เรื่องน่ารู้เกี่ยวกับ VOICE - AND VIDEO-ENABALED VPN (V³PN)

ทำไมเราจึงต้องสนใจเกี่ยวกับ V³PN ด้วย?

ระบบ voice and video-enabled virtual private network (V³PN) เป็นการผสมผสานเทคโนโลยีชนิดต่างๆ ของซิสโก้เพื่อรองรับบริการชนิดต่างๆ ที่ทำงานผ่าน IP Security (IPSec) VPN โซลูชันซึ่งสามารถนำมาใช้งานได้ประกอบด้วย VPN, Quality of Service (QoS), ระบบโทรศัพท์ไอพี และระบบประชุมร่วมผ่านวิดีโอ มีประโยชน์ดังนี้

ประหยัดค่าใช้จ่าย: ระบบโทรศัพท์ไอพี และ VPN ต่างสามารถประหยัดค่าใช้จ่ายและทำงานได้อย่างมีประสิทธิภาพ ถ้าหากนำเอาระบบทั้งสองชนิดมารวมกัน โซลูชันใหม่จะช่วยให้ประหยัดค่าใช้จ่ายได้มากขึ้นโดยการใช้ระบบสื่อสารผ่านอินเทอร์เน็ตแทนที่การใช้ระบบแวนเฉพาะซึ่งเสียค่าใช้จ่ายสูงกว่า

เพิ่มผลผลิตมากขึ้น: V³PN ขยายขอบเขตการทำงานของเสียง วิดีโอ ข้อมูล และแอพพลิเคชันต่างๆ ที่อยู่ภายในองค์กรให้ครอบคลุมไปถึงการทำงานของสาขาต่างๆ ซึ่งจะช่วยให้พนักงานที่อยู่ตามสาขาและสำนักงานขนาดเล็ก ทำงานได้มากขึ้นและมีประสิทธิภาพมากขึ้นเสมือนกับพนักงานที่อยู่ในสำนักงานใหญ่

ระบบรักษาความปลอดภัย: VPN ทำให้เครือข่ายมีความปลอดภัยสูงขึ้น โดยการใช้ระบบเข้ารหัสและระบบตรวจสอบสิทธิ์ที่ทันสมัยมากขึ้น V³PN ได้ขยายขอบเขตการรักษาความปลอดภัยให้ครอบคลุมแอพพลิเคชันเรื่องเสียงและวิดีโอด้วยซึ่งถือเป็นการปกป้องอีกชั้นหนึ่งซึ่งเกินกว่าการทำงานของระบบสื่อสาร PSTN หรือระบบแลนไร้สายจะทำได้

ความยืดหยุ่น: V³PN ช่วยขยายขอบเขตการทำงานของแอพพลิเคชันที่อยู่ในองค์กร เช่น ศูนย์ติดต่อแบบไอพี (IP Contact Center) ระบบประชุมร่วมผ่านวิดีโอ อีเลิร์นนิง และการทำงานจากบ้าน โดยไม่จำเป็นต้องคำนึงว่าทรัพยากรอยู่ตรงจุดไหนและผู้ใช้ทำงานจากที่ใด สิ่งที่ช่วยให้การใช้ V³PN เติบโตมากขึ้นก็คือเราเตอร์ Cisco IOS VPN ที่มีคุณสมบัติที่จำเป็นสำหรับการทำงานของ V³PN ไม่ว่าจะเป็น IPSec, Generic Routing Encapsulation (GRE), QoS และระบบโทรศัพท์ไอพี เป็นต้น

จุดมุ่งหมายหลักคืออะไร และมีอุปสรรคอะไรบ้าง?

V³PN มีจุดมุ่งหมายหลัก 2 ประการพร้อมๆ ทั้งมีความพยายามในการใช้ประโยชน์จากการลงทุนที่มีอยู่แล้วภายในองค์กรด้วย

1. การรับส่งข้อมูลเสียง วิดีโอ และแอพพลิเคชันอื่นๆ ในองค์กรโดยไม่รู้ว่าตัวเองกำลังทำงานผ่าน VPN อยู่
2. องค์ประกอบที่อยู่ภายใน เช่น IPSec VPN, QoS และระบบโทรศัพท์ไอพี (รวมทั้งวิดีโอ) ไม่ไปรบกวนการทำงานปกติ

อุปสรรคหลายอย่างซึ่งเกิดขึ้นเมื่อนำเอาเทคโนโลยีต่างๆ มาผสมผสานการทำงานกับ V³PN ก็คือ

แบนด์วิดธ์: ระบบเข้ารหัสและการจัดเตรียมช่องทางสำหรับระบบ voice over IP (VoIP) และวิดีโอแพ็กเก็ตทำให้ต้องมีการจัดสรรแบนด์วิดธ์เพิ่มขึ้น

ความล่าช้าและอาการสะดุดของเสียง: แพ็กเก็ต VoIP ที่เดินทางผ่าน VPN ต้องมีการเข้ารหัสและถอดรหัส ซึ่งเป็นองค์ประกอบใหม่ที่ก่อให้เกิดความล่าช้าขึ้นมาได้

ข้อมูลไบต์ Type-of-Service (ToS): IPSec VPN เข้ารหัสไอพีแพ็กเก็ตดั้งเดิมให้มีข้อมูลไบต์ ToS ลงไปด้วย โดย ToS ใช้เป็นตัวระบุลำดับความสำคัญของแพ็กเก็ตสำหรับ QoS จะใช้จัดลำดับความสำคัญของสัญญาณอีกทอดหนึ่ง

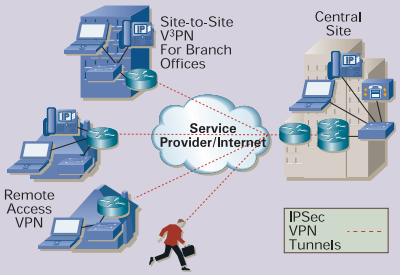
การโต้ตอบระหว่าง IPSec และ QoS: IPSec เป็นโพรโตคอลรักษาความปลอดภัยที่พยายามทำให้แพ็กเก็ตเรียงลำดับ ส่วน QoS พยายามที่จะถ่วงเวลาแพ็กเก็ตที่มีความสำคัญต่ำโดยการเปลี่ยนแปลงลำดับของแพ็กเก็ต

โมเดลการใช้งาน

การเชื่อมโยงระหว่างสาขา: V³PN สามารถเชื่อมโยงสำนักงานสาขาขนาดเล็ก กลาง และใหญ่ไปหาสำนักงานใหญ่ โดยใช้ช่องทางการสื่อสาร VPN แบบตายตัว โดยปกติแล้วการสื่อสารจะเกิดขึ้นผ่านแบ็กโบนของบริษัทผู้ให้บริการสื่อสารโดยใช้สื่อเลเยอร์ 2 แบบจุดต่อจุด เสียงและวิดีโอสามารถส่งผ่านโมเดลแบบนี้ได้โดยมีคุณภาพเท่ากับสัญญาณโทรศัพท์ทั่วไป

การเชื่อมโยงกับสำนักงานขนาดเล็ก (SOHO): V³PN สามารถใช้เชื่อมโยงสำนักงานขนาดเล็กหรือสำนักงานในบ้าน (SOHO) ไปยังสำนักงานใหญ่ขององค์กรโดยใช้ช่องทางการสื่อสาร VPN แบบตายตัว โดยปกติแล้วการสื่อสารจะผ่านเคเบิล DSL หรือระบบสื่อสารอื่นๆ ของบริษัทผู้ให้บริการสื่อสาร ซึ่งเสียงและวิดีโอสามารถส่งผ่านโมเดลแบบนี้ได้โดยมีโอกาสที่จะประสบความสำเร็จสูงมากขึ้นอยู่กับรูปแบบของการติดตั้ง

การสื่อสารจากระยะไกล: VPN ช่วยเชื่อมโยงพนักงานที่ทำงานจากบ้าน หรือจากสาขา หรือในขณะที่เดินทางไปยังสำนักงานใหญ่โดยใช้ช่องทางสื่อสาร VPN เฉพาะกิจได้ โดยปกติแล้วการติดต่อจะผ่านระบบสื่อสารไดอัลอัพ หรือบริษัทผู้ให้บริการสื่อสารเฉพาะ แม้ว่าการสื่อสารสัญญาณวิดีโอและเสียงผ่านโมเดลนี้สามารถทำได้ก็ตาม แต่เครื่องมืออย่าง QoS จะไม่อาจใช้กับระบบสื่อสารไดอัลอัพได้



การเปลี่ยนแปลงของระบบโทรศัพท์ไอพี และการออกแบบระบบ VPN ที่มีอยู่ในปัจจุบัน

สถาปัตยกรรมของระบบโทรศัพท์ไอพี ซึ่งประกอบด้วย Cisco CallManager ระบบโทรศัพท์ไอพี เกตเวย์ VoIP และอื่นๆ ยังคงเหมือนเดิม แต่เราต้องมีการจัดสรรแบนด์วิดธ์และมีระบบ Call Admission Control เพิ่มเติม เพื่อรองรับองค์ประกอบใหม่ๆ ที่เพิ่มเข้ามาในระบบ VPN

การติดตั้ง IPSec VPN โดยใช้เราเตอร์ Cisco IOS VPN ยังคงเหมือนเดิม แต่เราจำเป็นต้องมีการใช้ฮาร์ดแวร์เร่งความเร็วในการเข้ารหัส VPN เพื่อลดความล่าช้าและอาการกระตุกของสัญญาณ

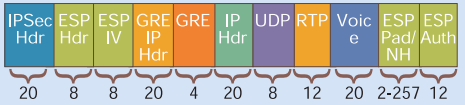
เครื่องมือ QoS ต่างๆ เช่น นโยบายการบริการ Class-Based Weighted Fair Queuing (CBWFQ), Link Fragmentation and Interleaving (LFI) และ Traffic Shaping ยังคงประยุกต์ใช้ได้เหมือนเดิม แต่ Real-Time Transport Protocol (RTP) Header Compression (cRTP) ไม่อาจใช้ได้เนื่องจากไม่คอมแพตทิเบิลกับ IPSec ส่วนคุณสมบัติใหม่ชื่อ QoS Pre-Classify ใน Cisco IOS Software สามารถเปิดใช้งานในเราเตอร์ VPN ของสาขาเพื่อช่วยให้งานการจัดลำดับความสำคัญในขณะที่เข้ารหัสมีความถูกต้องสมบูรณ์สูงสุด

Cisco Systems

PACKET

การคำนวณแบนด์วิดธ์ V³PN

IPSec (และ GRE) ทำให้แพ็กเก็ต VoIP มีภาระเพิ่มขึ้น ซึ่งภาระที่เพิ่มขึ้นนี้ขึ้นอยู่กับออปชัน IPSec, GRE และ VoIP ตัวอย่างด้านล่างนี้แสดงให้เห็นถึง G.729 Voice CODEC ที่ส่งข้อมูลเสียงออกไป 20 ไบต์ ในขณะที่ IP/RTP/UDP ทำให้ข้อมูลเพิ่มอีก 40 ไบต์ ส่วน GRE เพิ่มอีก 24 ไบต์และ IPSec เพิ่มอีก 52 ไบต์ สำหรับขนาดแพ็กเก็ต VoIP โดยรวมที่เข้ารหัสที่ 136 ไบต์



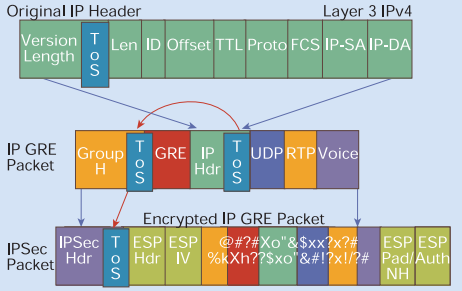
หลังจากที่คำนวณแพ็กเก็ต VoIP โดยรวมที่เข้ารหัสได้แล้ว เราสามารถคำนวณการจัดสรรแบนด์วิดธ์โดยการคูณขนาดแพ็กเก็ตโดยรวมกับอัตราของแพ็กเก็ต ตัวเลขนี้จะคูณโดย 8 (ตัวเลขของบิต/ไบต์) จนได้ผลออกมาเป็นอัตราบิต/วินาที ตัวอย่างการคำนวณมีดังนี้

G.711 CODEC, 20ms sampling, 50 pps

(200 VoIP+76 IPSec/GRE+4 L2)x50x8 = 133.6 Kbit/s

การจองไบต์ ToS

IPSec (และ GRE) จะจองข้อมูลไบต์ ToS โดยอัตโนมัติเพื่อรองรับนโยบายบริการ QoS โดยที่เนื้อหาของไบต์ ToS จากแพ็กเก็ตไอพีดั้งเดิมจะถูกคัดลอกในช่วงขั้นตอนการเข้ารหัสไปยังไอพีเฮดเดอร์ใหม่ที่ IPSec เพิ่มเข้าไป นโยบายบริการ QoS สามารถใช้ข้อมูลของไบต์ ToS ใน IPSec IP header เพื่อจัดลำดับความสำคัญของสัญญาณต่อไป



รายการสิ่งที่ต้องทำสำหรับการออกแบบ V³PN

- ❑ คำนวณความจำเป็นต้องใช้แบนด์วิดธ์ซึ่งอิงกับ CODEC และภาระที่เพิ่มขึ้นของ IPSec/GRE (ตัวเลข cRTP ใช้ไม่ได้)
- ❑ กำหนดนโยบายบริการ QoS และ Call AdminssionControl โดยอิงกับการจัดสรรแบนด์วิดธ์
- ❑ คัดเลือกผู้ให้บริการ (ขอแนะนำให้เลือกใช้บริการ IP Multiservice VPN จากบริษัทผู้ผ่านการรับรองของซิสโก้ (Cisco Powered Network provider)
- ❑ ติดตั้ง QoS ที่ขอบของแวนเหมือนกับระบบโทรศัพท์ไอพีกับระบบแวนส่วนตัว
- ❑ ติดตั้ง IPSec/GRE VPN รวมทั้งใช้ฮาร์ดแวร์เร่งความเร็ว VPN ในเราเตอร์ VPN
- ❑ เปิดการทำงานของ QoS Pre-Classify ในเราเตอร์ VPN ของสาขา
- ❑ แยกแยะว่า anti-replay และ crypto congestion ไม่ได้รับผลกระทบ