router
!
boot-startmarker
boot-end-marker
!
no aaa new-model
```


Cisco ASA Firewall “fips enable” command

Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.


Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

....

Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9 

INFO: FIPS Power-On Self-Test in process. Estimate completion in 90 seconds.

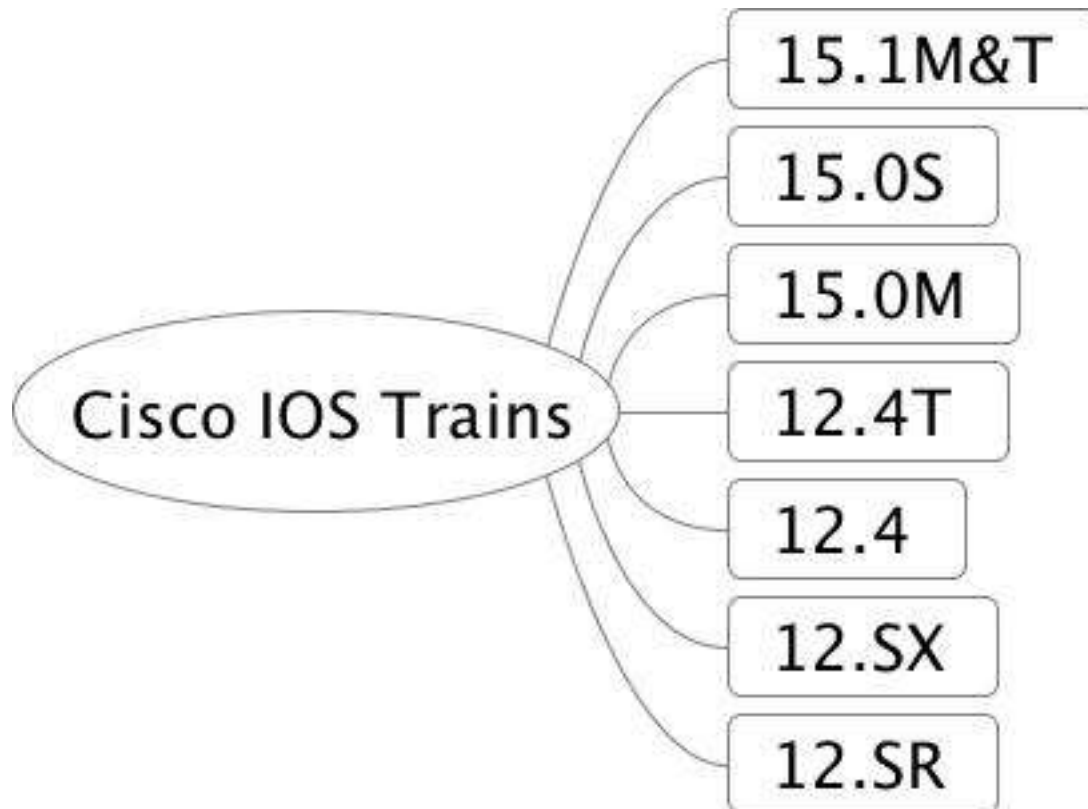
.....

INFO: FIPS Power-On Self-Test complete. 

Type help or '?' for a list of available commands.

sw8-5520>

Cisco IOS versions (Trains)



Juniper JUNOS SCAP

- junos-definitions-schema.xsd
- junos-system-characteristics-schema.xsd

```

1  <?xml version="1.0" encoding="utf-8"?>
2  <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-def"
3  <xsd:import namespace="http://oval.mitre.org/XMLSchema/oval-common-5" schemaLocation="oval-common-schema.xsd"/>
4  <xsd:import namespace="http://oval.mitre.org/XMLSchema/oval-definitions-5" schemaLocation="oval-definitions-schema.xsd"/>
5  <xsd:annotation>
6      <xsd:documentation> </xsd:documentation>
7      <xsd:appinfo>
8          <schema>JUNOS Definition</schema>
9          <version>5.10</version>
10         <date>10/28/2011 8:58:23 AM</date>
11         <terms_of_use> </terms_of_use>
12         <sch:ns prefix="oval-def" uri="http://oval.mitre.org/XMLSchema/oval-definitions-5"/>
13         <sch:ns prefix="junos-def" uri="http://oval.mitre.org/XMLSchema/oval-definitions-5#junos"/>
14         <sch:ns prefix="xsi" uri="http://www.w3.org/2001/XMLSchema-instance"/>
15     </xsd:appinfo>
16 </xsd:annotation>
17 <!-- ===== GLOBAL TEST ===== -->
18 <!-- ===== GLOBAL TEST ===== -->
19 <!-- ===== GLOBAL TEST ===== -->
20 <xsd:element name="global_test" substitutionGroup="oval-def:test">
53 <xsd:element name="global_object" substitutionGroup="oval-def:object">
90 <xsd:element name="global_state" substitutionGroup="oval-def:state">
</xsd:element>
107 <!-- ===== LINE TEST ===== -->
108 <!-- ===== LINE TEST ===== -->
109 <!-- ===== LINE TEST ===== -->
110 <!-- ===== LINE TEST ===== -->
111 <xsd:element name="line_test" substitutionGroup="oval-def:test">
144 <xsd:element name="line_object" substitutionGroup="oval-def:object">
182 <xsd:element name="line_state" substitutionGroup="oval-def:state">
204 </xsd:element>
205 <!-- ===== VERSION TEST ===== -->
206 <!-- ===== VERSION TEST ===== -->
207 <!-- ===== VERSION TEST ===== -->
208 <xsd:element name="version" substitutionGroup="oval-def:test">
241 <xsd:element name="version_object" substitutionGroup="oval-def:object">
251 <xsd:element name="version_state" substitutionGroup="oval-def:state">
304 <!-- ===== -->
305 <!-- ===== -->
306 <!-- ===== -->

```