030523114 Network Security

สาขาวิชาเทคโนโลยีอิเล็กทรอนิกส์ (ต่อเนื่อง)

ภาควิชาเทคโนโลยีวิศวกรรมอิเล็กทรอนิกส์

วิทยาลัยเทคโนโลยีอุตสาหกรรม

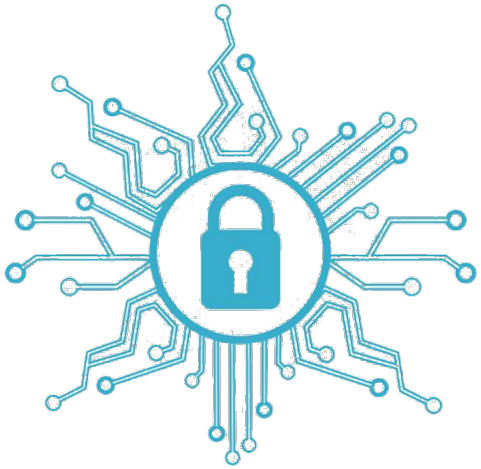
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

อาจารย์ ดร.เลอสรรค์ กิรสมุทรานนท์

ครั้งที่ 9 “Network Access Control”

NAC (Network Access Control)

- **Outline**
  - Intro NAC (Network Access Control)
  - What is NAC (Network Access Control) ?
  - หน้าที่ของ NAC (Network Access Control)
  - หลักการทางานของ NAC (Network Access Control)
  - Pre-Admission and Post-Admission
  - Agent and Agentless
  - Out-of-Band and Inline
  - การแก้ไข กักกัน และ Captive Portals
  - Cisco NAC Appliance

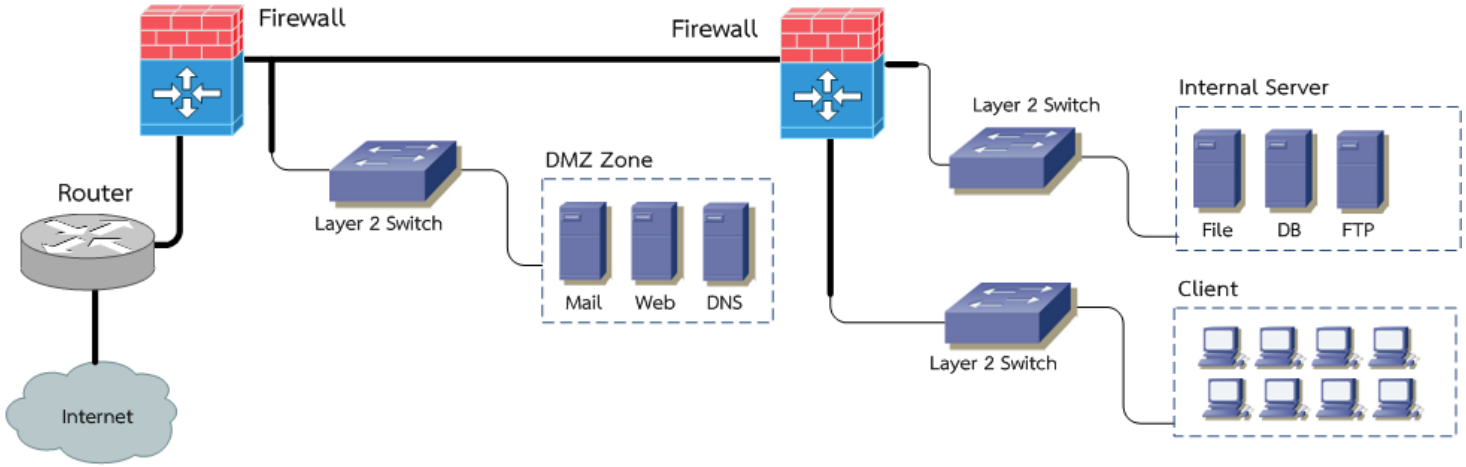


Intro NAC (Network Access Control)

- ภัยคุกคามต่อระบบเครือข่ายคอมพิวเตอร์
- การติดไวรัส เวอร์ม โทรจันสแปมแวร์ต่าง ๆ
- เกิดจากเครื่อง Client ในองค์กรและเครื่องพกพา เช่น Notebook
- หาระบบรักษาความปลอดภัยที่มีประสิทธิภาพมาป้องกันระบบคอมพิวเตอร์และข้อมูล

Intro NAC (Network Access Control)

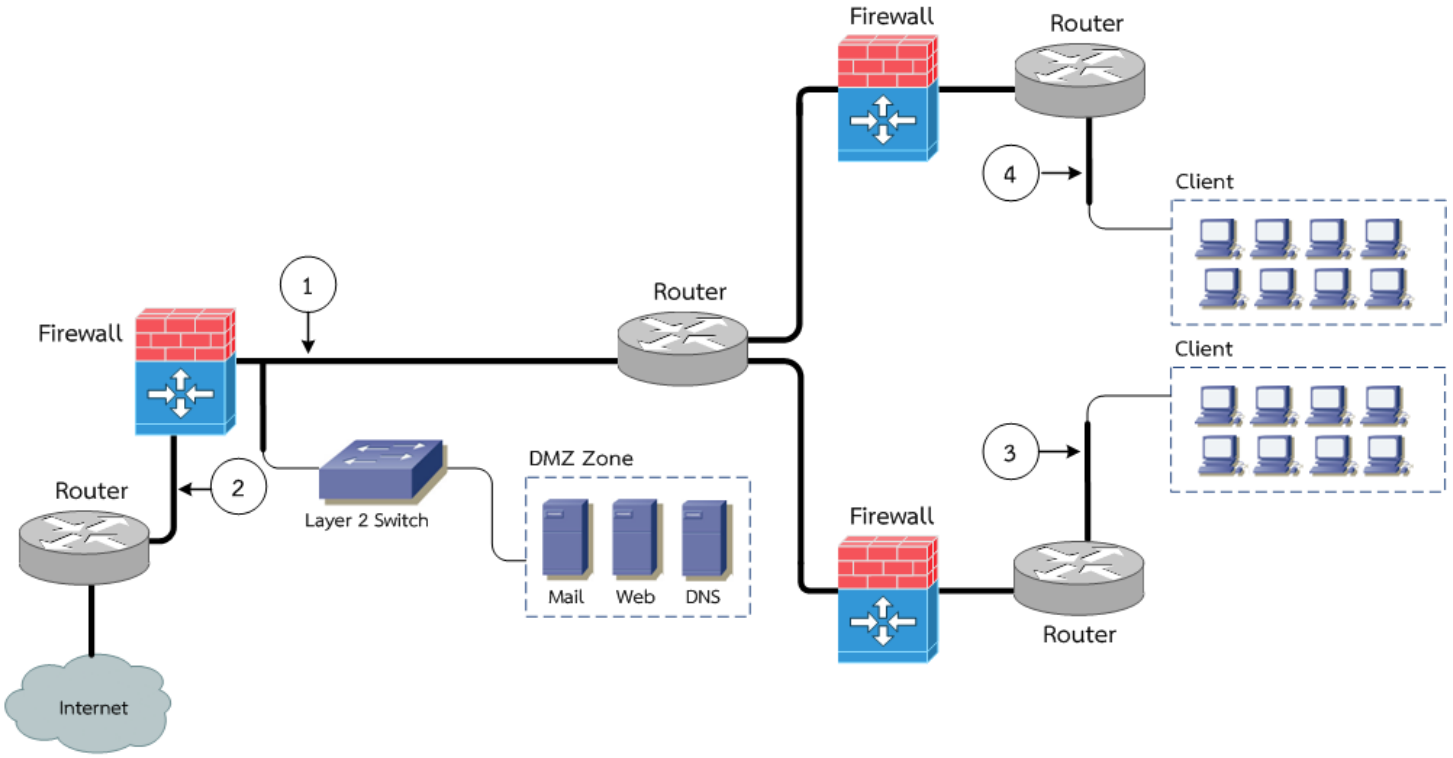
- การป้องกันด้วย Firewall ไม่สามารถป้องกันไวรัสที่แอบแฝงเข้ามาได้



Note.

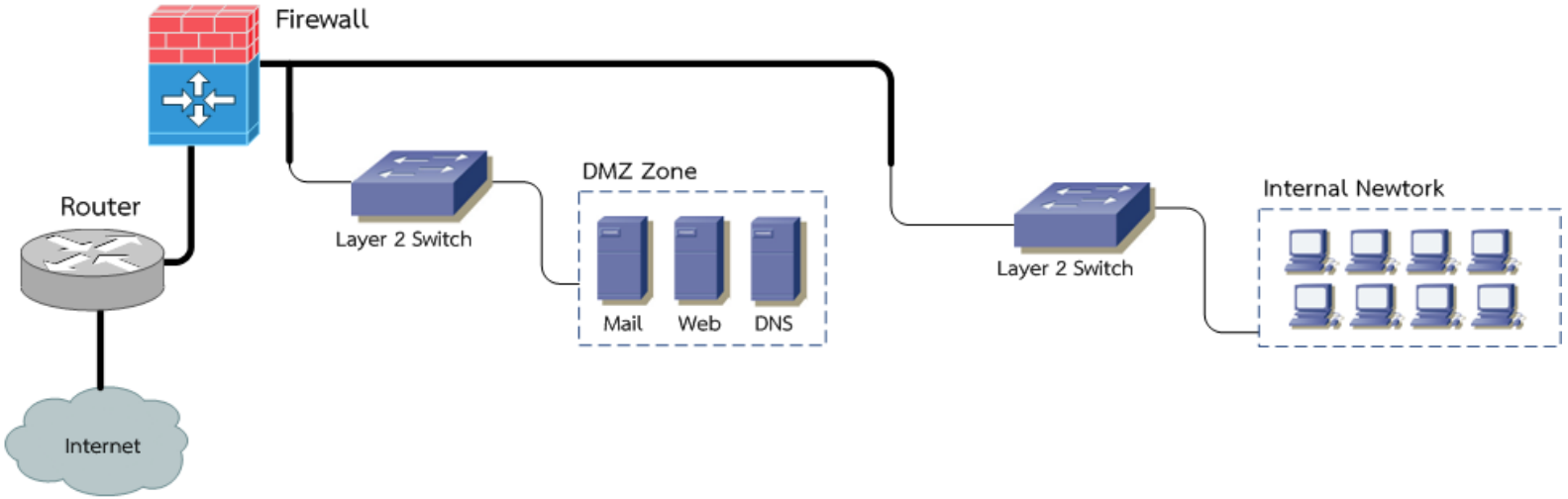
Intro NAC (Network Access Control)

- การใช้ IDS/IPS ไม่สามารถปกป้องได้ทั้งเครือข่ายหรือเครือข่ายภายในเอง 1,2,3,4 คือ ตัวอย่างจุดติดตั้งของ IDS/IPS



Intro NAC (Network Access Control)

- การใช้ Antivirus ในแต่ละเครื่อง อาจพบปัญหาไม่ได้อัดเดต จึงทาให้การทางานของ Antivirus สแกนหาไม่พบไวรัสใหม่ๆ หรือคนใน องศ์กรเองนาอุปกรณ์พกพาต่าง ๆ เข้ามาใช้ระบบ เช่น Notebook ที่ไม่มีความปลอดภัย เป็นต้น



Intro NAC (Network Access Control)

- Network Access Control (NAC) เป็นวิธีการหนึ่งทางด้านความปลอดภัยเครือข่ายคอมพิวเตอร์ที่ใช้เพื่อรวมเอาเทคโนโลยีทางด้านความปลอดภัย (เช่น แอนตี้ไวรัส Host Intrusion Prevention และ Vulnerability Assessment) ผู้ใช้หรือระบบพิสูจน์ตัวตน

- และการบังคับใช้การรักษาความปลอดภัยทางเครือข่ายเข้าด้วยกัน (Policy)

What is NAC (Network Access Control) ?

- NAC เป็นอุปกรณ์ที่ทาหน้าที่ในการตรวจสอบและควบคุมผู้ใช้งานและเครื่องที่ใช้งานในระบบเครือข่าย เพื่อป้องกันภัยที่อาจจะเกิดขึ้นภายในระบบเครือข่าย
  - ตรวจสอบโปรแกรม Antivirus, Personal Firewall
  - ป้องกันผู้ใช้งานที่ไม่ได้รับอนุญาตมาใช้งานเครือข่าย
  - ไม่อนุญาตให้ใช้งานเครือข่ายในกรณีที่เครื่องตรวจสอบไม่ผ่าน
  - วิเคราะห์หาพฤติกรรมที่เป็นการบุกรุกและรายงานสรุปเหตุการณ์เป็นต้น
  - ทั้งนี้ขึ้นอยู่กับแต่ละอุปกรณ์ที่อาจจะมีความสามารถเพิ่มเติม

หน้าที่ของ NAC (Network Access Control)

- Automatic Discovery and Classification : ทันทีที่ติดตั้งอุปกรณ์ NAC เข้าไปในระบบเครือข่ายอย่างน้อย ๆ อุปกรณ์ NAC จะต้องช่วยเราค้นหาอุปกรณ์อื่น ๆ
- Identity-Based Policy Enforcement : สามารถบังคับใช้นโยบายความปลอดภัยต่าง ๆ ในลักษณะของ Identity-Based ได้
- Network-Based Policy Enforcement : สามารถบังคับสิทธิ์ในการเข้าถึงระบบเครือข่ายของผู้ใช้งานรายบุคคลได้
- Application-Based Policy Enforcement : สามารถบังคับสิทธิ์การใช้งาน Application ของผู้ใช้งานในระบบได้

หน้าที่ของ NAC (Network Access Control)

- IPS-Based Policy Enforcement : สามารถทาหน้าที่เป็น IPS เพื่อตรวจจับการโจมตีระบบเครือข่ายจากผู้ใช้งานแต่ละคนได้
- Real Time Monitoring and Reporting : NAC ที่ดีจะต้องมีหน้าจอสาหรับทาการ Monitor แบบ Real Time

แต่ก็ไม่ใช่ NAC ทุกยี่ห้อที่จะมีความสามารถที่ครบครันแบบนี้ ดังนั้นควรเลือก NAC ให้เหมาะสมกับองค์กร

Note.

หลักการทางานของ NAC (Network Access Control)

- จะทำการตรวจสอบควบคุมการลงทะเบียนเครื่องคอมพิวเตอร์ของผู้ที่ต้องการเข้าระบบ ว่าเป็นผู้ที่มีสิทธิในการเข้าระบบหรือไม่
- Authentication กับอุปกรณ์เครือข่าย เช่น ใช้โปรโตคอล IEEE 802.1X
- ตรวจสอบเครื่องลูกข่ายว่าเป็นไปตามนโยบายความปลอดภัยขององค์กรหรือไม่
- Anti-Virus Signature ว่ามีการ Update ล่าสุดหรือไม่, Patch ของ Windows,
- มีการติดตั้ง Personal Firewall ที่เหมาะสมหรือไม่ เป็นต้น
- หากไม่เป็นไปตามนโยบายก็จะโยกเครื่องลูกข่ายนั้นไปยังเขตกักกัน
- จนกว่าเครื่องลูกข่ายจะมีการปรับปรุงให้ตรงตามนโยบาย
- หากตรงตามนโยบายก็อนุญาตให้ใช้งานเครือข่ายได้

Pre-Admission and Post-Admission

- Pre-Admission NAC เครื่องในเครือข่ายจะได้รับการตรวจสอบก่อนที่จะได้รับอนุญาตให้เข้าถึงเครือข่ายได้
- เพื่อป้องกันไคลเอนท์ที่ไม่ได้อัพเดท Signature ของไวรัสไม่ให้สามารถติดต่อกับเซิร์ฟเวอร์ที่มีข้อมูลความลับ เป็นต้น
- Post-Admission ใช้การบังคับโดยตัดสินใจจากการกระทาของผู้ใช้งาน หลังจากที่ผู้ใช้เหล่านี้สามารถเข้าถึงเครือข่ายได้แล้ว
- ปล่อยให้เข้ามาในระบบเครือข่ายก่อน หลังจากนั้นค่อยดูพฤติกรรมการใช้งานหากพบว่าไม่ปกติ ค่อยทาการจากัดการใช้งานต่อไป

Agent and Agentless

- การยอมให้ระบบ NAC สามารถตัดสินใจเกี่ยวกับการควบคุมการเข้าถึงเครือข่าย ข้อมูลเกี่ยวกับระบบของผู้ใช้เป็นข้อมูลสาหรับการตัดสินใจที่สำคัญของระบบ NAC
- Agent ติดตั้งโปรแกรมไว้ที่เครื่องผู้ใช้เพื่อรายงานลักษณะของเครื่องผู้ใช้หรือระบบปลายทาง
- Agentless ไม่มีการติดตั้งโปรแกรมที่เครื่องผู้ใช้ ใช้เทคนิคการสแกน Network Inventory เพื่อให้รู้ถึงลักษณะเหล่านี้จากระยะไกล

Note.

Out-of-Band and Inline

- ในระบบ Out-of-Band จะมีการใช้ Agent กับระบบปลายทางและรายงานข้อมูลข่าวสารมายังระบบควบคุมส่วนกลาง เพื่อให้สามารถควบคุมสวิตช์ให้บังคับใช้นโยบายได้
- Inline ใช้เครื่องเดียวที่ทาหน้าที่เป็นไฟร์วอลล์สำหรับเครือข่ายในระดับ Access Layer และบังคับใช้นโยบาย

การแก้ไข กักกัน และ Captive Portals

- การกักกัน (Quarantine) เครือข่ายกักกันเป็นเครือข่ายไอพีแบบจำกัดวงที่ยอมให้ผู้ใช้สามารถเข้าถึงโฮสต์และแอพพลิเคชั่นบางตัวเท่านั้น

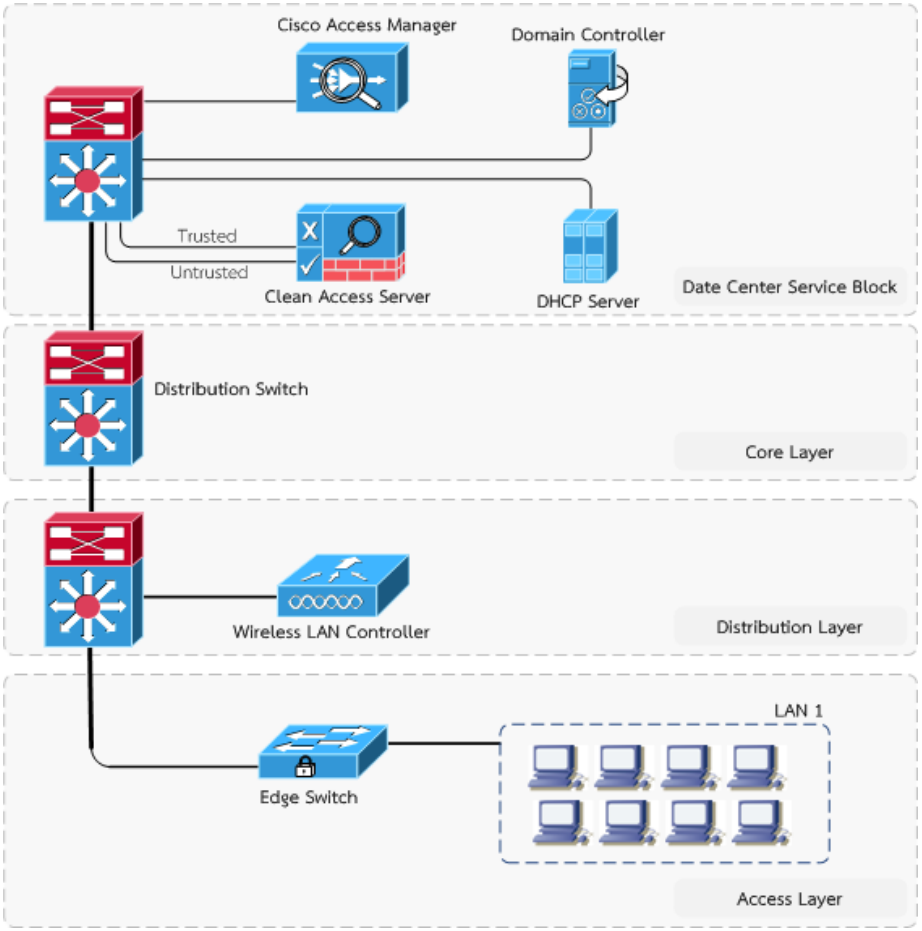
- การกักกันมักใช้ในรูปแบบของการกำหนด VLAN จะมีการกำหนดพอร์ทของสวิตช์ไปยัง VLAN ที่มีเส้นทางไปยังเซิร์ฟเวอร์สำหรับการอัพเดทซอฟท์แวร์เท่านั้น

- Captive Portals จะสกัดการเข้าถึงหน้าเว็บและเปลี่ยนเส้นทางของผู้ใช้ไปยังเว็บแอพพลิเคชั่นที่ให้คำแนะนาและเครื่องมือที่ใช้ในการอัพเดทคอมพิวเตอร์

ตัวอย่างเทคโนโลยีภายใต้แนวคิด NAC (Network Access Control)

- Cisco NAC Appliance โซลูชัน Cisco Clean Access เป็นโซลูชันที่ใช้เครือข่ายเป็นศูนย์กลาง ในการบังคับอุปกรณ์ทั้งหมดที่ต้องเกี่ยวข้องกับเครือข่ายขององค์กรให้ปฏิบัติตามนโยบายรักษาความปลอดภัย
- Cisco Clean Access เป็นโซลูชันควบคุมสิทธิในการเข้าถึงที่ครอบคลุมในตลาดการรักษาความปลอดภัยสารสนเทศ
- Cisco Clean Access เป็นโซลูชันแบบเบ็ดเสร็จ โดยเฉพาะองค์กรที่มีทรัพยากรน้อย
- ความง่ายและอินทิเกรตการติดตามเส้นทางแพตซ์ระบบปฏิบัติการ แอนตี้ไวรัส และอัพเดทช่องโหว่ของระบบ

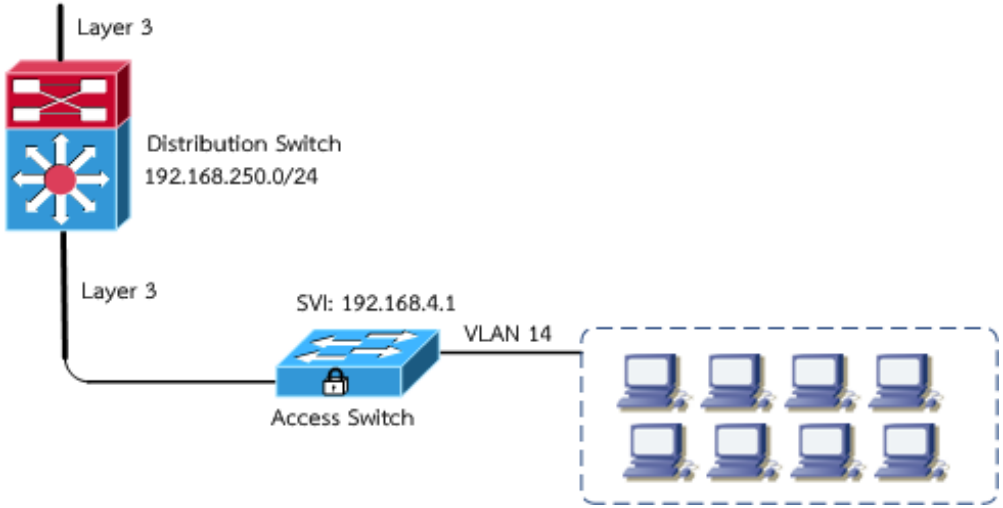
Cisco NAC Solution Architecture



แสดงตัวอย่างรูปแบบการติดตั้ง Cisco NAC Appliance

Cisco NAC Solution Architecture

- Access Layer มี VLAN ID : 14 บนตัว Access Switch โดย Cisco NAC Manager ทาหน้าที่ควบคุมแต่ละพอร์ตของ Switch



Cisco NAC Solution Architecture

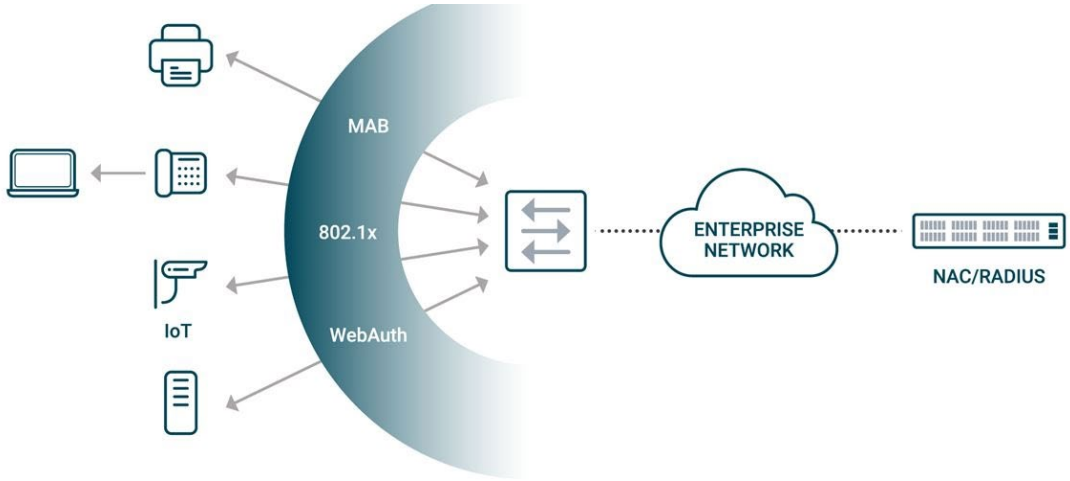
- **Distribution Layer** เป็นส่วนในการจัดการเรื่องของ Routing หรือเส้นทางการส่งผ่านข้อมูล ซึ่งโดยปกติแล้ว Cisco NAC Server จะไม่ได้วางอยู่ในส่วนของ Layer นี้
- **Core Layer** ในส่วนนี้จะมีข้อมูลที่วิ่งผ่านเยอะ โดยใช้ Router ในการกาหนดเส้นทางของข้อมูล (Hi- Speed Routing) ส่วนบริการต่าง ๆ นอกเหนือจาก Routing จะถูกกาหนดในส่วนของ Data Center Services Layer แทน
- **Data Center Services Layer** ใช้ Router และ Switch ในการจัดการ Cisco NAC Manager และ Cisco NAC Server จะวางอยู่ใน Layer นี้ เพื่อควบคุมการให้บริการต่าง ๆ

Cisco NAC Solution Architecture

- *Cisco NAC Manager เป็นศูนย์กลางสาหรับควบคุม เฝ้าติดตามและปรับแต่งการทางานของ Cisco NAC Server รวมทั้งบริหารจัดการนโยบายการเข้าถึงเครือข่ายต่าง ๆ ของผู้ใช้ และมีการปรับแต่ง ควบคุมพอร์ตของสวิตช์ด้วย*
- *Cisco NAC Server ทาหน้าที่ในการแยกส่วนของเครือข่ายที่ผ่านการอนุญาตแล้ว (Trusted) กับเครือข่ายที่ยังไม่ได้อนุญาต (Untrusted) โดยมีการติดต่อกับการพิสูจน์ตัวตนผู้ใช้ และมีการกาหนดนโยบาย (Polices) การเข้าใช้งานเครือข่ายจาก Cisco NAC Manager ให้กับเครื่องผู้ใช้งานด้วย*

Cisco NAC Solution Architecture

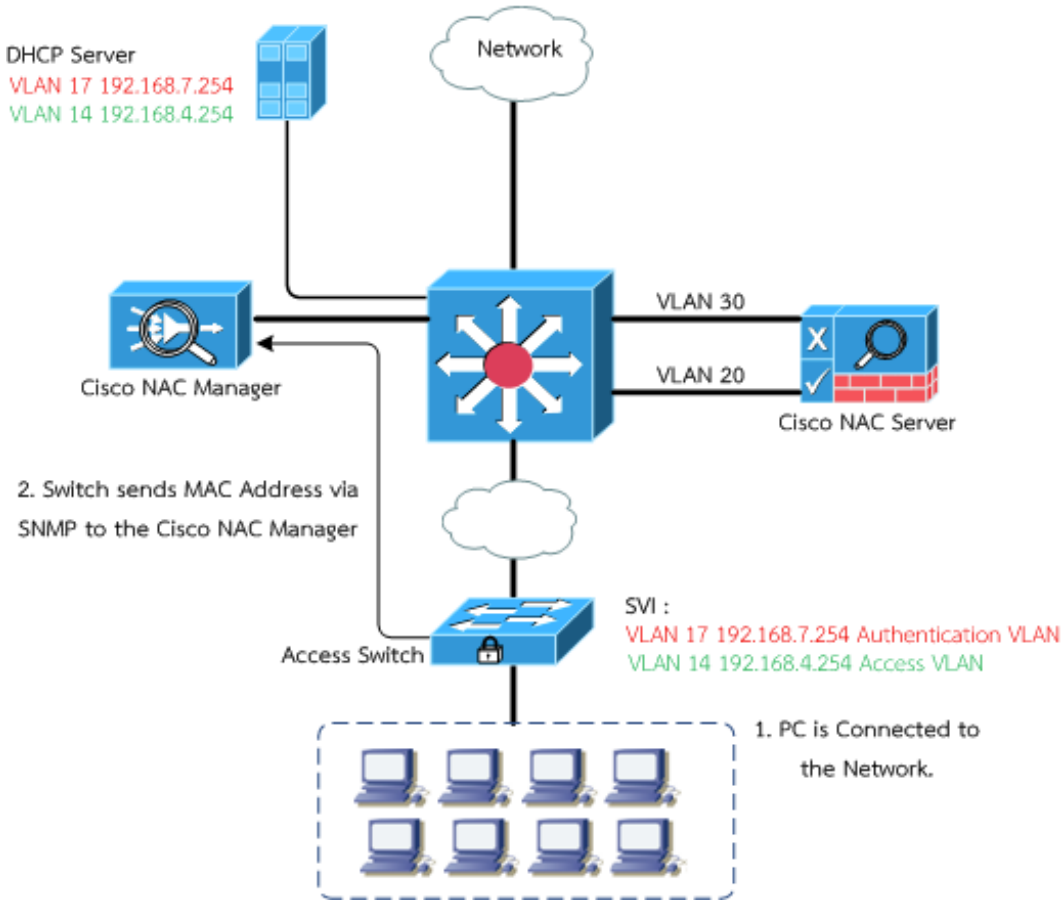
- *Cisco NAC Agent ใช้สำหรับตรวจสอบระบบปฏิบัติการและโปรแกรมต่าง ๆ ของเครื่องผู้ใช้ หากไม่พบโปรแกรมหรือไม่ตรงตามนโยบายที่กำหนดไว้ Cisco NAC Agent จะดำเนินการช่วยเหลือ โดยอาจจะใช้ลักษณะเป็น Web Portal ให้ทาการติดตั้งโปรแกรมหรือแพตซ์ต่าง ๆ ให้ครบ เป็นต้น*



Cisco NAC Solution Architecture

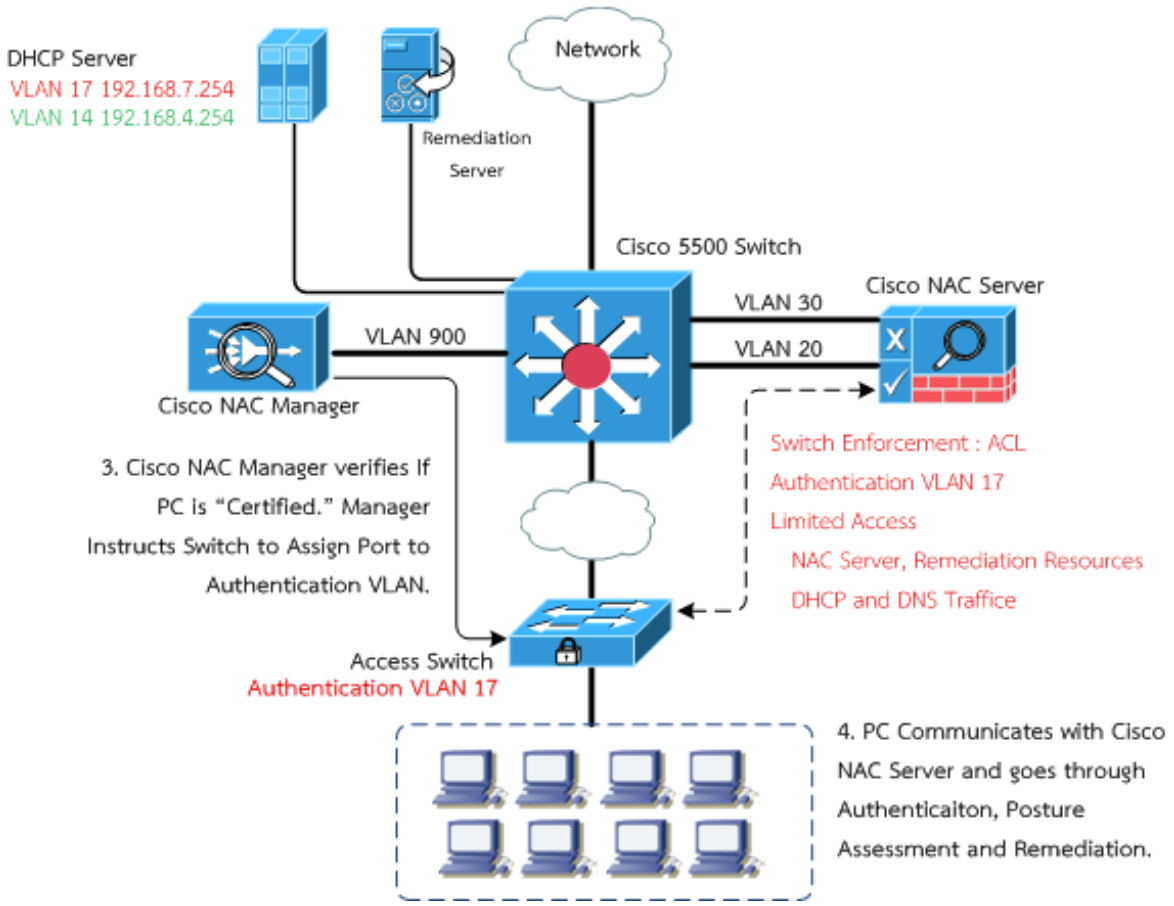
- **Out-of-Band (OOB) Mode** การติดตั้งแบบ OOB Cisco NAC Server จะมีการสื่อสารกับเครื่องผู้ใช้ในช่วงของพิสูจน์ตัวตน หลังจากที่ผ่านการพิสูจน์ตัวตนของผู้ใช้ เครื่องผู้ใช้จะไม่มีการติดต่อกับ Cisco NAC Server อีก
- ใน OOB Mode นี้ Cisco NAC Manager จะใช้ Simple Network Management Protocol (SNMP) เพื่อจัดการ VLAN ให้กับพอร์ตของสวิตช์ด้วย
- ใน Mode นี้ Cisco NAC Manager จำเป็นที่จะต้องควบคุมพอร์ตของสวิตช์ในการกำหนด VLAN ดังนั้น สวิตช์ที่ใช้งานต้อง Support ในส่วนนี้

Cisco NAC Solution Architecture



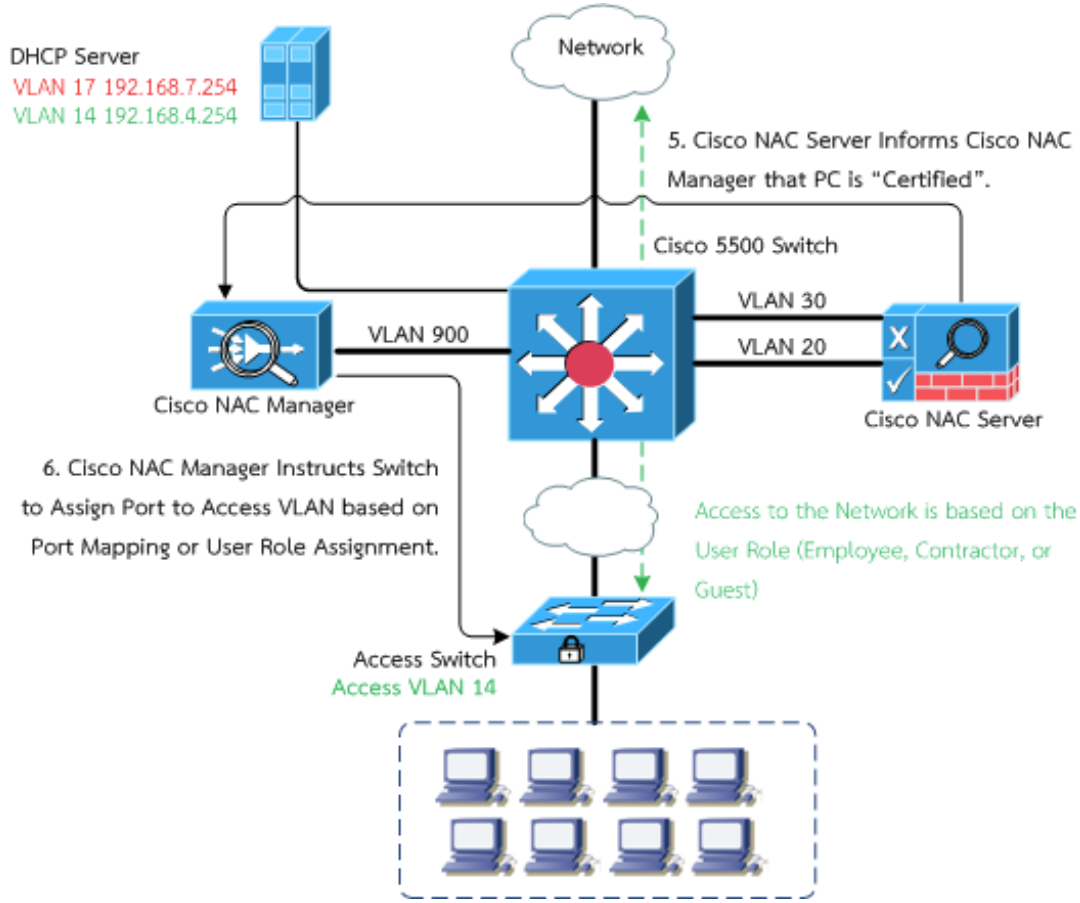
Process Flow

Cisco NAC Solution Architecture



Process Flow

Cisco NAC Solution Architecture



Process Flow

Cisco NAC Solution Architecture

1. เครื่องผู้ใช้เชื่อมต่อเข้าระบบเครือข่ายผ่านสวิตช์
2. สวิตช์ทำการส่ง MAC Address ของเครื่องของผู้ใช้โดยใช้ SNMP ไปให้ Cisco NAC Manager ตรวจสอบ
3. Cisco NAC Manager ทำการตรวจสอบ ถ้า
    - ไม่ผ่านการตรวจสอบ Cisco NAC Manager จะนาเครื่องผู้ใช้ไปอยู่ใน VLAN an authentication สำหรับให้เครื่องผู้ใช้ทำการติดตั้งโปรแกรมและอัพเดตเครื่องตัวเองให้เรียบร้อยก่อน (ขั้นตอนที่ 4)
    - ผ่านการตรวจสอบ Cisco NAC Server (ขั้นตอนที่ 5)

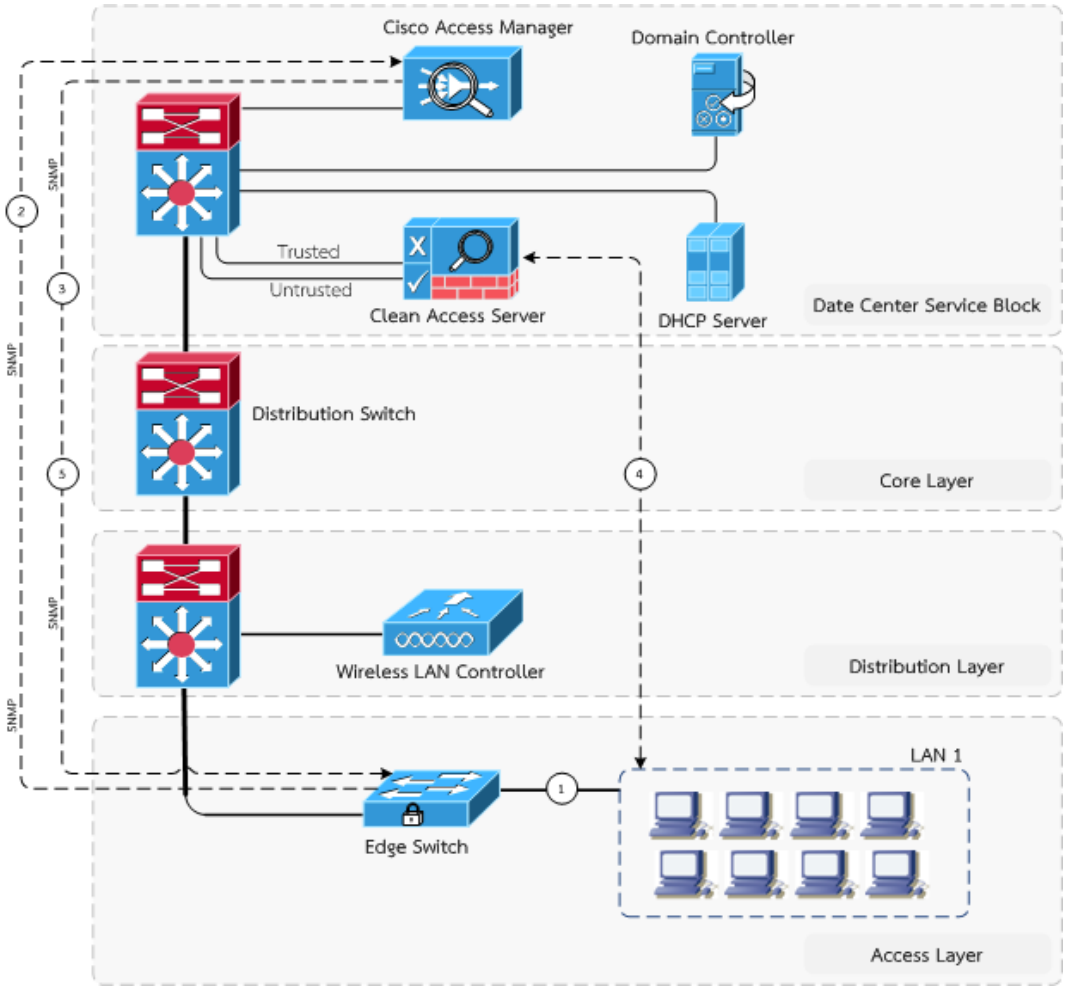
Cisco NAC Solution Architecture

4. เครื่องผู้ใช้ติดต่อไปที่ Cisco NAC Server เพื่อทาการลงโปรแกรมและอัพเดตเครื่องตัวเองให้เรียบร้อย

5. แจ้งให้ Cisco NAC Manager ทราบเพื่ออนุญาติให้ใช้งานเครือข่ายต่อไป

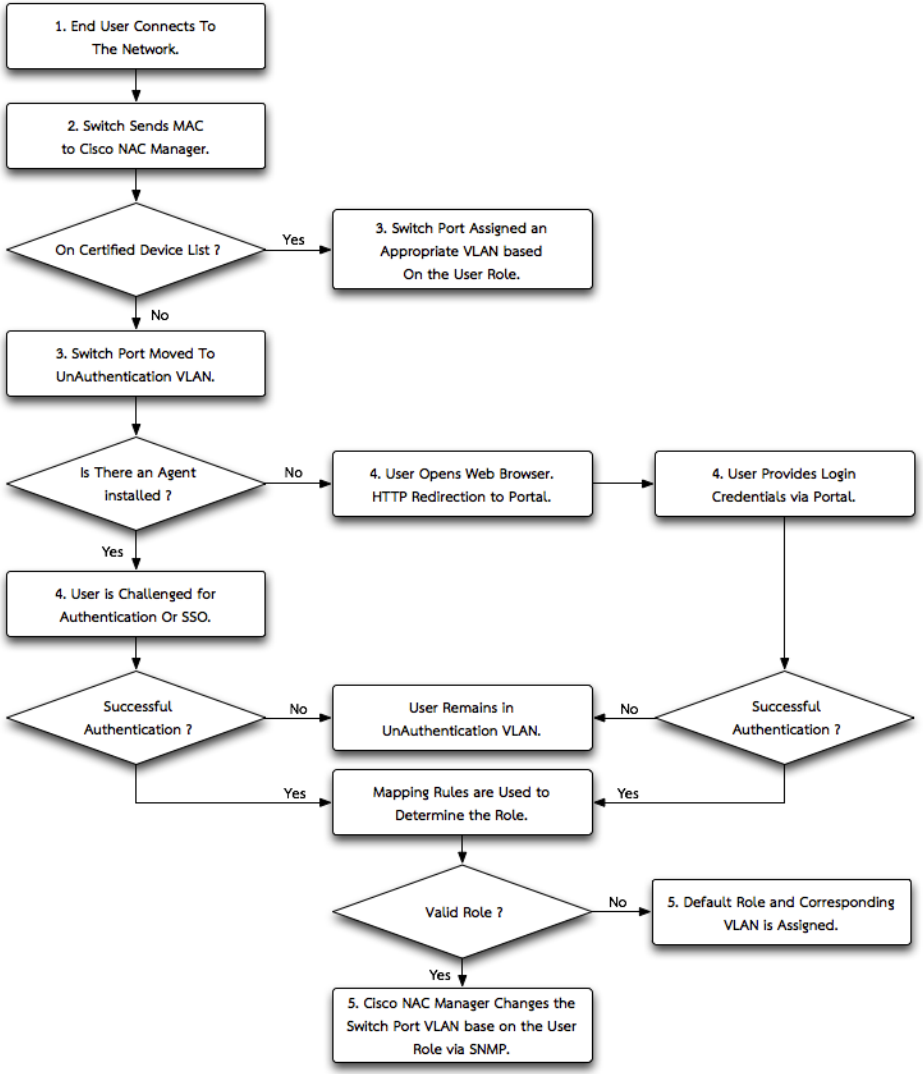
6. เครื่องผู้ใช้สามารถใช้งานเครือข่ายได้ตามนโยบายหรือกฎที่กาหนดไว้แล้ว

Cisco NAC Solution Architecture



NAC Process Flow for Layer 3 Out-Of-Band NAC Solution

Cisco NAC Solution Architecture



Process Flow Diagram

Reference

- http://www.cisco.com . วิธีสืบค้นวัสดุสารสนเทศ. [ออนไลน์]. เข้าถึงได้จาก : http : //www.cisco.com/web/TH/ technology/secure_clean.html. (วันที่สืบค้นข้อมูล 22 สิงหาคม 2553)
- SRAN Technology. Network Access Control คืออะไร. [ออนไลน์]. เข้าถึงได้จาก : http:// www.sran.net/archives/107. (วันที่สืบค้นข้อมูล 18 สิงหาคม 2553)
- Sophos. Sophos NAC 3.0 simplifies Network Access Control. [ออนไลน์]. เข้าถึงได้จาก : http://www.sophos.com/pressoffice/news/articles/2007/02/sophosnac.html. (วันที่สืบค้นข้อมูล 22 สิงหาคม 2553)
- IT Trends. Out-of-Band Network Access Control (NAC). [ออนไลน์]. เข้าถึงได้จาก : http://aruj-org.blogspot.com/2010/02/2010-it-trends-03-out-of-band-network.html. (วันที่สืบค้นข้อมูล 18 สิงหาคม 2553)