

APRICOT2015 Security Workshop:

# Detecting Sick Hosts

Sheryl Hermoso, APNIC  
sheryl@apnic.net

# Sick Hosts

- Host or end-user computers that have been “infected” or compromised
  - Servers, PC/Laptop, Smart phones
- Host can be infected by:
  - Virus, Malware, Trojan, Backdoor
- Host now becomes:
  - a bot
  - a spam engine
  - a ‘stepping stone’ for hiding tracks

# Risks to/from hosts

- Keystroke Loggers, malware, etc
- Other infected hosts in network
- Misbehaved users/clients (PEBCAK)
- Social engineering



How can you detect infected hosts?

# Logs

- Syslog (centralized)
- logwatch, swatch
- Key is to ensure you are informed of what is *\*important\** as opposed to every possible event. (or you'll start to ignore the logs)

# Syslog Facility Level

Facility Number	Keyword	Facility Description
0	Kern	Kernel message
1	User	User-level message
2	Mail	Mail system
3	Daemon	System daemon
4	Auth	Security/authorization messages
5	Syslog	Messages by syslogd
16	Local0	Local user 0
23	Local7	Local user 7

# Logwatch Example

##### Logwatch 7.3.4 (02/17/07) #####

Processing Initiated: Sun Sep 30 04:12:38 2012

Date Range Processed: yesterday

( 2012-Sep-29 )

Period is day.

Detail Level of Output: 10

Type of Output: unformatted

Logfiles for Host: [irrashai.up.edu.ph](http://irrashai.up.edu.ph)

#####

----- Cron Begin -----

Commands Run:

User cacti:

/usr/bin/php /usr/share/cacti/poller.php > /dev/null 2>&1: 287 Time(s)

User root:

/etc/webmin/bandwidth/[rotate.pl](#): 24 Time(s)

/etc/webmin/cron/[tempdelete.pl](#): 1 Time(s)

/root/backupMySQL.sh #everyday at 6am: 1 Time(s)

/usr/local/bin/refresh-dhcpdconf: 1440 Time(s)

root /usr/sbin/logwatch: 1 Time(s)

run-parts /etc/cron.daily: 1 Time(s)

run-parts /etc/cron.hourly: 24 Time(s)

wget -O - -q -t 1 /var/www/html/drupal/cron.php: 24 Time(s)

\*\*Unmatched Entries\*\*

error: Job execution of per-minute job scheduled for 13:20 delayed into :

----- Cron End -----

----- SSHD Begin -----

Didn't receive an ident from these IPs:

[201.67.47.69](#): 1 Time(s)

[202.92.128.188](#): 1 Time(s)

Failed logins from:

41.212.83.191 ([41.212.83.191.wananchi.com](#)): 138 times

root/password: 138 times

195.14.0.238 ([195-14-0-238.nuxit.net](#)): 1 time

root/password: 1 time

[202.106.46.42](#): 34 times

root/password: 34 times

221.204.253.107 ([107.253.204.221.adsl-pool.sx.cn](#)): 1 time

root/password: 1 time

Illegal users from:

41.212.83.191 ([41.212.83.191.wananchi.com](#)): 1 time

\_\_\_\_\_/password: 1 time

Received disconnect:

11: Bye Bye

202.106.46.42 : 34 Time(s)

41.212.83.191 : 139 Time(s)

\*\*Unmatched Entries\*\*

reverse mapping checking getaddrinfo for [41.212.83.191.wananchi.com](#) [41.212.83.191] failed - POSSIBLE BREAK-IN ATTEMPT! : 139 time(s)

Address 221.204.253.107 maps to [107.253.204.221.adsl-pool.sx.cn](#), but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT! : 1 time(s)

----- SSHD End -----

# Trends and alerts

- Bandwidth usage: CACTI
- Network events: NAGIOS
- Packet analyzers/dumpers for tracking down individual events.
- All the above depend on sanely designed network infrastructure.

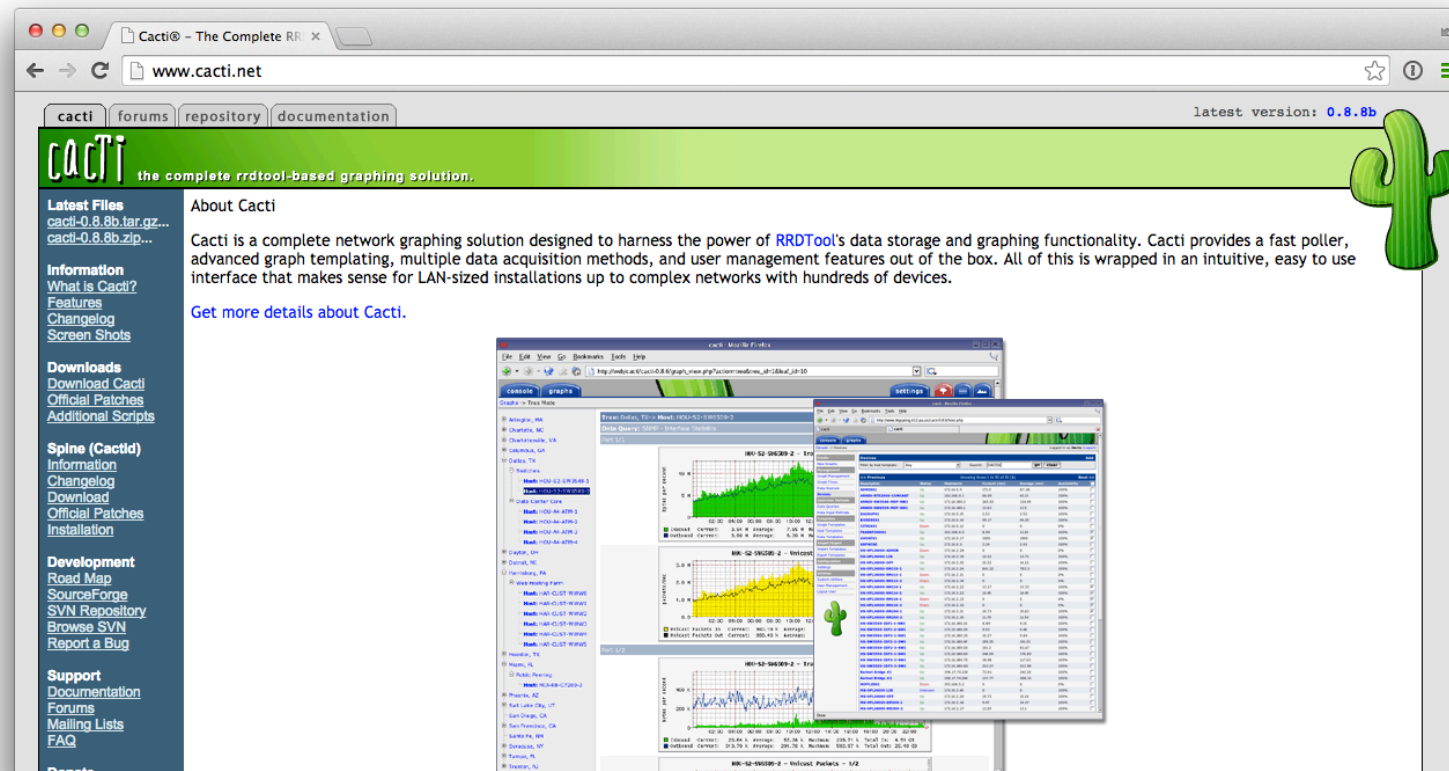


# Monitoring Tools

- Zabbix
- Observium
  - Provides auto-discovery of devices
  - Uses RRDTools for graphing
- Icinga
  - Modular design
- Cacti
  - Collects data via snmp

# Cacti

- Network monitoring and graphing tool



<http://www.cacti.net/>

# Nagios

- IT infrastructure monitoring
- Used for alerting and reporting
- Monitors
  - Applications
  - Operating systems
  - Network protocols
  - System metrics
    - CPU, memory, load

Nagios									
General									
Monitoring									
Service Detail									
Host Detail									
Status Overview									
Status Summary									
Status Map									
3-D Status Map									
Service Problems									
Host Problems									
Network Outages									
Comments									
Downtime									
Process Info									
Performance Info									
Scheduling Queue									
Reporting									
Trends									
Availability									
Alert Histogram									
Alert History									
Alert Summary									
Notifications									
Event Log									
Configuration									
View Config									

Host	Service	Status	Last Check	Next Check	Current Value	Unit	Output
webprod03	Check Users	OK	01-26-2007 14:58:59	0d 4h 53m 23s	1/4		USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:59:54	0d 4h 53m 23s	1/4		OK - load average: 0.21, 0.06, 0.05
	Memory Usage	OK	01-26-2007 14:55:29	0d 4h 53m 23s	1/4		OK - Memory Usage 56% - Total: 511 MB, Used: 287 MB, Free: 224 MB
	PING	OK	01-26-2007 14:56:14	0d 4h 50m 23s	1/4		PING OK - Packet loss = 0%, RTA = 0.16 ms
	Root Partition	OK	01-26-2007 14:57:09	0d 4h 50m 33s	1/4		DISK OK [243816 kB (5%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:57:44	0d 4h 50m 33s	1/4		Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:58:29	0d 4h 50m 33s	1/4		OK - 95 processes running
webprod04	Xen Virtual Machine Monitor	CRITICAL	01-26-2007 14:59:04	0d 0h 44m 34s	4/4		Critical Xen VMs Usage - Total NB: 0 - detected VMs:
	Check Users	OK	01-26-2007 14:59:54	0d 0h 15m 33s	1/4		USERS OK - 2 users currently logged in
	Current Load	OK	01-26-2007 14:55:34	0d 0h 14m 53s	1/4		OK - load average: 0.30, 0.60, 0.44
	Memory Usage	OK	01-26-2007 14:56:19	0d 0h 14m 13s	1/4		OK - Memory Usage 37% - Total: 511 MB, Used: 190 MB, Free: 321 MB
	PING	OK	01-26-2007 14:57:10	0d 0h 13m 23s	1/4		PING OK - Packet loss = 0%, RTA = 0.27 ms
	Root Partition	OK	01-26-2007 14:57:49	0d 0h 12m 43s	1/4		DISK OK [3948940 kB (94%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:58:34	0d 0h 11m 53s	1/4		Swap ok - (null) 0% (0 out of 16386)
webprod05	Total Processes	OK	01-26-2007 14:59:09	0d 0h 16m 22s	1/4		OK - 250 processes running
	Xen Virtual Machine Monitor	WARNING	01-26-2007 14:58:54	0d 0h 1m 33s	4/4		Warning Xen VMs Usage - Total NB: 1 - detected VMs: migrating-xen-vm4
	PING	OK	01-26-2007 14:55:39	0d 0h 24m 58s	1/4		PING OK - Packet loss = 0%, RTA = 0.25 ms
	Xen Virtual Machine Monitor	OK	01-26-2007 14:59:54	0d 0h 0m 33s	1/4		OK - Xen Hypervisor 'webprod05' is running 4 Xen VMs: xen-vm1 xen-vm2 xen-vm3 xen-vm4
xen-vm1	Check Users	OK	01-26-2007 14:58:09	0d 0h 17m 23s	1/4		USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:57:54	0d 3h 16m 21s	1/4		OK - load average: 1.54, 1.09, 0.48
	Memory Usage	OK	01-26-2007 14:58:39	0d 3h 15m 41s	1/4		OK - Memory Usage 8% - Total: 8195 MB, Used: 676 MB, Free: 7519 MB
	PING	OK	01-26-2007 14:59:15	0d 3h 15m 21s	1/4		PING OK - Packet loss = 0%, RTA = 0.49 ms
	Root Partition	OK	01-26-2007 14:59:59	0d 3h 14m 51s	1/4		DISK OK [4196280 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:44	0d 3h 14m 1s	1/4		Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:57:29	0d 0h 18m 3s	1/4		OK - 88 processes running
xen-vm2	Check Users	OK	01-26-2007 14:57:15	0d 3h 7m 41s	1/4		USERS OK - 0 users currently logged in
	Current Load	OK	01-26-2007 14:57:59	0d 3h 7m 1s	1/4		OK - load average: 0.00, 0.00, 0.00
	Memory Usage	OK	01-26-2007 14:58:44	0d 3h 6m 21s	1/4		OK - Memory Usage 6% - Total: 1023 MB, Used: 64 MB, Free: 959 MB
	PING	OK	01-26-2007 14:59:19	0d 0h 48m 14s	1/4		PING OK - Packet loss = 0%, RTA = 0.43 ms
	Root Partition	OK	01-26-2007 15:00:05	0d 1h 15m 4s	1/4		DISK OK [524220 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:49	0d 3h 9m 41s	1/4		Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:56:34	0d 3h 9m 1s	1/4		OK - 52 processes running

# BAYU

- Be aware you are uploading:
- [http://filesharing.uoregon.edu/bayu\\_notification.html](http://filesharing.uoregon.edu/bayu_notification.html)
- On a single enterprise/campus network you may have the ability (think permission) to move users into a “disciplinary pen” if their machine misbehaves.
- ISPs should not do as much policing, but some is possible

# Policies

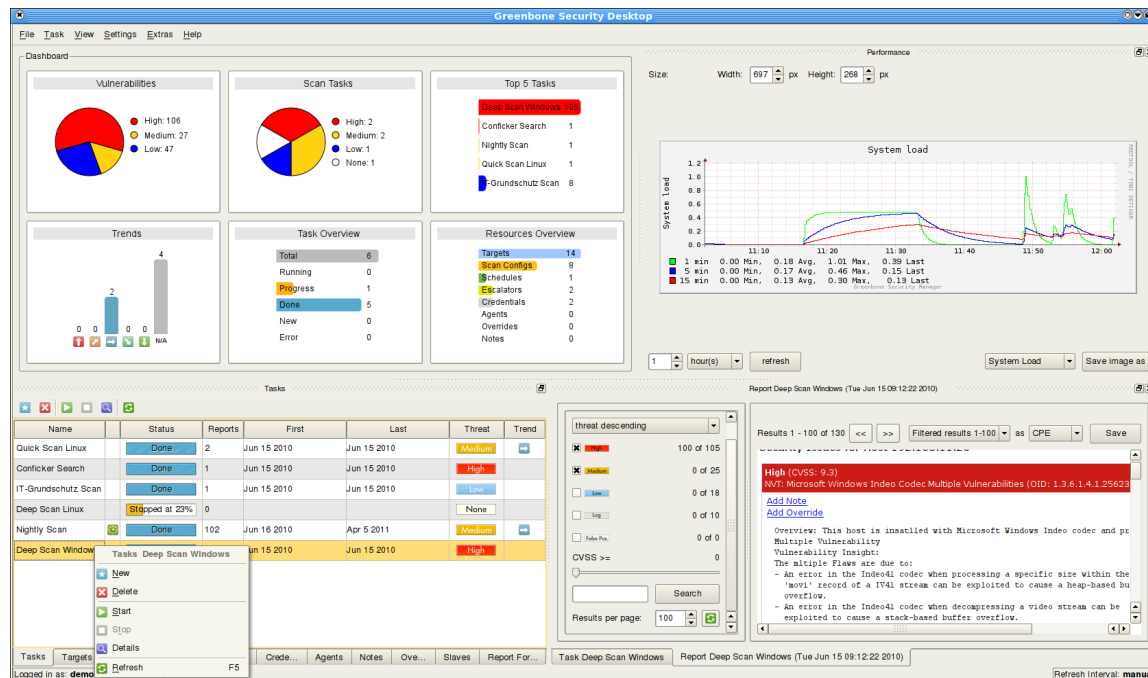
- Submit to a “scan” on connection
- Scan your own machines regularly
- Run an IDS
- What do you do with the results of that data?  
How do you scan?

# Nessus

- Comprehensive vulnerability scanner
- Free of charge for personal use
- Can scan for
  - Vulnerabilities that allow remote access
  - Misconfiguration
  - Default and common passwords (dictionary attack)
- Finds open ports, tries various exploits

# OpenVAS

- Open-source vulnerability scanner and manager
- Started as a fork to Nessus

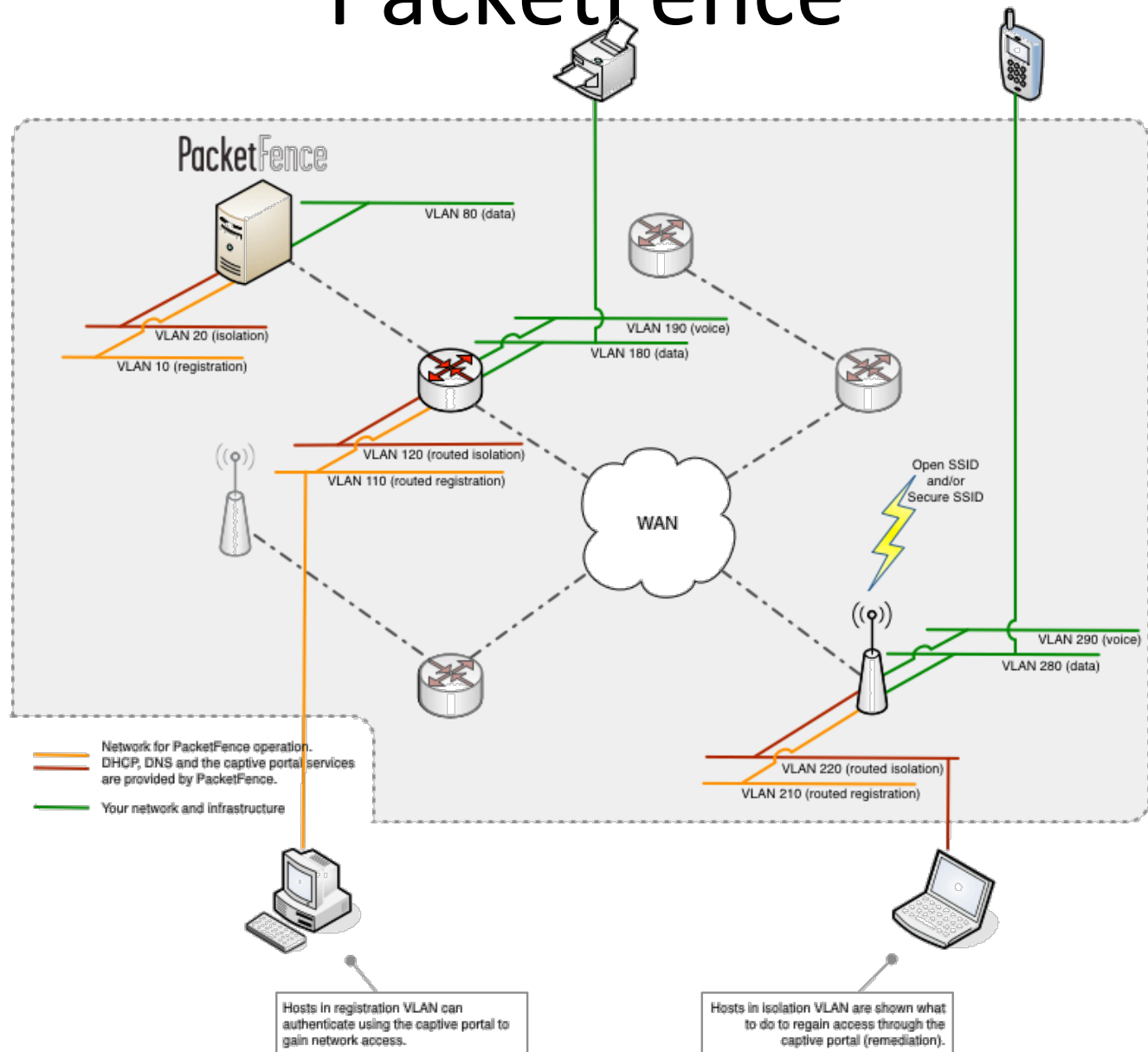


# PacketFence

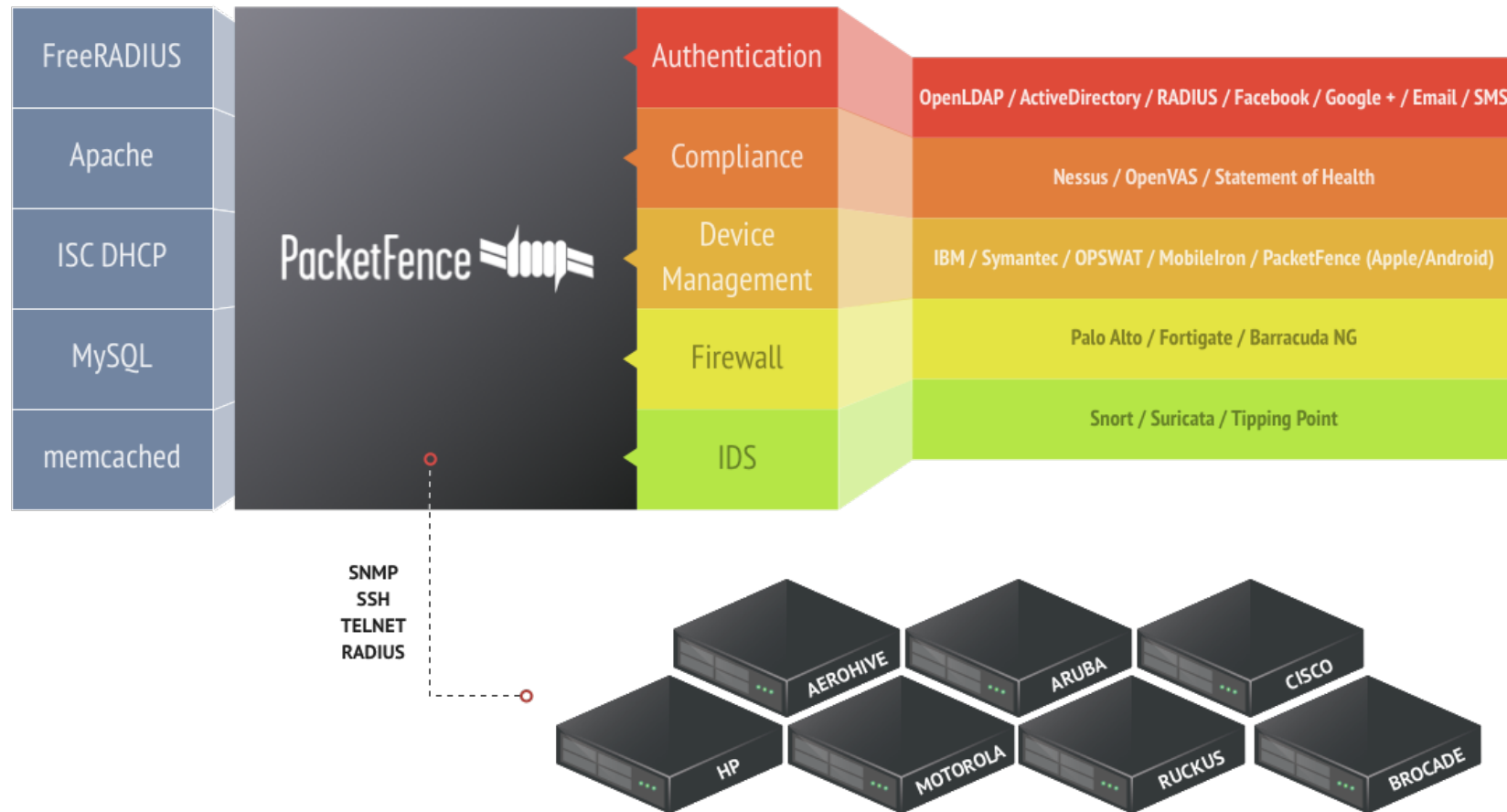
- Used for Network access control (NAC)
- Features:
  - Captive portal for registration and remediation
  - Centralized management
  - Detection of abnormal network activity with Snort
  - Vulnerability scans with Nessus
  - Isolation of problematic devices
- Zero-Effort NAC (ZEN) edition can be used to rapidly deploy PacketFence in your network



# PacketFence



# Packetfence



# Principles

- Do not scan inline – you end up adding a point of failure as well as a bottleneck. You do need a “mirror” or “monitor” port
- Need supported hardware with SNMP (Ubiquity support still in progress)
- In ISPs you can trigger custom Perl scripts based on particular “events” from network scanners.

# Principles

- In enterprises you can drop the users access port in a VLAN with restricted filters.
- For scalability you could have more boxes in different parts of the network.
- FreeNAC is an alternative piece of software (also opensource)

# Snort

- An open source network intrusion detection system
- A rule-based language combining signature, anomaly, and protocol inspection
- Must be placed close to the “choke point”
  - Where all traffic flows in/out of the network
  - Close to the border router or firewall
- Use a span/port mirror port to send traffic from

<http://www.snort.org/>



21

# Data gathering

- IDS systems
- Active scanners
- Netflow

# Questions

