คุณลักษณะเฉพาะ
อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ ๒
โรงพยาบาลมหาราชนครราชสีมา

ความต้องการ อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ ๒ จำนวน ๑ ชุด เพื่อใช้สนับสนุนด้านความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์

คุณสมบัติทางเทคนิค อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ ๒ มีคุณสมบัติอย่างน้อยดังต่อไปนี้

๑. เป็นอุปกรณ์เฉพาะ Hardware appliance ที่ออกแบบมาเพื่อทำหน้าที่ Next Generation Firewall โดยเฉพาะ
๒. มี Throughput สูงสุดไม่น้อยกว่า ๑๗ Gbps เมื่อเปิดการใช้งานแบบ Next Generation IPS ร่วมกับ Application control พร้อมกัน
๓. รองรับการเชื่อมต่อ Maximum current connections สูงสุดไม่น้อยกว่า ๒,๐๐๐,๐๐๐ sessions
๔. รองรับการเชื่อมต่อ New connections per second สูงสุดไม่น้อยกว่า ๑๓๐,๐๐๐ connections per second
๕. มี Network Interface แบบ ๑๐/๑๐๐/๑๐๐๐ จำนวน ๘ พอร์ต และ แบบ ๑/๑๐ Gigabit (SFP) Ethernet interfaces จำนวน ๘ พอร์ต และ รองรับการเพิ่ม Network Module (Expansion Slot) เพื่อสามารถรองรับการขยายได้ในอนาคต อย่างน้อย ๑ Slot
๖. มี Management Interface แบบ ๑๐/๑๐๐/๑๐๐๐ Base TX อย่างน้อย ๑ พอร์ต
๗. มี Hard disk แบบ Solid State ขนาดไม่น้อยกว่า ๙๐๐ GB และรองรับการเพิ่มขยายได้ไม่น้อยกว่า ๑ ช่อง (๑x spare slot)
๘. อุปกรณ์สามารถตรวจจับและป้องกันการโจมตี ในรูปแบบดังต่อไปนี้ ได้แก่ Worm, Backdoor, Spyware, Port Scans, VoIP Attacks, IPv๖ Attacks, Dos Attacks, Buffer Overflows, P๒P Attacks, Statistical Anomalies, Protocol Anomalies, Application Anomalies, Blended Threats และ Zero-day Threats
๙. สามารถวิเคราะห์ Unknown malware หรือ Advance Malware ได้โดยใช้เทคนิคการวิเคราะห์แบบ Analysis เช่นการวิเคราะห์การทำงานของไฟล์บนระบบที่มีการควบคุม (Cloud Sandboxing) หรือเสนออุปกรณ์เสริมภายนอกแบบ Appliance ได้
๑๐. สามารถควบคุมการใช้งาน Application ได้ไม่น้อยกว่า ๔,๐๐๐ application โดยครอบคลุมถึงกลุ่ม Application ต่างๆ เช่น Social Networking, Gaming, Instant Messaging และ P๒P เป็นอย่างน้อย
๑๑. สามารถกำหนดการใช้งาน URL Filtering โดยมีจำนวนของ URL Categories ไม่ต่ำกว่า ๘๐ Categories
๑๒. อุปกรณ์ที่เสนอต้องมี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๑๓. รองรับการทำงาน High Availability แบบ Active-Standby หรือ Active-Active หรือแบบ Stackable ได้เป็นอย่างน้อย

๑๔. รองรับ Open API เพื่อให้สามารถบริหารจัดการจาก ๓rd Party software หรือ ระบบบริหารจัดการภายนอกได้

๑๕. "อุปกรณ์ที่นำเสนอต้องมาพร้อมกับ Software หรือ Hardware สำหรับการทำงานแบบ Centralize management และสามารถบริหารจัดการ Next Generation Firewall ได้ เพื่อสะดวกต่อการจัดการบริหาร Next Generation Firewall โดยมีความสามารถดังต่อไปนี้

๑๕.๑ สามารถบริหารจัดการอุปกรณ์ได้ผ่าน Command-line หรือ GUI โดยผ่านเว็บแบบ HTTPS

๑๕.๒ สามารถแสดงสถานการณ์ทำงานของอุปกรณ์ (Dashboard) โดยสามารถแสดงถึงสถานการณ์ถูกโจมตีของระบบเครือข่าย

๑๕.๓ สามารถปรับแต่งการแสดงผล(Customize) ของ Dashboard ได้

๑๕.๔ สามารถตรวจสอบรายชื่อ Users ได้ เมื่อมีการทำงานร่วมกัน LDAP หรือ Active Directory

๑๕.๕ สามารถตรวจสอบ Client Applications และ Network servers ได้

๑๕.๖ สามารถตรวจสอบ Operating systems ได้

๑๕.๗ สามารถตรวจสอบ Malware file trajectory ได้ เพื่อช่วยในการตรวจสอบและจำกัดขอบเขตของปัญหาได้

<u>เงื่อนไขเฉพาะ</u>

๑. เป็นอุปกรณ์ที่ได้รับการรับรองความปลอดภัยในการใช้งานจาก EN , UL และ CSA เป็นอย่างน้อย

๒. มีขนาดมาตรฐานไม่เกิน ๑ U และ สามารถติดตั้งในตู้ RACK ขนาด ๑๙ นิ้วได้

๓. อุปกรณ์ที่นำเสนอต้องมาพร้อมกับ License สำหรับการสนับสนุนด้านข้อมูลจาก Threat intelligence และ Malware จากบริษัทเจ้าของผลิตภัณฑ์อย่างน้อย ๑ ปี

๔. อุปกรณ์ที่นำเสนอต้องมาพร้อมกับประกันอุปกรณ์อย่างน้อย ๑ ปี

๕. อุปกรณ์ที่นำเสนอจะต้องเป็นสินค้าใหม่ และได้รับการสนับสนุนหลังการขายจากเจ้าของผลิตภัณฑ์ โดยมีเอกสารรับรองจากเจ้าของผลิตภัณฑ์ หรือสาขาของเจ้าของผลิตภัณฑ์ภายในประเทศไทย อ้างถึงเลขที่ประกาศของโรงพยาบาล

(ลงชื่อ).....ประธานกรรมการ
(นางนงลักษณ์ ประยูรเสริฐ)

(ลงชื่อ).....กรรมการ
(นายสุพจน์ เพ็งที)

(ลงชื่อ).....กรรมการ
(นายยุติ แผลงรักษา)