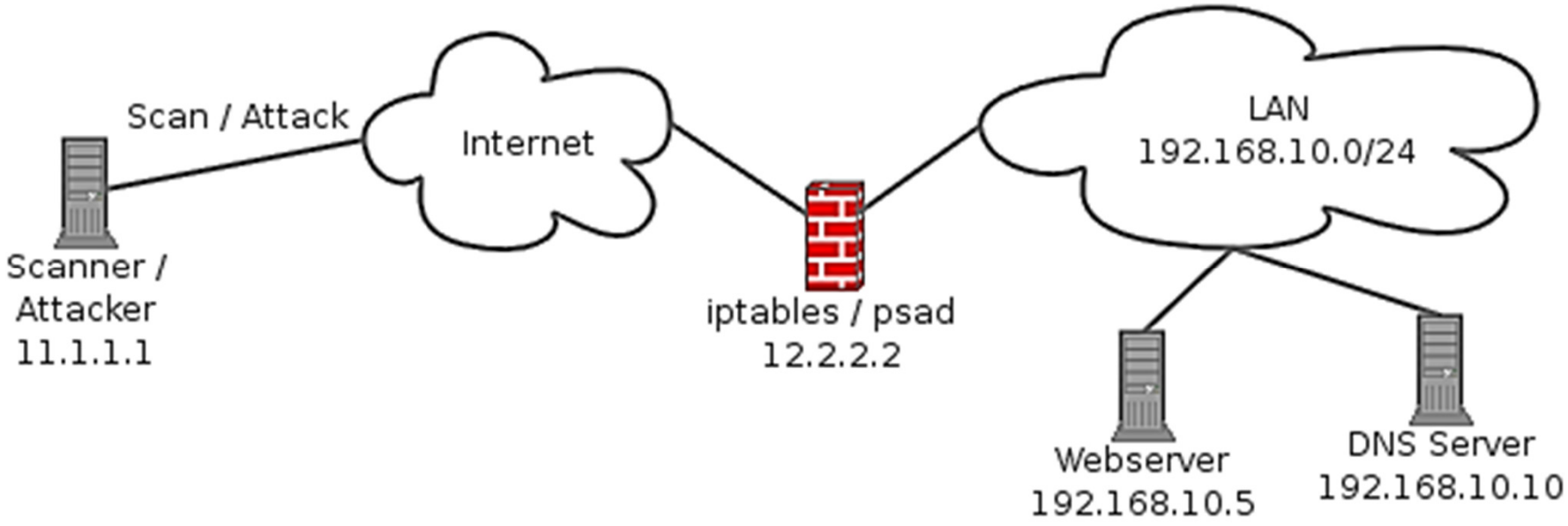
AN TOÀN HỆ THỐNG VỚI PSAD VÀ PFSENSE

PSAD: Giới thiệu

- Port Scan Attack Detector
- Jay Beale, Peter Watkins và Michael Rash phát triển một sản phẩm IDS mới có tích hợp tính năng firewall gọi là Bastille-NIDS.
- 2001 Michael Rash tách thành dự án riêng tạo ra sản phẩm IDS không phụ thuộc Bastille gọi là PSAD


Scan / Attack
Internet
LAN
192.168.10.0/24
Scanner /
Attacker
11.1.1.1
iptables / psad
12.2.2.2
Webserver
192.168.10.5
DNS Server
192.168.10.10

Tính năng của PSAD

- Phát hiện các dạng lưu lượng nghi ngờ
- Thăm dò các backdoor, các DDoS tool và các hành vi lạm dụng networking protocol
- Kết hợp với fwsnort có thể phát hiện hơn 60% tất cả Snort rules, bao gồm các yêu cầu phân tích sâu vào dữ liệu giao thức lớp ứng dụng.
- Có khả năng lấy dấu các hệ điều hành của các hệ thống phát sinh hành vi dò quét và nguồn gốc của lưu lượng độc hại.

Cài đặt PSAD

- Tải từ http://www.cipherdyne.org/psad/download
- Kiểm tra cả MD5 và GnuPG signature, có thể tìm GnuPG Public key tại http://www.cipherdyne.org/public_key. Ví dụ phiên bản pasd-2.0.8

```
$ cd /usr/local/src
$ wget http://www.cipherdyne.org/psad/download/psad-2.0.8.tar.bz2
$ wget http://www.cipherdyne.org/psad/download/psad-2.0.8.tar.bz2.md5
$ wget http://www.cipherdyne.org/psad/download/psad-2.0.8.tar.bz2.asc
$ md5sum -c psad-2.0.8.tar.bz2.md5
psad-2.0.8.tar.bz2: OK
$ gpg --verify psad-2.0.8.tar.bz2.asc
gpg: Signature made Sun Jul 29 13:18:58 2007 EDT using DSA key ID A742839F
$ tar xfj psad-2.0.8.tar.bz2
$ su –
Password:
# cd /usr/local/src/psad-2.0.8
# ./install.pl
```

Starting và Stopping psad

```
# /etc/init.d/psad start
 * Starting psad ...                    [ ok ]
# /etc/init.d/psad stop
 * Stopping psadwatchd ...              [ ok ]
 * Stopping kmsgsd ...                  [ ok ]
 * Stopping psad ..
```

...

- Khi khởi động psad, 3 daemon được khởi động: main psad daemon, kmsgsd, and psadwatchd
- Mục đích của kmsgsd là đọc tất cả iptables log messages từ /var/lib/psad/psadfifo và ghi vào /var/log/psad/fwdata, cho mục đích phân tích thời gian thực.
- psadwatchd daemon làm nhiệm vụ đảm bảo hai daemon kia phải chạy, nếu không sẽ khởi động lại.

Cấu hình iptables policy

- Về bản chất psad là bộ phân tích log. Cần đảm bảo iptable policy được cấu hình để thực hiện theo qui tắc “log and drop”.
- Psad có cơ chế tự động để kiểm tra chính sách iptable cục bộ có được cấu hình theo nguyên tắc log and drop. Cơ chế được thực hiện bởi script /usr/sbin/fwcheck_psad

Cấu hình Syslog

- Khi một gói trùng với LOG rule trong iptables, kernel thông báo sự kiện qua klogd. Sau đó kernel log message được chuyển đến syslog để đưa vào report file .
- Syslogd và syslog-ng daemons đều tương thích với psad. Cả hai đều có thể ghi bản tin log vào các named pipe. Psad lợi dụng điều này để ghi tất cả bản tin kern.info log vào /var/lib/psad/psadfifo

- Nếu psad đang chạy trên hệ thống có cài đặt syslogd, cần bổ sung vào /etc/syslog.conf

kern.info /var/lib/psad/psadfifo

→cấu hình syslogd để ghi kern.info messages vào /var/lib/psad/psadfifo

- Nếu dùng syslog-ng làm local system, bổ sung các dòng sau vào /etc/syslog-ng/syslog-ng.conf :

```
source psadsrc { unix-stream("/dev/log"); internal(); pipe("/proc/kmsg"); };
filter f_psad { facility(kern) and match("IN=") and match("OUT="); };
destination psadpipe { pipe("/var/lib/psad/psadfifo"); };
log { source(psadsrc); filter(f_psad); destination(psadpipe); };
```

Cấu hình PSAD

- Tất cả các psad daemons đều tham chiếu tập tin cấu hình /etc/psad/psad.conf
- Chứa hơn 100 biến cấu hình để điều khiển các khía cạnh hoạt động khác nhau của psad.
- Ví dụ :

```
### System hostname

HOSTNAME                    psad.cipherdyne.org;
```

Biến EMAIL_ADDRESSES

- Biến EMAIL_ADDRESSES chỉ định các địa chỉ email để psad gửi cảnh báo và các thông tin cần thiết khác.

EMAIL_ADDRESSES root@localhost, you@domain.com;

Biến DANGER_LEVEL{n}

- Mức nguy hiểm được gán dựa trên ba yếu tố:
  - Các đặc tính của scan (số gói, dải port và time interval)
  - Gói có liên hệ với signature được định nghĩa trong /etc/psad/signatures
  - Gói có bắt nguồn từ một IP hay mạng được liệt kê trong /etc/psad/auto_dl
- Biến DANGER_LEVEL{n} chỉ định số lượng gói thống kê để đạt mức nguy hiểm tiếp theo.

Biến HOME_NET

- HOME_NET định nghĩa local network nơi hệ thống chạy psad được triển khai.
- Có thể định nghĩa một danh sách các mạng

HOME_NET 71.157.X.X/24, 192.168.10.0/24;

Biến EXTERNAL_NET

- Biến EXTERNAL_NET xác định tập các mạng ngoài. Mặc nhiên là bất kỳ (any).
- Có thể liệt kê tùy ý các mạng tương tự như Home_net
- Trong hầu hết các cài đặt thường dùng any

```
EXTERNAL_NET                any;
```

Biến SYSLOG_DAEMON

- Biến SYSLOG_DAEMON báo cho psad biết loại syslog daemon nào đang chạy trên local system
- Các giá trị có thể cho biến này là: syslogd, syslog-ng, ulogd và metalog

Biến CHECK_INTERVAL

- Phần lớn thời gian psad ở trạng thái “ngủ”, nó chỉ “ thức” để xác định xem có iptables log message nào mới xuất hiện trong /var/log/psad/fwdata hay không.
- Thời gian giữa các lần “thức dậy” để kiểm tra được xác định theo giây bởi check_interval, mặc định là 5 giây.

Biến SCAN_TIMEOUT

- Psad dùng giá trị được chỉ định bởi biến này như khoảng thời gian tối đa để theo dõi một hành động dò quét. Mặc định là 1 giờ (3600 giây)
- Nếu một lưu lượng độc hại từ một IP đặc biệt không đạt đến mức nguy hiểm trong khoảng thời gian timeout này, psad sẽ không phát ra lời cảnh báo.

Biến ENABLE_PERSISTENCE

- Phần mềm phát hiện quét port thường phải cài đặt hai giá trị ngưỡng để xác định một port scan: số port bị thăm dò và khoảng thời gian thăm dò.
- Một attacker có thể cố hoạt động dưới ngưỡng bằng cách giảm số port hay quét chậm. Biến anable_persistence chỉ thị cho psad không dùng scan_timeout làm yếu tố phát hiện.

Biến PORT_RANGE_SCAN_THRESHOLD

- Biến này cho phép định nghĩa dải port tối thiểu phải bị quét trước khi psad gán một mức nguy hiểm cho hành động quét port.
- Mặc định biến này được cài là 1, nghĩa là tối thiểu có hai port bị quét trước khi mức nguy hiểm 1 được xác lập

Biến EMAIL_ALERT_DANGER_LEVEL

- Biến này cho phép cài đặt mức nguy hiểm thấp mà psad không gửi email cảnh báo trừ khi có địa chỉ IP được gán mức nguy hiểm từ giá trị này trở lên.
- Mặc định là 1

Biến MIN_DANGER_LEVEL

- MIN_DANGER_LEVEL threshold tác động như một global threshold để tất cả chức năng cảnh báo và theo dõi được thực thi bởi psad
- Ví dụ, nếu biến ngưỡng này được gán là 2 thì psad sẽ không ghi một địa chỉ IP vào /var/log/psad/ip cho đến khi đạt mức nguy hiểm 2

Biến SHOW_ALL_SIGNATURES

- Biến này chỉ thị cho psad gửi hay không tất cả thông tin về dấu hiệu liên quan với một địa chỉ IP trong mỗi cảnh báo.
- Mặc định là không, tuy nhiên psad sẽ gửi tất cả dấu hiệu mới

Biến ALERT_ALL

- Khi biến này được gán là Y, chỉ thị cho psad phát sinh email và syslog bất cứ khi nào có một hành động nguy hiểm mới được phát hiện từ một địa chỉ IP với mức nguy hiểm là 1

Biến SNORT_SID_STR

- Biến này định ra chuỗi con để đối sánh với các iptable log message nhằm xác định có message nào được phát sinh bởi một iptable rule mang đầy đủ đặc trưng của một Snort rule hay không.
- Các iptables rule như vậy thường được xác lập bởi fwsnort

Biến ENABLE_AUTO_IDS

- Nếu biến này được gán là Y sẽ chuyển psad từ daemon giám sát thụ động sang đáp ứng tấn công một cách chủ động bằng cách tái cấu hình động chính sách iptable để khóa một IP xâm phạm không cho tương tác với hệ thống
- Khóa với local system qua INPUT và OUTPUT chain
- Bảo vệ tất cả các system dựa vào FORWARD chain trên local system

Biến IMPORT_OLD_SCANS

- Thông tin về quét port và các hành vi nghi ngờ được psad thu thập và ghi vào /var/log/psad. Khi IP address đến mức nguy hiểm 1, một thư mục mới /var/log/psad/ip được tạo ra.
- Lúc khởi động psad thường xóa các thư mục /var/log/psad/ip nhưng có thể import tất cả data từ các thư mục cũ bằng cách đặt biến này thành Y.

Biến IGNORE_PORTS

- Một đặc tính quan trọng là có thể bỏ qua các data nào đó do admin chỉ định.
- Biến này chỉ cho psad bỏ qua các iptable log message dựa vào chỉ số port đích và giao thức liên quan (TCP hay UDP).
- Có thể kết hợp dải port, nhiều port và giao thức, ví dụ:

```
IGNORE_PORTS        udp/53, udp/5000, tcp/51000-61356;
```

Biến IGNORE_PROTOCOLS

- Với biến IGNORE_PROTOCOLS psad có thể được chỉ thị bỏ qua toàn bộ các giao thức.
- Ví dụ muốn psad bỏ qua tất cả các gói ICMP:

```
IGNORE_PROTOCOLS                    icmp;
```

Biến EMAIL_LIMIT

- Trong một số trường hợp một iptable policy được cấu hình để log lưu lượng không độc hại. Nếu để psad thông dịch lưu lượng này như scan nó sẽ gửi hàng loạt email cảnh báo.
- Để kiểm soát số lượng email cảnh báo dùng biến EMAIL_LIMIT

Biến ALERTING_METHODS

- Hầu hết các admin đều dùng cả email và syslog reporting mode. Đôi khi chỉ cần dùng một reporting mode.
- Biến này cho phép chọn một trong hai.
- noemail và nosyslog là hai tham số tương ứng bảo psad không gửi email và không gửi syslog cảnh báo

Biến FW_MSG_SEARCH

- FW_MSG_SEARCH xác định cách thức psad tìm kiếm các iptables log message.
- Để giới hạn psad chỉ phân tích các message chứa một tiền tố log đặc biệt. Tiền tố được định nghĩa bởi biến FW_MSG_SEARCH.
- Điều này cho phép iptable được cấu hình để gán các log prefix vào các gói mà psad không phân tích chúng.
- Ví dụ chỉ muốn psad phân tích các iptable log message chứa DROP, cấu hình như sau:

```
FW_MSG_SEARCH                    DROP;
```

Tập tin /etc/psad/auto_dl

- Hệ thống phát hiện cần được trang bị năng lực liệt kê các hệ thống, mạng, port hay giao thức được miễn kiểm tra bởi cơ chế tự động. Đồng thời cũng cần liệt kê danh sách các địa chỉ IP nào đó là không lành mạnh (backlist).
- Các yêu cầu này được xác lập dựa vào auto_dl file.

```
 Syntax:
ip/network  danger level    optional protocol/optional ports
Ví dụ:
192.168.10.3     0;
10.10.1.0/24     5     tcp/22;
```

Tập tin /etc/psad/signatures

- Tập tin /etc/psad/signatures chứa một tập khoảng 200 Snort rule được hiệu chỉnh
- Các rule tương ứng là các tấn công mà psad có thể phát hiện một cách trực tiếp từ iptable log message.
- Không luật nào cần đến kiểm thử ở lớp ứng dụng dựa vào lưu lượng mạng_fwsnort chạy các test trên lớp ứng dụng

Tập tin /etc/psad/snort_rule_dl

- Tương tự như /etc/psad/auto_dl file, the snort_rule_dl file chỉ thị cho psad tự động gán mức nguy hiểm của bất kỳ địa chỉ IP nào mà so trùng với một Snort rule.
- Cú pháp của file này là:

```
sid             danger level
```

Tập tin /etc/psad/ip_options

- Phần tùy chọn trong IP header thường không được dùng nhiều trên mạng nhưng iptable có thể log tùy chọn này.
- Nếu iptable log message có chứa IP option, psad phân tích chúng để phát hiện các hành vi nghi ngờ, ví dụ source routing.

Tập tin /etc/psad/pf.os

- OS database từ dự án p0f được sử dụng bởi psad để in dấu các hệ điều hành ở xa.
- Database này được cài đặt bởi psad như là tập tin /etc/psad/pf.os và được import lúc khởi động psad.

Giới thiệu pfSense

- Open Source operating system tập trung chức năng router/firewall.
- pfSense là một open source statefull firewall có thể mở rộng và là một application package system
- Được thiết kế để quản lý dễ dàng qua giao diện web
- Based on FreeBSD.
- Được phát triển từ năm 2004 bởi Chris Buechler và Scott Ullrich.
- IPv4 and IPv6 compatible

Các đặc tính mong muốn đối với Firewall mới

- Khả năng mở rộng lên từ 100Mbps đến 2Gbps.
- Khả năng bridge thay vì NAT.
- Packet shaping & QoS để tránh tắc nghẽn đối với critical traffic
- Tin cậy
- Giá thành thấp

Một số Firewall thương mại

- Palo Alto
- Fortinet's Fortigate
- Dell's Sonicwall series
- Watchguard's XTM series

Open source pfSense firewall

Ưu điểm

- Chi phí
- Dùng phần cứng phổ dụng.
- Tính năng IDS/IPS tương đương sản phẩm thương mại.

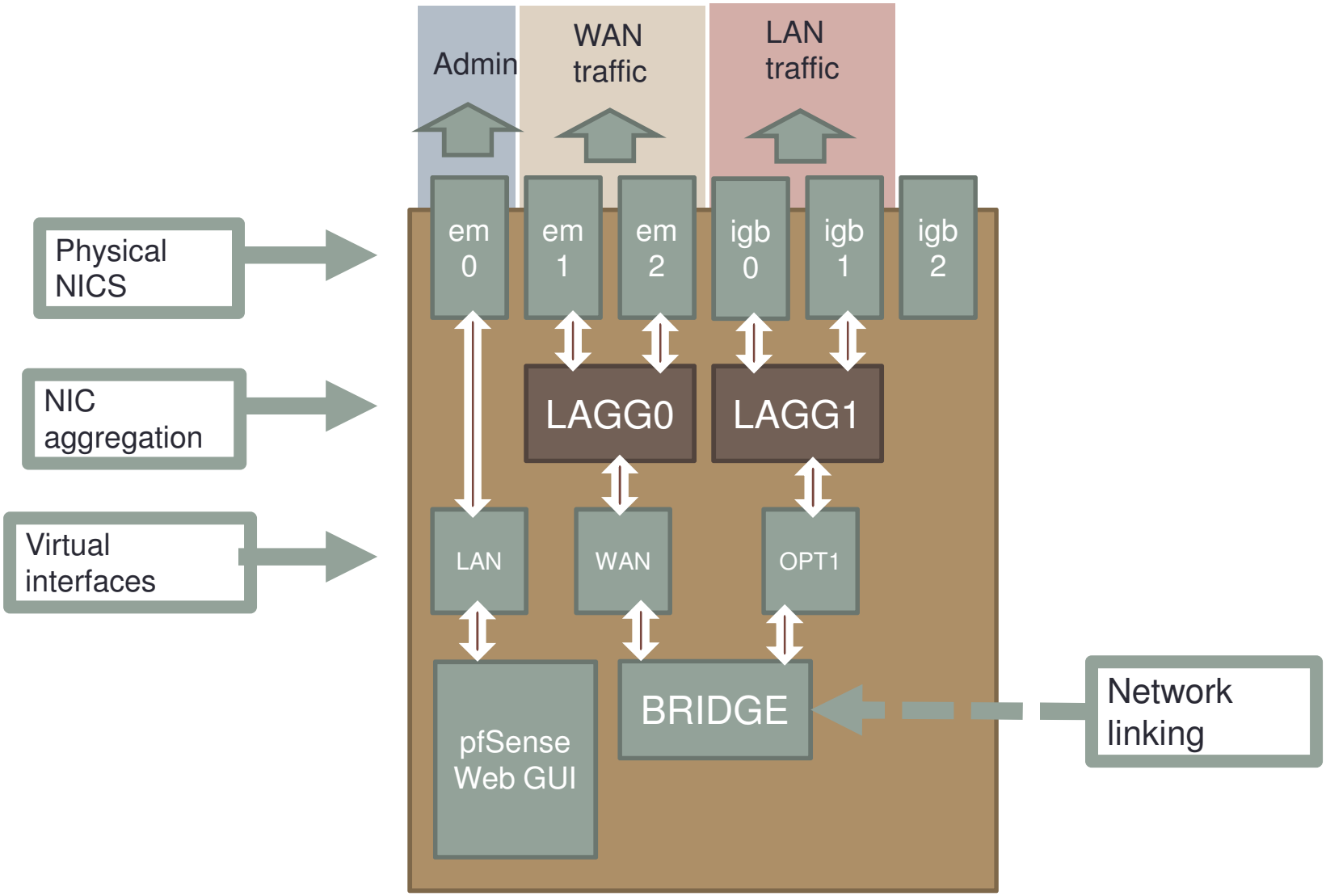
Nhược điểm:

- Cần nhiều thời gian và công sức để cài đặt và kiểm thử.
- Khó cài đặt giám sát và kiểm soát ứng dụng.
- Chưa sẵn sàng cho10Gbps.

Các yêu cầu của pfSense

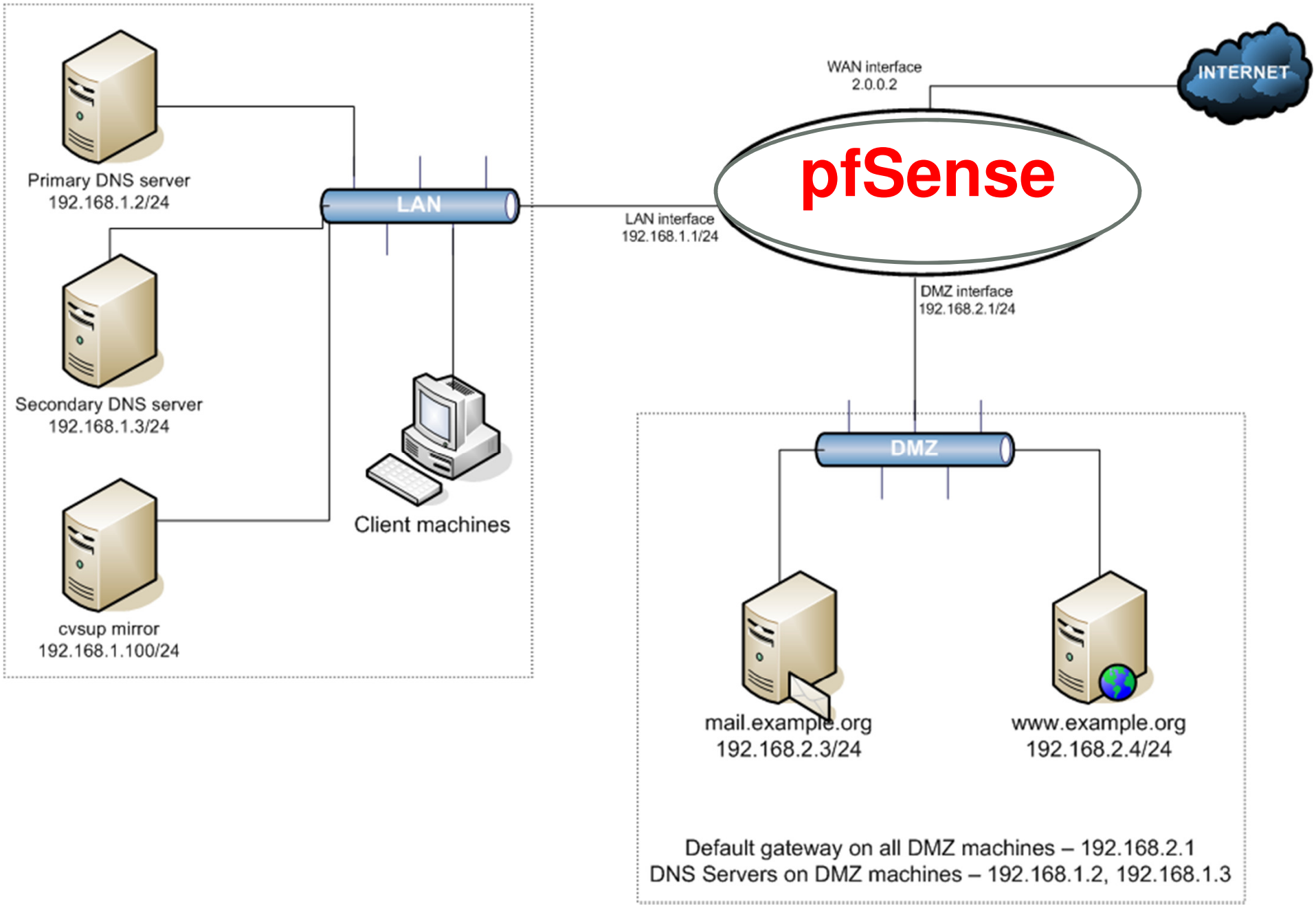
- pfSense tương thích với bất kỳ FreeBSD hardware trên i386 và amd64 platforms.
- pfSense không hỗ trợ PowerPC, MIPS, ARM, SPARC.
- Network Interfaces
  - Tất cả NICs được hỗ trợ bởi pfSense, nhưng không phải tất cả các driver đều tương thích.
  - Intel Pro/100, Pro/1000 NICs và Solid driver support in FreeBSD là tương thích tốt
- Wireless Adapters
  - Đa số được hỗ trợ, tuy nhiên các nhà phát triển thường dùng Atheros hardware.

Firewall networking view



Các ứng dụng của pfSense

- Perimeter Firewall
  - Là dạng phổ biến nhất của pfSense.
  - Hỗ trợ nhiều WAN, LAN, DMS.
  - BGP, connection redundancy, và load balancing
- LAN, WAN Router
- Wireless Access Point
- Special Purpose Appliances
  - VPN appliance
  - DNS Server
  - Sniffer Appliance
  - DHCP Server Appliance
- Supports VLANs


Primary DNS server
192.168.1.2/24
LAN
Secondary DNS server
192.168.1.3/24
Client machines
cvsup mirror
192.168.1.100/24
WAN interface
2.0.0.2
INTERNET
pfSense
LAN interface
192.168.1.1/24
DMZ interface
192.168.2.1/24
DMZ
mail.example.org
192.168.2.3/24
www.example.org
192.168.2.4/24
Default gateway on all DMZ machines – 192.168.2.1
DNS Servers on DMZ machines – 192.168.1.2, 192.168.1.3

Services

- Với cài đặt cơ bản pfSense cung cấp các dịch vụ cho cấu hình firewall và routing như sau:
  - IPv4/IPv6 DHCP Server
  - DHCP/DHCPv6 Relay
  - DNS Resolver
  - DNS Forwarder
  - Dynamic DNS
  - SNMP
  - UPnP & NAT-PMP
  - NTPD
  - Wake on LAN
  - PPPoE Server
  - IGMP Proxy

Các tính năng quan trọng

- Web Configurator
- User Management
  - RADIUS
  - LDAP
- Certificate Management/Certificate Authority
- VPN Server
- Traffic Shaper
- Load Balancing
- Captive Portal
- Package Manager

Web Configurator

- All in One configuration tool
- Trong khi vẫn có terminal console, tất cả đều có thể làm qua Web Configurator
- Được viết bằng PHP và dùng Twitter Bootstrap cho front end giúp bộ cấu hình có giao diện thân thiện
- Có thể đăng nhập qua HTTP hay HTTPS
- Configure setup, firewall rules, interfaces, services kèm với các công cụ chẩn đoán

User Management

- pfSense hỗ trợ quản lý truy xuất toàn bộ hay một phần các trang của Web Configurator
  - Allow access to All Pages, Dashboard, Password Manager, VPN,…
- Có thể dùng RADIUS hay LDAP cho xác thực các primary authentication server hay Local Database
- Nếu RADIUS hay LDAP bị trở ngại thì pfSense dùng Local Database

Certificate Manager/Certificate Authority

- pfSense cho phép tạo hay import một Cerfiticate Authority và thực hiện vai trò này.
- pfSense cũng có thể thực thi vai trò của một Intermediate CA
- Các chức năng cơ bản như creating, importing, removing và revoking các certificate

VPN Server

- OpenVPN – đề nghị của pfSense
  - Được cài trực tiếp vào Web Configurator
- PPTP VPN – hỗ trợ hạn chế
- L2TP with IPSec
  - Được cài trực tiếp vàoWeb Configurator
  - L2TP là giao thức thiết lập đường hầm thuần túy và không có mật mã, do đó được liên kết với kỹ thuật mật mã khác, ví dụ IPsec

Traffic Shaper

- Traffic Shaper có thể:
  - Giúp thao tác duyệt web mượt mà
  - Các cuộc gọi VoIP rõ ràng
  - Giảm “lag” trong video
  - Kiểm soát các P2P application
  - Áp đặt các giới hạn băng thông

Load Balancing

- Hai chức năng cân bằng tải (load balancing) có sẵn trong pfSense là Gateway và Server
- Gateway load balancing cho phép phân phối Internet-bound traffic qua nhiều kết nối WAN
- Server load balancing quản lý incoming traffic để chia sẻ tải giữa nhiều server nội bộ và dự phòng.
- Các gói hỗ trợ tính năng cân bằng tải đầy đủ hơn cho pfSense như HAProxy và Varnish.
- pfSense load balancer được xây dựng trên OpenBSDs relayd

Captive Portal

- Captive Portal cho phép chuyển user đến một trang web đặc biệt trước khi được phép truy cập Internet.
- Captive Portal Zones – Cho phép tách biệt các portal cho các giao tiếp khác nhau.
- Common Portal Scenarios
  - Portal Config không Authentication
  - Portal Config dùng Local Authentication hay Vouchers
  - Portal Config dùng Radius
- Chưa hỗ trợ IPv6

Package Manager

- Dựa trên FreeBSD package manager.
- Có thể cài đặt các package tiêu biểu như một server.
- Bất kỳ package nào được cài đặt đề đặt ra vấn đề an toàn vốn có của nó.

Các bước cài đặt pfSense

Tham khảo hướng dẫn cài đặt và cấu hình pfSense trong các tài liệu:

1.Christopher M. Buechler, Jim Pingle, pfSense: The Definitive Guide Version 2.1: The Definitive Guide to the pfSense Open Source Firewall and Router Distribution, Electric Sheep Fencing LLC, 2013

2.https://doc.pfsense.org/index.php/Installing_pfSense