030523114 Network Security

สาขาวิชาเทคโนโลยีอิเล็กทรอนิกส์ (ต่อเนื่อง)

ภาควิชาเทคโนโลยีวิศวกรรมอิเล็กทรอนิกส์

วิทยาลัยเทคโนโลยีอุตสาหกรรม

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

อาจารย์ ดร.เลอสรรค์ กิรสมุทรานนท์

ครั้งที่ 8 “IDS/IPS”

IDS/IPS

- **Outline**
  - Intro IDS/IPS
  - IDS/IPS
  - Honey Pot
  - ความสำคัญที่ต้องมี IDS
  - ความสามารถและข้อจำกัดของ IDS
  - ประเภทของ IDS/IPS
  - การแจ้งเตือนภัยของ IDS
  - การติดตั้ง IDS (Network-Based)

Intro IDS/IPS

- เครือข่ายอินเตอร์เน็ตในปัจจุบันนี้มีการเติบโตอย่างรวดเร็ว อันตรายนั้นก็ยิ่งเพิ่มมากขึ้นไม่ยิ่งหย่อนไปกว่ากัน ไฟร์วอล และ IDS(Intrusion Detection System) จึงเป็นสิ่งจำเป็นในการป้องกันอันตรายเหล่านั้นที่จะมีต่อระบบเครือข่ายภายในองค์กร
- IDS หรือระบบตรวจจับการบุกรุกนั้น เป็นเครื่องมือสำหรับการรักษาความปลอดภัยอีกประเภทหนึ่งที่ใช้สำหรับตรวจตรวจจับความพยายามที่จะบุกรุกเครือข่าย

IDS/IPS

- IDS ระบบตรวจจับการบุกรุก (Intrusion Detection System)
  - เปรียบ ระบบเหมือนบ้าน แล้ว IDS เหมือนยามรักษาการณ์
  - วิเคราะห์ข้อมูลที่ผ่านเข้าออก โดยดูจากลักษณะของข้อมูลเหล่านั้น
  - แค่แจ้งเตือนการบุกรุก แต่ไม่สามารถป้องกันการบุกรุกได้
  - มีการทำงานประสานกับส่วนอื่น เช่น Firewall, Antivirus บางตัว
  - มีการแบ่งการทำงานระบบย่อย เช่น ตรวจสอบฐานข้อมูล

Note.

IDS/IPS

เนื่องจาก IDS ไม่ใช่ระบบป้องกันการบุกรุก โดยเฉพาะอย่างยิ่งการโจมตีแบบเรียบไทม์ เช่น การโจมตีแบบ Dos (Denial of Service) หรือ DDos (Distributed Denail of Service) จากปัญหาดังกล่าว จึงมีการคิดค้นเทคโนโลยีใหม่ขึ้นมา โดยเรียกว่า IPS (Instrusion PreventionSystem) ซึ่งสามารถตรวจจับการบุกรุกและป้องกันได้อย่างทันท่วงที

Note.

IDS/IPS

- IPS หยุดการบุกรุก โดยการ

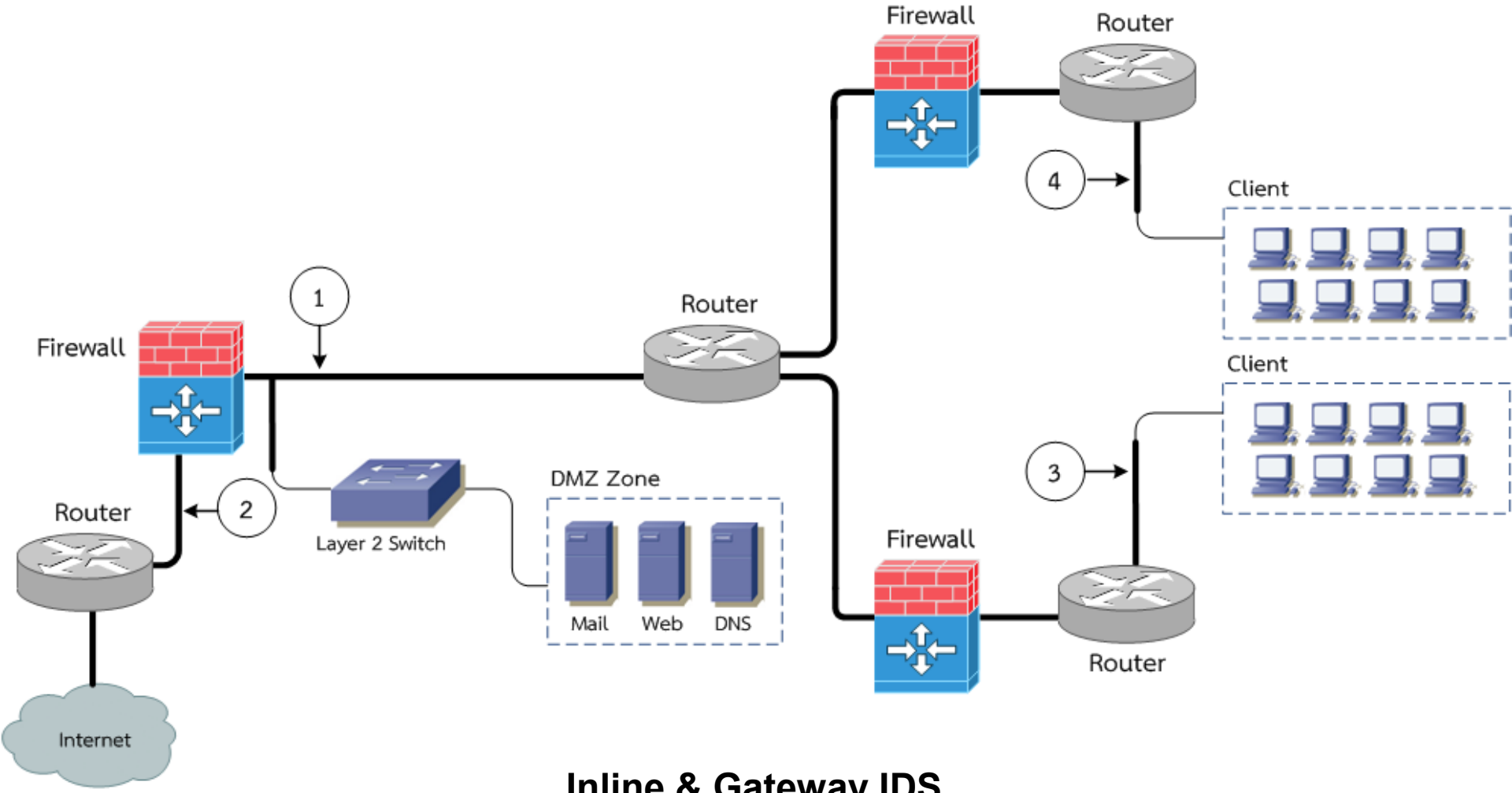
  - ส่งสัญญาณ TCP Reset เพื่อจัดกับกับเซสชั่น ที่คาดว่าจะเป็นการบุกรุก

  - แก้ไข Policy ใน Firewall แบบอัติโนมัติ ซึ่งบางครั้งอาจจะบล๊อคการใช้งานปกติของผู้ใช้ได้

  ใช้เทคโนโลยีขั้นสูงในการวิเคราะห์ข้อมูล เช่น Neural Network และ Fuzzy Logic เพื่อลดข้อผิดพลาด

Note.

IDS/IPS



Inline & Gateway IDS

IDS/IPS

หลักการทำงานของ IPS จะใช้หลักการที่เรียกว่า Inline หรือที่เรียกว่า Gateway IDS ซึ่งก็คือ

- การนำ IPS ไปกั้นกลางบนเส้นทางการส่งข้อมูล โดยไม่ต้องมีการกำหนดหมายเลขไอพีให้กับ IPS ปัญหาก็คือ หากตัว IPS เกิดเสียถ้า IPS ไม่สามารถบายพาสได้ด้วยตัวเอง ก็จะทำให้เกิดปัญหาในการรับส่งข้อมูลระหว่างต้นทางกับปลายทาง
- ถ้า IPS ตัดสินใจผิด การบล็อคแพ็กเก็ตที่ IPS คิดว่าเป็นการบุกรุกแต่จริง ๆ เป็นการใช้งานธรรมดาก็จะเกิดปัญหาอีกเช่นกัน

ความสำคัญที่ต้องมี IDS

- เพื่อเป็นเครื่องมือสำหรับการสืบสวนหาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด
- เพื่อตรวจจับความพยายามที่จะบุกรุกเครือข่ายและป้องกันก่อนที่จะเกิดการโจมตีจริง ๆ
- เพื่อเก็บสถิติเกี่ยวกับความพยายามที่บุกรุกหรือโจมตี และนำข้อมูลไปวิเคราะห์ภัยคุกคามที่อาจจะเกิดขึ้นกับองค์กรได้
- เพื่อเป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบการรักษาความปลอดภัยอื่นเช่นไฟร์วอล เป็นต้น

ความสามารถและข้อจำกัดของ IDS

- ความสามารถ
  - มอนิเตอร์และวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบและพฤติกรรมของผู้ใช้
  - ทดสอบระดับความปลอดภัยของระบบ
  - บอกถึงระดับมาตรฐานความปลอดภัยของระบบ
  - เรียนรู้ลำดับเหตุการณ์ของระบบที่เกิดจากการโจมตีที่รู้ล่วงหน้า
  - เรียนรู้ลำดับเหตุการณ์ของระบบที่แตกต่างจากเหตุการณ์ปกติ

ความสามารถและข้อจำกัดของ IDS

- ข้อจำกัด
  - ไม่สามารถปิดช่องโหว่หรือจุดอ่อนของระบบได้
  - ไม่สามารถตรวจจับ รายงาน และตอบโต้การโจมตีได้ในช่วงเวลาที่มีการใช้เครือข่ายอย่างหนาแน่น
  - ไม่สามารถตรวจจับการโจมตีแบบใหม่ได้ (Signature ไม่อัพเดต)
  - ไม่สามารถสืบหาผู้บุกรุกได้โดยอัตโนมัติ การสืบหานั้นต้องอาศัยคนช่วย
  - ไม่สามารถขัดขวางไม่ให้โจมตีตัวเองได้

ประเภทของ IDS

- Host-based IDS คือ ตรวจจับการโจมตีเฉพาะ**แต่ละเครื่อง**
- Network-based IDS คือ ตรวจจับการโจมตี**หลายเครื่อง**

Host-based IDS

- **ข้อดี**
  - ไม่ต้องทำงานหนักมาก เนื่องจากมีหน้าที่ตรวจจับเฉพาะโฮสต์ที่ติดตั้งซอฟต์แวร์ IDS ทำให้ตรวจจับได้ทุกรายละเอียด
  - ใช้งานง่าย มีให้เลือกใช้หลายตัว มีราคาถูก
- **ข้อเสีย**
  - เพิ่มภาระของผู้ดูแลระบบ เนื่องจากต้องติดตั้ง ดูแล ตรวจสอบ Log file ของ IDS แต่ละเครื่อง
  - การทำงานของ IDS อาจมีผลกระทบต่อประสิทธิภาพของโฮสตเนื่องจากโปรเซสของ IDS จะกินหน่วยความจำ และ CPU

Network-based IDS

- ข้อดี
  - โปรเซสของ IDS จะไม่กินหน่วยความจำ และ CPU
  - ไม่ต้องติดตั้ง ดูแล ตรวจสอบ Log file ของ IDS
- ข้อเสีย
  - IDS ต้องทำงานหนักมาก เพราะต้องตรวจจับหลายๆ โฮสต์พร้อมกันทำให้ไม่สามารถตรวจจับได้ทุกรายละเอียด
  - ติดตั้งยากกว่า Host-Based IDS
  - อุปกรณ์มีราคาแพง

ประเภทของ IPS

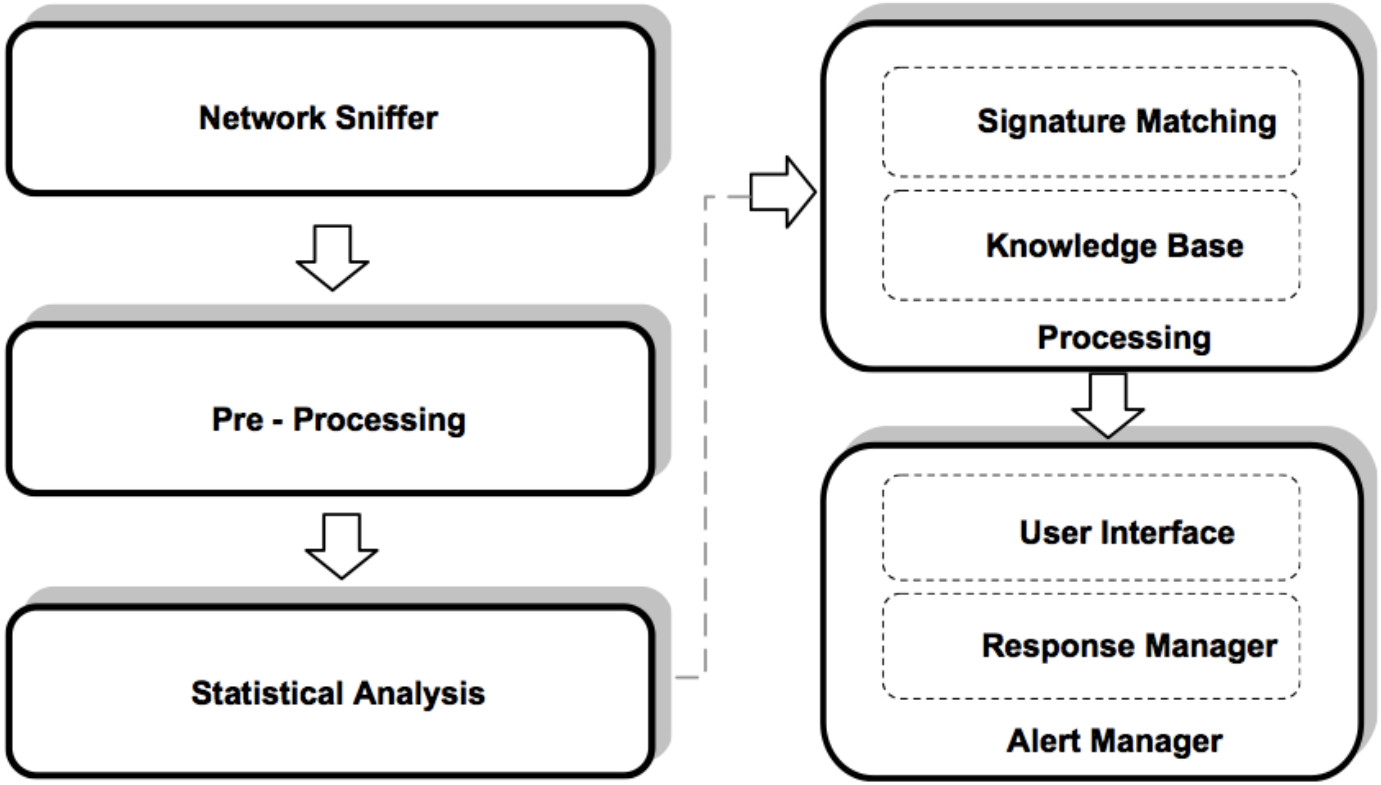
สามารถแบ่งได้ 2 ประเภทคือ

1. Network Based Intrusion Prevention System (NIPS)

IPS ที่ได้รับการติดตั้งไว้ที่ส่วนหนึ่งของระบบเครือข่ายเพื่อป้องกันการบุกรุก

2. Host Based Intrusion Prevention System (HIPS) ติดตั้งเข้าไปที่เครื่อง Client เพื่อป้องกันการบุกรุกหรือการโจมตีต่าง ๆ

องค์ประกอบของ IDS



- Host System/Network Sniffer : ทำหน้าที่เป็นตัวตรวจจับเหตุการณ์ต่าง ๆ ที่เกิดขึ้นใน Host หรือเครือข่าย

องค์ประกอบของ IDS

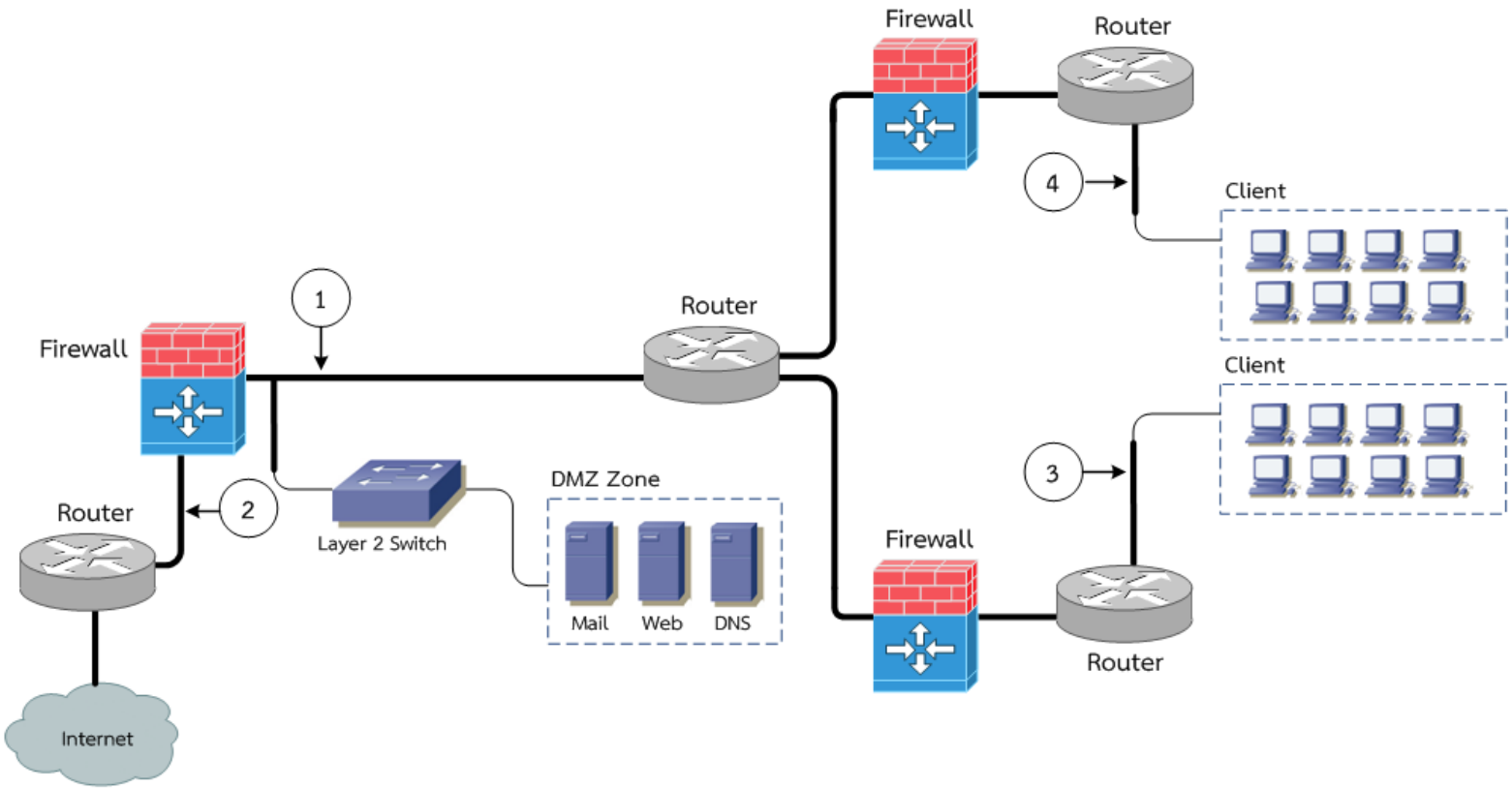
- Pre - Processing : จัดรูปแบบของ เพื่อให้นำไปประมวลผลได้สะดวกต่อไป
- Statistical Analysis : ส่วนวิเคราะห์ผลทางสถิติ
- Signature Matching : เปรียบเทียบกับ Signature ที่มีอยู่
- Knowledge Base : เป็นตัวเก็บข้อมูลเกี่ยวกับพฤติกรรมของการบุกรุก
- Alert Manager : ทำหน้าที่เป็นตัวตัดสินใจว่าจะต้องเตือนหรือไม่
- User Interface : เป็นส่วนที่โต้ตอบกับผู้ใช้ อาจจะเป็นการแสดงผลที่หน้าจอ
- Response Manager : รับข้อมูลจาก Alert Manager เพื่อนำมาตัดสินใจว่าจะโต้ตอบสนองการบุกรุกอย่างไร

การแจ้งเตือนภัยของ IDS

- วันเวลา
- ชื่อของการโจมตี
- หมายเลขไอพีต้นทางและปลายทาง
- หมายเลขพอร์ตของต้นทางและปลายทาง
- ชื่อโปรโตคอลที่ใช้สำหรับการโจมตี

Note.

การติดตั้ง IDS (Network-Based)



การติดตั้ง IDS (Network-Based)

- *ข้อดีของการติดตั้ง IDS หลังไฟร์วอล (Location 1)*
  - สามารถตรวจจับการบุกรุกจากภายนอกที่สามารถเจาะผ่านไฟร์วอลได้
  - ตรวจสอบความถูกต้องในการคอนฟิกไฟร์วอล
  - สามารถตรวจจับการโจมตีเซิร์ฟเวอร์ที่อยู่ใน DMZ

- *ข้อดีของการติดตั้ง IDS หน้าไฟร์วอล (Location 2)*
  - เก็บสถิติเกี่ยวกับ**จำนวนครั้ง**การโจมตีที่มาจากภายนอก
  - เก็บสถิติเกี่ยวกับ**ประเภท**การโจมตีที่มาจากภายนอก

การติดตั้ง IDS (Network-Based)

- *ข้อดีของการติดตั้ง IDS บนแบ็คโบนหลักของเครือข่าย (Location 3)*
  - มอนิเตอร์ทราฟฟิกหลักที่ไหลเวียนภายในเครือข่าย
  - ตรวจจับกิจกรรมที่ไม่ได้รับอนุญาตของผู้ใช้ทั่วไปอยู่ในเครือข่าย

- ข้อดีของการติดตั้ง IDS บนซับเน็ตที่มีความเสี่ยงสูง (Location 4)
  - ตรวจจับการโจมตีที่มีเป้าหมายเป็นระบบหรือรีซอร์สที่สำคัญ
  - เป็นการลดจำนวน IDS ที่ต้องใช้ และเป็นการมอนิเตอร์เฉพาะที่จุดสำคัญ

Reference

- อาจารย์ ธนัญชัย ตรีภาค สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and SourceCode in C, John Wiley & Sons Inc, December 1995
- Security Focus
- www.securityfocus.com