Release your FreeBSD

Part I

Yung-Zen Lai (yzlai@hotmail.com)

2003/11

Agenda

- Hour 1 (Basic FreeBSD)
  - Installation
  - Environment Settings
  - Upgrade, Kernel/World making
- Hour 2
  - Firewall – ipfw/ipfilter
  - NAT, VPN(PPTP)
- Hour 3
  - Ports/Packages
  - Apache
  - Postfix, AMaViS, SpamAssassin

Installation

- FreeBSD 4.9-RELEASE
  - the latest release of the FreeBSD -STABLE development branch.
  - support for large memory(> 4GB) i386 machines with Page Address Extensions (PAE)
- FreeBSD Handbook
  - http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/index.html

Installation (cont.)

- CD-ROM
  - ftp://ftpX.tw.freebsd.org/pub/releases/i386/ISO-IMAGES/4.9/4.9-i386-disc[12].iso
  - Disc1 is enough to install FreeBSD base
- Network
  - ftp://ftpX.tw.freebsd.org/pub/releases/i386/4.9-RELEASE/floppies/
    - kern.flp & mfsroot.flp
  - Media FTP: ftp://ftpX.tw.freebsd.org/pub/releases/

Installation (cont.)

- Slice **è** Logical Partitions
- Post Install Configure
  - Root Password
  - Time Zone
    - Set to local time
    - 5 Asia/43 Taiwan
  - Networking
    - Interfaces
    - inetd

Environment Settings

- /boot/loader.conf, /etc/sysctl.conf
- /etc
  - rc.conf, make.conf
  - csh.cshrc, csh.login
  - syslog.conf, newsyslog.conf
  - hosts, hosts.allow, hosts.deny
  - ftpusers, inetd.conf
  - cron
  - ssh/sshd_config

Upgrade

- CTM
- CVSup
  - (/usr/local)/etc/cvsupfile-*
    - tag=XXXX
  - run_cvsup
  - /etc/make.conf KERNCONF
  - make update
  - dmesg
- make (build/install)world >&! /tmp/mw.log &
- make (build/install)kernel >&! /tmp/mk.log &

Host-Based Firewall

- ipfw
  - first match
  - ipfw add/delete
  - ipfw list/flush
  - IPFIREWALL in KERNCONF
- ipfilter
  - best match
  - ipf -F <a|i|o|s|S> -f <filename>
  - ipfstat -i/-o
  - IPFILTER in KERNCONF

ipfw rules

- ipfw add
  - <allow|deny|reset>
  - <ip|tcp|udp|icmp>
- from
  - <src-ip> <src-port>
- to
  - <dst-ip> <dst-port>
- <flags> / <via interface>

ipfw rules (cont.)

- Allow packets that match rule
  - allow | accept | pass | permit
  - ipfw add allow all from me to any
  - ipfw add allow all from bbs to me
- Discard packets that match this rule.
  - deny | drop
  - ipfw add deny all from any to 224.0.0.0/8
- Send some notice back
  - reset(TCP), unreach <code>(ICMP)
  - ipfw add reset tcp from any to any 23

ipfw rules example

- # Telnet/SSH access control (controlled by hosts.allow)
  - ipfw add pass tcp from any to me 22 setup
  - ipfw add pass tcp from any to me 23 setup
- # Allow setup of SMTP/POP3
  - ipfw add pass tcp from any to me 25 setup
  - ipfw add pass tcp from any to me 110 setup
- # Allow setup of DNS
  - ipfw add pass tcp from any to me 53 setup
  - ipfw add pass udp from any to me 53
- # Default to deny
  - ipfw add add 65500 reset log tcp from any to any

ipfilter rules

- pass|block|nomatch
  - in|out
- proto
  - <tcp|udp|icmp>
- from
  - <src-ip> <port = XX>
- to
  - <dst-ip> <port = XX>
- flags <flags>

ipfilter rules (cont.)

- Allow packets that match rule
  - pass out from 163.21.249.172 to any
  - pass in from bbs to any
- Discard packets that match this rule.
  - block in proto udp from any to any port = 137
  - block in proto udp from any to any port = 138
- Send some notice back
  - block return-rst in proto tcp all flags S
  - block return-icmp[return-code]
- Resources: http://www.ipfilter.org/

ipfilter rules example

- # Telnet/SSH access control (controlled by hosts.allow)
  - pass in proto tcp from any to any port = ssh flags S keep state
  - pass in proto tcp from any to any port = telnet flags S keep state
- # Default to deny
  - block in log all
  - block return-rst in proto tcp all flags S

NAT(ipfw)

- /etc/rc.conf
  - gateway_enable=“YES”
  - natd_enable=“YES”
  - natd_interface=“”
- /sbin/natd
  - -a address
  - -n interface
- ipfw
  - divert natd all from any to any via <interface>
- Using userland natd, less effective.

NAT(ipfilter è ipnat)

- /etc/rc.conf
  - gateway_enable=“YES”
  - ipnat_enable=“YES”
  - ipnat_rules="/etc/ipnat.rules“
- ipnat.rules
  - map fxp0 192.168.100.0/24 -> 163.21.249.172/32
  - map fxp0 192.168.100.0/24 -> 163.21.249.172/32 proxy port ftp ftp/tcp
  - map fxp0 192.168.100.0/24 -> 163.21.249.172/32 portmap tcp/udp 40000:60000

PPTP VPN

- Compatible with the Microsoft Windows VPN adapter.
- KERNCONF
  - pseudo-device tun
- /usr/ports/net/poptop
- /etc/ppp/ppp.conf
  - set ifaddr 192.168.100.254 192.168.100.1-192.168.100.9 255.255.255.255
  - enable MSCHAPv2
  - set device !/etc/ppp/ppplogin

PPTP VPN (cont.)

- /etc/ppp/ppplogin
  - #!/bin/sh
  - exec /usr/sbin/ppp -direct loop-in
- /etc/ppp/ppp.secret
  - <account> <password> [ip address]
- pptp related proto/port
  - Proto GRE
  - Port 1723/tcp

Ports

- /usr/ports
  - make search [key|name] = OOXXABCD
  - make
    - fetch | extract | configure | all | packages | install | clear | distclean
- pkg_add, pkg_delete, pkg_info, …
- portupgrade
- All installed information stored in /var/db/pkg.

Apache

- www/apache13, www/apache2
- www/mod_*
- lang/php4

- .ht*
- Rewrite module

Postfix

- http://www.postfix.org/
- Useful features
  - header_checks
  - smtpd_XXXX_restrictions (client, sender, recipient)
  - Transport (like mailertable in Sendmail)
  - MySQL, LDAP lookup
  - Content filter
- SMTP reply codes (RFC 821)
  - 45x, Mail system, temporarily unavailable
  - 55x, Mail system, permanent unavailable

Postfix (cont.)

- Port Path: mail/postfix/
- Must filled values
  - myhostname
  - mynetworks
  - alias_maps
  - mydestination
  - relay-domains
  - smtpd_recipient_limit

Postfix (cont.)

- Most used commands
  - postfix [start|stop|reload]
  - postqueue -f/-p/-s
  - postmap <filename>
  - postsuper -d/-h/-H
  - postconf
  - postcat
- Sample settings
  - sample-XXXX.cf

AMaViS

- http://www.amavis.org/
- Interface between MTA and virus scanner
- Port Path: security/amavis*/
- amavisd-new
  - performance-enhanced daemonized version of amavis-perl
  - perl 5.6 or above
  - also supports SpamAssassin integration

AMaViS (cont.)

- /usr/local/etc/amavisd.conf
  - $MYHOME = '/var/amavis'
  - $mydomain
  - $daemon_user
  - $daemon_group
  - $final_(virus|spam)_destiny
  - $virus_admin
  - $sa_tag_level_deflt
  - $sa_tag2_level_deflt
  - $sa_spam_subject_tag

AMaViS (cont.)

- Postfix settings
  - master.conf
    - smtp-amavis unix - - n - 10 smtp
      -o disable_dns_lookups=yes
      -o smtp_data_done_timeout=120s
    - localhost::10025 inet n - n - - smtpd
      -o content_filter=
  - main.conf
    - content_filter=smtp-amavis:[127.0.0.1]:10024

SpamAssassin

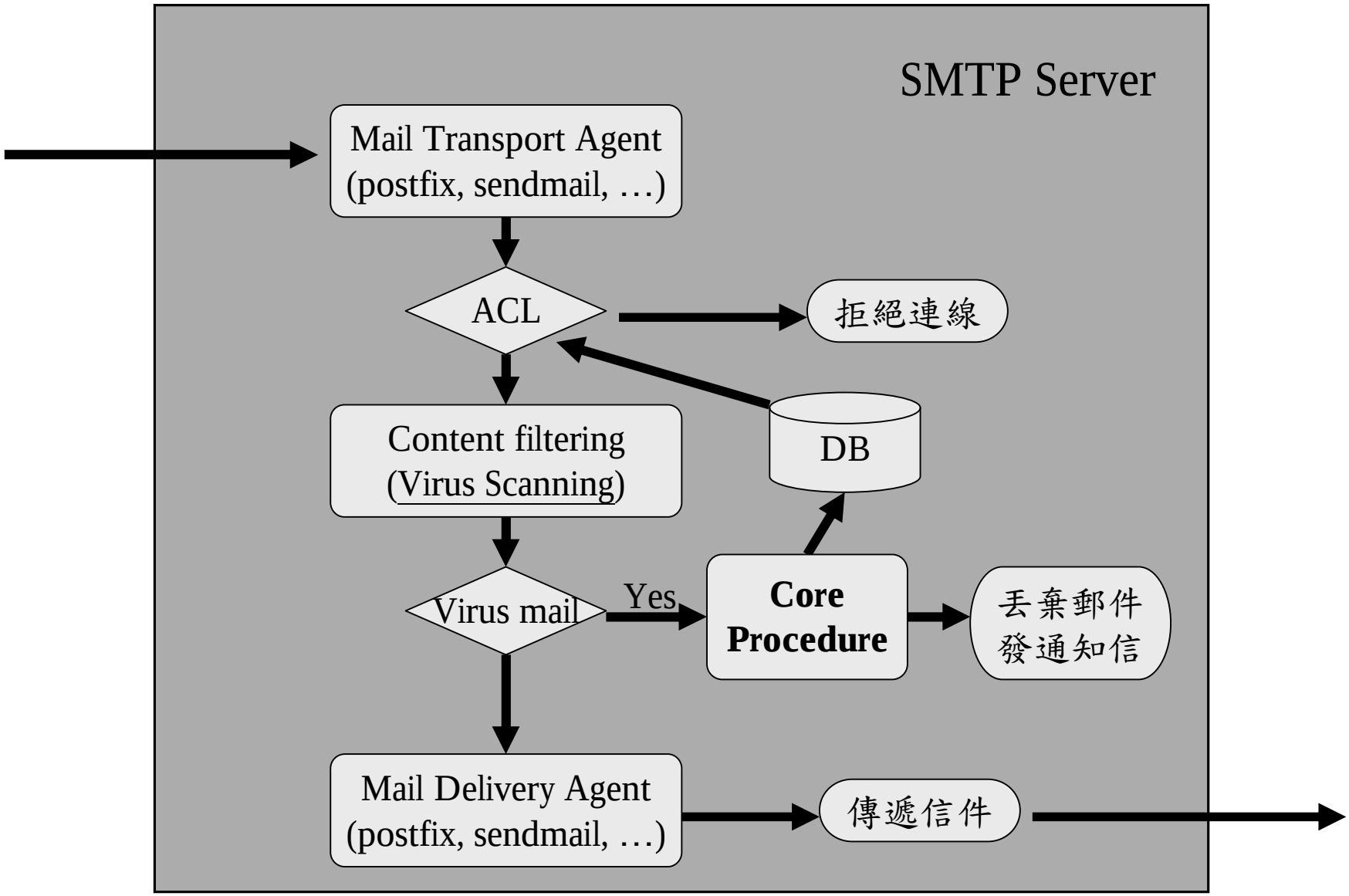
- http://www.spamassassin.org/
- spam-identification tactics used include
  - **header analysis**
  - **text analysis**
  - **blacklists**
  - **Razor**
- /var/amavis/.spamassassin
  - user_prefs
    - header YAHOO_EML Message-ID =~ /qmail\@web[\d]{5}.mail.tpe.yahoo.com/
    - describe YAHOO_EML God Damn Yahoo! eml forwards
    - score YAHOO_EML -5

SpamAssassin (cont.)

- http://www.spamassassin.org/tests.html
- Train SpamAssassin's Bayesian classifier
- /usr/local/bin/sa-learn
  - ham
  - spam
  - forget
  - rebuild

  - file
  - dir

Work flow for smtp.tp.edu.tw



Secure your FreeBSD

- No remote login for superuser
- /usr/ports/security/sudo
- Default to deny in ipfw/ipfilter
- /etc/rc.conf: accounting_enable="YES"
- Check FreeBSD Security Advisories frequently
- Check System Messages frequently
- How To: **Installing a secure BSD System**
  - http://www.littlewhitedog.com/reviews_other_00029.asp