# MPLS VPN ที่ปลอดภัยอย่างแท้จริง

## MPLS VPN มีระบบรักษาความปลอดภัยพอๆ กับเฟรมรีเลย์ และเอทีเอ็ม

องค์กรต่างๆ พอใจกับผลดีในเรื่องของความสามารถการให้บริการ และค่าใช้จ่ายที่ประหยัดได้จากการใช้บริการระบบเครือข่ายส่วนตัวเสมือนจริง (virtual private network - VPN) ที่ใช้เทคโนโลยีแบบ Multi Protocol Label Switching (MPLS) เนื่องจากระบบมีความปลอดภัยพอๆ กับเทคโนโลยีเฟรมรีเลย์ และเอทีเอ็ม และยิ่งได้รับการบริการจากผู้ให้บริการ (Service Provider) โดยบริษัทที่ได้รับการรับรองโดย Cisco Powered Network จะช่วยให้การโจมตีแบบพื้นฐานต่างๆ เช่น Denial of Services (DoS) และ spoofing ทำได้ยากขึ้นหรือทำไม่ได้เลย

หลายบริษัทยังคงมีความเชื่อแบบผิดๆ เกี่ยวกับระบบรักษาความปลอดภัยของเทคโนโลยี MPLS อยู่ สิ่งที่เข้าใจผิดมากที่สุดก็คือ IP VPN ที่อยู่บน MPLS ยังไม่ปลอดภัย แต่ที่จริงแล้ว MPLS ช่วยเสริมสร้างความแข็งแกร่งให้แก่ระบบเครือข่ายไอพีปกติ โดยมีความสามารถในการสร้าง Virtual Routing table แยกเฉพาะสำหรับลูกค้าแต่ละราย และมีการใช้ Label ในการส่งข้อมูลซึ่งทำให้ VPN แต่ละ VPN ของลูกค้าแต่ละรายนั้นสามารถที่จะใช้ระบบแอดเดรส แบบไพรเวทไอพีที่ซ้ำกันได้ โดยไม่ทำให้การรับส่งข้อมูลผิดพลาด พร้อมทั้งการทำแพ็กเก็ตฟิลเตอริง อีกทั้งยังสามารถที่จะซ่อนเครือข่ายของผู้ให้บริการ (Service Provider Network) จาก VPN ของผู้ใช้ ทำให้เครือข่ายของผู้ให้บริการปลอดภัยจากการถูกโจมตี

ความเชื่อแบบผิดๆ อีกอย่างหนึ่งก็คือกลัวว่าลูกค้ารายอื่นของบริษัทผู้ให้บริการสามารถเจาะเข้าไปใน VPN ของเราได้ เรื่องนี้เป็นไปไม่ได้เนื่องจาก MPLS VPN จะแยกเราติงเทเบิลออกจากกันโดยเด็ดขาด ความเข้าใจผิดเรื่องที่สามก็คือ MPLS VPNs มีโอกาสถูกโจมตี DoS จากอินเทอร์เน็ตภายนอกได้โดยง่าย เรื่องนี้ก็ไม่เป็นความจริงเช่นกัน เนื่องจากระบบเครือข่าย MPLS VPN มี นั้นมีการแยกเราติงเทเบิลของลูกค้าออกจากโกลบอลเราติงเทเบิลที่เก็บเส้นทางการส่งข้อมูลของ CORE เน็ตเวิร์กและเส้นทางไปสู่อินเทอร์เน็ต ซึ่งถ้าลูกค้าใช้บริการ VPN อย่างเดียวแต่ไม่ได้ใช้ต่ออินเทอร์เน็ตก็เป็นไปไม่ได้เลยที่ VPN ของลูกค้าจะโดนโจมตีจากอินเทอร์เน็ตภายนอก

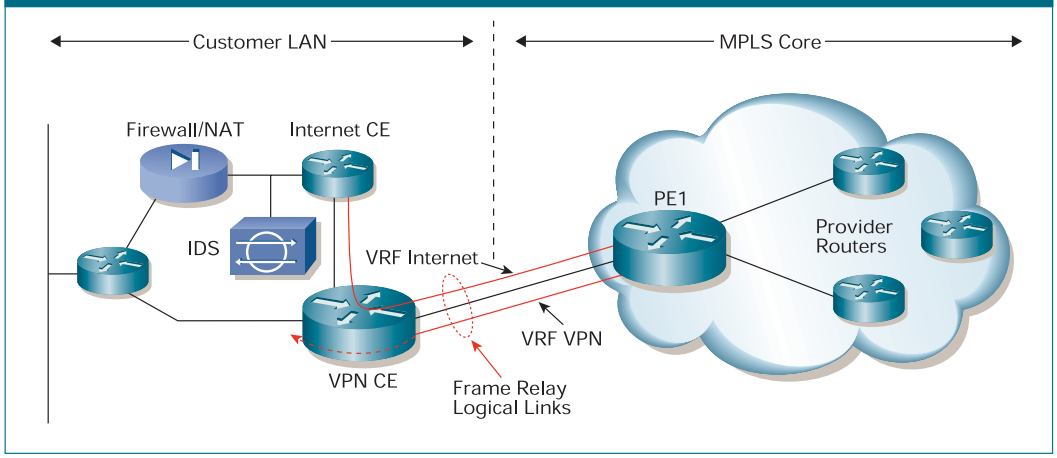
### การใช้ MPLS VPN ไม่ต้องเปลี่ยนระบบ Addressing

สำหรับองค์กรใหญ่ๆ ซึ่งมีการนำเอาไพรเวทไอพีแอดเดรสเข้ามาใช้กำหนดให้กับอุปกรณ์เครือข่ายภายในเองก็ดี หรือกำหนดให้เครื่องเดสก์ทอป และเซิร์ฟเวอร์ต่างๆ ด้วยเหตุผลในเรื่องของความปลอดภัย และในเรื่องของค่าใช้จ่าย องค์กรต่างๆ เมื่อหันมาใช้ VPN จึงไม่อยากที่จะเปลี่ยนแปลงระบบไอพีแอดเดรสที่ใช้อยู่ ซึ่ง MPLS VPN มีข้อดีที่รองรับกับความต้องการนี้ กล่าวคือ MPLS VPN ยอมให้องค์กรแต่ละองค์กรนั้นสามารถใช้ไพรเวทไอพีแอดเดรสชุดที่ซ้ำกันได้ (RFC 1918) ซึ่งโดยปกติแล้วระบบไอพีเน็ตเวิร์กทั่วๆ ไปนั้นจะไม่ยอมให้เครือข่ายที่มาเชื่อมต่อนั้นมีไอพีแอดเดรสที่ซ้ำกัน แต่เนื่องจาก MPLS VPN นั้นมีระบบในการแยกเราติงเทเบิลของเน็ตเวิร์กแต่ละองค์กรออกจากกันโดยอาศัยระบบแอดเดรสแบบ 96 บิต ซึ่งประกอบด้วย 32 บิตสำหรับ IPv4 แอดเดรส และส่วนขยายที่เรียกว่า RD (Route Distinguisher) ซึ่งตัว RD นี้จะเป็นตัวบอกความแตกต่างระหว่าง IPv4 แอดเดรสขององค์กรหนึ่งกับอีกองค์กรหนึ่ง แม้ว่าทั้งสององค์กรจะใช้ไอพีแอดเดรสชุดที่ซ้ำกันอยู่บนโครงข่ายแกนหลัก MPLS เดียวกันก็สามารถที่จะรับส่งข้อมูลภายในองค์กรเดียวกันโดยไม่มีปัญหาในเรื่องของระบบแอดเดรสที่ซ้ำกัน ทั้งนี้ทำให้แต่ละองค์กรที่มาใช้งาน MPLS VPN และตัวผู้ให้บริการโครงข่าย MPLS เองสามารถที่จะกำหนดระบบไอพีแอดเดรสได้เองเป็นอิสระจากกัน

### ระบบเราติง และข้อมูลที่แยกออกจากกัน

MPLS VPN นั้นมีระบบการแยกเราติงเทเบิลของแต่ละ VPN ออกจากกันโดยมีองค์ประกอบ 2 อย่างในการที่จะนำมาแยกระบบฐานข้อมูลเราติงบนตัวเราเตอร์ อย่างแรก ก็คือเราเตอร์สำหรับเชื่อมต่อกับ VPN ของลูกค้านั้น จะมีการสร้างฐานข้อมูลเราติงที่เรียกว่า Virtual Routing Forwarding เฉพาะให้กับแต่ละ VPN โดยในแต่ละ VRF บนเราเตอร์ของผู้ให้บริการแต่ละตัวนั้นก็จะบรรจุข้อมูลเส้นทาง (route) ของแต่ละ VPN โดยเฉพาะ ซึ่งข้อมูลเส้นทางหรือ route นั้นอาจได้มาจาก static route ที่ต้องระบุเอง หรือ dynamic routing protocol ที่ได้มาจากระบบแลกเปลี่ยนข้อมูลกันระหว่างเราเตอร์ของผู้ให้บริการ (Provider Edge Router - PE) ที่เชื่อมต่อกับเราเตอร์ของลูกค้า องค์ประกอบอีกอย่างหนึ่งก็คือ การใช้ตัว VPN identifier มาปะเพิ่มให้กับแอดเดรสใน BGP routing table ซึ่งในที่นี้ก็คือ Route Distinguisher 64 บิตที่ปะเพิ่มลงไปบน IPv4 แอดเดรส 32 บิตนั่นเอง ซึ่งตัว RD นี้เองทำให้ VPN ของแต่ละองค์กรสามารถใช้ไอพีแอดเดรสที่ 32 บิตที่ซ้ำกันได้โดยมี RD 64 บิตเป็นตัวบอกความแตกต่าง ซึ่งข้อมูลเส้นทางแบบ 96 บิต (IPv4 32 บิตรวมกับ RD 64 บิต) จะถูกแลกเปลี่ยนระหว่างเราเตอร์ของผู้ให้บริการแต่ละตัวที่ต่อ

**ใช้ระบบสื่อสารร่วมกัน: ระบบสื่อสารลอจิคอลผ่านเฟรมรีเลย์**




องค์กรสามารถควบคุมค่าใช้จ่ายและแยกบริการวีพีเอ็นออกจากระบบสื่อสารผ่านอินเทอร์เน็ตได้ โดยใช้ระบบเชื่อมต่อลอจิคอลหลายชุดผ่านเฟรมรีเลย์ ซึ่งเป็นการสื่อสารเพียงช่องทางเดียวระหว่างลูกค้าและบริษัทผู้ให้การสื่อสาร

เชื่อมกับองค์กรต่างๆ (Provider Edge Routors) ในแต่ละแห่ง โดยมีเราติงโพรโตคอล MP-BGP ทำหน้าที่ในการแลกเปลี่ยนข้อมูลระหว่างกันให้ โดยเราเตอร์แต่ละตัวก็จะมี VRF ที่แยกเก็บข้อมูลเส้นทางของแต่ละ VPN ของแต่ละองค์กรแยกจากกัน

ในส่วนของกลไกการแยกข้อมูลของแต่ละ VPN ที่ส่งไปบน MPLS เน็ตเวิร์กนั้น MPLS VPN ได้ใช้วิธีการแยกข้อมูลของ Layer3 ด้วยการใช้ IP VPN Forwarding table ที่แยกออกจากกัน และวิธีการที่ใช้ในการตัดสินใจเลือกเส้นทางที่จะส่งข้อมูลไปบน CORE เน็ตเวิร์กนั้นก็จะใช้ Label ในการอ้างอิงว่าข้อมูลนี้จะถูกส่งไปยังอินเทอร์เฟซไหน ซึ่งแตกต่างจาก IP lookup แบบปกติซึ่งใช้วิธีของการดูจากไอพีแอดเดรสปลายทาง (destination IP address) ที่อยู่บนเฮดเดอร์ของไอพีแพ็กเก็ต โดยวิธีการของ MPLS นั้นจะใช้วิธีการสร้างเส้นทางในการส่งข้อมูลที่เรียกว่า Label Switching Path (LSPs) ที่มีจุดเริ่มต้นจากเราเตอร์ PE ตัวหนึ่งไปสิ้นสุดยังเราเตอร์ PE อื่นๆ โดยข้อมูลจาก VPN ของผู้ใช้บริการนั้นจะถูกส่งเข้ามายังเราเตอร์ PE ของผู้ให้บริการที่อินเทอร์เฟซต่อเชื่อมกันกับเราเตอร์ของ VPN นั้นในรูปแบบของไอพีแพ็กเก็ต หลังจากนั้น เราเตอร์ PE ก็จะทำการตัดสินใจเลือกเส้นทางการส่งข้อมูลโดยดูจาก IP VPN Forwarding table ของอินเตอร์เฟซที่ต่ออยู่กับผู้ใช้บริการ VPN นั้นๆ เพื่อที่จะส่งข้อมูลต่อไปยังปลายทางโดยผ่านไปบน Label Switching Path ดังนี้ นี่คือกลไกหรือวิธีการที่ MPLS VPN ใช้ในการแยกระบบแอดเดรส แยกเส้นทางการส่งข้อมูล และแยกข้อมูลของแต่ละ VPN ไม่ให้มาปะปนกันบนคอร์เน็ตเวิร์ก (Core Network) โดยไม่ก่อให้เกิดปัญหาในเรื่องที่ว่าข้อมูลของแต่ละ VPN จะใช้ไพรเวทไอพีแอดเดรสที่ซ้ำกันไม่ได้ หรือปัญหาที่ว่าข้อมูลนั้นส่งผิดคือส่งจาก VPN ขององค์กรหนึ่งแต่ไปเข้าที่ VPN ขององค์กรอื่น ทั้งนี้ก็เพราะในการส่งข้อมูลนั้นไม่ได้ใช้ไอพีเฮดเดอร์ในการส่งข้อมูลบนคอร์เน็ตเวิร์ก หากแต่มีการนำเอา Label มาใช้ในการส่งผ่านข้อมูล ซึ่งวิธีการนี้ทำให้ MPLS VPN นั้นมีความสามารถในการแยกแยะข้อมูลของ VPN ต่างๆ เทียบเท่ากับการสร้างวีพีเอ็นบนเอทีเอ็ม หรือบนเฟรมรีเลย์

## การซ่อนคอร์เน็ตเวิร์กของผู้ให้บริการ

การซ่อนคอร์เน็ตเวิร์กของผู้ให้บริการให้พ้นจากการโจมตีจากเน็ตเวิร์กภายนอกอื่นไม่ว่าจะเป็นเน็ตเวิร์กของ VPN ต่างๆ หรือว่าอินเทอร์เน็ต นั้นมีความจำเป็นอย่างยิ่งเพื่อเพิ่มความปลอดภัยให้กับระบบ ซึ่ง MPLS นั้นใช้ทั้งการทำแพ็กเก็ตฟิลเตอริง และการป้องกันไม่ให้มีการอัพเดตข้อมูลของคอร์เน็ตเวิร์กออกไปยังเน็ตเวิร์กอื่นๆ ภายนอกที่มาต่ออยู่ด้วย การทำแพ็กเก็ตฟิลเตอริงนั้นจะช่วยป้องกันไม่ให้ข้อมูลเราติงของคอร์เน็ตเวิร์ก และข้อมูลเราติงของ VPN ต่างๆ นั้นรั่วไหลออกไปยังวีพีเอ็นของลูกค้ารายอื่น หรือรั่วไหลออกไปยังอินเทอร์เน็ตภายนอก ทั้งนี้ก็เพราะว่าวีพีเอ็นของลูกค้านั้นไม่จำเป็นต้องรู้โทโพโลยี (Topology) ของคอร์เน็ตเวิร์ก สิ่งที่ลูกค้าที่มาต่ออยู่กับเราเตอร์ PE ของผู้ให้บริการต้องรู้มีเพียงไอพีเอดเดรสของเราเตอร์ PE ที่ตัวเองต่ออยู่ด้วยเท่านั้นเพื่อใช้ในการแลกเปลี่ยนข้อมูลเราติงเทเบิลระหว่างกันและกัน และใช้เป็น Next hop ในการส่งข้อมูลออกไปยังเน็ตเวิร์กของผู้ให้บริการ

ในกรณีของการใช้ไดนามิกเราต์เพื่อแลกเปลี่ยนข้อมูลเส้นทางระหว่างตัวเราเตอร์ PE ของผู้ให้บริการกับเราเตอร์ขององค์กรที่ใช้บริการ ซึ่งเราเตอร์ขององค์กรที่ใช้บริการวีพีเอ็นจำเป็นต้องมีการประกาศเส้นทาง (route) ให้กับเราเตอร์ของผู้ให้บริการสำหรับกรณีนี้ ก็ไม่ต้องกลัวว่าจะเป็นการเปิดช่องโหว่ให้บุคคลอื่นเข้ามาโจมตีได้ ทั้งนี้เป็นเพราะว่าระบบ MPLS VPN นั้นไม่ได้มีการเปิดเผยข้อมูลเราติงและระบบไอพีแอดเดรสของ VPN ใดๆ ให้กับบุคคลที่สามซึ่งในกรณีนี้ก็หมายถึง ไม่มีการอัพเดตเราติงไปให้กับวีพีเอ็นอื่นๆ หรือไม่ได้มีการอัพเดตให้กับอินเทอร์เน็ต ซึ่งนั่นก็หมายความว่าบุคคลภายนอก VPN ไม่สามารถที่จะทราบเส้นทางและไอพีแอดเดรสที่จะเข้ามาโจมตีได้ และในกรณีที่มีการให้บริการ VPN ร่วมกับการให้บริการอินเทอร์เน็ตกับองค์กรนั้น ทางผู้ให้บริการ (Service Provider) ก็สามารถที่จะใช้วิธีการทำ Network Address Translation ร่วมด้วย เพื่อเป็นการซ่อนไอพีแอดเดรสของผู้ใช้บริการ ซึ่งวิธีนี้ก็เพียงพอที่จะทำให้ผู้ใช้บริการสามารถใช้

อ่านบทความประกอบเรื่อง "การวิเคราะห์ระบบรักษาความปลอดภัย MPLS VPN เปรียบเทียบกับระบบ L2VPNS แบบเก่า เช่น เฟรมรีเลย์ และเอทีเอ็ม รวมทั้งข้อแนะนำในการติดตั้งใช้งาน" ได้ที่ cisco.com/packet/164_5b1

บริการอินเทอร์เน็ตได้เหมือนๆ กับการให้บริการอินเทอร์เน็ตทั่วไป โดยไม่จำเป็นต้องเปิดเผยข้อมูลไอพีแอดเดรสทั้งหมดขององค์กรออกไปยังอินเทอร์เน็ต

## ระบบต่อต้านการโจมตี

การโจมตีการให้บริการ MPLS VPN นั้นแม้ว่าจะไม่สามารถโจมตีในลักษณะของการเจาะเข้าไปยังเน็ตเวิร์กของผู้ให้บริการ หรือเจาะเข้าไปยังเน็ตเวิร์กของผู้ใช้บริการวีพีเอ็นดังที่กล่าวไว้แล้วข้างต้น แต่ก็ยังมีความเสี่ยงในกรณีที่ผู้ไม่หวังดีจะหันมาโจมตีในรูปแบบของการทำ DoS (Denial of Service Attack) หรือการเจาะเข้ามายังตัวเราเตอร์ของผู้ให้บริการโดยตรงแล้วทำให้เราเตอร์ PE ของผู้ให้บริการไม่สามารถให้บริการได้ ซึ่งในกรณีนี้ผู้ให้บริการ MPLS VPN นั้นจะมีการออกแบบให้ระบบโครงข่ายที่ให้บริการนั้นปลอดภัยจากการโจมตีแบบดังกล่าวด้วยวิธีการทำแพ็กเก็ตฟิลเตอริงและการซ่อนระบบแอดเดรสของอุปกรณ์ในระบบเครือข่ายทั้งหมดเพื่อไม่ให้บุคคลภายนอกสามารถเข้าถึงตัวเราเตอร์ของผู้ให้บริการได้ โดยเทคนิคหนึ่งที่มีการนำมาใช้กันก็คือการทำ ACL (Access Control List) เพื่ออนุญาตให้เฉพาะข้อมูลเราติงโพรโตคอลระหว่างเราเตอร์ของผู้ใช้บริการเท่านั้นที่สามารถที่จะส่งเข้ามายังตัวเราเตอร์เพื่อแลกเปลี่ยนข้อมูลหรือทำเราติงอัพเดตเท่านั้น เพื่อป้องกันมิให้มีการเจาะระบบเข้ามาเพื่อควบคุมการทำงานของเราเตอร์ PE ของผู้ให้บริการ หรือทำอย่างอื่นอันจะเป็นอันตรายต่อการให้บริการ เช่น การโจมตีกลไกการทำงานของ MPLS signaling ด้วยวิธีการป้องกันเหล่านี้ถ้าหากได้มีการนำไปกำหนดใช้งานบนอุปกรณ์เราเตอร์ PE ของผู้ให้บริการอย่างเหมาะสมแล้วก็จะช่วยป้องกันการโจมตีดังที่กล่าวไปแล้วได้

การซ่อนไอพีแอดเดรสของอุปกรณ์ในเครือข่ายของผู้บริการเพื่อไม่ให้บุคคลภายนอกรู้ไอพีแอดเดรสแล้วเข้ามาโจมตีได้นั้น บางท่านอาจจะคิดว่าเป็นไปได้ไหมที่ผู้เจาะระบบอาจจะเป็นผู้ที่ใช้บริการอยู่ภายในวีพีเอ็นขององค์กรต่างๆ เองพยายามที่จะใช้วิธีการเดาไอพีแอดเดรสแล้วพยายามเจาะหรือโจมตีระบบเข้ามา เรื่องนี้นั้นเป็นไปไม่ได้เลยเนื่องจาก MPLS VPN นั้นมีการแยกระบบแอดเดรสของวีพีเอ็นแต่ละรายและแยกระบบแอดเดรสของเน็ตเวิร์กของผู้ให้บริการออกจากกัน ซึ่งหากมีการพยายามจะโจมตีระบบผ่านทางวีพีเอ็นขององค์กรโดยส่งแพ็กเก็ตเข้ามา แพ็กเก็ตนั้นก็จะถือว่าเป็นข้อมูลของวีพีเอ็นนั้นๆ ซึ่งก็จะถูกจำกัดให้ส่งไปที่ต่างๆ ภายในวีพีเอ็นนั้นๆ เท่านั้นไม่สามารถที่จะส่งเข้ามาโจมตีอุปกรณ์ของผู้ให้บริการได้ จึงทำให้ผู้ที่หวังจะอาศัยเน็ตเวิร์กของผู้ใช้บริการซึ่งต่อเข้ากับเน็ตเวิร์กของผู้ให้บริการเพื่อเข้ามาโจมตีโครงข่ายแกนหลักนั้นไม่สามารถทำได้ดังใจหวัง

วิธีการหนึ่งซึ่งจะช่วยให้เน็ตเวิร์กของผู้ให้บริการนั้นปลอดภัยมากยิ่งขึ้นจากผู้ที่หวังจะอาศัยอาศัยเน็ตเวิร์กของผู้ใช้บริการซึ่งต่อตรงกับเราเตอร์เข้ามาโจมตีก็คือการกำหนดให้ใช้เราติงโพรโตคอลแบบ Static Route ระหว่างเราเตอร์ของผู้ใช้บริการกับเราเตอร์ PE ของผู้ให้บริการ ในกรณีนี้เราเตอร์ของผู้ให้บริการจะปฏิเสธการส่ง หรือขอข้อมูลเราติงอัพเดตแบบ Dynamic route จากตัวเราเตอร์ของผู้ใช้บริการ ซึ่งทั้งผู้ให้บริการและผู้ใช้บริการสามารถที่จะกำหนดเส้นทางการส่งข้อมูลแบบ Static Route โดยระบุปลายทาง (next hop)ไปที่อินเทอร์เฟซที่ต่ออยู่ด้วยเท่านั้น ไม่จำเป็นต้องมีการระบุปลายทางเป็นไอพีแอดเดรสของเราเตอร์ PE ของผู้ให้บริการ ซึ่งวิธีนี้เราเตอร์ของผู้ใช้บริการไม่จำเป็นต้องรู้อะไรเลยเกี่ยวกับไอพีแอดเดรสของผู้ให้บริการ แม้กระทั่งไอพีแอดเดรสของเราเตอร์ PE ก็ไม่จำเป็นต้องรู้ ซึ่งวิธีนี้ถือได้ว่าปลอดภัยที่สุดที่จะป้องกันการโจมตีโดยอาศัยเน็ตเวิร์กของผู้ใช้บริการเองเป็นทางผ่านเข้ามา

สำหรับกรณีการเลือกใช้ Dynamic Routing ระหว่างเราเตอร์ของผู้ใช้บริการกับเราเตอร์ของผู้ให้บริการนั้นถือได้ว่ามีความเสี่ยงในการโจมตีจากเน็ตเวิร์กของผู้ใช้บริการที่ต่อตรงเข้ามามากกว่าเนื่องจากเราเตอร์ของผู้ใช้บริการนั้นจำเป็นที่จะต้องทราบไอพีแอดเดรสที่ใช้เป็น Router ID ของเราเตอร์ PE ซึ่งทางซิสโก้แนะนำว่าถ้าหากจำเป็นจะต้องใช้ Dynamic Routing แล้วก็ควรที่จะเลือกใช้วิธีการดังต่อไปนี้เพื่อเสริมความปลอดภัยให้มากขึ้น

- ถ้าหากเป็นไปได้ให้เลือกใช้ BGP เราติงเป็นโพรโตคอลระหว่างเราเตอร์ของผู้ใช้บริการและผู้ให้บริการจะเป็นการดีที่สุดสำหรับผู้ที่ต้องการความปลอดภัย เพราะว่า BGP เป็นเราติงโพรโตคอลที่มีคุณสมบัติในการรักษาความปลอดภัยมากที่สุด อีกทั้งยังมีเทคนิคหรือลูกเล่นในการเพิ่มความปลอดภัยให้กับระบบอีกหลายอย่าง เช่น prefix filtering และ dampening เป็นต้น
- ใช้ ACL (Access Control List) ในการจำกัดให้การส่งข้อมูลจากเราเตอร์ของผู้ใช้บริการที่มีจุดหมายปลายทางมายังไอพีของเราเตอร์ PE ของผู้ให้บริการ นั้นสามารถส่งมาได้เพียงเราติงโพรโตคอลเท่านั้น ซึ่งสามารถทำได้โดยการเปิดพอร์ตของเราติงโพรโตคอลนั้นและอนุญาตให้เฉพาะไอพีแอดเดรสที่มาจากเราเตอร์ของผู้ใช้บริการเท่านั้นที่จะส่งข้อมูลเราติงเข้ามาได้
- การใช้ Message Digest Five (MD5) ในการทำ authentication เพื่อตรวจสอบเราเตอร์ของผู้ใช้บริการที่ต่อเข้ามาเพื่อป้องกันการสวมรอยปลอมตัวเป็นเราเตอร์ของผู้ใช้บริการ (Spoofing)
- การจำกัดจำนวนข้อมูลเส้นทาง (จำนวน route) ให้กับแต่ละ Virtual Routing Forwarding (VRF) ที่จะรับได้ นี้จะเป็นการช่วยป้องกันการโจมตีแบบ DoS ที่พยายามจะทำ routing attack โดยส่งข้อมูลเส้นทางเข้ามาเป็นจำนวนมากๆ ได้

## การป้องกันการสวมรอย (spoofing) และการเข้ารหัสข้อมูล (Encrypted Communication)

ผู้ไม่หวังดีอาจจะพยายามโจมตีโดยอาศัยการสวมรอยทำ Spoofing Attack เพื่อที่จะเปลี่ยนแปลงเส้นทางการส่งข้อมูลก็ดี หรือพยายามที่จะเจาะเข้ามาในระหว่างมีการทำ authentication เพื่อที่จะใช้ข้อมูลเหล่านี้ในการเจาะระบบ ซึ่งเป็นไปได้ว่าอาจจะมีการทำ Spoof IP source address แล้วส่งข้อมูลเข้ามาใน MPLS เน็ตเวิร์ก แต่ด้วยกลไกการแยกตารางเส้นทางการส่งข้อมูล (Forwarding) ระหว่างวีพีเอ็นหนึ่งกับวีพีเอ็นอื่นๆ และคอร์เน็ตเวิร์กเองนั้น ได้มีการแยกออกจากกันอย่างเด็ดขาดจึงทำให้การทำ IP spoofing นั้นไม่เกิดประโยชน์หรือช่วยให้นักเจาะระบบสามารถเจาะข้ามวีพีเอ็น หรือเจาะเข้ามายังเน็ตเวิร์กของผู้ให้บริการได้เลย แล้วยิ่งถ้าคิดลึกไปถึงขนาดที่ว่าในเมื่อ MPLS ไม่ใช้การดูจาก IP Destination แต่ใช้ Label แล้วจะหันมา spoof label แทนนั้นยิ่งเป็นไปไม่ได้ เนื่องจากว่าระหว่างเราเตอร์ของผู้ให้บริการกับเราเตอร์ของผู้ใช้บริการนั้นจะไม่มีการอนุญาตให้มีข้อมูลที่เป็นแบบ Label packet ส่งเข้ามาโดยเด็ดขาด

องค์กรต่างๆ ที่ใช้บริการ MPLS VPN สามารถที่จะเสริมความปลอดภัยให้ยิ่งขึ้นด้วยการเพิ่มการเข้ารหัสข้อมูลที่ต้องการจะส่งผ่าน MPLS เน็ตเวิร์ก

โดยการทำ IPSec Tunnel ระหว่างเราเตอร์ของผู้ใช้บริการที่สาขาหนึ่งกับเราเตอร์ของผู้ใช้บริการที่อยู่อีกสาขาหนึ่งได้ โดยทั้ง MPLS และ IPsec นั้นสามารถนำมาให้บริการร่วมกันได้อย่างไม่มีปัญหา หรือว่าอาจจะใช้การเข้ารหัสข้อมูลที่ระดับ Application Layer แบบอื่นๆ บน MPLS เน็ตเวิร์กก็สามารถทำได้เช่นกัน

## การเลือกใช้บริการวีพีเอ็นร่วมกับการใช้บริการอินเทอร์เน็ต

หน่วยงานหรือองค์กรต่างๆ ที่ต้องการจะใช้บริการ MPLS VPN สามารถเลือกใช้บริการการเชื่อมต่อวีพีเอ็นร่วมกับการใช้บริการอินเทอร์เน็ตไปพร้อมๆ กันได้หลายรูปแบบขึ้นอยู่กับว่าต้องการความปลอดภัยมากน้อยในระดับไหน แล้วก็ขึ้นอยู่กับว่าค่าใช้จ่ายที่จะเกิดขึ้นในกรณีที่ต้องการความปลอดภัยที่สูงขึ้น ซึ่งก็ต้องมาชั่งน้ำหนักกันดูว่าวิธีไหนที่เหมาะสมที่สุดสำหรับองค์กรของท่าน ซึ่งการให้บริการ MPLS VPN นั้นทางผู้ให้บริการก็จะทำการควบคุมการส่งข้อมูลให้เป็นไปตามกลไกการทำ VPN Separation เพื่อให้การรับส่งข้อมูลของแต่ละวีพีเอ็นนั้นไม่มาปะปนกัน นอกจากนี้ผู้ให้บริการส่วนใหญ่ยังใช้เน็ตเวิร์กที่ให้บริการนั้นเชื่อมต่อกับอินเทอร์เน็ตเพื่อให้บริการอินเทอร์เน็ตควบคู่ไปพร้อมๆ กันกับบริการวีพีเอ็นด้วย ซึ่งการให้บริการแบบนี้นั้นทางซิสโก้เองแนะนำว่าจำเป็นอย่างยิ่งที่ผู้ให้บริการจะต้องเพิ่มความปลอดภัยให้กับระบบเพื่อสร้างความมั่นใจให้กับผู้ใช้บริการมากขึ้นโดยการใช้เทคนิควิธีการต่างๆ ที่ซิสโก้ได้แนะนำให้ โดยส่วนมากแล้วพบว่าการให้บริการ MPLS VPN นั้นมักจะให้บริการวีพีเอ็น และมีบริการเสริมโดยให้ใช้อินเทอร์เน็ต บนโครงข่าย MPLS เดียวกันด้วยเลย ซึ่งแตกต่างจากการให้บริการวีพีเอ็นบน เฟรมรีเลย์ และเอทีเอ็มที่จำเป็นต้องมีอุปกรณ์เน็ตเวิร์กและอินเทอร์เฟซต่างหาก สำหรับวีพีเอ็นชุดหนึ่งและสำหรับอินเทอร์เน็ตอีกชุดหนึ่ง ซึ่งมีค่าใช้จ่ายที่มากกว่า

แน่นอนว่าสำหรับการใช้บริการวีพีเอ็นร่วมกับบริการอินเทอร์เน็ตนั้นวิธีการที่ปลอดภัยที่สุดก็คือการแยกการเชื่อมต่อวีพีเอ็นกับการเชื่อมต่ออินเทอร์เน็ตออกจากกันโดยเด็ดขาด MPLS VPN ก็สามารถทำได้ ทำนองเดียวกันกับการให้บริการวีพีเอ็นบนเฟรมรีเลย์ หรือเอทีเอ็มดังรูปที่ 1 ลูกค้าองค์กรที่ต้องการใช้อินเทอร์เน็ตควบคู่กับวีพีเอ็น สามารถที่จะซื้อเราเตอร์ตัวหนึ่งและสื่อสัญญาณแบบแวนชุดหนึ่งสำหรับเชื่อมต่อกับบริการวีพีเอ็น และซื้อเราเตอร์อีกตัวหนึ่งกับสื่อสัญญาณแบบ WAN อีกชุดหนึ่งสำหรับต่อเข้ากับบริการอินเทอร์เน็ต ซึ่งทั้งบริการวีพีเอ็น และบริการอินเทอร์เน็ตนั้นให้บริการอยู่บนเราเตอร์ของผู้ให้บริการแยกกันคนละตัว วิธีการนี้ทำให้แน่ใจได้เลยว่าวีพีเอ็นจะไม่ถูกโจมตีจาก DoS Attack เพราะเราแยกเน็ตเวิร์กของวีพีเอ็นออกจากอินเทอร์เน็ตอย่างเด็ดขาดโดยทางกายภาพทั้งทางฝั่งของผู้ให้บริการและผู้ใช้บริการ

อีกวิธีหนึ่งก็คือผู้ใช้บริการนั้นแยกอุปกรณ์เราเตอร์กับสื่อสัญญาณชุดหนึ่งสำหรับเชื่อมต่ออินเทอร์เน็ต และอุปกรณ์เราเตอร์กับสื่อสัญญาณอีกชุดหนึ่งสำหรับเชื่อมต่อวีพีเอ็น แต่ว่าต่อเข้าไปยังเราเตอร์ PE ของผู้ให้บริการตัวเดียวกันซึ่งมีการแยกอินเทอร์เฟซสำหรับเส้นทางออกอินเทอร์เน็ต กับอินเทอร์เฟซสำหรับเส้นทางเข้าสู่วีพีเอ็น โดยใช้ Virtual Routing Forwarding ซึ่งเป็นเทคนิคในการแยกเส้นทางการส่งข้อมูลดังที่ได้กล่าวมาแล้ว ซึ่งวิธีนี้มีค่าใช้จ่ายถูกกว่าเนื่องจากเช่าอุปกรณ์เราเตอร์ของผู้ให้บริการเพียงตัวเดียว ในขณะที่ความสามารถในการป้องกันการโจมตีจาก DoS Attack ก็ถือว่าไม่แตกต่างจากแบบแรกเท่าไรมากนัก

อีกวิธีการหนึ่งก็คือทางองค์กรที่ต้องการใช้บริการวีพีเอ็นร่วมกับบริการอินเทอร์เน็ตสามารถที่จะใช้เราเตอร์เพียงตัวเดียวแล้วก็ใช้อินเทอร์เฟซเพียงอินเทอร์เฟซเดียวสำหรับทั้งสองบริการเลยก็ทำได้ เพื่อลดค่าใช้จ่ายในการเช่าสื่อสัญญาณและเช่าอุปกรณ์เราเตอร์ของผู้ให้บริการ แต่ทางเลือกนี้ย่อมมีข้อด้อยกว่าในการป้องกันการโจมตีแบบ DoS Attack เพราะว่าใช้อุปกรณ์ฮาร์ดแวร์ชุดเดียวกันทั้งหมดในการใช้งานทั้งสองบริการ ซึ่งในทางทฤษฎีแล้วมีความเสี่ยงมากกว่าที่จะถูกโจมตี แต่ในทางปฏิบัติแล้วความเสี่ยงที่ว่านี้ก็สามารถที่จะถูกลดลงได้โดยอาศัยการกำหนดค่า และการควบคุมอย่างถูกต้องจากผู้ให้บริการ และผู้ใช้บริการ โดยทั่วไปแล้วการเลือกใช้บริการในลักษณะนี้จะใช้ Frame Relay encapsulation บนอินเทอร์เฟซระหว่างเราเตอร์ของผู้ให้บริการกับเราเตอร์ของผู้ใช้บริการทั้งนี้ก็เพื่อที่จะทำวงจรเสมือนบนอินเทอร์เฟซจริง โดยแยกเป็นวงจรสำหรับวีพีเอ็นหนึ่งวงจรเพื่อเชื่อมกับ sub-interface ที่กำหนดไว้เป็น VRF ของวีพีเอ็น และอินเทอร์เน็ตอีกหนึ่งวงจรสำหรับอินเทอร์เน็ตหนึ่งวงจรเพื่อเชื่อมกับ sub-interface ที่กำหนดไว้เป็น VRF ของอินเทอร์เน็ต ดังรูปที่ 2 โดยทางกายภาพแล้วแม้ว่าจะใช้อุปกรณ์เราเตอร์และสื่อสัญญาณแบบวีพีเอ็นชุดเดียวกัน แต่ว่าในการทำงานจริงจะมีการแยกเส้นทางการส่งข้อมูลออกจากกันโดยข้อมูลที่เป็นอินเทอร์เน็ตก็จะถูกส่งเข้าไปที่เราเตอร์ที่ทำหน้าที่เป็นอินเทอร์เน็ตเกตเวย์ของลูกค้า (ในรูป อินเทอร์เน็ต CE) ส่วนข้อมูลที่เป็นวีพีเอ็นนั้นก็จะถูกส่งผ่านเราเตอร์ของผู้ใช้บริการวีพีเอ็น (ในรูป VPN CE) โดยผ่านทางวงจรเสมือน โดยที่ทั้งสองข้อมูลจะไม่ถูกส่งเข้ามาปะปนกัน

## จะมั่นใจได้อย่างไรกับผู้ให้บริการ

องค์กรต่างๆ สามารถที่จะเลือกใช้บริการจากผู้ให้บริการรายใดรายหนึ่งจากการสอบถามถึงมาตรการรักษาความปลอดภัยของ MPLS VPN ของบริษัทผู้ให้บริการสื่อสารโดยการตั้งคำถามดังนี้

**ถาม: การสื่อสารอินเทอร์เน็ตและวีพีเอ็นใช้คอร์เน็ตเวิร์กชุดเดียวกันหรือไม่?**

**ตอบ:** แม้ว่าการมีคอร์เน็ตเวิร์กสำหรับบริการวีพีเอ็นโดยเฉพาะจะมีความปลอดภัยสูงมากก็ตาม แต่ MPLS VPN ก็มีกลไกในการที่จะใช้เน็ตเวิร์กเดียวกันให้บริการทั้งวีพีเอ็น และอินเทอร์เน็ตโดยแยกการส่งข้อมูลออกจากกันอย่างปลอดภัย และอยู่ในระดับที่มีความปลอดภัยเพียงพอสำหรับองค์กรส่วนใหญ่เช่นกัน

**ถาม: การให้บริการ MPLS VPN ของท่านมีเราเตอร์ PE แยกจากกันคนละตัวสำหรับบริการอินเทอร์เน็ต และวีพีเอ็น หรือไม่?**

**ตอบ:** การใช้เราเตอร์ PE ร่วมกันทั้งบริการอินเทอร์เน็ตและบริการวีพีเอ็นอาจดูเหมือนว่ามีความเสี่ยงสูงกว่าในการที่จะถูกโจมตีจาก DoS Attack แต่ว่านักเจาะระบบก็ไม่สามารถที่จะเจาะข้ามระหว่างวีพีเอ็นหนึ่งมายังอีกวีพีเอ็นหนึ่งได้ หรือเจาะผ่านเข้ามาจากอินเทอร์เน็ตได้ ไม่ว่าจะใช้เราเตอร์ PE ตัวเดียวกันหรือแยกจากกันก็ตาม

**ถาม: คุณมีมาตรการป้องกันคอร์ เน็ตเวิร์กของคุณอย่างไร?**

**ตอบ:** ผู้ให้บริการที่ได้รับการรับรองจาก Cisco Power Network จะได้รับคำแนะนำในการวางระบบให้มีความปลอดภัยมากที่สุด ตามที่ได้มีการกำหนดไว้ใน Cisco security best Practices for securing an MPLS network ซึ่งทำให้ MPLS VPN นั้นมีความปลอดภัยในระดับที่ไม่แตกต่างไปจากเอทีเอ็ม หรือเฟรมรีเลย์ ■