How we made a Failed COTS solution Useful with FOSS

Agenda

- Background
- Personal Disclaimer
- COTS vs. FOSS
- Product Failure
- Official Approach – Worked with vendor
- Good Customer Approach – Help the vendor
- Fed-up Customer Approach – Replace Software
- Enhance Solution
- Final Thoughts

Background

- On contract to a US Agency as the Senior InfoSec Engineer for the CISO to evaluate, test, and design security solutions
- Among other things, the team is responsible for central-collection of ~25million security events per day from over 8000 devices, and analysis of this data

Personal Disclaimer

- Support FOSS but not in favor of a better COTS solution (if one exists)
- 3-year story, not a how-to
- Not vendor specific – COTS NIDS

COTS Incentives

- Update cycle (patches, signatures, etc)
- Supported
- Integrated technologies
- It Looks slick (when it works)
- Someone to blame
- “We are a [insert name-brand here] shop”
- “I just don't trust that freeware!”

FOSS Incentives

- Known and working
- No license or PO overhead
- Free?
- Adaptable to any environment
- Forums, Wikis and Message Boards, oh my
- COTS = tied hands
  - Can't make changes per license or closed source
  - Customer Support - The Golden Handcuffs

- Unattributed quote from government IT staff: “I would rather implement a COTS solution of unknown quality but have someone to blame then to put in FOSS software that we believe will work, but where I will have no one to turn to if there are problems.”

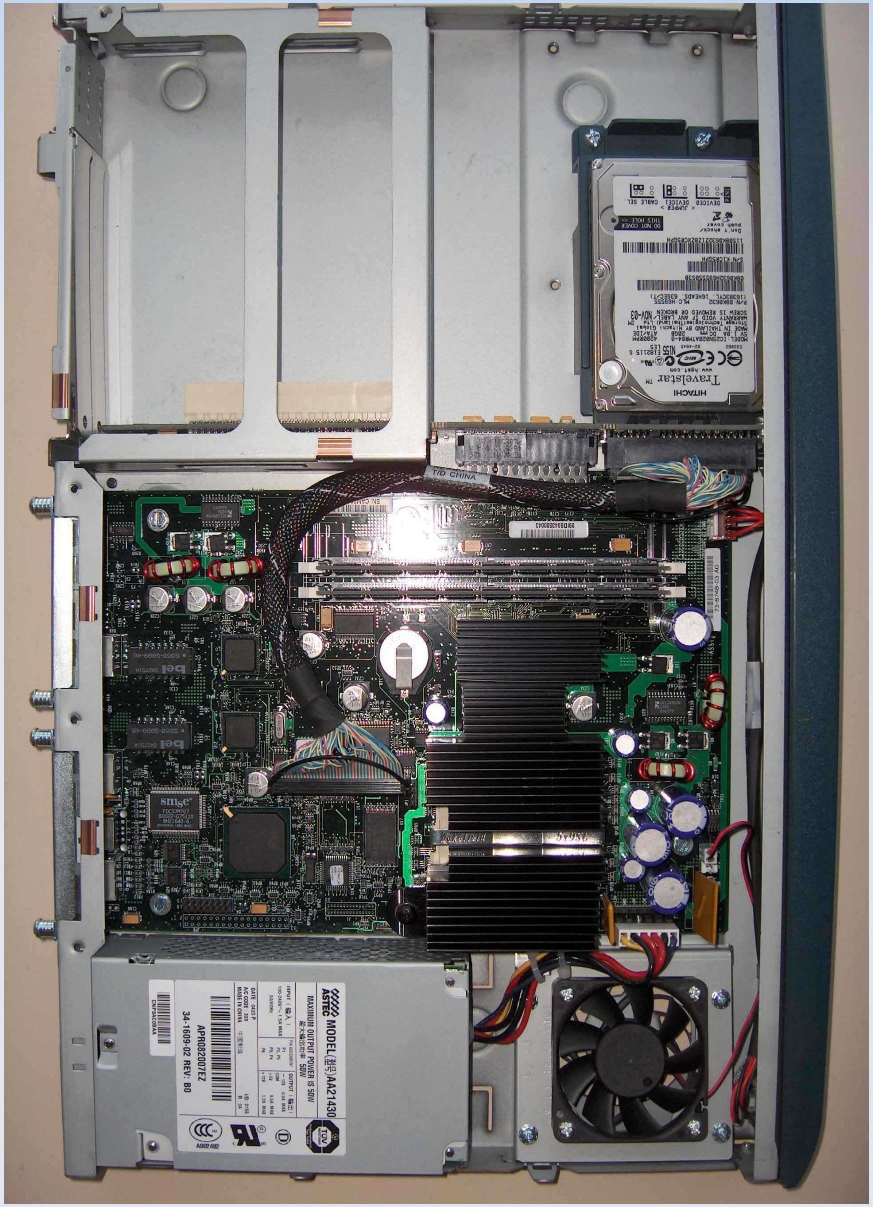
The Environment – Jun. 2004

- Over 90 offices in approx. 70 countries
- Highly-latent network links, fail-over to VSAT
- ~3/4 of offices have a local Internet gateway
- Project to deploy approx. 100 COTS NIDS Appliances mostly model 4215
    - This includes replacement of original 5 4210s

Rude Awakening – 6 Months In

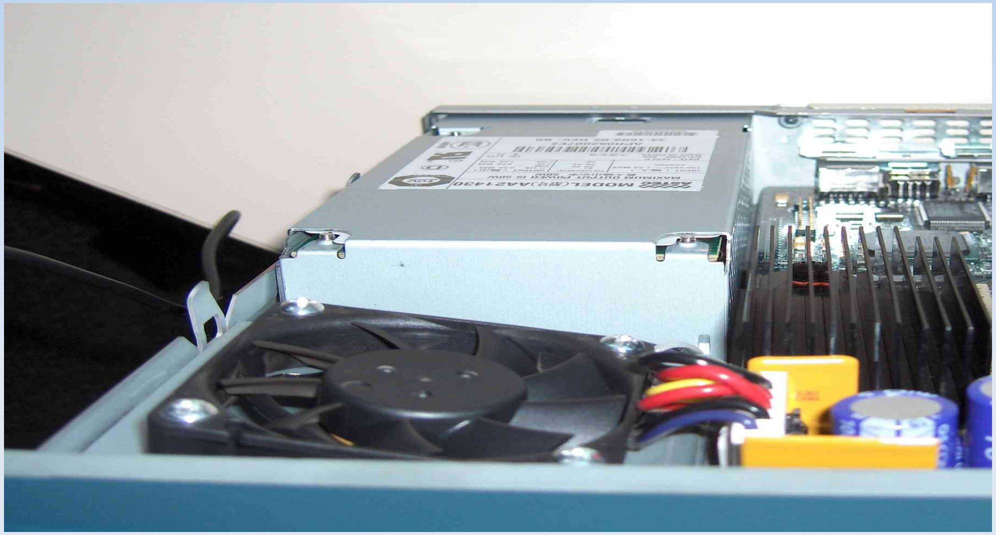
- Many sensors not reporting in
- Little visibility in many locations
- Mgmt system required frequent rebuilds
- Mgmt system clunky and buggy
- Eventually tasked to define key issues
  - 100 devices in over 90 offices all over the world
  - All installed in average server rooms

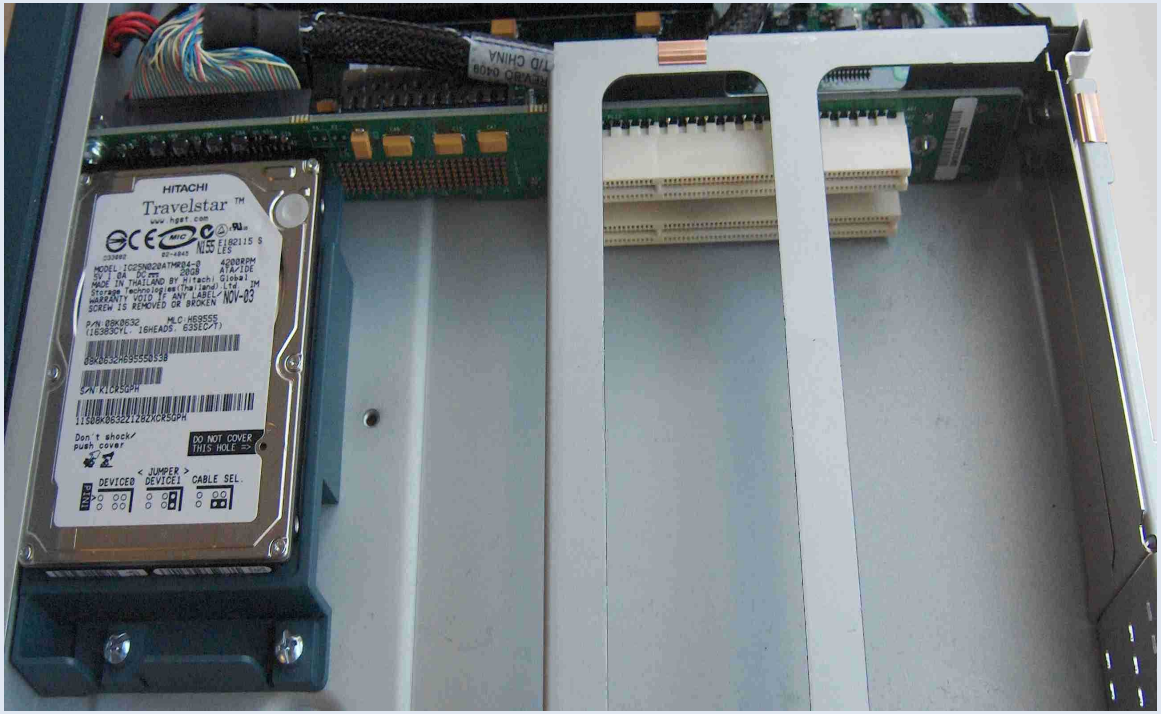
Problems - Hardware



- Poor design
- Unreachable systems were costly in time
- Long replacement cycle (slow international ship)
- Recovered drive is useless

Poor Design - Close-Up





Problems – Mgmt Overhead

- Managing the management solution
  - Sensitive
  - Rebuilt DB 4 times in 18 months
  - Frequent Errors (i.e. Java Exceptions)
- Slow management tasks
  - Version query took 45 minutes
  - Updates took many hours or days

Problems - Performance

- Advertised performance (80mb/s)
  - Marketing numbers?
  - No port bonding
- Our test revealed ~92% packet-loss at the NIC when burdened with 77mb/s of traffic
- Of the < 8% that got through, over ½ was dropped by the kernel

Problem - Failed Services

- NTP
  - Not compatible with “ntp keys”
  - Service ntpd frequently dies
  - NIDS time off by minutes/hours
- Sensing interface “downs” itself
- IDS software frequently dies

Problem - No updates

- Timeout due to high-latent links
- No notification for failed update
- Queries took 45 minutes
- Approximately 10% never would update

Problems - Signatures

- Signature Updates impossible
  - Over 10% timed-out due to latency
  - No mitigation for slow links
- Limited signature tuning capability
- No visible detection logic (on many sigs)
- High FP rate (updates revived tuned sigs)
- Little visibility into vendor-supplied rules
- Very limited on custom signatures

Official Approach

Tell Vendor to Fix Problem

Worked With Vendor

- Opened lots of customer support cases
- Updated sales team (e.g. Sales Engineer)
  - On-site visits and many conference calls
  - SE and entire Sales Team was no help at all
- Brought issues to product manager (con call)
- Bought new hardware for critical sites, model 4240

COTS NIDS Reality

- RMAed units, but we are blind for weeks
- Other reports of failure in Federal Agencies
- Usage & functionality problems were systemic
- Each next release didn't fix big issues
- Our new hardware investment had problems
- A full-scale replacement was not budgeted

Good Customer Approach

Encourage Product Work

Managed the NIDS

- Got r00t!
- Implemented shared keys
- Studied underlying system

Replaced Signature Updates

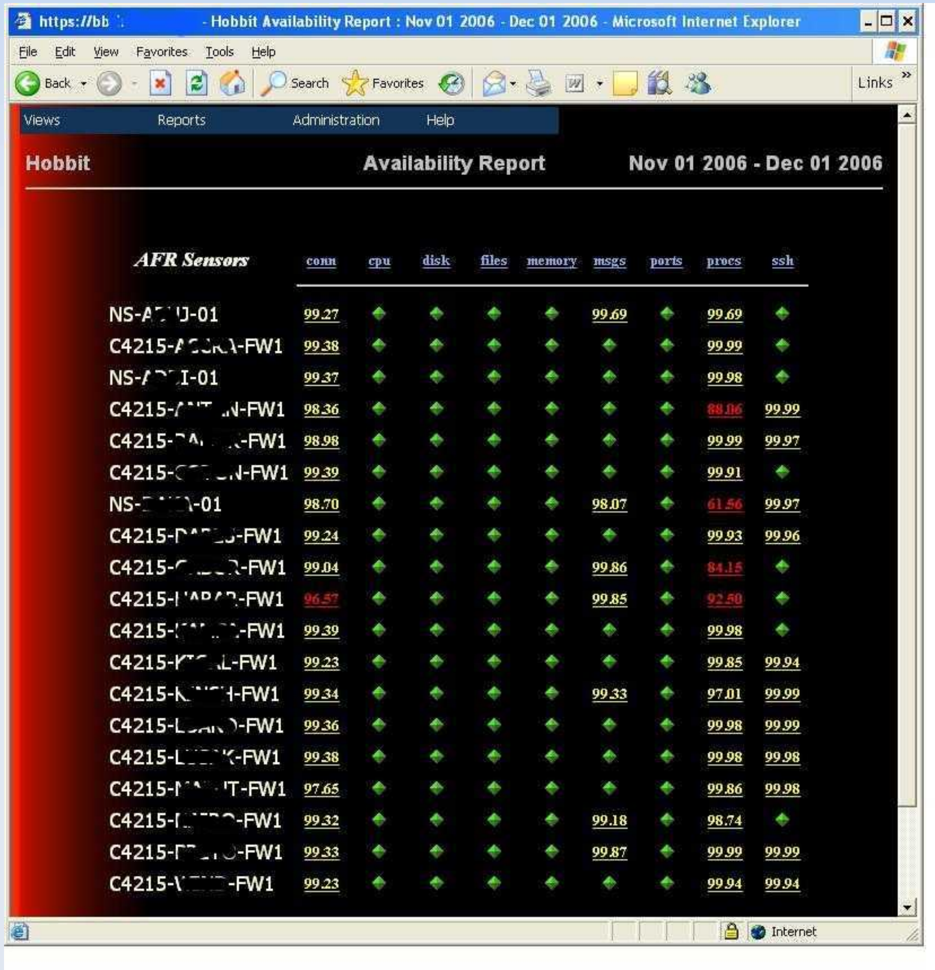
- Latency is a fact, need better solution
- Wrote script (i.e. wrapped wget) to download latest sig version centrally
- Synced latest version to NIDS local directory
- Configured NIDS to update from local

Continued Work with Vendor

- Opened more customer support cases
- Stayed in contact with sales team
  - More on-site visits and conference calls
- Met with vendor's security product panager
  - No hope in site
  - Chastised for patching our COTS NIDS using ssh

Implemented Monitoring

- Used Henrik Storner's Hobbitmon to monitor network-based services
- More visibility can be a scary thing
- Monitored icmp then ssh, then https, then certificate checks



https://bb[redacted] - Hobbit Availability Report : Nov 01 2006 - Dec 01 2006 - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Links
Views
Reports
Administration
Help
Internet

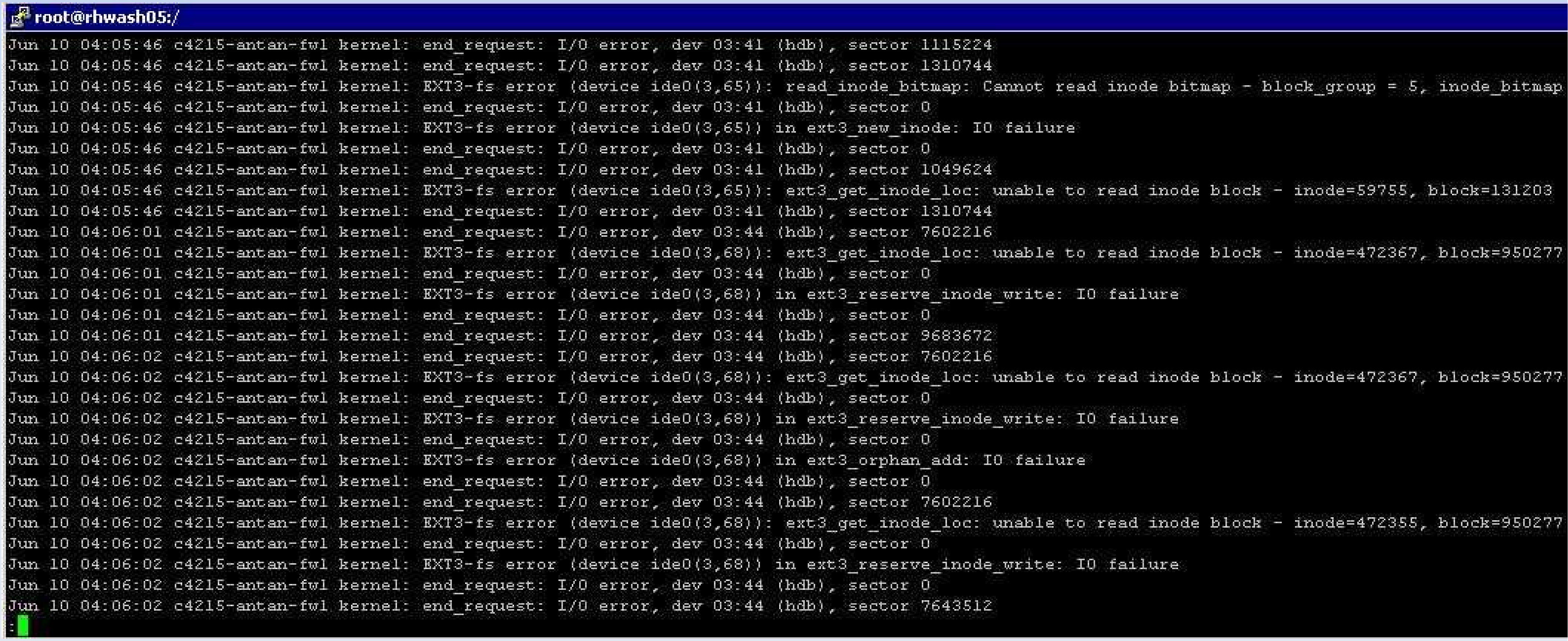
Hobbit Availability Report Nov 01 2006 - Dec 01 2006

AFR Sensors	conn	cpu	disk	files	memory	msgs	ports	procs	ssh
NS-A[redacted]U-01	99.27	◆	◆	◆	◆	99.69	◆	99.69	◆
C4215-A[redacted]A-FW1	99.38	◆	◆	◆	◆	◆	◆	99.99	◆
NS-A[redacted]I-01	99.37	◆	◆	◆	◆	◆	◆	99.98	◆
C4215-A[redacted]N-FW1	98.36	◆	◆	◆	◆	◆	◆	88.06	99.99
C4215-[redacted]-FW1	98.98	◆	◆	◆	◆	◆	◆	99.99	99.97
C4215-C[redacted]N-FW1	99.39	◆	◆	◆	◆	◆	◆	99.91	◆
NS-[redacted]-01	98.70	◆	◆	◆	◆	98.07	◆	61.56	99.97
C4215-D[redacted]-FW1	99.24	◆	◆	◆	◆	◆	◆	99.93	99.96
C4215-[redacted]R-FW1	99.04	◆	◆	◆	◆	99.86	◆	84.15	◆
C4215-[redacted]-FW1	96.57	◆	◆	◆	◆	99.85	◆	92.50	◆
C4215-[redacted]-FW1	99.39	◆	◆	◆	◆	◆	◆	99.98	◆
C4215-K[redacted]L-FW1	99.23	◆	◆	◆	◆	◆	◆	99.85	99.94
C4215-K[redacted]H-FW1	99.34	◆	◆	◆	◆	99.33	◆	97.01	99.99
C4215-L[redacted]-FW1	99.36	◆	◆	◆	◆	◆	◆	99.98	99.99
C4215-L[redacted]K-FW1	99.38	◆	◆	◆	◆	◆	◆	99.98	99.98
C4215-[redacted]T-FW1	97.65	◆	◆	◆	◆	◆	◆	99.86	99.98
C4215-[redacted]-FW1	99.32	◆	◆	◆	◆	99.18	◆	98.74	◆
C4215-[redacted]-FW1	99.33	◆	◆	◆	◆	99.87	◆	99.99	99.99
C4215-V[redacted]-FW1	99.23	◆	◆	◆	◆	◆	◆	99.94	99.94

More Visibility = Horror

- Monitoring demonstrated larger problem
  - About 30% of the COTS NIDS were not functioning
  - Some were in half hung state
  - Others had down sensing interfaces
  - Services were failing at a high frequency
  - Time varied greatly
- Hobbit effectively measured up-status
- Hobbit allowed us to report on outages

COTS NIDS – Half Hung State



```
Jun 10 04:05:46 c4215-antan-fwl kernel: end_request: I/O error, dev 03:41 (hdb), sector 1115224
Jun 10 04:05:46 c4215-antan-fwl kernel: end_request: I/O error, dev 03:41 (hdb), sector 1310744
Jun 10 04:05:46 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,65)): read_inode_bitmap: Cannot read inode bitmap - block_group = 5, inode_bitmap
Jun 10 04:05:46 c4215-antan-fwl kernel: end_request: I/O error, dev 03:41 (hdb), sector 0
Jun 10 04:05:46 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,65)) in ext3_new_inode: IO failure
Jun 10 04:05:46 c4215-antan-fwl kernel: end_request: I/O error, dev 03:41 (hdb), sector 0
Jun 10 04:05:46 c4215-antan-fwl kernel: end_request: I/O error, dev 03:41 (hdb), sector 1049624
Jun 10 04:05:46 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,65)): ext3_get_inode_loc: unable to read inode block - inode=59755, block=131203
Jun 10 04:05:46 c4215-antan-fwl kernel: end_request: I/O error, dev 03:41 (hdb), sector 1310744
Jun 10 04:06:01 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 7602216
Jun 10 04:06:01 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,68)): ext3_get_inode_loc: unable to read inode block - inode=472367, block=950277
Jun 10 04:06:01 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 0
Jun 10 04:06:01 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,68)) in ext3_reserve_inode_write: IO failure
Jun 10 04:06:01 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 0
Jun 10 04:06:01 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 9683672
Jun 10 04:06:02 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 7602216
Jun 10 04:06:02 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,68)): ext3_get_inode_loc: unable to read inode block - inode=472367, block=950277
Jun 10 04:06:02 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 0
Jun 10 04:06:02 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,68)) in ext3_reserve_inode_write: IO failure
Jun 10 04:06:02 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 0
Jun 10 04:06:02 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,68)) in ext3_orphan_add: IO failure
Jun 10 04:06:02 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 0
Jun 10 04:06:02 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 7602216
Jun 10 04:06:02 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,68)): ext3_get_inode_loc: unable to read inode block - inode=472355, block=950277
Jun 10 04:06:02 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 0
Jun 10 04:06:02 c4215-antan-fwl kernel: EXT3-fs error (device ide0(3,68)) in ext3_reserve_inode_write: IO failure
Jun 10 04:06:02 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 0
Jun 10 04:06:02 c4215-antan-fwl kernel: end_request: I/O error, dev 03:44 (hdb), sector 7643512
:
```

Replacement Options – ~3 Years

- Stay with existing vendor
- Invest in a new NIDS vendor
- Implement our own solution

Fed-up Customer Approach

Replace Vendor's Software
Implement our own **Known-Working** Solution

Approval

- Got approval to design a new solution using Free and Open Source Software and an in-house implementation
- Got approval to use existing hardware platform (point of no return)

Project Definition – Mid-Aug. 2006

- Time-frame
  - 7 Weeks until forced upgrade
  - Had 7 Weeks to:
    - Design solution
    - Build solution
    - Test solution
    - Implement solution
  - Prior commitments
- Initial goal: Replace existing functionality 1-for-1
- Leverage already-installed hardware

Architecture Challenges

- Six variations of NIDS
  - Three models of appliance (4215,4240,IDSM2)
  - Two base OS/Vers (4.x-RH7.3,5.x-busybox)
- Three naming schemes for interfaces
- Many quirks including:
  - Varying libraries
  - Diverse filesystem layout
  - Inconsistent software packages
  - Different environment (i.e. PATH)

Limitations of Platform

- Ver 4.x - modified Redhat 7.3
  - Specialized Kernel
  - Few tools and libs
- Ver 5.x - Busybox
  - Newer specialized kernel
  - Much fewer tools and libs
  - At boot, flash writes to ramdisk (no persistent FS)

Limitations of Hardware

- 4215s (mostly running 4.x)
  - Frequent hard drive failures
  - Very low net capacity (92% dropped packets etc)
- 4240s (mostly running 5.x)
  - Limited-sized CF disk (largest part. was 512 mb) only, no larger data store
  - Faster net but not great

Solution Replacement - Phase 1

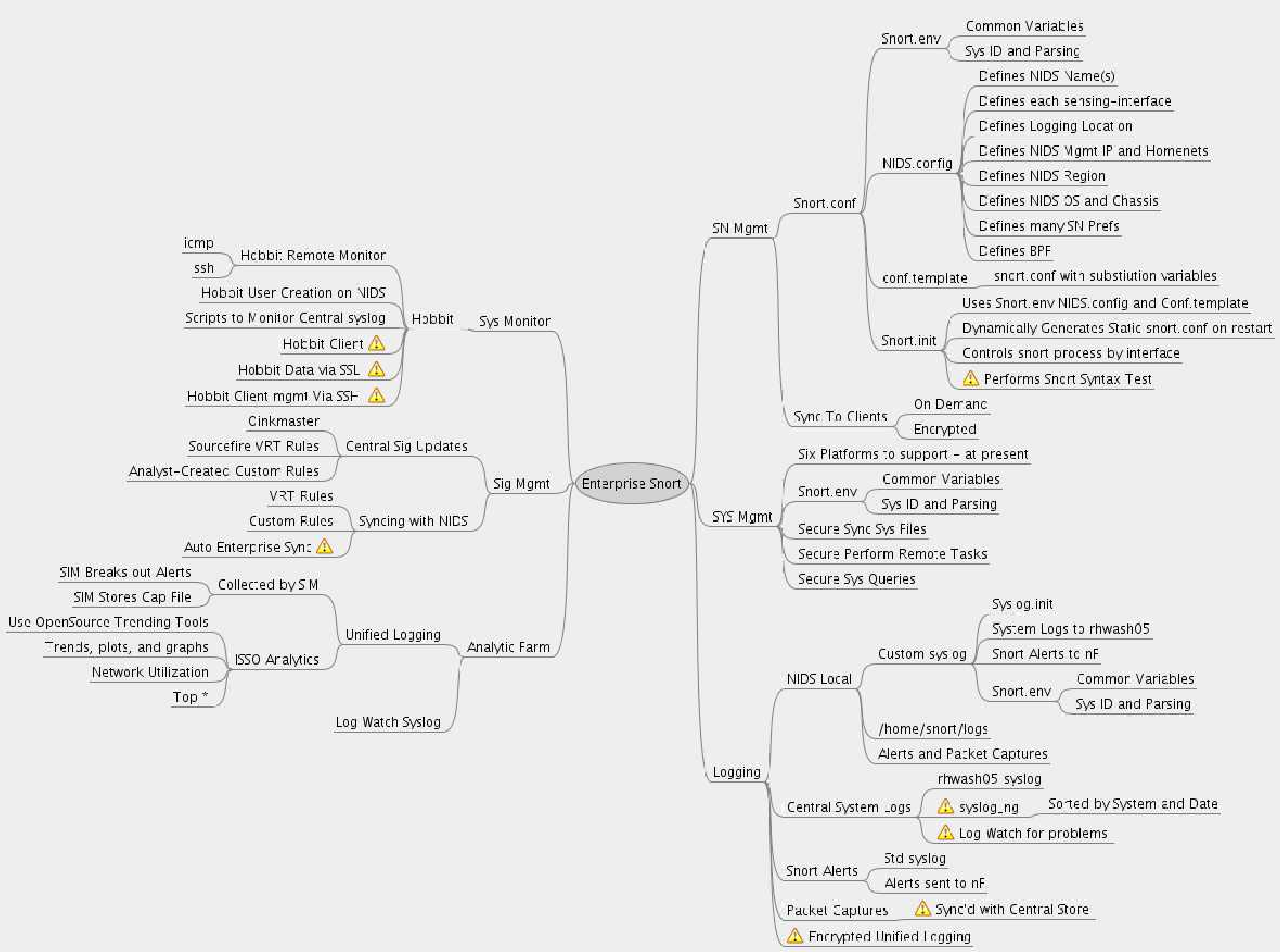
Phase 1 Goal

To maintain continuity of central management for the NIDS, a more complex management architecture was designed to obfuscate subtle differences in the six different platforms.

The primary goal was to keep the analysts watching packets and not configuring snort/systems.

Phase 1 Objectives

- Enhanced Monitoring (internals)
- System Management
- Signature Management
- Snort Management
- Log Management
- Implement/Cut-over and not miss events



- Enterprise Snort
  - SN Mgmt
    - Snort.conf
      - Snort.env
        - Common Variables
        - Sys ID and Parsing
      - NIDS.config
        - Defines NIDS Name(s)
        - Defines each sensing-interface
        - Defines Logging Location
        - Defines NIDS Mgmt IP and Homenets
        - Defines NIDS Region
        - Defines NIDS OS and Chassis
        - Defines many SN Prefs
        - Defines BPF
      - conf.template
        - snort.conf with substiution variables
      - Snort.init
        - Uses Snort.env NIDS.config and Conf.template
        - Dynamically Generates Static snort.conf on restart
        - Controls snort process by interface
        - ⚠ Performs Snort Syntax Test
    - Sync To Clients
      - On Demand
      - Encrypted
  - SYS Mgmt
    - Six Platforms to support - at present
    - Snort.env
      - Common Variables
      - Sys ID and Parsing
    - Secure Sync Sys Files
    - Secure Perform Remote Tasks
    - Secure Sys Queries
  - Logging
    - NIDS Local
      - Custom syslog
        - Syslog.init
        - System Logs to rhwash05
        - Snort Alerts to nF
        - Snort.env
          - Common Variables
          - Sys ID and Parsing
      - /home/snort/logs
      - Alerts and Packet Captures
    - Central System Logs
      - rhwash05 syslog
      - ⚠ syslog_ng
        - Sorted by System and Date
      - ⚠ Log Watch for problems
    - Snort Alerts
      - Std syslog
      - Alerts sent to nF
    - Packet Captures
      - ⚠ Sync'd with Central Store
    - ⚠ Encrypted Unified Logging
  - Sys Monitor
    - Hobbit
      - Hobbit Remote Monitor
        - icmp
        - ssh
      - Hobbit User Creation on NIDS
      - Scripts to Monitor Central syslog
      - Hobbit Client ⚠
      - Hobbit Data via SSL ⚠
      - Hobbit Client mgmt Via SSH ⚠
  - Sig Mgmt
    - Central Sig Updates
      - Oinkmaster
      - Sourcefire VRT Rules
      - Analyst-Created Custom Rules
    - Syncing with NIDS
      - VRT Rules
      - Custom Rules
      - Auto Enterprise Sync ⚠
  - Analytic Farm
    - Unified Logging
      - Collected by SIM
        - SIM Breaks out Alerts
        - SIM Stores Cap File
      - ISSO Analytics
        - Use OpenSource Trending Tools
        - Trends, plots, and graphs
        - Network Utilization
        - Top *
    - Log Watch Syslog

Monitoring

- Continue using Hobbitmon
- Built custom hobbit-client packages
- Monitor internals including
  - Snort service
  - Ntp service
  - Sensing interface status
  - Resources: disks, CPU, memory
  - Syslog

System Management

- Used rsync to sync system files
  - Start scripts
  - ntp.conf
  - Host keys

Signature Management

- Sync central sigs to VRT with oinkmaster
- Integrate custom rules as well
- Sync to NIDS with rsync (used bwlimit)
- Aside: Snort rules

Snort Mgmt - NIDS.conf

- Central NIDS.conf
  - Csv containing configuration parameters
  - Mgmt and sensing Ips
  - Interfaces and system-name
  - BPF option
  - Larger components of snort.conf

```
#01NAME_INT,02MGMT_IP,03NAME,04REGION,05MODEL,06OS,07HOME_NETS,08DEFAULT_LOCAL_VARS.include,09DEFAULT_ENT_VARS.include,10DEFAULT_DECODERS.include,11DEFAULT_PREPROCESSORS.include,12CXXLOGS,13DEFAULT_RULES.include,14DEFAULT_CONFIG_STATEMENTS.include,15ROLE,16NOTES,17FILTER,18BPF
```

Snort Mgmt - snort.env

- snort.env (library function)
  - Parses NIDS.conf on system
  - Assigns variables to csv fields from NIDS.conf

```
DEB_LOGS="/var/log/ns/snort/"
DEB_BIN="/usr/bin/"
C40_LOGS="/usr/cids/idsRoot/var/snort/"
C40_BIN="/usr/local/sbin"
C50_LOGS="/usr/cids/idsRoot/var/snort/"
C50_BIN="/usr/local/bin"


SN_RULES="`echo $instance | awk -F, '{ print $13 }'`"
SN_CONFIG="`echo $instance | awk -F, '{ print $14 }'`"
ROLE="`echo $instance | awk -F, '{ print $15 }'`"
NOTES="`echo $instance | awk -F, '{ print $16 }'`"
SN_FILTER="`echo $instance | awk -F, '{ print $17 }'`"
SN_BPF="$NIDS_SNORT_DIR/confs/`grep $NAMEOLD $NIDSCONF | awk -F, '{ print $18 }'`"
```

Snort Mgmt – Snort init

- snort.init
  - Sources snort.env
  - Uses values attained from NIDS.conf
  - Assembles snort.conf at runtime from template

```
Prep_Config(){
cp $TEMPLATE $CONF
$PERL -pi -e "s/HOMENETS/$SN_HOME_NETS/;" $CONF
$PERL -pi -e "s/DEFAULT_LOCAL_VARS.include/$SN_LOCAL_VARS/;" $CONF
$PERL -pi -e "s/DEFAULT_ENT_VARS.include/$SN_ENT_VARS/;" $CONF
$PERL -pi -e "s/DEFAULT_DECODERS.include/$SN_DECODERS/;" $CONF
$PERL -pi -e "s/DEFAULT_PRE_PROCESSORS.include/$SN_PREPROCESSORS/;" $CONF
$PERL -pi -e "s/ALERTFACILITY/$FACILITY/;" $CONF
rm $LOGDIR; ln -s $SN_LOGGING_DIR $LOGDIR
$PERL -pi -e "s/HOST/$NAME/;" $CONF
$PERL -pi -e "s/DEFAULT_CONFIG_STATEMENTS.include/$SN_CONFIG/;" $CONF
$PERL -pi -e "s/DEFAULT_RULES.include/$SN_RULES/;" $CONF
[ ! -d $BINDIR ] && ln -s $BINDIR $NIDS_SNORT_DIR/bin
}
```

Log Management

- Syslog to central syslog-ng server
- Syslog-ng server stores copy and redirects to SIM
- Analysts use shell scripts to parse logs in store
- Analysts use SIM to look at trends and correlations

Implementation

- Implementation scripts
- Parallel sensing for a time
  - COTS IDS and snort running simultaneously
  - Analysts use COTS, but validate snort
- Disable COTS IDS
  - On S-Day, analysts start using snort only
  - Disable IDS software on COTS appliance
- Narrowly missed deadline

Enhancement - Phase 2

Phase 2 Begins – Dec. 2006

- Evaluate hardware replacement
- Call for reinforcements - hire help
- NIDS becomes NS (Network Sensor)

Replace Hardware

- Determine approximate specs
- Market survey for custom appliances
- Got demo boxes from MBX (Advertised in LJ every month)

Flexibility is Everything to Us

Your software on a customized platform, configured to your specifications, with your branding and has to work perfectly. **Got it.** Need five or five thousand? **No problem.** Logistics, shipping and support? **Handled.**

We're flexible so you can focus on your customers. Or getting more of them.

Visit us at www.mbx.com or call 1-800-560-1195 today

Hardware Evaluation Environment

- Structured one month testing
- Built testing environment in lab
- Used live capture files
- Extensive network tests
  - 100T
  - 1000T
  - Bonded
  - Spanned
  - Tapped

Evaluation Parameters

- Tested two versions of legacy hardware
- Tested new hardware with two OS (debian and gentoo)
- Tested multiple quad-ethernet cards
- Built custom image (Debian etch)

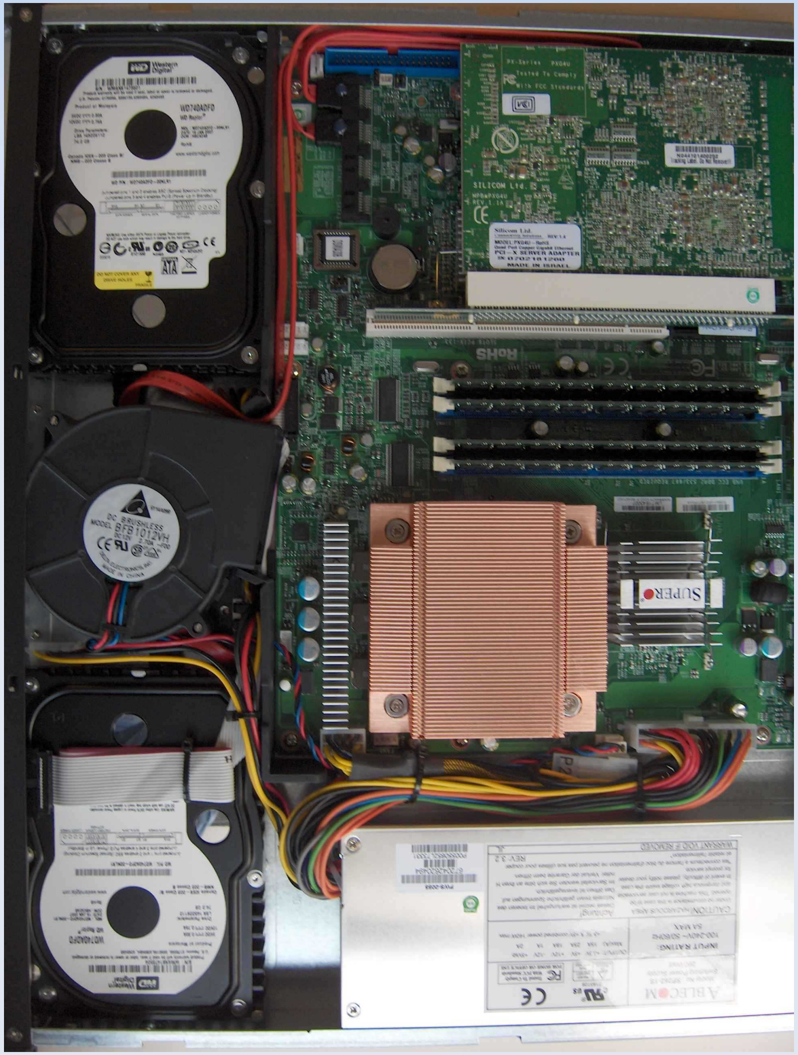
Sample Evaluation Results

	Run 1	Run 2	Run 3
MBX (Debian)	**Snort received 21704005 packets** **Analyzed: 21670880(99.847%)** **Dropped: 33125(0.153%)**	**Snort received 21703824 packets** **Analyzed: 21679190(99.886%)** **Dropped: 24634(0.114%)**	**Snort received 21703720 packets** **Analyzed: 21663726(99.816%)** **Dropped: 39994(0.184%)**
COTS (4215)	Snort received 13547505 packets Analyzed: 534193(3.943%) Dropped: 13013312(96.057%)	Snort received 13547781 packets Analyzed: 524820(3.874%) Dropped: 13022961(96.126%)	Snort received 13540634 packets Analyzed: 515204(3.805%) Dropped: 13025430(96.195%)
COTS (4240)	Snort received 21704004 packets Analyzed: 17329402(79.844%) Dropped: 4374602(20.156%)	Snort received 21704004 packets Analyzed: 17754109(81.801%) Dropped: 3949895(18.199%)	Snort received 21704004 packets Analyzed: 17774793(81.896%) Dropped: 3929211(18.104%)

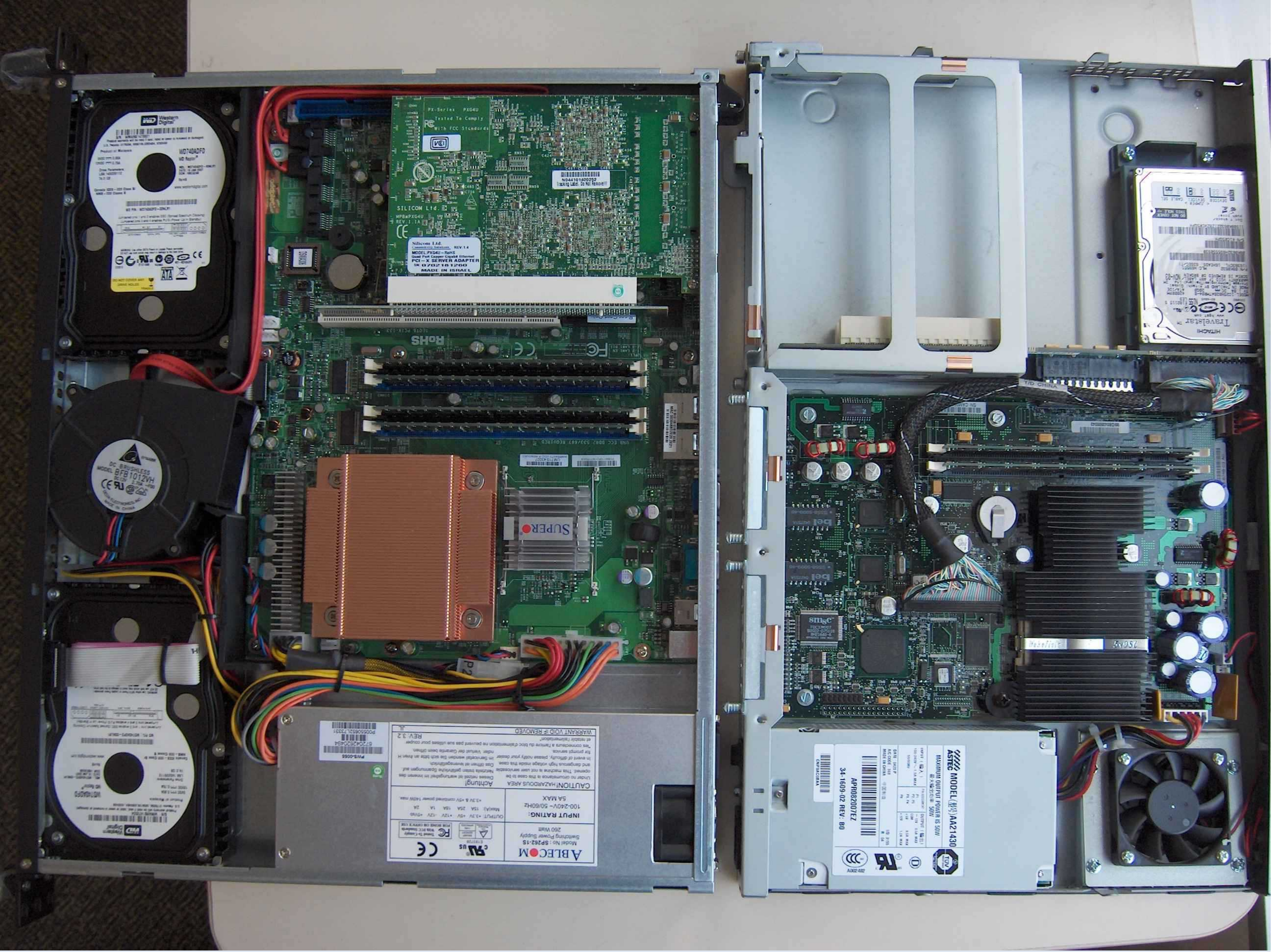
The 4215 processes only 8.61% of the entire amount of packets sent, while the MBX machine processes 98.55% of the entire amount of packets sent.

The 4240 and the MBX saw about the same amount of packets but snort on the 4240 dropped approximately 19% of the packets.

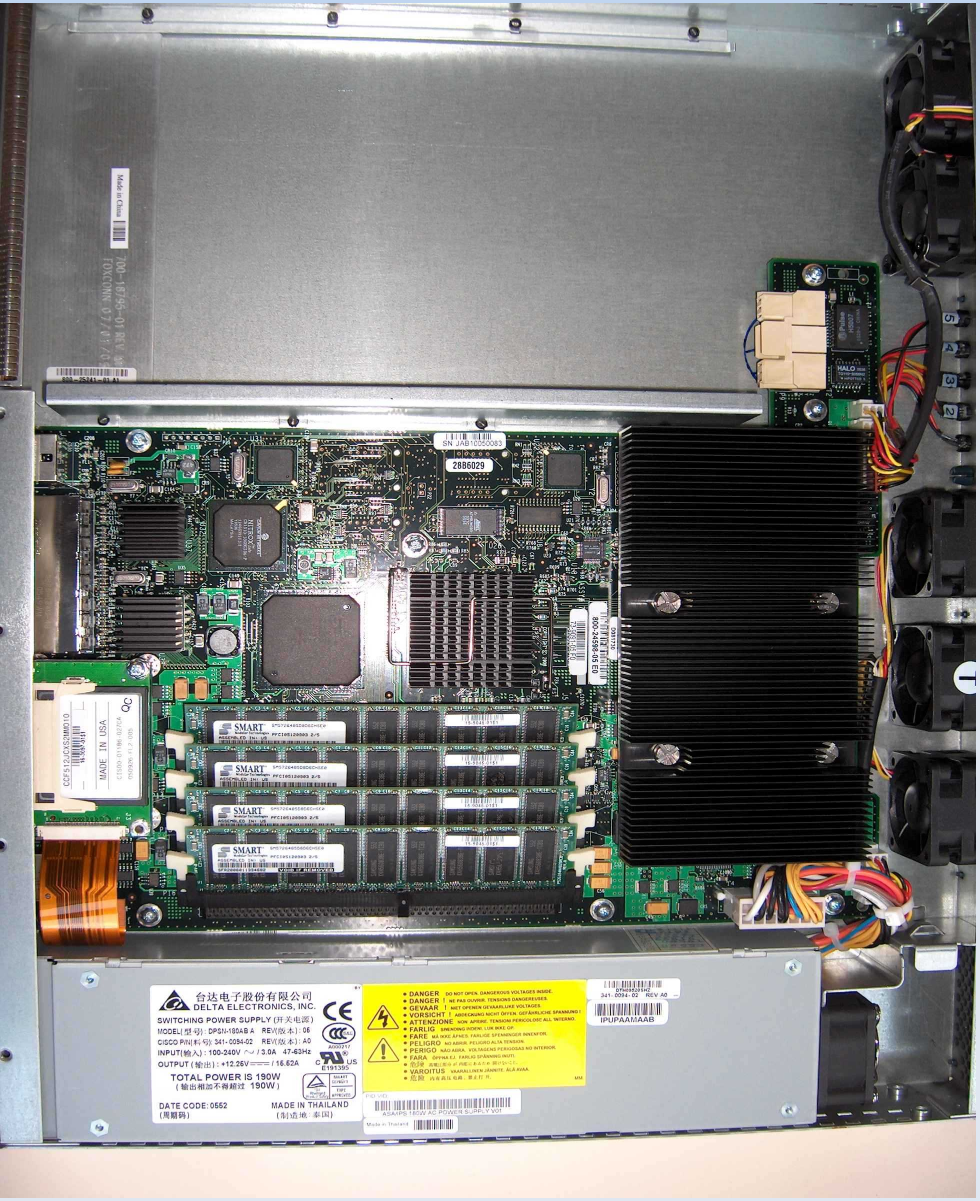
MBX Hardware

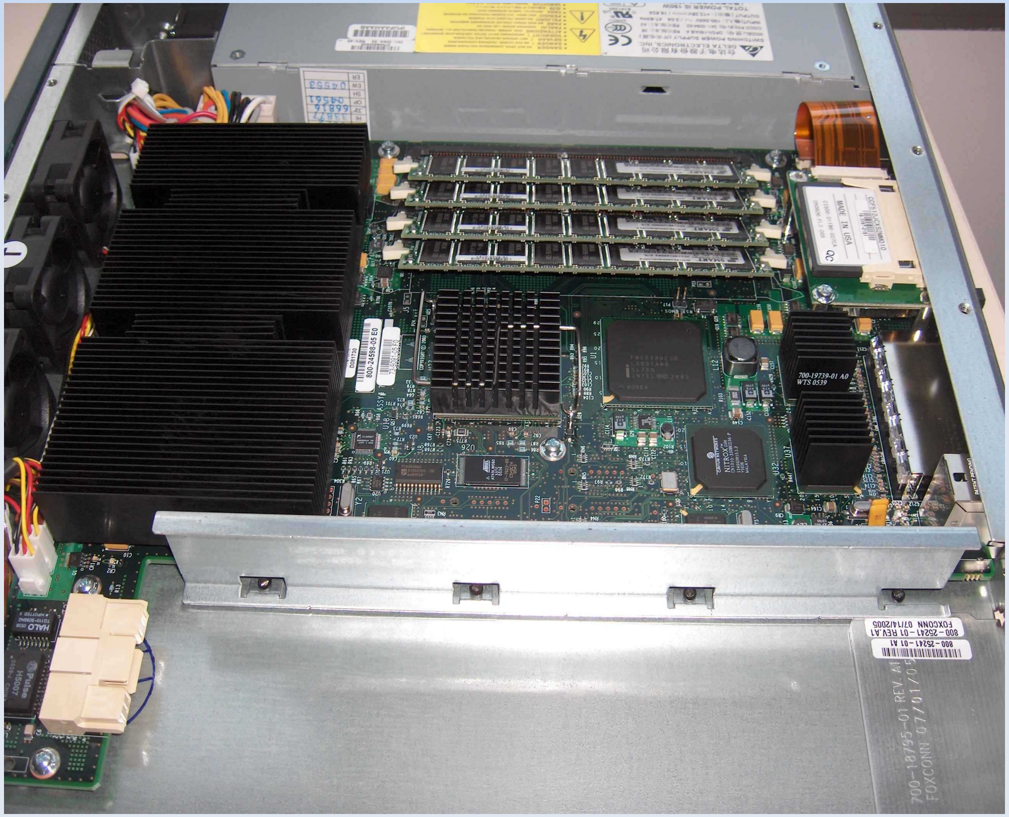


- All name brand components
- Option for high-end options
- Well designed/cooled
- Upgradeable
- Inexpensive in comparison


Western Digital
WD740ADFD
PX-Series PXG4U
SILICOM Ltd.
Silicom Ltd.
MODEL:PXG4U-RoHS
PCI-X SERVER ADAPTER
MADE IN ISRAEL
RoHS
DC BRUSHLESS
MODEL BFB1012VH
SUPER
ABLECOM
SP262-1S
260 Watt
CAUTION!HAZARDOUS AREA
Achtung!
WARRANTY VOID IF REMOVED
Travelstar
HITACHI
ASTEC MODEL AA21430
34-1609-02 REV: B0
SMSC
bel

Model 4240


Made in China
700-18795-01 REV A1
FOXCONN 07/01/05
800-25241-01 A1
SN JAB10260083
28B6029
800-24598-05 E0
SMART
HALO
台达电子股份有限公司
DELTA ELECTRONICS, INC.
SWITCHING POWER SUPPLY (开关电源)
MODEL(型号): DPSN-180AB A REV(版本): 06
CISCO P/N(料号): 341-0094-02 REV(版本): A0
INPUT(输入): 100-240V ~ / 3.0A 47-63Hz
OUTPUT (输出): +12.26V ⎓ / 16.52A
TOTAL POWER IS 190W
(输出相加不得超过 190W)
DATE CODE: 0552
(周期码)
MADE IN THAILAND
(制造地: 泰国)
A000217
E191395
DANGER DO NOT OPEN. DANGEROUS VOLTAGES INSIDE.
DANGER ! NE PAS OUVRIR. TENSIONS DANGEREUSES.
GEVAAR ! NIET OPENEN GEVAARLIJKE VOLTAGES.
VORSICHT ! ABDECKUNG NICHT ÖFFEN. GEFÄHRLICHE SPANNUNG !
ATTENZIONE NON APRIRE. TENSIONI PERICOLOSE ALL 'INTERNO.
FARLIG SPÆNDING INDENI. LUK IKKE OP.
FARE MÅ IKKE ÅPNES. FARLIGE SPENNINGER INNENFOR.
PELIGRO NO ABRIR. PELIGRO ALTA TENSION.
PERIGO NÃO ABRA. VOLTAGENS PERIGOSAS NO INTERIOR.
FARA ÖPPNA EJ. FARLIG SPÄNNING INUTI.
VAROITUS VAARALLINEN JÄNNITE. ÄLÄ AVAA.
危险 内有高压电器，禁止打开。
DTH09520SHZ
341-0094-02 REV A0
IPUPAAMAAB
ASA/IPS 180W AC POWER SUPPLY V01
Made in Thailand


800-24598-05 E0
700-19739-01 A0
WTS 0539
MADE IN USA
NITROX
HALO
FOXCONN 07/14/2005
800-25241-01 REV A1
800-25241-01 A1
700-18795-01 REV A1
FOXCONN 07/01/05
DELTA ELECTRONICS, INC.
TOTAL POWER IS 190W

Pulled Trigger Feb. 2007

- Tested new hardware in place of existing
- Fantastic results
- Many additional features e.g.
  - Port bonding (eases Tap input/Increases bandwidth)
  - Easily replaceable/upgradeable hardware
  - Highly reliable hardware
- Ordered replacements for all NIDS 100+
- Ordered separate build and test systems

ISSO Appliance Implementation

- Sever ties with COTS vendor
- Launch the “ISSO Appliance”

Debian Build Process

- Build with fai (fully-automated installer) via PXE
- Documented process for an assembly-line
- Deployed APT-Proxy for patches
- Deployed APT-Repository for custom debs
- Appliance-ish install
  - Labeled NICS for easy change
  - Include color “Dell Like” instructions for local staff

Change Mindset to NS

- Network Sensor, more than just a NIDS
- Create framework for modularity on NS
- Flow data collection
- URL parsing
- Ad-hoc packet capture
- Specialized packet-capture (i.e. dns,http)
- Regional syslog collection*

Custom APT-Repo Packages

- Argus
- URLSnarf
- Snort
- SSH-Confs
- System-Confs
- Ad-Hoc

Next Steps

- Finish deployment of MBX boxes
- Develop and integrate VPN for mgmt traffic
- Automate deb package creation process
- Consider logging improvements

Final Thoughts

- Due diligence – demand quality from vendors
- Carefully consider your position as a customer
- FOSS is powerful and useful in the enterprise
- When you can't find a product you are happy with, consider making it yourself
  - Much more functionality
  - May not be the cheaper option
- An appliance solution is not necessarily auto-pilot, but this path may void your warranty

Sean Wilkerson
sean@aleric.net