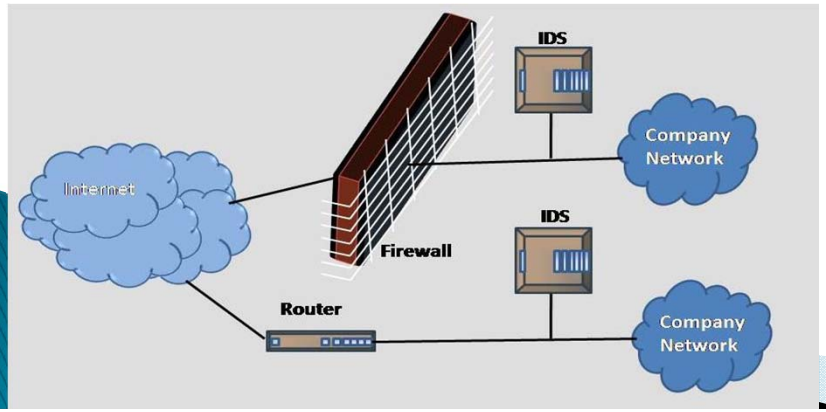
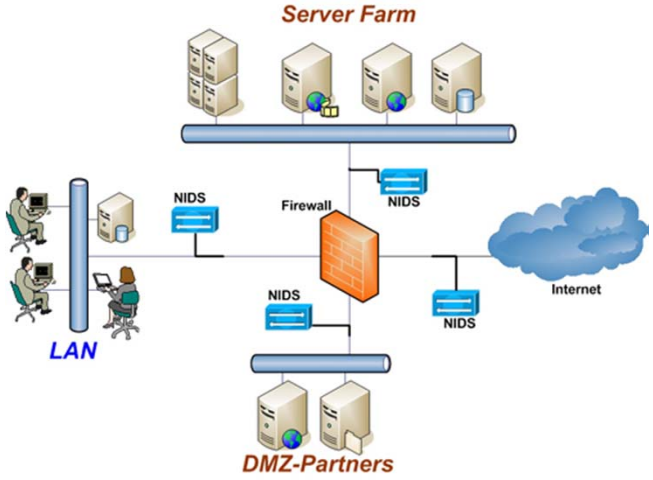
# Intrusion Detection System : IDS

MS1 Thanin Muangpool

# What is a IDS ?

**Intrusion Detection System : IDS** หมายถึง Hardware or Software ที่ติดตามตรวจสอบสัญญาณจราจร (Traffic) ที่ส่งผ่านบนเครือข่ายคอมพิวเตอร์ด้วยการ วิเคราะห์รูปแบบพฤติกรรมในแพ็กเก็ตข้อมูล (Packet Data) เพื่อค้นหาสิ่งที่ผิดปกติ (Anomaly) แล้วนำเข้าสู่กระบวนการทำนาย (Prediction) เพื่อตัดสินว่าเป็นเหตุการณ์บุกรุกจริงแล้วแจ้งเตือน (Alert) ให้ผู้รับผิดชอบระบบทราบเพื่อดำเนินการป้องกันและแก้ไขต่อไป



# Intrusion

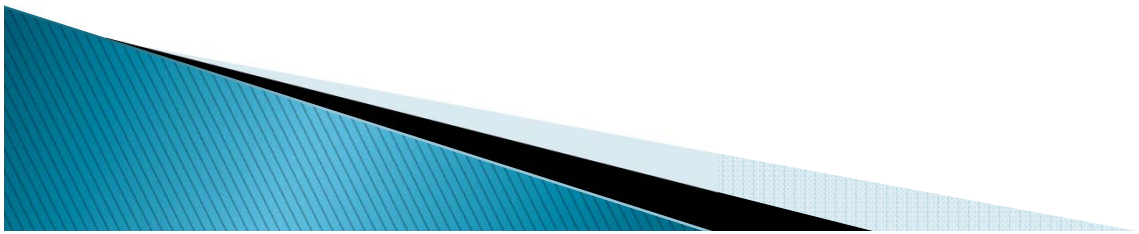
เป็น Attack ที่ทำให้ระบบทำงานผิดปกติและเป็นอันตราย ในแผนรับมือเหตุการณ์ไม่คาดคิด (Incident Response Plan) ขององค์กร มีส่วนหนึ่งที่ระบุกิจกรรมที่อาจเกิดขึ้น 4 กิจกรรม ได้แก่

**1. Intrusion Protection** เป็นการค้นหาช่องโหว่ แล้วติดตั้งกลไกป้องกัน

**2. Intrusion Detection** สร้างขั้นตอนการทำงานและระบบตรวจจับแล้วแจ้งเตือน

**3. Intrusion Reaction** เป็นการประเมินความเสียหายและฟื้นฟูการทำงานของระบบ

**4. Intrusion Correction** เป็นการแก้ไขระบบ เพื่อไม่ให้มีการโจมตีแบบเดิมอีก



# ความสำคัญของ IDS

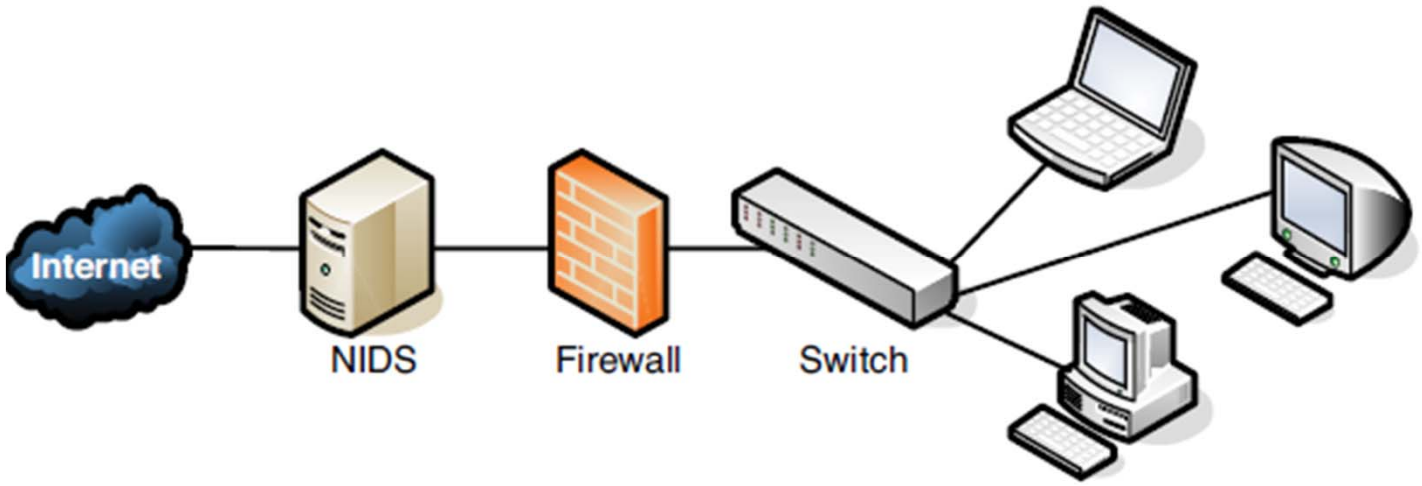
สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology : NIST) ได้ระบุสาเหตุไว้ 6 ประการ คือ

1. เพื่อป้องกันปัญหาที่จะเกิดขึ้น
2. เพื่อตรวจจับการโจมตี
3. เพื่อตรวจจับและตอบสนองเมื่อเกิดการโจมตี
4. เพื่อจัดทำเอกสารภัยคุกคามที่เกิดขึ้น
5. เพื่อใช้ควบคุมคุณภาพของ Admin
6. เพื่อเป็นการจัดเตรียมสารสนเทศเกี่ยวกับการบุกรุกไว้วิเคราะห์ฟื้นฟู และแก้ไขระบบตามปัจจัยที่เป็นสาเหตุ

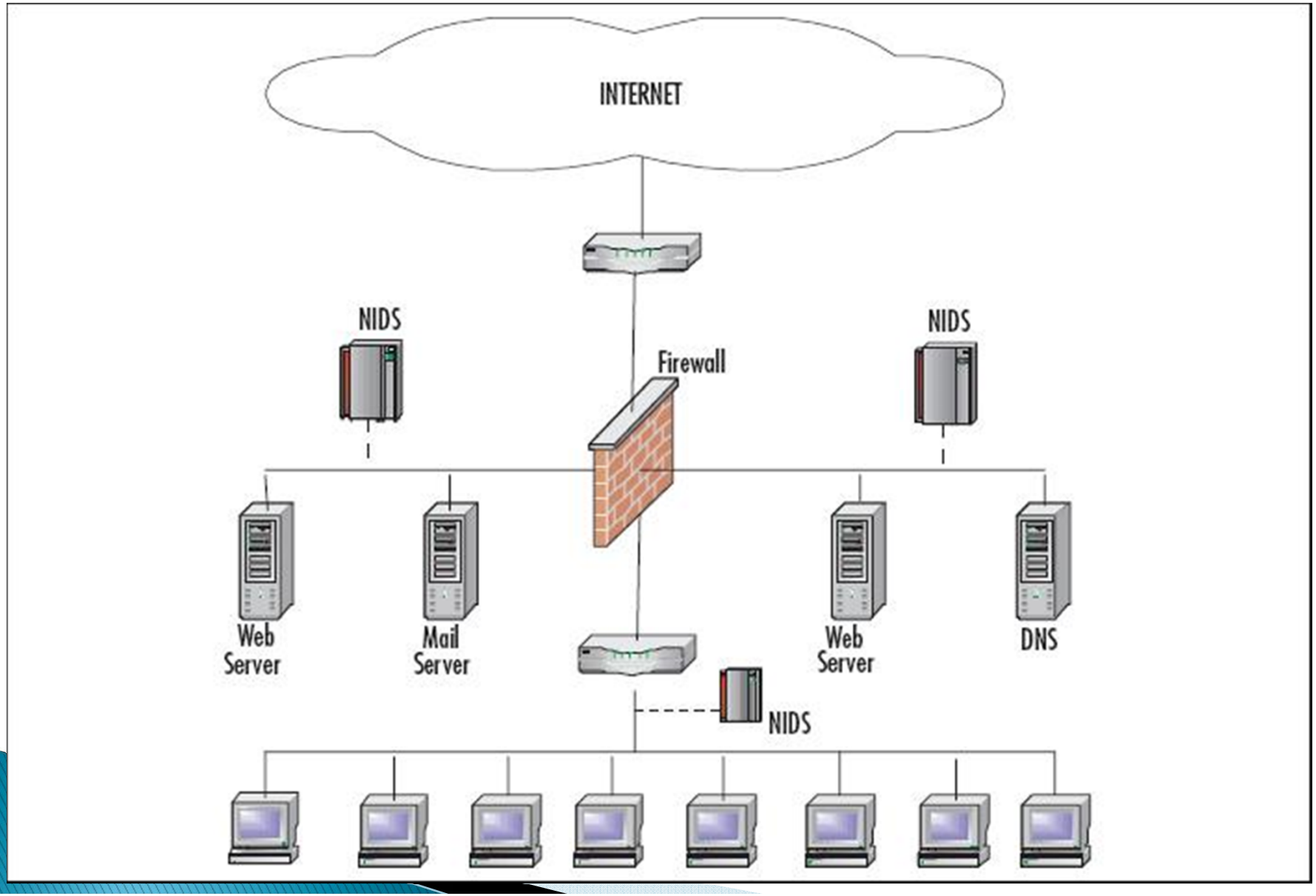
# IDS Architecture

The architectural structure of the IDS has two forms.

**1. Network-based IDS : NIDS** จะทำงานในเครือข่ายคอมพิวเตอร์ ด้วยการติดตามตรวจสอบสัญญาณจราจร (Traffic) ที่อยู่ในรูปของ Packet Data เพื่อตรวจสอบว่า Packet ใดมีลักษณะที่ผิดปกติ



# IDS Architecture → Network-based IDS : NIDS



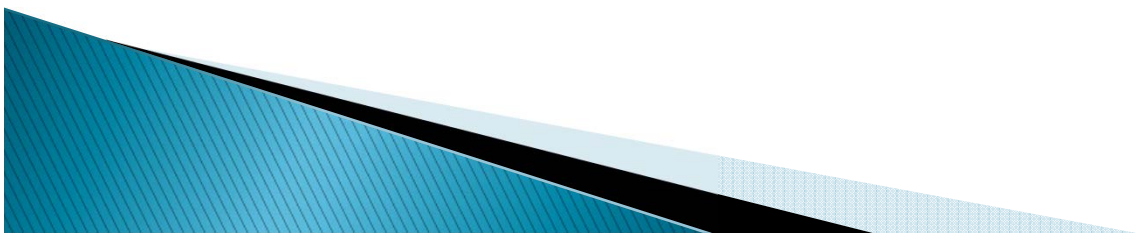
# IDS Architecture → Network-based IDS : NIDS

**ข้อดีของ NIDS**

1. องค์กรขนาดใหญ่จะใช้อุปกรณ์จำนวนน้อย
2. ติดตั้งได้ง่าย ไม่รบกวนการทำงานของระบบเดิม
3. ไม่เป็นที่สังเกตของผู้โจมตี

**ข้อเสียของ NIDS**

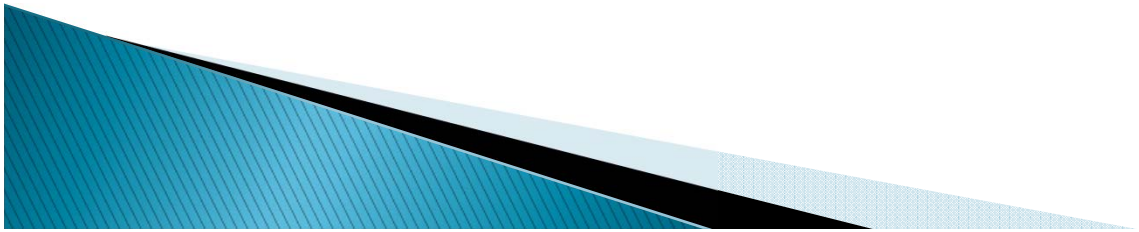
1. ไม่สามารถวิเคราะห์ Packet Data ที่เข้ารหัสได้
2. ไม่สามารถตรวจจับการโจมตีที่มากับ Fragmented Packet



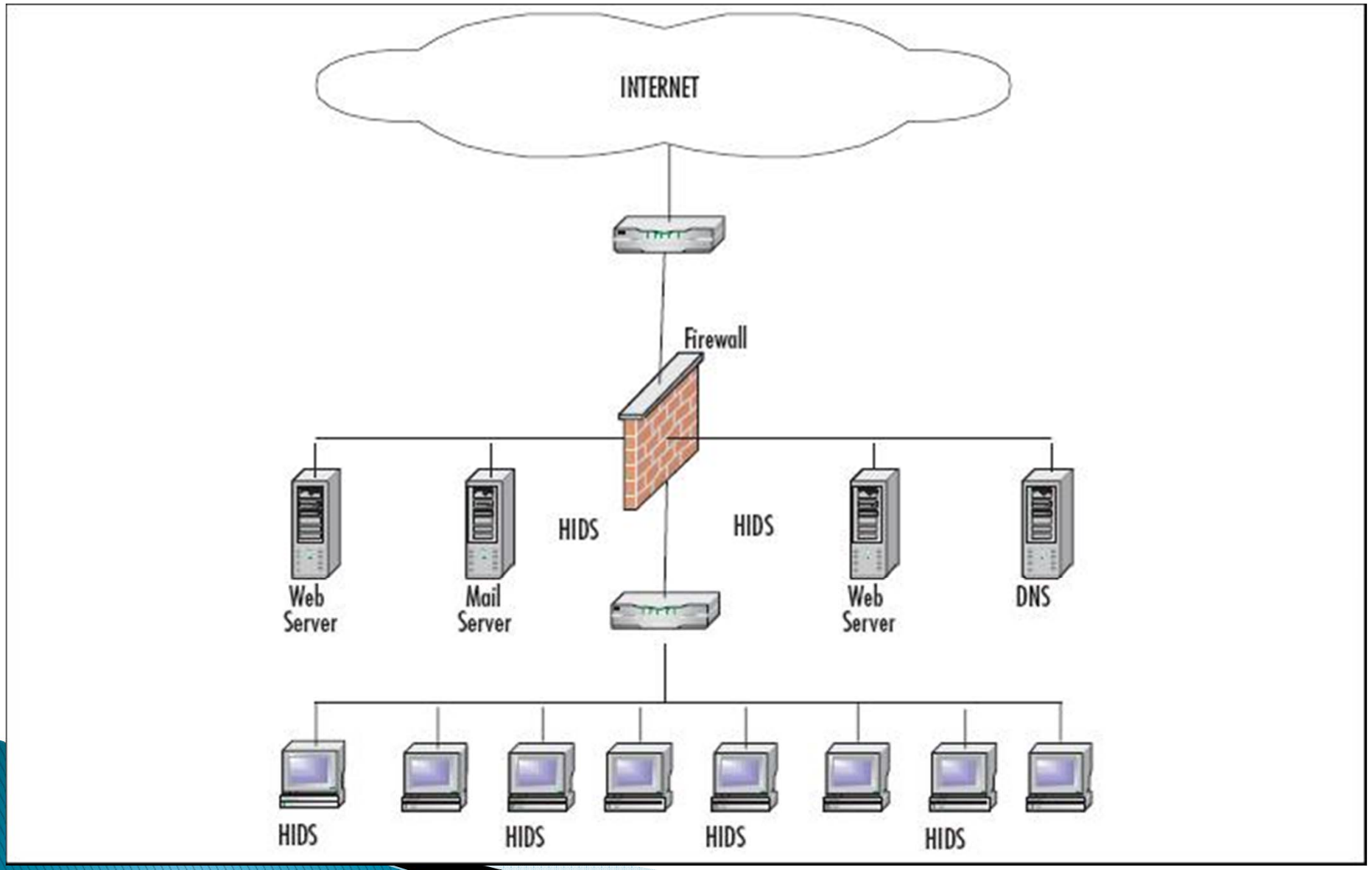
# IDS Architecture

The architectural structure of the IDS has two forms.

**2. Host-based IDS : HIDS** จะทำงานในเครื่องคอมพิวเตอร์ ด้วยการติดตามตรวจสอบสัญญาณจราจร (Traffic) ที่อยู่ในรูปของ Packet Data และตรวจสอบการใช้งานโปรแกรมประยุกต์ (Application) ในเครื่องคอมพิวเตอร์จากไฟล์ บันทึกข้อมูลการใช้ (Log File) เพื่อตรวจสอบว่า Packet ใดมีลักษณะที่ผิดปกติ



# IDS Architecture → Host-based IDS : HIDS



# IDS Architecture → Host-based IDS : HIDS

**ข้อดีของ HIDS**

1. ตรวจสอบเหตุการณ์ที่เกิดขึ้นกับเครื่อง Host และเครือข่ายได้
2. ตรวจสอบข้อมูลที่เข้ารหัสได้
3. ตรวจสอบการใช้งานได้จาก Audit Log File

**ข้อเสียของ HIDS**

1. ต้องติดตั้งทุก Host
2. ไม่สามารถ Scan Port ที่อุปกรณ์เครือข่ายอื่นๆ ได้
3. ถูกตรวจจับได้ง่ายจากการโจมตีแบบ DoS
4. ต้องใช้พื้นที่ของ Hard disk มากเพื่อใช้เก็บ Audit Log File

# หลักการทำงานของระบบตรวจหาการบุกรุก

**1. การตรวจหาการใช้งานที่ผิด (Misuse Detection) หรือ (Signature-based)** เป็นการตรวจหารูปแบบการบุกรุกด้วยการวิเคราะห์พฤติกรรมหรือเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย โดยการเปรียบเทียบพฤติกรรมหรือเหตุการณ์ที่เข้ามาในเครือข่าย ณ เวลาขณะนั้นกับพฤติกรรม หรือเหตุการณ์ที่เป็นการบุกรุกซึ่งจัดเก็บไว้ในฐานข้อมูลระบบ หากเปรียบเทียบแล้วตรงกันแสดงว่าพฤติกรรมหรือเหตุการณ์นั้นเป็นการบุกรุกระบบก็จะแจ้งเตือนให้ผู้รับผิดชอบระบบทราบ มี 2 ชนิดคือ

- Pattern Matching เป็นการเปรียบเทียบ Packet ของ Signature
- Stateful Matching เป็นการเปรียบเทียบรูปแบบของกิจกรรมทั่วไป

# หลักการทำงานของระบบตรวจหาการบุกรุก

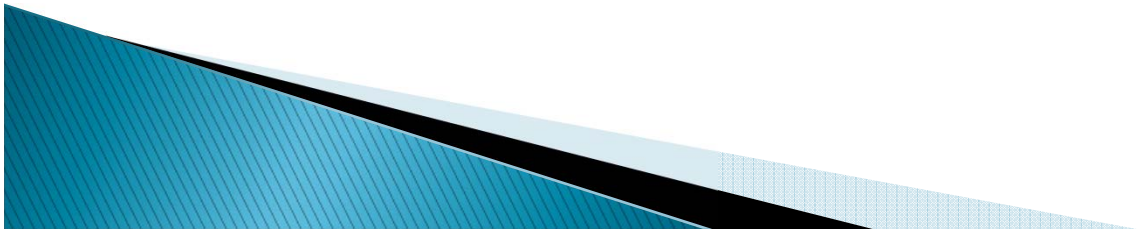
**2. การตรวจหาเหตุการณ์ผิดปกติ (Anomaly-based Detection)** เป็นการตรวจหารูปแบบการบุกรุกด้วยการวิเคราะห์พฤติกรรมหรือเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย โดยการเปรียบเทียบพฤติกรรมหรือเหตุการณ์ที่เข้ามาในเครือข่าย ณ เวลาขณะนั้นกับพฤติกรรมหรือเหตุการณ์ที่ปกติซึ่งจัดเก็บไว้ในฐานข้อมูลระบบ หากเปรียบเทียบแล้วไม่ตรงกันแสดงว่าพฤติกรรมหรือเหตุการณ์นั้นเป็นการบุกรุกระบบก็จะแจ้งเตือนให้ผู้รับผิดชอบระบบทราบ ตัวอย่างวิธีการทางานของระบบตรวจหาเหตุการณ์ผิดปกติที่นิยมในปัจจุบัน

# หลักการทำงานของระบบตรวจหาการบุกรุก

**2.1 ด้วยสถิติ (Statistical Anomaly-Based)** เป็นวิธีการวัดการกระจาย (Distribution) คุณสมบัติของ Profile ที่ใช้วิธีการทางสถิติรวบรวมแล้วสุ่มเหตุการณ์มาเปรียบเทียบกับค่ามาตรฐานที่กำหนดขึ้นเองหรือเปรียบเทียบกับค่าที่วัดได้จากในอดีต หากเบี่ยงเบนไปจากค่ามาตรฐานที่กำหนดไว้ถือว่าผิดปกติ

**2.2 ด้วยโพรโตคอล (Protocol Anomaly-Based)** เป็นการระบุโพรโตคอลที่ใช้นอกเหนือจากขอบเขตพื้นฐาน

**2.3 ด้วยสัญญาณจราจร(Traffic Anomaly-Based)** เป็นการระบุกิจกรรมที่ผิดปกติของจราจรในเครือข่าย



# หลักการทำงานของระบบตรวจหาการบุกรุก

**3. การวัดตามกฎ (Rule-based Measure)** เป็นวิธีการวัดโดยกำหนดพฤติกรรมหรือเหตุการณ์ปกติเป็นกฎไว้แล้วนำพฤติกรรมหรือเหตุการณ์ที่เกิดขึ้นในเครือข่าย ณ เวลาในขณะนั้นมาเปรียบเทียบกับกฎ หากไม่ตรงกันแสดงว่าเป็นรูปแบบการโจมตี เช่น ใช้กฎพื้นฐาน IF/THEN ของการเขียนโปรแกรมในระบบผู้เชี่ยวชาญ (Expert System) ใช้การอนุญาตของระบบผู้เชี่ยวชาญสำหรับคุณลักษณะของปัญญาประดิษฐ์ (Artificial Intelligence)

# การตอบสนองของการตรวจจับการบุกรุก

- Audible/ Visual Alarm ตอบสนองที่เป็นเสียง หรือข้อความ
- SNMP Trap โดยผ่าน SNMP Console
- Email Message เหมาะสำหรับ Smart Phone
- Mobile Notification ส่ง Message ไปที่ Mobile or Pager
- Log Entry ตรวจสอบจากของเหตุการณ์จาก Log File
- Trap & Trace , Back-Hacking เป็นการแกะรอยย้อนกลับเมื่อตรวจพบ
- Exit Program ออกจากโปรแกรม หรือสั่งให้เปิดโปรแกรมเพื่อแกะรอย
- Firewall Configuration ส่งคำสั่งไปตั้งค่าใน Firewall
- Stop Session หยุดการทำงานของ Session ที่การโจมตีนั้นใช้
- Disconnect Switch, Port ส่งคำสั่งไปตัดการเชื่อมต่อ Port นั้น

# การเลือกระบบการตรวจจับการบุกรุกมาใช้งาน

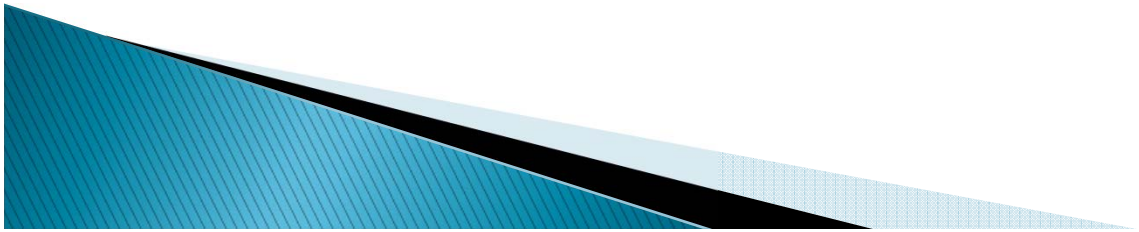
ควรพิจารณาเงื่อนไขและความต้องการด้านต่างๆ ดังนี้

- ด้านเทคนิคและนโยบาย เช่น
  - เทคนิคของระบบมีอะไรบ้าง
  - เทคนิคของการป้องกันความมั่นคงปลอดภัยมีอะไรบ้าง
  - เป้าหมายขององค์คืออะไร
  - ต้องการเอกสารที่เป็นทางการจากระบบหรือไม่
  - วัตถุประสงค์หรือเป้าหมายที่นำเอาระบบ IDS มาใช้คืออะไร
  - นโยบายของระบบความมั่นคงปลอดภัยที่มีอยู่แล้วคืออะไร
- ด้านความต้องการขององค์กรและข้อจำกัด
- ด้านคุณภาพและการทำงานของระบบ IDS

# ข้อดี-ข้อเสียของระบบการตรวจจับการบุกรุก

**ข้อดี**

- ติดตามและวิเคราะห์เหตุการณ์และพฤติกรรมของ User and Network
- ทดสอบสถานะ Security Computer System and Network
- จัดทำสถานะมาตรฐานของ Computer System and Network
- จำรูปแบบของเหตุการณ์ของการโจมตีได้
- จำรูปแบบของกิจกรรมที่ทำให้การทำงานเบี่ยงเบนไปได้
- สร้าง Log File and Audit Trail พร้อมจัดการ File เหล่านี้ได้
- แจ้งเตือน Admin ทันทีที่ตรวจพบการบุกรุก



# ข้อดี-ข้อเสียของระบบการตรวจจับการบุกรุก

**ข้อเสีย**

- ถ้ามีภาระงานมากจะไม่สามารตรวจจับการบุกรุก รายงาน และแจ้งเตือนได้ทันทีเมื่อตรวจพบการบุกรุก
- ไม่สามารถตรวจจับการโจมตีชนิดใหม่ ๆ ได้ทันที จนกว่าจะมีการ Update Signature ก่อน
- ไม่สามารถตอบสนองการโจมตีของผู้โจมตีที่มีความชำนาญได้
- ต้องให้ Admin ตั้งค่าการตรวจสอบการโจมตีอัตโนมัติ
- ไม่สามารถต่อต้านการโจมตีที่พยามทำให้ระบบคอมพิวเตอร์และเครือข่ายทำงานล้มเหลว

# การควบคุม IDS

**1. Centralized IDS Control** เป็นรูปการควบคุมที่จัดให้ทุกฟังก์ชันงานควบคุมและงานจัดการระบบจะอยู่ที่ IDS Console ซึ่งมีหน้าที่

- ควบคุมการทำงานทั้งหมดของระบบ IDS ทำหน้าที่รวบรวมข้อมูลจาก Sensor ที่จุดต่าง ๆ

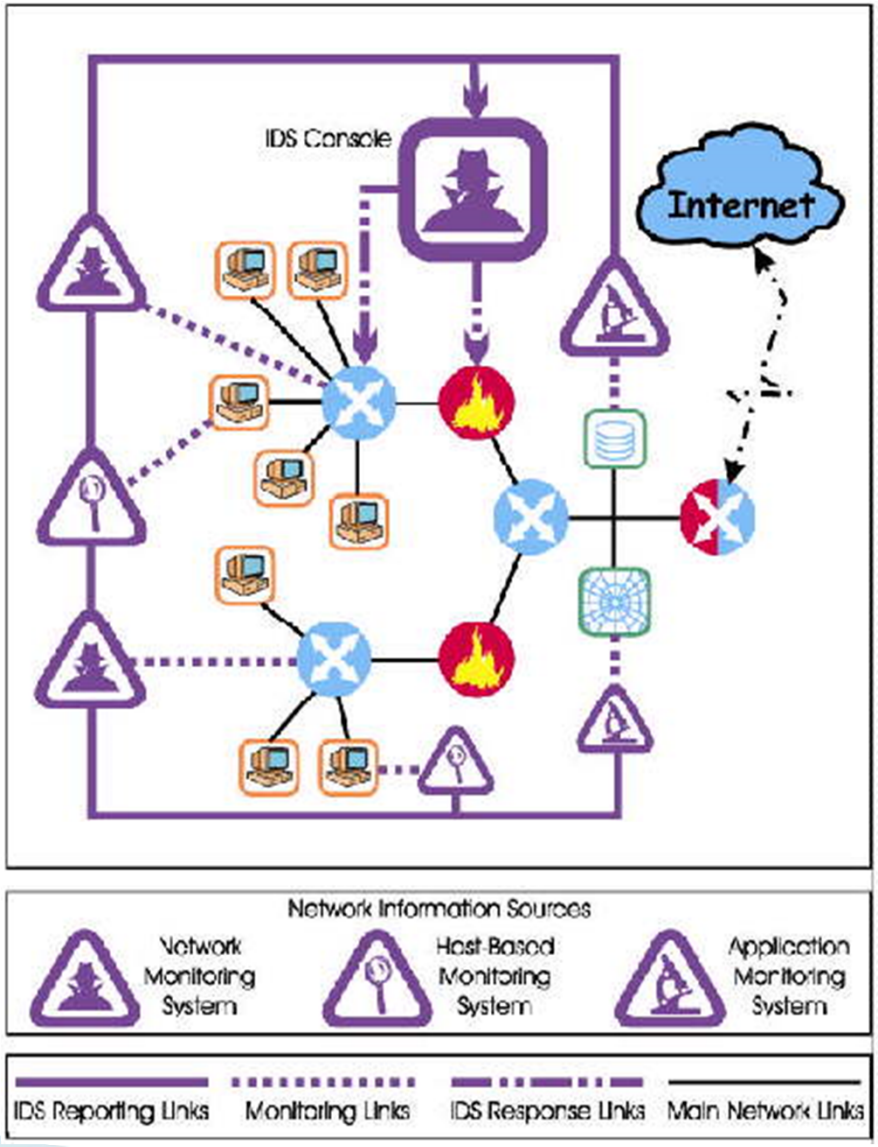
- วิเคราะห์ผลการติดตามเหตุการณ์เพื่อตัดสินใจว่าเหตุการณ์นั้นปกติหรือไม่

- จัดทำและจัดการรายงานชนิดต่างๆ

**ข้อดี**

ต้นทุนต่ำ และควบคุมการทำงานได้ง่าย เนื่องจากอยู่จุดเดียว

# การควบคุม IDS → Centralized IDS Control



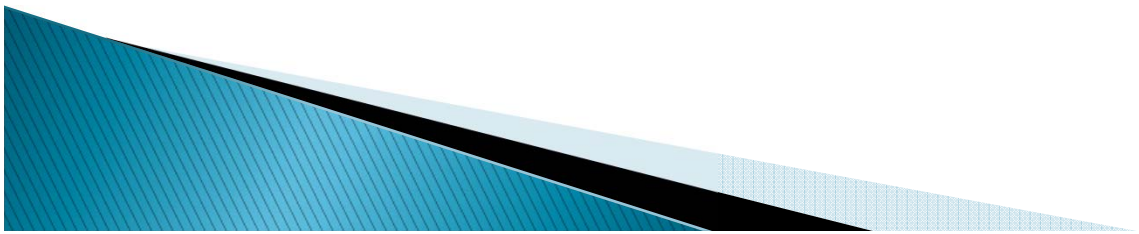

อ้างอิงจาก E.Whittman and J.Mattore,2005

# การควบคุม IDS

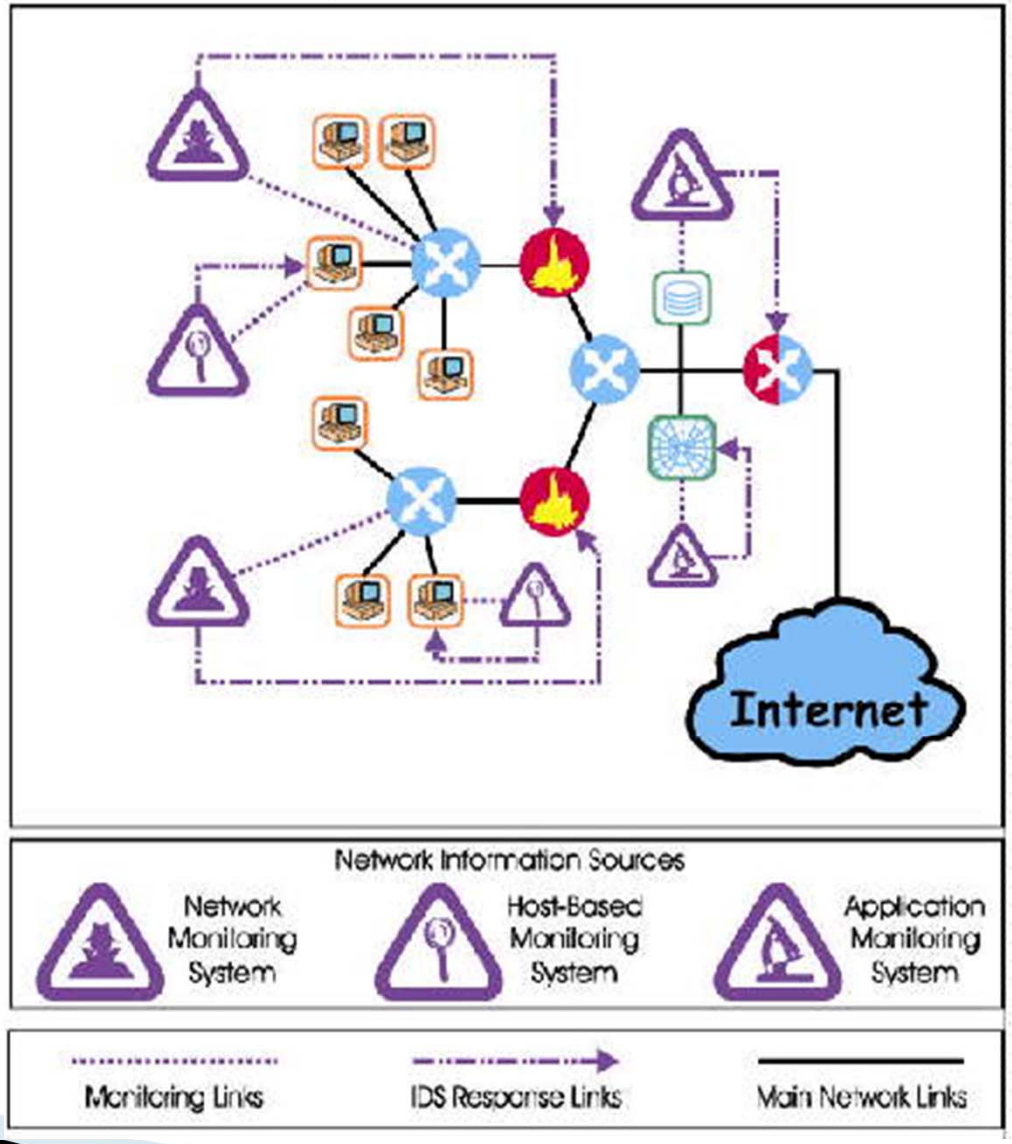
**2. Fully Distributed IDS Control** เป็นรูปการควบคุมที่จัดให้ทุกฟังก์ชันกระจายไปตามระบบ IDS ย่อยที่ติดตั้งตามกลุ่มต่างๆ ระบบนี้จะไม่มี IDS Console เนื่องจากระบบ IDS ย่อยสามารถจัดการและควบคุมงานได้เอง

**ข้อดี**

แต่ละระบบย่อย IDS ไม่จำเป็นต้องรอคำสั่งจาก IDS Console จึงทำงานได้เร็วกว่า



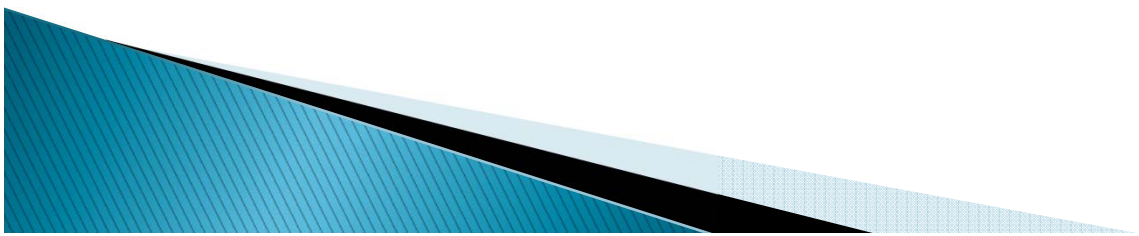
# การควบคุม IDS → Fully Distributed IDS Control



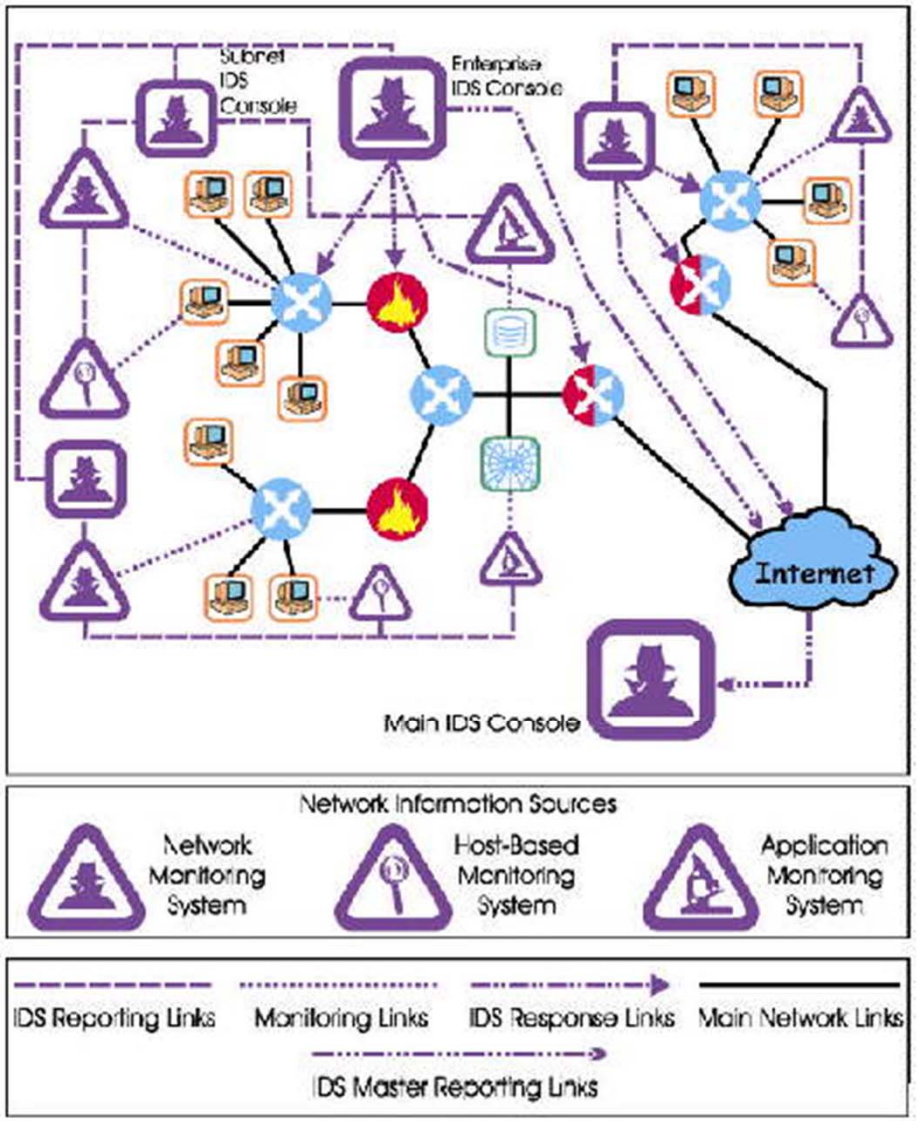

อ้างอิงจาก E.Whittman and J.Mattore,2005

# การควบคุม IDS

**3. Partial Distributed IDS Control** เป็นรูปการควบคุมที่รวมเอาทั้งสองวิธีมาอยู่ด้วยกัน โดยมี Main IDS Console ควบคุมการทำงานของ IDS ย่อยที่อยู่ตาม Site ต่างๆ ซึ่ง IDS ย่อยสามารถวิเคราะห์และตอบสนองต่อการโจมตีได้เอง แต่ต้องรายงานให้ Main IDS Console เพื่อบันทึกเหตุการณ์ต่างๆ ให้ Main IDS Console รู้จักกับการโจมตีกับทุก Site และสามารถป้องกันการบุกรุกได้ครอบคลุมทั้งหมด



# การควบคุม IDS → Partial Distributed IDS Control




อ้างอิงจาก E.Whittman and J.Mattore,2005

# การนำระบบ NIDS ไปใช้งาน

E. Whittman and J. Mattord ได้เสนอทางเลือกในการติดตั้ง Sensor Agent ให้กับ NIDS ไว้ 4 ทางเลือกคือ

**Location 1** วาง Sensor ไว้ด้านในต่อจาก External Firewall ในเขต DMZ ข้อดีคือ

- มองเห็นการโจมตีจากภายนอกและอาจป้องกันไว้ได้ทันท่วงที
- ระบุปัญหาที่เกิดขึ้นได้โดยพิจารณาจากกฎเกณฑ์ของ Firewall
- มองเห็นการโจมตีที่ดำลังจะมุ่งหน้ามายัง Web Server or FTP Server ที่อยู่ในเขต MDZ
- ตรวจจับเส้นทางการเชื่อมต่อจากภายในที่จะออกไปสู่เครือข่ายภายนอก

# การนำระบบ NIDS ไปใช้งาน

**Location 2** วาง Sensor ไว้ด้านนอกของ External Firewall ข้อดีคือ

- สามารถจัดทำเอกสารแสดงจำนวนการโจมตีจาก Internet ที่มีเป้าหมายคือ Internal Network

- สามารถจัดทำเอกสารแสดงจำนวนการโจมตีจาก Internet ที่มีเป้าหมายคือ External Network

**Location 3** วาง Sensor ไว้ที่เครือข่ายหลักขององค์กร ข้อดีคือ

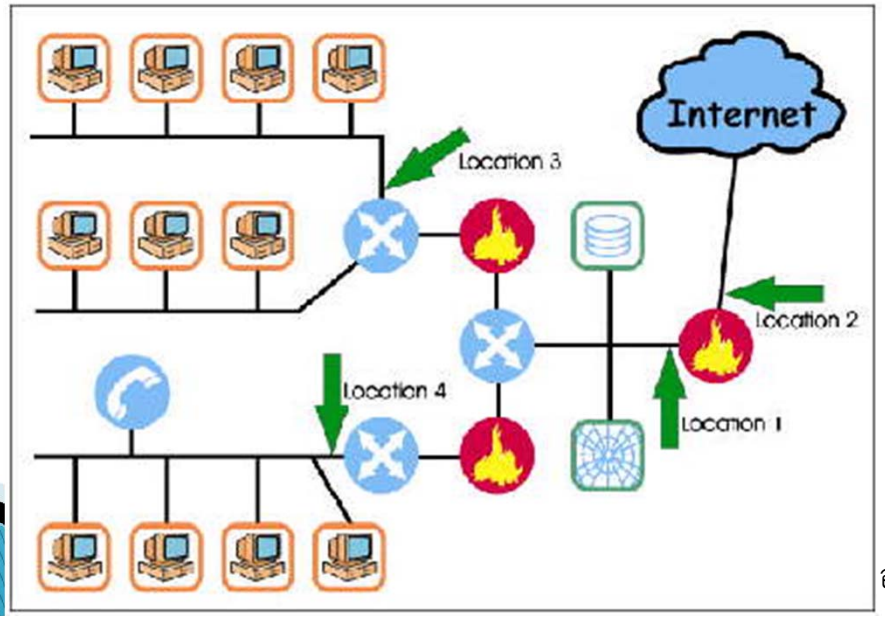
- สามารถตรวจจับการบุกรุกที่มากับเครือข่ายได้อย่างวงกว้าง

- สามารถตรวจจับกิจกรรมบางอย่างของ User ที่ไม่ได้รับอนุญาตภายในองค์กร

# การนำระบบ NIDS ไปใช้งาน

**Location 4** วาง Sensor ไว้ที่เครือข่ายย่อยที่สำคัญขององค์กร ข้อดีคือ

- สามารถตรวจจับการโจมตีที่มุ่งหน้ามายังระบบสำคัญขององค์กร
- การติดตั้งเฉพาะระบบที่สำคัญเป็นการจำกัดขอบเขตของการดูแลความปลอดภัย จึงทำให้การทำงานมีความเข้มงวดและรอบคอบขึ้น




อ้างอิงจาก E.Whittman and J.Mattore,2005

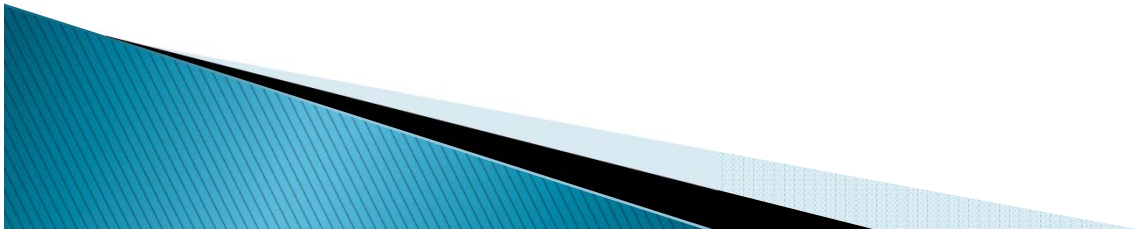
# การนำระบบ HIDS ไปใช้งาน

จะแตกต่างจาก NIDS เพราะต้องติดตั้งที่ Host แต่ละเครื่องบน Network ดังนั้นสิ่งที่ต้องคำนึกถึงจึงเป็นประเด็นขั้นตอนและระยะเวลาการติดตั้ง โดยพิจารณาได้ 3 ประการ ดังนี้

1. การติดตั้งระบบ HIDS อาจใช้เวลานาน

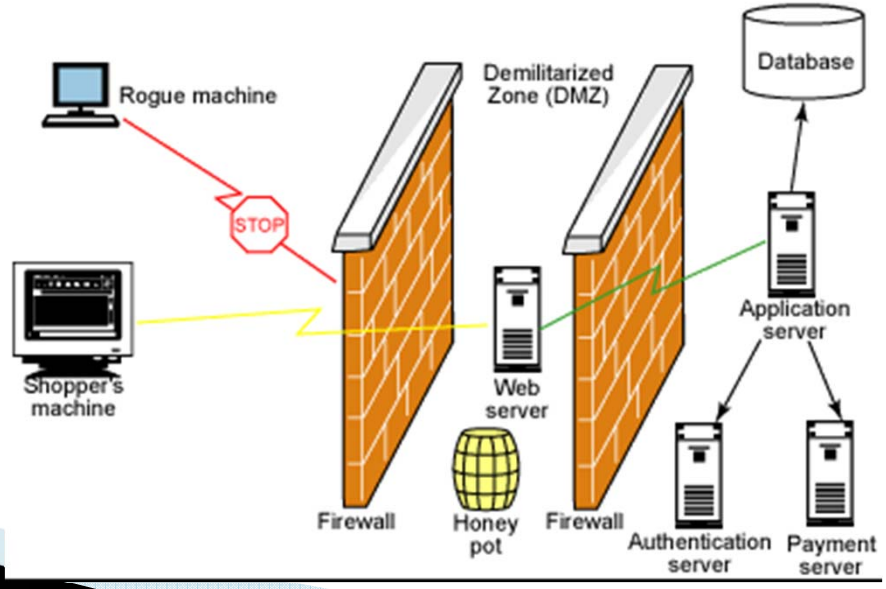
2. ควรติดตั้งระบบ HIDS ที่เครือข่ายย่อยหรือที่ระบบที่สำคัญหรือวิกฤติที่สุดก่อน

3. ที่เครือข่ายย่อยควรติดตั้งตามความสำคัญจนครบตามแผนงานที่กำหนดไว้

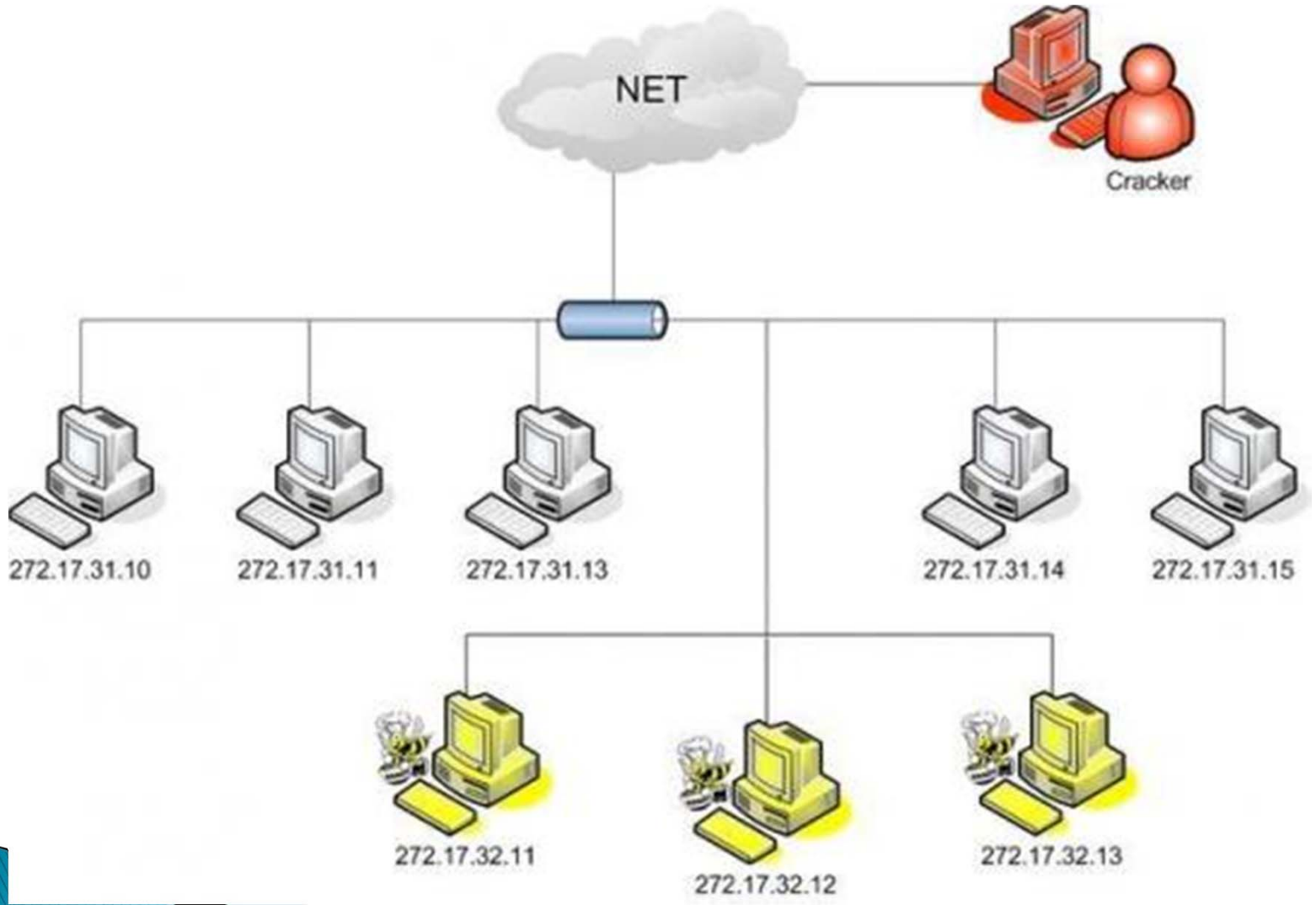


# Honey Pot

**Honey Pot** คือ ระบบหลุมพรางที่ออกแบบมาให้เป็นเหยื่อล่อผู้โจมตี ให้มาโจมตีที่เครื่อง Honey pot แทนที่จะโจมตีระบบสำคัญหรือระบบวิกฤติขององค์กร ถ้านำหลายชุดมาเชื่อมต่อกันจะเรียกว่า Honey Net โดยสามารถติดตั้งไว้ภายในหรือภายนอก Firewall ดังนั้นระบบ Honey Pot ไม่ใช่ระบบรักษาความปลอดภัย แต่เป็นการติดตั้งเพิ่มเติมอีกระดับชั้นหนึ่ง



# Honey Pot




อ้างอิงจาก E.Whittman and J.Mattore,2005

# ข้อดี-ข้อเสียของการทำ Honey Pot

- **ข้อดี**
  - ผู้โจมตีเบี่ยงเบนเป้าหมายไปยังระบบจำลองซึ่งไม่มีข้อมูลความลับ
  - ผู้ดูแลระบบมีเวลาตัดสินใจว่าจะตอบสนองต่อผู้โจมตีอย่างไร
  - สามารถติดตามรูปแบบการโจมตีได้ง่ายดาย
  - สามารถตรวจจับการโจมตีจากภายในได้
- **ข้อเสีย**
  - กฎหมายไม่รองรับการใช้ Honey Pot
  - หากผู้โจมตีทราบว่าตกหลุมพราง Honey Pot จะเพิ่มความรุนแรงของการโจมตี
  - การใช้งาน Honey Pot ต้องอาศัยความชำนาญอย่างมาก

# Questions and Answers

MS1 Thanin Muangpool

Thank you