รายละเอียดคุณลักษณะงานเช่าอุปกรณ์ป้องกันเครือข่าย (Firewall) จำนวน 1 ระบบ
มหาวิทยาลัยราชภัฏนครศรีธรรมราช

1. คุณสมบัติทั่วไปของผู้เสนอราคา

1.1 เป็นนิติบุคคลผู้มีอาชีพขายเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วง ที่ประมูลด้วยวิธีทางอิเล็กทรอนิกส์

1.2 ไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว

1.3 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกัน

1.4 ผู้เสนอราคาต้องมีประสบการณ์ในอุปกรณ์ที่นำเสนอในงานจัดซื้อหรืองานจ้างบำรุงรักษา โดยต้องมีหนังสือรับรองผลงาน สำหรับอุปกรณ์ป้องกันเครือข่ายแบบ Next Generation Firewall ภายใต้ผู้ผลิตเดียวกันกับสินค้าที่นำเสนอ วงเงินไม่น้อยกว่า 1,300,000 บาท ในระยะเวลาไม่เกิน 5 ปี นับจากวันยื่นซองประกวดราคา ไม่น้อยกว่า 3 สัญญาและเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานภาคการศึกษา หน่วยงานของรัฐ หรือหน่วยงานเอกชนที่มหาวิทยาลัยราชภัฏนครศรีธรรมราชเชื่อถือ โดยเอกสารต้องลงนามและประทับตรา(ถ้ามี) ของหน่วยงานที่ออกหนังสือรับรองให้

1.5 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

2. ข้อกำหนดทางเทคนิค

อุปกรณ์ป้องกันเครือข่ายแบบ Next Generation Firewall พร้อมระบบวิเคราะห์ Log จำนวน 1 ระบบ คุณสมบัติดังต่อไปนี้

2.1 เป็นอุปกรณ์ Appliance ที่ออกแบบขึ้นมาเฉพาะ เพื่อทำหน้าที่เป็น Next Generation Firewall และ มีหน่วยประมวลผลเป็นแบบ SPU เพื่อทำหน้าที่สนับสนุนการทำงานของตัวอุปกรณ์

2.2 อุปกรณ์ที่นำเสนอต้องอยู่ภายใต้ Gartner Magic Quadrant for Network Firewall ปี 2022 (September) หรือใหม่กว่า ในระดับ Leaders

2.3 อุปกรณ์จะต้องมี Interface สำหรับเชื่อมต่อระบบเครือข่ายแบบ Gigabit Ethernet (RJ-45) ไม่น้อยกว่า 16 ช่อง, SFP ไม่น้อยกว่า 8 ช่อง และแบบ SFP+ ไม่น้อยกว่า 4 ช่อง และ SFP28 จำนวนไม่น้อยกว่า 4 ช่อง โดยทุก Interface ต้องสนับสนุนการกำหนด (Interface Rule)

ลงชื่อ.....ประธานกรรมการ
ลงชื่อ.....กรรมการ
ลงชื่อ.....กรรมการ
ลงชื่อ.....กรรมการ
ลงชื่อ.....กรรมการและเลขานุการ

เป็น LAN, WAN หรือ DMZ ได้ และสามารถกำหนด (Interface Zone) ที่ผู้ดูแลระบบกำหนดขึ้นมาเองได้โดยอิสระ หรือสามารถกำหนดให้เป็น Interface สำหรับทำ HA ได้

2.4 สนับสนุน IPv4 Firewall Throughput สำหรับการรับส่งข้อมูลแบบ UDP ที่ 1518 Byte ได้ไม่น้อยกว่า 139 Gbps

2.5 สนับสนุนการเชื่อมต่อพร้อมกัน (Concurrent Sessions) แบบ TCP ได้ไม่น้อยกว่า 8,000,000 Sessions พร้อมสนับสนุนการสร้างการเชื่อมต่อใหม่ต่อวินาที (New Sessions/ Second) ได้ไม่น้อยกว่า 550,000 Sessions

2.6 สนับสนุนการตรวจสอบและป้องกันการโจมตีโดยมี IPS Throughput ไม่น้อยกว่า 14 Gbps, Threat Protection Throughput ไม่น้อยกว่า 10.5 Gbps และ Next Generation Firewall Throughput ไม่น้อยกว่า 11.5 Gbps

2.7 สนับสนุนการทำ IPsec VPN และ SSL VPN โดยมี Throughput ไม่น้อยกว่า 55 Gbps และ 4.3 Gbps ตามลำดับ

2.8 สนับสนุนการทำ SSL VPN จากเครื่อง Client ไม่น้อยกว่า 5,000 Users พร้อมลิขสิทธิ์ในการใช้งาน

2.9 สนับสนุนการบริหารการจัดการอุปกรณ์ผ่าน Console และ Web Browser เช่น Firefox หรือ Google Chrome ได้

2.10 สนับสนุนการสร้าง Firewall Policies ผสมผสานกันระหว่าง IP Address, User, NAT, Security Profile ภายใต้ Firewall Policies ในข้อเดียวกันได้

2.11 สนับสนุนการกำหนดให้อุปกรณ์ป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้ สนับสนุนการกำหนดให้ป้องกัน Java applet, Cookies และ Active X ได้ และมีความสามารถในการตรวจจับและหยุดการทำงานของ Malware, Phishing หรือ Pharming ได้

2.12 สนับสนุนการป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้

2.13 สนับสนุนการตรวจจับและป้องกัน Virus ที่ผ่านช่องทาง HTTP, FTP, SMTP, POP3, IMAP และ MAPI ได้

2.14 สนับสนุนการป้องกัน Spam Email ด้วยวิธี IP address check, URL check และ Email checksum ได้

2.15 อุปกรณ์ต้องมีระบบป้องกัน Web Application (Web Application Firewall)

2.16 สนับสนุนการทำงานในลักษณะ Content Filtering ได้ โดยสามารถกำหนดให้อุปกรณ์ป้องกันการเข้าถึง URL หรือ Web site ที่ต้องห้ามได้ (URL blocking หรือ URL Filtering)

ลงชื่อ.....ประธานกรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการและเลขานุการ

2.17 สนับสนุน IPv6 ในการทำงานต่างๆ ดังต่อไปนี้ Routing, Firewall Policy, UTM, NAT64, NAT46, IPSec และ VRRP ได้

2.18 มีความสามารถในการป้องกันการบุกรุก (Intrusion Prevention) โดยสามารถตรวจจับการบุกรุกได้ด้วยวิธีการตรวจสอบด้วย Signature และ Anomaly-based Defense เป็นอย่างน้อย

2.19 สนับสนุนการสร้างฐานข้อมูลรูปแบบการบุกรุกได้ด้วยตนเอง (Custom Signature)

2.20 สนับสนุนการควบคุมการเชื่อมโยงและจำกัดการใช้งาน Bandwidth ให้แก่โปรแกรมประเภท peer-to-peer ได้

2.21 สนับสนุนการทำ SD-WAN โดยสนับสนุนการตรวจสอบคุณภาพของเส้นทางด้วย packet loss, latency และ jitter พร้อมกำหนด Load Balancing ได้

2.22 สนับสนุนการทำ Auto-Discovery VPN (ADVPN) โดยสนับสนุนการทำงานแบบ UDP hole punching ได้

2.23 รองรับการตรวจสอบผู้ใช้งาน (User Authenticator) กับ Local User ภายในตัวอุปกรณ์เอง, LDAP และ Radius รวมถึงสามารถทำงานแบบ Single Sign-On กับ ฐานข้อมูลผู้ใช้งานบน Active Directory (AD) และ Radius ได้

2.24 สนับสนุนการบริหารจัดการอุปกรณ์ได้ทั้งทาง Web GUI (HTTP หรือ HTTPS), SSH, SNMP (v1, v2c, v3)

2.25 สนับสนุนการทำการแจ้งเตือนผู้ดูแลระบบด้วยอีเมล (Email notification) ได้

2.26 สนับสนุนการสร้างบัญชีผู้ใช้งาน (User Account) ประเภท Guest หรือ Temp User ที่มีรหัสผ่านแบบสุ่ม (Random Password) และสนับสนุนการพิมพ์บัญชีผู้ใช้งานดังกล่าวในรูปแบบตั๋ว (Ticket) ได้

2.27 รองรับการทำงานแบบ Two Factor Authentication ได้โดยไม่ต้องติดตั้ง Token Server

2.28 สนับสนุนการแบ่งระดับของผู้ดูแลระบบได้หลายระดับเพื่อความปลอดภัยของการจัดการอุปกรณ์ได้ Administrator Profile

2.29 สนับสนุนการส่ง Log แบบ Syslog ตามมาตรฐาน RFC-3195 และ CEF ไปยัง Server ภายนอกได้มากกว่า 1 Server

2.30 สนับสนุนการกำหนดช่วงเวลา Update Signature ใหม่ ได้อย่างน้อยทุกๆ 1 ชั่วโมง

2.31 สนับสนุนการทำ High Availability (HA) ด้วยการทำงานแบบ Active-Active ได้

2.32 สนับสนุนการกำหนด Virtual Domains ได้ไม่น้อยกว่า 10 Virtual Domains

2.33 อุปกรณ์ต้องได้รับการรับรองจาก ICSA Labs ดังนี้ Firewall, IPsec, IPS, Antivirus และ SSL-VPN

2.34 อุปกรณ์ที่นำเสนอต้องผ่านมาตรฐาน FCC และ UL หรือเทียบเท่า

ลงชื่อ.....ประธานกรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการและเลขานุการ

2.35 อุปกรณ์จะต้องมีแหล่งจ่ายไฟแบบ Redundant Power Supply

2.36 อุปกรณ์ต้องมีการรับประกันโดยผู้ผลิต โดยต้องสามารถ Update Services ต่างๆ ได้ เช่น IPS, Antivirus และ Web Filtering ตลอดระยะเวลาของการรับประกัน 3 ปี

2.37 อุปกรณ์ทุกชิ้นต้องได้รับรองจากบริษัทผู้ผลิตฯ ที่เป็นตัวแทนในประเทศไทยเท่านั้น ในการเปิด case เพื่อสนับสนุนทางด้านเทคนิคและการบริการหลังการขาย

2.38 ระบบวิเคราะห์ Log จำนวน 1 เครื่อง มีคุณสมบัติดังต่อไปนี้

2.38.1 เป็นอุปกรณ์ Hardware Appliance ที่สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่เกิดขึ้นบนอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) หรือ SD-WAN ที่เสนอมาในโครงการได้ และอยู่ภายใต้เครื่องหมายการค้าเดียวกัน

2.38.2 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1 GE ชนิด RJ-45 จำนวนไม่น้อยกว่า 4 พอร์ต

2.38.3 มี Storage แบบ 4TB ไม่น้อยกว่า 2 หน่วย และมีคุณสมบัติการทำ RAID 0, 1 ได้เป็นอย่างน้อย

2.38.4 มีอัตราความสามารถในการจัดเก็บข้อมูลเพื่อวิเคราะห์ได้ไม่น้อยกว่า 2,000 Logs per second และสามารถรองรับจำนวน log ได้ไม่น้อยกว่า 100 GB ต่อวัน หรือสามารถเสนอระบบอื่นเพิ่มเติมเพื่อให้จัดเก็บข้อมูลได้ตามข้อกำหนด

2.38.5 รองรับการทำงานร่วมกับ Device หรือ Virtual Domain ได้สูงสุดไม่น้อยกว่า 180 devices/VDOMs

2.38.6 สามารถตรวจสอบความถูกต้องของข้อมูลที่จัดเก็บ (Checksum) ตามมาตรฐาน MD5 หรือ SHA-1 หรือดีกว่า

2.38.7 สามารถบริหารจัดการอุปกรณ์ผ่านโปรโตคอล HTTPS ผ่าน Web Browser ได้โดยตรงโดยไม่ต้องติดตั้งซอฟต์แวร์เพิ่มเติม และโปรโตคอล SSH ได้เป็นอย่างน้อย

2.38.8 สามารถแสดงข้อมูล Log เช่น Date, Time, Source IP, User, Destination IP และ Services ได้เป็นอย่างน้อย

2.38.9 มีรูปแบบรายงาน (Report templates) มาให้อย่างน้อย 30 รูปแบบ และสามารถแสดงรายงานในรูปแบบของ PDF, HTML และ CSV ได้เป็นอย่างน้อย

2.38.10 มี Power Supply แบบ Redundant พร้อมคุณสมบัติ Hot Swap

2.38.11 มีคุณสมบัติดังต่อไปนี้ ได้โดยไม่ต้องปรับการตั้งค่าใดๆ บนอุปกรณ์วิเคราะห์ Log เดิมและอุปกรณ์ป้องกันเครือข่ายที่เสนอ

ลงชื่อ.....ประธานกรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการและเลขานุการ

1) แสดงข้อมูล Top sources, Top destinations, Top applications, Top websites, Top threats, System events และ Resource usage ได้

2) ออกรายงาน ตาม Template เช่น 360 Protection Report, Admin and System Events Report, Cyber Threat Assessment ได้เป็นอย่างน้อย

2.38.12 ได้รับการรับรองตามมาตรฐาน FCC, VCCI, CE, CB, RCM และ UL เป็นอย่างน้อย

2.38.13 อุปกรณ์ต้องมีการรับประกันโดยผู้ผลิต ตลอดระยะเวลาของการรับประกัน 3 ปี

2.38.14 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง เพื่อการให้บริการที่ถูกต้อง

2.38.15 อุปกรณ์ทุกชิ้นต้องได้รับรองจากบริษัทผู้ผลิตฯ ที่เป็นตัวแทนในประเทศไทยเท่านั้น ในการเปิด case เพื่อสนับสนุนทางด้านเทคนิคและการบริการหลังการขาย

3. ข้อกำหนดในการติดตั้ง

3.1 ผู้ชนะการประกวดราคาต้องดำเนินการติดตั้งอุปกรณ์ในโครงการนี้ให้พร้อมใช้งาน

3.2 ดำเนินการติดตั้งค่าตามที่มหาวิทยาลัยกำหนด โดยต้องดำเนินการจัดการทำ Authentication ร่วมกับระบบฐานข้อมูลเดิมของมหาวิทยาลัย เพื่อควบคุมการใช้งานระบบอินเทอร์เน็ต เป็นต้น

3.3 จัดทำแผนงานการติดตั้ง Gantt Chart เพื่อกำหนดแผนการดำเนินงาน เสนอต่อคณะกรรมการตรวจรับพัสดุก่อนการติดตั้ง Gantt Chart

3.4 หลังการติดตั้งเสร็จต้องทำ UAT หรือ User Acceptance Test เพื่อสรุปผลการติดตั้ง และเสนอต่อคณะกรรมการตรวจรับพัสดุ

4. ระยะเวลาการส่งมอบงาน

4.1 ผู้ชนะการเสนอราคาต้องส่งมอบงานภายในระยะเวลา 60 วัน นับถัดจากวันที่ลงนามในสัญญา

5. การรับประกันและบำรุงรักษา

5.1 ผู้เสนอราคาต้องรับประกันอุปกรณ์และวัสดุที่นำเสนอทุกชิ้นส่วน ทั้งฮาร์ดแวร์และซอฟต์แวร์ เป็นระยะเวลาอย่างน้อย 3 ปี (ค่าอะไหล่และค่าบริการ) โดยมีเอกสารรับรองจากบริษัทผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย

5.2 กรณีที่เกิดปัญหาทางด้านฮาร์ดแวร์และซอฟต์แวร์ ผู้เสนอราคาต้องเข้ามาทำการแก้ไข ซ่อมแซม ณ สถานที่ติดตั้ง (Onsite Service) ตลอดระยะเวลารับประกัน โดยมีเอกสารรับรองจากบริษัทผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย

ลงชื่อ.....ประธานกรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการและเลขานุการ

6. งวดงานงวดเงิน

6.1 กำหนดระยะเวลาเช่าเป็นจำนวน 3 ปี นับถัดจากวันที่ได้รับพัสดุครบและถูกต้อง

6.2 การชำระเงินเป็นงวด จำนวน 3 งวด ปีละ 1 งวด โดยเบิกจ่ายค่าเช่าเมื่อสิ้นงวด

7. ข้อกำหนดทั่วไป

7.1 หากมีข้อที่จะต้องวินิจฉัยหรือที่จะต้องพิจารณานอกเหนือจากข้อกำหนดนี้ จะต้องยึดผลประโยชน์ของทางราชการเป็นสำคัญ หรือให้ยึดตามมติของคณะกรรมการตรวจรับพัสดุที่ได้รับการแต่งตั้งขึ้น

7.2 รายละเอียดนี้เป็นข้อกำหนดมาตรฐานขั้นต่ำสุด คณะกรรมการตรวจรับพัสดุจะพิจารณารายละเอียดที่เทียบเท่าหรือดีกว่า เพื่อประโยชน์ของทางราชการ

7.3 อุปกรณ์และวัสดุทุกชิ้นนำมาใช้ในการติดตั้งในงานนี้ จะต้องเป็นของใหม่ที่ไม่เคยใช้งานมาก่อน และจะต้องทำงานร่วมกันเป็นระบบเดียวกัน โดยไม่มีปัญหาใดๆ และสามารถทำงานกับระบบเดิมได้

7.4 ผู้เสนอราคาต้องเสนอราคาที่รวมทั้งราคาสินค้า (ซึ่งรวมภาษีและอากรทุกชนิดแล้ว) ค่าขนส่งถึงสถานที่ติดตั้ง ค่าติดตั้ง ค่าฝึกอบรม และค่าใช้จ่ายอื่นๆ อันพึงมีในการดำเนินการครั้งนี้

7.5 ผู้ชนะการประกวดราคาจะต้องติดตั้ง อุปกรณ์ ทุกชิ้นให้สามารถใช้งานได้อย่าง มีประสิทธิภาพ และสามารถทำงานร่วมกับอุปกรณ์ในระบบเดิมที่มีอยู่แล้วได้เป็นอย่างดี

7.6 อุปกรณ์และวัสดุทุกชิ้นส่วนซึ่งผู้เสนอราคาจัดหาและได้นำมาเก็บรักษาไว้ในหน่วยงานที่ติดตั้งงาน ผู้เสนอราคาจะต้องรับผิดชอบ ทั้งในการบำรุงรักษา การเสื่อมสภาพ การสูญหาย การถูกทำลาย และความเสียหายใดๆ ตลอดระยะเวลารับประกัน 3 ปี โดยมีเอกสารรับรองจากผู้เสนอราคาหรือตัวแทนจำหน่ายในประเทศไทย

7.7 หลังจากสิ้นสุดสัญญาอุปกรณ์ป้องกันเครือข่าย (Firewall) ในโครงการเช่าอุปกรณ์ป้องกันเครือข่าย (Firewall) จะถือเป็นกรรมสิทธิ์ของมหาวิทยาลัย โดยมีเอกสารรับรองจากผู้เสนอราคาหรือตัวแทนจำหน่ายในประเทศไทย

7.8 ระยะเวลาการส่งมอบไม่เกิน 120 วัน ยืนราคาไม่น้อยกว่า 120 วัน

มหาวิทยาลัยราชภัฏนครศรีธรรมราช

ลงชื่อ.....ประธานกรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการ

ลงชื่อ.....กรรมการและเลขานุการ