บทที่ 7 : IDS/IPS Part2

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

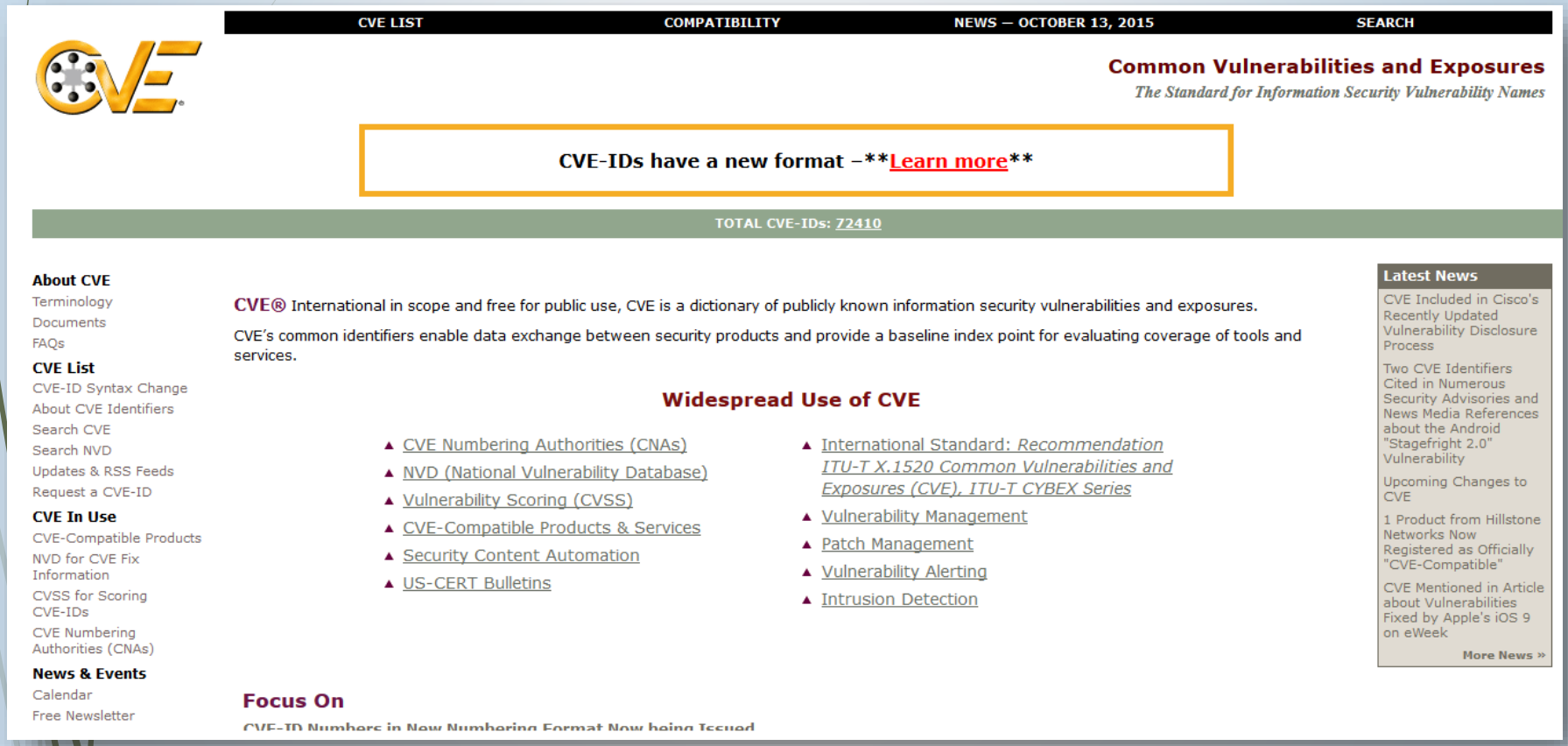
Outline

- ช่องโหว่ของระบบคอมพิวเตอร์
- การรายงานแจ้งเตือนภัย
- การออกแบบและติดตั้ง IDS
- ผลิตภัณฑ์ IDS/IPS

ช่องโหว่ของระบบคอมพิวเตอร์

- มาตรฐานสำหรับการเรียกชื่อช่องโหว่และการโจมตีที่นิยมมากที่สุดคือ CVE (Common Vulnerabilities and Exposure) สร้างโดยบริษัท MITRE
- เป็นการรวบรวมข้อมูลจากผู้เชี่ยวชาญด้านการรักษาความปลอดภัยทั่วโลก
- สามารถดูข้อมูลได้จากเว็บไซต์ https://cve.mitre.org

เว็บไซต์ https://cve.mitre.org



CVE LIST | COMPATIBILITY | NEWS – OCTOBER 13, 2015 | SEARCH

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE-IDs have a new format –**Learn more**

TOTAL CVE-IDs: 72410

About CVE
Terminology
Documents
FAQs

CVE List
CVE-ID Syntax Change
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID

CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVSS for Scoring CVE-IDs
CVE Numbering Authorities (CNAs)

News & Events
Calendar
Free Newsletter

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- CVE Numbering Authorities (CNAs)
- NVD (National Vulnerability Database)
- Vulnerability Scoring (CVSS)
- CVE-Compatible Products & Services
- Security Content Automation
- US-CERT Bulletins
- International Standard: *Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures (CVE), ITU-T CYBEX Series*
- Vulnerability Management
- Patch Management
- Vulnerability Alerting
- Intrusion Detection

Latest News

CVE Included in Cisco's Recently Updated Vulnerability Disclosure Process

Two CVE Identifiers Cited in Numerous Security Advisories and News Media References about the Android "Stagefright 2.0" Vulnerability

Upcoming Changes to CVE

1 Product from Hillstone Networks Now Registered as Officially "CVE-Compatible"

CVE Mentioned in Article about Vulnerabilities Fixed by Apple's iOS 9 on eWeek

More News »

Focus On

CVE-ID Numbers in New Numbering Format Now being Issued

ช่องโหว่ของระบบคอมพิวเตอร์ [2]

- ส่วนใหญ่ IDS จะรายงานโดยบอกรายละเอียดของการโจมตีนั้นๆ รวมไปถึงช่องโหว่ที่การโจมตีนั้นใช้ประโยชน์ ซึ่งเป็นสิ่งสำคัญที่จะทำให้ผู้ดูแลระบบสามารถวิเคราะห์และปิดช่องโหว่นั้นๆได้

ช่องโหว่ของระบบคอมพิวเตอร์ [3]

ช่องโหว่ที่มักพบเป็นประจำได้แก่

- Input Validation Error
  - Buffer Overflow
  - Boundary Condition Error
- Access Validation Errors
- Exceptional Condition Handling Error
- Environmental Error
- Configuration Error
- Race Condition

การรายงานแจ้งเตือนภัย

- สิ่งที่ผู้ดูแลระบบจะต้องคอนฟิกให้กับ IDS คือ
  - 1) ซิกเนเจอร์ของการบุกรุก
  - 2) เหตุการณ์ที่ผู้ดูแลระบบให้ความสำคัญหรือคาดว่าจะเป็นการนำไปสู่การบุกรุกในภายหน้า
- เหตุการณ์ที่ IDS จะรายงานให้ทราบมี 3 ประเภท คือ
  - การสำรวจเครือข่าย
  - การโจมตี
  - เหตุการณ์น่าสงสัยหรือผิดปกติ

การรายงานแจ้งเตือนภัย

: การสำรวจเครือข่าย

เป็นการสำรวจเครือข่ายเพื่อพยายามรวบรวมข้อมูลก่อนที่โจมตีจริงๆ วิธีการเช่น

- IP Scans
- Port Scans
- Trojan Scans
- Vulnerability Scans
- File Snooping

การรายงานแจ้งเตือนภัย

: การโจมตี

- การโจมตีเครือข่ายจะมีการแบ่งลำดับความสำคัญเอาไว้ตามความรุนแรง
- หาก IDS รายงานการโจมตีที่มีระดับความรุนแรงสูง ผู้ดูแลระบบจะต้องตอบสนองทันที เพื่อป้องกันการสูญเสียที่มากกว่านี้
- ปกติแล้วผู้ดูแลระบบจะต้องทำการวิเคราะห์เพิ่มเติมว่าเป็นการโจมตีจริงหรือการสแกน

การรายงานแจ้งเตือนภัย

: เหตุการณ์ที่น่าสงสัย

- เป็นเหตุการณ์ที่นอกเหนือจากที่กล่าวมาข้างต้น
- ซึ่ง IDS ไม่มีข้อมูลเพียงพอที่จะบอกได้ว่าเป็นเหตุการณ์อะไร แต่จะแจ้งเตือนให้ผู้ดูแลระบบทราบเพื่อสืบหาสาเหตุต่อไป
- เช่น ได้รับแพ็คเก็ตที่มีส่วนหัวผิดไปจากที่กำหนดในมาตรฐาน ซึ่งอาจเป็นการโจมตีแบบใหม่ หรือเน็ตเวิร์คการ์ดเครื่องส่งอาจจะเสียก็ได้

การออกแบบและติดตั้ง IDS

- ก่อนที่จะติดตั้งและใช้งาน IDS ควรมีการสำรวจความต้องการ ศึกษาวิธีในการตรวจจับการบุกรุก แล้วค่อยเลือกโซลูชั่นที่เหมาะสมกับโครงสร้างและนโยบายการรักษาความปลอดภัย
- องค์กรควรเลือกใช้ทั้งโฮสต์เบสและเน็ตเวิร์คเบสไอดีเอสควบคู่กัน เพื่อการทำงานร่วมกันอย่างมีประสิทธิภาพ
- ติดตั้งเน็ตเวิร์คเบสก่อน จากนั้นป้องกันเซิร์ฟเวอร์ที่สำคัญด้วยโฮสต์เบส
- ควรใช้เครื่องมือวิเคราะห์ช่องโหว่เพื่อทดสอบการทำงานของ IDS
- ควรมีการใช้ Honeypot ร่วมด้วย

การออกแบบและติดตั้ง IDS

: การเชื่อมต่อ IDS เข้ากับเครือข่าย

- การติดตั้ง IDS ลงบนเครือข่ายที่ใช้ Hub เป็นเรื่องที่ง่าย เพราะฮับจะแจกจ่ายแพ็คเก็ตแบบ Broadcast อยู่แล้ว ซึ่งสามารถปรับเน็ตเวิร์คการ์ดของ IDS ให้รับทุกๆแพ็คเก็ตได้เลย
- ถ้าเป็นเครือข่ายที่ใช้สวิตช์การติดตั้งจะมีความยุ่งยากมากขึ้น เนื่องจากสวิตช์จะส่งแพ็คเก็ตไปยังพอร์ตที่ปลายทางเชื่อมต่ออยู่เท่านั้น จึงทำให้ IDS ไม่สามารถจับทุกๆแพ็คเก็ตที่วิ่งในเครือข่ายได้

การออกแบบและติดตั้ง IDS

: การเชื่อมต่อ IDS เข้ากับเครือข่าย [2]

เทคนิคการเชื่อมต่อ IDS เข้ากับเครือข่ายที่ใช้สวิตช์ มีอยู่ 3 วิธี คือ

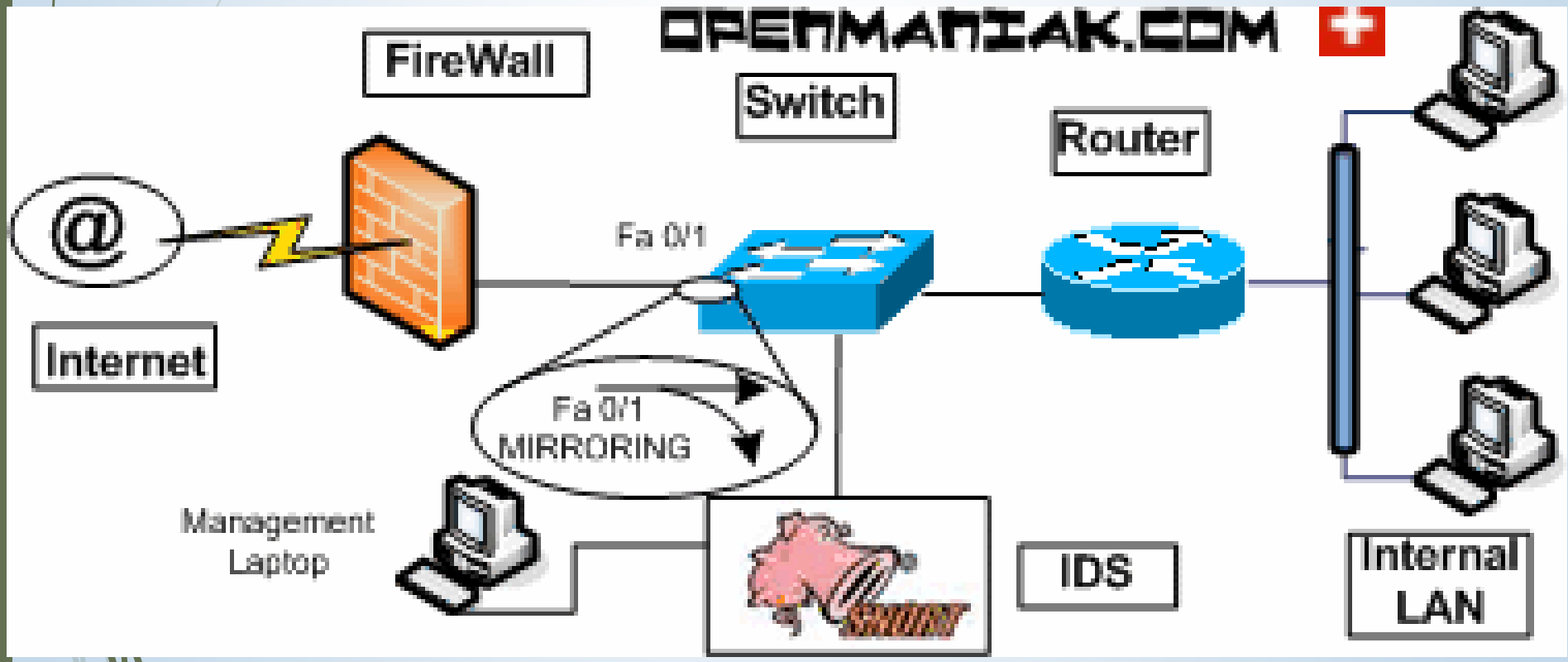
- การทำ Port Mirroring
- การใช้ฮับ
- การใช้แท็พ (Tap)

การออกแบบและติดตั้ง IDS

: การเชื่อมต่อ IDS เข้ากับเครือข่าย : Port Mirroring

- จะใช้สวิตช์ที่มีคุณสมบัติการทำ Port Mirroring ได้ บางครั้งเรียกว่า Spanning Port
- สวิตช์จะส่งต่อทุกๆแพ็คเก็ตที่รับจากพอร์ตหนึ่งไปยังอีกพอร์ตหนึ่ง
- การใช้งาน เช่น การทำ Port Mirroring จากพอร์ตที่เชื่อมกับเราเตอร์หรือไฟร์วอลล์

การเชื่อมต่อ IDS แบบ Port Mirroring



ข้อดี-ข้อเสียของการเชื่อมต่อ IDS แบบ Port Mirroring

ข้อดี	ข้อเสีย
ง่ายต่อการติดตั้ง เพราะไม่ต้องเปลี่ยนโครงสร้างใดๆบนเครือข่าย	สามารถทำได้แบบพอร์ตต่อพอร์ตเท่านั้น
ไม่มีผลกระทบต่อการคอนฟิกไฟร์วอลล์	ประสิทธิภาพของสวิตช์จะลดลง
	สวิตช์จะส่งต่อแพ็คเก็ตที่สมบูรณ์เท่านั้น ทำให้ไม่สามารถตรวจจับบางแพ็คเก็ตที่สำคัญในการวิเคราะห์ได้

การออกแบบและติดตั้ง IDS

: การเชื่อมต่อ IDS เข้ากับเครือข่าย : การใช้ฮับ

- ใช้งานโดยการวางฮับระหว่างสวิตช์และเราเตอร์ แล้วนำ IDS ไปเชื่อมต่อเข้ากับพอร์ตหนึ่งของฮับ
- ข้อมูลยังคงไหลระหว่างเราเตอร์และสวิตช์ได้ และ IDS ยังสามารถตรวจจับทุกๆแพ็คเก็ตที่วิ่งผ่านเราเตอร์และฮับได้ด้วย

ข้อดี-ข้อเสียของการเชื่อมต่อ IDS แบบใช้ฮับ

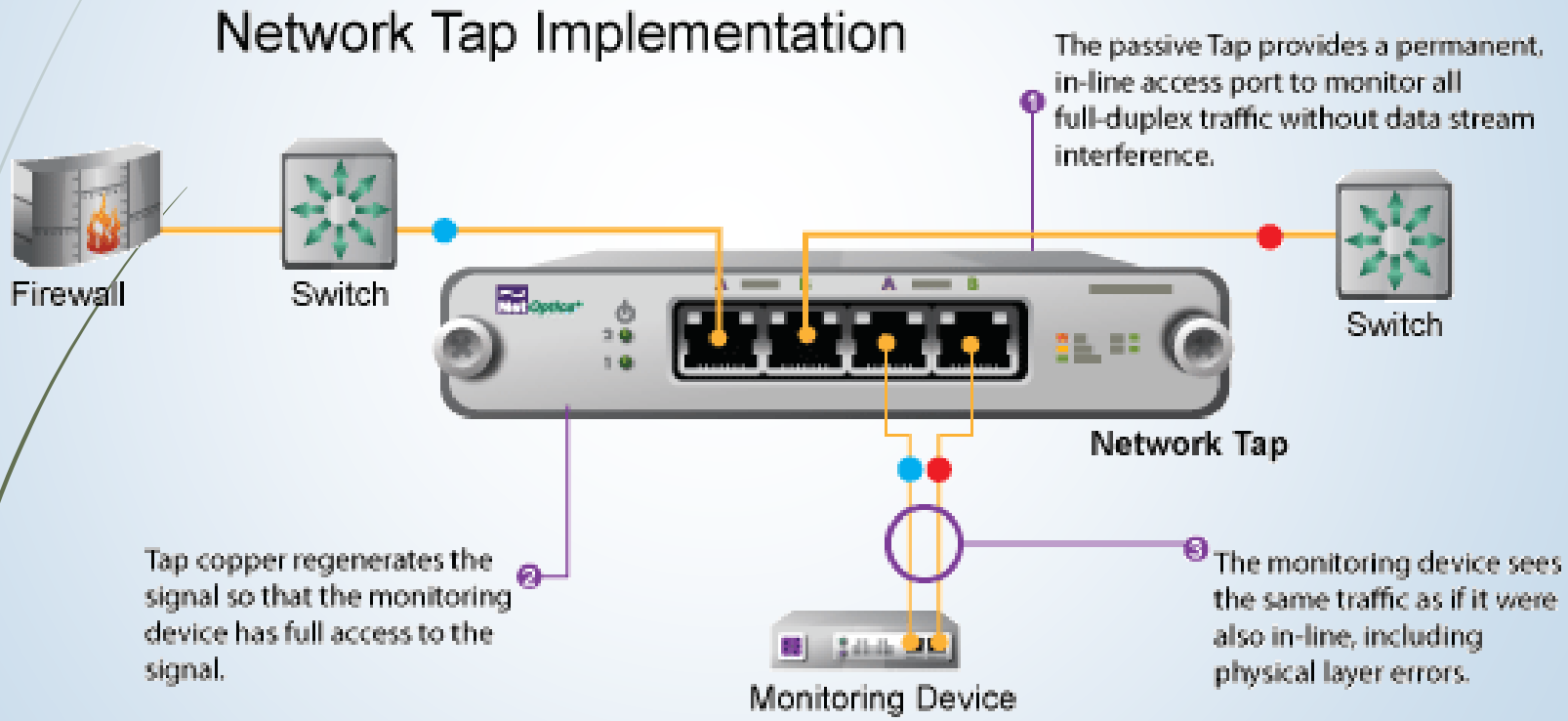
ข้อดี	ข้อเสีย
ง่ายต่อการคอนฟิก	ไม่สามารถเชื่อมต่อได้ถ้าลิงก์ระหว่างเราเตอร์กับสวิตช์เป็นแบบ Full Duplex แต่ฮับจะเป็นแบบ Half-Duplex
ไม่มีผลกระทบต่อการคอนฟิกไฟร์วอลล์	ถ้าบริหาร IDS ผ่านฮับตัวเดียวกัน จะทำให้เพิ่มโอกาสการชนกันของข้อมูล
มีราคาถูก	ฮับเกิดการชำรุดได้ง่าย
	เป็นวิธีที่ไม่เป็นที่นิยม เพราะเกิดปัญหามากกว่าวิธีอื่นๆ และทำให้ประสิทธิภาพของเครือข่ายลดลง

การออกแบบและติดตั้ง IDS

: การเชื่อมต่อ IDS เข้ากับเครือข่าย : การใช้แท็พ

- เป็นวิธีการที่ใช้แก้ปัญหาการเชื่อมต่อโดยใช้ฮับหรือ Port Mirroring
- อุปกรณ์ Tap จะทำหน้าที่คล้ายๆฮับ แต่แท็พสามารถทนต่อข้อผิดพลาดได้ (Fault Tolerance)
- การเชื่อมต่อจะเป็นแบบถาวร (Hardwired) ระหว่างสองพอร์ตหลัก

การเชื่อมต่อ IDS ด้วยแท็พแบบ 4 พอร์ต



ข้อดี-ข้อเสียของการเชื่อมต่อ IDS แบบใช้แท็พ

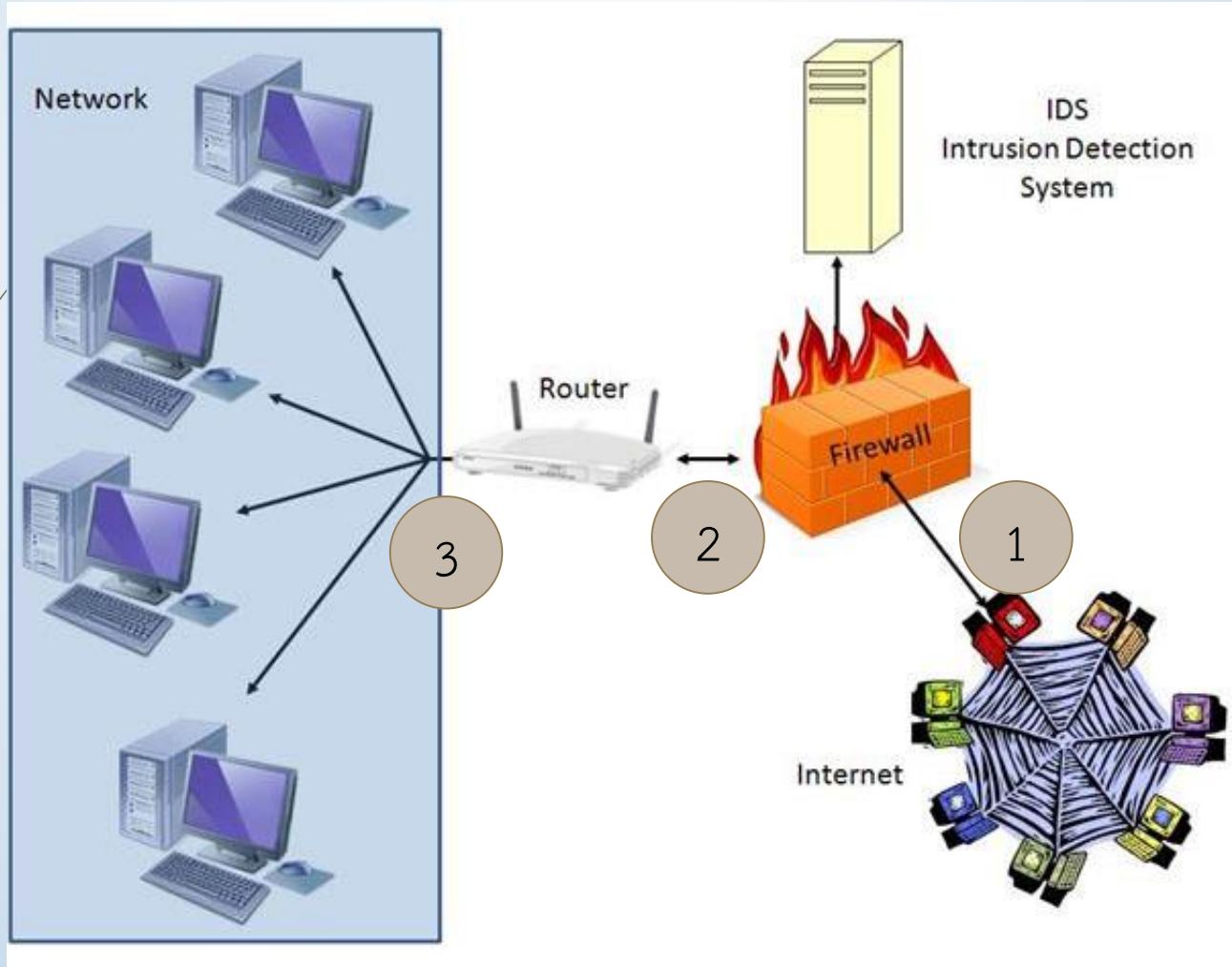
ข้อดี	ข้อเสีย
ทนต่อข้อผิดพลาด หากไฟฟ้าของแท็พดับ ลิงก์ระหว่างสองพอร์ตหลักยังคงใช้งานได้อยู่	แท็พมีราคาแพง
ไม่มีผลกระทบต่อการไหลของทราฟิก	การสิ้นสุดเซสชั่นอาจต้องมีการคอนฟิกเพิ่ม
ไม่ทำให้โครงสร้างของเครือข่ายเปลี่ยนไป	IDS ต้องทำงานในโหมดหายตัว (Stealth Mode) เท่านั้น
ไม่ทำให้ประสิทธิภาพของเครือข่ายลดลง	
IDS สามารถมอนิเตอร์แพ็คเก็ตที่ผิดปกติได้	

การออกแบบและติดตั้ง IDS

: การติดตั้ง Network-Based IDS

- คำถามแรกในการติดตั้งเน็ตเวิร์คเบสไอดีเอสคือจะติดตั้งตรงจุดไหนของเครือข่าย?
- หน้าไฟร์วอลล์ หรือหลังไฟร์วอลล์ จะดีกว่ากัน?

จะติดตั้ง Network-Based IDS จุดไหนดี?



การออกแบบและติดตั้ง IDS

: การติดตั้ง Network-Based IDS [2]

- ข้อดีของการติดตั้งหลังไฟร์วอลล์
  - สามารถตรวจจับการบุกรุกที่สามารถเจาะผ่านไฟร์วอลล์มาได้
  - ใช้ตรวจสอบการคอนฟิกและประสิทธิภาพของไฟร์วอลล์ได้
  - สามารถตรวจจับการโจมตีเซิร์ฟเวอร์ที่อยู่ใน DMZ ได้
  - อาจตรวจเจอแพ็คเก็ตที่จะส่งไปภายนอกได้
- ข้อดีของการติดตั้งหน้าไฟร์วอลล์
  - เก็บสถิติของจำนวนครั้งของการโจมตีที่มาจากภายนอกได้
  - เก็บสถิติของประเภทการโจมตีที่มาจากภายนอกได้

การออกแบบและติดตั้ง IDS

: การติดตั้ง Network-Based IDS [3]

- ข้อดีของการติดตั้งบนแบ็คโบนหลักของเครือข่าย
  - มอนิเตอร์ทราฟิกหลักที่ไหลเวียนอยู่ในเครือข่าย เพื่อวิเคราะห์ที่มาหรือเป้าหมายหลักในการโจมตีได้
  - ตรวจจับกิจกรรมที่ไม่ได้รับอนุญาตของผู้ใช้ทั่วไปได้
- ข้อดีของการติดตั้งบนซับเน็ตที่มีความเสี่ยงสูง
  - ตรวจจับการโจมตีเป้าหมายเป็นระบบที่สำคัญ
  - ลดจำนวนไอดีเอสที่ต้องใช้ และมอนิเตอร์เฉพาะจุดสำคัญเท่านั้น เพื่อความคุ้มค่าในการใช้งาน IDS

การออกแบบและติดตั้ง IDS

: การติดตั้ง Host-Based IDS

- ควรติดตั้งโฮสต์เบสไอดีเอสเฉพาะกับเซิร์ฟเวอร์ที่สำคัญๆ จะทำให้ลดค่าใช้จ่ายลง และทำให้ผู้ดูแลระบบจดจ่อกับรายงานการแจ้งเตือนที่มาจากเซิร์ฟเวอร์สำคัญๆเท่านั้น
- หากจะติดตั้งกับโฮสต์ส่วนใหญ่ ควรเลือกใช้งานระบบ IDS ที่สามารถบริหารจัดการจากส่วนกลางได้
- ประสิทธิภาพของโฮสต์เบสไอดีเอสจะขึ้นอยู่กับความชำนาญของผู้ดูแลระบบเป็นหลัก เพราะฉะนั้นผู้ดูแลระบบต้องใช้เวลาพอสมควรในการเรียนรู้

ผลิตภัณฑ์ IDS/IPS

- IDS ที่นิยมใช้งานอย่างแพร่หลายคือโปรแกรมที่ชื่อว่า Snort ซึ่งเป็น IDS/IPS แบบ Open Source สามารถใช้ได้ทั้งบน Windows และ Unix มีโหมดการใช้งาน 3 โหมด คือ
  - Sniffer Mode
  - Packet Logger Mode
  - Network IDS Mode
  - Inline Mode

Snort : www.snort.org