ประกาศ มหาวิทยาลัยราชภัฏเชียงราย
เลขที่ ๘๗/๒๕๕๘
เรื่อง เปลี่ยนแปลงประกาศเชิญชวน สอบราคาซื้อครุภัณฑ์ จำนวน ๖ รายการ

ตามประกาศ มหาวิทยาลัยราชภัฏเชียงราย เรื่อง สอบราคาซื้อครุภัณฑ์ จำนวน ๖ รายการ ลงวันที่ ๒๓ มีนาคม ๒๕๕๘ โดยกำหนดวัน ขอรับเอกสาร ในวันที่ ๒๓ มีนาคม ๒๕๕๘ ถึงวันที่ ๒ เมษายน ๒๕๕๘ ตั้งแต่เวลา ๐๘.๓๐ น. ถึงเวลา ๑๕.๐๐ น. ความละเอียดแจ้งแล้วนั้น เพื่อให้เกิดการแข่งขันให้มากราย มหาวิทยาลัยราชภัฏเชียงราย ขอเปลี่ยนแปลงประกาศ สอบราคาซื้อครุภัณฑ์ จำนวน ๖ รายการ ดังนี้

รายการที่ ๖. อุปกรณ์ป้องกันการโจมตีเครือข่าย (Firewall) จำนวน ๑ เครื่อง
คุณลักษณะ

๑. อุปกรณ์ต้องเป็น Hardware Appliance ที่ถูกออกแบบมาเป็น Next Generation Firewall โดยเฉพาะ
๒. อุปกรณ์มี Hard Disk ความจุไม่น้อยกว่า ๕๐๐GB และมีหน่วยความจำ RAM ขนาดไม่น้อยกว่า ๔G
๓. มีประสิทธิภาพการทำงาน Firewall Throughput ไม่น้อยกว่า ๑๒Gbps
๔. มีประสิทธิภาพการทำงาน Firewall Throughput แบบ App & URL enabled ไม่น้อยกว่า ๑Gbps
๕. มีประสิทธิภาพการทำงาน IPS Throughput ไม่น้อยกว่า ๖๕๐Mbps
๖. มีประสิทธิภาพการทำงาน Web Application Firewall(WAF) Throughput ไม่น้อยกว่า ๕๕๐Mbps
๗. สามารถรองรับการเชื่อมต่อพร้อมกัน (Max concurrent session) ได้ไม่น้อยกว่า ๒,๓๐๐,๐๐๐sessions
๘. สามารถรองรับการเชื่อมต่อใหม่ในหนึ่งวินาที (New sessions per second) ได้ไม่น้อยกว่า ๙๐,๐๐๐sessions
๙. มี Network Interfaces อย่างน้อยดังต่อไปนี้
   ๙.๑ แบบ ๑๐/๑๐๐/๑๐๐๐ จำนวนไม่น้อยกว่า ๘ พอร์ต โดยสามารถทำ Bypass ได้ ๒ คู่
   ๙.๒ มีช่องเสียบ Network Interfaces แบบ ๑G Fiber SFP จำนวนไม่น้อยกว่า ๒ พอร์ต
๑๐. มีการทำงาน Firewall ด้วยเทคโนโลยี Package Filtering แบบ Static และ Dynamic
๑๑. สามารถทำงาน Routing แบบ Policy Routing, OSPF, และ RIP ได้เป็นอย่างน้อย
๑๒. สามารถติดตั้งใช้งานได้หลายรูปแบบ เช่น Gateway, Bridge, Bypass mode, Virtual wire, และ Mix mode
๑๓. มีความสามารถในการป้องกันการโจมตีระบบเครือข่ายจากรูปแบบดังต่อไปนี้ได้เป็นอย่างน้อย ได้แก่ Attack of Lands, Smurf, Fraggle, WinNuke, Ping of Death, Tear Drop, IP Spoofing, SYN Flood, ICMP Flood, UDP Flood, DNS Query Flood, ARP cheating, ICMP redirection เป็นต้น พร้อมสิทธิในการปรับปรุง (Update) ฐานข้อมูล Application ให้ทันสมัยโดยอัตโนมัติได้ตลอดช่วงระยะเวลาของการรับประกันอุปกรณ์
๑๔. สามารถระบุและควบคุมการใช้งานอินเทอร์เน็ตโดยแยกแยะตามชนิดของ Application ได้ พร้อมสิทธิในการปรับปรุง (Update) ฐานข้อมูล Application ให้ทันสมัยโดยอัตโนมัติได้ตลอดช่วงระยะเวลาของการรับประกันอุปกรณ์

๑๕. สามารถกรอง (Filter) การเข้าถึง Website (URL) โดยกำหนดตามประเภทของ URL Category ได้ พร้อมสิทธิในการปรับปรุง (Update) ฐานข้อมูล URL Category ให้ทันสมัยโดยอัตโนมัติได้ตลอดระยะเวลาของการรับประกันอุปกรณ์

๑๖. สามารถป้องกันการบุกรุก (Intrusion Prevention) และป้องกันการโจมตี Web Application (WAF) โดยอ้างอิงตามมาตรฐานจาก CVE และ OWASP ได้เป็นอย่างน้อย พร้อมสิทธิในการปรับปรุง (Update) ฐานข้อมูล IPS และ WAF ให้ทันสมัยโดยอัตโนมัติได้ตลอดช่วงระยะเวลาของการรับประกันอุปกรณ์

๑๗. มีความสามารถตรวจจับ Malware เช่น Trojan, Adware, Spy, Backdoor, Worm, Exploit, Hack Tool ได้

๑๘. มีความสามารถในการป้องกัน Web Application โดยสามารถป้องกัน ๑๐ อันดับความเสี่ยงช่องโหว่ด้าน Web Application อ้างอิงจากองค์กรกลาง OWASP เช่น SQL injection, XSS attack, CRSF ได้เป็นอย่างน้อย

๑๙. สามารถทำงานร่วมกับ Active Directory (AD), LDAP, RADIUS และ POP๓ เพื่อใช้ฐานข้อมูลดังกล่าวในการพิสูจน์ตัวตนของผู้ใช้งานได้เป็นอย่างน้อย และสามารถ Mapping โดยใช้ IP, MAC, IP/MAC binding, hostname, และ USB-Key ได้

๒๐. สามารถทำการยืนยันตัวตนแบบ Single Sign-On (SSO) โดยต้องสามารถใช้ฐานข้อมูลร่วมกับ Active Directoryได้เป็นอย่างน้อย

๒๑. สามารถปรับแต่ง (Custom) หน้า Webpage ดังต่อไปนี้ได้เป็นอย่างน้อย เช่น Authentication Successful, Access Denied, Virus Detected, Change Password, Bulletin, Web-Access Portal, และ Locked User Login Failure

๒๒. สามารถทำงาน Bandwidth Management เช่น Guarantee / Limit bandwidth ตาม User, Application, IP address, File type, Website type, และช่วงเวลา (Schedule) ได้เป็นอย่างน้อย

๒๓. มีความสามารถทำงานแบบ Multiple WAN Link เพื่อทำ Load Balancing ได้

๒๔. มีความสามารถในการทำงาน Anti-Defacement สำหรับปกป้อง Webpage ได้

๒๕. มีความสามารถในการตรวจจับและป้องกันข้อมูลรั่วไหล (DLP) โดยใช้เทคนิคและวิธีการดังต่อไปนี้ ได้เป็นอย่างน้อย

๒๕.๑ User-defined sensitive information เช่น Username, Password, Mailbox เป็นต้น

๒๕.๒ HTTP connection

๒๕.๓ Database leakage

๒๖. สามารถทำการตรวจสอบหาช่องโหว่ความเสี่ยงภัย (Risk Assess) ดังต่อไปนี้ได้เป็นอย่างน้อย

๒๖.๑ สามารถทำ Port และ Service Scanning และประเมินความเสี่ยงภัย (Security Risk) สำหรับ Server ได้

๒๖.๒ สามารถตรวจสอบหา Weak Password สำหรับ FTP, MYSQL, ORACLE, MSSQL, SSH, RDP, NetBIOS, และ VNC services ได้เป็นอย่างน้อย

๒๖.๓ สามารถทำงานแบบ Cross-module ในการสร้างนโยบายความปลอดภัยสำหรับ Firewall, IPS, WAF ได้อัตโนมัติ

๒๗. มีความสามารถทำ DoS/DDoS protection และ ARP protection

๒๘. มีระบบจัดเก็บ Log โดยสามารถแสดง Alert หรือแจ้งเตือน ในกรณีที่เกิดเหตุการณ์ต่างๆ ได้ และมีระบบการจัดเก็บข้อมูล Log แบบ History เพื่อใช้ในการดูรายงาน (Report) ย้อนหลังได้บนตัวอุปกรณ์เอง หรือผู้เสนอราคาสามารถนำเสนออุปกรณ์เสริมที่มียี่ห้อเดียวกันกับ Firewall ที่เสนอ เพื่อให้สามารถทำงานดังกล่าวข้างต้นได้

๒๙. รองรับการทำงานแบบ High Availability โดยรองรับการทำ Configuration Synchronization ได้

๓๐. อุปกรณ์ต้องมีแหล่งจ่ายไฟฟ้าแบบ Dual Power Supply

๓๑. ผู้เสนอราคาต้องนำเสนออุปกรณ์พร้อม License แบบไม่จำกัดจำนวนผู้ใช้งาน และการรับประกัน Hardware และการอัพเดต Firmware เป็นเวลาไม่น้อยกว่า ๑ ปี

๓๒. ผู้เสนอราคาต้องมีหนังสือรับรองการรับประกันสินค้าโดยตรงจาก บริษัทเจ้าของผลิตภัณฑ์หรือบริษัทสาขาของเจ้าของผลิตภัณฑ์ประจำประเทศไทยมาแสดงในวันยื่นราคา

ส่วนข้อความอื่นๆ ให้เป็นไปตามเดิมทุกประการ

ประกาศ ณ วันที่ ๓๐ มีนาคม พ.ศ. ๒๕๕๘

(ผู้ช่วยศาสตราจารย์เจษฎา สุวรรณ)
รองอธิการบดี รักษาราชการแทน
อธิการบดี