

The background of the slide features a faded, light blue image of a business meeting. Several people in professional attire are gathered around a table, looking at a laptop screen. The image is semi-transparent, allowing the text overlay to be clearly visible.

POISE TECHNOLOGY

Thailand VoIP Specialist Company

IP Telephony Performance/Security
Normal Practice

- VoIP เป็นการใช้งานระบบโทรศัพท์ ผ่านระบบเครือข่ายคอมพิวเตอร์ โดยมีการใช้งานอยู่ 3 รูปแบบ
 - การใช้งานภายในระบบเครือข่ายของตนเองเท่านั้น (Private Network)
เช่น การใช้งานตู้สาขาแบบ IP โดยทั่วๆ ไป หรือ มีการเชื่อมโยงแต่ละสาขาเข้าด้วยกันผ่าน VPN เป็นต้น
 - การใช้งานผ่านระบบเครือข่ายอินเทอร์เน็ต (Internet/Public Network)
เช่น การใช้งานกับผู้ใช้บริการโทรศัพท์ผ่านระบบ IP หรือ การใช้งาน Cloud Based
 - แบบผสมผสาน โดยมีการใช้งานทั้งบน Private และ ทั้งบน Public Network
เช่น การใช้งานตู้สาขาแบบ IP พร้อมการเปิดให้มีผู้ใช้งานจากระบบอินเทอร์เน็ตด้วย เป็นต้น



- อะไรคือปัจจัยเสี่ยงและความเสียหายที่อาจเกิดกับระบบ IP-Telephony
 - การใช้งานโทรศัพท์ไปยังเบอร์ปลายทางโดยไม่ได้รับอนุญาต Toll-fraud (high risk)
 - การถูกทำให้ระบบใช้งานไม่ได้ (medium risk)
 - ระบบใช้งานไม่ได้ที่เกิดจากตัวอุปกรณ์เอง (medium risk)
 - การถูกแอบอ้างการใช้งาน เช่น spam (low risk)
 - การถูกแอบฟังการสนทนา (low risk)



- ปัจจัยเสี่ยงที่เกิดกับระบบ IP-Telephony เกิดจาก
 - บุคคลภายใน ผู้ใช้งานระบบโทรศัพท์ภายในองค์กรเอง
 - ผู้ดูแลระบบในองค์กร
 - บุคคลภายนอก (hacker)
 - อุปกรณ์ที่ไม่ได้มาตรฐาน หรือ ไม่เสถียร
 - การที่ไม่มีระบบสำรองต่างๆ



VoIP Performance/Security – How to reduce that risk?

- การลดปัจจัยเสี่ยง ของระบบ IP-Telephony แบ่งเป็น หลายขั้นตอน โดยเป็นการแก้ไขจากต้นเหตุของปัญหา
 - การเลือก Hardware
 - ค่าที่เหมาะสมสำหรับระบบ
 - ผู้ใช้งานระบบ
 - ผู้ดูแลระบบ
 - ระบบ network
 - ระบบ internet
 - Others Consideration



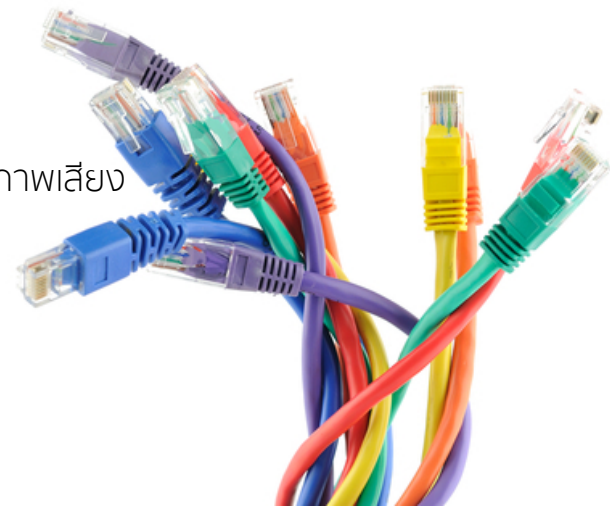
ในการทำระบบ IP telephony ให้ดีนั้นการเลือก hardware ที่เหมาะสม เป็นส่วนประกอบหลักที่จะมีผลต่อคุณภาพโดยรวมของระบบ โดยอาจมีหลักในการเลือกตามกลุ่มเช่น

- ระบบเครือข่าย
- ระบบ security
- หัวเครื่องโทรศัพท์
- ตู้สาขาโทรศัพท์



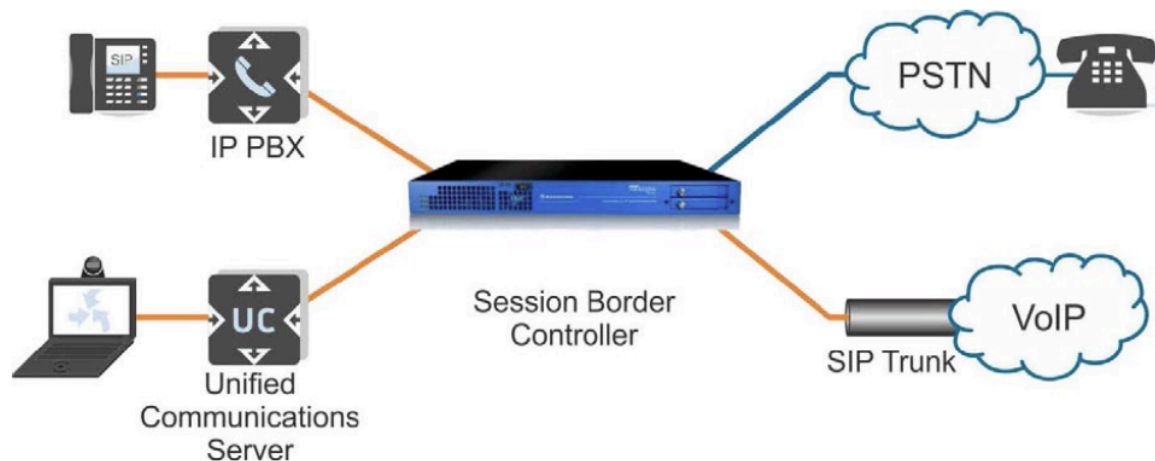
ระบบเครือข่ายภายใน/ภายนอก ที่จะนำมาใช้งานร่วมกับระบบ VoIP ในแง่ Performance

- มีค่า delay/latency ไม่รวมเกิน 250ms, ภายใน one-way ไม่เกิน 150ms
- ไม่มี package loss ในระบบ
- Why PoE?
 - ป้องกัน Power Loss ได้ดีกว่า
- Why Gigabit?
 - Faster Traffic pass-through, ไม่มีผลโดยตรงต่อคุณภาพเสียง
- QoS?
 - ปรับความสำคัญของการส่ง packet
 - without QoS, FIFO

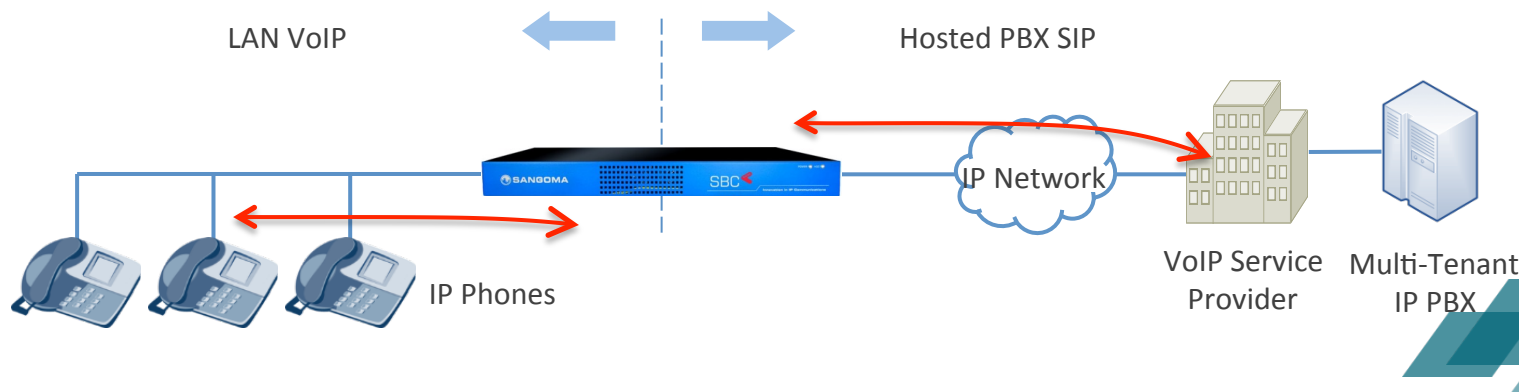


อุปกรณ์ VoIP Security

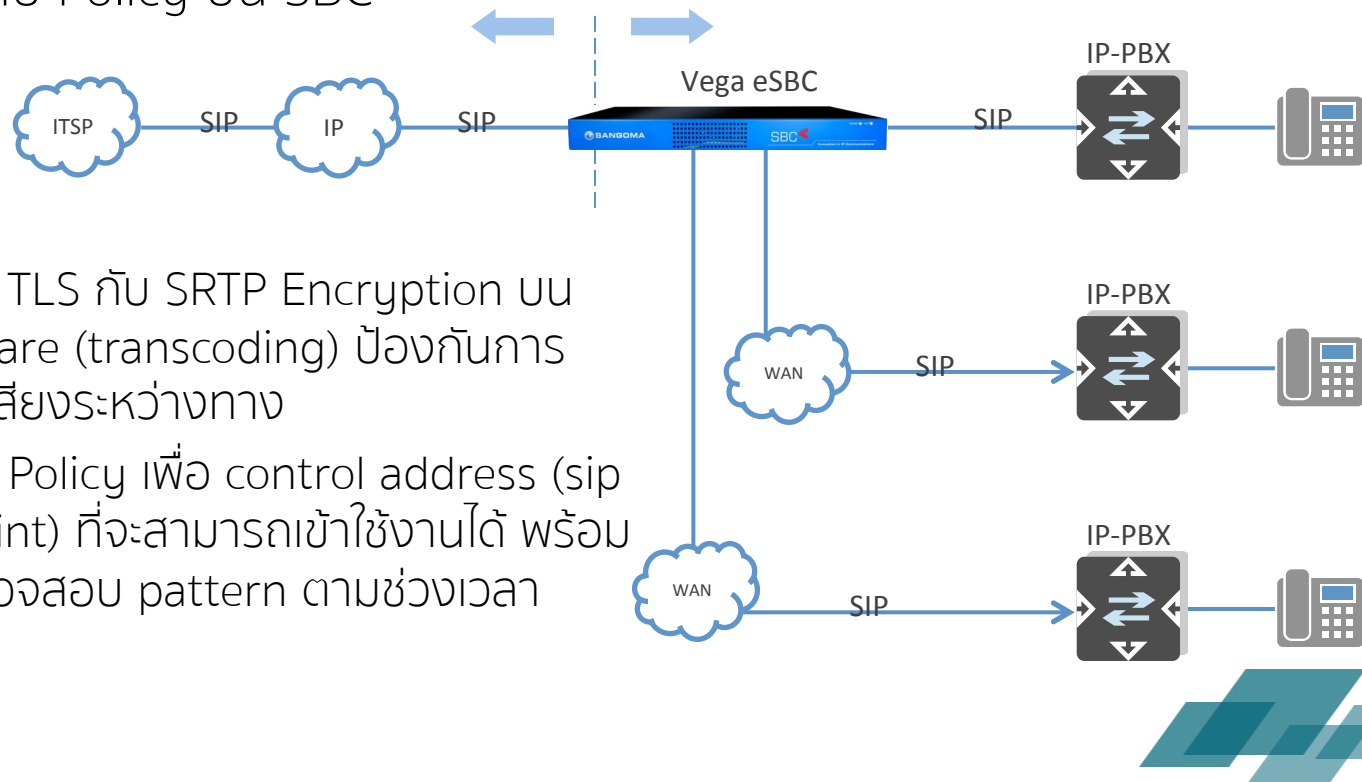
- SBC คืออะไร? ใช้ทำอะไร?
 - Security, Encryption, Policy, Call Routing, SIP Interoperability, Media transcoding, DTMF detection/generation, Scalability



- ฟังก์ชันรักษาความปลอดภัยของอุปกรณ์ SBC (Security Features)
 - Complete Control & Topology hiding (remove via), terminate each call on one side and re-originates the call on another side
 - denial of service (DoS) attack – operate at kernel level (fast)
 - detect malformed packet (used to break SIP stack) and block
 - limit concurrent calls, detect too many wrong password



- Encryption กับ Policy บน SBC



- รองรับ TLS กับ SRTP Encryption บน Hardware (transcoding) ป้องกันการดักฟังเสียงระหว่างทาง
- การตั้ง Policy เพื่อ control address (sip endpoint) ที่จะสามารถเข้าใช้งานได้ พร้อมการตรวจสอบ pattern ตามช่วงเวลา



อุปกรณ์ VoIP Security

- Firewall ช่วย VoIP ด้านความปลอดภัยอย่างไร?
 - Basic DoS
 - Firewall Rules เพื่อควบคุม address ต้นทาง และ ปลายทาง
 - PLEXTEL Country Based Rules?
- ฟังก์ชัน VPN



รูปแบบหัวเครื่องโทรศัพท์, ควรใช้หัวเครื่องที่เหมาะสมกับผู้ใช้งาน

- **ผู้ใช้งานโทรศัพท์ที่มีปริมาณการโทรมาก**
 - หัวเครื่องมีสาย (wired telephone)
 - หากเน้นคุณภาพเสียง (call center) ควรเลือกรุ่นที่เน้นเรื่องคุณภาพเสียง ราคาปานกลางขึ้นไป
 - เลือกรุ่นที่มีความเสถียรภาพ ไม่ต้องทำการ reset
 - สำหรับ operator ควรเป็นรุ่นที่รองรับจำนวนสายได้มาก พร้อมปุ่ม hardkey (Ex, Yealink T27P)
 - รองรับ PoE เพื่อสามารถใช้งานได้ต่อเนื่องในกรณีไฟฟ้าดับ

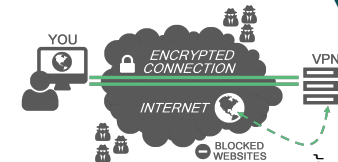


• ผู้ใช้งานโทรศัพท์ที่มีปริมาณการต่อพ่วงใช้งาน data จำนวนมาก

- หัวเครื่องมีสาย (wired telephone) รองรับ Gigabit
- เลือกุ่นที่มีความเสถียรภาพ ไม่ต้องทำการ reset, ควรทำการทดสอบในการส่งผ่าน Data ทดสอบจำนวนมากๆ เพื่อทดสอบความเสถียร
- รองรับ PoE เพื่อสามารถใช้งานได้ต่อเนื่องในกรณีไฟฟ้าดับ



VoIP Security – การเลือก Hardware หัวเครื่องโทรศัพท์



• ผู้ใช้งานโทรศัพท์ที่อยู่บนระบบ internet

- ควรทำระบบ VPN หรือเลือกหัวเครื่องที่รองรับ VPN ได้ในตัว (Ex: Yealink T21P ขึ้นไป)
- เลือกรุ่นที่มีความเสถียรภาพสูงสุด เพื่อลดการดูแลรักษา

• สำหรับองค์กรขนาดใหญ่ที่มี จำนวนหัวเครื่องติดตั้งจำนวนมาก

- เลือกรุ่นที่มีความเสถียรภาพสูงสุด เพื่อลดการดูแลรักษา
- รองรับ PoE



- ผู้ใช้งานทั่วไป เน้น ราคาประหยัด มีสายนอกและการใช้งานคู่สายไม่มากทดแทน PABX เดิม หรือ ใหม่
 - Zycoo IP-PBX
- ผู้ใช้งานระดับกลางเน้นการบันทึกเสียง มีการใช้งานคู่สายค่อนข้างมาก
 - Passwitch IP-PBX
 - Sangoma FreePBX
- ผู้ใช้งานระดับ enterprise,
 - Pexxel IP-PBX
 - Sangoma PBXact
- callcenter หรือ เน้นการ customization
 - Pexxel IP-PBX



VoIP Security – How to reduce that risk?

- การลดปัจจัยเสี่ยง ของระบบ IP-Telephony แบ่งเป็น หลายขั้นตอน โดยเป็นการแก้ไขจากต้นเหตุของปัญหา
 - การเลือก Hardware
 - ค่าที่เหมาะสมสำหรับระบบ
 - ผู้ใช้งานระบบ
 - ผู้ดูแลระบบ
 - SBU network
 - SBU internet
 - Others Consideration



- **ผู้ใช้งานระบบ**

- ควรจัดกลุ่มผู้ใช้งานและทำการจัดเรื่องสิทธิในการโทรศัพท์ให้เหมาะสม
- ควรแยกผู้ใช้งานที่อยู่บน internet ออกมาอีกกลุ่ม และ ไม่ควรอนุญาตให้ใช้งานการโทรออกต่างประเทศได้
- ควรกำหนดความสามารถในการโทรออก ตามช่วงเวลาที่ใช้งานจริง, ลดการโทรออกโดยไม่ได้รับอนุญาต เช่น สามารถโทรออกได้เฉพาะช่วงเวลาทำงาน
- หากมีความจำเป็นสามารถเพิ่ม password สำหรับการโทรออกไปยังเบอร์ที่มีค่าใช้จ่ายสูง



- **ผู้ดูแลระบบ**
 - แยกกลุ่มงานของผู้ดูแลออกตามความเหมาะสม เช่น การฟังไฟล์เสียง, การปรับค่า configอื่นๆ
 - การตั้งค่าโดยผู้ดูแล ควรทำเฉพาะภายในระบบเนทเวอร์คตัวเอง หรือ ผ่าน VPN เท่านั้น



VoIP Security – How to reduce that risk?

- การลดปัจจัยเสี่ยง ของระบบ IP-Telephony แบ่งเป็น หลายขั้นตอน โดยเป็นการแก้ไขจากต้นเหตุของปัญหา
 - การเลือก Hardware
 - **ค่าที่เหมาะสมสำหรับระบบ**
 - ผู้ใช้งานระบบ
 - ผู้ดูแลระบบ
 - ระบบ network
 - ระบบ internet
 - Others Consideration



- **ระบุ Network**

- ควรจัดกลุ่มผู้ใช้งานและทำการจัดเรื่องสิทธิในการโทรศัพท์ให้เหมาะสม
- ควรแยกผู้ใช้งานที่อยู่บน internet ออกมาอีกกลุ่ม และ ไม่ควรอนุญาตให้ใช้งานการโทรออกต่างประเทศได้
- ควรกำหนดความสามารถในการโทรออก ตามช่วงเวลาที่ใช้งานจริง, ลดการโทรออกโดยไม่ได้รับอนุญาต เช่น สามารถโทรออกได้เฉพาะช่วงเวลาทำงาน
- หากมีความจำเป็นสามารถเพิ่ม password สำหรับการโทรออกไปยังเบอร์ที่มีค่าใช้จ่ายสูง
- ตั้งค่า ACL สำหรับ เบอร์ ภายใน (ใช้ได้เฉพาะ network ภายใน)



- **ระบุ Internet / Firewall**

- ตั้งค่า firewall ให้อยอมรับการทำงานจากเฉพาะกลุ่ม IP (thailand IP only)
- การทำ VPN
- ตั้งค่า DoS filter (wrong password)
- ปิด Firewall สำหรับ service อื่นๆ ทั้งหมด , เปิด เฉพาะ กลุ่ม admin เท่านั้น



- **Others Consideration**
 - การกำหนดค่าโทรศัพท์สูงสุด กับ ผู้ให้บริการโทรศัพท์
 - การใช้ SIM มือถือแบบ เหมาะจะจ่าย





THANK YOU.

บริษัท พอยซ์ เทคโนโลยี จำกัด
76 ซอยสุขุมวิท 2 แขวงคลองเตย เขตคลองเตย กรุงเทพฯ 10110
โทรศัพท์ : 02-656-8598 Fax : 02-250-9769

www.poisetechnology.com
Facebook : Poise Technology
ID Line : @poisetechnology