

3 ขั้นตอนในการทำ เน็ตเวิร์กเวอร์ชวลไลเซชัน

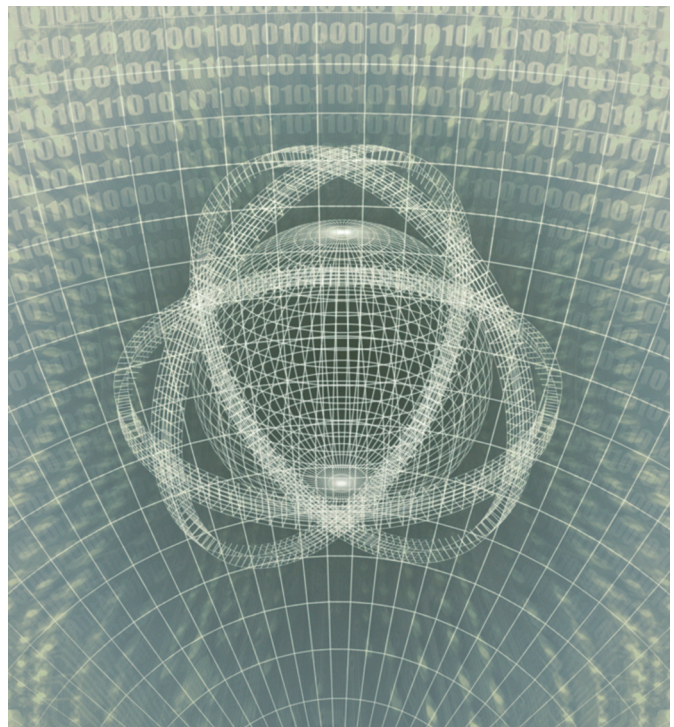
สำเร็จได้ด้วยสวิตช์ Catalyst 6500 Series

เมื่อองค์กรต่างๆ ทำการขยายเครือข่าย ติดตั้งแอปพลิเคชันใหม่ๆ รวมทั้งเพิ่มความเร็วของระบบเก็บข้อมูลให้สูงขึ้น ทำให้จำนวนอุปกรณ์ในศูนย์ข้อมูล (Data Center) เพิ่มขึ้นอย่างรวดเร็ว โดยที่อุปกรณ์หลายๆ ตัวซึ่งมีคุณสมบัติเหมือนกันมีอัตราการใช้งานของแต่ละตัวไม่มากนัก ส่งผลให้สิ้นเปลืองเวลา และงบประมาณของฝ่ายไอทีไปมีใช้น้อย เราจะทำอย่างไรเพื่อจะสามารถใช้งานทรัพยากรเครือข่ายให้มีอัตราการใช้งานที่สูงขึ้น?

การแปลงอุปกรณ์เครือข่ายให้เป็นแบบเสมือน (Virtualization)

ตัวอย่างของ Virtualization ที่ผู้ใช้งานส่วนใหญ่คุ้นเคยกันดี เช่น การจัดสรรระบบเครือข่ายโดยการแปลงระบบแลน (LAN) ในองค์กรเป็นแลนเสมือน (virtual LANs - VLANs) ซึ่งปัจจุบัน Cisco ได้ขยายความสามารถในการทำ Virtualization ไปในอุปกรณ์อื่นๆ ตัวอย่างเช่น ในเครือข่ายระบบเก็บข้อมูล (Storage Area Network - SAN) Cisco ได้นำระบบสวิตช์แบบมัลติดีเลย์อร์ Cisco MDS 9000 Series เข้ามาใช้ควบรวมฮาร์ดดิสก์อาร์เรย์ (Storage Array) หลายๆ ชุดลงบนเครือข่ายระบบเก็บข้อมูลเดียวกัน โดยแบ่งสรรเป็นหลายๆ Virtual SANs (VSANs) เพื่อตอบสนองความต้องการของระบบเก็บข้อมูลที่มีความจุสูงเพิ่มขึ้นอย่างรวดเร็ว

ปัจจุบันนี้การทำระบบเครือข่ายเสมือนนั้นฉลาดขึ้นกว่าเดิมมาก บริษัทที่มีความจำเป็นในการขยายศูนย์ข้อมูล (ขนาดใหญ่ขึ้นและมีความซับซ้อนมากขึ้น) มีการติดตั้งแอปพลิเคชันจำนวนมาก การเป็นพันธมิตรกับบริษัทอื่น และการปฏิบัติตามกฎระเบียบมาตรฐานสากลต่างๆ จะพบว่าระบบเครือข่ายของตนเองจะมีความซับซ้อนมากขึ้น เทคนิคเวอร์ชวลไลเซชันหลายรูปแบบบนสวิตช์ Cisco Catalyst 6500 Series สามารถช่วยตอบปัญหาที่เกิดกับการติดตั้งแอปพลิเคชัน และนโยบายความปลอดภัย กับเครือข่ายที่มีความซับซ้อนเหล่านั้นได้เป็นอย่างดี ตัวอย่างเช่น Cisco Application Control Engine (ACE) ซึ่งติดตั้งได้ใน Cisco Catalyst 6500 series ได้รวมเอาฟังก์ชันของอุปกรณ์เครือข่ายหลายๆ ตัว เช่น Load Balancer, Firewall และ SSL off-load ไว้ด้วยกัน แล้วเปิดโอกาสให้เลือกฟังก์ชันต่างๆ ข้างต้น และแบ่งสรรทรัพยากรของ ACE ลงบนแต่ละเวอร์ชวล (ดูรูปประกอบ) โดยแต่ละเวอร์ชวล มีคุณสมบัติการทำงานเป็นอิสระแยกจากกันโดยสมบูรณ์



การทำเน็ตเวิร์กเวอร์ชวลไลเซชันนั้น สามารถแบ่งออกได้เป็น 3 ขั้นตอน คือ ควบคุมการเข้าถึง การแบ่งแยกเส้นทางของข้อมูล และการบังคับใช้นโยบาย

ขั้นตอนแรก: ควบคุมการเข้าถึง

การเพิ่มขึ้นของปริมาณและช่องทางการติดต่อสื่อสารกับลูกค้าและพันธมิตรทางธุรกิจในปัจจุบัน ทำให้เกิดความจำเป็นในการกำหนดสิทธิ์ในการเข้าถึงแอปพลิเคชันต่างๆ ไว้หลายระดับ ตัวอย่างเช่น ผู้มาติดต่อนั้นมักจะได้รับสิทธิ์ "guest" ในการเข้าใช้อินเทอร์เน็ตทั้งทางแลนและแบบไร้สาย ซึ่งพหลายเออร์หรือผู้ผลิตให้เราตามสัญญา (ซึ่งอาจทำงานให้กับคู่แข่งทางธุรกิจของเราด้วยก็ได้) ก็เป็นอีกปัจจัยหนึ่งที่ทำให้ระบบเครือข่ายของเราต้องยืดออกไปนอกขอบเขตทางกายภาพของบริษัท เป็นต้น ความยุ่งยากซับซ้อนในการกำหนดสิทธิ์การเข้าระบบเครือข่ายเหล่านี้หลายๆ ครั้ง มักจะลงเอยด้วยการสร้างระบบเครือข่ายหลายๆ วง แยกกัน ก่อให้เกิดความซับซ้อนในการจัดการ และยิ่งเกิดความซ้ำซ้อนในการลงทุนของอุปกรณ์และเซอวิสต่างๆ อย่างมากมาย

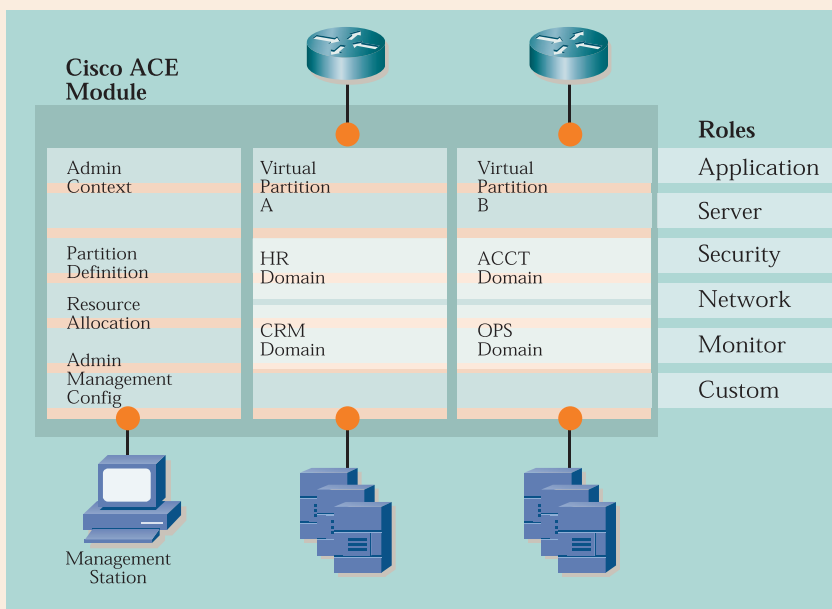
มาตรฐานการพิสูจน์ตัวตน IEEE 802.1X port authentication ที่มีอยู่ใน Catalyst 6500 Series สามารถควบคุมการเข้าถึงระดับกายภาพ เมื่อพิสูจน์ทราบตัวตนของผู้ใช้ หรือเครื่องที่เชื่อมต่อเข้ามาแล้ว ก็สามารถกำหนด (อนุญาตหรือปฏิเสธ) สิทธิ์การเข้าถึง รวมทั้งกำหนดเงื่อนไขในการเข้าใช้เครือข่ายด้วย ตัวอย่างเช่น ผู้ใช้งานเครือข่ายที่เชื่อมต่อเข้าสู่ VPN (ซึ่งสามารถมองได้ว่าเป็นเวอร์ชวลไลเซชันของเน็ตเวิร์กรูปแบบหนึ่ง) จะถูกจำกัดการใช้งานไว้เฉพาะในส่วนที่อนุญาตเท่านั้น เป็นต้น

Rice University ในเมืองฮูสตัน มลรัฐเท็กซัสใช้ฟังก์ชันนี้ในการแยกแยะการใช้อินเทอร์เน็ตของนักศึกษา ออกจากเครือข่ายของแผนกต่างๆ และเครือข่ายการวิจัยระหว่างมหาวิทยาลัย William Deigaard ผู้อำนวยการฝ่ายปฏิบัติการของศูนย์ข้อมูลและโทรคมนาคมเครือข่ายของ Rice University กล่าวว่า "เมื่องานวิจัยของทางคณะ และความคาดหวังของนักศึกษาทวีจำนวนมากขึ้น ความจำเป็นในการติดตั้งระบบเชื่อมโยงอินเทอร์เน็ตที่มีความปลอดภัยและเสถียรภาพสูงก็ทวีขึ้นไม่แพ้กัน เรานำ Catalyst 6500 มาใช้เพื่อจัดสรรเครือข่ายให้เป็นหลายๆ วง แล้วกำหนดเงื่อนไขการใช้งานให้แต่ละวงไม่ซ้ำกัน เราใช้ความสามารถของเครือข่ายเสมือนในการจัดการและคุ่มกันเครือข่ายของทางมหาวิทยาลัย รวมทั้งพิสูจน์ตัวตนให้ทราบว่าเป็นใคร และในขณะที่เดียวกันก็สามารถให้บริการกับผู้มาติดต่ออย่างราบรื่น

ขั้นที่ 2: การแบ่งแยกเส้นทางของข้อมูล

ขั้นตอนที่ 2 ในการทำเน็ตเวิร์กเวอร์ชวลไลเซชันคือการแยกแยะเส้นทางของข้อมูล (traffic flow) ที่หลากหลาย เนื่องด้วยระเบียบข้อกฎหมาย และระดับความลับของข้อมูล ทำให้จำเป็นต้องแยกแอปพลิเคชันที่ใช้เฉพาะบางแผนก (เช่น ฝ่ายการเงิน และฝ่ายบุคคล) ออกเป็นเอกเทศจากกัน Catalyst 6500 Series จัดการแยกแยะในลักษณะนี้ผ่านทาง VLANs และการทำสวิตชิงในเลเยอร์ 2 และ 3 และใช้การ

คุณสมบัติการควบคุมโครงสร้างพื้นฐานทางต้นแอปพลิเคชันของ Cisco ACE



หมายเหตุ: Cisco ACE รองรับฟังก์ชันของอุปกรณ์เครือข่ายมากมายไว้ด้วยกัน

Cisco ACE ช่วยให้อเนกประสงค์ของการขยายระบบแบบโมดูลาร์เติบโต

Cisco ACE สำหรับ Catalyst 6500 สามารถแบ่งทรัพยากรออกเป็น 250 เวอร์ชวลพาร์ทิชัน โดยในแต่ละพาร์ทิชันนั้นสามารถกำหนดตามประเภทลูกค้า องค์กรธุรกิจ แอปพลิเคชัน หรือการจัดสรรทรัพยากร (อย่างเช่น แบนด์วิดท์หรือจำนวนของการเชื่อมต่อ ณ ขณะใดขณะหนึ่ง)

การควบคุมการเข้าถึงโดยอิงกับหน้าที่ (Role-Based Access Control - RBAC) ของ Cisco ACE ช่วยให้สามารถจัดสรรให้กับธุรกิจหรือเจ้าหน้าที่ฝ่ายไอทีที่เหมาะสม สามารถเข้าไปบริหารจัดการแต่ละเวอร์ชวลพาร์ทิชันได้ โดยภายในแต่ละเวอร์ชวลพาร์ทิชันนั้นสามารถสร้างโดเมน (ประเภทของสิทธิ์) เพื่อการจัดการได้ถึง 10 โดเมน จึงช่วยให้การควบคุมสิทธิ์ภายในเวอร์ชวลพาร์ทิชันนั้นๆ เป็นไปอย่างละเอียด ตัวอย่างเช่น เจ้าหน้าที่ดูแลเครือข่ายสามารถกำหนดค่าตัวแปรของเลเยอร์ 3 ได้ เจ้าหน้าที่ดูแลระบบความปลอดภัยสามารถควบคุมกฎตามชนิดของแอปพลิเคชัน องค์กรธุรกิจ หรือประเภทผู้ใช้งาน บนพาร์ทิชันกลาง หรือระบุพาร์ทิชันใดเป็นการเฉพาะเจาะจงก็ได้ ในขณะที่เจ้าหน้าที่แพนเอมพลีเคชันและเซิร์ฟเวอร์สามารถเฝ้าติดตามและจัดการเวอร์ชวลเซิร์ฟเวอร์ได้โดยไม่มีผลกระทบต่อการทำงานของด้านไอทีอื่นๆ และสามารถนำเซิร์ฟเวอร์เข้าไปใช้งานหรือนำออกมาเพื่อการบำรุงรักษาได้

ความยืดหยุ่นของ RBAC เช่นนี้ช่วยให้ทำการติดตั้งเซิร์ฟเวอร์ได้รวดเร็วยิ่งขึ้น การทำเวิร์กโฟลว์ในฝ่ายไอทีก็ง่ายขึ้น และลดข้อผิดพลาดในการกำหนดค่าได้อีกด้วย ระบบความปลอดภัยแบบรวมศูนย์ช่วยให้เกิดการบังคับใช้ที่เป็นไปในทิศทางเดียวกันทุกๆ ภาคส่วนขององค์กร นอกจากนี้ยังช่วยลดความซับซ้อนและลดค่าใช้จ่ายในการดำเนินงาน ซึ่งเกิดขึ้นจากการใช้โมบายที่แตกต่างกันหลายๆ ตัว

นอกจากนี้ซอฟต์แวร์ Cisco Application Networking Manager (ANM) ซึ่งเป็นแพ็คเกจการจัดการที่รันบนเซิร์ฟเวอร์ยังช่วยให้การจัดการเวอร์ชวลพาร์ทิชันของ Cisco ACE ย่ำลงอีกด้วย

Cisco ANM นั้นช่วยให้การกำหนดค่า บำรุงรักษา การปฏิบัติการ และการเฝ้าติดตามประสิทธิภาพของเวอร์ชวลพาร์ทิชันภายใน หรือข้ามโมดูลของ Cisco ACE เสร็จสิ้นได้ด้วยแอปพลิเคชันนี้เพียงตัวเดียว การกำหนดค่าบนแพลตฟอร์มช่วยให้องค์กรสามารถแบ่งพาร์ทิชันให้แก่แอปพลิเคชันได้อย่างรวดเร็ว ผู้ดูแลระบบหลายๆ คน (เข้าระบบพร้อมๆ กัน) สามารถเข้าไปยังพาร์ทิชันและโมดูลใดๆ ได้อย่างไม่ยากเย็น ดังนั้น การแบ่งพาร์ทิชันจึงช่วยลดจำนวนการกำหนดค่าและทำซ้ำขึ้น อีกทั้งยังช่วยลดโอกาสของการเกิดข้อผิดพลาดอีกด้วย

แบ่งแยกแยะเส้นทางหลากหลายประเภทสำหรับแต่ละกลุ่มผู้ใช้งาน เช่น การใช้ Generic Routing Encapsulation (GRE) เพื่อใช้สร้างกลุ่มผู้ใช้ที่ต้องจำกัดวงไม่ก็กลุ่มในเครือข่ายของมหาวิทยาลัย (ตัวอย่างเช่น การเข้าใช้ VLAN ด้วยสิทธิ์ guest) หรือจะใช้เทคนิค VPN Routing and Forwarding (VRF-lite) เพื่อการแบ่งเซกเมนต์ของมหาวิทยาลัย โดยไอพีแอดเดรสใน VPN แต่ละวงสามารถให้ซ้ำกันได้ (แต่ละวงสามารถกำหนดไอพีของตนได้อย่างอิสระ) หรือจะเป็นเทคนิค Multiprotocol Label Switching (MPLS) ซึ่งใช้เพื่อสร้างกลุ่มผู้ใช้ผ่านทาง VPN ที่เป็นอิสระจากกันระหว่างแต่ละ VPN บนแกนกลาง (core) ของระบบเครือข่าย (VPN ทุกวงสามารถกำหนดค่าให้เชื่อมต่อกับผู้ใช้และทรัพยากรจากที่ใดก็ได้ภายในเครือข่าย)

Unique Zurich Airport ผู้ดูแลสนามบินซูริกซ์ในสวิตเซอร์แลนด์ต้องการเครือข่ายที่สามารถสนับสนุนแอปพลิเคชันหลากหลายประเภท เช่น การใช้เครือข่ายไร้สายสาธารณะ การดำเนินงานสายการบิน และการควบคุมจราจรทางอากาศที่ปลอดภัยสูงสุด เพื่อให้บริการแก่บริษัทต่างๆ 180 แห่ง วิศวกรที่องค์กรต่างๆ ไปใช้กันมักจะมีปัญหาด้านความยืดหยุ่นในการปรับใช้หรือการแก้ไขปัญหาเบื้องต้น ผู้ให้บริการเครือข่ายโทรคมนาคม (Service Provider) หลายรายได้ใช้ MPLS VPN ในการให้บริการเพื่อตอบสนองปัญหาข้างต้นมาเป็นเวลาก่อนหน้าหลายปี แต่สวิตช์ระดับองค์กรส่วนใหญ่ไม่มีฟังก์ชันนี้ คุณสมบัติเวอร์ชวลไลเซชันที่ปัจจุบันมีอยู่ใน Catalyst 6500 Series สามารถช่วยให้สนามบินซูริกซ์ใช้ MPLS VPN เพื่อสนับสนุนการเชื่อมต่อทางเครือข่ายหลากหลายรูปแบบ รวมทั้งตอบ

สนองความต้องการประสิทธิภาพหลายระดับพร้อมกัน บนเน็ตเวิร์กเวอร์ชวลพาร์ทิชันจำนวนมาก ทั้งหมดนี้รวมอยู่ในเครื่องฮาร์ดแวร์เพียงเครื่องเดียวเท่านั้น

Peter Zopfi หัวหน้าแผนกวิศวกรรมสื่อสารของ Unique กล่าวว่า เครือข่ายที่ใช้ Catalyst 6500 ของซิสโก้ ซึ่งติดตั้งอยู่ที่สนามบินซูริกซ์ช่วยให้เราสามารถนำเสนอบริการเครือข่าย (ในระดับมาตรฐานเดียวกับที่บริษัทผู้ให้บริการเครือข่ายโทรคมนาคมทั่วไปใช้กัน) แก่ลูกค้าทั้งหลายของสนามบินซูริกซ์ ได้แก่ สายการบิน ฝ่ายปฏิบัติการสนามบินและบริการเสริมอื่นๆ สรุปได้ว่าเป็นเทคโนโลยีระดับเดียวกับผู้ให้บริการเครือข่ายในราคาเท่ากับระบบเครือข่ายในองค์กรเท่านั้น

แอปพลิเคชันจำนวนมากขึ้น ย่อมต้องการความเสถียรยิ่งขึ้น

สิ่งที่มีผลกระทบต่อประสิทธิภาพของแอปพลิเคชันอย่างมากก็คือจำนวนของเซิร์ฟเวอร์ที่เซิร์ฟเวอร์ต้องรันเพิ่มขึ้น กิจกรรมอย่างเช่น การเข้ารหัส/ถอดรหัส Secure Sockets Layer (SSL) การทำออปติไมเซชัน TCP การตรวจสอบเพื่อความปลอดภัยหลายระดับ และการประมวลผลที่เกี่ยวข้องกับภาพ เสียง และวิดีโอจำนวนมาก จะใช้ทรัพยากรของเซิร์ฟเวอร์ค่อนข้างมาก

โมดูลเซิร์ฟเวอร์ ACE ใน Catalyst 6500 ของซิสโก้สามารถเลือกทำโหนดบาลานซ์แอปพลิเคชันไปยังกลุ่มเซิร์ฟเวอร์อย่างชาญฉลาด ด้วยประสิทธิภาพที่นำหน้าคู่แข่งในตลาด

ทั้งเรื่องของปริมาณการส่งข้อมูลต่อวินาที (Throughput) และ อัตราสร้างการเชื่อมต่อ (Connection Setup Rate) นอกจากนี้แล้ว ACE สามารถเพิ่มประสิทธิภาพได้ด้วยการอัปเดตไลเซนส์ของซอฟต์แวร์ ดังนั้น ผู้ใช้งานจึงสามารถเลือกซื้อไลเซนส์ของอุปกรณ์ได้ตามความต้องการใช้งานจริง เมื่อจำเป็นต้องใช้งานเพิ่มขึ้น ก็สามารถซื้อไลเซนส์เพื่ออัปเดตที่หลังได้บนฮาร์ดแวร์เดิม ทำให้ผู้ใช้งานไม่จำเป็นต้องลงทุนจำนวนมากตั้งแต่ตอนเริ่มต้น

ด้วยคุณสมบัติเวอร์ชวลพาธิชัน (ได้สูงสุดถึง 250 พาธิชันต่อโมดูล) Cisco ACE ช่วยให้ผู้ใช้ดูแลระบบสามารถควบคุมการทำงานของระบบเครือข่ายให้สามารถรองรับแอปพลิเคชันได้อย่างราบรื่น สำหรับในแต่ละเวอร์ชวลพาธิชันนั้น ผู้ดูแลระบบสามารถกำหนดค่าทรัพยากรในการประมวลผล แบนด์วิดท์ อัตราการสร้างการเชื่อมต่อ อัตราการส่งข้อมูล SSL อัตราปริมาณการส่ง syslog ทรัพยากรหน่วยความจำ จำนวนการเชื่อมต่อ ณ ขณะใดขณะหนึ่ง (concurrent connections) รายการควบคุมการเข้าถึง (ACL) และอื่นๆ อีกมากมาย ดังนั้นองค์กรธุรกิจ ลูกค้า/สมาชิก และแอปพลิเคชันสามารถแบ่งสรรการใช้งานโมดูล ACE ได้โดยอิสระและไม่ปะปนกัน

ที่สำคัญที่สุด ผู้ประกอบการที่ใช้เวอร์ชวลพาธิชันสามารถสั่งรันแอปพลิเคชันหรือเซอวิสตัวใหม่ได้ด้วยการคลิกเพียงไม่กี่ครั้ง โดยไม่จำเป็นต้องผ่านขั้นตอนยุ่งยาก และใช้เวลานานในการเลือก ปรับแต่ง ติดตั้ง และแก้ปัญหาเบื้องต้น ซึ่งตามมากับการจัดซื้ออุปกรณ์ตัวใหม่

Cisco ACE ได้นำเทคนิคการทำออปติไมเซชันมาใช้หลายเทคนิค ตัวอย่างเช่น TCP หลายๆ การเชื่อมต่อ (TCP connection) สามารถควบคุมรวมเข้าไว้ใน การเชื่อมต่อไม่มีการเชื่อมต่อสำหรับเซิร์ฟเวอร์แต่ละตัว เพื่อว่าการเชื่อมต่อ TCP ของไคลเอนต์ตัวใหม่จะได้ไม่ต้องเปลืองทรัพยากรของเซิร์ฟเวอร์มากไปกว่าเดิม หรือเรื่องของเซสชัน SSL ที่สามารถถูกจัดการได้โดยตรงโดย Cisco ACE ช่วยเพิ่มความยืดหยุ่นเพิ่มปริมาณการรองรับ SSL และลดภาระของเซิร์ฟเวอร์

การทำระบบสำรองของโมดูลนั้น สามารถเลือกทำได้ทั้งบนแชสซีเดียว หรือจะข้ามแชสซีภายในศูนย์ข้อมูลเดียวกัน หรือข้ามศูนย์ข้อมูลเลยก็ได้ ACE นำเสนอความสามารถเฉพาะตัวในการป้องกันในระดับแอปพลิเคชันต่อ

SONA: ปรับเปลี่ยนรูปแบบมาสู่การใช้งาน

เวอร์ชวลไลเซชันเป็นส่วนสำคัญของ Cisco Service-Oriented Network Architecture (SONA) ซึ่งจัดทำโครงสร้างเพื่อช่วยให้องค์กรต่างๆ สามารถสร้างเครือข่ายที่คลาดยิ่งขึ้น ชับซ้อนน้อยลง และมีประสิทธิภาพมากขึ้น ส่งผลให้สามารถประหยัดงบประมาณในด้านโครงสร้างพื้นฐานเพื่อนำไปใช้กับด้านแอปพลิเคชันและเซอร์วิสอื่น ซึ่งเป็นการเพิ่มศักยภาพในการทำงานและเพิ่มความได้เปรียบในการแข่งขัน

SONA ได้รับการออกแบบให้มักจะเป็นแบบโมดูล เมื่อองค์กรได้นำไปใช้งานสามารถให้ผลตอบแทนที่คุ้มค่าการลงทุน นอกจากนี้ยังคงสภาพการออกแบบเครือข่ายเดิมไว้อีกด้วย สามารถหาข้อมูลเพิ่มเติมได้ที่ www.cisco.com/go/sona

แอปพลิเคชันผ่านทางโมดูล ACE สองตัว (High Availability) โดยใช้เวอร์ชวลพาธิชัน

ขั้นตอนที่ 3: การบังคับใช้นโยบาย

โมดูล Integrated services ของ Catalyst 6500 Series ช่วยให้สามารถบังคับใช้นโยบายจากส่วนกลางได้ ยกตัวอย่างเช่น ฟังก์ชันไฟร์วอลล์บน ACE ซึ่งสามารถทำเป็นแบบเวอร์ชวลได้ รองรับการทำการตรวจสอบ (inspection) และการใช้งาน (fixup) โพรโตคอลต่างๆ ที่เป็นที่ยอมรับในศูนย์ข้อมูล เช่น HTTP, FTP, RSTP, ICMP, DNS เป็นต้น รองรับการทำ NAT (Network Address Translation) ได้ถึง 1 ล้าน NAT และเพิ่มกฎควบคุมการเข้าถึง (Access Control List) ได้จนถึง 256,000 ข้อ ซึ่งจำนวน NAT และกฎเหล่านี้สามารถแบ่งสรรไปสู่หลายๆ เวอร์ชวลพาธิชันได้ ในกรณีที่มีความจำเป็นต้องใช้ฟังก์ชันไฟร์วอลล์ที่รองรับจำนวนแอปพลิเคชันโพรโตคอลได้หลายๆ โพรโตคอล Cisco Catalyst 6500 Firewall Services Module (FWSM) สามารถรองรับจำนวนของโพรโตคอลที่กว้างกว่าสำหรับการทำไฟร์วอลล์ให้แก่ อินเทอร์เน็ตและอินเทอร์เน็ต นอกจากนี้ยังสามารถทำไฟร์วอลล์แบบลอคจิคอลหลายๆ ตัวบนแพลตฟอร์มฮาร์ดแวร์แบบฟิสิคัลเพียงตัวเดียวโดยใช้เทคนิคเวอร์ชวลไลเซชันโมดูล ACE ทำงานร่วมกับ FWSM เพื่อทำโหนดบาลานซ์ไฟร์วอลล์ หรือให้ FWSM ช่วยป้องกันไม่ให้โพรโตคอลที่ ACE ไม่ได้รองรับเข้ามาได้

โดยทั่วไปคุณสมบัติเวอร์ชวลไลเซชันในสวิตช์ Cisco Catalyst 6500 Series ช่วยให้องค์กรของคุณสามารถแบ่งสรรทรัพยากรเครือข่ายได้ในขณะที่ยังคงรักษาความลับข้อมูลระหว่างแต่ละแอปพลิเคชัน องค์กร กลุ่ม หรือบุคคล ให้มีความปลอดภัยแยกจากกันโดยสมบูรณ์ การส่งข้อมูลในระหว่างแผนก ลูกค้า และซัพพลายเออร์ผ่านเครือข่ายสามารถแบ่งสรรได้แบบลอคจิคอลโดยไม่จำเป็นต้องสร้างเครือข่ายโอเวอร์เลย์หรือติดตั้งอุปกรณ์แยกต่างหากอีก ทำให้แอปพลิเคชันที่มีความสำคัญมากๆ สามารถติดตั้งได้โดยใช้ทั้งทรัพยากรและเวลาที่น้อยลง และโครงสร้างพื้นฐานของแอปพลิเคชันนั้นก็พร้อมที่จะให้ผู้ดูแลระบบที่มีหน้าที่ต่างๆ กันในแผนกไอทีดูแลเฉพาะส่วนที่ตัวเองเกี่ยวข้องได้ทันที ■

อ่านเพิ่มเติม

- [cisco network Virtualization solutions](http://cisco.network.Virtualization.solutions)
http://cisco.com/en/US/netsol/ns658/networking_solutions_package.html