Google for Education

Google Education – คำแนะนำการเตรียมโครงสร้างพื้นฐานการเข้าถึงอินเตอร์เนต

สารบัญ

  แบนด์วิดท์เข้าสู่สถานศึกษา (รวมถึงระบบสำรอง)

Google Education – คู่มือโครงสร้างพื้นฐานของการเข้าถึง

ภาพรวม

เอกสารนี้จัดทำขึ้นเพื่อเป็นแนวทางในการสร้างโครงสร้างพื้นฐานของการเข้าถึงอินเทอร์เน็ต (ระบบเครือข่าย) สำหรับสถานศึกษาซึ่งจะสนับสนุนบริการระบบคลาวด์ โดยจะแนะนำองค์ประกอบต่างๆ ของการเข้าถึงที่คุณควรพิจารณา ตลอดจนมาตรฐานที่จำเป็นสำหรับเครือข่ายที่ใช้งานง่ายและสามารถใช้ในการเข้าถึงบริการระบบคลาวด์และสิ่งที่ควรทำเมื่อทำให้โครงสร้างพื้นฐานใช้งานได้ และจะชี้ให้เห็นถึงโซลูชันบางอย่างที่ใช้ได้ในปัจจุบันและพาร์ทเนอร์ในหลากหลายภูมิภาคของโลกที่จะช่วยทำให้เครือข่ายใช้งานได้อย่างมีประสิทธิภาพ นอกจากนี้ยังมีเทมเพลตสำหรับการพัฒนาแผนปฏิบัติงานของคุณ

ข้อจำกัดความรับผิด

Google ไม่ได้ให้การสนับสนุนทางเทคนิคในการกำหนดค่าผลิตภัณฑ์ของบุคคลที่สาม ในกรณีที่เกิดปัญหากับผลิตภัณฑ์ของบุคคลที่สาม คุณควรปรึกษาผู้ดูแลระบบเครือข่าย GOOGLE ไม่มีส่วนรับผิดชอบต่อผลิตภัณฑ์ของบุคคลที่สาม คุณสามารถติดต่อผู้ให้บริการโซลูชันของ Google เกี่ยวกับบริการให้คำปรึกษาได้ ลิงก์ไปยังเว็บไซต์ของบุคคลที่สามมีให้เพื่ออำนวยความสะดวก ลิงก์และเนื้อหาที่เชื่อมโยงกับลิงก์อาจมีการเปลี่ยนแปลงโดยไม่ได้แจ้งให้ทราบ โปรดอ่านข้อมูลในเว็บไซต์ผลิตภัณฑ์ที่เกี่ยวข้องเพื่อดูข้อมูลล่าสุดในการกำหนดค่าและการสนับสนุน

องค์ประกอบของโครงสร้างพื้นฐานของการเข้าถึง

ต่อไปนี้เป็นส่วนต่างๆ ทั้งหมดของเครือข่ายการเข้าถึงที่มีผลต่อการทำให้ใช้งานได้ในสถานศึกษาที่ประสบผลสำเร็จ

a. แบนด์วิดท์เข้าสู่สถานศึกษา (รวมถึงระบบสำรอง)
b. ไฟร์วอลล์
c. การเชื่อมต่อ WAN / ระหว่างวิทยาเขต
d. LAN
    i. เราเตอร์
    ii. สวิตช์
    iii. VLANS
    iv. พอร์ตแบบใช้สาย
    v. Wi-Fi
        1. การวางแผนสัญญาณวิทยุ AP
        2. กำลังของ AP
    vi. เครื่องมือควบคุมการเข้าถึง
    vii. DHCP
    viii. DNS
e. ซอฟต์แวร์การจัดการเครือข่าย
f. ซอฟต์แวร์การตรวจสอบ
g. การกรองเนื้อหา
h. การควบคุมการเข้าถึง / การรักษาความปลอดภัย
    i. SSO
    ii. RADIUS

เอกสารนี้จะกล่าวถึงหัวข้อต่างๆ ข้างต้นที่ปรากฏเป็นตัวหนา ส่วนที่เหลือจะมีการกล่าวถึงใน
เอกสารของ Google “แนวทางปฏิบัติที่แนะนำของเครือข่ายสำหรับการทำให้ใช้งานได้ขนาดใหญ่”

มาตรฐานขั้นต่ำสำหรับการเข้าถึงบริการระบบคลาวด์ของ Google

ตารางด้านล่างนี้แสดงความเร็วขั้นต่ำที่ต้องการสำหรับผู้ใช้แต่ละรายที่ใช้งานพร้อมกัน เพื่อที่จะมีประสบการณ์ในการใช้งานที่ยอมรับได้ในขั้นต่ำ โดยสรุป

ต่อ**ผู้ใช้ที่ใช้งานพร้อมกัน** คุณต้องการความเร็วระหว่าง 64kbps ถึง 1Mbps โดยขึ้นอยู่กับว่าผู้ใช้ของคุณใช้บริการอะไร สูตรง่ายๆ ก็คือ

$$TBWx = (\%C * CCUx * SBWx)_1 + (\%C * CCUx * SBWx)_2 + ... + (\%C * CCUx * SBWx)_n$$

- TBWx = BW รวมที่ระดับ X ของเครือข่าย
- CCUx = จำนวนผู้ใช้ที่ใช้งานพร้อมกันที่ระดับ X ของเครือข่าย
- %C = เปอร์เซ็นต์ของผู้ใช้ที่ใช้งานพร้อมกันสำหรับบริการหนึ่งๆ ในระดับ x ของเครือข่าย
- SBWx = ค่า Kbps ที่แนะนำโดยอ้างอิงบริการ (ดูตารางด้านล่าง)
- n = จำนวนบริการที่เข้าถึงในระดับ x ของเครือข่าย

ประสบการณ์ของผู้ใช้จะได้รับผลกระทบอย่างมากจากเวลาในการตอบสนองของเซิร์ฟเวอร์ของ Google

บริการของ Google Apps	การเชื่อมต่อ 12Kbps	การเชื่อมต่อ 32Kbps	การเชื่อมต่อ 64Kbps	การเชื่อมต่อ 128Kbps ขึ้นไป
Gmail	2 นาทีในการโหลด ถ้าโหลดได้	หน้าเริ่มต้น 8-20 วินาที โหลดทั้งหมด > 1 นาที	- โหลดทั้งหมด 2 - 5 วินาที	ดีกว่า 64kbs
แชทใน Gmail	ไม่สามารถโหลด	> 1 นาทีในการโหลด ถ้าโหลดได้	โหลดใน 4 - 10 วินาที	ดีกว่า 64kbs
เอกสาร/สเปรดชีต (เปิดเอกสาร)	ไม่สามารถโหลด	- หน้าเริ่มต้น 5-20 วินาที - โหลดทั้งหมด > 1 นาที	4 - 10 วินาที	ดีกว่า 64kbs
เอกสาร/สเปรดชีต (การแก้ไขร่วมกัน)	ไม่สามารถโหลด	การแก้ไขจะปรากฏช้ากว่ามากเมื่อเทียบกับ 64K	การเปลี่ยนแปลงจะปรากฏโดยเร็วพอที่จะดูเหมือนเป็นการสนทนา กล่าวคือเป็นแบบเรียลไทม์	ดีกว่า 64kbs
การแก้ไขไซต์	ไม่มีการทดสอบ	ไม่มีการทดสอบ	หน้าข้อความจะโหลดใน 3 - 5 วินาที เครื่องมือแก้ไขจะโหลดภายในเวลาเทียบได้กับการโหลดภาพไฟล์ jpeg ขนาด 385KB ประมาณ 1 นาที	หน้าข้อความโหลดใน 2 - 4 วินาที เครื่องมือแก้ไขโหลดภายในเวลาเทียบได้กับการโหลดภาพไฟล์ jpeg ขนาด 385KB ประมาณ 25 วินาที
สไลด์			4 - 10 วินาที ความเร็วอยู่ในระดับพอทำงานได้สำหรับการแก้ไข	ดีกว่า 64kbps
แฮงเอาท์	ไม่มีข้อมูล	ไม่มีข้อมูล	เสียงเท่านั้น: 35kbps อัปโหลด/ดาวน์โหลด	วิดีโอ: เริ่มต้นที่ 150kbps อัปโหลด / 500kbps ดาวน์โหลด จนถึงค่าที่เหมาะสม = 1 Mbps อัปโหลด/ดาวน์โหลด
ไดรฟ์			4 - 8 วินาที ความเร็วอยู่ในระดับพอทำงานได้ในการโหลดรายชื่อในไดรฟ์	ดีกว่า 64kbps
Youtube				500kbps ขึ้นไป
Chromebook **และแท็บเล็ต**				แนะนำ 200kbps ถึง 512kbps ต่อผู้ใช้ที่ใช้งานพร้อมกัน แท็บเล็ต

คู่มือการทำให้ใช้งานได้

สำหรับองค์ประกอบของเครือข่ายการเข้าถึงที่ไม่ได้กล่าวถึงในเอกสารของ Google “แนวทางปฏิบัติที่แนะนำสำหรับการทำให้ใช้งานได้ขนาดใหญ่” ตารางด้านล่างจะให้คำแนะนำการทำให้ใช้งานได้สำหรับเครือข่ายขนาดเล็ก ปานกลาง และขนาดใหญ่

พื้นที่ในการเข้าถึง	**เครือข่ายขนาดเล็ก** ให้บริการผู้ใช้ที่ใช้งานพร้อมกัน < 500 คน - ผู้ใช้รวมไม่เกิน 2000 คน - 1 หรือ 2 อาคาร - < 1000 ตารางเมตร	**เครือข่ายขนาดกลาง** ให้บริการผู้ใช้ที่ใช้งานพร้อมกัน 500 - 2000 คน - ผู้ใช้รวมระหว่าง 2K -> 10K - 3 ถึง 15 อาคาร - วิทยาเขตเดียว	**เครือข่ายขนาดใหญ่** ให้บริการผู้ใช้ที่ใช้งานพร้อมกัน 2000 - 5000 คน - **ผู้ใช้รวมระหว่าง** 10K -> 50K - 16 ถึง 100 อาคาร - หลายวิทยาเขต
แบนด์วิดท์เข้าสู่สถานศึกษา (รวมถึงระบบสำรอง) 64kbps, 128kbps **หรือ** 512kbps **ต่อผู้ใช้ที่ใช้งานพร้อมกัน**	ต่ำสุด = 32 Mbps ปานกลาง = 64 Mbps สูง = 256 Mbps	ต่ำสุด = 32 Mbps ปานกลาง = 256 Mbps สูง = 1 Gbps	ต่ำสุด = 320 Mbps ปานกลาง = 640 Mbps สูง = 2.5 Gbps
ไฟร์วอลล์	ถ้าคุณสามารถดำเนินการได้โดยไม่ต้องใช้การควบคุมไฟร์วอลล์ L7 คุณสามารถใช้ ACL ของเราเตอร์สำหรับกฎอนุญาต/ปฏิเสธแบบง่าย มิฉะนั้นให้ซื้อไฟร์วอลล์ขนาดกลางที่มีการกำหนดขนาดอย่างเหมาะสม (โปรดดูที่การกำหนดขนาดองค์ประกอบในเครือข่ายขนาดใหญ่)	ถ้าคุณสามารถดำเนินการได้โดยไม่ต้องใช้การควบคุมไฟร์วอลล์ L7 คุณสามารถใช้ ACL ของเราเตอร์สำหรับกฎอนุญาต/ปฏิเสธแบบง่าย มิฉะนั้นให้ซื้อไฟร์วอลล์ขนาดกลางที่มีการกำหนดขนาดอย่างเหมาะสม (โปรดดูที่การกำหนดขนาดองค์ประกอบในเครือข่ายขนาดใหญ่)	ตามปกติคุณจะต้องใช้ไฟร์วอลล์ขนาดใหญ่ ซึ่งกำหนดขนาดสำหรับ - ความจุของเครือข่าย - การเชื่อมต่อต่อวินาที - การเชื่อมต่อในเวลาเดียวกัน - แพ็กเก็ตต่อวินาที - อัตราการส่งผ่าน VPN (ถ้าต้องการ) - อัตราการส่งผ่าน IPS (ถ้าต้องการ) - เมตริกความจุอื่นๆ
LAN : เราเตอร์	เลือกเราเตอร์ที่มีความจุ (CPU, หน่วยความจำ, แบ็คเพลน...) เพื่อ - กำหนดเส้นทางสำหรับความเร็วลิงก์ - มีอินเทอร์เฟซหลากหลายซึ่งคุณจะใช้ในปัจจุบันและในอนาคตอันใกล้ (T3/E3, GbE Copper หรือ Fiber (SFP)	เลือกเราเตอร์ที่มีความจุ (CPU, หน่วยความจำ, แบ็คเพลน...) เพื่อ - กำหนดเส้นทางสำหรับความเร็วลิงก์ - มีอินเทอร์เฟซหลากหลายซึ่งคุณจะใช้ในปัจจุบันและในอนาคตอันใกล้ (T3/E3, GbE Copper หรือ Fiber (SFP)	เลือกเราเตอร์ที่มีความจุ (CPU, หน่วยความจำ, แบ็คเพลน...) เพื่อ - กำหนดเส้นทางสำหรับความเร็วลิงก์ - มีอินเทอร์เฟซหลากหลายซึ่งคุณจะใช้ในปัจจุบันและในอนาคตอันใกล้ (T3/E3, GbE Copper หรือ Fiber (SFP)
LAN : สวิตช์	พิจารณาองค์ประกอบต่อไปนี้ในบทความนี้เมื่อเลือกแฟบริกของสวิตช์	พิจารณาองค์ประกอบต่อไปนี้ในบทความนี้เมื่อเลือกแฟบริกของสวิตช์	พิจารณาองค์ประกอบต่อไปนี้ในบทความนี้เมื่อเลือกแฟบริกของสวิตช์
LAN : VLANS	ในการลดขนาดของโดเมนการเผยแพร่ของคุณ โปรดพิจารณาใช้ VLAN (ดูบทความและบทแนะนำแบบง่าย) นอกจากนี้สามารถใช้การแท็ก VLAN กับการรับส่งข้อมูลไร้สายตราบเท่าที่ AP และเครื่องมือควบคุมระบบไร้สายสามารถรองรับได้ นอกจากนี้ ขอแนะนำว่าแต่ละ SSID ควรมี VLAN ของตนเอง	ในการลดขนาดของโดเมนการเผยแพร่ของคุณ โปรดพิจารณาใช้ VLAN (ดูบทความและบทแนะนำแบบง่าย) นอกจากนี้สามารถใช้การแท็ก VLAN กับการรับส่งข้อมูลไร้สายตราบเท่าที่ AP และเครื่องมือควบคุมระบบไร้สายสามารถรองรับได้ นอกจากนี้ ขอแนะนำว่าแต่ละ SSID ควรมี VLAN ของตนเอง	ในการลดขนาดของโดเมนการเผยแพร่ของคุณ โปรดพิจารณาใช้ VLAN (ดูบทความและบทแนะนำแบบง่าย) นอกจากนี้สามารถใช้การแท็ก VLAN กับการรับส่งข้อมูลไร้สายตราบเท่าที่ AP และเครื่องมือควบคุมระบบไร้สายสามารถรองรับได้ นอกจากนี้ ขอแนะนำว่าแต่ละ SSID ควรมี VLAN ของตนเอง

ต่อ

พื้นที่ในการเข้าถึง	**เครือข่ายขนาดเล็ก**	**เครือข่ายขนาดกลาง**	**เครือข่ายขนาดใหญ่**
LAN : **พอร์ตแบบใช้สาย**	พิจารณาว่าต้องใช้พอร์ตเครือข่ายแบบใช้สายหรือไม่ และในพื้นที่ใด	พิจารณาว่าต้องใช้พอร์ตเครือข่ายแบบใช้สายหรือไม่ และในพื้นที่ใด	พิจารณาว่าต้องใช้พอร์ตเครือข่ายแบบใช้สายหรือไม่ และในพื้นที่ใด
	ใช้พอร์ตจำนวนเท่าใดต่อพื้นที่ และมีจำนวนเท่าใดสำหรับ AP และอุปกรณ์อื่นๆ	ใช้พอร์ตจำนวนเท่าใดต่อพื้นที่ และมีจำนวนเท่าใดสำหรับ AP และอุปกรณ์อื่นๆ	ใช้พอร์ตจำนวนเท่าใดต่อพื้นที่ และมีจำนวนเท่าใดสำหรับ AP และอุปกรณ์อื่นๆ
	การเดินสาย - อย่างน้อย CAT 5 (สูงสุด 100Mbps)	การเดินสาย - อย่างน้อย CAT 5e พิจารณาไฟเบอร์ถ้าระยะห่างระหว่างโหนด > 100 เมตร (สูงสุด 1Gbps)	การเดินสาย - อย่างน้อย CAT 6 ใช้ไฟเบอร์เพื่อเชื่อมต่อวิทยาเขต (สูงสุด 10Gbps)
LAN : Wi-Fi : **การวางแผนสัญญาณวิทยุ AP**	การวางแผนสัญญาณวิทยุเป็นเรื่องสำคัญมากสำหรับการทำให้ Wi-Fi ใช้งานได้ผลสำเร็จ วางแผนใช้หลายช่วงความถี่วิทยุ	การวางแผนสัญญาณวิทยุเป็นเรื่องสำคัญมากสำหรับการทำให้ Wi-Fi ใช้งานได้ผลสำเร็จ วางแผนใช้หลายช่วงความถี่วิทยุ	การวางแผนสัญญาณวิทยุเป็นเรื่องสำคัญมากสำหรับการทำให้ Wi-Fi ใช้งานได้ผลสำเร็จ วางแผนใช้หลายช่วงความถี่วิทยุ
	- 2.4Ghz (802.11 b,g,n) - 5Ghz (802.11 a, n **และ** ac)	- 2.4Ghz (802.11 b,g,n) - 5Ghz (802.11 a, n **และ** ac)	- 2.4Ghz (802.11 b,g,n) - 5Ghz (802.11 a, n **และ** ac)
	ขอแนะนำให้ใช้สัญญาณวิทยุ 5Ghz ถ้าขอบเขตการติดตั้งมีขนาดใหญ่ เนื่องจากมีช่องที่แยกห่างจากกันมากกว่า และสามารถรองรับสัญญาณวิทยุ AP ได้มากกว่า และรองรับผู้ใช้มากกว่า	ขอแนะนำให้ใช้สัญญาณวิทยุ 5Ghz ถ้าขอบเขตการติดตั้งมีขนาดใหญ่ เนื่องจากมีช่องที่แยกห่างจากกันมากกว่า และสามารถรองรับสัญญาณวิทยุ AP ได้มากกว่า และรองรับผู้ใช้มากกว่า	ขอแนะนำให้ใช้สัญญาณวิทยุ 5Ghz ถ้าขอบเขตการติดตั้งมีขนาดใหญ่ เนื่องจากมีช่องที่แยกห่างจากกันมากกว่า และสามารถรองรับสัญญาณวิทยุ AP ได้มากกว่า และรองรับผู้ใช้มากกว่า
	ขั้นตอนการวางแผนขั้นพื้นฐานมีอ้างอิงอยู่ใน**บทความนี้**	ขั้นตอนการวางแผนขั้นพื้นฐานมีอ้างอิงอยู่ใน**บทความนี้**	ขั้นตอนการวางแผนขั้นพื้นฐานมีอ้างอิงอยู่ใน**บทความนี้**
	ในทุกกรณี คุณควรใช้เครื่องมือวางแผน ซึ่งเป็นไปได้มากว่าจะมีให้จากผู้ขายอุปกรณ์ของคุณ	ในทุกกรณี คุณควรใช้เครื่องมือวางแผน ซึ่งเป็นไปได้มากว่าจะมีให้จากผู้ขายอุปกรณ์ของคุณ	ในทุกกรณี คุณควรใช้เครื่องมือวางแผน ซึ่งเป็นไปได้มากว่าจะมีให้จากผู้ขายอุปกรณ์ของคุณ
LAN : Wi-Fi : **กำลังของ AP**	พิจารณาใช้ Power over Ethernet (PoE) เพื่อให้พลังงานกับ AP และอุปกรณ์อื่นๆ วิธีนี้จะทำให้คุณไม่ต้องใช้สายไฟ/พอร์ตไฟฟ้าแยกต่างหากสำหรับ AP, โทรศัพท์ IP, กล้อง และอื่นๆ	พิจารณาใช้ Power over Ethernet (PoE) เพื่อให้พลังงานกับ AP และอุปกรณ์อื่นๆ วิธีนี้จะทำให้คุณไม่ต้องใช้สายไฟ/พอร์ตไฟฟ้าแยกต่างหากสำหรับ AP, โทรศัพท์ IP, กล้อง และอื่นๆ	พิจารณาใช้ Power over Ethernet (PoE) เพื่อให้พลังงานกับ AP และอุปกรณ์อื่นๆ วิธีนี้จะทำให้คุณไม่ต้องใช้สายไฟ/พอร์ตไฟฟ้าแยกต่างหากสำหรับ AP, โทรศัพท์ IP, กล้อง และอื่นๆ
	PoE: 15.4 W ต่อพอร์ต สามารถให้พลังงานกับ AP ตามปกติจะไม่เพียงพอที่จะให้พลังงานกับกล้องหรือโทรศัพท์ IP	PoE: 15.4 W ต่อพอร์ต สามารถให้พลังงานกับ AP ตามปกติจะไม่เพียงพอที่จะให้พลังงานกับกล้องหรือโทรศัพท์ IP	PoE: 15.4 W ต่อพอร์ต สามารถให้พลังงานกับ AP ตามปกติจะไม่เพียงพอที่จะให้พลังงานกับกล้องหรือโทรศัพท์ IP
	PoE+: 25.5 W ต่อพอร์ต ราคาแพงกว่า แต่สามารถให้พลังงานกับโทรศัพท์ กล้อง และอุปกรณ์อื่นๆ	PoE+: 25.5 W ต่อพอร์ต ราคาแพงกว่า แต่สามารถให้พลังงานกับโทรศัพท์ กล้อง และอุปกรณ์อื่นๆ	PoE+: 25.5 W ต่อพอร์ต ราคาแพงกว่า แต่สามารถให้พลังงานกับโทรศัพท์ กล้อง และอุปกรณ์อื่นๆ
	* โปรดทราบว่าสวิตช์ LAN ของคุณควรรองรับมาตรฐาน PoE ที่คุณเลือก บางพอร์ตของสวิตช์อาจไม่รองรับ PoE คุณสามารถใช้สวิตช์ทั้ง 2 มาตรฐานร่วมกันเพื่อจ่ายพลังงานต่างระดับในพื้นที่หนึ่งๆ	* โปรดทราบว่าสวิตช์ LAN ของคุณควรรองรับมาตรฐาน PoE ที่คุณเลือก บางพอร์ตของสวิตช์อาจไม่รองรับ PoE คุณสามารถใช้สวิตช์ทั้ง 2 มาตรฐานร่วมกันเพื่อจ่ายพลังงานต่างระดับในพื้นที่หนึ่งๆ	* โปรดทราบว่าสวิตช์ LAN ของคุณควรรองรับมาตรฐาน PoE ที่คุณเลือก บางพอร์ตของสวิตช์อาจไม่รองรับ PoE คุณสามารถใช้สวิตช์ทั้ง 2 มาตรฐานร่วมกันเพื่อจ่ายพลังงานต่างระดับในพื้นที่หนึ่งๆ

ต่อ

พื้นที่ในการเข้าถึง	เครือข่ายขนาดเล็ก	เครือข่ายขนาดกลาง	เครือข่ายขนาดใหญ่
LAN : เครื่องมือควบคุมการเข้าถึง Wi-Fi	สำหรับเครือข่ายขนาดเล็กมาก < 10 จุดเชื่อมต่อ คุณอาจสามารถติดตั้งใช้งานโดยไม่ต้องมีเครื่องมือควบคุมการเข้าถึง ถ้าคุณใช้เครื่องมือควบคุมการเข้าถึง คุณจะสามารถเลือกได้ระหว่าง - เครื่องมือควบคุมแบบซอฟต์แวร์ที่คุณสามารถติดตั้งในคอมพิวเตอร์ (เช่น ubiquiti Unifi) - อุปกรณ์ฮาร์ดแวร์ (เช่น Rukus, Mikrotik รุ่น CCR) - เครื่องมือควบคุมระบบคลาวด์ (เช่น Meraki) ในทุกกรณี โปรดใช้เครื่องมือควบคุมการเข้าถึงที่ผลิตโดย และตรงกับผู้ให้บริการ AP ของคุณ และถ้าคุณมีเครือข่ายแบบไฮบริด ซึ่งมี AP สองประเภทขึ้นไปซึ่งมีการจัดการโดยเครื่องมือควบคุมการเข้าถึงสองแบบขึ้นไป โปรดดำเนินการให้มั่นใจว่าคุณได้จัดให้ AP ชุดหนึ่งและเครื่องมือควบคุมการเข้าถึงที่สอดคล้องกันอยู่ในพื้นที่ติดกัน อย่าผสม AP หลายประเภท และฟังก์ชันการทำงานของเครื่องมือควบคุมหลายแบบไว้ในพื้นที่เดียวกัน เนื่องจากจะลดความสามารถและประสิทธิภาพของเครื่องมือควบคุม	เป็นไปได้ว่าในเครือข่ายขนาดนี้คุณจะมี AP มากกว่า 10 เครื่อง และขอแนะนำให้คุณใช้เครื่องมือควบคุมการเข้าถึงที่ตรงกับแบรนด์ของ AP ที่ใช้ คุณจะมีตัวเลือกระหว่าง - เครื่องมือควบคุมแบบซอฟต์แวร์ที่คุณสามารถติดตั้งในคอมพิวเตอร์ (เช่น ubiquiti Unifi) - อุปกรณ์ฮาร์ดแวร์ (เช่น Rukus) - เครื่องมือควบคุมระบบคลาวด์ (เช่น Meraki) ในทุกกรณี โปรดใช้เครื่องมือควบคุมการเข้าถึงที่ผลิตโดย และตรงกับผู้ให้บริการ AP ของคุณ และถ้าคุณมีเครือข่ายแบบไฮบริด ซึ่งมี AP สองประเภทขึ้นไปซึ่งมีการจัดการโดยเครื่องมือควบคุมการเข้าถึงสองแบบขึ้นไป โปรดดำเนินการให้มั่นใจว่าคุณได้จัดให้ AP ชุดหนึ่งและเครื่องมือควบคุมการเข้าถึงที่สอดคล้องกันอยู่ในพื้นที่ติดกัน อย่าผสม AP หลายประเภท และฟังก์ชันการทำงานของเครื่องมือควบคุมหลายแบบไว้ในพื้นที่เดียวกัน เนื่องจากจะลดความสามารถและประสิทธิภาพของเครื่องมือควบคุม	แทบจะเรียกได้ว่าเป็นข้อกำหนดที่คุณจะต้องมีเครื่องมือควบคุมการเข้าถึงที่ตรงกับแบรนด์ของ AP ที่คุณใช้ คุณจะมีตัวเลือกระหว่าง - เครื่องมือควบคุมแบบซอฟต์แวร์ที่คุณสามารถติดตั้งในคอมพิวเตอร์ (เช่น ubiquiti Unifi) - อุปกรณ์ฮาร์ดแวร์ (เช่น Rukus) - เครื่องมือควบคุมระบบคลาวด์ (เช่น Meraki) ในทุกกรณี โปรดใช้เครื่องมือควบคุมการเข้าถึงที่ผลิตโดย และตรงกับผู้ให้บริการ AP ของคุณ และถ้าคุณมีเครือข่ายแบบไฮบริด ซึ่งมี AP สองประเภทขึ้นไปซึ่งมีการจัดการโดยเครื่องมือควบคุมการเข้าถึงสองแบบขึ้นไป โปรดดำเนินการให้มั่นใจว่าคุณได้จัดให้ AP ชุดหนึ่งและเครื่องมือควบคุมการเข้าถึงที่สอดคล้องกันอยู่ในพื้นที่ติดกัน อย่าผสม AP หลายประเภท และฟังก์ชันการทำงานของเครื่องมือควบคุมหลายแบบไว้ในพื้นที่เดียวกัน เนื่องจากจะลดความสามารถและประสิทธิภาพของเครื่องมือควบคุม

ต่อ

พื้นที่ในการเข้าถึง	**เครือข่ายขนาดเล็ก**	**เครือข่ายขนาดกลาง**	**เครือข่ายขนาดใหญ่**
LAN DHCP	ใช้เซิร์ฟเวอร์ DHCP ในเครือข่ายของคุณเพื่อมอบหมายที่อยู่ IP แบบไดนามิกให้กับอุปกรณ์แต่ละชิ้น เราเตอร์และสวิตช์ส่วนใหญ่มีเซิร์ฟเวอร์ DHCP ในตัว ถ้าอุปกรณ์ของคุณไม่มี คุณสามารถใช้เซิร์ฟเวอร์ DHCP ในเครื่อง Linux (dhcpd) มอบหมาย IP แบบไดนามิกให้กับไคลเอ็นต์ (เดสก์ท็อป แล็ปท็อป อุปกรณ์เคลื่อนที่ เป็นต้น) แต่มอบหมายที่อยู่ IP แบบคงที่ให้กับเซิร์ฟเวอร์และเราเตอร์ เก็บช่วงที่อยู่ IP ที่อยู่นอกช่วงของ DHCP ไว้สำหรับกรณีเหล่านี้ กำหนดค่า DHCP ของคุณเพื่อให้ช่วงของที่อยู่ IP ที่สามารถออกได้นั้นมีมากพอที่จะรองรับไคลเอ็นต์ทั้งหมดในเครือข่ายปัจจุบัน + ผู้ใช้ภายนอก + การขยายตัวในอนาคต พิจารณากำหนดค่าช่วง IP ที่ต่างกันสำหรับไคลเอ็นต์ที่ใช้สายและไร้สาย	ใช้เซิร์ฟเวอร์ DHCP ในเครือข่ายของคุณเพื่อมอบหมายที่อยู่ IP แบบไดนามิกให้กับอุปกรณ์แต่ละชิ้น เราเตอร์และสวิตช์ส่วนใหญ่มีเซิร์ฟเวอร์ DHCP ในตัว ถ้าอุปกรณ์ของคุณไม่มี คุณสามารถใช้เซิร์ฟเวอร์ DHCP ในเครื่อง Linux (dhcpd) มอบหมาย IP แบบไดนามิกให้กับไคลเอ็นต์ (เดสก์ท็อป แล็ปท็อป อุปกรณ์เคลื่อนที่ เป็นต้น) แต่มอบหมายที่อยู่ IP แบบคงที่ให้กับเซิร์ฟเวอร์และเราเตอร์ เก็บช่วงที่อยู่ IP ที่อยู่นอกช่วงของ DHCP ไว้สำหรับกรณีเหล่านี้ กำหนดค่า DHCP ของคุณเพื่อให้ช่วงของที่อยู่ IP ที่สามารถออกได้นั้นมีมากพอที่จะรองรับไคลเอ็นต์ทั้งหมดในเครือข่ายปัจจุบัน + ผู้ใช้ภายนอก + การขยายตัวในอนาคต พิจารณากำหนดค่าช่วง IP ที่ต่างกันสำหรับไคลเอ็นต์ที่ใช้สายและไร้สาย นอกจากนี้คุณยังสามารถกำหนดช่วงให้ต่างกันสำหรับแต่ละเครือข่ายย่อย สำหรับเครือข่ายขนาดกลางคุณสามารถมีระบบ DHCP สำรอง	ใช้เซิร์ฟเวอร์ DHCP ในเครือข่ายของคุณเพื่อมอบหมายที่อยู่ IP แบบไดนามิกให้กับอุปกรณ์แต่ละชิ้น เราเตอร์และสวิตช์ส่วนใหญ่มีเซิร์ฟเวอร์ DHCP ในตัว ถ้าอุปกรณ์ของคุณไม่มี คุณสามารถใช้เซิร์ฟเวอร์ DHCP ในเครื่อง Linux (dhcpd) มอบหมาย IP แบบไดนามิกให้กับไคลเอ็นต์ (เดสก์ท็อป แล็ปท็อป อุปกรณ์เคลื่อนที่ เป็นต้น) แต่มอบหมายที่อยู่ IP แบบคงที่ให้กับเซิร์ฟเวอร์และเราเตอร์ เก็บช่วงที่อยู่ IP ที่อยู่นอกช่วงของ DHCP ไว้สำหรับกรณีเหล่านี้ กำหนดค่า DHCP ของคุณเพื่อให้ช่วงของที่อยู่ IP ที่สามารถออกได้นั้นมีมากพอที่จะรองรับไคลเอ็นต์ทั้งหมดในเครือข่ายปัจจุบัน + ผู้ใช้ภายนอก + การขยายตัวในอนาคต พิจารณากำหนดค่าช่วง IP ที่ต่างกันสำหรับไคลเอ็นต์ที่ใช้สายและไร้สาย นอกจากนี้คุณยังสามารถกำหนดช่วงให้ต่างกันสำหรับแต่ละเครือข่ายย่อย สำหรับเครือข่ายขนาดใหญ่คุณควรมีระบบ DHCP สำรอง ถ้าคุณมีผู้ใช้ภายนอกจำนวนมาก คุณสามารถลดระยะเวลาของการมอบหมายได้
LAN : DNS	ยกเว้นกรณีที่คุณมีอุปกรณ์ < 5 เครื่อง (คอมพิวเตอร์, สวิตช์, เราเตอร์, AP และอื่นๆ) ในเครือข่ายคุณจะต้องใช้ DNS ภายในเพื่อแปลค่าชื่อของเครื่อง เซิร์ฟเวอร์ DHCP ส่วนใหญ่มีเซิร์ฟเวอร์ DNS อยู่แล้ว ทำให้การกำหนดค่าง่ายขึ้นในการแปลค่า IP แบบคงที่และแบบไดนามิกในเครือข่ายภายในของคุณ สำหรับการแปลค่าชื่อภายนอก (เช่น www.google.com) คุณควรใช้ ISP DNS หรือ DNS สาธารณะของ Google ตาม**เอกสารนี้** ในกรณีที่เป็นไปได้ คุณควรมีเซิร์ฟเวอร์ DNS หลายรายการ (สำรอง) เพื่อป้องกันปัญหาการแปลค่าชื่อที่อาจทำให้ดูเหมือนทั้งเครือข่ายของคุณใช้ไม่ได้สำหรับผู้ใช้	คุณจะต้องใช้ DNS ภายในเพื่อแปลค่าชื่อของเครื่อง เซิร์ฟเวอร์ DHCP ส่วนใหญ่มีเซิร์ฟเวอร์ DNS อยู่แล้ว ทำให้การกำหนดค่าง่ายขึ้นในการแปลค่า IP แบบคงที่และแบบไดนามิกในเครือข่ายภายในของคุณ สำหรับการแปลค่าชื่อภายนอก (เช่น www.google.com) คุณควรใช้ ISP DNS หรือ DNS สาธารณะของ Google ตาม**เอกสารนี้** ในกรณีที่เป็นไปได้ คุณควรมีเซิร์ฟเวอร์ DNS หลายรายการ (สำรอง) เพื่อป้องกันปัญหาการแปลค่าชื่อที่อาจทำให้ดูเหมือนทั้งเครือข่ายของคุณใช้ไม่ได้สำหรับผู้ใช้	คุณจะต้องใช้ DNS ภายในเพื่อแปลค่าชื่อของเครื่อง เซิร์ฟเวอร์ DHCP ส่วนใหญ่มีเซิร์ฟเวอร์ DNS อยู่แล้ว ทำให้การกำหนดค่าง่ายขึ้นในการแปลค่า IP แบบคงที่และแบบไดนามิกในเครือข่ายภายในของคุณ สำหรับการแปลค่าชื่อภายนอก (เช่น www.google.com) คุณควรใช้ ISP DNS หรือ DNS สาธารณะของ Google ตาม**เอกสารนี้** ในกรณีที่เป็นไปได้ คุณควรมีเซิร์ฟเวอร์ DNS หลายรายการ (สำรอง) เพื่อป้องกันปัญหาการแปลค่าชื่อที่อาจทำให้ดูเหมือนทั้งเครือข่ายของคุณใช้ไม่ได้สำหรับผู้ใช้

ต่อ

พื้นที่ในการเข้าถึง	เครือข่ายขนาดเล็ก	เครือข่ายขนาดกลาง	เครือข่ายขนาดใหญ่
ซอฟต์แวร์การจัดการเครือข่ายและซอฟต์แวร์การตรวจสอบเครือข่าย	ซอฟต์แวร์การจัดการจะช่วยให้คุณจัดการเครือข่ายจากจุดเดียว โดยที่ส่วนใหญ่จะมี GUI ให้ใช้ ดูรายการตรวจสอบสำหรับเครื่องมือจัดการเครือข่ายในบทความนี้เป็นข้อพิจารณา เมื่อประเมินเครื่องมือเหล่านี้ โปรดพิจารณาว่าคุณสามารถจัดการอุปกรณ์ใดบ้าง และมีจำนวนเท่าใด Spiceworks (ฟรี) OpenNMS Cacti MRTG GFI (ฟรี) เมื่อเลือกซอฟต์แวร์การจัดการเครือข่าย โปรดตรวจสอบว่ามีคุณลักษณะใดให้ฟรี และคุณลักษณะใดมีค่าใช้จ่าย และโปรดตรวจสอบว่ามีเวอร์ชันที่ใช้ได้สำหรับแพลตฟอร์มของคุณ โซลูชันการจัดการเครือข่ายส่วนใหญ่จะมีฟังก์ชันการตรวจสอบให้ด้วย แต่คุณสามารถหาซอฟต์แวร์ที่ทำหน้าที่เฉพาะการตรวจสอบเครือข่ายเพียงอย่างเดียว เช่น Solarwinds (ทดลองใช้ฟรี)	สำหรับเครือข่ายขนาดกลางและขนาดใหญ่ จะสามารถใช้ซอฟต์แวร์การจัดการเครือข่ายและการตรวจสอบเครือข่ายได้ โปรดทราบว่าโมเดลการออกใบอนุญาตสำหรับโซลูชันที่มีค่าใช้จ่ายบางรายการจะอ้างอิงจำนวนอุปกรณ์ที่จัดการ/ตรวจสอบ ดังนั้นถ้าเครือข่ายมีขนาดใหญ่ ใบอนุญาตซอฟต์แวร์ก็จะยิ่งมีราคาแพง	สำหรับเครือข่ายขนาดกลางและขนาดใหญ่ จะสามารถใช้ซอฟต์แวร์การจัดการเครือข่ายและการตรวจสอบเครือข่ายได้ โปรดทราบว่าโมเดลการออกใบอนุญาตสำหรับโซลูชันที่มีค่าใช้จ่ายบางรายการจะอ้างอิงจำนวนอุปกรณ์ที่จัดการ/ตรวจสอบ ดังนั้นถ้าเครือข่ายมีขนาดใหญ่ ใบอนุญาตซอฟต์แวร์ก็จะยิ่งมีราคาแพง
การกรองเนื้อหา	ภายในสถานศึกษานั้นการกรองเนื้อหาเป็นเรื่องที่จำเป็นมาก เพื่อให้คุณสามารถบล็อกภาพอนาจาร ไม่ทำให้องค์กรของคุณได้รับความเสี่ยงต่อการดำเนินคดีตามกฎหมายเนื่องจากการละเมิดลิขสิทธิ์ เนื่องจากผู้ใช้มีการใช้ทอเรนต์เพื่อดาวน์โหลดซอฟต์แวร์และภาพยนตร์ ยังไม่รวมถึงการปรับปรุงประสิทธิภาพของแบนด์วิดท์ ตัวอย่างของตัวกรองเว็บแบบโอเพนซอร์สได้แก่ squidproxy ถ้าคุณใช้ตัวเลือกที่เป็นแบบโอเพนซอร์ส หรือพร็อกซี/ตัวกรองที่มีจำหน่าย โปรดพิจารณาสิ่งต่อไปนี้ 1) การที่สามารถใช้พร็อกซีที่มีความโปร่งใส เพื่อให้คุณไม่ต้องใส่การกำหนดค่าพร็อกซีในไคลเอ็นต์ทั้งหมดของคุณ 2) ตรวจสอบว่าพร็อกซีของคุณสามารถรับมือกับการรับส่งข้อมูลอินเทอร์เน็ตทั้งหมด เนื่องจากคุณไม่ต้องการให้เกิดภาวะคอขวด 3) พิจารณาระบบสำรองหรือการจำลองเครื่องเสมือนเพื่อให้พร็อกซีไม่เป็นจุดที่ทำให้เกิดข้อผิดพลาดกับทั้งระบบได้	ภายในสถานศึกษานั้นการกรองเนื้อหาเป็นเรื่องที่จำเป็นมาก เพื่อให้คุณสามารถบล็อกภาพอนาจาร ไม่ทำให้องค์กรของคุณได้รับความเสี่ยงต่อการดำเนินคดีตามกฎหมายเนื่องจากการละเมิดลิขสิทธิ์ เนื่องจากผู้ใช้มีการใช้ทอเรนต์เพื่อดาวน์โหลดซอฟต์แวร์และภาพยนตร์ ยังไม่รวมถึงการปรับปรุงประสิทธิภาพของแบนด์วิดท์ ตัวอย่างของตัวกรองเว็บแบบโอเพนซอร์สได้แก่ squidproxy ถ้าคุณใช้ตัวเลือกที่เป็นแบบโอเพนซอร์ส หรือพร็อกซี/ตัวกรองที่มีจำหน่าย โปรดพิจารณาสิ่งต่อไปนี้ 1) การที่สามารถใช้พร็อกซีที่มีความโปร่งใส เพื่อให้คุณไม่ต้องใส่การกำหนดค่าพร็อกซีในไคลเอ็นต์ทั้งหมดของคุณ 2) ตรวจสอบว่าพร็อกซีของคุณสามารถรับมือกับการรับส่งข้อมูลอินเทอร์เน็ตทั้งหมด เนื่องจากคุณไม่ต้องการให้เกิดภาวะคอขวด 3) พิจารณาระบบสำรองหรือการจำลองเครื่องเสมือนเพื่อให้พร็อกซีไม่เป็นจุดที่ทำให้เกิดข้อผิดพลาดกับทั้งระบบได้	ภายในสถานศึกษานั้นการกรองเนื้อหาเป็นเรื่องที่จำเป็นมาก เพื่อให้คุณสามารถบล็อกภาพอนาจาร ไม่ทำให้องค์กรของคุณได้รับความเสี่ยงต่อการดำเนินคดีตามกฎหมายเนื่องจากการละเมิดลิขสิทธิ์ เนื่องจากผู้ใช้มีการใช้ทอเรนต์เพื่อดาวน์โหลดซอฟต์แวร์และภาพยนตร์ ยังไม่รวมถึงการปรับปรุงประสิทธิภาพของแบนด์วิดท์ ตัวอย่างของตัวกรองเว็บแบบโอเพนซอร์สได้แก่ squidproxy ถ้าคุณใช้ตัวเลือกที่เป็นแบบโอเพนซอร์ส หรือพร็อกซี/ตัวกรองที่มีจำหน่าย โปรดพิจารณาสิ่งต่อไปนี้ 1) การที่สามารถใช้พร็อกซีที่มีความโปร่งใส เพื่อให้คุณไม่ต้องใส่การกำหนดค่าพร็อกซีในไคลเอ็นต์ทั้งหมดของคุณ 2) ตรวจสอบว่าพร็อกซีของคุณสามารถรับมือกับการรับส่งข้อมูลอินเทอร์เน็ตทั้งหมด เนื่องจากคุณไม่ต้องการให้เกิดภาวะคอขวด 3) พิจารณาระบบสำรองหรือการจำลองเครื่องเสมือนเพื่อให้พร็อกซีไม่เป็นจุดที่ทำให้เกิดข้อผิดพลาดกับทั้งระบบได้

ต่อ

พื้นที่ในการเข้าถึง	เครือข่ายขนาดเล็ก	เครือข่ายขนาดกลาง	เครือข่ายขนาดใหญ่
การควบคุมการเข้าถึง / การรักษาความปลอดภัย: Radius / SSO	การเข้าถึงเครือข่ายของคุณ โดยเฉพาะ Wi-Fi ควรมีการควบคุมซึ่งสามารถทำได้โดยใช้เซิร์ฟเวอร์ Radius และการกำหนดค่า AP ของ Wi-Fi ให้ใช้โครงสร้างพื้นฐาน Radius AAA ในการตรวจสอบสิทธิ์และการเก็บข้อมูล ในการใช้ข้อมูลประจำตัวของ Google สำหรับการเข้าถึง Wi-Fi (แนะนำ) คุณจะต้องเปลี่ยนเส้นทางของการตรวจสอบสิทธิ์ Wi-Fi ไปยังพอร์ทัลที่มีการจำกัดการเข้าถึง และเปลี่ยนเส้นทางไปยังการลงชื่อเข้าใช้ Google ซึ่งสนับสนุน Oauth ผ่านบริการเช่น Cloudessa	การเข้าถึงเครือข่ายของคุณ โดยเฉพาะ Wi-Fi ควรมีการควบคุมซึ่งสามารถทำได้โดยใช้เซิร์ฟเวอร์ Radius และการกำหนดค่า AP ของ Wi-Fi ให้ใช้โครงสร้างพื้นฐาน Radius AAA ในการตรวจสอบสิทธิ์และการเก็บข้อมูล ในการใช้ข้อมูลประจำตัวของ Google สำหรับการเข้าถึง Wi-Fi (แนะนำ) คุณจะต้องเปลี่ยนเส้นทางของการตรวจสอบสิทธิ์ Wi-Fi ไปยังพอร์ทัลที่มีการจำกัดการเข้าถึง และเปลี่ยนเส้นทางไปยังการลงชื่อเข้าใช้ Google ซึ่งสนับสนุน Oauth ผ่านบริการเช่น Cloudessa	การเข้าถึงเครือข่ายของคุณ โดยเฉพาะ Wi-Fi ควรมีการควบคุมซึ่งสามารถทำได้โดยใช้เซิร์ฟเวอร์ Radius และการกำหนดค่า AP ของ Wi-Fi ให้ใช้โครงสร้างพื้นฐาน Radius AAA ในการตรวจสอบสิทธิ์และการเก็บข้อมูล ในการใช้ข้อมูลประจำตัวของ Google สำหรับการเข้าถึง Wi-Fi (แนะนำ) คุณจะต้องเปลี่ยนเส้นทางของการตรวจสอบสิทธิ์ Wi-Fi ไปยังพอร์ทัลที่มีการจำกัดการเข้าถึง และเปลี่ยนเส้นทางไปยังการลงชื่อเข้าใช้ Google ซึ่งสนับสนุน Oauth ผ่านบริการเช่น Cloudessa

เอกสารการวางแผนสัญญาณวิทยุที่มีรายละเอียด (เอกสารนี้เป็นเอกสารที่มีขนาดใหญ่และคุณสามารถใช้อ้างอิงในหัวข้อต่างๆ ได้ตามต้องการ)

โซลูชันที่สามารถใช้ได้
ลิงก์ด้านล่างนี้มีให้ตามสภาพ และ Google ไม่ได้ให้การรับประกันหรือแนะนำโซลูชันอย่างหนึ่งอย่างใดของบุคคลที่ 3 การตัดสินใจว่าโซลูชันใดสามารถตอบสนองความต้องการของสถานศึกษา ขึ้นอยู่กับสถานศึกษานั้นเอง

1. แบนด์วิดท์เข้าสู่สถานศึกษา (รวมถึงระบบสำรอง), การเชื่อมต่อ WAN และการเชื่อมโยงระหว่างวิทยาเขต
    a. ในทุกกรณีจะเป็นการให้บริการโดยผู้ให้บริการอินเทอร์เน็ต/บริษัทโทรคมนาคมในพื้นที่ของคุณ

2. ไฟร์วอลล์
    a. Checkpoint
    b. McAFee
    c. Juniper
    d. Cisco
    e. Barracuda
    f. MicroTik
    g. Fortinet - fortigate

3. LAN : เราเตอร์, สวิตช์
    a. Cisco
    b. Dell
    c. HP
    d. Juniper
    e. Brocade
    f. Netgear
    g. Huawei
    h. ZyXel
    i. Frotinet
    j. MicroTik (router board)
    k. Dlink

4. LAN : Wi-Fi (รวมเครื่องมือควบคุมการเข้าถึง)
   a. Cisco
   b. Ubiquiti
   c. Dell
   d. HP
   e. Juniper
   f. Huawei
   g. ZyXel
   h. MicroTik (Routerboard)
   i. DLink
   j. Fortinet
   k. Aruba
   l. Ruckus
   m. Aerohive
   n. Meru
   o. Xirrus (ประสิทธิภาพสูง)

5. DHCP และ DNS

   ผลิตภัณฑ์สวิตช์ส่วนใหญ่ข้างต้นจะมีเซิร์ฟเวอร์ DHCP / DNS ในตัวหรือเป็นตัวเลือกสแตนด์อโลน ตัวเลือกอื่นๆ ที่ควรพิจารณาได้แก่

   a. ISC.org
   b. Solarwinds

6. ซอฟต์แวร์การจัดการและการตรวจสอบเครือข่าย

   ผลิตภัณฑ์สวิตช์ส่วนใหญ่ข้างต้นจะมีแพลตฟอร์มซอฟต์แวร์การจัดการและการตรวจสอบ และตามปกติคุณจะใช้ซอฟต์แวร์ของผู้ผลิตรายเดียวกันเพื่อจัดการฮาร์ดแวร์ แต่ก็มีโซลูชัน SNMP ทั่วไปเช่นกัน

   a. MRTG (การตรวจสอบ SNMP) (ฟรี)
   b. Nagios (การตรวจสอบทั่วไป)
   c. CACTI
   d. Spiceworks (ฟรี)
   e. OpenNMS
   f. GFI (ฟรี)
   g. Brocade
   h. Cisco
   i. Juniper
   j. HP
   k. Dell
   l. Huawei
   m. Ubiquiti
   n. Fortinet

7. การกรองเนื้อหา
   a. Squid proxy (ฟรี)
   b. Cisco
   c. Barracuda
   d. Fortinet
   e. MicroTik
   f. Checkpoint
   g. Mcafee

8. การควบคุมการเข้าถึง / การรักษาความปลอดภัย (SSO, RADIUS)
   a. Freeradius (ฟรี)
   b. Zeroshell (ฟรี)
   c. Cloudessa (ระบบคลาวด์)
   d. Clearbox
   e. MIcrosoft radius server
   f. Aradial

พัฒนาแผนปฏิบัติงานของคุณ

1. กำหนดขอบเขตขนาดเครือข่ายของคุณ
    a. ระยะเวลาวางแผนสำหรับเครือข่ายนี้ (1, 2, 3, 4, 5 ...10 ปี)
    b. จำนวนผู้ใช้และอุปกรณ์ทั้งหมด
    c. **จำนวนผู้ใช้ที่ใช้งานพร้อมกัน** โดยพิจารณาช่วงเวลาที่มีการใช้งานน้อยและใช้งานสูงสุด
    d. % ของผู้ใช้ที่ใช้สายและไร้สาย
    e. แอปพลิเคชันประเภทอื่นนอกเหนือจากบริการระบบคลาวด์ที่จะทำงาน ในเครือข่ายของคุณ
    f. พูดคุยและตัดสินใจเกี่ยวกับประเด็นด้านนโยบาย การกรองเนื้อหา ใครสามารถเข้าถึงเมื่อใด
2. วางแผนองค์ประกอบของเครือข่ายที่คุณจะเพิ่ม/อัปเกรดเพื่อตอบสนองความต้องการของขอบเขต
3. ขอความเห็นพ้องในองค์กรสำหรับขอบเขตและแผน
4. รับ RFP จากผู้ขาย (ใช้กระบวนการนี้ในการหาความรู้เกี่ยวกับความหลากหลายของโซลูชันต่างๆ ที่มีให้)
5. เลือกจากการส่ง RFP ของผู้ขาย
6. การตรวจทานโซลูชันที่ได้รับเลือกโดยผู้มีส่วนเกี่ยวข้อง และการตกลงซื้อ
7. ออกใบสั่งซื้อ
8. จัดซื้ออุปกรณ์และดำเนินการทำให้ใช้งานได้ (รวมถึงการจัดการการเปลี่ยนแปลง ถ้ามี)
9. ทดสอบการทำให้ใช้งานได้
10. แก้ไขปัญหาที่มี
11. เริ่มใช้งานจริง