เลขที่ 19-55

คุณลักษณะเฉพาะ รพ.ตร. อนุมัติ ลงวันที่ 1 พ.ค.2555

ระบบรักษาความปลอดภัยระบบคอมพิวเตอร์ (Firewall)
และอุปกรณ์จัดเก็บ Log File ในระบบเครือข่ายโรงพยาบาลตำรวจ

---

๑. **วัตถุประสงค์การใช้งาน**

เพื่อติดตั้งระบบรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ (Firewall) และระบบจัดเก็บ Log File ในระบบเครือข่ายให้สามารถป้องกันการบุกรุก จากระบบเครือข่ายอินเตอร์เน็ตได้อย่างมีประสิทธิภาพ สามารถ ตรวจสอบข้อมูลย้อนหลัง และสามารถทำงานร่วมกับระบบปัจจุบันของทาง โรงพยาบาลตำรวจ ได้อย่างมีประสิทธิภาพ

๒. **ลักษณะทั่วไป**

๒.๑ อุปกรณ์บริหารและจัดเก็บ Log File ระบบเครือข่าย

๒.๒ อุปกรณ์รักษาความปลอดภัยระบบคอมพิวเตอร์(Firewall)

๓. **คุณลักษณะเฉพาะทางวิชาการ**

๗ก.๓.๓

๓.๑. อุปกรณ์บริหารและจัดเก็บ Log File ระบบเครือข่าย

๓.๑.๑ เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่างๆ ระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย ๑๕ อุปกรณ์ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้

๓.๑.๒ มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลตามมาตรฐาน MD5 หรือ SHA-1 หรือการเข้ารหัสข้อมูลวิธีอื่น ที่มีหลักฐานว่าเป็นการป้องกันการถอดรหัสข้อมูลได้ดีกว่า

๓.๑.๓ สามารถเก็บ log File ในรูปแบบ Syslog ของอุปกรณ์ Firewall, router, switch, VPN, Server เป็นต้นได้

๓.๑.๔ สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTP, HTTPS, Command line Interface และ Secure shell (SSH) ได้

๓.๑.๕ สามารถจัดเก็บ Log File ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐานสากล เช่น มาตรฐานสากล Payment Card Industry Data Security Standard (PCI DSS) หรือมาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. ๔๐๐๓.๑/๒๕๕๒) เป็นต้น

๓.๑.๖ สามารถทำการสำรองข้อมูล (Data Back up) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้น ได้

๓.๑.๗ สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events per Seconds) ได้ไม่น้อยกว่า 40,000 eps หรือจัดเก็บข้อมูล log per seconds ได้ไม่น้อยกว่า 1,000 log/sec หรือ 6500 Flow/sec

๓.๑.๘ มี Hard disk อย่างน้อย ๒ ลูก และมีความจุของ hard disk ไม่น้อยกว่าลูกละ 500 GB และสามารถทำ RAID 10 ได้

พ.ต.อ.....ประธานกรรมการ พ.ต.ท.....กรรมการ

พ.ต.ท.....กรรมการ

รพ.ตร. อนุมัติ ลงวันที่ 1 พ.ค.2555

๓.๑.๙ สามารถเก็บ Log ได้หลายรูปแบบ ได้แก่ Traffic Log, Event Log, Virus Log และ Attack Log ได้เป็นอย่างน้อย

๓.๑.๑๐ สามารถทำการตรวจสอบข้อมูลการใช้งานย้อนหลังของผู้ใช้งานแต่ละรายโดยกำหนดเงื่อนไขจาก User name, E-mail, IP Address พร้อมทั้งออก Report ได้

๓.๑.๑๑ สามารถระบุบุคคลที่ใช้เครือข่ายได้ไม่น้อยกว่า ๙๐ วัน

๓.๒. อุปกรณ์รักษาความปลอดภัยระบบคอมพิวเตอร์(Firewall)

๓.๒.๑ เป็นอุปกรณ์ Firewall ชนิด Stateful Inspection Firewall แบบ Appliance

๓.๒.๒ มี Throughput ของ Firewall Inspection จำนวนไม่น้อยกว่า 30 Gbps

๓.๒.๓ สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อยดังนี้

๓.๒.๓.๑ Syn Flood

๓.๒.๓.๒ UDP Flood

๓.๒.๓.๓ ICMP Flood

๓.๒.๓.๔ IP Address Spoof และ IP Spoof

๓.๒.๓.๕ IP Address Sweep และPing Sweeps และ ICMP Sweep

๓.๒.๓.๖ Port Scan

๓.๒.๓.๗ DoS and DDoS

๓.๒.๓.๘ Teardrop Attack

๓.๒.๓.๙ Land Attack

๓.๒.๓.๑๐ TCP Fragment และ TCP disassembly

๓.๒.๓.๑๑ ICMP Fragment

๓.๒.๔ สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

๓.๒.๕ สามารถทำงานลักษณะ Transparent Mode ได้

๓.๒.๖ สามารถ Routing แบบ Static, Source based Routing, Policy Routing และ Dynamic Routing ได้

๓.๒.๗ สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTP, HTTPS ได้เป็นอย่างน้อย

๓.๒.๘ สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) โดยส่งเป็น Syslog ได้

๓.๒.๙ มี Power Supply แบบ Redundant และ Hot Swap ได้

๓.๒.๑๐ รองรับมาตรฐาน IPv6

๓.๒.๑๑ มีประสิทธิภาพในการทำงาน IPSec VPN ได้ไม่น้อยกว่า 10 Gbps

๓.๒.๑๒ มีประสิทธิภาพในการทำงาน Intrusion Protection System (IPS) ได้ไม่น้อยกว่า 1 Gbps

๓.๒.๑๓ รองรับการเชื่อมต่อพร้อมๆ กันได้ไม่น้อยกว่า 2,000,000 sessions (Concurrent Session)

๓.๒.๑๔ มี Interface ชนิด Gigabit Ethernet ๑๐/๑๐๐/๑๐๐๐ Base จำนวนอย่างน้อย 16 interface

๓.๒.๑๕ มีความสามารถในการ Block Application ต่างๆได้ โดยเฉพาะ Social Network เช่น Youtube, Bittorent, facebook, MSN และ skype เป็นต้น

พ.ต.อ.....ประธานกรรมการ พ.ต.ท.....กรรมการ

พ.ต.ท.....กรรมการ

เลขที่ 19-55

๔.<u>ส่วนประกอบและอุปกรณ์อะไหล่</u> รพ.ตร. อนุมัติ สั่งซื้อ 1 พ.ค.2555

๔.๑ Rack ๔๒U ขนาด ๖๐ x ๙๐ เซนติเมตร สีดำ สำหรับติดตั้งอุปกรณ์ขนาด ๑๙ นิ้ว จำนวน ๑ ตู้ พร้อมกับโครงการนี้ด้วย

๔.๒ คู่มือการใช้งาน สำหรับอุปกรณ์รักษาความปลอดภัยระบบคอมพิวเตอร์ และอุปกรณ์บริหารและจัดเก็บ Log File ระบบเครือข่าย เป็นภาษาไทยและภาษาอังกฤษ จำนวน 1 ชุด

๕. <u>การทดสอบและผล</u>

๕.๑ ตรวจพินิจตามข้อ ๒, ๓ และ ๔

๕.๒ ทำการทดสอบจนสามารถใช้การได้

๖. ข้อกำหนดอื่น ๆ

๖.๑ ต้องดำเนินการติดตั้งระบบรักษาความปลอดภัยระบบคอมพิวเตอร์ (Firewall) และอุปกรณ์จัดเก็บ Log File ในระบบเครือข่าย ให้สามารถเชื่อมโยงกับระบบเครือข่ายของ รพ.ตร ให้สามารถใช้งานได้ตามวัตถุประสงค์ของ รพ.ตร.

๖.๒ ต้องรับประกันคุณภาพการใช้งานและอะไหล่เป็นเวลาอย่างน้อย ๑ ปี โดยไม่มีค่าใช้จ่ายใดๆ ทั้งสิ้น

๖.๓ ต้องจัดการอบรมการใช้งานระบบรักษาความปลอดภัยระบบคอมพิวเตอร์ (Firewall) และอุปกรณ์จัดเก็บ Log File ระบบเครือข่าย ที่มากับโครงการนี้ จำนวน ๑๐ คน เป็นเวลาไม่ต่ำกว่า ๑๒ ชั่วโมง

พ.ต.อ. ประธานกรรมการ
(อดิศักดิ์ เมฆาอภิรักษ์)
ผกก.วบ.บก.อก.รพ.ตร.

ประธานกรรมการพิจารณาคุณลักษณะเฉพาะโรงพยาบาลตำรวจ
ให้มีมติเห็นชอบตามคุณลักษณะเฉพาะ ที่เสนอในครั้งนี้ประชุม กรรมการ
ครั้งที่ 5/2555 (สุรชัย แก้วพิกุล)
พล.ต.ต. รอง ผกก.วบ.บก.อก.รพ.ตร.
(ชำนาญ สุดเนรัญ)
ผบก.อก.รพ.ตร./กรรมการและเลขานุการฯ

พ.ต.ท. กรรมการ
(จำเริญ ลุสวัสดิ์)
เภสัชกร (สบ ๓) กลุ่มงานเภสัชกรรม รพ.ตร.

เห็นชอบ
พล.ต.ต.
(สุรพงษ์ พงษ์อร่าม)
ผบก.อก.รพ.ตร.