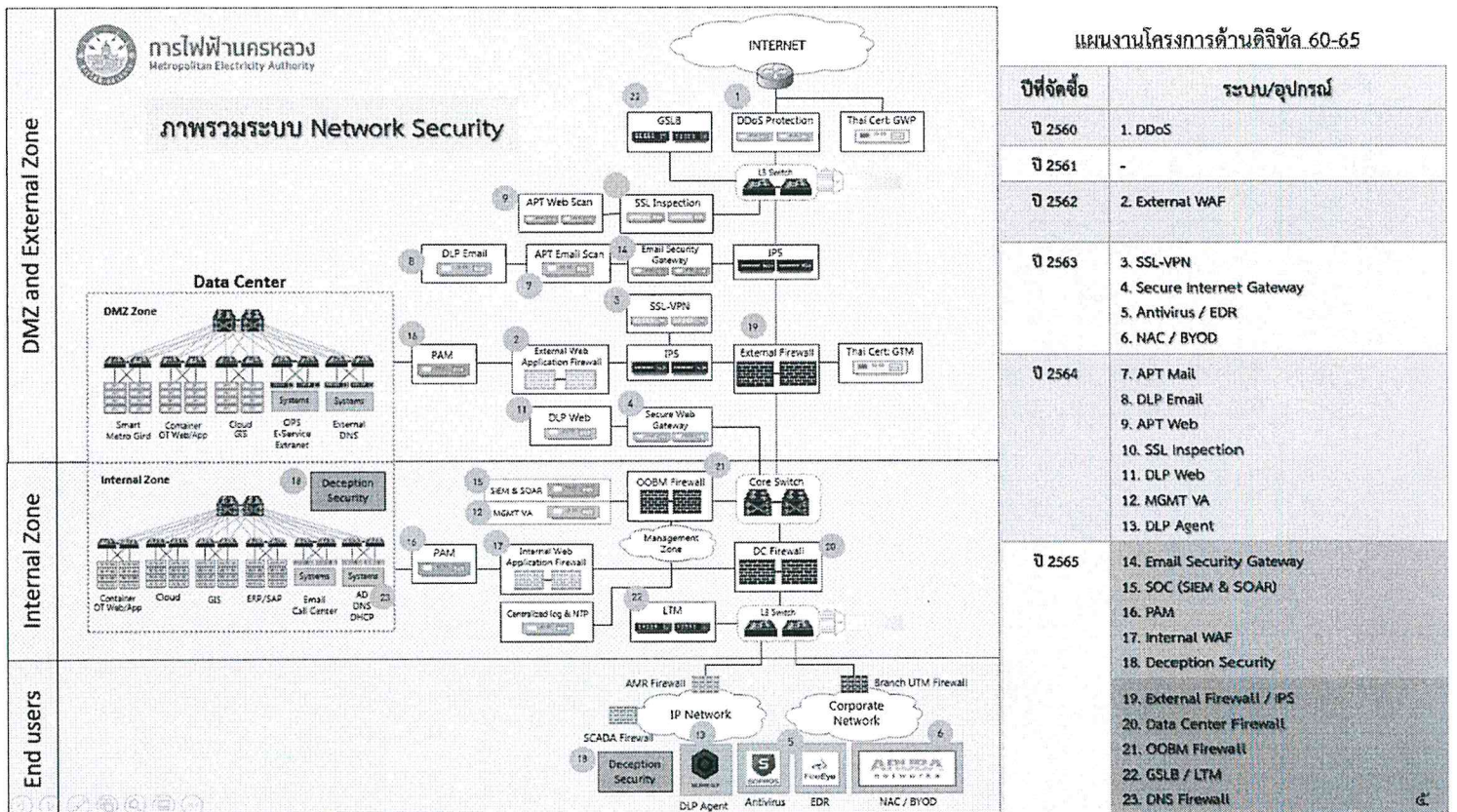


รายละเอียดเพิ่มเติมตามความคิดเห็นและข้อเสนอแนะของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์
ของกระทรวงมหาดไทย ในการประชุมครั้งที่ ๒/๒๕๖๕ วันที่ ๑๘ กุมภาพันธ์ ๒๕๖๕

ชื่อโครงการ จัดซื้อระบบ Security เครือข่ายคอมพิวเตอร์ด้านสำนักงาน
หน่วยงานเจ้าของโครงการ การไฟฟ้านครหลวง
วงเงินโครงการ ๑๓๘,๑๖๔,๑๙๐.๐๐ บาท

ระบบ Security เครือข่ายคอมพิวเตอร์ด้านสำนักงานที่การไฟฟ้านครหลวง (กฟน.) ใช้งานอยู่ในปัจจุบัน
ติดตั้งใช้งานมาเป็นระยะเวลาอันยาวนาน อุปกรณ์บางส่วนในระบบ End of life ไม่สามารถ Upgrade Firmware เพื่อ
ปิดช่องโหว่ และไม่สามารถ Update Security feature ได้ ทำให้ระบบเครือข่ายมีความเสี่ยงต่อภัยคุกคาม ซึ่งจะ
ส่งผลกระทบต่อระบบงานสำคัญที่ใช้ในการขับเคลื่อนธุรกิจของ กฟน. อีกทั้งยังมีสถาปัตยกรรมเครือข่าย
คอมพิวเตอร์ที่ไม่รองรับเทคโนโลยีใหม่ อาทิเช่น Cloud computing หรือ Virtualization, IoT Platform ที่ม
ีความซับซ้อนและมี Traffic จำนวนมาก ซึ่งต้องการระบบที่มีเสถียรภาพและความปลอดภัยที่ดีขึ้น

๑. ภาพรวมของระบบ Network Security ของการไฟฟ้านครหลวง (กฟน.) และแผนระยะยาว ๕ - ๑๐ ปี



กฟน.

๒. ในปัจจุบันมีอุปกรณ์ IoT มากขึ้น มีปริมาณข้อมูลมากขึ้น ระบบ Security เครือข่ายคอมพิวเตอร์มีการป้องกัน และตรวจสอบอุปกรณ์ IoT อย่างไร

๑. การ update ความปลอดภัยทางด้านเครือข่าย เช่น update Firewall, IPS รวมถึงไปถึง Anti-malware
๒. การตรวจสอบวิเคราะห์ช่องโหว่ในระบบ Network เพื่อป้องกันในเบื้องต้น
๓. การ update patch เพื่อปกช่องโหว่ในระบบ Network
๔. การพิสูจน์ตัวตน เช่น PAM, การใช้ ๒-Factor Authentication หรือ Multi-Factor Authentication, การใช้ Digital Certificate
๕. การทำ Security Analytics บน IoT
๖. ความปลอดภัยของ API สำหรับ IoT

ทั้งนี้ กพน. ได้ทำตามกระบวนการงาน iso๒๗๐๐๑ อีกทั้งยังมีแผนระยะยาว ๕ ปี (ปี ๒๕๖๖-๒๕๗๐) ในโครงการจ้างที่ปรึกษามิให้เขาช่วยวิเคราะห์ gap ด้าน IoT ให้หน่วยงานด้วย