COMPUTER CENTER

SIEM

SECURITY INFORMATION AND EVENT MANAGEMENT

กกม.ศคพ.สอ.ทอ.

26460

1.คำจำกัดความของ SIEM

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM) คือ ระบบที่ใช้ในการจัดการกับ LOG และ EVENT ต่าง ๆ ด้านความปลอดภัยขององค์กร เป็นระบบ AUTOMATION ที่คอยทำหน้าที่วิเคราะห์หาความเชื่อมโยงของ EVENT ต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัยทั้งหมด ไปจนถึงทำการ ALERT ระบุตำแหน่งของภัยคุกคามให้ทีม CSOC ทราบเมื่อมี EVENT ที่ผิดปกติ ทำให้องค์กรสามารถป้องกัน และตอบสนองภัยคุกคามได้อย่างรวดเร็ว

SIEM เปรียบเหมือนศูนย์กลางในการรวบรวมข้อมูลและเป็นตัวคัดกรอง EVENT ระหว่าง IT FRAMEWORK และ SECURITY FRAMEWORK รวมทั้งยังรวบรวมข้อมูลจากระบบ HOST ,NETWORK ,FIREWALL ,ANTIVIRUS และอุปกรณ์ SECURITY ต่าง ๆ SIEM สร้าง THREAT RULES ทำให้ทราบถึง INSIGHT ของ ATTACKER จนเข้าใจ TACTICS, TECHNIQUES และ PROCEDURES ของ ATTACKER (TTPS) รวมทั้งรู้ถึง INDICATORS OF COMPROMISE (IOC)

องค์ประกอบของ THREAT DETECTION สามารถช่วยให้ตรวจเจอภัยคุกคามใน EMAILS, ทรัพยากร CLOUD, แอปพลิเคชัน, ทรัพยากร EXTERNAL THREAT INTELLIGENCE และ ENDPOINTS

เมื่อเกิดเหตุหรือมีการระบุ EVENT, ANALYZED และ CATEGORIZED จากนั้น SIEM จะทำการจัดส่งรายงานและแจ้งเตือนไปยังทีมงานผู้เกี่ยวข้องในองค์กร ซึ่งในส่วนนี้อาจรวมถึง USER และ ENTITY BEHAVIOR ANALYTICS (UEBA) ที่จะช่วยวิเคราะห์พฤติกรรม กิจกรรม เพื่อมอนิเตอร์ ติดตามพฤติกรรมที่ไม่ปกติ ซึ่งอาจบ่งชี้ถึงภัยคุกคามที่กำลังจะเกิดได้

2.ประวัติความเป็นมาของ SIEM

ระบบ SIEM ตัวช่วยสำคัญในการเฝ้าระวังภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ แจ้งเตือนภัยคุกคามได้ทันที ทำให้ผู้ดูแลระบบสามารถรับมือได้อย่างรวดเร็ว

โดยระบบ SIEM ถูกนำมาใช้เพื่อเพิ่มประสิทธิภาพในการเฝ้าระวังภัยคุกคามของระบบเครือข่ายและเป็นส่วนสำคัญที่ช่วยให้องค์กรปฏิบัติตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 56 ที่ระบุว่า

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) กำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติฯ”

2.ประวัติความเป็นมาของ SIEM (ต่อ)

องค์กรขนาดใหญ่หรือ CII ที่มีการเก็บ LOG จำนวนมากจากอุปกรณ์รักษาความปลอดภัยภายในเครือข่าย จึงเลือกจัดตั้ง ศูนย์ปฏิบัติการ CSOC (CYBER SECURITY OPERATIONS CENTER) ที่มี SIEM บริหารจัดการหรือให้หน่วยงานภายนอกที่มีบริการศูนย์ CSOC รูปแบบเฝ้าระวังภัยคุกคามทางไซเบอร์และมีเจ้าหน้าที่ผู้เชี่ยวชาญ ด้าน CYBERSECURITY ตลอด 24/7 เพื่อให้สามารถปฏิบัติได้ตามที่กฎหมายกำหนด

แต่สำหรับหน่วยงานที่ไม่ถูกระบุเป็น CRITICAL INFORMATION INFRASTRUCTURE (CII) ก็สามารถใช้ SIEM แบบ OPEN SOURCE บริหารจัดการเองได้เช่นกัน

ในการเฝ้าระวัง ป้องกัน เก็บข้อมูล วิเคราะห์ และแก้ไขปัญหาที่เกี่ยวข้องกับภัยไซเบอร์มีความจำเป็นอย่างมากที่จะต้องเก็บรวบรวมข้อมูล LOG ของกิจกรรมต่าง ๆ ที่เกิดขึ้น ไปจนถึงการวิเคราะห์หาพฤติกรรม หรือกิจกรรมที่น่าสงสัย และข้อมูลที่มากมายไม่ว่าจะจากทั้งภายในและภายนอกองค์กร

ระบบ SIEM จึงได้ถือกำเนิดขึ้นมา เพื่อเป็นเครื่องมือในการเก็บรวบรวมข้อมูล LOG ที่เกิดขึ้น วิเคราะห์เปรียบเทียบ และช่วยแจ้งเตือนเหตุการณ์ที่เป็นความเสี่ยง ทำให้สามารถวิเคราะห์ข้อมูลจำนวนมาก ๆ ได้ ช่วยให้ทีม CSOC หรือ ADMIN ที่ดูแลระบบไอที สามารถตรวจสอบหากิจกรรมที่น่าสงสัยได้อย่างรวดเร็ว ตอบสนองได้ทันท่วงทีมากยิ่งขึ้น ทำให้การทำงานด้าน CYBERSECURITY มีประสิทธิภาพมากยิ่งขึ้น

3.ความสามารถและรูปแบบการทำงานของ SIEM

01 การจัดเก็บข้อมูล LOG

02 การวิเคราะห์และตรวจสอบภัยคุกคาม

03 ติดตามภัยคุกคามได้แบบ REALTIME

04 การจัดหมวดหมู่ EVENT

05 ลดเวลา RESPONSE TIME

06 การทำงานร่วมกับระบบด้านความปลอดภัยอื่น ๆ

07 การแสดงผลข้อมูล DASHBOARD

4.กระบวนการจัดการใน SIEM

การรวบรวมข้อมูล (Data Collection)

เป็นการรวบรวมข้อมูลจากแหล่งข้อมูลความปลอดภัยในระบบหรือเครือข่ายทั้งหมด เช่น ข้อมูล Log ระบบปฏิบัติการ ซอฟต์แวร์ป้องกันไวรัส ระบบป้องกันการบุกรุก Server และ Firewall เป็นต้นเพื่อทำการบันทึกข้อมูลเก็บไว้ก่อนนำไปวิเคราะห์หาจุดอ่อนภายในระบบในคราวเดียว ช่วยให้ประหยัดเวลาและพื้นที่ในการดำเนินงาน

01

ข้อกำหนด(Policies)

คือสิ่งที่ถูกสร้างโดย SIEM administrator เพื่อกำหนดพฤติกรรมของ Enterprise system (ระบบศูนย์กลางของทั้งองค์กร) ภายใต้สถานการณ์ปกติและระหว่างเหตุการณ์ด้านความปลอดภัยที่อาจเกิดขึ้น SIEMs มีความสามารถสร้าง default rules, การแจ้งเตือน, รีพอร์ท และแดชบอร์ด ที่สามารถปรับแต่งให้สอดคล้องกับความจำเป็นด้านความปลอดภัยที่เราต้องการเฉพาะ

02

การจัดการความสัมพันธ์ (Data consolidation and correlation)

โดย SIEM จะจัดเรียงแปลงข้อมูล วิเคราะห์ และหาความสัมพันธ์ของ Log ต่าง ๆ ที่ทำการเก็บมา แล้วจัดประเภทข้อมูลและข้อกำหนด เพื่อให้ได้ตำแหน่งของจุดเสี่ยงที่อาจถูกภัยคุกคามทางไซเบอร์โจมตีได้

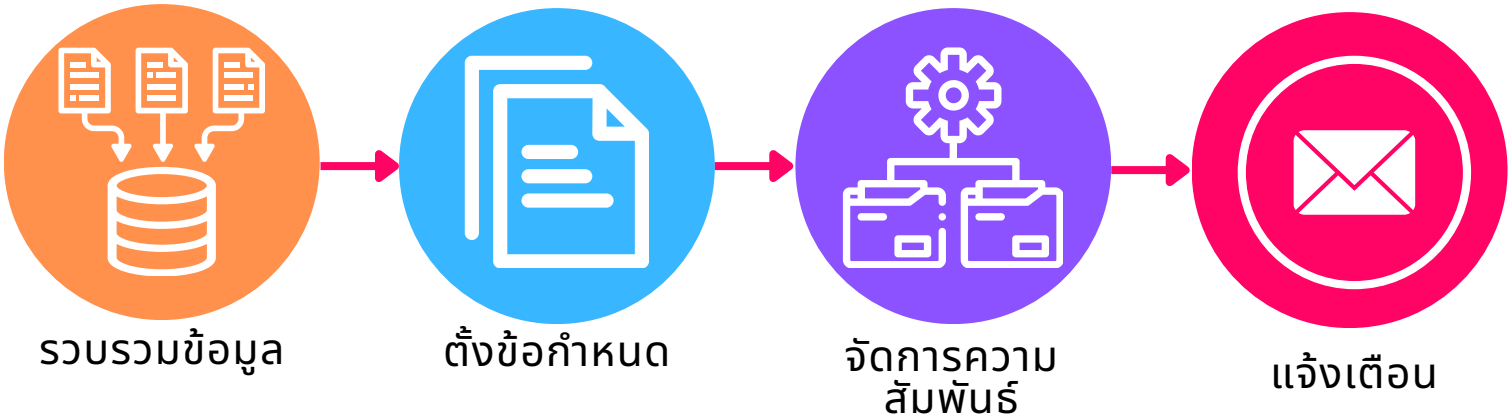
03

การแจ้งเตือน (Alerts & Notifications)

ถ้ามี event หรือ set ของ event trigger กับ SIEM rule ระบบจะแจ้งเตือนเจ้าหน้าที่ด้าน Security

04

SIEM



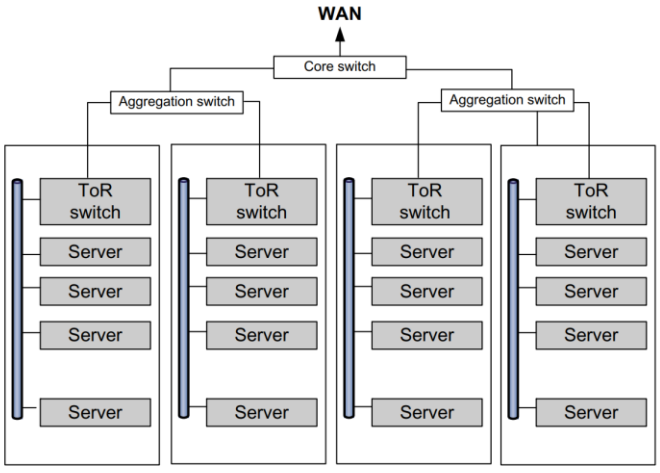
Software Defined Networking (SDN): ระบบเครือข่ายที่ถูกกำหนดด้วยซอฟท์แวร์

การเปลี่ยนแปลงทางเทคโนโลยี ในโลกเกิดขึ้นอย่างรวดเร็ว ทุกวันนี้การออกแบบครือข่ายที่เกิดขึ้นในรอบไม่กี่ทศวรรษที่ผ่านมานั้น มีทั้งซับซ้อนและความท้าทายป็นอย่างยิ่ง เพื่อที่จะตอบสนองการขยายตัวอย่างรวดเร็วของระบบงานและเทคโนโลยีต่าง ๆ ซึ่ง SDN หรือ Software Defined Network นั้นก็เป็น วิถีทางใหม่ที่ถูกออกแบบมาเพื่อตอบสนองและลดจุดอ่อนของของการใช้งานเครือข่ายในกรอบแนวคิดปัจจุบัน และ SDN นี้ก็เป็นแนวทางในการที่จะ program ไปที่ switch เพื่อควบคุมพฤติกรรมของเครือข่ายให้ทำงานตอบสนองการใช้เครือข่ายข้อมูลยุคใหม่(Modernized networks data) ได้อย่างมีประโยชน์และมีประสิทธิภาพสูงสุด

SDN นั้นใช้หลักการของการออกแบบเครือข่ายเพื่อรองรับการขยายตัวอย่างยิ่งยวด (hightly scalbility) และใช้สถาปัตยกรรมการควบคุมพฤติกรรมของเครือข่ายแบบรวมศูนย์ (centralized networks control architecture) ซึ่งมีความเหมาะสมกับพฤติกรรมของศูนย์ข้อมูล(Data Center) ที่ต้องรองรับระบบสารสนเทศและเทคโนโลยีในปัจจุบันที่ขยายตัวอย่างรวดเร็ว และนอกจากนั้นแทนที่จะปล่อยให้การใช้งานข้อมูลเฉพาะบางอย่างส่งไปด้วยสถาปัตยกรรมเครือข่ายแบบเดิมซึ่งไม่เหมาะสมกับการใช้งาน SDN จะใช้ข้อมูลต่าง ๆ เพื่อทำการกำหนดรูปแบบของเครือข่ายโดยการกำหนดแนวทางในการส่งต่อข้อมูลของ switch ให้มีประสิทธิภาพและเหมาะสมกับการใช้งานในรูปแบบเฉพาะต่าง ๆ

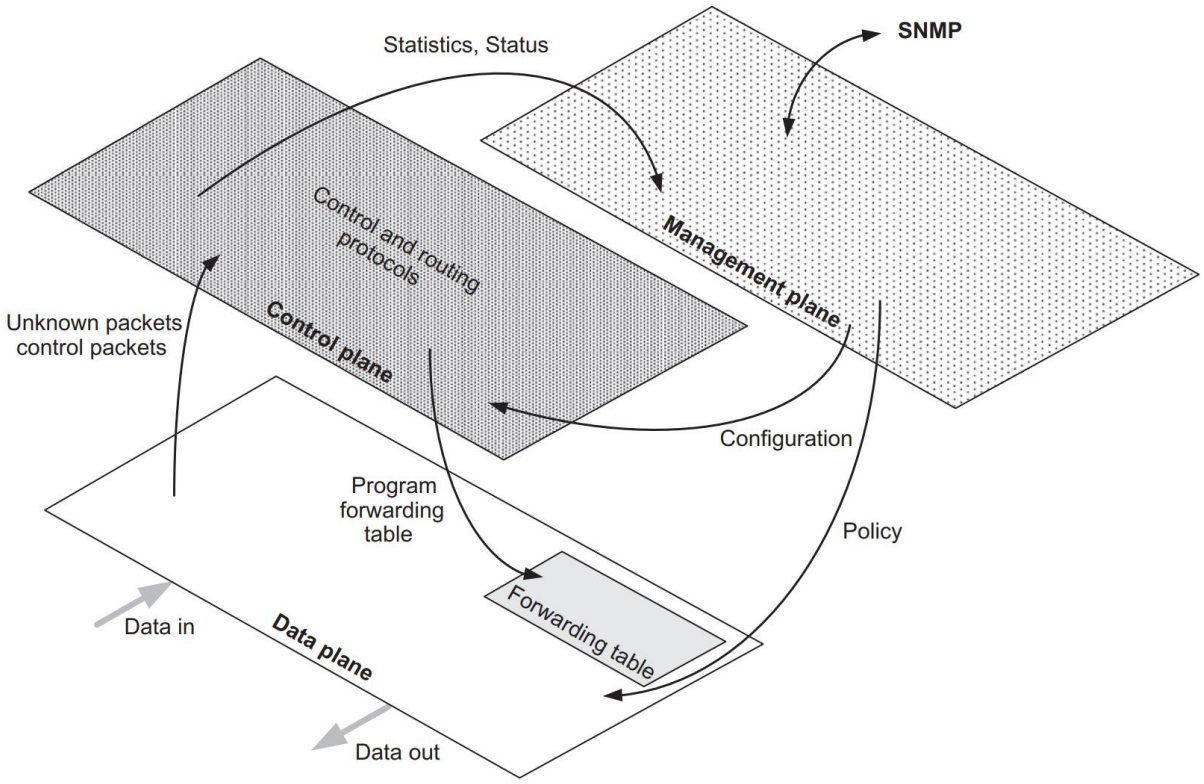
ความเป็นมาของ การใช้ Software Defined Networking(SDN)

ก่อนหน้านี้ โครงสร้างของระบบเครือข่ายมักจะประกอบด้วยอุปกรณ์ต่างๆ เช่น สวิตช์ รูเตอร์ และไฟร์วอลล์ที่มีการควบคุมและการทำงานอยู่ภายในอุปกรณ์เหล่านี้เอง ซึ่งทำให้การปรับแต่งและการจัดการเครือข่ายมักจะต้องทำผ่านการกำหนดค่าและการตั้งค่าในอุปกรณ์เหล่านั้นๆ ทำให้มีความยุ่งยากและซับซ้อนในการดูแลรักษาและการจัดการ และรวมถึงการใช้งาน protocol บางอย่างซึ่งอาจมีข้อจำกัดและทำให้เกิดปัญหาที่เรียกว่า Internet Ossification



ภาพสถาปัตยกรรมแบบเดิม

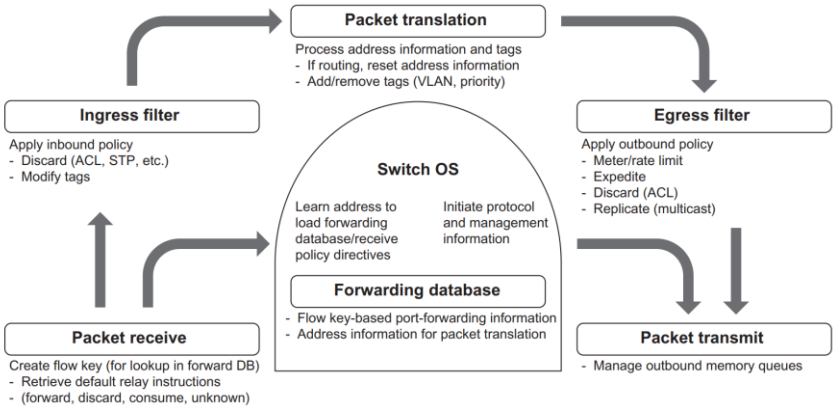
โดยสถาปัตกยกรรมแบบเดิมนั้น router หรือ switch นั้นจะทำการมีการแบ่งข้อมูลออกเป็น plan ต่าง ๆ ดังนี้



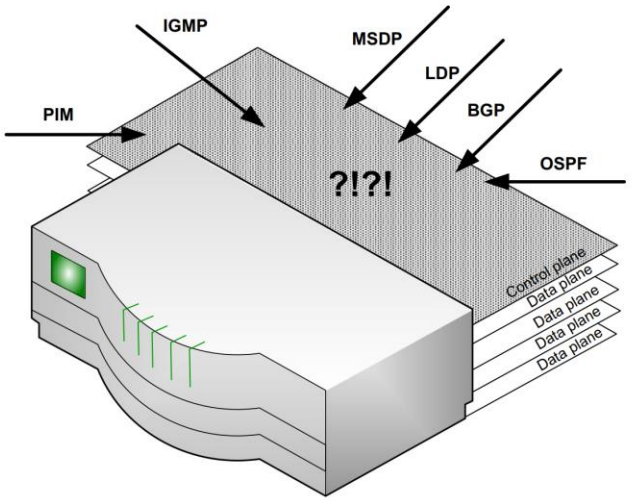
ภาพ การแบ่งหน้าที่การทำงานของ switch ออกเป็น plane ต่าง ๆ

1. Data Plane คือส่วนที่ทำหน้าที่ส่งต่อข้อมูลตามที่ มีการกำหนดไว้ใน Forwarding table
2. Control Plane คือส่วนที่ทำหน้าที่กำหนดหรือเลือกเส้นทางที่จะให้ข้อมูลนั้น ไหลไป
3. Management Plane คือส่วนที่ทำหน้าที่ในการรับส่งข้อมูลที่ใช้สำหรับตรวจสอบหรือบริหารจัดการ อุปกรณ์เครือข่าย

ทั้งนี้ในการทำงานของ switch หรือ router นั้นหากมองในเชิงของ ข้อมูล(packet) จะทำหน้า ดังภาพด้านล่าง

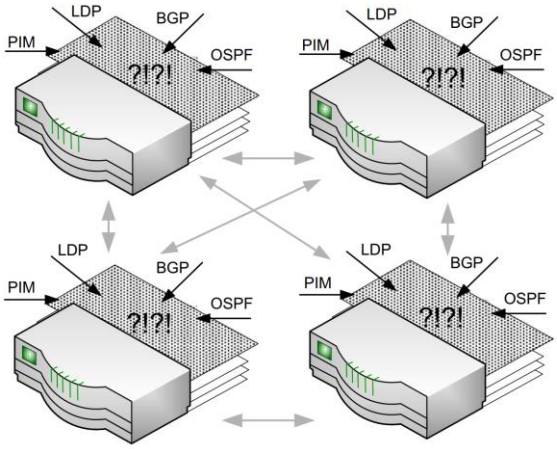


ดังนั้น ในการใช้งาน switch นั้นจะเกิดการทำงานหลายอย่าง และมีการแลกเปลี่ยนข้อมูลหลายอย่าง ที่ control plane



ภาพ โปรโตคอลต่าง ๆ ที่ ทำงานใน control plane

และหากนำ switch ไปต่อกัน หลาย ๆ ตัวจะพบว่าเกิด Overhead ขึ้นในระบบเครือข่ายดังภาพด้านล่าง

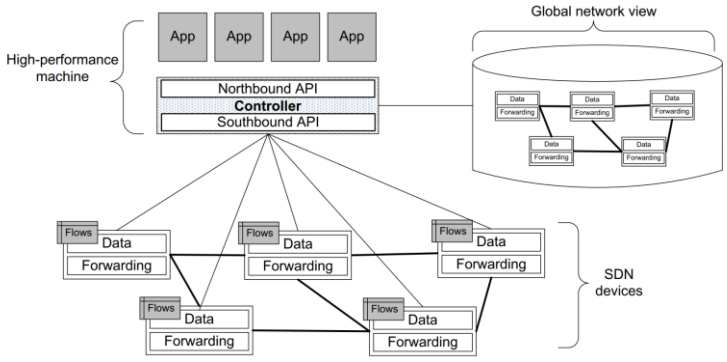


โครงสร้างของ SDN

SDN มีโครงสร้างที่แตกต่างออกไปจากระบบเครือข่ายทั่วไป โดยมีส่วนประกอบหลัก 2 ส่วนคือ

Data Plane (Forwarding Plane): เป็นส่วนของระบบเครือข่ายที่รับผิดชอบในการส่งข้อมูลไปมาระหว่างอุปกรณ์ ใน SDN ส่วนนี้จะไม่มีการประมวลผลควบคุมเพราะควบคุมจะถูกแยกออกมาอยู่ในส่วนของ Controller

Control Plane: เป็นส่วนที่ควบคุมการทำงานของ Data Plane โดยตรง ซึ่งประกอบด้วย SDN Controller ซึ่งมีหน้าที่ควบคุมการเปลี่ยนแปลงใน Data Plane ตามการกำหนดค่าและการตั้งค่าที่ได้รับ



ประโยชน์ของ SDN

ความยืดหยุ่นและความสามารถในการปรับเปลี่ยน: SDN ช่วยให้ง่ายต่อการปรับเปลี่ยนโครงสร้างของเครือข่ายเพื่อรองรับการใช้งานที่ต่างกันได้อย่างรวดเร็ว

การจัดการและการดูแลรักษาที่ง่ายขึ้น: ด้วยการควบคุมที่เป็นศูนย์กลาง ช่วยลดความซับซ้อนในการดูแลและการจัดการเครือข่าย

ประหยัดค่าใช้จ่าย: ช่วยลดค่าใช้จ่ายในการดูแลรักษาและการใช้งานของเครือข่าย

ความรวดเร็วและประสิทธิภาพ: การควบคุมแบบศูนย์กลางช่วยเพิ่มประสิทธิภาพและความรวดเร็วในการส่งข้อมูล

การใช้งาน SDN ในปัจจุบัน

SDN ได้รับความนิยมและได้รับการนำมาใช้งานในสถานการณ์ต่างๆ ไม่ว่าจะเป็นในองค์กร ศูนย์ข้อมูล หรือในโลกของระบบเครือข่ายมหาวิทยาลัย เพื่อช่วยให้การจัดการเครือข่ายเป็นไปอย่างมีประสิทธิภาพและรวดเร็วขึ้น

ดังนั้น SDN จึงเป็นเทคโนโลยีที่มีการเปลี่ยนแปลงทางเทคโนโลยีในโลกของเครือข่ายอย่างมีนัยสำคัญ ช่วยเพิ่มความยืดหยุ่น ความสามารถในการปรับเปลี่ยน และความง่ายในการจัดการและดูแลรักษาเครือข่ายในปัจจุบัน ทำให้เป็นที่นิยมและนำมาใช้งานในหลายสถานการณ์และองค์กรต่างๆ อย่างกว้างขวาง