ขอบเขตของงาน (Terms of Reference: TOR)

จัดซื้ออุปกรณ์ SSL VPN ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี ๒ ชุด

๑. ความเป็นมา

สำนักคอมพิวเตอร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช ได้ให้บริการแก่ผู้ใช้งาน (User) ในการเข้าใช้ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของมหาวิทยาลัยจากภายนอก เช่น ระบบบริการสารสนเทศ มสธ. (e-Service) ระบบการลาอิเล็กทรอนิกส์ ระบบสารบรรณอิเล็กทรอนิกส์ (e-document) และฐานข้อมูลออนไลน์ของห้องสมุด โดยระบบสารสนเทศดังกล่าวข้างต้น ต้องใช้งานผ่านระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเท่านั้น ไม่สามารถใช้งานจากเครือข่ายภายนอกได้ ในปัจจุบันอุปกรณ์ SSL VPN ที่ทำหน้าที่ให้บริการแก่ผู้ใช้งานจากภายนอกเครือข่ายนั้นได้ใช้งานมาเป็นระยะเวลา ๘ ปี บริษัทผู้ผลิตได้ประกาศยุติการให้บริการทางเทคนิคและการรับประกันแล้ว ดังนั้นมหาวิทยาลัยจึงจำเป็นต้องจัดซื้ออุปกรณ์ SSL VPN ทดแทนของเดิมที่หมดอายุการใช้งาน และรองรับความต้องการใช้งานระบบคลังข้อสอบออนไลน์ของมหาวิทยาลัยให้มีความมั่นคงปลอดภัยทางไซเบอร์อย่างมีประสิทธิภาพ

๒. วัตถุประสงค์

๒.๑ เพื่อทดแทนอุปกรณ์ SSL VPN ที่หมดอายุการใช้งาน รหัสครุภัณฑ์ มสธ.๐๙-๐๐๖-๑๓๕/๖๐-๐๐๐๑ ซึ่งไม่สามารถจัดซื้อการรับประกันอุปกรณ์ และไม่สามารถ Update firmware ต่อได้ เนื่องจากใช้งานมาเป็นระยะเวลา ๘ ปี

๒.๒ เพื่อเพิ่มประสิทธิภาพในการให้บริการระบบสารสนเทศของมหาวิทยาลัยแก่นักศึกษาและบุคลากรจากเครือข่ายภายนอกให้สามารถเข้ามาใช้งานระบบอินทราเน็ตของมหาวิทยาลัย

๒.๓ เพื่อรองรับการใช้งานของระบบคลังข้อสอบออนไลน์ของมหาวิทยาลัย

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

๓.๑ คุณสมบัติของผู้ยื่นข้อเสนอเป็นไปตามคณะกรรมการนโยบายฯ กำหนด (รายละเอียดระบุในเอกสารประกาศประกวดราคา/หนังสือเชิญชวน)

๓.๒ ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทยอย่างถูกต้องตามกฎหมาย โดยให้ยื่นขณะเสนอราคา

๔. รายการคอมพิวเตอร์ที่ซื้อขาย

จัดซื้ออุปกรณ์ SSL VPN ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี ๒ ชุด

๕. คุณลักษณะเฉพาะของครุภัณฑ์

อุปกรณ์ SSL VPN ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี ๒ ชุด ในแต่ละชุดประกอบไปด้วยอุปกรณ์ดังนี้

๕.๑ อุปกรณ์ SSL VPN มีคุณลักษณะเฉพาะดังนี้

๕.๑.๑ เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อใช้เป็น SSL VPN โดยเฉพาะ

๕.๑.๒ มีค่า VPN Throughput ไม่น้อยกว่า 20 Gbps และสามารถรองรับผู้ใช้งาน VPN แบบ Remote Access ได้ไม่น้อยกว่า 20,000 Concurrent Connections

๕.๑.๓ มี Next Generation Firewall Throughput ไม่น้อยกว่า 15 Gbps และค่า Firewall Throughput ไม่น้อยกว่า 55 Gbps

๕.๑.๔ มีค่า Threat Prevention Throughput ไม่น้อยกว่า 6.5 Gbps

๕.๑.๕ มีค่า IPS throughput ไม่น้อยกว่า 25 Gbps

๕.๑.๖ สามารถรองรับ Concurrent Connections ได้ถึง 16,000,000 Connections และสามารถสร้าง New Connection ได้ถึง 190,000 Connections ต่อวินาที

๕.๑.๗ มีพอร์ตสำหรับเชื่อมต่อระบบเครือข่าย (Network Interface) ดังนี้

๑) พอร์ตแบบ RJ45 ใช้งานที่ความเร็ว 1 Gbps จำนวนไม่น้อยกว่า 8 พอร์ต

๒) พอร์ตแบบ 1/10GbE SFP+ จำนวนไม่น้อยกว่า 8 พอร์ต

๕.๑.๘ มี Transceiver ใช้งานกับพอร์ตสำหรับเชื่อมต่อระบบเครือข่ายแบบ 10Gbase-SR จำนวน 2 โมดูลและ 10Gbase-LR จำนวน 2 โมดูล โดย Transceiver ต้องเป็นผลิตภัณฑ์ยี่ห้อเดียวกันกับอุปกรณ์ที่นำเสนอ

๕.๑.๙ มี Storage แบบ SSD ขนาดไม่น้อยกว่า 480 GB

๕.๑.๑๐ สามารถตรวจสอบและควบคุม Applications ได้อย่างน้อย 10,000 Applications

๕.๑.๑๑ สามารถแจ้งเตือนและสอบถามผู้ใช้งานได้ในแบบ Real-Time เพื่อให้ข้อมูลและสอบถามผู้ใช้งาน Applications และ URLs ในแต่ละ Filtering rule กรณีเข้าใช้งาน Web Site ที่อันตรายหรือไม่ได้รับอนุญาต โดยให้ผู้ใช้งานยืนยันการเข้าใช้งานและเป็นผู้รับความเสี่ยงเอง

๕.๑.๑๒ มี Secure Web Browser สำหรับใช้ในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ภายในของมหาวิทยาลัยได้อย่างปลอดภัย โดยสามารถรองรับการใช้งานได้ถึง 100 users มีคุณสมบัติดังนี้

๑) สามารถทำการบันทึก Session ระหว่างการใช้งานได้

๒) สามารถตรวจเช็คเครื่องคอมพิวเตอร์ เช่น มีการติดตั้ง Anti-Virus หรือ Anti-Malware หรือ xDR หรือมีการทำ Disk Encryption อย่างใดอย่างหนึ่งไว้แล้วก่อนมีสิทธิ์ให้เข้าใช้งาน Secure Web Browser

๓) สามารถป้องกันข้อมูลรั่วไหลด้วยการควบคุมการใช้งาน ดังนี้

๓.๑) ป้องกันไม่ให้ทำการ Copy, Paste และ Print ข้อมูลได้

๓.๒) ป้องกันไม่ให้เข้าดู Source Code ได้

๓.๓) มี Watermark แสดงบนเนื้อหา

๓.๔) สามารถทำ PII Masking เพื่อไม่ให้แสดงข้อมูลทั้งหมดได้

๓.๕) ป้องกันไม่ให้ทำการ Screen Capture ได้

๓.๖) ควบคุมไฟล์ที่อนุญาตให้ Upload ได้

๓.๗) สามารถจำกัดจำนวนตัวอักษรที่ให้ใช้พิมพ์ถามใน Generative AI ได้

๕.๑.๑๓ มีโปรแกรม VPN Client สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ใช้ระบบปฏิบัติการ Windows และ MacOS

๕.๑.๑๔ มี VPN Client แอปพลิเคชันสำหรับติดตั้งบนอุปกรณ์พกพา ที่ใช้ระบบปฏิบัติการ iOS และ Android

๕.๑.๑๕ สามารถกำหนด Security Policy ตาม User, User Group และ Machine ด้วยการ Integrate เข้ากับ Active Directory โดยไม่ต้องติดตั้งซอฟท์แวร์ (Agent) เพิ่มเติมบน Domain Controller และเครื่องคอมพิวเตอร์ของผู้ใช้งาน

๕.๑.๑๖ สามารถแสดงสถิติการใช้งาน (Hit Count Statistic) ของแต่ละ Policy ทั้ง Access Control Rule และ NAT Rule ได้

๕.๑.๑๗ สามารถใช้งาน Routing แบบ Dynamic Routing ได้แก่ OSPFv2 และ OSPFv3 , BGP, RIP, IGMP และ PIM ได้เป็นอย่างน้อย

๕.๑.๑๘ สามารถป้องกันภัยคุกคามดังต่อไปนี้ได้

๑) Known Exploit

๒) Protocol Misuse

๓) Tunneling Attempt

๔) Vulnerability

๕) Outbound Malware Communication

๕.๑.๑๙ สามารถตรวจจับ Virus โดยป้องกันการดาวน์โหลดไฟล์ที่มีมัลแวร์ และตรวจสอบไฟล์ที่มีการย่อขนาด เช่น zip,gzip,gz,7z,rar และ tar เป็นอย่างน้อย รวมทั้งสามารถ Scan Virus ตาม Link ที่แนบมาในจดหมายอิเล็กทรอนิกส์ได้

๕.๑.๒๐ สามารถตรวจจับ Bot ได้ด้วยวิธีการตรวจสอบจาก C&C address หรือ Website หรือ Communication Pattern ของ Bot และ Bot Behavior ได้เป็นอย่างน้อย

๕.๑.๒๑ สามารถป้องกันการโจมตีผ่านโปรโตคอล DNS ในรูปแบบ DGA (Domain Generation Algorithm) และ DNS Tunneling โดยการใช้ Machine Learning ในการตรวจสอบ

๕.๑.๒๒ สามารถป้องกัน Spam Mail ผ่านโปรโตคอล POP3 และ SMTP และสามารถป้องกันโดยใช้รูปแบบ IP Reputation Anti-spam, Content-based Anti-spam และ Block/allow list anti-spam ได้

๕.๑.๒๓ สามารถทำ URL Filtering เพื่อเพิ่มความปลอดภัยในการใช้งาน Web site โดยมีการจัดประเภทของ Content ได้ทั้งแบบ Pre-defined category และ Custom category ได้ และสามารถ Update ฐานข้อมูลได้อย่างสม่ำเสมอ

๕.๑.๒๔ สามารถทำงานแบบ High Availability ได้ทั้งแบบ Active/Active และ Active/Passive โดยสามารถทำ Session Failover ในกรณีเกิด Device Failure และ Link Failure ได้

๕.๑.๒๕ สามารถป้องกันการโจมตีในรูปแบบ Phishing ผ่านการใช้งาน Web หรือ URL ทั้งแบบ Zero-day และ Known phishing แบบ Real time และสามารถป้องกันการโจมตีด้วย Artificial Intelligence (AI) ได้

๕.๑.๒๖ สามารถป้องกันภัยคุกคามแบบ Zero-day โดยการส่งไฟล์ต้องสงสัยไปตรวจสอบที่ Sandbox บน Cloud ได้

๕.๑.๒๗ สามารถตรวจสอบการโจมตีทั้งในระดับ CPU Level และ OS Level

๕.๑.๒๘ สามารถป้องกันการดาวน์โหลดไฟล์จนกว่าอุปกรณ์จะทำการตรวจสอบไฟล์สำเร็จ เพื่อป้องกัน Malware ที่ยังไม่ผ่านการตรวจสอบเข้าไปยังระบบเครือข่ายของมหาวิทยาลัย

๕.๑.๒๙ สามารถแยก Active content และ Embedded object บนไฟล์ออก และทำการสร้างไฟล์ใหม่เป็นรูปแบบ PDF เพื่อส่งไฟล์ที่ปลอดภัยให้แก่ผู้ใช้งานในขณะที่ระบบทำการตรวจสอบไฟล์จริง

๕.๑.๓๐ มีแหล่งจ่ายไฟจำนวนไม่น้อยกว่า 2 หน่วย และมีพัดลมระบายอากาศจำนวนไม่น้อยกว่า 2 หน่วย

๕.๑.๓๑ ผ่านการรับรองมาตรฐานทางด้านความปลอดภัยของ UL หรือ EN

๕.๑.๓๒ ผ่านการรับรองมาตรฐานการแผ่กระจายคลื่นแม่เหล็กไฟฟ้าของ FCC หรือ EN

๕.๑.๓๓ ผลิตภัณฑ์ยี่ห้อที่นำเสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ประเภท Hybrid Mesh Firewall ปี 2025 หรือปีล่าสุดเป็นอย่างน้อย

๕.๒ อุปกรณ์สำหรับบริหารจัดการ (Management Devices) มีคุณลักษณะเฉพาะดังนี้

๕.๒.๑ เป็นอุปกรณ์ที่มีระบบปฏิบัติการแบบเฉพาะผ่านการทำ Hardening เรียบร้อยแล้ว

๕.๒.๒ สามารถบริหารจัดการอุปกรณ์ SSL VPN ผ่าน Application GUI ได้

๕.๒.๓ สามารถจัดการ Policy และจัดเก็บข้อมูล Log ได้

๕.๒.๔ สามารถวิเคราะห์เหตุการณ์ที่เกิดขึ้นบนอุปกรณ์และจัดทำรายงานได้

๕.๒.๕ มีพอร์ตสำหรับเชื่อมต่อระบบเครือข่าย (Network Interface) ดังนี้

๑) พอร์ตแบบ RJ45 ใช้งานที่ความเร็ว 1 Gbps จำนวนไม่น้อยกว่า 1 พอร์ต

๒) พอร์ตแบบ 1/10GbE SFP+ จำนวนไม่น้อยกว่า 4 พอร์ต

๕.๒.๖ มี Transceiver ใช้งานกับพอร์ตสำหรับเชื่อมต่อระบบเครือข่ายแบบ 1G Base-T RJ45 จำนวน 2 โมดูล โดย Transceiver ต้องเป็นผลิตภัณฑ์ยี่ห้อเดียวกันกับอุปกรณ์ที่นำเสนอ

๕.๒.๗ สามารถแบ่งกลุ่มของ Security Policy เป็น Section Title เพื่อใช้ในการบริหารจัดการ Security Policy จำนวนมากได้ และสามารถสร้าง Policy โดยแบ่งชั้นแบบ Inline layer หรือ Sub-rule ได้

๕.๒.๘ สามารถตรวจสอบ Security Policy แบบ Heuristic Verification หรือแบบอื่นที่ป้องกันการกำหนด Security Policy ที่ซ้ำซ้อนทำให้ระบบไม่ปลอดภัย

๕.๒.๙ สามารถจัดการ Security policy ต่างๆ และจัดเก็บ Log ได้ทั้งแบบ Real Time และสามารถส่ง Syslog ไปยัง Syslog Server ของมหาวิทยาลัยเพื่อตรวจสอบย้อนหลังตามกฎหมายได้

๕.๒.๑๐ สามารถให้ผู้ดูแลระบบ (Administrator) เข้าใช้งานได้พร้อมกันหลายคน โดยแยกการทำงานกันไม่ให้เกิดการขัดแย้งของ Policy ได้

๕.๒.๑๑ สามารถกำหนดสิทธิ์ของผู้ดูแลระบบในระดับที่แตกต่างกันและสิทธิ์ที่ต่างกันได้ (User Role) โดยทำการกำหนดผู้ดูแลระบบใช้งานและทำการ Authentication ผ่านทาง Active Directory (On-premise or Microsoft Entra ID) แบบตรวจสอบและยืนยันตัวตนหลายขั้นตอนการพิสูจน์ตัวจริงด้วยปัจจัยหลายอย่าง (Multi-Factor Authentication : MFA)

๕.๒.๑๒ สามารถกำหนด Threat Prevention Profiles สำหรับป้องกันการโจมตีแบบอัตโนมัติ (Autonomous) ได้ โดยมี Profile ให้เลือกได้แก่ Recommended และ Strict Profile สำหรับ Perimeter, Data Center East/West, Internal network และ Guest network ได้เป็นอย่างน้อยหรือมีกระบวนการที่เทียบเท่า

๕.๒.๑๓ สามารถหาความสัมพันธ์ (Correlation) ของ Log ต่างๆ ที่จัดเก็บ พร้อมทั้งแสดงข้อมูลเป็นเหตุการณ์ (Event) ต่างๆ และแนวโน้มของเหตุการณ์ในลักษณะของ Timelines, Charts และ Maps ได้

๕.๒.๑๔ สามารถทำการกำหนด Exception ในหมวดของ IPS Protection ได้โดยตรงจาก Log หรือ Event ทันที

๕.๒.๑๕ สามารถใช้งานแบบ Indexed Search Logging ได้ โดยค้นหา Log ได้แบบ Google-Like Search และสามารถแสดง Log ที่เกิดจาก Feature Firewall, IPS, URL Filtering, Anti-Virus และ Anti-Bot บนหน้าจอ Console เดียวกันแบบ Single Unified Log View ได้

๕.๒.๑๖ สามารถจัดทำรายงานแบบ Predefined Report ได้แก่รายงานประเภท Threat Prevention Report, Application and URL Filtering Report และ User Activity Report ได้เป็นอย่างน้อย รวมทั้งสามารถปรับแต่ง (Customize) รายงานเพิ่มเติมได้

๕.๒.๑๗ สามารถกำหนดช่วงเวลาที่ต้องการให้สร้างและแสดงผลรายงานได้ (Scheduled Report) และกำหนดให้ส่งรายงานผ่านทาง Email ได้เป็นอย่างน้อย

๕.๒.๑๘ มีกระบวนการในการขออนุมัติการแก้ไขเปลี่ยนแปลง Policy Firewall และกำหนดสิทธิ์แยกผู้ดูแลระบบให้เป็นผู้ขอและผู้อนุมัติ โดยระบบสามารถส่งอีเมลเพื่อแจ้งขอการอนุมัติพร้อมรายละเอียดการแก้ไขเปลี่ยนแปลง Policy ในรูปแบบรายงาน (Review Change Report) โดยอัตโนมัติได้เป็นอย่างน้อย

๕.๒.๑๙ สามารถตรวจสอบค่า Configuration แบบ Real Time Compliance Monitoring ของอุปกรณ์ SSL VPN ได้ ตามมาตรฐานสากลต่างๆ ได้แก่ CIS Benchmarks , NIST 800-53, NIST 800-41 และ ISO 27002 เป็นอย่างน้อย

๕.๒.๒๐ สามารถตรวจสอบ วิเคราะห์สถานะ และมี Artificial Intelligence (AI) ช่วยในการวิเคราะห์เพื่อคาดเดาปัญหาที่อาจจะเกิดขึ้นก่อนที่จะส่งผลกระทบในการทำงาน หรือเกิดการหยุดทำงานของอุปกรณ์ที่นำเสนอแบบ Real-time เช่น CPU, Memory พร้อมทั้งแนะนำการแก้ไขปัญหา หรือเสนอระบบอื่นเพิ่มเติมได้ในการตรวจสอบ Network Performance Monitoring

๕.๒.๒๑ มี AI Copilot หรือ Generative AI อื่น ที่สามารถเรียนรู้และเข้าใจนโยบายขององค์กร เช่น Access rules, Objects, logs และ Product Documentation ช่วยให้คำตอบกับผู้ดูแลระบบ (Administrator) ได้

๕.๒.๒๒ สามารถตรวจสอบการกำหนด Policy บนอุปกรณ์แบบ Segment-to-Segment หรือ Zone-to-Zone ในลักษณะตารางแบบ NxN โดยสามารถระบุ Policy ที่ไม่สอดคล้องหรือขัดแย้งกันได้ เช่น การอนุญาต (Permit) ให้เข้าถึง Zone ที่ห้ามเข้าถึงได้ หรือเสนออุปกรณ์อื่นเพิ่มเติมได้

๕.๒.๒๓ สามารถทำ Firewall Policy Optimize หรือเสนออุปกรณ์อื่นเพิ่มเติมได้ โดยมีความสามารถในการทำงานดังนี้

๑) สามารถแนะนำการเข้าถึงจาก Source IP, Destination IP และ Port ที่อนุญาตมากเกินความจำเป็น

๒) สามารถตรวจสอบ Policy ที่ซ้ำซ้อนกันหรือขัดแย้งกันได้

๓) สามารถวิเคราะห์ Policy และให้คำแนะนำสำหรับการทำ Policy Cleanup

๔) สามารถแจ้งเตือน Unmatch Rules หรือ Objects พร้อมแนะนำการปรับปรุงได้

๕.๒.๒๔ สามารถทำการ Sync Time กับ NTP Server ของมหาวิทยาลัยได้

๖. รายละเอียดการติดตั้ง

ผู้ขายต้องดำเนินการติดตั้งอุปกรณ์ SSL VPN โดยมีรายละเอียดดังต่อไปนี้

๖.๑ ผู้ขายต้องส่งมอบแผนการดำเนินงานในโครงการจัดซื้อ พร้อมรายชื่อผู้ประสานงานและทีมงาน โดยส่งสำเนาบัตรประชาชนทุกคนที่เข้าปฏิบัติงาน ให้กับทางมหาวิทยาลัยพิจารณาก่อนการเข้าปฏิบัติงาน ภายใน ๗ วัน นับถัดจากวันที่ลงนามในสัญญา

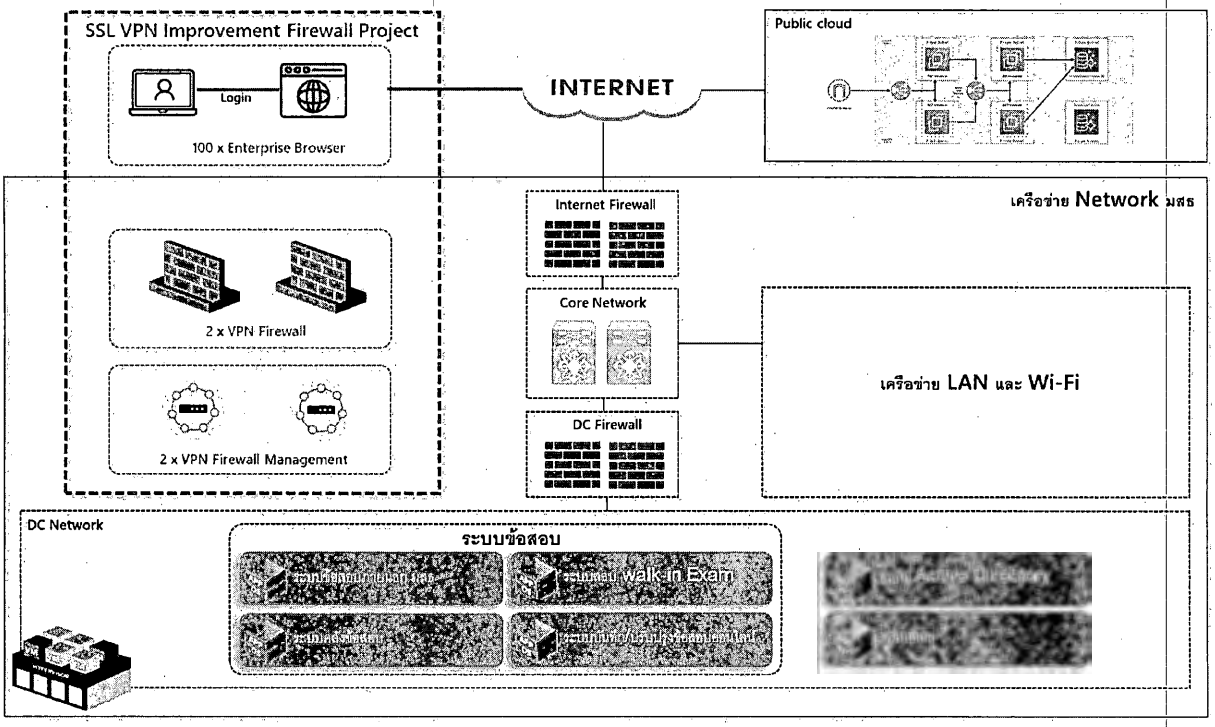
๖.๒ ส่งมอบและติดตั้งอุปกรณ์ SSL VPN ณ ห้องศูนย์กลางเครือข่ายคอมพิวเตอร์หลัก อาคารศูนย์ฝึกอบรมเทคโนโลยีการพิมพ์แห่งชาติ ชั้น ๒ จำนวน ๑ ชุด

๖.๓ ส่งมอบและติดตั้งอุปกรณ์ SSL VPN ณ ห้องศูนย์กลางเครือข่ายคอมพิวเตอร์หลัก อาคารวิชาการ ๑ ชั้น ๒ จำนวน ๑ ชุด

๖.๔ ผู้ขายต้องจัดเตรียมอุปกรณ์ที่ต้องใช้ในการติดตั้งให้ครบถ้วน สามารถติดตั้งให้มหาวิทยาลัยใช้งานได้ตามที่กำหนดไว้ในรายการคุณลักษณะเฉพาะของครุภัณฑ์

๖.๕ ทำการเชื่อมต่ออุปกรณ์ SSL VPN เข้ากับระบบเครือข่ายคอมพิวเตอร์ตามที่มหาวิทยาลัยกำหนด โดยผู้ขายเป็นผู้จัดเตรียมและติดตั้ง Transceiver ที่ต้องใช้ในการเชื่อมต่อเครือข่ายบนอุปกรณ์ Core Switch ของมหาวิทยาลัย

๖.๖ ผู้ขายต้องทำการ Set up Configuration ตามภาพ



๗. การยื่นเอกสารที่ต้องยื่นเพื่อประกอบการพิจารณาคุณลักษณะเฉพาะ

ผู้ยื่นข้อเสนอต้องยื่นเอกสารเพื่อให้มหาวิทยาลัยพิจารณา ณ วันยื่นข้อเสนอ โดยมีรายละเอียดดังต่อไปนี้

๗.๑ ผู้เสนอราคาต้องทำการจัดทำเอกสารเพื่อเสนอต่อมหาวิทยาลัย เช่น Datasheet หรือเอกสารที่พิมพ์จาก Web Site ของผลิตภัณฑ์ที่เสนอราคา หรือเอกสารประกอบอื่น ๆ ที่แสดงให้เห็นข้อมูลที่ชัดเจนสำหรับประกอบการพิจารณา

๗.๒ผู้เสนอราคาต้องทำการเปรียบเทียบรายการที่เสนอทุกข้อกำหนด ดังรายละเอียดในตารางที่ ๑ **โดยข้อกำหนดของมหาวิทยาลัยทุกข้อ ถือเป็นเกณฑ์ขั้นต่ำสุดที่ผู้เสนอราคาต้องปฏิบัติ และมหาวิทยาลัยถือเป็นสาระสำคัญในการพิจารณา**

ตารางที่ ๑ ตัวอย่างการเปรียบเทียบคุณลักษณะเฉพาะ

ข้อกำหนดของมหาวิทยาลัย	ข้อเสนอของบริษัท	หน้าที่อ้างอิง
	ยี่ห้อ : สินค้า รุ่น : ทดสอบ	
๑. มีค่า IPS throughput ที่ 25 Gbps	ตรงตามข้อกำหนด	หน้าที่ ๕๕ จาก ๙๙
๒. มี Storage แบบ SSD ขนาด 480 GB	ตรงตามข้อกำหนด	หน้าที่ ๕๖ จาก ๙๙

๗.๓ ในกรณีที่อ้างอิงตาม Datasheet หรือเอกสารที่พิมพ์จาก Web Site ของผลิตภัณฑ์ที่เสนอราคา หรือเอกสารประกอบอื่น ๆ ผู้เสนอราคาต้องนำข้อมูลล่าสุด (Update) โดยต้องมีที่มาและรายละเอียดจากสำนักงานใหญ่หรือสำนักงานประจำประเทศไทยของบริษัทผู้ผลิต และต้องแสดงให้ชัดเจนเพื่อประกอบการพิจารณา การ

เสนอรายละเอียดของผลิตภัณฑ์ต้องทำการอ้างอิง **และต้องระบุหัวข้อพร้อมขีดเส้นใต้ หรือทำแถบสีข้อความลงในเอกสารต่าง ๆ ที่นำมาแสดงให้เห็นอย่างชัดเจน และระบุข้อกำหนดให้ครบถ้วน**

๗.๔ ในกรณีที่ต้องมีการรับรองคุณลักษณะเฉพาะทางเทคนิคหรือรายละเอียดต่าง ๆ ที่เกี่ยวข้องกับผลิตภัณฑ์ที่เสนอขาย เพื่อประกอบการพิจารณาหรือการตรวจรับ ต้องรับรองโดยสำนักงานใหญ่หรือสำนักงานประจำประเทศไทยของบริษัทผู้ผลิตเท่านั้น

๗.๕ ในกรณีการเสนอรายละเอียดของผลิตภัณฑ์ต่าง ๆ มหาวิทยาลัยจะพิจารณารายละเอียดต่าง ๆ ณ วันที่เสนอราคา

๗.๖ ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทยอย่างถูกต้องตามกฎหมาย โดยให้ยื่นขณะเสนอราคา

๘. การอบรมคอมพิวเตอร์และคู่มือ

๘.๑ ผู้ขายต้องดำเนินการเสนอหัวข้อในการจัดอบรมวิธีการใช้งาน และการดูแลบำรุงรักษาอุปกรณ์ SSL VPN ให้มหาวิทยาลัยพิจารณา และกำหนดวันอบรมตามที่มหาวิทยาลัยกำหนดโดยจะแจ้งให้ผู้ขายทราบในภายหลัง

๘.๒ ผู้ขายต้องจัดอบรมให้กับเจ้าหน้าที่ของมหาวิทยาลัยในระดับผู้ดูแลระบบ จำนวนไม่น้อยกว่า ๕ คน โดยต้องทำการอบรมการใช้งานไม่น้อยกว่า ๑๒ ชั่วโมง

๘.๓ ผู้ขายต้องจัดทำคู่มือในการอบรมในระดับผู้ดูแลระบบ จำนวนไม่น้อยกว่า ๕ ชุด สำหรับใช้ในการทำงานและการดูแลบำรุงรักษาอุปกรณ์ SSL VPN

๘.๔ ผู้ขายต้องจัดอบรมให้กับเจ้าหน้าที่ของมหาวิทยาลัยในระดับผู้ใช้งาน (User) โดยต้องทำการอบรมการใช้งานไม่น้อยกว่า ๖ ชั่วโมง พร้อมจัดทำคู่มือในระดับผู้ใช้งานในรูปแบบเอกสารอิเล็กทรอนิกส์

๘.๕ ผู้ขายต้องจัดทำคู่มือการติดตั้ง (Install and Configuration) ที่จัดซื้อในครั้งนี้ในรูปแบบฮาร์ดดิสก์แบบพกพาสำหรับเก็บข้อมูล (SSD)

๙. การทดสอบประสิทธิภาพการทำงานของระบบที่นำเสนอ

ผู้ขายต้องดำเนินการทดสอบการทำงานของอุปกรณ์ SSL VPN ตามรายละเอียดที่กำหนดในคุณลักษณะเฉพาะของครุภัณฑ์

๑๐.การรับประกันความชำรุดบกพร่องและบริการหลังการขาย

ผู้ขายต้องรับประกันสินค้าและบริการให้คำปรึกษาทางด้านเทคนิค เป็นระยะเวลา ๑ ปี นับถัดจากวันที่มหาวิทยาลัยได้ตรวจรับครุภัณฑ์เรียบร้อยแล้ว โดยผู้ขายต้องจัดการซ่อมแซมแก้ไขให้สามารถใช้งานได้ ภายใน ๑ วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

๑๑.ระยะเวลาส่งมอบ

ผู้ขายต้องส่งมอบงานภายในระยะเวลา ๙๐ วัน นับถัดจากวันลงนามในสัญญา

๑๒.วงเงินในการจัดหา

๓,๐๐๐,๐๐๐ บาท (สามล้านบาทถ้วน)

๑๓.งวดงานและการจ่ายเงิน

มหาวิทยาลัยจะจ่ายเงินเมื่อผู้ขายส่งมอบอุปกรณ์ SSL VPN เรียบร้อยแล้ว และมหาวิทยาลัยได้ตรวจรับเป็นที่เรียบร้อย

๑๔.หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

โดยใช้เกณฑ์ราคา

๑๕.อัตราค่าปรับ

กำหนดค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของมูลค่าโครงการทั้งหมด

การติดต่อสอบถามรายละเอียด

หากต้องการเสนอแนะ วิจารณ์ หรือมีความเห็นเกี่ยวกับรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จัดหา กรุณาให้ความเห็นเป็นลายลักษณ์อักษรมาที่ กองพัสดุ มหาวิทยาลัยสุโขทัยธรรมาธิราช ภายในระยะเวลาที่กำหนดก่อนการประกาศประกวดราคาอิเล็กทรอนิกส์

๑. กรณีส่งเป็นหนังสือ โปรดส่งโดยระบุที่อยู่ ดังนี้

กองพัสดุ สำนักงานอธิการบดี มหาวิทยาลัยสุโขทัยธรรมาธิราช

เลขที่ ๙/๙ หมู่ ๙ ถนนแจ้งวัฒนะ ตำบลบางพูด อำเภอปากเกร็ด

จังหวัดนนทบุรี ๑๑๑๒๐

๒. กรณีส่งเป็นโทรสาร โปรดส่งที่หมายเลข ๐-๒๕๐๓-๒๕๙๘

๓. กรณีส่งเป็น E-mail โปรดส่งที่ E-mail Address : pm.proffice@stou.ac.th