



Sniff-Log 2.0

User Guide

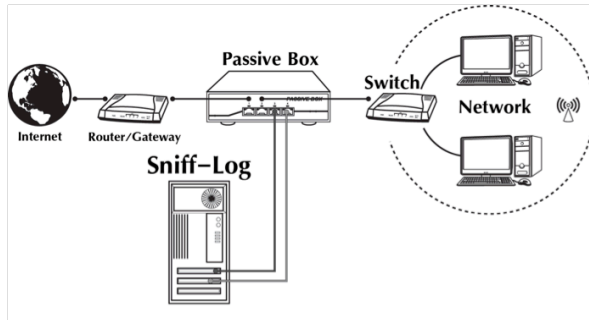
Solution การเก็บ Log file โดย Sniff-Log	1-2
Hardware Required สำหรับ Sniff-Log	3
การติดตั้งโปรแกรม Sniff-log	4-6
การตั้งค่า Sniff-Log กับระบบเครือข่าย	7-8
การ Activate โปรแกรม Sniff-Log	9
การใช้งาน Passive Mode	10-11
การใช้งาน Centralize Mode	12-13

รูปแบบการจัดเก็บ Log file ให้ตรงตาม พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 นั้นขึ้นอยู่กับหน่วยงานหรือองค์กรนั้น เป็นผู้ให้บริการประเภทอะไรบ้าง ซึ่งเมื่อนำมาสู่แนวทางปฏิบัติจริงสามารถแบ่งได้ดังนี้

1. หน่วยงานเป็นผู้บริการเฉพาะอินเทอร์เน็ต

Solution A

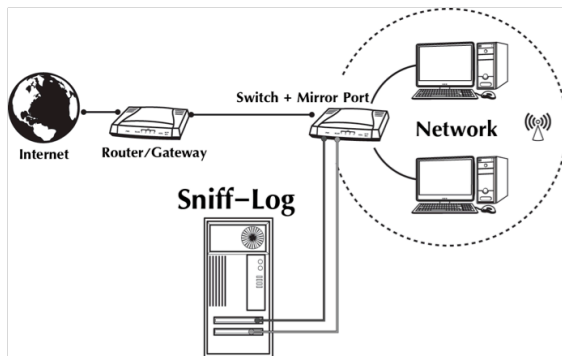
หน่วยงานที่มีอินเทอร์เน็ตให้บริการโดยใช้ Router เป็น Gateway



การจัดเก็บ Log กระทำได้โดยใช้โปรแกรม Sniff-Log และใช้อุปกรณ์ Passive Box ช่วยในการจัดเก็บ Log file แบบ Passive Mode

Solution B

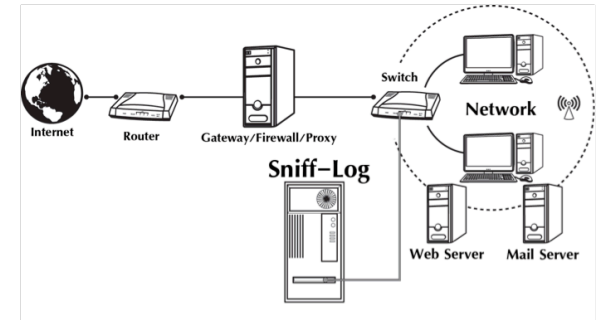
หน่วยงานที่มีอินเทอร์เน็ตให้บริการโดยใช้ Router เป็น Gateway



การจัดเก็บ Log กระทำได้โดยใช้โปรแกรม Sniff-Log และใช้อุปกรณ์ Switch ที่มีคุณสมบัติสามารถทำ Mirror Ports ช่วยในการจัดเก็บ Log file แบบ Passive Mode

Solution C

หน่วยงานที่มีอินเทอร์เน็ตให้บริการโดยมี Gateway เป็น Proxy / Firewall / IIS หรืออื่นๆ เป็นต้น



การจัดเก็บ Log กระทำได้โดยใช้โปรแกรม Sniff-Log แบบ Centralize Mode โดยให้ Gateway ส่งข้อมูล Log file * มาจัดเก็บที่ Sniff-Log

Note

โปรแกรม Sniff-Log 2.0 สามารถจัดเก็บ Log file ตาม พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ได้ 2 รูปแบบ คือ

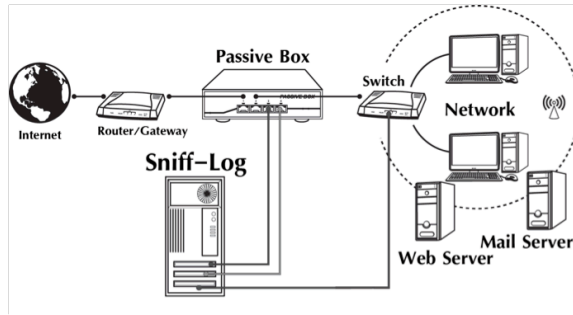
1. แบบ **Passive Mode** โดยจัดเก็บ Internet Logfile ระหว่าง Gateway และผู้ใช้งาน สำหรับ ผู้ให้บริการอินเทอร์เน็ต ที่มีข้อจำกัดของอุปกรณ์ที่ไม่มี Logfile จัดเก็บในระบบ
2. แบบ **Centralize Mode** โดยจัดเก็บ Log file จากอุปกรณ์ต่างๆที่จัดส่งมาเก็บ โดยอุปกรณ์ที่จัดส่งสามารถจัดส่ง Logfile ได้ตามมาตรฐาน Syslog-ng

* สามารถศึกษารายละเอียด *Log file* ได้จากคู่มือการใช้งาน *Sniff-Log*

2. หน่วยงานเป็นผู้บริการ อินเทอร์เน็ต ,Web Server ,Mail Server และอื่น ๆ

Solution D

หน่วยงานมีการให้บริการ
อินเทอร์เน็ต, Web
Server ,Mail Server และอื่น ๆ



การจัดเก็บ Log กระทำได้โดยใช้โปรแกรม Sniff-Log แบบ Passive Mode และ Centralize Mode โดย Gateway อาจไม่สามารถส่ง Log file* มาให้ Sniff-Log ได้ทำให้ต้องใช้ Passive Box ช่วยจัดส่ง Log file มาจัดเก็บที่ Sniff-Log แบบ Passive Mode โดยให้ Web Server , Mail Server ส่งข้อมูล Log file * มาจัดเก็บที่ Sniff-Log แบบ Centralize Mode

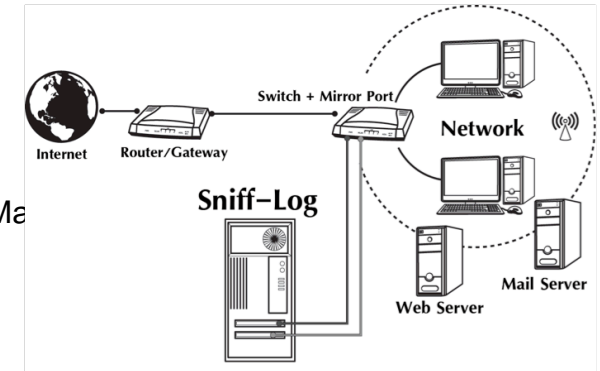
Note

- รูปแบบการจัดเก็บ Log file ที่เห็นอยู่ในตลาดประกอบด้วย 3 รูปแบบคือ
1. แบบ Active Mode เช่น Firewall , Proxy เป็นต้น
 2. แบบ Passive Mode เช่น Sniff-Log และ Logkeeper เป็นต้น
 3. แบบ Centralize Mode เช่น Syslog-NG,Syslog-D และ Sniff-Log เป็นต้น

2

Solution E

หน่วยงานมีการให้บริการ
อินเทอร์เน็ต, Web Server ,Ma
il Server และอื่น ๆ



การจัดเก็บ Log กระทำได้โดยใช้โปรแกรม Sniff-Log แบบ Centralize Mode โดยให้ Gateway , Firewall, Proxy, Web Server , Mail Server ส่งข้อมูล Log file * มาจัดเก็บที่ Sniff-Log (ความสามารถส่งข้อมูล Log file มาจัดเก็บที่ Sniff-Log นั้นเป็นความสามารถของอุปกรณ์ที่จัดส่ง เช่น Gateway , Firewall, Proxy, Web Server , Mail Server เป็นต้น)

Hardware Required

Sniff-Log อยู่บนพื้นฐานของระบบปฏิบัติการ Ubuntu โดยพัฒนาขึ้นเพื่ออำนวยความสะดวกในการติดตั้ง Sniff-Log เหมาะสำหรับผู้ที่ยังใหม่ต่อระบบปฏิบัติการตระกูล Ubuntu/ Debian GNU/Linux



โดยเครื่องคอมพิวเตอร์สำหรับติดตั้งโปรแกรม Sniff-Log 2.0 นั้นจะต้องมีคุณสมบัติขั้นต่ำดังนี้

Spec ขั้นต่ำ	Spec แนะนำ
CPU : 1.8 GHz	CPU : 2.4 GHz
Memory : 512 MB	Memory : 1GMB

Harddisk : สำหรับลงโปรแกรม OS Ubuntu และ Sniff-Log 2 GB สำหรับจัดเก็บข้อมูลการจราจร (Log file) ไม่น้อยกว่า 90 วัน แต่ไม่เกิน 365 วัน(1ปี)

รูปแบบการจัดเก็บ	อินเทอร์เน็ต	ระยะเวลาการใช้งาน	ขนาด Haddisk (90 วัน)
Passive Mode	1 Mb/s	24 ชม (1 วัน)	1 GB/1 วัน เพราะฉะนั้น 90 วันคาดว่าจะใช้งาน 90 GB
Centralize Log	พิจารณาตามขนาด Log file ของแต่ละ Server ที่ใช้งาน เช่น Mail Server , Web Server , Appliation Server ที่เก็บแต่ละวัน และนำมาคำนวณ		

Lancard : จำนวน Lancard ที่ใช้งานพิจารณาตามลักษณะรูปแบบการจัดเก็บและอุปกรณ์ช่วยในการจัดเก็บ

รูปแบบการจัดเก็บ	อุปกรณ์ช่วยในการจัดเก็บ	จำนวน Lancard	หมายเหตุ
Solution A Passive Mode แบบที่ 1	Pssive box หรือ Hub อย่างน้อย 4 Ports	3 ใบ	ใบที่ 1 สำหรับ Manage เครื่อง Sniff-log ใบที่ 2,3 สำหรับ ใช้จัดเก็บ Log file
Solution B Passive Mode แบบที่ 2	Switch ที่มีคุณสมบัติทำ Mirror Ports ได้	2 ใบ	ใบที่ 1 สำหรับ Manage เครื่อง Sniff-log ใบที่ 2 สำหรับ ใช้จัดเก็บ Log file
Solution C Centralize Mode	-	1 ใบ	ใบที่ 1 สำหรับ Maneg เครื่อง Sniff-Log พร้อมจัดเก็บ Log file แบบ Centralize
Solution D Passive แบบที่ 1+ Centralize Mode	Pssive box หรือ Hub อย่างน้อย 4 Ports	3 ใบ	ใบที่ 1 สำหรับ Manage เครื่อง Sniff-log พร้อมจัดเก็บ Log file แบบ Centralize ใบที่ 2,3 สำหรับ ใช้จัดเก็บ Log file แบบ Passive Mode
Solution E Passive แบบที่ 2 + Centralize Mode	Switch ที่มีคุณสมบัติทำ Mirror Ports ได้	2 ใบ	ใบที่ 1 สำหรับ Manage เครื่อง Sniff-log พร้อมจัดเก็บ Log file แบบ Centralize ใบที่ 2 สำหรับ ใช้จัดเก็บ Log file แบบ Passive Mode

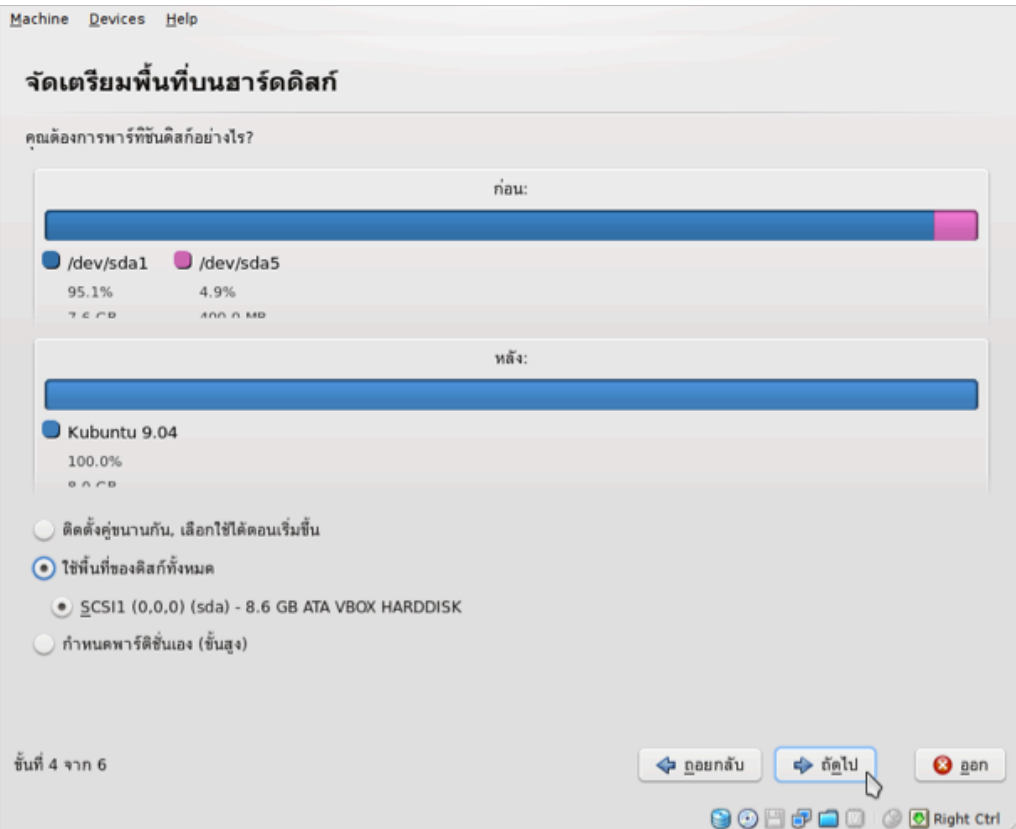
Lancard ใบที่ 1

หมายเหตุ : Lancard ที่ใช้ติดตั้งในเครื่องคอมพิวเตอร์ที่จะลงโปรแกรม Sniff-Log จะต้องติดตั้งไปก่อนที่จะติดตั้งโปรแกรม

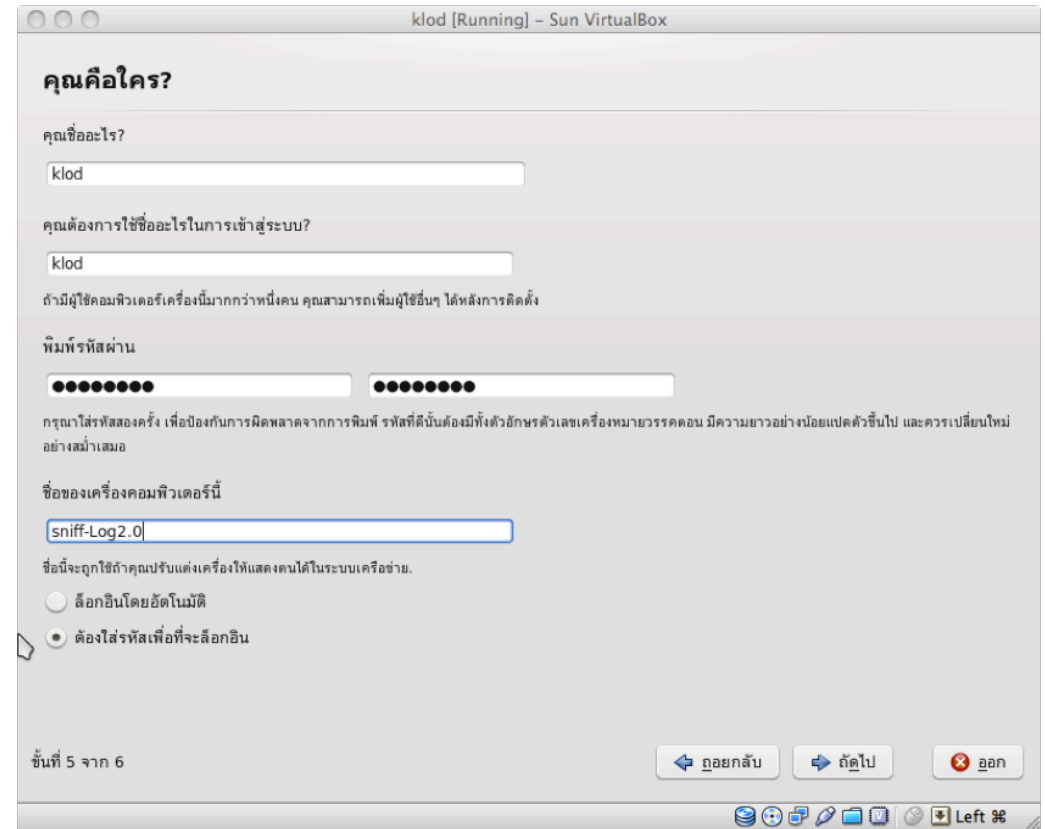
Lancard ใบที่ 2

Lancard ใบที่ 3

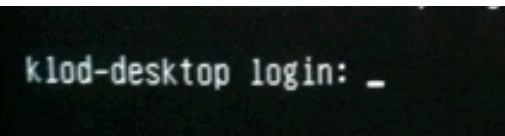


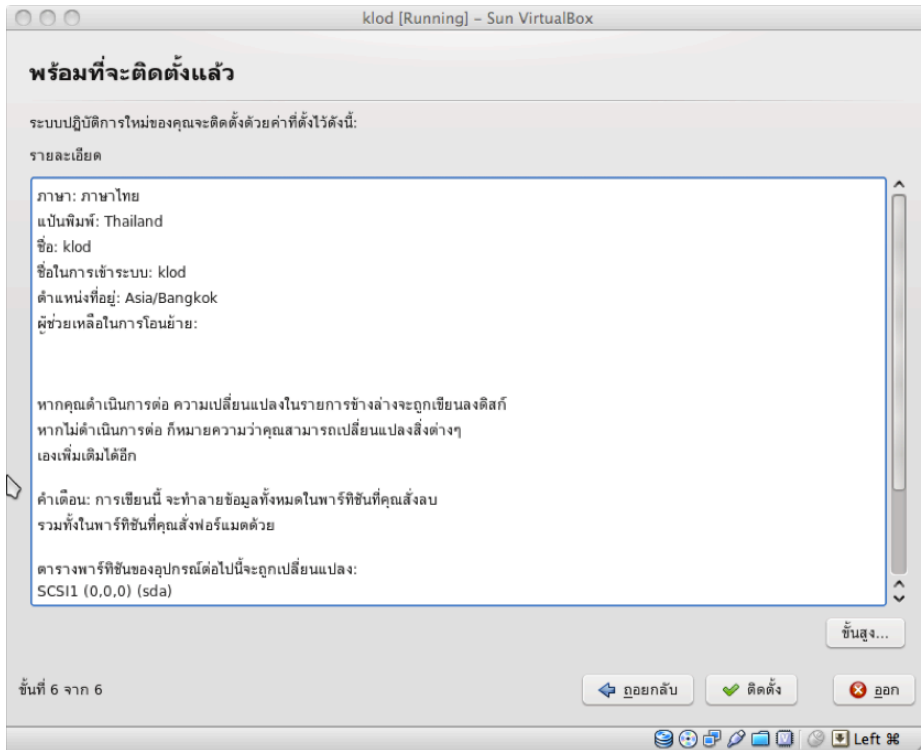


6. กำหนดพื้นที่บนฮาร์ดดิสก์ที่จะติดตั้ง และแนะนำให้ใช้พื้นที่ของฮาร์ดดิสก์ทั้งหมด (ตัวเลือกที่สอง) แต่โปรดระวัง ข้อมูลของท่านที่มีในฮาร์ดดิสก์จะหายหมด



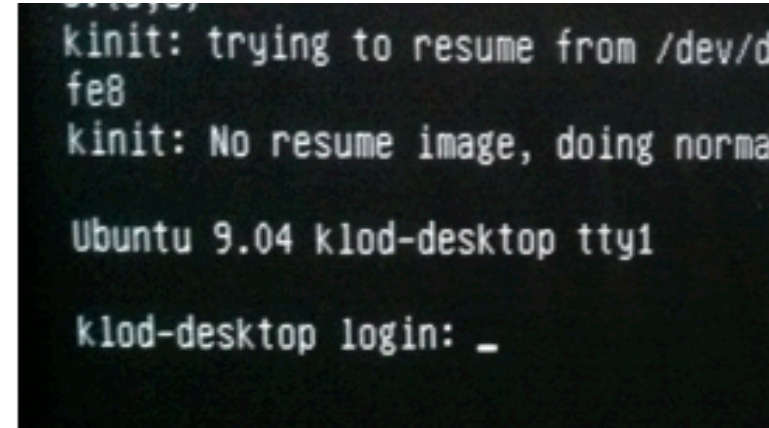
7. กำหนดชื่อผู้ใช้, รหัสผ่าน โดย ชื่อผู้ใช้ และรหัสผ่าน นี้จะนำไปใช้ในระบบปฏิบัติการ Ubuntu และ ค่อยตั้งชื่อเครื่องคอมพิวเตอร์





8. ระบบจะพร้อมติดตั้ง ให้กดปุ่ม ติดตั้ง การติดตั้งจะใช้เวลา 20-30 นาที ขึ้นอยู่กับประสิทธิภาพของเครื่องคอมพิวเตอร์

9. เมื่อเสร็จสิ้น ระบบจะแจ้งให้เอาแผ่น CD ออกจากเครื่อง(ให้นำแผ่น CD ออก) เพื่อที่จะทำการ Restart ระบบ หลังจาก Restart แล้ว ระบบจะแสดงหน้าจอพร้อมทำงาน



10. โดยนำ ชื่อผู้ใช้งาน ที่ตั้งเป็นชื่อ Login และ รหัสผ่าน เป็น Password สำหรับตั้งโปรแกรม Sniff-Log ต่อไป

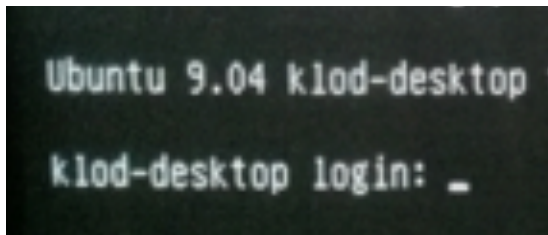
การตั้งค่าโปรแกรม Sniff-Log

แบ่งเป็น 3 ขั้นตอน คือ

1. ตั้งค่า Lincard ของเครื่อง Sniff-Log ตามระบบเครือข่าย
2. ตั้งค่า วันและเวลา เบื้องต้น
3. ลบค่าข้อมูล Log file เดิมก่อนนำไปใช้งาน *

1. ตั้งค่า Lincard ของเครื่อง Sniff-Log ตามระบบเครือข่าย

การตั้งค่า Network (IP Address, Gateway เป็นต้น) สามารถทำได้ตามขั้นตอนดังนี้



1. Log-in โดยใส่ ชื่อที่เข้าสู่ระบบ และรหัสผ่าน และกด Enter
2. พิมพ์ sudo -s และกด Enter
3. Root mode และ ป้อนรหัสผ่านอีกครั้ง
4. พิมพ์คำสั่ง nano /etc/network/interfaces แล้วกด Enter

```
auto eth0
allow-hotplug eth0
iface eth0 inet static
address 10.1.1.200
netmask 255.255.255.0
gateway 10.1.1.1
```

```
auto eth1
iface eth1 inet dhcp

auto eth2
iface eth2 inet dhcp
```

5. เข้าปรับปรุง
Lincard ตาม
ชุดคำสั่งนี้

6. เมื่อพิมพ์ข้อมูลข้อ 5
เรียบร้อยแล้ว
กดปุ่ม Control + X
เพื่อ Save
ข้อมูลที่ปรับปรุง

```
auto eth0
allow-hotplug eth0
iface eth0 inet static
address 10.1.1.200
netmask 255.255.255.0
gateway 10.1.1.1
```

eth0 คือ Lincard ไบที่ 1 สำหรับ Manage และรับข้อมูลแบบ Centralize address คือ Address ของเครื่อง Sniff-Log gateway คือ Gateway สำหรับออกอินเทอร์เน็ต

```
auto eth1
iface eth1 inet dhcp
```

eth1 คือ Lincard ไบที่ 2 เพื่อรับข้อมูลแบบ Passive

```
auto eth2
iface eth2 inet dhcp
```

eth2 คือ Lincard ไบที่ 3 เพื่อรับข้อมูล แบบ Passive

2 การตั้งค่าวันที่และเวลาในเครื่องคอมพิวเตอร์

ควรทำต่อจากตั้งค่า Lincard เพื่ออยู่ในสถานะ root

พิมพ์คำสั่ง `date 012700242011` แล้วกด Enter

หมายเหตุ: สมมติเวลาปัจจุบันคือ 27 มกราคม 2524 เวลา 00:24 น. คำสั่งตั้งเวลาจะอยู่ในรูปแบบ ดังนี้

`date MMDDhhmmYYYY`

```
klod@klod-desktop:~$
klod@klod-desktop:~$
klod@klod-desktop:~$ reboot
reboot: Need to be root
klod@klod-desktop:~$ sudo -s
[sudo] password for klod:
Sorry, try again.
[sudo] password for klod:
root@klod-desktop:~# date 012700242011
๒๗. ๒๗ ม.ค. ๒๕๕๔ ๐๐:๒๔:๐๐ ICT
root@klod-desktop:~# _
```

Note การตั้งเวลาโดย STP ภายในโปรแกรม Sniff-Log โดยโปรแกรม Webmin เพื่อให้เวลาของเครื่อง Sniff-Log ตรงกับมาตรฐานเวลาที่ พรบ.กำหนดไว้ ให้ไม่เกิน Statum 0 ไม่เกิน 10 MSc สามารถกระทำได้หลังจากตั้งเวลากลางของเครื่องเรียบร้อยแล้วเพื่อให้ช่วงเวลามีการปรับแบบเหมาะสมไม่เช่นนั้นช่วงเวลามีช่วงห่างมากเกินไปอาจทำให้การดึงข้อมูลผิดพลาดได้

3 ลบค่าข้อมูลLog file เดิมก่อนนำไปใช้งาน

*ควรทำต่อจากตั้งเวลา Lincard เพื่ออยู่ในสถานะ root

ลบข้อมูลของ Passive Log ที่ระบบจัดเก็บไว้ก่อนหน้านี้ เนื่องจากเวลาไม่ตรงกันจึงต้องทำการลบข้อมูลเก่า ออกเสียก่อน

- | | |
|--|--------------|
| 1.พิมพ์คำสั่ง <code>rm -rf /home/netsniffer/default/*</code> | แล้วกด Enter |
| 2.พิมพ์คำสั่ง <code>rm -rf /home/netsniffer/IN/*</code> | แล้วกด Enter |
| 3.พิมพ์คำสั่ง <code>rm -rf /home/netsniffer/OUT/*</code> | แล้วกด Enter |

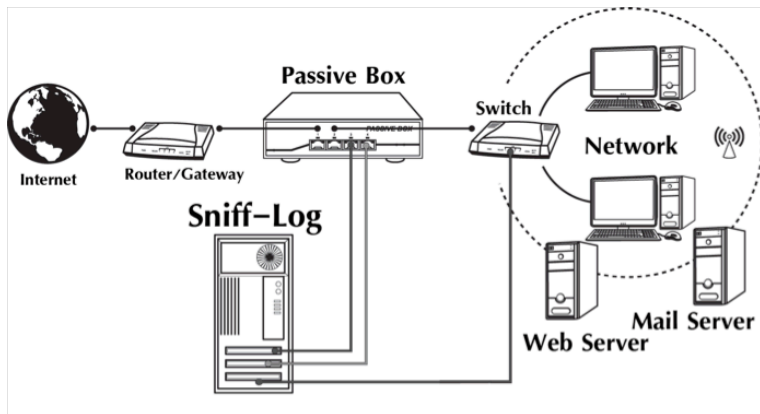
Note โปรแกรม Sniff-Log จะทำการจัดเก็บข้อมูล Log ตั้งแต่เริ่มต้นติดตั้งโปรแกรมฯทำให้จะต้องลบข้อมูล Log เดิมก่อนเพื่อไม่ให้เกิดความสับสน

ให้พิมพ์คำสั่ง `Reboot` แล้ว Enter เพื่อทำการ Restart อุปกรณ์เพื่อ Active ค่าต่าง ๆที่ได้กำหนดไว้

การ Activate โปรแกรม Sniff-Log

เมื่อติดตั้ง เครื่องคอมพิวเตอร์ ที่ลงโปรแกรม Sniff-Log เข้ากับระบบเครือข่าย
ดังตัวอย่าง Solution D และทำการ Set Up Lincard และ gateway ให้กับ เครื่อง Sniff-Log เรียบร้อยแล้ว

9



ให้เครื่องคอมพิวเตอร์ถูกข่ายที่อยู่ในเครือข่ายเดียวกัน
(IP Group เดียวกัน)

- 1.เปิด Browser เช่น IE, FireFox หรือ Safari
- 2.พิมพ์ IP Adress ของเครื่อง Sniff-Log ที่ได้ตั้งค่าไว้
จะปรากฏหน้าโปรแกรม Sniff-Log ที่รอ Active ดังรูป
- 3.ให้ใส่หมายเลข Product Key ที่ได้รับ
(ขั้นตอนนี้จะ Sniff-Log จะต้องเชื่อมต่อกับ
อินเทอร์เน็ต)

แสดงว่า Product Key ถูกต้อง

ให้ใส่ข้อมูล Customer Information
เพื่อรับบริการจาก SGC Network
ต่อไป (เป็นการลงทะเบียนกับ SGC
Network)



Product Key
จากหน้าปก CD



เมื่อติดตั้ง Sniff-Log แล้วระบบ Passive จะทำงานอัตโนมัติ เมื่อทำการเชื่อมต่ออุปกรณ์ Passive Box เข้ากับระบบเครือข่ายตามรูปแบบ Solution ก็จะสามารถจัดเก็บข้อมูล Log file ได้ทันที

1.รายงานการจัดเก็บ Log file

Configurations | Passive Log

Internet : ■ | Passive Status : ■ | Contra
 Storage : 226.43 GB GB | Passive Used : 0.84 GB | Centra
 36 Used : 14.62/226.43 GB | 0.37 %

Passive Report
 Export Passive Data
 Passive Configuration
 Service Management

เลือกเมนู
Passive Report

รายงานข้อมูล Passive Log

Date : 28 February 2011
 Time : 9 : 36 : 53
 Amount : 500
 Arrange Mode : DESC
 View : default

View Report

เลือกวัน
และเวลาที่
ต้องการงาน

Note

แสดงที่อยู่ รายละเอียดของเว็บไซต์ที่จัดเก็บไว้ได้

IP address: 202.142.221.128 / IP or ISP location: Bangkok in Krung Thep

Domain: www.ipaddress.com
 IP address: 202.142.221.128
 IP country: Thailand
 IP Address state: Krung Thep
 IP Address city: Bangkok
 IP latitude: 13.7500
 IP longitude: 100.5167
 ISP: DeaServer Limited Partnership CO.
 Organization: DeaServer Limited Partnership CO.
 Host: mail.deaserv.net

แสดงรายงาน Log file แบบ Passive Mode

Passive Log > Passive Report > View - รายงาน Passive Log

Date : 28 Feb 2011 09:36:53

No.	Date Time	Sub Sec	Status	Mac	IP Source	Port	IP Destination	Port	Protocol	Service	Package
1.	23 Feb 2011 00:13:57	785135	P	00:25:22:59:c3:d9	192.168.1.200	80	192.168.1.2	51851	tcp	-	1448
2.	23 Feb 2011 00:13:57	785012	P	00:25:22:59:c3:d9	192.168.1.200	80	192.168.1.2	51850	tcp	-	1448
3.	23 Feb 2011 00:13:57	784889	P	00:25:22:59:c3:d9	192.168.1.200	80	192.168.1.2	51850	tcp	-	1448
4.	23 Feb 2011 00:13:57	784765	P	00:25:22:59:c3:d9	192.168.1.200	80	192.168.1.2	51850	tcp	-	1448
5.	23 Feb 2011 00:13:57	784642	P	00:25:22:59:c3:d9	192.168.1.200	80	192.168.1.2	51850	tcp	-	1448
6.	23 Feb 2011 00:13:57	784519	P	00:25:22:59:c3:d9	192.168.1.200	80	192.168.1.2	51850	tcp	-	1448
7.	23 Feb 2011 00:13:57	784397	P	00:25:22:59:c3:d9	192.168.1.200	80	192.168.1.2	51850	tco	-	1448

2. การนำ Log file ออก หรือ นำส่งเจ้าหน้าที่ แบบ Passive หรือ

The screenshot shows the SGC Network Present Sniff-Log 2.0 interface. At the top, there are navigation buttons: 'Configurations', 'Passive Log', 'Access Log', and 'Logout'. A blue callout bubble points to the 'Passive Log' button with the text 'เลือกเมนู Export Passive'. Below the navigation bar, there is a status section with various indicators and a pie chart showing disk usage: 0.4% Passive, 0.0% Centralize, 6.1% Other, and 93.5% Free. A second blue callout bubble points to the 'Export Passive Data' option in the 'Passive Report' dropdown menu with the text 'เลือกวันและเวลาที่ต้องนำข้อมูล Passive ออก'. Below this, the 'Export Passive Data' configuration page is shown, with a third blue callout bubble pointing to the date and time selection fields with the text 'กด Save ข้อมูล'. The configuration includes 'Date-Time Start' and 'Date-Time End' fields, both set to 28 February 2011, and '00:00' to '23:59'. There are 'Search' and 'View All' buttons. Below the configuration, a table displays export records with columns for name, MD5, Record Start, Record End, File Size, Last Modified, and Save to Disk. The table contains three rows of data. At the bottom right, there is a link for 'Download TCPDump Software' and a copyright notice for '© 2011 SGC Network Co., Ltd.'.

เมื่อเครื่องคอมพิวเตอร์ที่ลงโปรแกรม Sniff-Log เชื่อมกับระบบเครือข่าย การใช้งาน Centralize Mode นั้น จำเป็นจะต้องให้แหล่งกำเนิด(Host) Log file เช่น Proxy , Firewall , Mail Server , FTP Server ทำการส่ง Log file มาที่ IP Address ของเครื่องคอมพิวเตอร์ Sniff-Log มาให้เบื้องต้นก่อนถึงจะสามารถจัดเก็บข้อมูลแบบ Centralize Log ได้

1.กำหนดแหล่งกำเนิด(Host) Log file ที่ส่ง Log file มาเก็บ

เลือกเมนู Source Manager

คลิก "เพิ่มอุปกรณ์ต้นทาง"

ชื่อในระบบ	ชนิด	Mac Address	IP Address	ข้อมูล	แก้ไข	ลบ
1.3	File Server	40:4A:03:2C:6D:56	192.168.1.3			

configuration > Source Manager > New Source - เพิ่มข้อมูลอุปกรณ์ต้นทาง

ชื่อ:

ชื่อในระบบ:

ชนิด: * (เช่น web server, mail server, firewall เป็นต้น)

Mac Address:

IP Address:

Software (Agent):



หมายเหตุ:

* ห้ามเว้นว่าง

เพิ่ม กลับ

Note

Log file ที่ส่งมาจากแหล่งกำเนิด กรณีชื่อข้อมูลในระบบ หรือ เป็นการจัดเก็บข้อมูลซ้ำซ้อน ก็จะปรากฏแถบสีเตือน

-  ไม่มีข้อมูลชื่อในระบบ
-  ข้อมูลมีความซ้ำซ้อน

ถ้ามีข้อมูล Log file จากแหล่งกำเนิด Log file ส่งมา ก็จะปรากฏชื่อแหล่งกำเนิด หรือ IP (ถ้าไม่ปรากฏแสดงว่า Log file ไม่ถูกส่งมา)

2.รายงาน และการนำข้อมูล Log file ออก หรือ นำส่งเจ้าหน้าที่แบบ Centralize

เลือกเมนู Centralize Report

เลือก Server ที่ต้องการข้อมูล และวัน เวลาที่ต้องแสดงรายงาน

Search Conditions
 Host Name : Zyxel NSA210
 Date-Time Start : 28 February 2011 00:00:00
 Date-Time End : 28 February 2011 23:59:59
 View

Note

สามารถ Search ข้อมูล เฉพาะเจาะจงลงไปได้ว่าต้องการหาอะไร

Search Message :

Host Name	Date
192.168.1.3	2011-02-28 0

เลือกเมนู Export Passive

เลือก Server ที่ต้องการข้อมูล และวัน เวลาที่ต้องนำข้อมูลออก

Search Conditions
 Host Name : Zyxel NSA210
 Date-Time Start : 28 February 2011 00:00:00
 Date-Time End : 28 February 2011 23:59:59
 Export to file...

