หน่วยที่ 5
การทำงานของ Network Address Translation และไฟร์วอลล์ (Firewall)

สาระการเรียนรู้

1. ความหมายของ Network Address Translation
2. การทำงานของ Network Address Translation
3. การตั้งค่า Network Address Translation
4. ความหมายของไฟร์วอลล์ (Firewall)
5. ประเภทของไฟร์วอลล์ (Firewall)
6. การตั้งค่าไฟร์วอลล์ (Firewall)

จุดประสงค์ทั่วไป

มีความรู้ความเข้าใจ เกี่ยวกับ ความหมาย Network Address Translation การทำงานของ Network Address Translation การตั้งค่า Network Address Translation ความหมายไฟร์วอลล์ (Firewall) การทำงานของไฟร์วอลล์ (Firewall) และการตั้งค่าไฟร์วอลล์ (Firewall)

จุดประสงค์เชิงพฤติกรรม

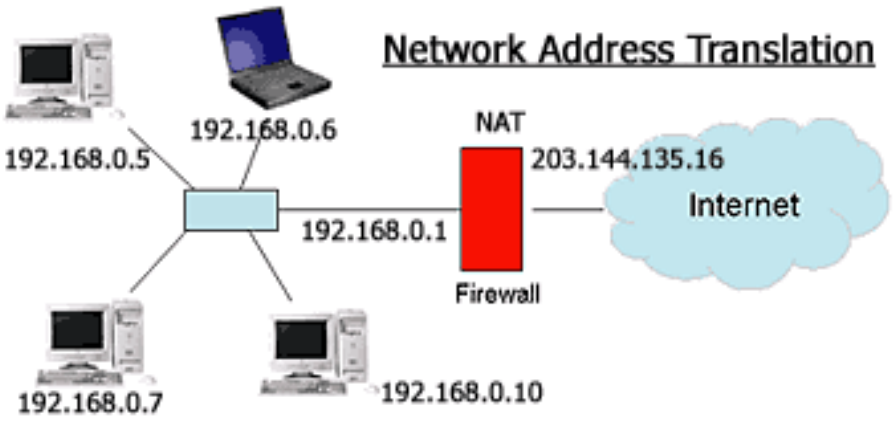
1. บอกความหมาย Network Address Translation ได้
2. บอกการทำงานของ Network Address Translation ได้
3. อธิบายการตั้งค่า Network Address Translation ได้
4. บอกความหมายไฟร์วอลล์ (Firewall) ได้
5. บอกการทำงานของไฟร์วอลล์ (Firewall) ได้
6. อธิบายการตั้งค่าไฟร์วอลล์ (Firewall) ได้

การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์นั้น จำเป็นที่จะต้องมีไอพีแอดเดรส (IP Address) ซึ่งเป็นหมายเลขขนาด 32 บิท ที่ไม่ซ้ำกัน สำหรับใช้ในการระบุถึงสถานที่ตั้งของเครื่องคอมพิวเตอร์ภายในระบบเครือข่าย เพื่อที่จะสามารถทำการส่งข้อมูลไปยังเครื่องคอมพิวเตอร์แต่ละเครื่องได้ เมื่อครั้งตอนทำการออกแบบไอพีแอดเดรส (IP Address) ใน เวอร์ชั่น 4 (Version 4) หรือที่เรียกว่า IPv4 นั้น ผู้ออกแบบคิดว่าปริมาณของหมายเลขไอพีแอดเดรส (IP Address) ของ IPv4 นั้นมีจำนวนมากเกินความต้องการ เนื่องจากในทางทฤษฎีแล้ว IPv4 สามารถที่จำนวนหมายเลข IP Address ที่ไม่ซ้ำกันได้ถึง 4,294,967,296 หมายเลข (แต่สามารถใช้งานได้ประมาณ 3.2 ถึง 3.3 พันล้านหมายเลข เนื่องจากบาง IP Address ได้ถูกสำรองไว้ใช้งานอื่น ๆ เช่น multicasting, broadcast เป็นต้น) แต่เนื่องจากในปัจจุบันมีการใช้งานอินเทอร์เน็ตอย่างแพร่หลายมากขึ้น จนเกินความคาดหมายของผู้ออกแบบ IPv4 ทำให้ IP Address ที่สามารถนำมาใช้งานได้ในปัจจุบันกำลังจะหมดลงไป ในการใช้งาน IPv4 ในปัจจุบันนี้จึงต้องมีการใช้งานอย่างประหยัดมากขึ้น และการทำเน็ตเวิร์กแอดเดรสทรานเลชั่น (Network Address Translation : NAT) ก็เป็นวิธีการหนึ่งที่จะช่วยในการประหยัดการใช้งาน IP Address ได้

องค์กร IANA (Internet Assigned Nubbers Authority) ได้ทำการกำหนดช่วงของไอพีแอดเดรส (IP Address) สำหรับการใช้งานในเครือข่ายภายในเอาไว้หรือที่เรียกว่า Private IP Address ซึ่งเป็น IP Address แบบ Unregistered โดยจะไม่สามารถใช้งานไอพีแอดเดรส (IP Address) เหล่านี้ในเครือข่ายสาธารณะหรือเครือข่ายอินเทอร์เน็ตได้ แต่สร้างขึ้นมาเพื่อใช้งานสำหรับเครือข่ายภายในองค์กรเท่านั้น ซึ่งในแต่ละองค์กรก็อาจจที่จะใช้ไอพีแอดเดรส (IP Address) ในช่วงเดียวกันหรือซ้ำกันก็ได้ ยกตัวอย่างเช่น ไอพีแอดเดรส (IP Address) ในชุด 192.168.x.x ที่มีการใช้งานอย่าแพร่หลาย แต่เมื่อมีเครื่องในเครือข่ายภายในแต่ละองค์กรต้องการที่จะติดต่อกับเครือข่ายอินเทอร์เน็ต ก็จะถูกทำการ NAT IP Address แบบ Private IP Address เหล่านี้ไปเป็นไอพีแอดเดรส (IP Address) แบบ Public IP Address หรือ IP Address แบบ Registered ได้

1. เน็ตเวิร์กแอดเดรสทรานเลชั่น (Network Address Translation : NAT)

เน็ตเวิร์กแอดเดรสทรานเลชั่น (Network Address Translation : NAT) คือ วิธีการทางเครือข่ายที่จะเปลี่ยนค่าเน็ตเวิร์กแอดเดรส (Network Address) จากหมายเลขหนึ่งไปเป็นอีกหมายเลขหนึ่ง ซึ่งทำให้เกิดการเชื่อมต่อไปยังเครื่องปลายทางได้ โดยเครื่องต้นทางไม่จำเป็นต้องเปลี่ยนแปลงค่าทางเครือข่าย การทำแน็ท (NAT) ช่วยให้การใช้งานเครือข่ายทำได้อย่างมีประสิทธิภาพมากขึ้นกว่าที่เป็นอยู่ รวมทั้งมีส่วนในการรักษาความปลอดภัยในเครือข่ายได้ด้วย ซึ่งโดยทั่วไปจะเป็นความสารถหนึ่งในไฟร์วอลล์ (Firewall) หรืออุปกรณ์เครือข่ายทั่วไปอยู่แล้ว



ภาพที่ 5.1 เน็ตเวิร์กแอดเดรสทรานเลชั่น (Network Address Translation)
ที่มา : http://thaicourt.blogspot.com

จากภาพจะเห็นว่าตัว แน็ทเซิร์ฟเวอร์ (NAT Server) มีไอพีแอดเดรส (IP Address) เป็น 192.168.0.1 สำหรับเครือข่ายภายใน (Inside Network) และมี ไอพีแอดเดรส (IP Address) เป็น 203.144.135.16 สำหรับเครือข่ายภายนอก (Outside Network) เมื่อเครื่อง 192.168.0.5 ต้องการเอ็กพอร์ท (Export) ทาง อินเทอร์เน็ตแน็ทเซิร์ฟเวอร์ (Internet NAT Server) ก็จะแปลงไอพี (IP) จาก 192.168.0.5 ไปเป็น 203.144.135.16 และข้อมูลขาออกที่ออกไปยัง เอ็กเทอร์นัล (External Network) นั้นจะเป็นข้อมูลที่มี ซอร์ตไอพีแอดเดรส (Source IP Address) เป็นเครือข่ายภายนอก (Outside IP Address) ของแน็ทเซิร์ฟเวอร์ (NAT Server)

2. การทำงานของ Network Address Translation

โดยทั่วไปในระบบเครือข่ายภายในองค์กร โดยเฉพาะองค์กรที่มีเซิร์ฟเวอร์ (Server) เป็น ลีนุกซ์ (Linux), วินโดว์ เอ็นที (Windows NT), วินโดว์ 2000 เซิร์ฟเวอร์ (Windows 2000 Server) จะมีการกำหนดไอพี (IP) ภายในองค์กรที่เรียกว่า ไปรเวทไอพี (Private IP) เช่น 192.168.0.1 หรือ 10.0.0.1 เป็นต้น ซึ่งไอพี (IP) เหล่านี้เป็นไอพี (IP) ที่ไม่สามารถนำไปใช้งานในระบบอินเตอร์เน็ตได้ การทำแน็ท (NAT) จะเป็นการแปลงไปรเวทไอพี (Private IP) ให้เป็นไอพี (IP) ที่สามารถใช้งานบนระบบอินเตอร์เน็ตได้ หรือที่เราเรียกว่า รีจีสเตอร์ไอพี (Registered IP)

2.1 ขั้นตอนการทำงาน

แน็ท (NAT) จะสร้างตารางภายในซึ่งมีไว้สำหรับบรรจุข้อมูลไอพีแอดเดรส (IP Address) ของเครื่องในเครือข่ายภายในที่ส่งแพ็กเกจ (Packet) ผ่าน แน็ทเซิร์ฟเวอร์ (NAT Server) จากนั้นก็จะสร้างตารางไว้สำหรับเก็บข้อมูลหมายเลขพอร์ต (Port Number) ที่ถูกใช้ไปโดย เอาท์ไซต์ไอพีแอดเดรส (Outside IP address) จะมีกระบวนการทำงานดังนี้

2.1.1 จะบันทึกข้อมูลซอร์ตไอพีแอดเดรส (Source IP Address) และซอร์ตไอพีพอร์ตนัมเบอร์ (Source port number) ไว้ในล็อกไฟล์ (Log File)

2.1.2 จะแทนที่ไอพี (IP) ของแพ็กเกจ (Packet) ด้วยไอพี (IP) ขาออกของ แน็ทเซิร์ฟเวอร์ (NAT Server) เมื่อ แน็ทเซิร์ฟเวอร์ (NAT Server) ได้รับแพ็กเกจ (Packet) ย้อนกลับมาจากเครือข่ายภายนอก (external network) ก็จะตรวจสอบปลายทางของพอร์ตนัมเบอร์ (Destination port number) ของแพ็กเกจ (Packet) นั้น ๆ แล้วนำมาเปรียบเทียบกับข้อมูล ซอร์ตพอร์ตนัมเบอร์ (Source port number) ในล็อกไฟล์ (Log File) ถ้าเจอข้อมูลที่ตรงกันก็จะเขียนทับ destination port number, destination IP address ของ packet นั้น ๆ แล้วจึงส่ง packet นั้นไปยังเครื่องอยู่ภายในเครือข่ายภายใน

2.2 ไปรเวทไอพีแอดเดรส (Private IP Address)

หมายเลขไอพีแอดเดรสในช่วงที่ไม่สามารถนำมาเชื่อมต่อกับเครือข่ายอื่นๆ ได้โดยตรง ซึ่งช่วงของหมายเลขไอพีแอดเดรสที่เป็นไปรเวทไอพีแอดเดรส (Private IP) นั้น จะแบ่งเป็น 3 กลุ่มด้วยกันคือ

1.3.1 ช่วงหมายเลข 10.0.0.0 – 10.255.255.255 (10 / 8)

1.3.2 ช่วงหมายเลข 172.16.0.0 – 172.32.255.255 (172.16 / 12)

1.3.3 ช่วงหมายเลข 192.168.0.0 – 192.168. 255.255 (192.168 / 16)

2.3 คุณสมบัติของอุปกรณ์แน็ท (NAT)

อุปกรณ์เครือข่าย หรือโปรแกรมที่ใช้ในการทำ NAT จะต้องมีความสามารถในการทำงานต่าง ๆ เหล่านี้คือ

2.3.1 สามารถกำหนดหมายเลขไอพีแอดเดรสได้ (Transparent address assignment)

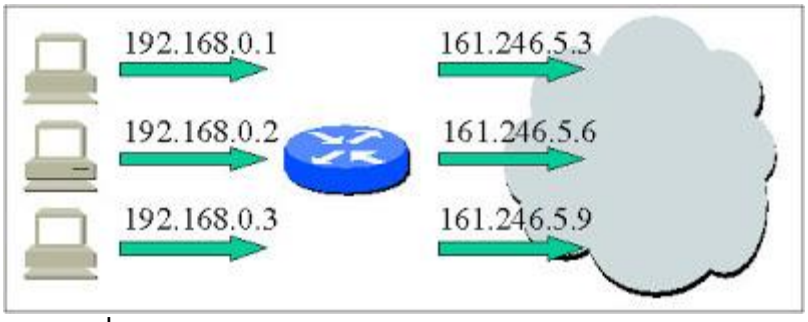
2.3.2 สามารถส่งผ่านแพคเก็จของข้อมูลที่มีการเปลี่ยนแปลงแอดเดรสได้ (Transparent address routing through address transition)

2.3.3 สามารถเปลี่ยนแปลงข้อมูลของ ICMP payload ได้ (ICMP error message payload translation)

2.4 รูปแบบในการเปลี่ยนแปลงค่าไอพีแอดเดรส (IP Address)

2.4.1 Static NAT (static assignment and basic NAT)

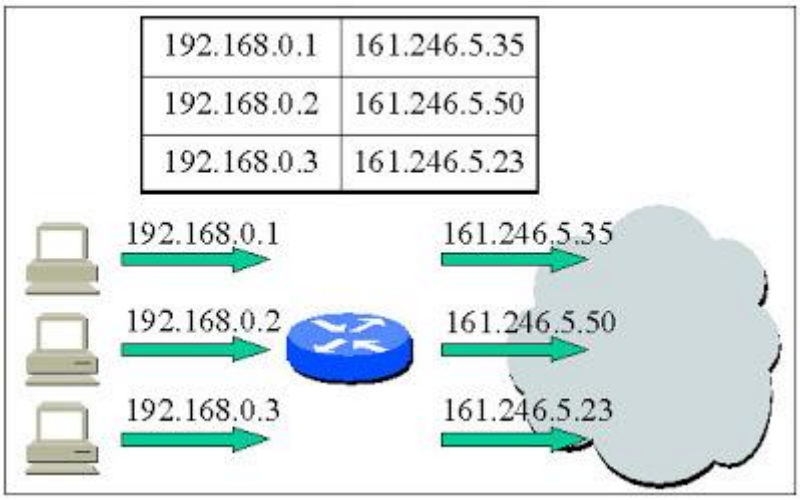
เป็นการเปลี่ยนแปลงค่าหมายเลขไอพีแอดเดรสโดยมีการจับคู่กันของหมายเลขไอพีแอดเดรสตลอดการทำงานของอุปกรณ์ ซึ่งจะเปลี่ยนแปลงค่าไอพีแอดเดรสจาก Private IP เป็นหมายเลขไอพีภายนอก และเปลี่ยนจากหมายเลขไอพีแอดเดรสภายนอกเป็น Private IP แบบหนึ่งต่อหนึ่งไปตลอด



ภาพที่ 5.2 Static NAT (static assignment and basic NAT)
ที่มา : https://www.gotoknow.org/posts/481846

2.4.2 Dynamic NAT (dynamic assignment and basic NAT)

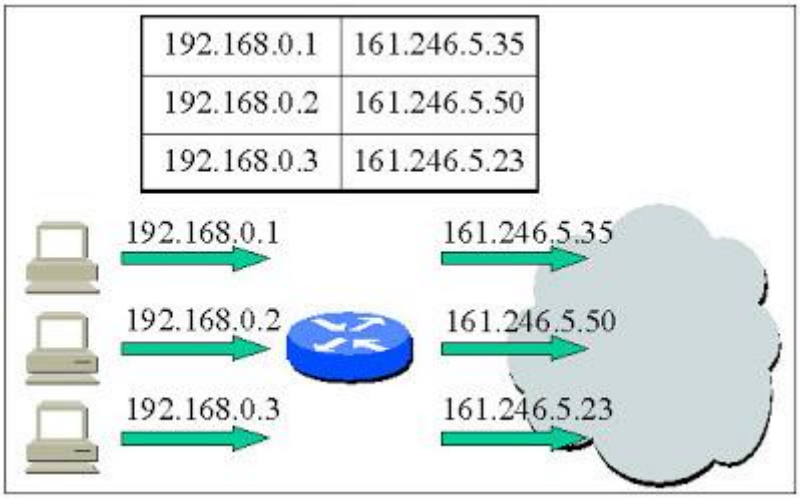
เป็นการเปลี่ยนแปลงค่าหมายเลขไอพีแอดเดรสโดยมีการจับคู่กันของหมายเลขไอพีแอดเดรสที่เป็น Private IP กับหมายเลขไอพีแอดเดรสภายนอกเพียงชั่วคราวเท่านั้น โดยอุปกรณ์ NAT จะจับคู่หมายเลขไอพีแอดเดรสในช่วงเวลาที่ session มีการเชื่อมต่อกันอยู่เท่านั้น หลังจากที่ใช้งาน session เสร็จเรียบร้อยแล้วจะไม่เก็บข้อมูลการจับคู่นั้นไว้อีก เมื่อมีการเชื่อมต่อกับเครือข่ายภายนอกอีกครั้ง อุปกรณ์ NAT จะเลือกหมายเลขไอพีแอดเดรสภายนอกใหม่อีกครั้งหนึ่ง ซึ่งไม่จำเป็นต้องซ้ำกับหมายเลขเดิม



ภาพที่ 5.3 Dynamic NAT (dynamic assignment and basic NAT)
ที่มา : https://www.gotoknow.org/posts/481846

2.4.3 Overloading (NAPT)

เป็นการเปลี่ยนแปลงหมายเลขไอพีแอดเดรสเพียงหมายเลขเดียว แต่มีการเปลี่ยนแปลงหมายเลขพอร์ตต้นทางในการเชื่อมต่อแทน เมื่อมีการตอบกลับจากเครื่องภายนอกเครือข่ายแล้ว ที่อุปกรณ์ NAT จะดูหมายเลขพอร์ตปลายทางในส่วนหัวของข้อมูลว่าเป็นหมายเลขอะไร แล้วจึงเปลี่ยนข้อมูลส่วนหัวให้ตรงกับเครื่องคอมพิวเตอร์ที่ทำการร้องขออีกครั้ง



ภาพที่ 5.4 Overloading (NAPT)

ที่มา : https://www.gotoknow.org/posts/481846

3. การติดตั้ง Network Address Translation (NAT)

การคอนฟิก NAT (Network Address Translation) บนลีนุกซ์ ด้วยไอพีเทเบิล (iptables) โดยจะแยกเป็นข้อต่าง ๆ ตามลักษณะการใช้งาน ซึ่งในแต่ละข้อ จะเคลียร์คอนฟิก rule ทั้งหมดของ nat ออกก่อน ด้วยออปชั่น '-F' แล้วเริ่มคอนฟิกใหม่ ทั้งนี้เพื่อให้ผู้อ่านสามารถนำไปทดสอบดูผลลัพธ์ที่เกิดขึ้นได้ แล้วหลังจากเข้าใจ สามารถนำ rule ต่าง ๆ มารวมกันเพื่อคอนฟิก NAT ในหลายรูปแบบพร้อม ๆ กันได้

เครื่องที่ทดลอง

1) ติดตั้งลินุกซ์ CentOS 7
2) พอร์แลนที่ 1 : eth0 IP Address 192.168.1.1/24 (ต่อเครือข่ายภายในองค์กร)
3) พอร์แลนที่ 2 : eth1 IP Address 192.168.100.11/24 (ต่อเครือข่ายภายนอก)
4) ปิด iptables rule ที่ทำหน้าที่เป็น firewall
5) ทุกเครื่องที่อยู่เครือข่ายภายใน (192.168.1.0/24) ชี้ default gateway ที่ 192.168.1.1

3.1 คอนฟิกลีนุกซ์ทำหน้าที่เป็นเราเตอร์ (Router)

โดยดีฟอลต์แล้ว ลีนุกซ์ไม่ได้ทำหน้าที่เป็นเราเตอร์ (Router) คือจะไม่ส่งต่อข้อมูล (IP packet forwarding) ใด ๆ ระหว่างอินเตอร์เฟซ ดังนั้น ถ้าต้องการให้ลีนุกซ์ทำเราติ้ง (Routing) ได้ ต้องเปิดคุณสมบัตินี้ก่อน ซึ่งสามารถทำได้โดยแก้ไขไฟล์ /etc/sysctl.conf เปลี่ยนคอนฟิกของ net.ipv4.ip_forward จากค่า 0 เป็น 1

แก้ไขไฟล์ /etc/sysctl.conf เพื่อคอนฟิกเป็นเราเตอร์ (Router)

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

หลังจากแก้ไขไฟล์แล้ว ต้องรันคำสั่ง sysctl -p เพื่อให้ค่าที่แก้ไขไปมีผลทันที

ตัวอย่างการรันคำสั่ง sysctl

```
[root@linux-router ~]# sysctl -p
net.ipv4.ip_forward = 1
...
```

3.2 เปลี่ยน SOURCE IP ADDRESS แบบ MASQUERADE

ความต้องการ: เปลี่ยน Source IP Address ของ packet ที่ส่งจากเน็ตเวิร์ก 192.168.1.0/24 ไปยังเครื่องภายนอก เช่น 192.168.200.0/24

คำสั่งที่ใช้

```
# iptables -t nat -F
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth1 -j MASQUERADE
# iptables -t nat -L -v -n
```

ผลลัพธ์ที่จะแสดง

```
# iptables -t nat -F
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth1 -j MASQUERADE
# iptables -t nat -L -v -n
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  all  --  *      eth1    192.168.1.0/24       0.0.0.0/0
```

```
Chain OUTPUT (policy ACCEPT 31 packets, 2328 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

การใช้งาน :

เป็นการทำ NAT เพื่อให้เครื่องที่อยู่ในองค์กรที่ใช้ Private IP Address สามารถใช้งานเน็ตเวิร์กภายนอกหรืออินเตอร์เน็ตได้พร้อมกัน

IP Address ของพอร์ต eth1 ที่ต่อกับเน็ตเวิ็กภายนอก มีการเปลี่ยนแปลงไปเรื่อย ๆ เช่น ต่อเน็ตโดยใช้ ADSL, คุณสมบัติของ MASQUERADE จะเปลี่ยน Source IP Address เป็น IP ของพอร์ต eth1 โดยอัตโนมัติ

3.3 เปลี่ยน SOURCE IP ADDRESS แบบ SNAT

ความต้องการ: เปลี่ยน Source IP Address ใน packet ที่ส่งจากเน็ตเวิร์ก 192.168.1.0/24 ไปยังเครื่องภายนอก เช่น 192.168.200.0/24 ให้กลายเป็น Source IP 192.168.200.11

คำสั่งที่ใช้

```
# iptables -t nat -F
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j SNAT --to-source 192.168.200.11
# iptables -t nat -L -v -n
```

ผลลัพธ์ที่จะแสดง

```
# iptables -t nat -F
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j SNAT --to-source 192.168.200.11
# iptables -t nat -L -v -n
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 SNAT       all  --  *      *       192.168.1.0/24       0.0.0.0/0           to:192.168.200.11
```

```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

การใช้งาน :

เป็นการทำ NAT เพื่อให้เครื่องที่อยู่ในองค์กรที่ใช้ Private IP Address สามารถใช้งานเน็ตเวิร์กภายนอกหรืออินเตอร์เน็ตได้พร้อมกัน

IP Address ของพอร์ต eth1 ที่ต่อกับเน็ตเวิ็กภายนอก ไม่เปลี่ยนแปลง มีการ fix ไว้ ต้องระบุ IP ลงไปในคำสั่งเลย หลังออปชั่น '–to-source'

ถ้ารู้ IP ของพอร์ตขานอกแน่นอน ให้ใช้เป็น SNAT แล้วระบุ '–to-source' เพื่อเพิ่มประสิทธิภาพการทำ NAT เพราะว่าในการทำงาน ลีนุกซ์ไม่ต้องเสียเวลาไปค้นหา IP Address จากพอร์ตอีกครั้ง

3.4 เปลี่ยน DESTINATION IP ADDRESS แบบ DNAT

ความต้องการ: เปลี่ยน Destination IP Address ใน packet เพื่อส่งต่อ (redirect) packet ไปยัง IP Address ภายในที่ต้องการได้

ตัวอย่างเช่น

เมื่อเน็ตเวิร์กภายนอกเชื่อมต่อมาที่ IP 192.168.200.11 พอร์ต 80 ให้ส่งต่อ packet นี้ไปยังเครื่องภายในที่มี IP 192.168.1.2 พอร์ต 80

คำสั่งที่ใช้

```
# iptables -t nat -F
```

iptables -t nat -A PREROUTING -p tcp -d 192.168.200.11 --dport 80 -j DNAT --to-destination 192.168.1.2:80
iptables -t nat -A POSTROUTING -p tcp -s 192.168.1.2 --sport 80 -j SNAT --to-source 192.168.200.11:80
iptables -t nat -L -v -n

ผลลัพธ์ที่จะแสดง

```
# iptables -t nat -F
# iptables -t nat -A PREROUTING -p tcp -d 192.168.200.11 --dport 80 -j DNAT --to-destination 192.168.1.2:80
# iptables -t nat -A POSTROUTING -p tcp -s 192.168.1.2 --sport 80 -j SNAT --to-source 192.168.200.11:80
# iptables -t nat -L -v -n
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            192.168.200.11          tcp dpt:80
to:192.168.1.2:80
```

```
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 SNAT       tcp  --  *      *       192.168.1.2          0.0.0.0/0            tcp spt:80
to:192.168.200.11:80
```

```
Chain OUTPUT (policy ACCEPT 31 packets, 2328 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

การใช้งาน :

ตั้ง web server ไว้เน็ตเวิร์กภายในองค์กร แต่ต้องการให้คนภายนอกเช่นจากอินเตอร์เน็ตสามารถเรียกใช้งานได้ เราต้องคอนฟิกให้ภายนอกเชื่อมต่อเข้ามาที่ไอพี ของพอร์ตภายนอก (172.16.1.1) แล้วคอนฟิก DNAT เพื่อส่งต่อ packet เข้ามายังเครื่องภายใน

การคอนฟิกตัวอย่างด้านบน เป็นการระบุที่พอร์ตเลย เราสามารถใช้หลายๆ พอร์ตพร้อมกัน คอนฟิกจากพอร์ตนึงไปเป็นอีกพอร์ต หรือแต่ละพอร์ตส่งต่อไปยังหลาย ๆ เครื่องได้

เพิ่มคอนฟิกในไฟล์ /etc/sysconfig/iptables

สุดท้ายหลังจากทดสอบการทำ NAT แบบต่าง ๆ ตามที่ต้องการได้แล้ว ต้องนำ rule ที่ได้ เพิ่มเข้าไปในไฟล์ /etc/sysconfig/iptables ซึ่งเป็นไฟล์กำหนด rule ของ iptables ที่ถูกโหลดโดย service iptables ตอนบู๊ตเครื่อง

วิธีการเพิ่มแบบแรกคือ จากคำสั่งที่ใช้รันตัดคำว่า iptables -t nat ออกไป แล้วพิมพ์ส่วนที่เหลือต่อท้ายบรรทัดที่มีคำว่า COMMIT ของคอนฟิก table filter เช่นต้องการเพิ่มคอนฟิกทำ DNAT จากข้อ 3 สามารถทำได้โดย

```
[root@linux-nat ~]# cat /etc/sysconfig/iptables
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT
```

```
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING  -p tcp -d 192.168.200.21 --dport 80 -j DNAT --to-destination 192.168.1.2:80
-A POSTROUTING -p tcp -s 192.168.1.2 --sport 80 -j SNAT --to-source 192.168.200.12:80
COMMIT
```

อีกวิธีการหนึ่งในการบันทึก rule ที่ใช้งานอยู่ ลงในไฟล์ /etc/sysconfig/iptables คือ รันคำสั่ง service iptables save

```
[root@linux-nat ~]# iptables -t nat -L -v -n
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            192.168.200.11          tcp dpt:80
to:192.168.1.2:80
```

```
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 SNAT       tcp  --  *      *       192.168.1.2          0.0.0.0/0           tcp spt:80
to:192.168.200.11:80
```

```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
[root@linux-nat ~]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

```
[root@linux-nat ~]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.1.1 on Sun Feb  8 19:25:37 2009
*nat
```

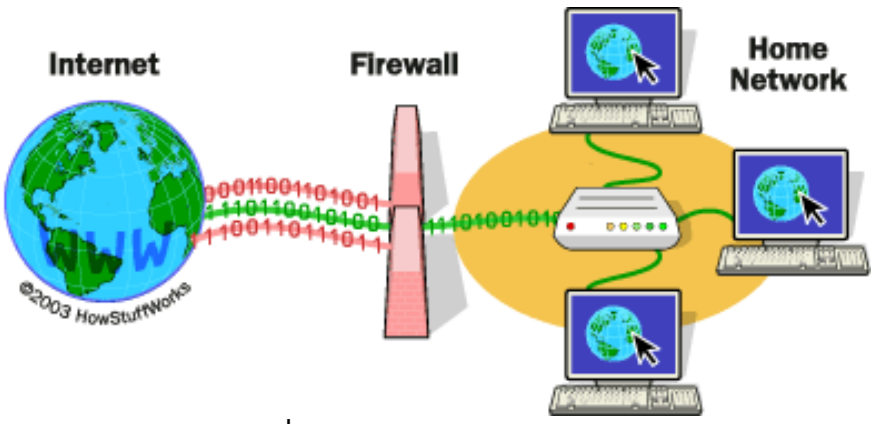
```
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -d 192.169.200.11/24 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.1.2:80
-A POSTROUTING -s 192.168.1.2/32 -p tcp -m tcp --sport 80 -j SNAT --to-source 192.168.200.11:80
COMMIT
# Completed on Sun Feb  8 19:25:37 2009
# Generated by iptables-save v1.4.1.1 on Sun Feb  8 19:25:37 2009
*filter
:INPUT ACCEPT [425:31352]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [393:41372]
COMMIT
# Completed on Sun Feb  8 19:25:37 2009
```

ทดสอบการรีโหลด IPTABLES RULES ด้วยคำสั่ง SERVICE IPTABLES

สามารถใช้คำสั่ง service iptables restart เพื่อตรวจสอบคอนฟิกไฟล์ /etc/sysconfig/iptables ถูกต้อง

```
[root@linux-nat ~]# service iptables restart
iptables: Flushing firewall rules:                 [  OK  ]
iptables: Setting chains to policy ACCEPT: nat filter  [  OK  ]
iptables: Unloading modules:                       [  OK  ]
iptables: Applying firewall rules:                 [  OK  ]
```

4. ความหมายของไฟร์วอลล์ (Firewall)



ภาพที่ 5.5 ลักษณะของ Firewall

ที่มา : https://avestatechnology.blogspot.com/2019/04/firewall.html

ไฟร์วอลล์ (Firewall) คือซอฟต์แวร์หรือฮาร์ดแวร์ ทำหน้าที่ ตรวจสอบและควบคุมระบบข้อมูลที่มาจากอินเทอร์เน็ตหรือเครือข่าย โดยคุณสามารถกำหนดว่าข้อมูลนั้น อนุญาตให้เพื่อนๆหรือพนักงานเข้าถึงข้อมูลไหนบ้าง หากเป็นผู้บุกรุกจะไม่มีสิทธิเข้าถึงข้อมูลนั้นได้ ทั้งนี้ การมี ไฟร์วอลล์ (Firewall) จะตรวจสอบผู้ใช้ก่อนเข้าถึงข้อมูล

การมี ไฟร์วอลล์ (Firewall) นี้ จะช่วยให้คอมพิวเตอร์ในเครือข่าย ได้รับการป้องกันไม่ให้แฮกเกอร์ (Hacker) หรือซอฟต์แวร์อันตราย โจมตี เข้าถึงคอมพิวเตอร์ของคุณผ่านทางเครือข่ายหรืออินเทอร์เน็ต นอกจากนี้ ไฟร์วอลล์ (Firewall) ยังช่วยป้องกันไม่ให้คอมพิวเตอร์ที่เป็นเหยื่อมัลแวร์นั้นส่งซอฟต์แวร์อันตรายไปยังคอมพิวเตอร์เครื่องอื่นอีกด้วย

ภาพที่ 5.6 ลักษณะการทำงานของ Firewall

5. ประเภทของไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ (Firewall) โดยทั่วไปจะถูกแบ่งออกเป็น 2 ประเภทคือ ไฟร์วอลล์ (Firewall) ระดับ Network (network level firewall) และไฟร์วอลล์ (Firewall) ระดับ Application (application level firewall)

ไฟร์วอลล์ (Firewall) ระดับ network จะตัดสินใจยอมให้ traffic ใดผ่านนั้นจะดูที่ address ผู้ส่งและผู้รับ และ port ในแต่ละ IP packet เมื่อพิจารณาแล้วเห็นว่า traffic สามารถผ่านไปได้ก็จะ route traffic ผ่านตัวมันไปโดยตรง router โดยทั่วไปแล้วก็จะถือว่าเป็น firewall ระดับ network ชนิดหนึ่ง firewall ประเภทนี้จะมีความเร็วสูงและจะ transparent ต่อผู้ใช้ (คือผู้ใช้มองไม่เห็นความแตกต่างระหว่างระบบที่ไม่มี firewall กับระบบที่มี firewall ระดับ network อยู่) การที่จะใช้ firewall ประเภทนี้โดยมากผู้ใช้จะต้องมี IP block (ของจริง) ของตนเอง

ไฟร์วอลล์ (Firewall) ระดับ application นั้นโดยทั่วไปก็คือ host ที่ run proxy server อยู่ firewall ประเภทนี้สามารถให้รายงานการ audit ได้อย่างละเอียดและสามารถบังคับใช้นโยบาย

ความปลอดภัยได้มากกว่า firewall ระดับ network แต่ firewall ประเภทนี้ก็จะมีความ transparent น้อยกว่า firewall ระดับ network โดยที่ผู้ใช้จะต้องตั้งเครื่องของตนให้ใช้กับ firewall ประเภทนี้ได้ นอกจากนี้ firewall ประเภทนี้จะมีความเร็วน้อยกว่า firewall ระดับ network บางแหล่งจะกล่าวถึง firewall ประเภทที่สามคือประเภท stateful inspection filtering ซึ่งใช้การพิจารณาเนื้อหาของ packets ก่อนๆในการที่จะตัดสินใจให้ packet ที่กำลังพิจารณาอยู่เข้ามา

5.1 ขีดความสามารถของไฟร์วอลล์ (Firewall)

ขีดความสามารถของ ไฟร์วอลล์ (Firewall) ทั่ว ๆ ไปนั้นมีดังต่อไปนี้

5.1.1 ป้องกันการ login ที่ไม่ได้รับอนุญาตที่มาจากภายนอกเครือข่าย

5.1.2 ปิดกั้นไม่ให้ traffic จากนอกเครือข่ายเข้ามาภายในเครือข่ายแต่ก็ยอมให้ผู้ที่อยู่ภายในเครือข่ายสามารถติดต่อกับโลกภายนอกได้

5.1.3 เป็นจุดรวมสำหรับการรักษาความปลอดภัยและการทำ audit (เปรียบเสมือนจุดรับแรงกระแทกหรือ \"choke\" ของเครือข่าย)

5.2 ข้อจำกัดของไฟร์วอลล์ (Firewall)

ข้อจำกัดของ firewall มีดังต่อไปนี้

5.2.1 ไฟร์วอลล์ (Firewall) ไม่สามารถป้องกันการโจมตีที่ไม่ได้กระทำผ่านไฟร์วอลล์ (Firewall) เช่น การโจมตีจากภายในเครือข่ายเอง

5.2.2 ไม่สามารถป้องกันการโจมตีที่เข้ามากับ application protocols ต่าง ๆ (เรียกว่าการ tunneling) หรือกับโปรแกรม client ที่มีความล่อแหลมและถูกดัดแปลงให้กระทำการโจมตีได้ (โปรแกรมที่ถูกทำให้เป็น Trojan horse)

5.2.3 ไม่สามารถป้องกันไวรัส (Virus) ได้อย่างมีประสิทธิภาพเนื่องจากจำนวน ไวรัส (Virus) มีอยู่มากมาย จึงจะเป็นการยากมากที่ไฟร์วอลล์ (Firewall) จะสามารถตรวจจับ pattern ของไวรัส (Virus) ทั้งหมดได้

6. การตั้งค่า Firewall

สิ่งที่เปลี่ยนไปอีกอย่างในเซ็นโอเอส 7 (CentOS 7) หรือ เรดแฮทเอ็นเตอร์ไพรส์ 7 (Red Hat Enterprise 7) เมื่อเทียบกับเวอร์ชันเดิม (5, 6) คือเปลี่ยนมาใช้ firewalld เพื่อช่วยให้การคอนฟิก firewall ในลีนุกซ์ทำได้ง่ายขึ้น โดยมีการจัดแบ่งเป็นโซน (zone) จัดกลุ่มพอร์ต (port) เป็นเซอร์วิส (service) และอื่นๆ

เบื้องหลัง firewalld ก็ไปเรียกคำสั่ง iptables เพื่อใช้คอนฟิก Netfilter ซึ่งเป็นโมดูลอยู่ในเคอร์เนลลีนุกซ์ ในการจัดการควบคุมแพ็กเกจ (packet filtering) เข้าออกเครื่อง

ในที่นี้ขอยกตัวอย่างการใช้คำสั่ง firewall-cmd เพื่อเพิ่มเซอร์วิสเช่น http ให้เครื่องอื่นสามารถมาเรียกใช้เซอร์วิสเว็บในเครื่องได้

firewalld จะติดตั้งมาให้โดยดีฟอลต์อยู่แล้ว และโดยคอนฟิกดีฟอลต์จะอนุญาตให้เครื่องอื่นๆ เรียกใช้เซอร์วิสที่รันอยู่ในเครื่องได้แค่ ssh เท่านั้น คือให้เครื่องอื่น ๆ สามารถรีโมดเข้ามาเครื่องเราโดยใช้คำสั่งหรือโปรแกรมประเภท ssh เท่านั้น

6.1 วิธีการคอนฟิก firewalld สามารถทำได้โดยสองแบบคือ

firewall-config เป็นโปรแกรมกราฟิกรันบน X Window จำเป็นต้องลง GNOME หรือ KDE firewall-cmd รันเป็นคำสั่งรูปแบบเท็กซ์ ซึ่งจะใช้ในบทความนี้ก่อนอื่น ลองตรวจสอบสถานะการรัน firewalld บนเครื่อง

ใช้คำสั่ง systemctl status เพื่อดูสถานะการรันของ firewalld

 # systemctl status firewalld

ใช้คำสั่ง firewall-cmd ระบุออปชัน –list-services เพื่อดูสถานะการอนุญาตให้มีการเรียกใช้เซอร์วิสของโซนที่ระบุในออปชัน –zone

 # firewall-cmd --zone=public --list-services

dhcpv6-client ssh

โดยดีฟอลต์จะอนุญาตให้ใช้เซอร์วิส ssh เข้ามาทางอินเตอร์เฟซที่อยู่ในโซน public เท่านั้น

เพิ่มให้สามารถใช้เซอร์วิส http ของเครื่องเราในโซนที่ระบุได้ ก็สามารถทำได้โดยระบุออปชัน –add-service หากต้องการกำหนดเซอร์วิสอื่น ๆ ก็สามารถทำได้โดยการระบุ ชื่อเซอร์วิส

 # firewall-cmd --zone=public --add-service=http

success

คอนฟิก firewall ที่แก้ไขไป จะอยู่ชั่วคราวเท่านั้น ถ้ามีการรีสตาร์ตเครื่องใหม่ คอนฟิกที่เพิ่ม จะหายไปต้องระบุออปชัน –permanent เพื่อให้บันทึกการคอนฟิกลงในไฟล์

 # firewall-cmd --permanent --zone=public --add-service=http

Success

สรุป

การทำเน็ตเวิร์กแอดเดรสทรานเลชั่น (Network Address Translation : NAT) เป็นวิธีการหนึ่งที่จะช่วยให้เครื่องคอมพิวเตอร์ที่ใช้ Private IP Address สามารถเชื่อมต่อเครือข่ายอินเทอร์เน็ตได้และมีความปลอดภัยในระดับหนึ่ง ถึงแม้ว่าการทำเน็ตเวิร์กแอดเดรสทรานเลชั่น (Network Address Translation : NAT) จะไม่ใช่ทางเลือกที่ดีสำหรับการรักษาความปลอดภัยให้กับระบบเครือข่ายขนาดใหญ่ แต่ก็สามารถป้องกันข้อมูลด้าน Internal Network ได้

ไฟร์วอลล์ (Firewall) คือซอฟต์แวร์หรือฮาร์ดแวร์ ทำหน้าที่ ตรวจสอบและควบคุมระบบข้อมูลที่มาจากอินเทอร์เน็ตหรือเครือข่าย โดยคุณสามารถกำหนดว่าข้อมูลนั้น อนุญาตให้เพื่อนๆหรือพนักงานเข้าถึงข้อมูลไหนบ้าง หากเป็นผู้บุกรุกจะไม่มีสิทธิเข้าถึงข้อมูลนั้นได้ ทั้งนี้ การมี ไฟร์วอลล์ (Firewall) จะตรวจสอบผู้ใช้ก่อนเข้าถึงข้อมูล การมี ไฟร์วอลล์ (Firewall) นี้ จะช่วยให้คอมพิวเตอร์ในเครือข่าย ได้รับการป้องกันไม่ให้ แฮกเกอร์ (Hacker) หรือซอฟต์แวร์อันตราย โจมตี เข้าถึงคอมพิวเตอร์ของคุณผ่านทางเครือข่ายหรืออินเทอร์เน็ต นอกจากนี้ ไฟร์วอลล์ (Firewall) ยังช่วยป้องกันไม่ให้คอมพิวเตอร์ที่เป็นเหยื่อมัลแวร์นั้น ส่งซอฟต์แวร์อันตรายไปยังคอมพิวเตอร์เครื่องอื่นอีกด้วย

แบบฝึกหัดหน่วยที่ 5

เรื่อง **การทำงานของ Network Address Translation (NAT) และไฟร์วอลล์ Firewall**

ชื่อ – นามสกุล.....ชั้น/ปีที่ .....กลุ่ม/ห้อง.....

ชื่อ - นามสกุลผู้ตรวจ.....วัน / เดือน / ปี .....

****

<u>คำสั่ง</u> จงตอบคำถามต่อไปนี้ให้ถูกต้อง

จุดประสงค์เชิงพฤติกรรม: บอกความหมาย Network Address Translation (NAT) ได้

1. จงบอกความหมาย Network Address Translation (NAT) (3 คะแนน)

.....

.....

.....

.....

.....

.....

.....

.....

.....

จุดประสงค์เชิงพฤติกรรม: บอกการทำงานของ Network Address Translation (NAT) ได้

2. จงบอกการทำงานของ Network Address Translation (NAT) (4 คะแนน)

.....

.....

.....

.....

.....

.....

.....

.....

จุดประสงค์เชิงพฤติกรรม: อธิบายการตั้งค่า Network Address Translation (NAT) ได้

3. จงอธิบายการตั้งค่า Network Address Translation (NAT) (3 คะแนน)

.....

.....

.....

.....

.....

.....

จุดประสงค์เชิงพฤติกรรม: บอกความหมาย Firewall ได้

4. จงบอกความหมาย Firewall (3 คะแนน)

.....

.....

.....

.....

.....

.....

.....

.....

จุดประสงค์เชิงพฤติกรรม: บอกการทำงานของ Firewall ได้

5. จงบอกการทำงานของ Firewall (4 คะแนน)

.....

.....

.....

.....

.....

.....

.....

.....

จุดประสงค์เชิงพฤติกรรม: อธิบายการตั้งค่า Firewall ได้

6. จงอธิบายการตั้งค่า Firewall (3 คะแนน)

.....

.....

.....

.....

.....

.....

.....

.....

<u>หมายเหตุ</u> เกณฑ์การให้คะแนน

ถูกต้องและครบถ้วน ให้ได้คะแนน *เต็ม*

ถูกต้องแต่*<u>ไม่</u>*ครบถ้วน ให้ได้คะแนน *ครึ่งหนึ่งของคะแนนเต็ม*

*<u>ไม่</u>*ถูกต้อง ให้ได้คะแนน *ศูนย์*

แบบทดสอบก่อนเรียน/หลังเรียน หน่วยที่ 5

เรื่อง **การทำงานของ Network Address Translation (NAT) และไฟร์วอลล์ Firewall**

ชื่อ – นามสกุล.....ชั้น/ปีที่ .....กลุ่ม/ห้อง.....

ชื่อ - นามสกุลผู้ตรวจ.....วัน / เดือน / ปี .....

****

คำสั่ง ทำเครื่องหมายวงกลมล้อมรอบข้อคำตอบที่ถูกที่สุดเพียงข้อเดียว

1. ข้อใดคือความหมายของเน็ตเวิร์กแอดเดรสทรานเลชั่น (Network Address Translation : NAT)
   ก. เป็นจุดต่อเชื่อมของเครือข่ายทำหน้าที่เป็นทางเข้าสู่ระบบเครือข่ายต่าง ๆ บนอินเตอร์เน็ต
   ข. เป็นจุดต่อเชื่อมอินเตอร์เน็ต
   ค. เป็นอุปกรณ์ฮาร์ดแวร์ที่เชื่อมต่อเครือข่าย
   ง. เป็นการแปลงไปรเวทไอพีให้เป็นไอพีที่สามารถใช้งานบนระบบอินเตอร์เน็ตได้
   จ. เป็นการกำหนดหมายเลขไอพีแอดเดรสให้กับเครื่องลูกข่าย
2. รูปแบบในการเปลี่ยนแปลงค่าไอพีแอดเดรส (IP Address) มีอยู่กี่แบบ
   ก. 1 แบบ ข. 2 แบบ
   ค. 3 แบบ ง. 4 แบบ
   จ. 5 แบบ
3. ข้อใดคือความหมายของ Firewall
   ก. ฮาร์ดแวร์ ทำหน้าที่ ตรวจสอบและควบคุมระบบข้อมูลที่มาจากอินเทอร์เน็ต
   ข. ซอฟต์แวร์ ทำหน้าที่ ตรวจสอบและควบคุมระบบข้อมูลที่มาจากอินเทอร์เน็ต
   ค. ป้องกันการบุกรุก
   ง. ช่วยให้คอมพิวเตอร์ในเครือข่าย ได้รับการป้องกันไม่ให้แฮกเกอร์ (Hacker) หรือซอฟต์แวร์อันตราย โจมตี เข้าถึงคอมพิวเตอร์ของคุณผ่านทางเครือข่าย
   จ. ถูกทุกข้อ
4. Firewall โดยทั่วไปจะถูกแบ่งออกเป็นกี่ประเภท
   ก. 1 ประเภท
   ข. 2 ประเภท
   ค. 3 ประเภท
   ง. 4 ประเภท
   จ. 5 ประเภท
5. ข้อใดคือใช้คำสั่งเพื่อดูสถานะการรันของ firewalld
   ก. *firewall-cmd --permanent --zone=public --add-service=http*
   ข. *firewall-cmd --zone=public --list-services*
   ค. *firewall-cmd --zone=public --add-service=http*
   ง. *systemctl status firewall*
   จ. *systemctl status firewalld*

เอกสารอ้างอิง หน่วยที่ 5

การตั้งค่า NAT(Network Address Translation) บน Cisco IOS [ออนไลน์]. เข้าถึงได้จาก http://running-config.blogspot.com/2010/11/natnetwork-address-translation-cisco.html (วันที่สืบค้น 1 มีนาคม 2561)

firewall สำคัญอย่างไร [ออนไลน์]. เข้าถึงได้จาก https://avestatechnology.blogspot.com/2019/04/firewall.html (วันที่สืบค้น 1 มีนาคม 2561)

NAT : Network Address Translation [ออนไลน์]. เข้าถึงได้จาก http://thaicourt.blogspot.com/2012/03/nat-network-address-translation.html (วันที่สืบค้น 1 มีนาคม 2561)

Network Address Translation (NAT) [ออนไลน์]. เข้าถึงได้จาก https://www.gotoknow.org/posts/481846 (วันที่สืบค้น 1 มีนาคม 2561)