ขอบเขตของงาน

"จัดซื้ออุปกรณ์รักษาความปลอดภัย"

1. หลักการและเหตุผล

บริษัท เฮงลิสซิ่ง แอนด์ แคปปิตอล จำกัด (มหาชน) มีความประสงค์จะจัดซื้ออุปกรณ์รักษาความปลอดภัย เพื่อนำมาใช้เป็นอุปกรณ์หลักในการรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ และพัฒนาประสิทธิภาพอุปกรณ์รักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ให้ทันสมัย และเพียงพอต่อการใช้งานในอนาคต

2. คุณสมบัติและประสบการณ์ของผู้เสนอราคา

2.1 เป็นผู้ที่มีประสบการณ์ในการขาย และติดตั้ง อุปกรณ์รักษาความปลอดภัย

2.2 มีความสามารถในการออกแบบและติดตั้งระบบตามความต้องการของบริษัท

2.3 ไม่เป็นผู้ถูกขึ้นบัญชีละทิ้งงาน หรืออยู่ระหว่างถูกดำเนินคดีในงานที่รับจ้างกับภาครัฐและเอกชน

2.4 ต้องได้รับการสนับสนุนในด้านเทคนิคและการบริการทั้งฮาร์ดแวร์ และซอฟท์แวร์ จากผู้ผลิตเดียวกันโดยตรง และอุปกรณ์ที่เสนอต้องยังอยู่ในสายการผลิต และเป็นอุปกรณ์ใหม่ ไม่เป็นของเก่าเก็บ โดยมีหนังสือรับรองอย่างเป็นทางการจากผู้ผลิต

2.5 ต้องเป็นบริษัทที่มีที่ตั้ง หรือสำนักงานสาขาในจังหวัดเชียงใหม่ หรือต้องแสดงว่าสามารถให้บริการด้านเทคนิคแบบ 24 x7x4 ได้ ทั้งนี้เพื่อให้สามารถเข้ามาดำเนินการแก้ไขปัญหาในกรณีร้ายแรงได้อย่างทันท่วงที และสอดคล้องต่อความต้องการด้านบริการของธุรกิจ

3. ขอบเขตของงาน

3.1 อุปกรณ์รักษาความปลอดภัยเครือข่าย จำนวน 2 ตัว

3.1.1 เป็นอุปกรณ์ Appliance ที่ออกแบบขึ้นมาเฉพาะ เพื่อทำหน้าที่เป็น Next Generation Firewall และมีหน่วยประมวลผลเป็นแบบ SPU เพื่อทำหน้าที่สนับสนุนการทำงานของตัวอุปกรณ์

3.1.2 อุปกรณ์ที่นำเสนอต้องอยู่อยู่ภายใต้ Gartner Magic Quadrant for Network Firewalls ในระดับ Leaders

3.1.3 อุปกรณ์จะต้องมี Interface สำหรับเชื่อมต่อระบบเครือข่ายแบบ Gigabit Ethernet (RJ-45) ไม่น้อยกว่า 16 ช่อง, แบบ SFP ที่รองรับการติดตั้ง SFP Transceivers ไม่น้อยกว่า 8 ช่อง และแบบ SFP+ ที่รองรับการติดตั้ง SFP+ Transceivers ไม่น้อยกว่า 8 ช่อง โดยทุก Interface จะต้องสามารถกำหนด (Interface Role) เป็น LAN, WAN หรือ DMZ ได้ และสามารถกำหนด (Interface Zone) ที่ผู้ดูแลระบบกำหนดขึ้นมาเองได้โดยอิสระ หรือสามารถกำหนดให้เป็น Interface สำหรับทำ HA ได้

3.1.4 มีความเร็วในการทำงาน Firewall Throughput (1518 Byte UDP) ไม่น้อยกว่า 75 Gbps

3.1.5 สามารถรองรับการเชื่อมต่อพร้อมกัน (Concurrent Sessions) TCP ได้ไม่น้อยกว่า 7,500,000 Sessions

3.1.6 สามารถตรวจสอบ และป้องกันการโจมตีเครือข่ายโดยมี IPS Throughput ไม่น้อยกว่า 12 Gbps และมี Threat Protection Throughput ไม่น้อยกว่า 9 Gbps

3.1.7 สามารถทำการเชื่อมโยง IPsec VPN ซึ่งมีความเร็วในการทำงานไม่น้อยกว่า 55 Gbps

3.1.8 สามารถทำการเชื่อมโยง SSL VPN จากเครื่อง Client ไม่น้อยกว่า 5,000 Users พร้อมลิขสิทธิ์ในการใช้งาน

3.1.9 สามารถบริหารการจัดการอุปกรณ์ผ่าน Console และ Web Browser เช่น Firefox หรือ Google Chromeได้

3.1.10 สามารถสร้าง Firewall Policies ผสมผสานกันระหว่าง IP Address, User, NAT, Security Profile ภายใต้ Firewall Policies ในข้อเดียวกันได้

3.1.11 สามารถตรวจจับ และป้องกัน Virus ที่ผ่านมากับโปรโตคอล HTTP, IMAP, SMTP, POP3, MAPI และ FTP ได้

3.1.12 สามารถทำงานในลักษณะ SD-Wan ที่ควบคุมเส้นทางของ Traffic ต่อไปนี้ได้เป็นอย่างน้อย

3.1.12.1 Load Balancing จาก คุณภาพของ Link เช่น Latency, Jitter, Package Loss

3.1.12.2 Load Balancing จาก Cloud Service เช่น Office 365

3.1.13 สามารถป้องกัน Spam Email ด้วยวิธี IP address check, URL check และ Email checksumได้

3.1.14 อุปกรณ์ต้องมีระบบป้องกัน Web Application (Web Application Firewall)

3.1.15 สามารถรองรับการทำงานกับ IPV6 ได้ดังนี้ Routing, Firewall, UTM, NAT64, NAT46, IPSec

3.1.16 สามารถส่งข้อมูลขึ้นไปตรวจสอบความเสี่ยงในระบบ Sandbox Cloud เพื่อตรวจจสอบ Unknown Malware ได้

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

3.1.18 สามารถรองรับการทำงานแบบ Two Factor Authentication ได้โดยไม่ต้องติดตั้ง Token Server

3.1.19 สามารถแบ่งระดับของผู้ดูแลระบบได้หลายระดับเพื่อความปลอดภัยของการจัดการอุปกรณ์ได้ Administrator Profile

3.1.20 สามารถสร้างบัญชีผู้ใช้งาน (User Account) ประเภท Guest หรือ Temp User ที่มีรหัสผ่านแบบสุ่ม (Random Password) และสามารถพิมพ์บัญชีผู้ใช้งานดังกล่าวในรูปแบบตั๋ว (Ticket) ได้

3.1.21 สามารถรองรับการบริหารจัดการอุปกรณ์กระจายสัญญาณแบบไร้สาย (Wireless Controller) ที่รองรับการเชื่อมต่ออุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ภายใต้ยี่ห้อเดียวกันกับอุปกรณ์รักษาความปลอดภัย ที่นำเสนอ

3.1.22 สามารถส่ง Log แบบ Syslog ตามมาตรฐาน RFC-3195 และ CEF ไปยัง Server ภายนอกได้มากกว่า 1 Server

3.1.23 สามารถกำหนดช่วงเวลา Update Signature ใหม่ ได้อย่างน้อยทุกๆ 1 ชั่วโมง

3.1.24 รองรับการทำงานลักษณะ Virtual Domains ได้อย่างน้อย 10 Virtual Domains

3.1.25 อุปกรณ์ที่นำเสนอต้องผ่านมาตรฐาน FCC และ UL

3.1.26 มี Power Supply แบบ Redundant พร้อมคุณสมบัติ Hot Swap

3.1.27 แผนงานและขั้นตอนการเปลี่ยนถ่ายอุปกรณ์รักษาความปลอดภัยเดิม

3.1.28 สนับสนุนทางด้านเทคนิคและการบริการอย่างน้อย 1 ปี

3.1.29 ผู้เสนอราคาต้องเป็น Partner กับผลิตภัณฑ์ที่เสนอเพื่อให้ บริษัทได้รับบริการด้านเทคนิคและการช่วยเหลือด้านอุปกรณ์

3.2 ข้อกำหนดด้านการติดตั้ง

3.2.1 ผู้เสนอราคาต้องเสนอแผนในการดำเนินงานแนบมาเพื่อประกอบการพิจารณา โดยต้องนำเสนอแผนงานครอบคลุม ดังนี้

3.2.1.1 แผนการติดตั้งอุปกรณ์ใหม่

3.2.1.2 แผนการย้าย Configuration จากอุปกรณ์รักษาความปลอดภัยเครือข่ายตัวเก่า ไปยังอุปกรณ์รักษาความปลอดภัยเครือข่ายตัวใหม่

3.2.2 ผู้เสนอราคาต้องทำการติดตั้งอุปกรณ์ภายในตู้ Rack ที่บริษัทจัดเตรียมไว้ให้

3.2.3 ผู้เสนอราคาต้องทำการติดตั้งอุปกรณ์และตั้งค่าอุปกรณ์แบบ HA

3.2.4 ผู้เสนอราคาต้องนำเสนอแผนในการติดตั้งอุปกรณ์ แผนการทำงาน โดยแสดงระยะเวลาในการดำเนินงาน

3.2.5 ผู้เสนอราคาต้องวางแผนติดตั้งอุปกรณ์ให้เสร็จภายใน วันอาทิตย์ พร้อมทั้งมีบุคลากรคอยสนับสนุน ในวันจันทร์ หลังจากเปลี่ยนแปลงระบบ

3.2.6 ผู้เสนอราคาต้องจัดเตรียม 10GE SFP+ transceiver module ที่รองรับกับอุปกรณ์รักษาความปลอดภัยเครือข่ายที่เสนอให้พร้อมสำหรับการติดตั้ง อย่างน้อย 4 ตัว

3.2.7 ในกรณีที่เกิดปัญหาร้ายแรง บริษัทที่เสนอราคาและได้รับการคัดเลือกต้องสามารถเข้าสนับสนุนที่ไซต์ Datacenter ของบริษัท เฮงลิสซิ่ง แอนด์ แคปปิตอล จำกัด (มหาชน) ภายใน 4 ชั่วโมง และต้องตอบสนองต่อการแจ้งบริการภายใน 2 ชั่วโมง ตลอดสัญญาการบริการ

3.2.8 ผู้เสนอราคาต้องมีประสบการณ์ให้บริการติดตั้งและคอนฟิกระบบไฟร์วอลล์ (firewall) ให้กับบริษัท เฮงลิสซิ่ง แอนด์ แคปปิตอล จำกัด (มหาชน) มาก่อน หรือ เคยติดตั้ง คอนฟิกมีประสบการณ์ ให้บริการระบบไฟร์วอลล์ (firewall) องค์กรเอกชนอื่นๆ โดยแนบคู่สัญญาหรือใบสั่งซื้ออุปกรณ์ Firewall และบริการมาประกอบการพิจารณา

4. ระยะเวลาดำเนินการและการส่งมอบ

ระยะเวลาดำเนินการ พฤษภาคม 2566 – มิถุนายน 2566

5. ข้อมูลการยื่นเสนอราคา

5.1 คุณสมบัติของผู้เสนอราคา

5.2 รายละเอียดข้อเสนอ ตามขอบเขตของงานและการบริการ

5.3 เงื่อนไขการจ่ายเงิน ระยะเวลาเครดิต

5.4 ค่าใช้จ่ายหรือส่วนลด และรายละเอียดอื่นที่เป็นประโยชน์ต่อการพิจารณา

6. หลักเกณฑ์ในการพิจารณา

บริษัท ฯ ให้คะแนนตามวิธีการและดุลยพินิจของบริษัท ฯ และตามหลักเกณฑ์การคัดเลือกที่กำหนด โดยไม่พิจารณาจากราคาต่ำสุด

อนุมัติโดย

.....

นายสุพจน์ ภู่ทอง

ผู้ช่วยกรรมการผู้จัดการใหญ่ฝ่ายเทคโนโลยีสารสนเทศ