Agenda

- What is Network Security
- General Configuration Security
- Logging and Auditing
- Tools to help!

This talk is focused on securing your Cisco network infrastructure, if you would like to talk about securing content services (email, web servers etc…) or Junipers please come and see me afterwards.

2

What is network security?

Firstly lets talk about what devices/software are commonly mentioned when discussing network security:

1. Firewalls (Deep packet inspection)
2. Intrusion Detection Systems (IDS)
3. Intrusion Prevention Systems (IPS)
4. Event correlation
5. Routers, Switches
6. Virus Scanners
7. Network scanning tools

4

What is network security?

So as you have just seen, there is not one device/appliance/tool that provides network security.

Cisco Press has many books which state that they believe Network Security is a system and that the system is:

A collection of network-connected devices, technologies and best practises that work in complementary ways to provide security to information assets. – Network Security Architectures

5

What is network security?

To know your Enemy, you must become your Enemy

Sun Tzu, The Art of War

6

What is network security?

Why?

7

What is network security?

Take advantage of the enemy's unpreparedness; travel by unexpected routes and strike him where he has taken no precautions.

Sun Tzu, The Art of War

8

General Infrastructure Security

- Do you know what's out on your network?
- Have you recently scanned your IPv4 infrastructure to see if anything new has been added? (IPv4)
- With IPv6 scanning your network becomes next to impossible.
  - *Have you got tools that utilise other methods to detect if a IPv6 device exists?*
- Do you check if your servers/routers/switches/firewalls/ids/ips etc… comply with your expected base configuration?

10

General Infrastructure Security

Things you really want to make sure you have used and are working:

NTP (this is key for identifying when attacks happened across multiple devices)

Sequence Numbers in your log files:

"service *sequence-number* timestamps debug uptime"

"service *sequence-number* timestamps log datetime msec"

11

General Infrastructure Security

"*service password-encryption*" – This make sure all passwords are encrypted in the config.

Use "*enable secret*" rather than "enable password" as you can decrypt the "enable password" but not the "enable secret" hash.

And obviously you need a local username:

"username <username> secret <password>"

DO NOT USE "enable password or username <user> password <passwd>

12

General Infrastructure Security

Do you have a “line aux 0” in your config? If so have you disabled it unless you really need it?

```
line aux 0
 exec-timeout 0 1
 login local
 no exec
 transport input none
!
```


General Infrastructure Security

Do you have a “line vty 0 4” or “line vty 0 15” in your config? Is it secured? i.e SSH only, do you have IPv4 and IPv6 access?

```
line vty 0 15
 access-class VTY-IPv4-INCOMING in
 exec-timeout 0 0
 password 7 050303032D435F1C1C16031C0E18567A7A75
 ipv6 access-class VTY-IPv6-INCOMING in
 transport input ssh
!
```

General Infrastructure Security

```
ip access-list extended VTY-IPv4-INCOMING
 permit ip X.X.X.X 0.0.0.255 any
deny   ip any any

ipv6 access-list VTY-IPv6-INCOMING
 permit ipv6 XXXX:XXXX:XXXX::/64 any
!
```

15

General Infrastructure Security

Services or Features you should be questioning:

Finger, HTTP/S Server, BootP Server, PAD [X.25], IP Source routing, proxy-arp, ip directed broadcast, ip unreachable, ip redirects, MOP [Decnet], NTP, SNMP, DNS, CDP

Do you need to really run any of those?

16

General Infrastructure Security

Do you have passwords on your IGP sessions? (OSPF/OSPF3/RIP/ISIS/EIGRP)

Are you leaking your IGP on interfaces to external parties?

(Read about OSPF vulnerabilities here: http://tools.ietf.org/html/draft-ietf-rpsec-ospf-vuln-01)

Do you have password on your exterior routing protocols?

General Infrastructure Security

Do you have SNMP enabled, if so do you have it secured to a select group of hosts via an ACL?

snmp-server community <community name> RO <acl number>

snmp-server trap link ietf

snmp-server trap-source <Interface>

snmp-server packetsize 9000

snmp-server location <Where in the world is Waldo>

snmp-server contact <An email address for Waldo>

General Infrastructure Security

What logging options have you got enabled?

logging buffered 65536
logging console informational
logging history informational
logging trap debugging
logging source-interface <interface>
logging <host>

19

General Infrastructure Security

Do you perform CoPP (Control Plane Policing) on your switches and routers?

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/copp.html

20

General Infrastructure Security

Finally a useful feature:

```
archive
 log config
  logging enable
  logging size 10
 path ftp://ftp/$h/$h-$t
 write-memory
!
```

21

Logging!

Logging can be an invaluable resource for knowing what's been happening on your network. It can also be an overload of information!

23

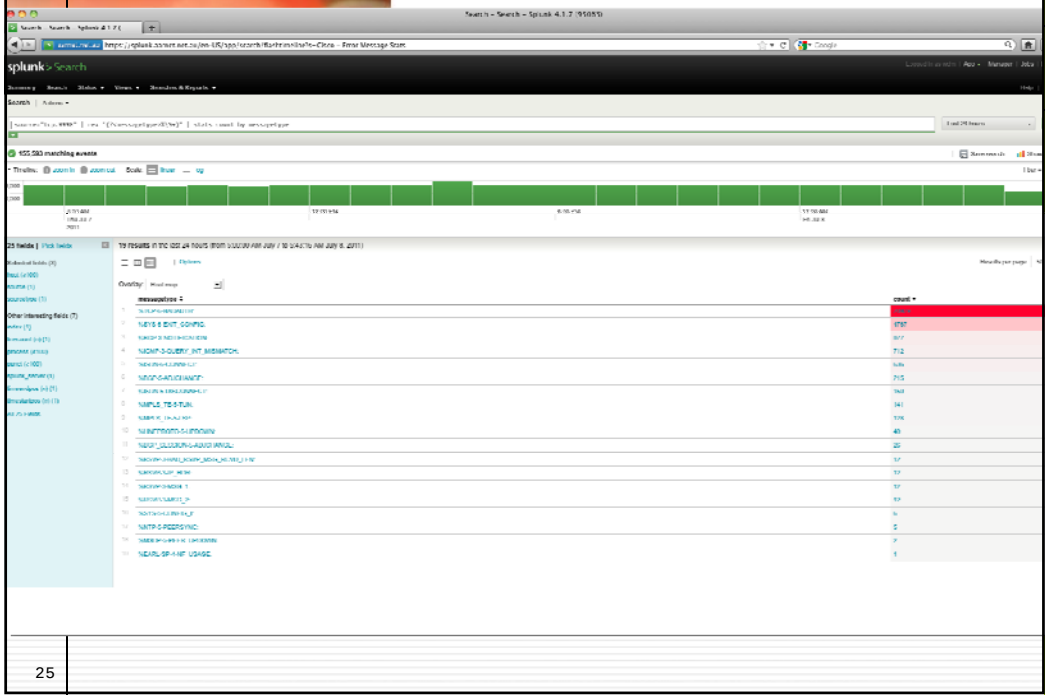
For those who use Splunk!

I use the following search each morning to see what's been happening:

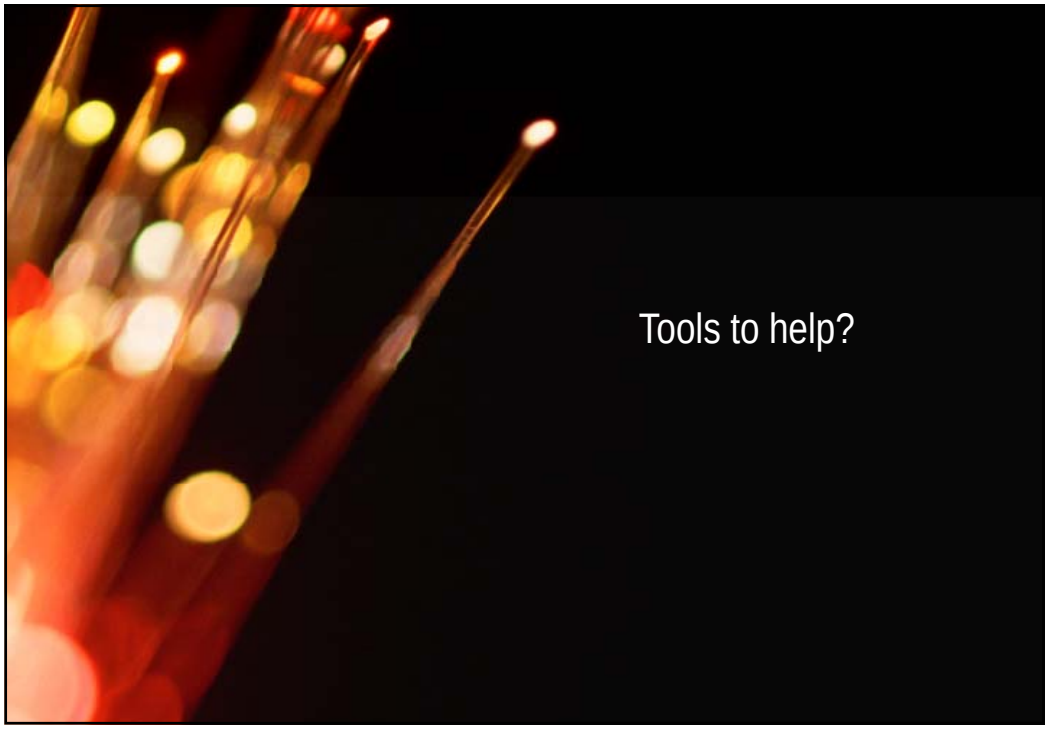
source="tcp:9998" | rex "(?<messagetype>%\S+)" | stats count by messagetype

Note *This is a Cisco search*.

24

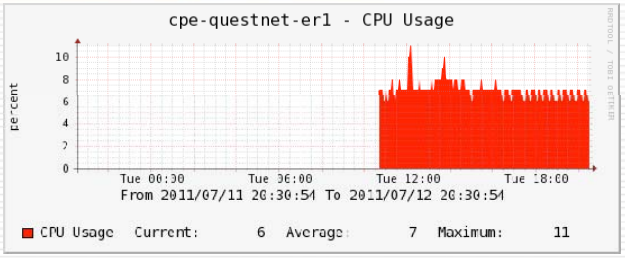


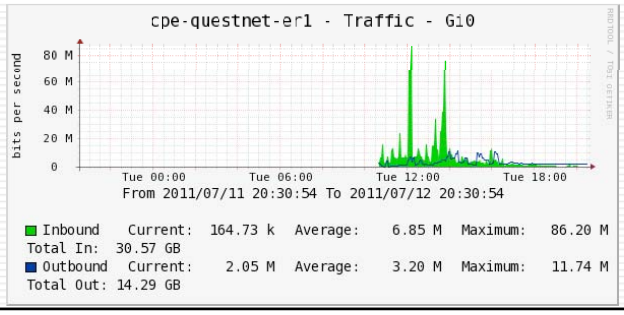
25



Tools/Assistance

MRTG/Cacti:

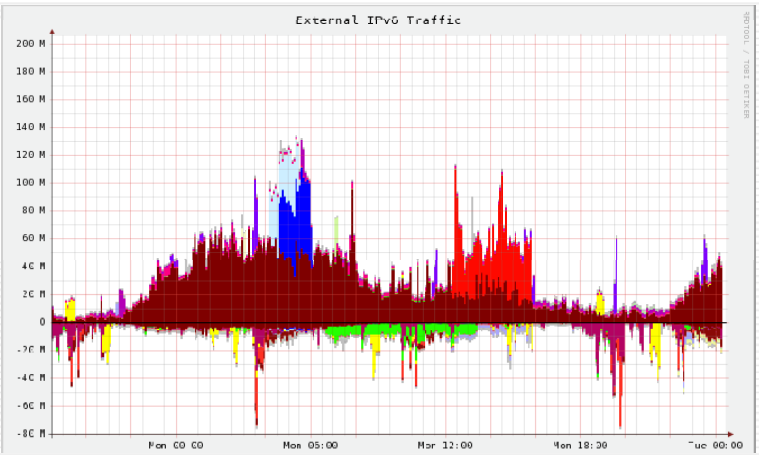




27

Tools/Assistance

Netflow:



28

Tools/Assistance

NSA provide an extremely valuable document on how to best secure your Cisco equipment:
http://www.nsa.gov/ia/guidance/security_configuration_guides/cisco_router_guides.shtml

Cisco:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Juniper:
http://www.juniper.net/techpubs/software/junos/junos74/swconfig74-system-basics/html/software-overview22.html

Tools/Assistance

Defence Signals Directorate have published – The DSD Information Security Manual:
http://www.dsd.gov.au/infosec/ism/index.htm

Cymru provide a Junos Template:
http://www.cymru.com/gillsr/documents/junos-template.pdf

Cymru provide a Cisco template:
http://www.cymru.com/Documents/secure-ios-template.html

Tools/Assistance

Rancid:

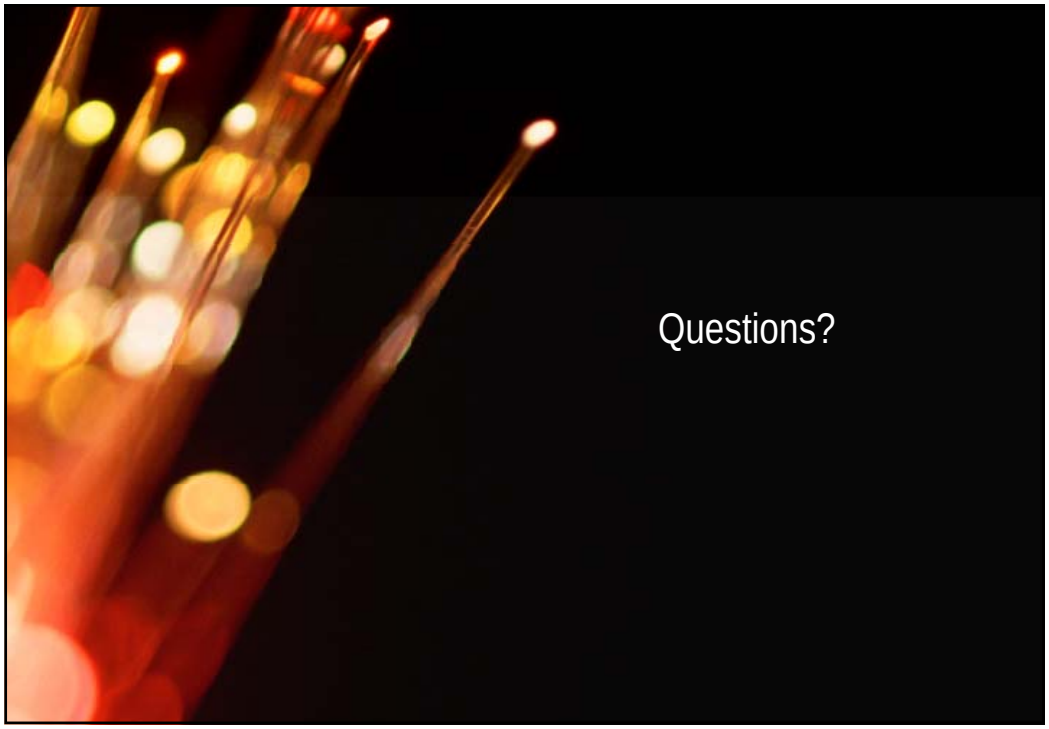
```
!RANCID-CONTENT-TYPE: cisco
!
!Chassis type: 877W-M - a 877W-M router
!CPU: MPC8272
!
!Memory: main 236544K/25600K
!Memory: nvram 128K
!
!Processor ID: XXXXXXXXX
!
!Image: Software: C870-ADVIPSERVICESK9-M, 12.4(24)T4, RELEASE SOFTWARE (fc2)
!Image: Compiled: Fri 03-Sep-10 17:16 by prod_rel_team
!Image: flash:c870-advipservicesk9-mz.124-24.T4.bin
!
!ROM Bootstrap: Version 12.3(8r)YI4, RELEASE SOFTWARE
!Flash: 53248K bytes of processor board System flash (Intel Strataflash)
!Flash: Directory of flash:/
!Flash:    2  -rwx    21890692   Jul 1 2011 01:06:14 +08:00  c870-advipservicesk9-mz.124-24.T4.bin
!Flash:    3  -rwx    26444544  Jun 30 2011 17:18:03 +08:00  c870-advipservicesk9-mz.151-4.M.bin
!Flash: 52383744 bytes total (4040704 bytes free)
```

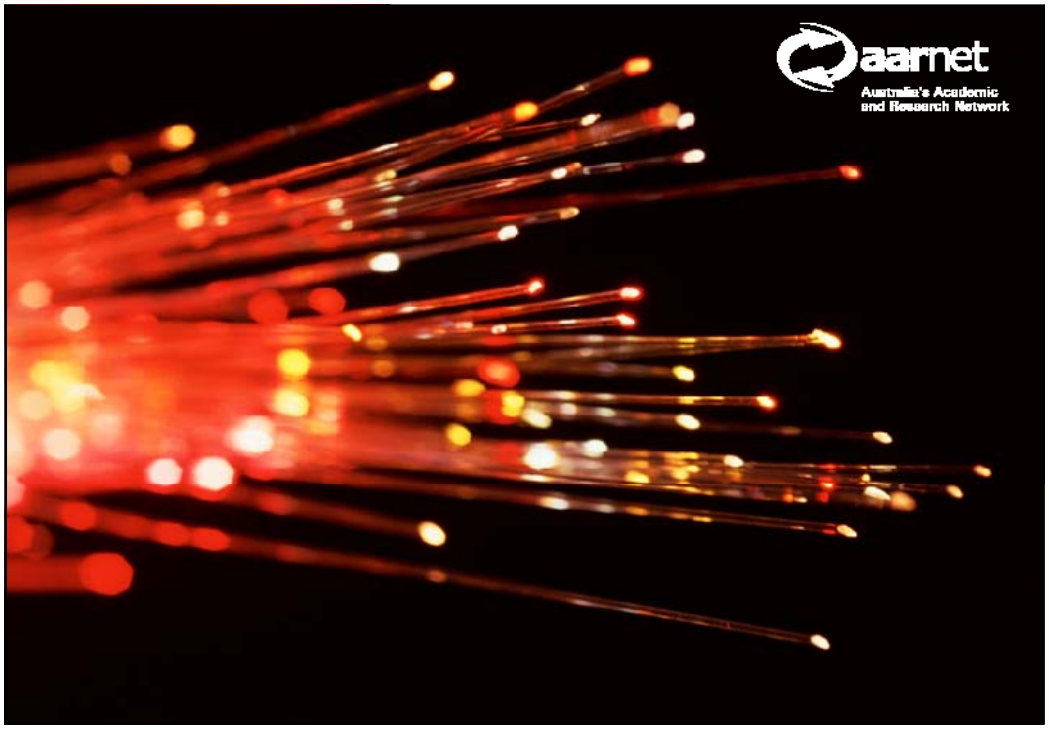

Tools/Assistance

Rancid has some useful tools available and you can easily write your own to identify what ACL's etc are no longer in use in your router configs.

http://ftp.isc.org/isc/toolmakers/filter_audit-1.01.tar.gz

http://www.isc.org/community/toolmakers


Questions?


aarnet
Australia's Academic
and Research Network