รายละเอียดคุณลักษณะเฉพาะของครุภัณฑ์คอมพิวเตอร์
ในการจัดซื้ออุปกรณ์เพิ่มประสิทธิภาพโครงสร้างพื้นฐานด้านอินเทอร์เน็ต
และระบบเครือข่าย จำนวน 1 ชุด

ความเป็นมา

มหาวิทยาลัยอุบลราชธานี เป็นมหาวิทยาลัยของรัฐ จัดตั้งเมื่อวันที่ 29 กรกฎาคม 2533 อยู่ในพื้นที่ภาคตะวันออกเฉียงเหนือตอนล่าง เป็นมหาวิทยาลัยกลุ่ม 2 ที่เน้นการพัฒนาเทคโนโลยีและส่งเสริมการสร้างนวัตกรรม มีพันธกิจหลัก คือ การผลิตบัณฑิต การวิจัย การบริการวิชาการ และการทำนุบำรุงศิลปวัฒนธรรม ปัจจุบันมีจำนวนนักศึกษามากกว่า 15,000 คน และบุคลากรมากกว่า 1,500 คน

มหาวิทยาลัยอุบลราชธานี มีแผนปรับปรุงโครงสร้างพื้นฐานด้านอินเทอร์เน็ตและระบบเครือข่ายในภาพรวมของมหาวิทยาลัย ซึ่งการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเครือข่ายถือว่ามีความสำคัญเป็นอย่างมากต่อระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย ในการป้องกันการบุกรุกจากกลุ่มผู้ไม่ประสงค์ดีจากภายนอกมหาวิทยาลัยหรือภัยคุกคามต่าง ๆ ทางอินเทอร์เน็ต ตลอดจนการจัดหาอุปกรณ์เครือข่ายเพื่อการเพิ่มประสิทธิภาพในด้านความเร็ว ความครอบคลุม ตลอดจนการยืนยันตัวตนอย่างมีเสถียรภาพในการใช้งานเครือข่ายอินเทอร์เน็ต

ดังนั้น เพื่อให้โครงสร้างพื้นฐานด้านอินเทอร์เน็ตและระบบเครือข่ายของมหาวิทยาลัย มีความพร้อมรองรับการใช้งานของมหาวิทยาลัยในปัจจุบันและอนาคต จึงต้องดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลการจราจรทางเครือข่ายอินเทอร์เน็ต อุปกรณ์รักษาความความปลอดภัยและเพิ่มประสิทธิภาพการใช้งานเครือข่ายอินเทอร์เน็ตเพื่อรองรับการใช้งานของนักศึกษาและบุคลากร ตลอดจนการเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีความมั่นคงปลอดภัยและมีประสิทธิภาพ

วัตถุประสงค์

1. เพื่อจัดหาอุปกรณ์จัดเก็บข้อมูลการจราจรทางเครือข่ายอินเทอร์เน็ต
2. เพื่อจัดหาอุปกรณ์รักษาความปลอดภัยของระบบโครงสร้างพื้นฐานด้านอินเทอร์เน็ตและระบบเครือข่ายที่มีประสิทธิภาพ
3. เพื่อเพิ่มประสิทธิภาพระบบเครือข่ายหลักและการให้บริการด้านเครือข่ายอินเทอร์เน็ตของมหาวิทยาลัย

คุณสมบัติของผู้ยื่นข้อเสนอ

1. มีความสามารถตามกฎหมาย
2. ไม่เป็นบุคคลล้มละลาย
3. ไม่อยู่ระหว่างเลิกกิจการ
4. เป็นผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว
5. ไม่เป็นบุคคลอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ไม่ผ่านเกณฑ์ประเมินการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

(ผู้ช่วยศาสตราจารย์อชิพงศ์ สุริยา) (ผู้ช่วยศาสตราจารย์อารยา ฟลอเรนซ์) (นายจิรานุวัฒน์ จันทรุกขา) (นางสาวกรรณิการ์พร กุลบุญญา) (นายวิมล แสวงวงศ์) (นายสุรศักดิ์ ศรีวิเศษ) (นายณัฐพล มารุตะพันธ์)

6. ไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสานสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินการในกิจการของนิติบุคคลนั้นด้วย

7. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

8. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุดังกล่าว

9. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ มหาวิทยาลัยฯ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม

10. ต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) ของกรมบัญชีกลาง

รายละเอียดคุณลักษณะเฉพาะของอุปกรณ์เพิ่มประสิทธิภาพโครงสร้างพื้นฐานด้านอินเทอร์เน็ตและระบบเครือข่าย จำนวน 1 ชุด ประกอบด้วย

1. ระบบบริหารจัดเก็บข้อมูลจราจรเครือข่ายแบบรวมศูนย์ (Centralized Log Management) จำนวน 1 ระบบ โดยมีคุณสมบัติอย่างน้อย ดังต่อไปนี้

1.1 เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่าง ๆระบบปฏิบัติการ, ระบบ application, ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้ไม่จำกัดจำนวนอุปกรณ์ต่อระบบ

1.2 มีหน่วยประมวลผลกลางแบบ Octa Cores เป็นอย่างน้อย

1.3 มีขนาดของหน่วยความจำหลักสำหรับทำงานขนาดไม่น้อยกว่า 32 GB

1.4 มีช่องสัญญาณสำหรับเชื่อมต่อเครือข่ายแบบ 10/100/1000 BaseTX หรือดีกว่า จำนวนไม่น้อยกว่า 2 Ports

1.5 มีส่วนควบคุม RAID ที่รองรับการทำ RAID 0, 1 และ 5 หรือดีกว่า พร้อมฮาร์ดดิสก์ขนาดไม่น้อยกว่า 8 TB จำนวนไม่น้อยกว่า 2 หน่วย และมีฮาร์ดดิสก์ชนิด SSD ขนาดไม่น้อยกว่า 480 GB จำนวนไม่น้อยกว่า 2 หน่วยเพื่อเพิ่มประสิทธิภาพในการเขียนและอ่านข้อมูลมากยิ่งขึ้น

1.6 มีแหล่งจ่ายไฟ (AC Power Supply) แบบ Redundant Power Supply

1.7 ระบบต้องสามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events per Seconds) ได้ไม่น้อยกว่า 30,000 EPS

1.8 มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน SHA-256

1.9 ระบบต้องสามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server เป็นต้น ได้

1.10 ระบบต้องสามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้

1.11 ระบบต้องสามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่มีผลบังคับใช้ โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ตามมาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2560)

1.12 ระบบต้องสามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage ได้

1.13 ระบบต้องสามารถเข้ารหัสของข้อมูล log แบบ AES-256, AES-128 และ DES ได้เป็นอย่างน้อย ในกรณีที่มีการดาวน์โหลดไฟล์ออกจากระบบเพื่อป้องกันการแก้ไขข้อมูล log ได้

1.14 ระบบต้องสามารถแจ้งเตือน (Alert) ไปยังผู้ดูและระบบเมื่อมีเหตุการณ์ตรงตามเงื่อนไข ที่สร้างไว้หรือเหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่าน E-mail และ Line Notify ได้

1.15 ระบบต้องสามารถบีบอัดข้อมูลบนพื้นที่จัดเก็บได้อย่างน้อย 15:1

1.16 ระบบต้องสามารถจัดเก็บฐานข้อมูลในรูปแบบ NOSQL เพื่อความรวดเร็วในการจัดเก็บและค้นหาได้

1.17 ระบบต้องมีเทคโนโลยีการ Index ข้อมูล Log File เพื่อประสิทธิภาพในการค้นหาโดยรองรับทั้งแบบ Full-text Search และแบบกำหนด Field ในการค้นหา โดยสามารถระบุเงื่อนไขในการค้นหาได้ เช่น AND, OR, Wildcard expression, Regular expression และกำหนดช่วงเวลาหรือขอบเขตในการค้นหาได้

1.18 ระบบต้องรองรับการทำ custom log parser หรือ custom log template ได้บนระบบโดยไม่จำเป็นต้องใช้ software อื่นมาช่วย (third party software)

1.19 ระบบต้องสามารถทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในลักษณะของ Centralized และ Forwarder mode ได้

1.20 ระบบต้องสามารถสร้างรายงานแบบรายครั้ง (ad-hoc report), รายวัน, รายสัปดาห์และรายเดือนได้

1.21 ระบบต้องมีส่วนของการรายงานผลกราฟและตารางข้อมูลที่สามารถทำงานบน appliance เดียวกัน (on-box reporting) โดยมีข้อมูลดังต่อไปนี้เป็นอย่างน้อย Top 10 Source IP, Top 10 User, Top 10 URL, Top 10 Application, Top 10 Threat

1.22 ระบบต้องสามารถจัดทำรายงาน Graphic ในรูปแบบของ Bar Chart, Line Chart, Pie Chart, Radar Chart, Donut Chart และ Polar Area Chart ได้

1.23 ระบบต้องสามารถส่งออกรูปแบบรายงานในรูปแบบไฟล์ PDF, XML, XLSX, CSV, HTML, XHTML, DOCX, และ OpenOffice ได้

1.24 ระบบต้องสามารถตรวจสอบสถานะของอุปกรณ์ที่ส่ง Log เข้ามาว่ายังทำงานอยู่ได้ และสามารถบอกวันสุดท้ายของ Log ที่ส่งเข้ามายังระบบได้

1.25 ระบบต้องสามารถแสดงค่าเฉลี่ยของการรับ Log (Average EPS) และแสดงจำนวน Log ที่รับสูงสุด (Peak EPS) ในแบบรายวัน รายสัปดาห์ และรายเดือนได้

1.26 ระบบต้องสามารถแยกการเก็บ Log ตามแต่ละหน่วยงาน (Domain) และแยกสิทธิ์การเข้าถึงได้

1.27 ระบบต้องสามารถกำหนดสิทธิ์การใช้งานระบบของผู้ดูแลระบบแต่ละคนแตกต่างกันได้

1.28 ระบบต้องสามารถค้นหาข้อมูล Log จากอุปกรณ์ที่ส่ง Log ผ่านทาง IPv4 และ IPv6 ได้

1.29 ระบบต้องสามารถทำงานเป็น NTP Server ให้กับอุปกรณ์ภายในเครือข่ายได้

2. อุปกรณ์กระจายสัญญาณ (Switch) แบบที่ 1 จำนวน 4 ชุด โดยแต่ละชุดมีคุณสมบัติต่อชุดอย่างน้อย ดังต่อไปนี้

2.1 มีความสามารถในการทำงาน Layer 3 switch ได้

2.2 อุปกรณ์ต้องรองรับ Switching Capacity ไม่น้อยกว่า 880 Gbps และ Forwarding Performance ได้ไม่น้อยกว่า 480 Mpps

2.3 อุปกรณ์ต้องมี Redundant Power Supply หรือ 1+1 power backup

2.4 สามารถทำงานกับระบบไฟฟ้าแบบ AC ในประเทศไทยได้

2.5 มี Interface ที่รองรับการทำงานแบบ 1G/10G Base-T จำนวนไม่น้อยกว่า 24 ช่อง และต้องสามารถรองรับการจ่ายไฟแบบ POE ได้ รวมไม่น้อยกว่า 600 วัตต์ หรือดีกว่า

2.6 มี Interface ชนิด 10 GE แบบ SFP+ จำนวนไม่น้อยกว่า 4 ช่อง พร้อมเสนอ SFP+ module ไม่น้อยกว่า 4 ตัวต่อ 1 ชุด หรือดีกว่า

2.7 สามารถทำงานตามมาตรฐาน OpenFlow หรือ NETCONF (Network Configuration Protocol) ได้

2.8 สามารถทำงาน VLAN, GVRP, Voice VLAN และ Guest VLAN และสามารถรองรับ VLAN ได้ไม่น้อยกว่า 4K VLAN

2.9 รองรับจำนวน MAC Address ได้ไม่น้อยกว่า 32K MAC Address

2.10 สามารถทำงานตามมาตรฐาน IPv4 Routing Protocol ได้แก่ Static Routing, RIPv2, OSPF, BGP ได้เป็นอย่างน้อย

2.11 สามารถทำงานตามมาตรฐาน IPv6 Routing Protocol ได้แก่ OSPFv3, BGP4 หรือ BGP4+ และ IS-IS หรือดีกว่า

2.12 สามารถทำงานตามมาตรฐาน IP Multicast Routing Protocol ได้แก่ PIM-SM และ Internet Group Management Protocol (IGMP) ได้เป็นอย่างน้อย

2.13 สามารถทำงานตามมาตรฐาน IEEE802.1Q, IEEE 802.1D, IEEE 802.1w, และ IEEE 802.1s ได้

2.14 สามารถทำ Authentication แบบ AAA, RADIUS และ HWTACACS หรือ TACACS+ ได้

2.15 สามารถกำหนดคุณภาพการให้บริการ (QoS) ได้

2.16 ทำการป้องกันการโจมตี หรือการบุกรุกด้วย Denial of Service (DoS) Attack defense, ARP attack defense และ BPDU Protection ได้

2.17 อุปกรณ์รองรับการทำ VXLAN เพื่อสามารถสร้าง VXLAN L2 และ L3 gateway ได้ โดยสามารถเพิ่มเติมได้ในอนาคต

2.18 ทำการดูแลจัดการด้วยโปรโตคอล SNMP, Telnet, Secure Shell (SSH) และ Command Line Interface (CLI) ได้

(ผู้ช่วยศาสตราจารย์อธิพงศ์ สุริยา) (ผู้ช่วยศาสตราจารย์อารยา ฟลอเรนซ์) (นายจิรานุวัฒน์ จันทรุกขา) (นางสาวกรรณิการ์พร กุลบุญญา) (นายวิมล แสวงวงศ์) (นายสุรศักดิ์ ศรีวิเศษ) (นายณัฐพล มารุตะพันธ์)

2.19 อุปกรณ์ที่เสนอต้องสามารถติดตั้งบนตู้ Rack ขนาด 19 นิ้ว ได้

2.20 ผู้ผลิตต้องอยู่ใน Quadrant: Leader ปี ล่าสุด ของ Gartner Magic Quadrant ในหัวข้อเรื่อง "Wired and Wireless LAN Access Infrastructure"

2.21 ผ่านการรับรองตามมาตรฐาน EN และ UL เป็นอย่างน้อย

2.22 สามารถทำงานร่วมกับระบบ Software Define Network (SDN) เดิมของหน่วยงานได้ หรือเสนอ ระบบ Software Define Network (SDN) ที่สามารถทำงานร่วมกับอุปกรณ์ที่เสนอได้ และต้องเสนอ License ให้อุปกรณ์รองรับการทำงานร่วมกับ SDN ได้อย่างครบถ้วน จำนวน 5 License ต่อ 1 ชุด

3. อุปกรณ์กระจายสัญญาณ (Switch) แบบที่ 2 จำนวน 20 ชุด โดยแต่ละชุดมีคุณสมบัติต่อชุดอย่างน้อย ดังต่อไปนี้

3.1 เป็น Layer 3 Switch ที่มีขนาด Switching Capacity หรือ Switching Bandwidth รวมไม่น้อยกว่า 56 Gbps และมีประสิทธิภาพในการส่งผ่านข้อมูล Capacity in Millions of Packets per Second (mpps) (64-Byte Packet) ไม่น้อยกว่า 41.6 mpps

3.2 มีช่องต่อสัญญาณ(พอร์ต) แบบ 10/100/1000 BASE-T จำนวนไม่น้อยกว่า 24 พอร์ต และสามารถจ่ายไฟได้ตามมาตรฐาน PoE 802.3af และ PoE+ 802.3at รวมไม่น้อยกว่า 195 วัตต์

3.3 มีช่องต่อสัญญาณ(พอร์ต) แบบ 1G SFP จำนวนไม่น้อยกว่า 4 พอร์ต

3.4 มีหน่วยความจำชนิด Flash ไม่น้อยกว่า 512 MB และชนิด DRAM ไม่น้อยกว่า 1 GB

3.5 สนับสนุนการทำ Routing แบบ Static Route ไม่น้อยกว่า 990 Static Routes และ VLAN interface ไม่น้อยกว่า 128 IP Interface

3.6 สนับสนุนการทำ VLAN Spanning Tree ได้

3.7 สนับสนุนจำนวน MAC table ได้สูงสุดไม่น้อยกว่า 16,000 MAC Address

3.8 สามารถรองรับการทำงานตาม Link Aggregation Control Protocol (LACP) ได้

3.9 รองรับการกำหนดคุณภาพการให้บริการ (Quality of Service) ได้

3.10 รองรับมาตรฐาน IEEE802.1D, IEEE802.1w, IEEE802.1p, IEEE802.1q, IEEE802.3ad, IEEE802.3x, IEEE802.1x ได้เป็นอย่างน้อย

3.11 สนับสนุนการทำ VLAN ไม่น้อยกว่า 4,000 VLANs

3.12 ผ่านการรับรองตามมาตรฐานความปลอดภัย UL, CSA, CE mark และ FCC ได้เป็นอย่างน้อย

3.13 อุปกรณ์ต้องสามารถติดตั้งบน Rack 19 นิ้วได้

4. อุปกรณ์ควบคุมระบบเครือข่ายไร้สาย (Wireless Controller) จำนวน 1 ชุด โดยมีคุณสมบัติต่อชุดอย่างน้อย ดังต่อไปนี้

4.1 เป็นอุปกรณ์แบบ Hardware Appliance ที่ออกแบบมาเพื่อทำหน้าที่บริหารจัดการอุปกรณ์ Access Point โดยเฉพาะ

4.2 รองรับการทำ High Availability แบบ controller clustering หรือ Active/Active ได้เป็นอย่างน้อย

4.3 สามารถรับการเชื่อมต่อจากเครื่องลูกข่ายได้ไม่น้อยกว่า 2 ล้านอุปกรณ์ (Maximum concurrent users/devices)

4.4 รองรับการบริหารจัดการอุปกรณ์ Wireless Access Point ได้ไม่น้อยกว่า 1,024 อุปกรณ์ ทั้งรองรับการขยายได้ถึง 2,048 อุปกรณ์ โดยไม่ต้องเปลี่ยน Hardware Appliance ใหม่

4.5 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ SFP+ หรือดีกว่า จำนวน 4 ช่อง พร้อมเสนอโมดูล SFP+ จำนวนไม่น้อยกว่า 4 ตัว

4.6 สามารถทำงานเป็น Stateful Firewall เพื่อใช้ในการกำหนดสิทธิ์การใช้งาน (Policy) และมี Firewall Throughput ไม่น้อยกว่า 30 Gbps พร้อมทั้งรองรับการขยายได้ไม่น้อยกว่า 40 Gbps โดยไม่ต้องเปลี่ยน Hardware Appliance ใหม่ หรือสามารถเสนออุปกรณ์ Firewall ที่มาจากผู้ผลิตเดียวกันกับอุปกรณ์ Wireless Controller ที่เสนอ เพิ่มเติมเข้ามาได้ โดยมี Throughput ไม่น้อยกว่า 40 Gbps

4.7 สามารถทำงานแบบ Deep Packet Inspection (DPI) เพื่อตรวจสอบและควบคุมการใช้งาน Application ได้หรือเสนอระบบอุปกรณ์เพิ่มเติมเพื่อให้สามารถทำงานได้

4.8 มีแหล่งจ่ายไฟ (Power supply) จำนวน 2 ชุดที่สามารถทำงานแบบ Redundant ได้

4.9 สามารถทำงาน Roaming ตามมาตรฐาน 802.11k, 802.11v, 802.11r ได้

4.10 สามารถตรวจสอบสิทธิผู้ใช้งานในรูปแบบ 802.1X, captive portal, MAC address authentication ได้

4.11 สามารถบริหารจัดการผ่าน SNMP, SSH และ Web browser ได้

4.12 สามารถเข้ารหัสข้อมูลตามมาตรฐาน WPA2, WPA3 และ Enhanced Open ได้

4.13 สามารถทำ Client optimization โดยเลือก Access Point ที่ให้ประสิทธิภาพสูงสุดให้กับผู้ใช้งานได้

4.14 สามารถทำ RF optimization โดยปรับช่องสัญญาณและความแรงของสัญญาณให้เข้ากับสภาพแวดล้อมได้โดยอัตโนมัติ

4.15 สามารถตรวจสอบสิทธิผู้ใช้งานร่วมกับ LDAP, RADIUS, TACACS+, Microsoft Active Directory (AD) ได้เป็นอย่างน้อย

4.16 รองรับการทำ GRE tunnel เพื่อทำ Policy Enforcement Firewall ให้กับ user ได้ทั้ง wired และ wireless

4.17 สามารถตรวจจับและป้องกันการโจมตี (Wireless Intrusion Protection) ได้อย่างน้อยดังนี้

4.17.1 การตรวจจับสัญญาณรบกวน Wi-Fi ได้ (Wi-Fi interference detection)

4.17.2 การสแกนและระบุอุปกรณ์ไร้สายที่ไม่ปลอดภัย (Wireless rogue scanning and identification) หรือเทียบเท่า

4.17.3 การกักกันอุปกรณ์ไร้สายที่ไม่ได้รับอนุญาตผ่านการยกเลิกการอนุมัติ (Wireless rogue containment) หรือเทียบเท่า

4.18 อุปกรณ์จะต้องผ่านการรับรองมาตรฐาน FCC, EN และ UL เป็นอย่างน้อย

4.19 เป็นผลิตภัณฑ์ของบริษัทที่อยู่ใน Leaders Quadrant ของ Gartner Magic Quadrant for the Wired and Wireless LAN Access Infrastructure ปีล่าสุด เป็นอย่างน้อย

(ผู้ช่วยศาสตราจารย์อธิพงศ์ สุริยา) (ผู้ช่วยศาสตราจารย์อารยา ฟลอเรนซ์) (นายจิรานุวัฒน์ จันทรุกขา) (นางสาวกรรณิการ์พร กุลบุญญา) (นายวิมล แสวงวงศ์) (นายสุรศักดิ์ ศรีวิเศษ) (นายณัฐพล มารุตะพันธ์)

4.20 อุปกรณ์ที่เสนอต้องสามารถทำงานร่วมกับ Wireless Controller และ Access Point เดิมของมหาวิทยาลัยได้

4.21 ผู้เสนอราคาจะต้องดำเนินการอัพเดทเฟิร์มแวร์ของ Access Point เดิมของมหาวิทยาลัยเพื่อให้ทำงานร่วมกับอุปกรณ์ที่เสนอได้

4.22 ผู้เสนอราคาจะต้องตั้งค่าอุปกรณ์ Wireless Controller เดิมของมหาวิทยาลัยให้สามารถทำงานเป็นระบบสำรอง เมื่ออุปกรณ์ที่เสนอไม่สามารถทำงานได้

5. อุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (Firewall) จำนวน 1 ชุด โดยมีคุณสมบัติต่อชุดอย่างน้อย ดังต่อไปนี้

5.1 เป็นอุปกรณ์รักษาความปลอดภัยเครือข่าย (Firewall) ชนิด Next Generation Firewall และทำหน้าที่ในการป้องกันด้าน Web Application หรือ Web Service สามารถ ติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด 19 นิ้ว ได้

5.2 ได้รับการรับรองหรือทดสอบจาก CyberRatings ระดับ “AAA” หรือ “Recommended”

5.3 มี Firewall Throughput ไม่น้อยกว่า 30 Gbps และ Threat Prevention Throughput ไม่น้อยกว่า 3 Gbps ละรองรับการส่งผ่านข้อมูล New Connections ได้ไม่น้อยกว่า 180,000 Transactions ต่อวินาที

5.4 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) ชนิด 10/100/1000 Base-T หรือดีกว่า จำนวนรวมไม่น้อยกว่า 16 ช่อง

5.5 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) ชนิด 10G SFP+ หรือดีกว่า จำนวนรวมไม่น้อยกว่า 6 ช่อง พร้อมเสนอ SFP+ module ไม่น้อยกว่า 6 ตัว

5.6 มี Interface ที่สามารถรองรับการทำ Hardware Bypass หรืออุปกรณ์เพิ่มเติมจำนวน 4 คู่ เป็นอย่างน้อย ในกรณีฮาร์ดแวร์ขัดข้อง

5.7 มีระบบตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment เป็นต้นได้

5.8 มีฟังก์ชันหรือซอฟต์แวร์เพิ่มเติมในการตรวจพบช่องโหว่แบบ Real-time (Passive Vulnerability Scanner)

5.9 มีความสามารถในการป้องกัน Vulnerability Protection, Content Security, Botnet Detection และ Slow Brute-Force Attacks เพื่อป้องกันการโจมตีจาก Ransomware Attack

5.10 มีความสามารถตรวจสอบการเปิดพอร์ต, ช่องโหว่ และการสแกนรหัสผ่านที่ไม่รัดกุมในการป้องกัน Ransomware

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

5.12 มีความสามารถกำหนด Geolocation เพื่อกำหนดนโยบายความปลอดภัยโดยระบุเป็นรายประเทศได้

5.13 มีความสามารถในการป้องกัน APT (Advanced Persistent Threat) หรือ Threat ด้วยเทคโนโลยี Cloud-Based Sandbox Threats Analysis โดยใช้ ตรวจจับ Botnet, Remote Access Trojan และ Malware ได้เป็นอย่างน้อย

5.14 มีความสามารถในการทำงานแบบ Bandwidth Management โดยควบคุมการทำงานในระดับ Application , User/Group , IP Address , Country/Region และ VLAN interface ได้เป็นอย่างน้อย

5.15 สามารทำงานลักษณะ Transparent Mode ได้

5.16 สามารถ Routing แบบ Static, Dynamic Routing ได้

5.17 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

5.18 สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้

5.19 สามารถใช้งานตามมาตรฐาน IPv6 ได้

5.20 มีอุปกรณ์แบบ Appliance หรือ มี Software ซึ่งทำหน้าที่เป็น Web Application Firewall (WAF) ที่มี Throughput ไม่น้อยกว่า 3.2 Gbps หรือเสนอ Cloud Service ซึ่งทำหน้าที่เป็น Web Application Firewall (WAF) สำหรับเว็บไซต์อย่างน้อย 1 Domain และรองรับ WAF Rules ไม่น้อยกว่า 100 WAF Rules

5.21 ได้รับการรับรองหรือทดสอบจาก NSS Labs ระดับ "Recommended" หรือดีกว่า ในหัวข้อการทดสอบ Web Application Firewall ในกรณีที่เสนออุปกรณ์แบบ Appliance หรือ Software ซึ่งทำหน้าที่เป็น Web Application Firewall (WAF)

5.22 มีความสามารถในการป้องกันการบุกรุกโจมตีเว็บไซต์ (Web Application Firewall) เพื่อให้มีประสิทธิภาพในการป้องกันการโจมตี อย่างน้อยดังนี้

5.22.1 Cross-site Scripting

5.22.2 Cookie Poisoning หรือ Cookie-Based Attack

5.22.3 Buffer Overflow

5.22.4 SQL injection

5.22.5 XML Parser หรือ XML Data Protection

5.22.6 HTTP Request Anomaly

5.22.7 Password Protection

5.22.8 Parameter Protection

5.23 ผลิตภัณฑ์ได้รับมาตรฐานความปลอดภัย เช่น UL หรือ CE หรือ FCC เป็นอย่างน้อย

6. ซอฟต์แวร์ตรวจจับและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์สำหรับเครื่องคอมพิวเตอร์ จำนวนไม่น้อยกว่า 600 สิทธิ์การใช้งาน โดยมีคุณสมบัติอย่างน้อย ดังต่อไปนี้

6.1 ซอฟต์แวร์ Endpoint Detection and Response (EDR) สามารถติดตั้งได้บนระบบปฏิบัติการ ต่อไปนี้ได้เป็นอย่างน้อย

6.1.1 Microsoft Windows 7/8.1/10/11

(ผู้ช่วยศาสตราจารย์อธิพงศ์ สุริยา) (ผู้ช่วยศาสตราจารย์อารยา ฟลอเรนซ์) (นายจิรานุวัฒน์ จันทรุกขา) (นางสาวกรรณิการ์พร กุลบุญญา) (นายวิมล แสวงวงศ์) (นายสุรศักดิ์ ศรีวิเศษ) (นายณัฐพล มารุตะพันธ์)

6.1.2 Microsoft Windows Server 2008/2008 R2/2012/2016/2019

6.1.3 MacOS 10/11/12

6.1.4 Ubuntu 12/13/14/16/18/20

6.2 มีระบบบริหารจัดการจากส่วนกลางแบบ On-Premise

6.3 จัดกลุ่มความแตกต่างของ Endpoint ได้

6.4 มีหน้าจอสำหรับแสดงภาพรวมการตรวจจับภัยคุกคามหรือเหตุการณ์ทางด้านไซเบอร์ที่เกิดขึ้น

6.5 แสดงข้อมูล Hostname, IP Address, OS Version และสถานะ Online/Offline เครื่อง Endpoint ได้

6.6 สามารถ Uninstall และ Restart/Reboot Endpoint Agent ได้

6.7 สามารถในการค้นหาไฟล์ต้องสงสัยที่อาจจะมีอยู่ในเครื่องคอมพิวเตอร์ (Infected File Tracking หรือ Threat Hunting)

6.8 สามารถจัดการภัยคุกคามตาม Event และภัยคุกคามต่อ Endpoint โดยการ Fix หรือ Cleanup และ Isolate ได้

6.9 สามารถทำ Remote support ไปยังเครื่อง Endpoint ได้

6.10 มีคุณลักษณะในการตรวจสอบไวรัสคอมพิวเตอร์ ดังนี้

6.10.1 มีรูปแบบ Traditional Anti-Virus หรือ Signature-based หรือ Gene Analysis, AI-based, Behavioral และ Cloud based engine หรือ Cloud analysis ได้

6.10.2 สามารถตั้งเวลาในการตรวจสอบ (Scheduled Scan) และการตรวจสอบทันที (Real Time) เป็นต้น

6.10.3 สามารถตรวจสอบไฟล์ประเภท Document, Script และ Compressed ได้

6.10.4 มีคุณลักษณะในการตรวจจับ Web shell และ fileless attack ได้

6.11 สามารถป้องกันผู้ใช้งานสั่งปลดการทำงานและการถอดการติดตั้ง Endpoint เช่น การป้องกันโดยการกำหนดรหัสผ่าน Password ก่อนการออกจากโปรแกรมหรือการถอนการติดตั้ง

6.12 มีความสามารถในการสแกนช่องโหว่ (Vulnerability Scan) บน Windows OS หรือ Linux OS

6.13 มีความสามารถในการอุดช่องโหว่ (patch management) หรือการอุดช่องโหว่แบบเสมือน (Virtual Patching)

6.14 มีคุณลักษณะในการตรวจจับและป้องกัน Ransomware ได้

6.15 มีความสามารถในการป้องกันและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์สำหรับเครื่องคอมพิวเตอร์ผู้ใช้งาน (Endpoint Protection and Response หรือ Endpoint Detection and Response)

6.16 สามารถค้นหา Audit Log หรือ Security log โดยสามารถกำหนด Time range, Endpoint name หรือ IP Address ได้

6.17 สามารถออกรายงานภัยคุกคามทางไซเบอร์ (Security Report หรือ Event Report) ในรูปแบบของ PDF ได้เป็นอย่างน้อย

6.18 สามารถทำงานร่วมกับ Firewall เดิมของมหาวิทยาลัยได้

7. ผู้ชนะการเสนอราคาส่งมอบแบตเตอรี่ ขนาด 12V 55Ah จำนวนไม่น้อยกว่า 34 ลูก โดยเปลี่ยนแบตเตอรี่ของเครื่องสำรองไฟฟ้า UPS ขนาด 40KVA รุ่น Liebert Nxr ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

8. ผู้ชนะการเสนอราคาส่งมอบตู้แบตเตอรี่พร้อมแบตเตอรี่ ขนาด 12V 55Ah จำนวนไม่น้อยกว่า 34 ลูก โดยทำการติดตั้งตู้แบตเตอรี่พร้อมแบตเตอรี่ให้กับเครื่องสำรองไฟฟ้า UPS ขนาด 40KVA รุ่น Liebert Nxr พร้อมติดตั้งสายไฟฟ้าต่างๆ ให้สามารถทำงานได้อย่างมีประสิทธิภาพ

9. ผู้ชนะการเสนอราคาต้องทำการติดตั้งอุปกรณ์ในโครงการนี้ ตามจุดที่มหาวิทยาลัยกำหนด ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

10. ผู้ชนะการเสนอราคาต้องทำการอบรมการใช้งานอุปกรณ์ทั้งหมดในโครงการนี้ พร้อมส่งมอบคู่มือการใช้งานแก่ผู้ดูแลระบบของมหาวิทยาลัยอุบลราชธานี

11. มีการรับประกันอุปกรณ์ทั้ง Hardware และ Software ทุกชิ้นส่วนไม่น้อยกว่า 3 ปี และต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา

12. อุปกรณ์ที่เสนอทั้งหมดต้องเป็นของใหม่ที่ยังมิได้ทำการติดตั้งใช้งาน ณ ที่ใดมาก่อน และไม่เป็นอุปกรณ์ที่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt) และเป็นรุ่นที่ยังอยู่ในสายการผลิตโดยต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา

กำหนดเวลาส่งมอบพัสดุ

ส่งมอบภายใน 90 วัน นับถัดจากวันที่ลงนามในสัญญา

หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ใช้เกณฑ์ราคา

วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร

วงเงินงบประมาณ เป็นเงินทั้งสิ้น 7,600,000 บาท (เจ็ดล้านหกแสนบาทถ้วน) รวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงแล้ว

งวดงานและการจ่ายเงิน

มหาวิทยาลัยฯ จะจ่ายเงินให้แก่ผู้ขายงวดเดียว เมื่อผู้ขายได้ส่งมอบพัสดุครบถ้วนและคณะกรรมการตรวจรับพัสดุไว้เรียบร้อยแล้ว

อัตราค่าปรับ

ในกรณีผู้ขายไม่สามารถส่งมอบพัสดุได้ตามสัญญา ผู้ขายจะต้องชำระค่าปรับให้ผู้ซื้อเป็นรายวันในอัตราร้อยละ 0.20 ของราคาพัสดุที่ยังไม่ได้รับมอบ นับถัดจากวันครบกำหนดตามสัญญาจนถึงวันที่ผู้ขายได้นำสิ่งของมาส่งมอบให้แก่ผู้ซื้อจนถูกต้องครบถ้วนตามสัญญา

(ผู้ช่วยศาสตราจารย์อธิพงศ์ สุริยา) (ผู้ช่วยศาสตราจารย์อารยา ฟลอเรนซ์) (นายจิรานุวัฒน์ จันทรุกขา) (นางสาวกรรณิการ์พร กุลบุญญา) (นายวิมล แสวงวงศ์) (นายสุรศักดิ์ ศรีวิเศษ) (นายณัฐพล มารุตะพันธ์)