# Managing 600 OpenBSD-based Firewalls in Microsoft-Centric Small and Medium Businesses

Lawrence Teo

lawrence.teo@calyptix.com

www.calyptix.com


The New York City BSD Conference (NYCBSDCon) 2010

November 13, 2010

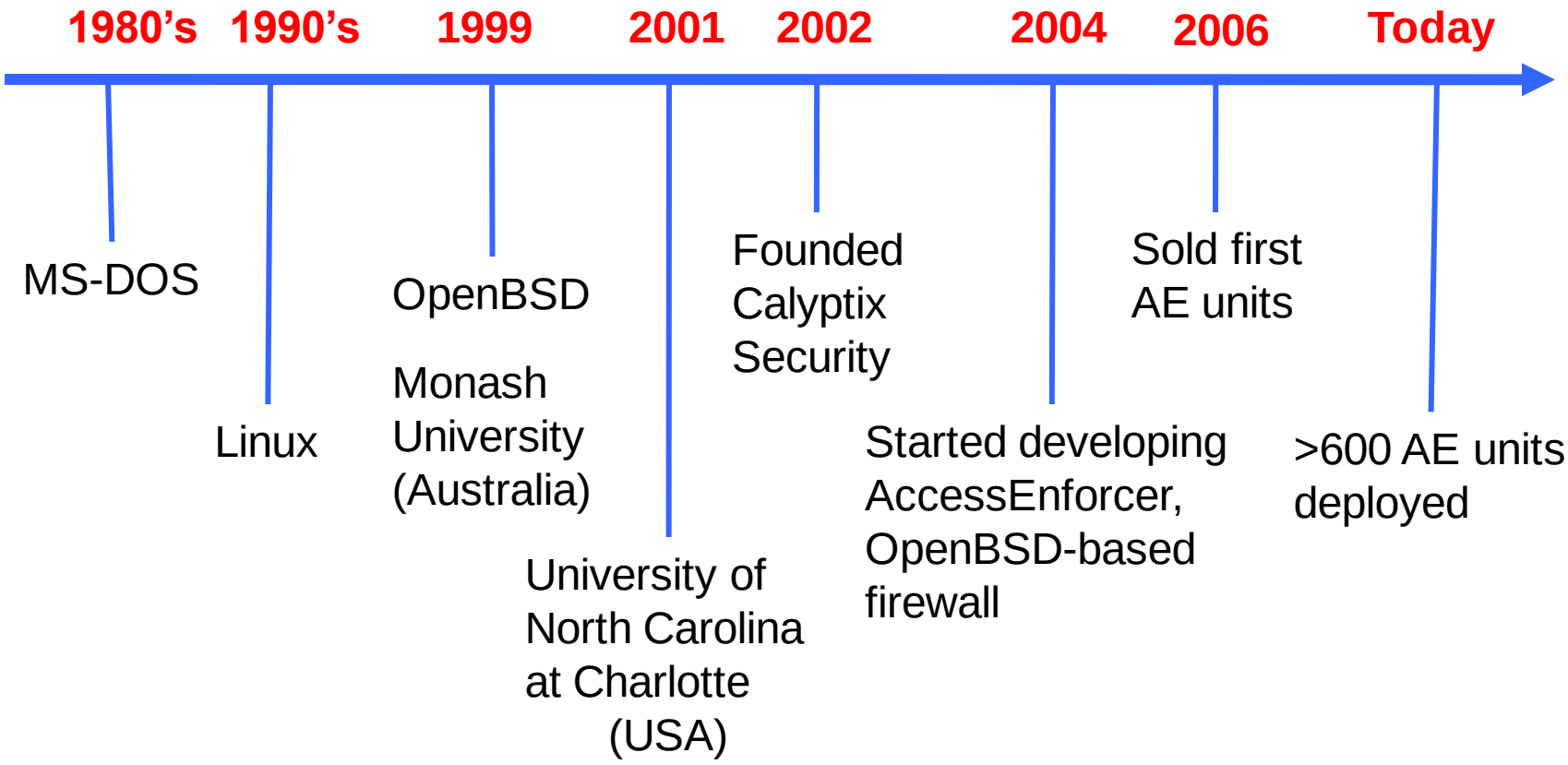
# Outline

calyptix™ SECURITY

- AccessEnforcer: OpenBSD-based firewall
- Overview of development
- How OpenBSD is used
- Packaging and updates
- Challenges & lessons learned
- Conclusion

# Timeline

calyptix™ SECURITY



# AccessEnforcer

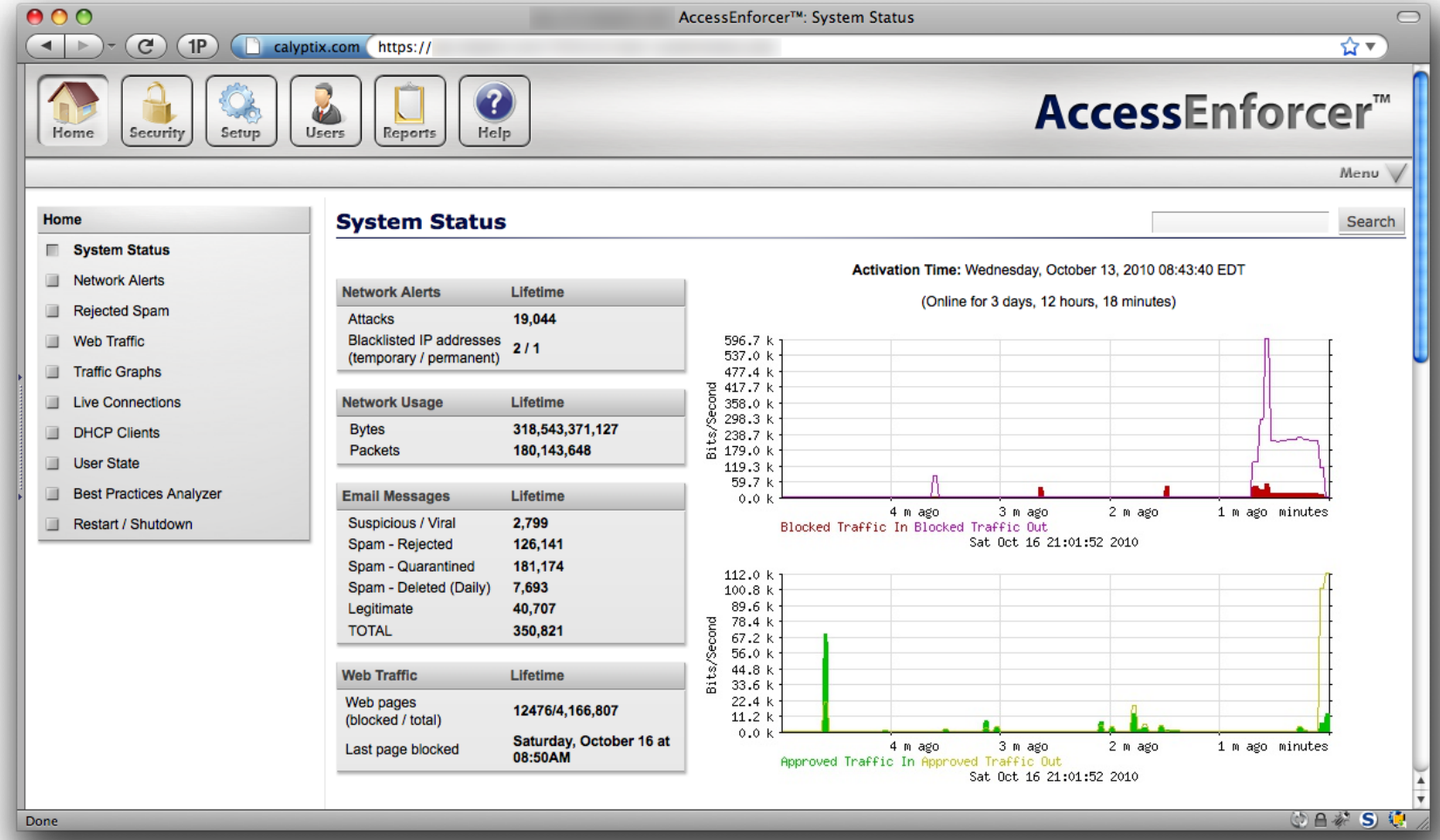
calyptix™ SECURITY

- **An OpenBSD-based multifunction firewall**
  - A Unified Threat Management (UTM) appliance
  - Built for SMB IT professionals who use Microsoft-centric products and technologies
- **Functionality**
  - Firewall (PF)
  - IDS/IPS (Snort)
  - Email filtering (spam & antivirus)
  - Web filtering
  - IPsec VPN
  - CalyptixVPN (OpenVPN)
  - Active Directory integration
  - Reporting

AE3000

# AccessEnforcer GUI

calyptix™ SECURITY



# AccessEnforcer Models

calyptix™ SECURITY


**AE750** — **Up to 10 users**


**AE1000** — **Up to 25 users**


**AE2000** — **Up to 50 users**


**AE3000** — **Up to 100 users**

Standard GUI across all units

# My official role at Calyptix

calyptix™ SECURITY

Code!

# My REAL role at Calyptix

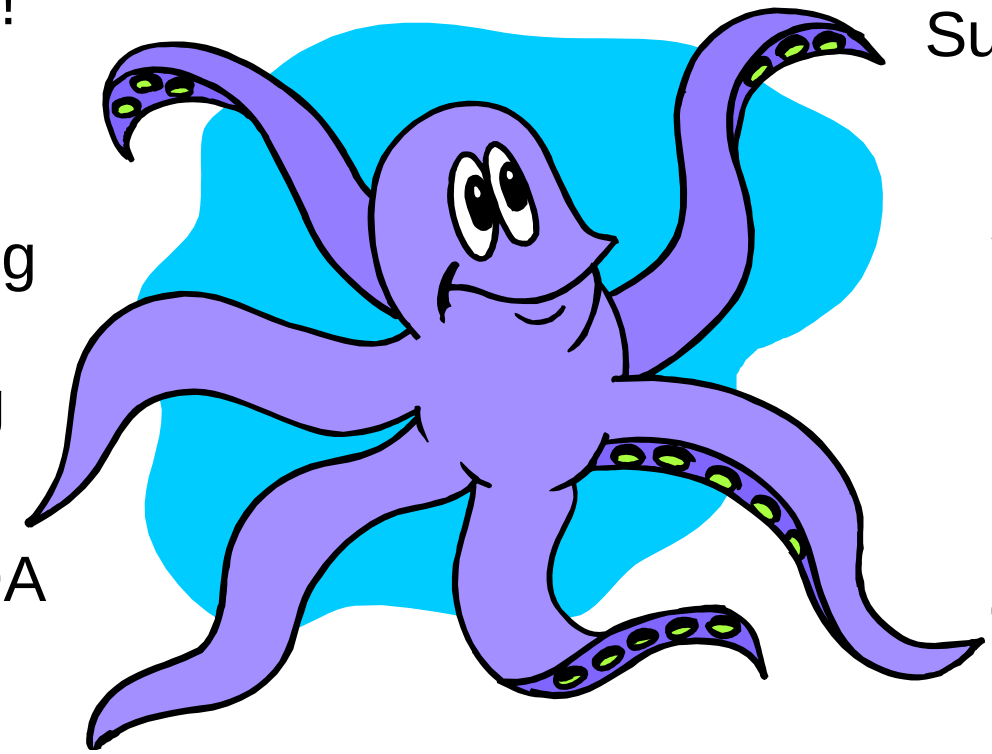
calyptix™ SECURITY

Code!

Release engineering

Provide training

Testing & QA



Interface with sales & marketing

Support/firefighting

Strategy

Admin UNIX servers

Oversee manufacturing

Booth bunny

# Microsoft-Centric SMB defined

calyptix™ SECURITY

- 1 to 250 users
- Most are in the < 25 range
- IT Manager
  - Usually an outside IT consultant/firm
  - Larger sites may have an inside IT manager
  - Microsoft specialist; little to no UNIX experience
- Microsoft-centric products
  - 95% have a Windows Server (almost always Small Business Server) with Microsoft Exchange
  - Active Directory
  - Microsoft Outlook, Office, SharePoint, etc

# Our SMB customers

calyptix™ SECURITY

- CPA firms
- Law firms
- Furniture stores
- Private schools
- Churches
- Hotels
- Doctors' offices
- Restaurants
- Hospitals
- Chemists
- Defense contractors
- Software development firms
- Manufacturing firms
- Museums
- Firehouses
- Chambers of commerce
- Funeral homes
- *Also a few home users…*

# Why Microsoft-Centric SMBs?

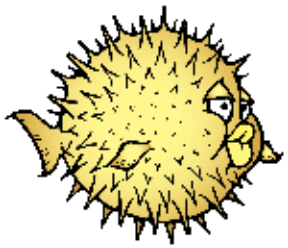
calyptix™ SECURITY

- SMBs are the backbone of the US economy
  - **>26 million SMBs** in the USA
  - Half of all private sector jobs
  - Created **~70% of all new jobs** in past decade
- Small businesses
  - Least IT resources
  - Budget constraints
  - A serious security incident could affect the entire company
- Microsoft Windows
  - Most popular = Most targeted!
- **Needs security the most!**

# Why OpenBSD?

calyptix™ SECURITY

- Security and code quality
  - Secure by default
  - Readable, peer-reviewed code
- Simplicity and practicality
  - Sane defaults
  - Less is more
- Great documentation
  - Documentation is not an afterthought
  - Readable man pages!

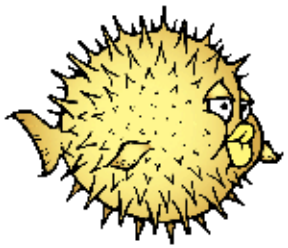


OpenBSD

# Why OpenBSD?

calyptix™ SECURITY

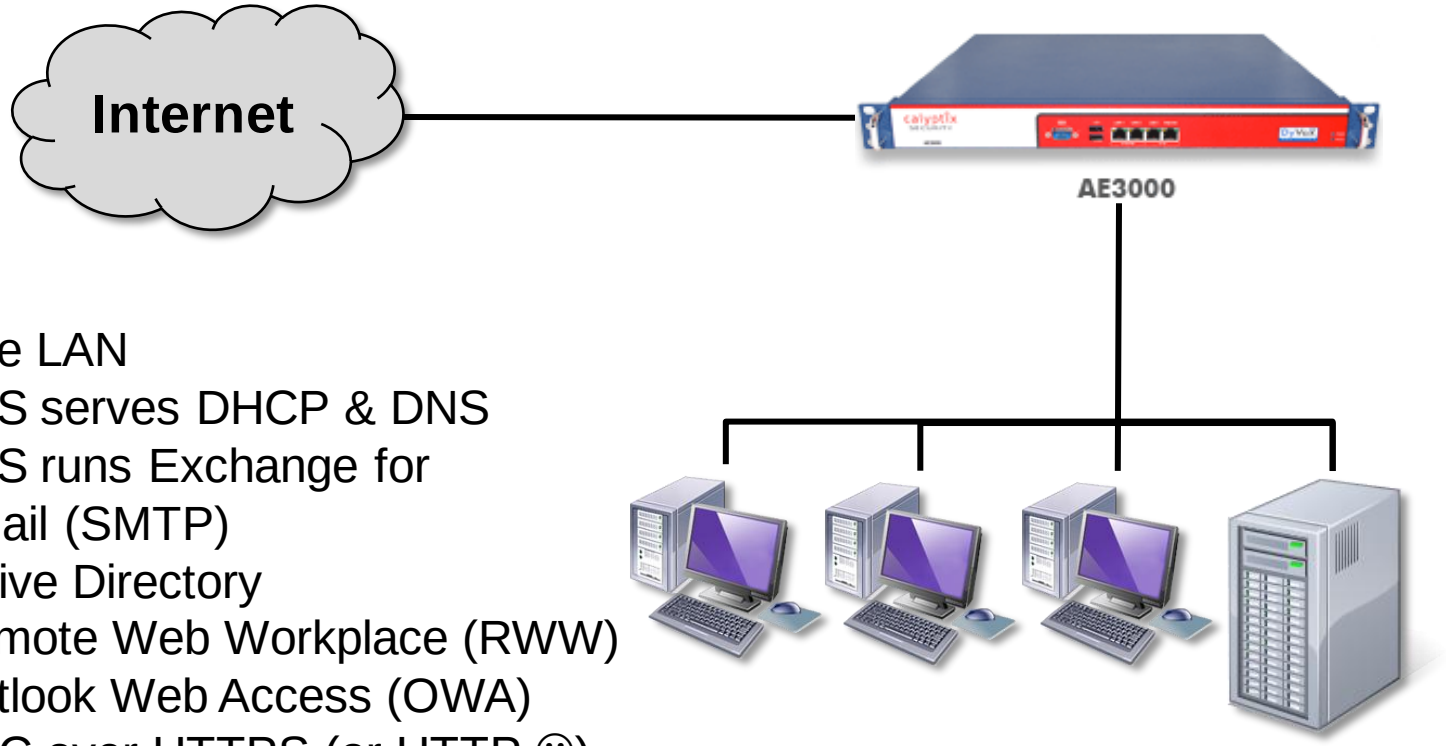
- Great development environment out of the box
  - Convenient data structures for C: queue.h, tree.h
  - Secure coding facilities: strlcpy(3), strlcat(3), strtonum(3), arc4random(3)
  - Features like ProPolice help detect bugs in our software
  - Useful libraries and tools in base, e.g. libevent, tmux, etc.
- PF (and access to latest version of PF)
- True Freedom
  - It's really free! Unencumbered code in base
  - Thorough license audit



OpenBSD

# Most Common Deployment

calyptix™ SECURITY




- One LAN
- SBS serves DHCP & DNS
- SBS runs Exchange for email (SMTP)
- Active Directory
- Remote Web Workplace (RWW)
- Outlook Web Access (OWA)
- RPC over HTTPS (or HTTP ☹)
- Remote Desktop Protocol (RDP)
- SharePoint
- PPTP ☹

# AccessEnforcer Development

# Design Decisions

calyptix™ SECURITY

For the Microsoft-trained IT Manager:

- Web interface GUI
  - Limited CLI shell for recovery
- Make it easy
  - Admin should not need to know *any* UNIX whatsoever to operate the product
- Simplicity and sane defaults!
  - As few knobs as possible
  - Just the stuff they need (no BGP, etc)
- Seamless integration with Microsoft products
  - Especially Windows Small Business Server

# Design Decisions

calyptix™ SECURITY

Our own requirements:

- Secure by default as much as possible
  - Each unit has randomly-generated default passwords (no two units have same passwords)
  - HTTPS-only web interface
- Discourage or do not support weak protocols
  - Definitely no telnet server!
  - Example: DES intentionally not supported, MD5 highly discouraged
- It should "just work"

# Our Dev Environment

calyptix™ SECURITY

- C, Ruby, Korn shell, Perl, PHP, Lua, some C++
- Visual Studio for Windows apps
- PostgreSQL
- Started with CVS, recently moved to Git
- Source tree compiled using BSD make
- Multi-platform development environment
  - OpenBSD
  - Windows XP, Vista, 7
  - Windows SBS 2003, SBS 2008
  - Mac OS X 10.5, 10.6
  - Ubuntu Linux

# Adopted OpenBSD practices

calyptix™ SECURITY

- Source tree organized roughly according to hier(7)
  - Compiled with BSD make; no autotools, thankfully
- Coding style
- Code auditing and review
  - Manual review each other's code
  - Review of GUI code for web application security issues, e.g. SQL injections, cross-site scripting, and CSRF
  - Static analysis with LLVM clang
- Branch name conventions (e.g. AEF_3_0)
- -Wall

# AccessEnforcer versions

calyptix™ SECURITY

- AccessEnforcer v1.0 (Ancient History; EOL'ed)
  - OpenBSD 3.8
- AccessEnforcer v2.0
  - OpenBSD 4.0, with backported security fixes and programs from OpenBSD CVS
- AccessEnforcer v3.0
  - OpenBSD 4.7, with errata patches

# How OpenBSD is used

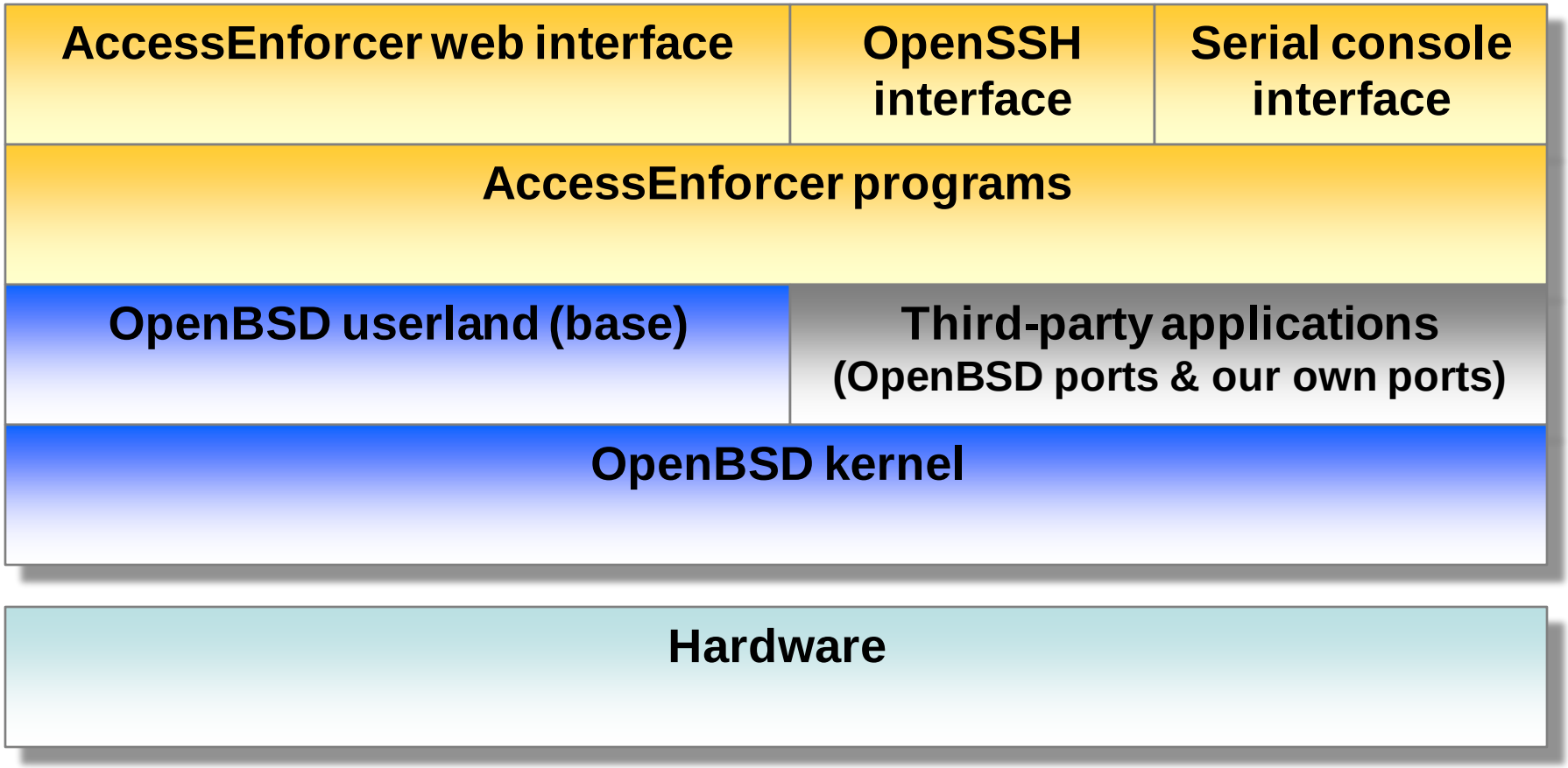
# How OpenBSD is used

calyptix™ SECURITY

- Minimal installation
  - bsd, bsd.rd, base47.tgz, and etc47.tgz
- GENERIC kernel
- Many base tools, some with modifications
- PF enabled
  - NAT, rdr-to for port forwarding rules, and a LOT of other networking functions

# Software Stack

calyptix™ SECURITY



# Changes to OpenBSD

calyptix™ SECURITY

- /etc/rc replaced with our own startup script
- No rc.conf
- Init scripts placed in init.d
  - Generally a conf script to generate the config file
  - Init script to start/restart/stop program
  - Background watchdog program to ensure all programs in correct state
- Turned off unused services (echo, daytime, etc)

# OpenBSD base tools

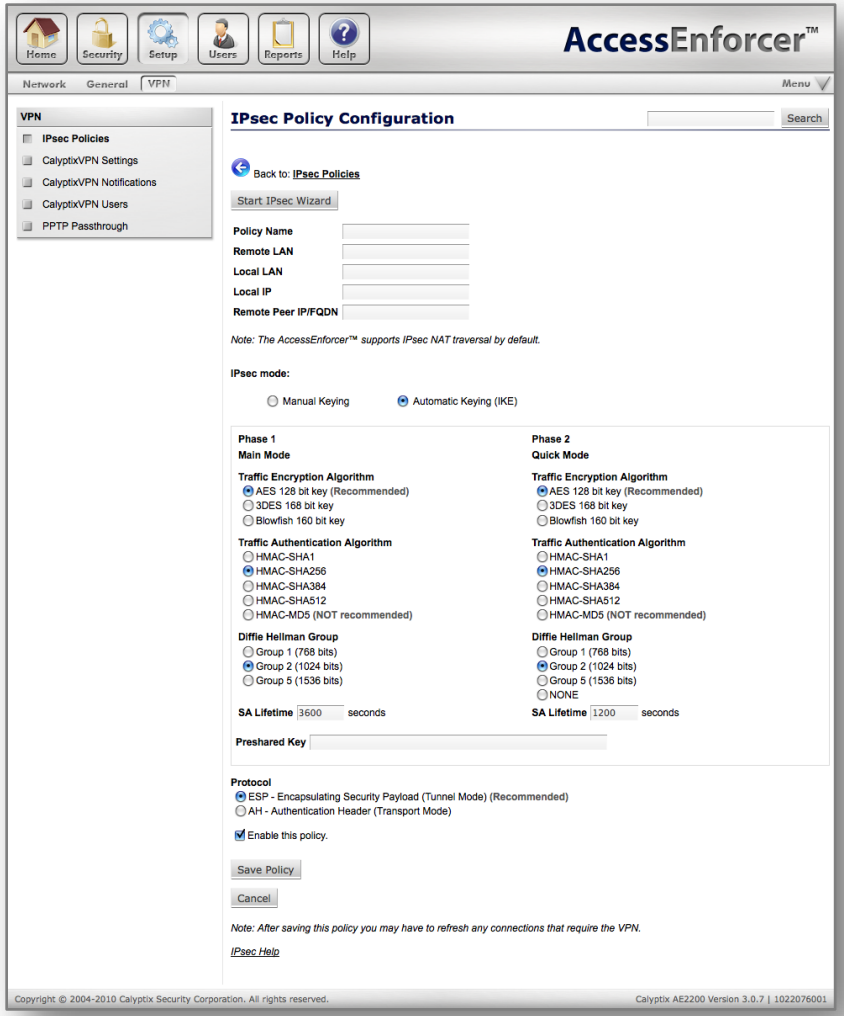
calyptix™ SECURITY

- **Firewall & Networking**
  - ifconfig, pfctl, ftp-proxy
- **DHCP**
  - dhcpd, dhclient
- **IPsec VPN**
  - ipsecctl, isakmpd
- **Diagnostic tools**
  - arp, dig, ping, traceroute, tcpdump, whois
- **Monitoring**
  - snmpd, syslogd
- **Many more…**
  - Examples: ntpd, halt, ifstated, etc.

# Example: IPsec VPN

calyptix™ SECURITY

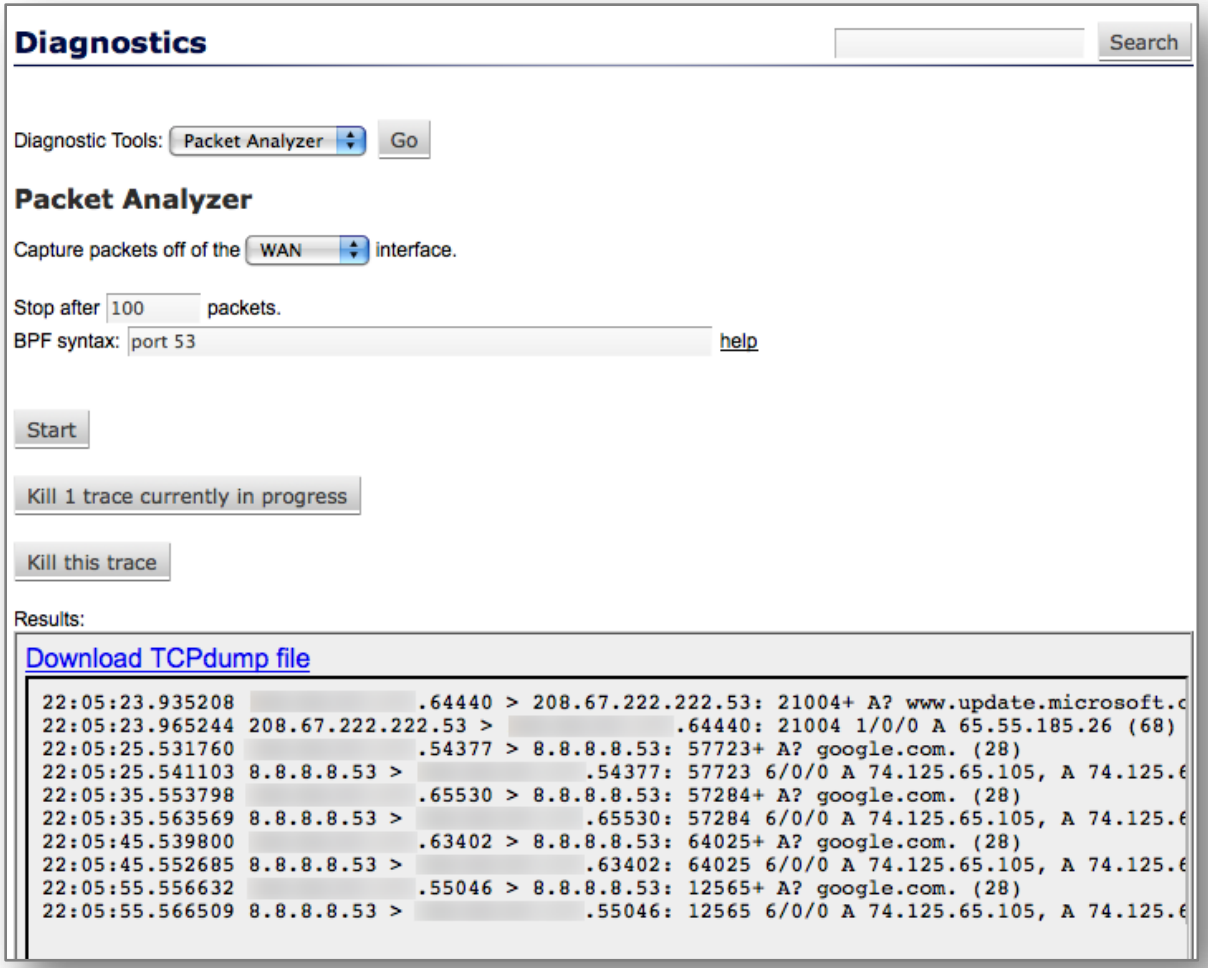
- Powered by ipsecctl(8), isakmpd(8) and ipsec.conf
- Manual keying and automatic keying
- Encryption and authentication algorithms
- Single-page setup!



# Example: tcpdump

calyptix™ SECURITY

- Packet Analyzer diagnostic tool
- Accepts BPF syntax



# Packaging

# Packaging/Update Decisions

calyptix™ SECURITY

- How to package and update…
  - Our own software
  - Kernel
  - Errata patches
  - Third-party applications (ports) that need modification
  - Nightly updates, like virus signatures
- Writing our own packaging tool vs. using OpenBSD's pkg_* tools

# Kernel Port

calyptix™ SECURITY

```
COMMENT=       OpenBSD kernel

DISTNAME=      kernel-${OSREV}.20100317
PKGNAME=       ${DISTNAME}p1
CATEGORIES=    kernel
MASTER_SITES=  ${FTP_MIRROR}/${OSREV}/

# For common errata patches
MASTER_SITES0=  ${FTP_MIRROR}patches/${OSREV}/common/

# For architecture-specific errata patches
MASTER_SITES1=  ${FTP_MIRROR}patches/${OSREV}/${ARCH}/

PREFIX=/
```

# Kernel Port

calyptix™ SECURITY

```
ERRATA_COMMON+= 002_mpi.patch:0
ERRATA_COMMON+= 004_pfsync.patch:0
ERRATA_COMMON+= 005_pfsync.patch:0
ERRATA_COMMON+= 006_scsi.patch:0
ERRATA_COMMON+= 007_scsi.patch:0

ERRATA_ARCH+=

SRC_FILES=      sys.tar.gz

DISTFILES=  ${SRC_FILES} ${ERRATA_COMMON} ${ERRATA_ARCH}
DIST_SUBDIR=    ${PKGNAME}
```

# Kernel Port

calyptix™ SECURITY

**do-extract:**

```
cd ${WRKDIR} ; tar zxvf ${DISTDIR}/${DIST_SUBDIR}/${SRC_FILES}
```

**pre-patch:**

```
cd ${WRKDIR}/sys ; \
for i in `/bin/ls ${DISTDIR}/${DIST_SUBDIR}/*.patch`; \
do \
        patch -t -p1 < $$i; \
done
```

# Kernel Port

calyptix™ SECURITY

**do-build:**

```
.for conffile in GENERIC GENERIC.MP
        ( cd ${WRKDIR}/sys/arch/${ARCH}/conf ; \
        config ${conffile} ; \
        cd ${WRKDIR}/sys/arch/${ARCH}/compile/${conffile}; \
        make depend && make )
.endfor
```

**do-install:**

```
        install -m 0755 -o root -g wheel \
                ${WRKDIR}/sys/arch/${ARCH}/compile/GENERIC/bsd \
                ${PREFIX}/bsd.sp
        install -m 0755 -o root -g wheel \
                ${WRKDIR}/sys/arch/${ARCH}/compile/GENERIC.MP/bsd \
                ${PREFIX}/bsd.mp
```

# Packing Errata Patches

calyptix™ SECURITY

- Errata patches built using a chroot environment
- Results in errata packages that can be added via pkg_add
- http://labs.calyptix.com/openbsd-binary-patches-chroot.php

# errata-base port

calyptix™ SECURITY

- Extract OpenBSD's file sets (baseXX.tgz, compXX.tgz, etc) to /var/errata-base
- You will end up with all the files and directories of a bare OpenBSD system

$ **ls /var/errata-base/**

altroot dev home root stand tmp var
bin etc mnt sbin sys usr

# Errata Port for 4.7 001_kerberos

calyptix™ SECURITY

```
ERRATA_NAME=    001_kerberos
ERRATA_ARCH=    common
ERRATA_DATE=    20100331

BUILD_STEPS= "( \
    cd /usr/src/lib/libkrb5 ; \
    make obj ; make depend ; make ; make install ; \
    cd /usr/src/kerberosV/libexec/kdc ; \
    make obj ; make depend ; make ; make install \
)"

BUILD_DEPENDS=  :errata_base_$(OSREV)_$(MACHINE)-*:errata/$(OSREV)/base

.include "../bsd.errata.mk"
.include <bsd.port.mk>
```

# bsd.errata.mk

calyptix™ SECURITY

- Download patch
- Apply patch to /var/errata-base/usr/src
- Generate build script
- Move /var/errata-base/dev out of the way
- Create a memory filesystem at /var/errata-base/dev with the contents of the original
- Run “/var/errata-base/dev/MAKEDEV std”
- Chroot to /var/errata-base and run build script

# Build script

calyptix™ SECURITY

- Touch a “pre-build” cookie
- Run build steps defined in errata port (e.g. cd /usr/src/lib/libkrb5 ; make ..)
- Touch a “post-build” cookie
- Generate a packing list using find(1) to find all files:
  - That changed after pre-build cookie
  - That changed before post-build cookie
  - Excluding /usr/src, /usr/obj, /usr/share/man, /usr/include
- Create a tarball of the changed files

# Other ports

calyptix™ SECURITY

- Some stock OpenBSD ports require X11
  - Modified ports to work without X11
- Custom ports
  - Modified to provide better integration with our programs or remove unnecessary dependencies
  - Example: ClamAV does not need zoo, lha, arc archivers in the Microsoft world
- Dynamic ports
  - ClamAV virus signatures, spam signatures, URL blacklist database, etc.

# clamav-virus-sigs dynamic port

calyptix™ SECURITY

**clamav-virus-sigs Makefile:**

```
COMMENT=        ClamAV virus signatures

PKGNAME=    clamav-virus-sigs-${TS}
CATEGORIES=     security
MASTER_SITES=   ${HOMEPAGE}

…
```

**External shell script:**

```
TS=`date +'%Y-%m-%d %H:%M:%S'`
make
```

# Managing Updates

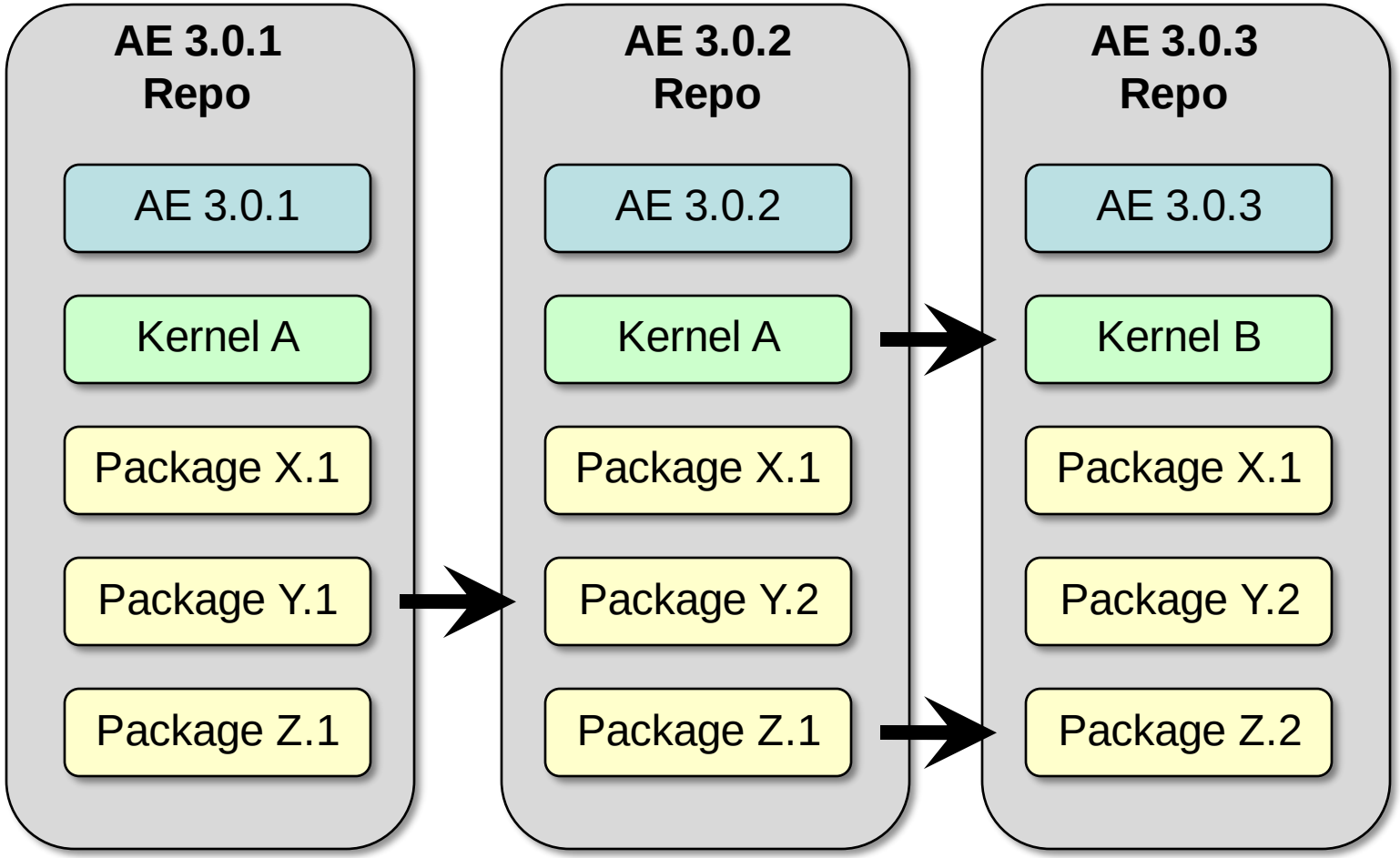
# Update mechanism

calyptix™ SECURITY

- SSL-based update client/server system
  - Mutual authentication
- Two types of updates
  - Nightly packages (e.g. ClamAV virus signatures and spam patterns)
  - Major updates (e.g. v3.0.1 to v3.0.2)
- Update mechanism updates packages using the OpenBSD pkg_* tools

# Update repositories

calyptix™ SECURITY



# Update rollout

calyptix™ SECURITY

- >600 units
- Tuesdays, Wednesdays, Thursdays
  - Avoid Microsoft Patch Tuesday
- Between 2am and 5am
- Client notified by email a week before scheduled update
- Phased rollout
  - New releases are rolled out to authorized reseller partners' own units first, then their clients
  - Bugs and issues caught early

# OpenBSD 4.0 to 4.7 upgrade

calyptix™ SECURITY

- **NOTE: This is work in progress! Not tested in production!**
- Download 4.7 file sets
- Backup old kernel, /sbin/reboot, and /bin/rm
- Extract base47.tgz
- Create a cookie and reboot
- On reboot, rc script detects cookie, performs upgrade steps from faq/upgrade4{1..7}.html, and other steps
- Reboot

# Challenges & Lessons Hopefully Learned

# Challenges: Microsoft

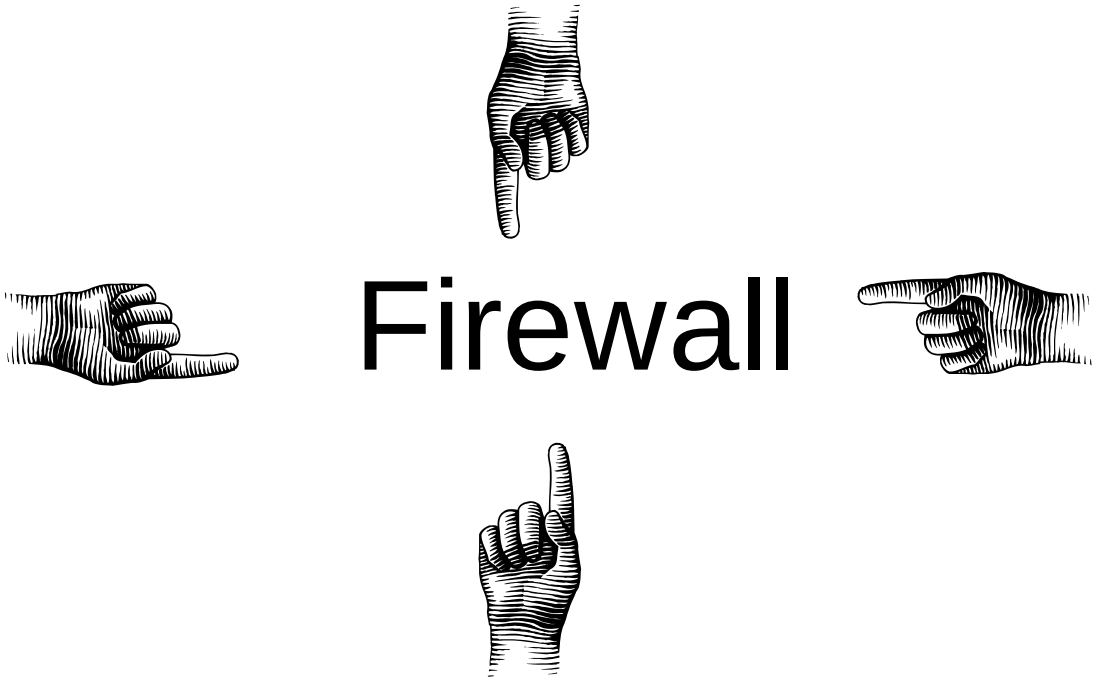
calyptix™ SECURITY

- Updates break things (surprise!)
- Windows Server insists on being DHCP and DNS server
- Upgraded system != New system
- Remote WMI and GPO may not work as expected
- Diversity of Windows systems
- UAC and OpenVPN
- Exchange rewrites headers
- PPTP and PF

# Challenges: NKOTB

calyptix™ SECURITY

"Something is wrong. Who gets the blame?"



# Challenges: "I don't care!"

calyptix™ SECURITY

- ~~Nobody~~Very few people truly care about security in the small business world
- "I just want it to work!"
- Plaintext passwords
  - Vendors building products based on plaintext FTP ☹
  - RPC or OWA over HTTP ☹
  - Sending passwords via email ☹
- Business owner wants to be exempted from all security filters

# Challenges: Keeping Up

calyptix™ SECURITY

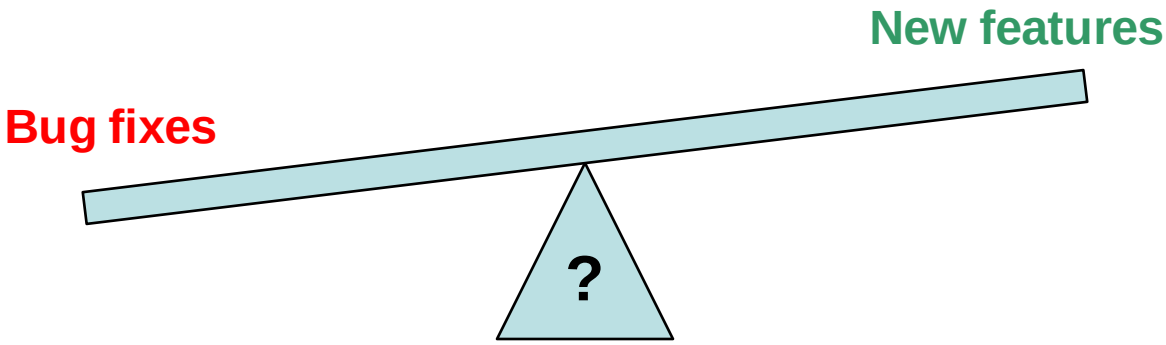
- New technologies
  - Cloud, virtualization, etc.
- New mobile devices
  - iPhones, Android, etc.
- Lack of standards
  - VOIP phones


Image source: http://commons.wikimedia.org/wiki/File:NYC_subway-4C.svg

# Lessons Hopefully Learned

calyptix™ SECURITY

- It's not about you, it's about the user
- But the customer is not always right
- Match your users' environment as closely and as early as possible
- Build self-help tools as soon as possible!
  - Knowledgebase articles, forums, etc.
  - Training



# Conclusion

calyptix™ SECURITY

- OpenBSD is a great development platform!
  - Great tools and documentation
  - Excellent development practices can be adopted in a commercial dev environment
- Simplicity and sane defaults make sense in any product
- OpenBSD thrives in non-UNIX environments
  - More than 600 Microsoft-centric SMB sites, running OpenBSD!

# Thank You!

calyptix™ SECURITY

Questions?

Lawrence Teo
lawrence.teo@calyptix.com
Twitter: @lteo

www.calyptix.com