รายละเอียดคุณลักษณะเฉพาะ

จัดซื้ออุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) และ อุปกรณ์กระจายสัญญาณความเร็วสูง (Distribute Switch) สำหรับศูนย์ข้อมูล (Data Center)

1. ความเป็นมา

เพื่อทดแทนอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) และ อุปกรณ์กระจายสัญญาณหลักที่มีอายุการใช้งานเกิน 6 ปี และ เพิ่มความสามารถป้องกันและลดความเสี่ยงจากภัยคุกคามด้านไซเบอร์ เช่น ข้อมูลรั่วไหล ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 (มาตรา 45) โดยจะสามารถสร้างการเชื่อมต่อที่ปลอดภัยระหว่างสำนักงานใหญ่กับสำนักงานย่อย (Site-to-Site VPN) และ เพิ่มคุณสมบัติการยืนยันตัวตนโดยใช้หลายปัจจัย (MFA) ให้สอดคล้องตามประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2567

2. วัตถุประสงค์

เพื่อเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและระบบสารสนเทศที่สำคัญ โดยมีการจัดหาเพื่อทดแทน ดังต่อไปนี้

(1) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) หลัก จำนวน 1 เครื่อง

(2) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) สำหรับ Datacenter จำนวน 1 เครื่อง

(3) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) สำหรับสำนักงานย่อย 1 เครื่อง

(4) อุปกรณ์กระจายสัญญาณความเร็วสูง (Distribute Switch) สำหรับเชื่อมต่อกับอุปกรณ์กระจายสัญญาณหลัก (Core Switch) 2 เครื่อง

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการ ผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน หรือหนังสือเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

3.11 ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) ที่ 0405.2/ว124 ลงวันที่ 1 มีนาคม 2566

3.13 ผู้ยื่นข้อเสนอต้องมีผลงานจำหน่ายอุปกรณ์หรือระบบหรือซอฟต์แวร์ที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ จำนวน 1 - 2 ผลงาน วงเงินรวมกันไม่น้อยกว่า 1,800,000 บาท (หนึ่งล้านแปดแสนบาทถ้วน) ในระยะเวลาไม่เกิน 5 ปี จนถึงวันที่ยื่นข้อเสนอ และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงาน

เอกชนที่ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) เชื่อถือ โดยยื่นสำเนาหนังสือรับรองผลงานและสำเนาสัญญาหรือใบสั่งซื้อ ซึ่งเป็นงานเดียวกัน

3.14 ผู้ยื่นข้อเสนอต้องจัดทำรายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้างซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี)

3.15 ผู้ยื่นข้อเสนอต้องส่งมอบแผนการทำงานตลอดระยะเวลาตามสัญญา ภายใน 14 วัน นับถัดจากวันลงนามในสัญญา

หลักฐานการยื่นข้อเสนอ

(1) ผู้ยื่นข้อเสนอต้องได้รับแต่งตั้งให้เป็นตัวแทนจำหน่ายอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) รายการที่ 1-3 ตามข้อกำหนดทางเทคนิค จากเจ้าของผลิตภัณฑ์หรือตัวแทนจำหน่ายในประเทศไทยเพื่อแสดงถึงการสนับสนุนทางด้านเทคนิค เพื่อให้คำปรึกษาแนะนำการใช้งานในผลิตภัณฑ์ที่ได้นำเสนอ โดยจะต้องมีหนังสือรับรองตัวจริง มาประกอบการพิจารณา (นับถัดจากวันที่ยื่นข้อเสนอในระบบของกรมบัญชีกลาง)

(2) ผู้ยื่นข้อเสนอหรือผู้จัดจำหน่าย (Distributor) ต้องมีศูนย์ที่บริการที่ได้รับมาตรฐานบริการหลังการขายหรือมีกระบวนการ (Process) การให้บริการในภาพรวมตาม ISO 9001:2008 หรือ 2015 โดยศูนย์บริการดังกล่าวต้องมีบริการ Call Center ให้บริการหมายเลขโทรฟรี ตลอด 7 วัน 24 ชม.

(3) ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความความเชี่ยวชาญด้านการติดตั้งและบริหารจัดการเครือข่ายองค์กรตามผลิตภัณฑ์ที่ทาง สสวท. ใช้งานอยู่ในปัจจุบัน โดยต้องได้รับ Certificate ระดับ Cisco Certified Network Professional (CCNP) Routing and Switching

(4) ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความความเชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ (Cybersecurity) โดยต้องได้รับ Certificate เช่น CompTIA Security+ เทียบเท่าหรือดีกว่า

(5) ผู้ยื่นข้อเสนอต้องเสนอข้อมูลทางด้านเทคนิคของครุภัณฑ์ ที่เสนอ โดยจัดทำเอกสารเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะครุภัณฑ์ที่กำหนดข้างต้นทั้งหมด กับรายละเอียดที่ผู้ยื่นข้อเสนอเสนอ โดยระบุเอกสารอ้างอิง แคตตาล็อก ให้ถูกต้อง และในเอกสารอ้างอิง แคตตาล็อก ต้องขีดเส้นใต้ หรือใช้ปากกาเน้นข้อความระบุหมายเลขข้อที่อ้างอิงให้ชัดเจน ทั้งนี้จะต้องส่งมาพร้อมกับเอกสารแสดงคุณลักษณะ สสวท. ขอสงวนสิทธิ์ที่จะไม่พิจารณาผู้ยื่นข้อเสนอ หากไม่ปฏิบัติตามไม่ว่ากรณีใดๆ ทั้งสิ้นตามตัวอย่างด้านล่าง

ตัวอย่าง ตารางเปรียบเทียบ

รายละเอียดที่ สสวท. กำหนด	รายละเอียดที่ผู้ยื่นข้อเสนอ เสนอ	เอกสารอ้างอิง (ระบุเลขหน้า)
	* ต้องระบุเอกสารให้ชัดเจน ห้ามมี ไม่น้อยกว่า	

4. รายละเอียดคุณลักษณะเฉพาะ

<u>รายการที่ 1 อุปกรณ์ป้องกันเครือข่ายหลัก (Next Generation Firewall)</u>

เป็นอุปกรณ์รักษาความปลอดภัยเครือข่ายแบบ Appliance-Based Firewall ที่ออกแบบมาเพื่อทำหน้าที่ตรวจจับและควบคุมการใช้งาน Application, User และ Content ได้อย่างมีประสิทธิภาพ เพื่อเพิ่มความมั่นคงปลอดภัยของระบบเครือข่ายหลักขององค์กร จำนวน 1 ชุด อุปกรณ์ดังกล่าวต้องมีสมรรถนะสูงและรองรับการทำงานในสภาพแวดล้อมระดับองค์กร (Enterprise Environment) โดยมีคุณลักษณะ ดังนี้

1) มี Firewall Throughput ไม่น้อยกว่า 8.5 Gbps ภายใต้เงื่อนไขการทดสอบแบบ AppMix หรือ Enterprise Traffic Mix และ มี Threat Prevention Throughput ไม่น้อยกว่า 4.5 Gbps ภายใต้เงื่อนไขการทดสอบเดียวกัน
2) รองรับจำนวนการเชื่อมต่อพร้อมกัน (Maximum Concurrent Sessions) ได้ไม่น้อยกว่า 945,000 Sessions และ รองรับจำนวนการเชื่อมต่อใหม่ต่อวินาที (New Sessions per Second) ได้ไม่น้อยกว่า 100,000 Sessions/Second
3) มี Network Interface แบบ 10/100/1000 ไม่น้อยกว่า 8 พอร์ต, 1G/2.5G/5G POE ไม่น้อยกว่า 4 พอร์ต , 1G SFP ไม่น้อยกว่า 6 พอร์ต และ 1G/10G SFP/SFP+ ไม่น้อยกว่า 4 พอร์ต รวมทั้งมี Interface แบบ 100/1000 เพื่อใช้สำหรับบริหาร จัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า 1 พอร์ต โดยแยกออกจาก Network Interface ปกติ
4) อุปกรณ์ต้องมี Storage แบบ SSD สำหรับเก็บข้อมูลระบบไม่น้อยกว่า 120 GB
5) สามารถใช้กับระบบเครือข่ายแบบ VLAN ผ่าน Protocol 802.1Q ได้ไม่น้อยว่า 4,000 VLAN per interface
6) สามารถติดตั้งในรูปแบบ L2, L3, Tap และ Virtual Wire (Transparent Mode) ได้พร้อมกัน (Multiple Deployment) โดยไม่ต้องแบ่ง Virtual System
7) สามารถทำ Dynamic Routing Protocol ได้แก่ RIP, OSPF และ BGP ได้เป็นอย่างน้อย
8) สามารถป้องกันภัยคุกคามประเภท Vulnerability, Virus และ Spyware ได้โดยสามารถมีการอัพเดท Signature ใหม่ๆแบบอัตโนมัติ
9) สามารถป้องกัน Command and control traffic ที่ไม่รู้จักด้วยเทคโนโลยี Deep Learinging และ Machine Learning ได้.
10) สามารถกำหนดนโยบายการเข้าถึง website (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category และกำหนด Block list, Allow list รวมทั้งต้องมีการจัด Category ให้แต่ละ Website ไม่น้อยกว่า 2 Category และมีระบบ Machine Learning (ML) สำหรับวิเคราะห์ URL แบบ real time ได้

11) มีความสามารถในการป้องกันภัยคุกคามด้วยเทคโนโลยี Inline Machine Learnings (ML) หรือ Inline Artificial intelligence (AI) หรือ On-premise Learning

12) มีระบบตรวจจับ Advanced Malware แบบ Cloud-Based และใช้เทคโนโลยีแบบ Sandbox เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ และมี report พฤติกรรมการทำงานของ malware ดังกล่าวได้

13) สามารถตรวจจับ และป้องกันการเข้าถึง Malicious Domain ภายในองค์กรได้ โดยต้องมีความสามารถอย่างน้อยดังนี้
    - มีระบบในการตรวจหาเทคนิคอัลกอริทึม Domain generation algorithms (DGA) ได้
    - สามารถตรวจจับและป้องกัน DNS Tunneling ได้
    - ทำงานแบบ Real time และไม่มีข้อจำกัดรองรับปริมาณ Malicious Domain ที่เพิ่มขึ้นในอนาคต

14) มีความสามารถทำงานในลักษณะ SD-WAN เพื่อควบคุมเส้นทางของ Traffic จากคุณภาพของ Link เช่น Latency, Jitter, Package Loss ได้เป็นอย่างน้อย

15) สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้ โดยสามารถทำได้บนตัวอุปกรณ์ Firewall ไม่ต้องมีระบบใดๆเพิ่มเติม

16) สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย

17) สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ดาวน์โหลดและอัพโหลดบนแต่ละ Applications ได้ รวมทั้งสามารถป้องกันการ รั่วไหลของข้อมูล (Data Filtering) ออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต และสามารถสร้างรูปแบบได้ตามความ ต้องการ

18) สามารถทำ Security Policy Rule Optimization เพื่อปรับปรุง Policy จาก Port base เป็น Application base ได้ โดยสามารทำได้บนตัวอุปกรณ์ Firewall และไม่ต้องมีระบบใดๆเพิ่มเติม

19) อุปกรณ์ต้องสามารถทำงานร่วมกับ CrowdStrike Falcon Endpoint Protection เพื่อตรวจสอบความปลอดภัยร่วมกันได้

20) สามารถเรียกดูสรุปข้อมูลของ Data ในรูปแบบของกราฟฟิคได้ โดยสามารถ ปรับแต่งรายงานตามความต้องการ (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้ และสามารถทำรายงานต่าง ๆ อย่างน้อยดังนี้
    - Top Application, Application Category
    - Top Source, User, Destination
    - User activity report

21) สามารถบริหารจัดการผ่านทาง Web Interface แบบ HTTPS และ Command Line Interface ได้

22) มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ Redundant

23) สามารถจัดเก็บบันทึกข้อมูลโดยส่ง Syslog และ SNMP ไปยังระบบจัดการเครือข่ายที่รองรับคุณสมบัติดังกล่าวได้

24) สามารถรองรับการติดตั้งเพื่อทำ High Availability (HA) แบบ Active/Passive และ Active/Active ได้

25) ผู้เสนอราคาจะต้องเสนอ อุปกรณ์เชื่อมต่อเครือข่ายระยะไกล (VPN Appliance) เพื่อให้ผู้ใช้งานสามารถเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในของสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จากภายนอกได้อย่างปลอดภัย โดยมีคุณลักษณะขั้นต่ำดังต่อไปนี้

25.1 เป็นอุปกรณ์ VPN แบบ Appliance ที่มีคุณสมบัติในการตรวจสอบ ควบคุม และบริหารจัดการการเชื่อมต่อของ VPN Client โดยเฉพาะ และต้องเป็น ยี่ห้อเดียวกันกับอุปกรณ์ Next Generation Firewall (NGFW) เพื่อให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ จำนวน 1 ระบบ

25.2 มีสมรรถนะดังต่อไปนี้

- Firewall Throughput ไม่น้อยกว่า 1.8 Gbps
- Threat Prevention Throughput ไม่น้อยกว่า 1.2 Gbps
- รองรับการเชื่อมต่อพร้อมกันสูงสุด (Max Concurrent Sessions) ไม่น้อยกว่า 98,000 Sessions
- รองรับการเชื่อมต่อใหม่ต่อวินาที (New Sessions per Second) ไม่น้อยกว่า 15,000 Sessions/Second

25.3 มี Network Interface ความเร็ว 10/100/1000 Mbps จำนวนไม่น้อยกว่า 8 พอร์ต และ Management Port แยกเฉพาะ อย่างน้อย 1 พอร์ต

25.4 อุปกรณ์ต้องสามารถให้บริการ Client VPN (Remote Access VPN) รองรับการเชื่อมต่อพร้อมกันได้ไม่น้อยกว่า 250 ผู้ใช้งาน (Concurrent Users) และต้องสามารถใช้งานร่วมกับระบบปฏิบัติการอย่างน้อยดังนี้ Windows (ทั้ง 32-bit และ 64-bit), macOS, Android, Apple iOS

<u>รายการที่ 2 อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) สำหรับ DataCenter</u>

เป็นอุปกรณ์ Appliance ที่ออกแบบขึ้นมาเฉพาะ เพื่อทำหน้าที่เป็น Next Generation Firewall เพิ่มความมั่นคงปลอดภัยให้กับระบบสารสนเทศและระบบบริการสำคัญขององค์กรที่ตั้งอยู่ภายในศูนย์ข้อมูล (Data Center) โดยการแยกการควบคุมความปลอดภัยออกจากระบบไฟร์วอลล์หลักขององค์กร ช่วยลดความเสี่ยงจากการโจมตีและการ

แพร่กระจายของภัยคุกคามภายในเครือข่าย ทั้งนี้เป็นไปตามแนวทางของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยเน้นการแบ่งโซนเครือข่ายระหว่างส่วนผู้ใช้ (User Zone) และส่วนศูนย์ข้อมูล (Server Zone) เพื่อให้สามารถตรวจสอบและควบคุมความปลอดภัยได้อย่างมีประสิทธิภาพ โดยมีคุณสมบัติดังนี้

1) มี Threat Protection Throughput ไม่น้อยกว่า 6 Gbps และ มีความเร็วในการทำงาน Firewall Throughput ไม่น้อยกว่า 39 Gbps
2) สามารถรองรับการเชื่อมต่อพร้อมกัน (Concurrent Sessions) ได้ไม่น้อยกว่า 11,000,000 Sessions และสามารถรับการเชื่อมต่อใหม่ (New Sessions / Second) ได้ไม่น้อยกว่า 400,000 Sessions
3) สามารถทำการเชื่อมโยง IPsec VPN ซึ่งมีความเร็วในการทำงานไม่น้อยกว่า 36 Gbps
4) อุปกรณ์มี Interface สำหรับเชื่อมต่อระบบ โดยมีคุณสมบัติดังต่อไปนี้
   - มีพอร์ต Gigabit Ethernet แบบ RJ45 ไม่น้อยกว่า 8 Ports
   - มีพอร์ต 5/2.5/Gigabit Ethernet แบบ RJ45 ไม่น้อยกว่า 8 Ports
   - มีพอร์ต Gigabit Ethernet แบบ SFP ไม่น้อยกว่า 4 Slots
   - มีพอร์ต 10 Gigabit Ethernet แบบ SFP+ ไม่น้อยกว่า 8 Slots
   - มีพอร์ต console แบบ RJ45 ไม่น้อยกว่า 1 Port
5) รองรับการทำงานลักษณะ Virtual Domains/Systems ได้อย่างน้อย 10 Virtual Domains/Systems
6) รองรับการทำ High Availability (HA) แบบ Active-Active และ Active-Passive ได้
7) สามารถส่ง File ไปทำการตรวจสอบ กับระบบ Cloud Service เพื่อตรวจสอบ ว่าเป็นภัยคุกคามหรือไม่
8) สามารถตรวจสอบและควบคุมการเข้าถึงเว็บไซต์ (Web Filter) ซึ่งสามารถกรองเว็บไซต์โดยระบุเป็นกลุ่มเว็บไซต์ได้ (Website Category) และสามารถกรองเว็บไซต์ โดยระบุ URL ได้ (Based on URL)
9) สามารถบริหารจัดการอุปกรณ์ที่นำเสนอผ่านระบบ Cloud Service ได้ และอยู่ภายใต้เครื่องหมายการค้าเดียวกัน
10) สามารถส่ง Log ไประบบ Cloud Service ที่สามารถเก็บข้อมูลได้อย่างน้อย 1 ปี และมี Preconfigured Report ที่สามารถตั้ง Scheduled Reports และส่ง Email แบบอัตโนมัติได้
11) รองรับการตรวจสอบผู้ใช้งาน (User Authenticator) กับ ฐานข้อมูลผู้ใช้งานภายในอุปกรณ์ (Local User) , Active Directory (AD) และ Radius รวมถึงสามารถทำงานแบบ Single Sign-on ได้
12) สามารถส่ง Log แบบ Syslog ตามมาตรฐาน RFC-3195 ไปยัง Server ภายนอกได้มากกว่า 1 Server
13) สามารถทำ Application Control หรือ Visibility ได้อย่างน้อย 1,000+ Application ขึ้นไป
14) สามารถทำ Dynamic routing แบบ OSPF, BGP, RIP ได้

15) รองรับการทำ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

16) มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ Redundant

<u>รายการที่ 3 อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) สำหรับ Branch Office</u>

เป็นอุปกรณ์ Appliance ที่ออกแบบขึ้นมาเฉพาะ เพื่อทำหน้าที่เป็น Next Generation Firewall เพื่อใช้งานเป็นอุปกรณ์รักษาความปลอดภัยเครือข่ายในสำนักงานสาขา (Branch Office) สำหรับเชื่อมต่อกับสำนักงานใหญ่ ในรูปแบบ Site-to-Site VPN เพื่อให้การสื่อสารระหว่างเครือข่ายมีความมั่นคงปลอดภัย และสามารถบริหารจัดการนโยบายความปลอดภัยแบบรวมศูนย์ได้ โดยมีคุณสมบัติ ดังนี้

1) เป็นอุปกรณ์ Appliance-Based Firewall ที่ออกแบบมาเพื่อทำหน้าที่ตรวจจับและควบคุมการใช้งาน Application, User และ Content ได้อย่างมีประสิทธิภาพ ต้องมีสมรรถนะขั้นต่ำดังนี้
   - Firewall Throughput: ไม่น้อยกว่า 1.8 Gbps
   - Threat Prevention Throughput: ไม่น้อยกว่า 1.2 Gbps
   - Maximum Concurrent Sessions: ไม่น้อยกว่า 98,000 sessions
   - New Sessions per Second: ไม่น้อยกว่า 15,000 sessions/second
2) มี Network Interface แบบ 10/100/1000 Mbps (RJ-45) จำนวนไม่น้อยกว่า 8 พอร์ต และ Management Port แยกเฉพาะ อย่างน้อย 1 พอร์ต
3) รองรับการทำงานแบบ Site-to-Site VPN, IPSec VPN และ SSL VPN ได้ โดยสามารถเข้ารหัสข้อมูลได้อย่างน้อยระดับ AES-256 และต้องสามารถทำงานร่วมกับ PA-1410 ที่สำนักงานใหญ่ได้อย่างสมบูรณ์
4) รองรับระบบ Dynamic Routing Protocol ได้อย่างน้อย RIP, OSPF และ BGP
5) รองรับการทำงานแบบ Multiple Deployment Mode ได้ เช่น Layer 2, Layer 3, Tap และ Virtual Wire (Transparent Mode) โดยไม่ต้องแบ่ง Virtual System
6) รองรับการทำงานกับระบบเครือข่าย VLAN ผ่าน Protocol 802.1Q ได้ไม่น้อยกว่า 4,000 VLAN ต่อ Interface
7) สามารถป้องกันภัยคุกคามประเภท Vulnerability, Virus, Spyware และ Malware ได้ โดยสามารถอัปเดต Signature อัตโนมัติจาก Cloud Threat Intelligence ของ Palo Alto Networks
8) มีเทคโนโลยี Inline Machine Learning (ML) และ AI-based Threat Detection เพื่อป้องกัน Command and Control (C&C) Traffic และภัยคุกคามแบบ Zero-day ได้แบบ Real-time

9) มีระบบตรวจจับ Advanced Malware ด้วยเทคโนโลยี Cloud-based Sandbox (เช่น WildFire) สำหรับวิเคราะห์ และสร้าง Signature เพื่อป้องกัน Zero-day Malware โดยอัตโนมัติ
10) สามารถกรอง URL และควบคุมการเข้าถึง เว็บไซต์ (URL Filtering) ได้ตาม Category พร้อมระบบ Machine Learning วิเคราะห์ URL แบบ Real-time และสามารถกำหนด Allow / Block List ได้
11) รองรับ SD-WAN Functionality เพื่อควบคุมเส้นทางของ Traffic ตามคุณภาพของ Link เช่น Latency, Jitter และ Packet Loss
12) รองรับการยืนยันตัวตนผู้ใช้งานกับระบบ Active Directory, LDAP และ Radius ได้ และสามารถตรวจสอบผู้ใช้จาก User ID Agent หรือ Syslog ได้โดยตรง
13) สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ดาวน์โหลด หรือ อัปโหลด ได้ รวมถึง การกรองข้อมูลสำคัญ (Data Filtering) เช่น หมายเลขบัตรเครดิต หรือ ข้อมูลอ่อนไหว อื่น ๆ ตามที่ผู้ดูแลระบบกำหนด
14) รองรับการจัดเก็บ และส่งต่อข้อมูล Syslog และ SNMP ไปยังระบบ SOC หรือ Centralized Log ได้
15) รองรับการทำงานแบบ High Availability (HA) ได้ทั้ง Active/Passive และ Active/Active Mode เพื่อเพิ่มความต่อเนื่องของการให้บริการ
16) มีความสามารถในการบริหารจัดการผ่าน Web Interface (HTTPS) และ Command Line Interface (CLI) ได้
17) มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ Redundant
18)

<u>รายการที่ 4 อุปกรณ์กระจายสัญญาณความเร็วสูง (Distribute Switch) สำหรับเชื่อมต่อกับอุปกรณ์กระจายสัญญาณหลัก (Core Switch) จำนวน 2 เครื่อง</u>

เป็นอุปกรณ์ Layer 3 Managed Switch แบบ Rack Mountable สำหรับติดตั้งในตู้แร็คมาตรฐานขนาด 19 นิ้ว โดยมีคุณสมบัติ ดังนี้

1) มีสมรรถนะการสวิตช์ข้อมูล (Switching Capacity) ไม่น้อยกว่า 480 Gbps และมีอัตราการส่งข้อมูล (Forwarding Rate) ไม่น้อยกว่า 357 Mpps (64-byte packets)
2) มีพอร์ตเชื่อมต่อระบบเครือข่ายแบบ SFP+ (10 Gigabit Ethernet) จำนวนไม่น้อยกว่า 24 พอร์ต และ ต้องติดตั้ง SFP+ Module ชนิด SR (10 Gigabit) พร้อมใช้งานจำนวนไม่น้อยกว่า 12 พอร์ตต่อเครื่อง และมีสาย Fiber Patch Cord ยาว 3 เมตร จำนวนเท่ากับ SFP+ Module ที่จัดให้
3) มี CPU แบบ Dual-Core และหน่วยความจำ (DRAM) ไม่น้อยกว่า 1 GB

4) ต้องสามารถเชื่อมต่อและทำงานร่วมกันในลักษณะ Stackable หรือใช้เทคโนโลยีการรวมสวิตช์ของ Cisco เช่น Cisco StackWise Virtual หรือเทียบเท่า เพื่อให้บริหารจัดการได้ในลักษณะอุปกรณ์เดียวกัน (Single Management)
5) สามารถทำงานในระบบ Stacking หรือ Clustering ได้ไม่น้อยกว่า 8 เครื่อง เพื่อรองรับการขยายระบบในอนาคต
6) รองรับจำนวน MAC Addresses ไม่น้อยกว่า 16,000 รายการ และรองรับ VLAN ไม่น้อยกว่า 4,000 VLANs ตามมาตรฐาน IEEE 802.1Q
7) รองรับมาตรการรักษาความปลอดภัยของระบบเครือข่าย ได้แก่ IEEE 802.1X Port-based Authentication, Access Control Lists (ACLs), DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
8) มีไฟแสดงสถานะการทำงานของพอร์ตทุกช่อง (LED Indicators)
9) รองรับการบริหารจัดการอุปกรณ์ผ่าน Command Line Interface (CLI), Telnet / SSH, และ Web GUI (HTTPS)
10) ต้องผ่านมาตรฐานความปลอดภัยสากล เช่น FCC, UL หรือเทียบเท่า

คุณลักษณะเฉพาะเพิ่มเติม

1) ผู้ยื่นข้อเสนอต้องส่งมอบพร้อมติดตั้งให้แล้วเสร็จอยู่ในสภาพพร้อมที่จะใช้งานได้ทันทีโดยเดินสายให้อยู่ในราง หรือวัสดุอื่นๆ ให้เรียบร้อย โดยผู้ยื่นข้อเสนอต้องจัดเตรียมสายเชื่อมต่อต่างๆ ให้เพียงพอกับตามความต้องการ ภายในระยะเวลา 90 วัน นับถัดจากวันลงนามในสัญญา
2) มีหมายเลขประจำเครื่อง (Serial Number) ติดที่เครื่องอย่างชัดเจนมาจากโรงงาน และสามารถตรวจสอบหมายเลขประจำเครื่องผ่านซอฟต์แวร์หรือผ่านเว็บไซต์ได้
3) ผู้ยื่นข้อเสนอต้องได้รับการสนับสนุนทางด้านเทคนิคจากบริษัทเจ้าของผลิตภัณฑ์ เพื่อให้คำปรึกษาแนะนำการใช้งานในผลิตภัณฑ์ที่ได้นำเสนอ
4) บริษัทเจ้าของผลิตภัณฑ์ต้องมีศูนย์ที่บริการที่ได้รับการแต่งตั้ง โดยต้องได้รับมาตรฐานบริการหลังการขายหรือมีกระบวนการ (Process) การให้บริการในภาพรวมตาม ISO 9001:2008 โดยศูนย์บริการดังกล่าวต้องมีบริการ Call Center ให้บริการหมายเลขโทรฟรี ตลอด 7 วัน 24 ชม.

5. หลักเกณฑ์และสิทธิในการพิจารณาราคา

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาตัดสิน โดยใช้หลักเกณฑ์ราคา เพียงอย่างเดียว และ การพิจารณาผู้ชนะการยื่นข้อเสนอ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาจาก ราคารวม (รวมภาษีมูลค่าเพิ่มแล้ว) ที่เสนอราคาต่ำสุด

6. วงเงินงบประมาณ จำนวน 3,900,000 บาท (สามล้านเก้าแสนบาทถ้วน) รวมภาษีมูลค่าเพิ่ม

7. ระยะเวลาดำเนินการ

ส่งมอบพร้อมติดตั้งตามที่ สสวท. กำหนด ภายใน 90 วัน นับถัดจากวันลงนามในสัญญา ดังนี้

7.1 ส่งมอบแผนการทำงานตลอดระยะเวลาตามสัญญา ภายใน 14 วัน นับถัดจากวันลงนามในสัญญา

7.2 ก่อนการส่งมอบบริษัท จะต้องทำหนังสือแจ้งกำหนดการส่งมอบล่วงหน้าไม่น้อยกว่า 7 วันทำการ

7.3 ผู้เสนอราคาต้องทำการติดตั้งอุปกรณ์พร้อมสายสัญญาณระหว่างอุปกรณ์ที่เสนอการจัดซื้อครั้งนี้ ให้สามารถใช้งานร่วมกับระบบเครือข่ายของ สสวท ได้เป็นอย่างดี

7.4 ส่งมอบเอกสาร รูปแบบการติดตั้งระบบพร้อมอุปกรณ์ทั้งหมด (Configuration) พร้อมเอกสารแสดงรายละเอียดของอุปกรณ์ โดยระบุชนิด ยี่ห้อ รุ่น จำนวน และ Serial Number ในรูปแบบเอกสารอิเล็กทรอนิกส์ (PDF)

8. การส่งมอบงานและการชำระเงิน

ชำระเงิน 100% เมื่อ สสวท. ได้ทดสอบการใช้งานและตรวจรับเรียบร้อยแล้ว

9. รายละเอียดการรับประกัน การบำรุงรักษา

9.1 อุปกรณ์ทุกชิ้นส่วนและลิขสิทธิ์ซอฟต์แวร์ต่างๆ ต้องอยู่ภายใต้การรับประกันของเจ้าของผลิตภัณฑ์ และมีการให้บริการถึงสถานที่ติดตั้ง (On-Site Service) แบบ 8x5x4 พร้อมให้บริการใน 8 ชั่วโมง ตลอด 5 วันทำการ วันจันทร์ถึงศุกร์ และมีการตอบสนอง (Response Time) ภายในระยะเวลา 4 ชั่วโมง หลังจากได้รับแจ้งเหตุผิดปกติ ตลอดระยะเวลาการรับประกัน 3 ปี

9.2 ต้องมีบริการให้คำแนะนำที่เกี่ยวเนื่องกับระบบของ Server, Storage, Networking, Virtualization ในกรณีที่ลูกค้าต้องการปิดระบบ เพื่อทดสอบ หรือ สำรองข้อมูล หรืออัพเกรดระบบ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

9.3 ต้องจัดทำรายงานสถานะของเครื่อง (Existing Report) เพื่อรายงานประสิทธิภาพ (Performance Report) ของอุปกรณ์ดังกล่าว ตามที่ สสวท. ระบุ และ ทำการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance: PM) บำรุงรักษาเชิงป้องกันอุปกรณ์ เพื่อให้เครื่องอยู่ในสภาพที่ใช้งานได้เป็นปกติ และมีประสิทธิภาพตลอดการ

รับประกัน โดยจะต้องมีรายงานสรุปรายเดือนในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ (PDF)

9.4 ในกรณีที่อุปกรณ์เสียหายไม่สามารถใช้งานได้ตามปกติ จะต้องนำอุปกรณ์มาเปลี่ยนแทนอุปกรณ์ที่เสีย และในกรณีที่ต้องใช้ระยะเวลาในการซ่อมเกินกว่า 3 วันทำการ ผู้ยื่นข้อเสนอจะต้องนำเสนอแผนที่จะสามารถทำให้ระบบคอมพิวเตอร์ของ สสวท. สามารถทำงานได้เป็นปรกติในช่วงเวลาการซ่อม

9.5 สถาบันฯ จะต้องมีสิทธิ์ได้รับการปรับปรุงผลิตภัณฑ์ (Upgrade) ระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องให้เป็น Version หรือ Release ใหม่ตามที่ร้องขอ โดยต้องทำการแก้ไขปรับปรุงผลิตภัณฑ์ให้โดยจะต้องไม่มีผลกระทบต่อการทางานของระบบทั้งหมดที่เกี่ยวข้องและไม่คิดค่าใช้จ่ายเพิ่ม

9.6 ผลิตภัณฑ์ที่เสนอต้องเป็นรุ่นที่ยังอยู่ในสายการผลิตและเป็นผลิตภัณฑ์ที่ผู้ผลิตยังไม่ประกาศภาวะสิ้นสุดการขายหรือสิ้นสุดอายุหรือสิ้นสุดการบริการ (End-of-Sale หรือ End-of-Life หรือ End-of-Service) รวมทั้งต้องเป็นเครื่องใหม่ ที่ยังไม่เคยติดตั้งใช้งานที่ใดมาก่อนและไม่เป็นเครื่องที่ถูกนำมาปรับปรุงสภาพใหม่ โดยต้องมีหนังสือรับรองจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทยมาแสดงในวันยื่นซองเอกสารรายละเอียดทางเทคนิค

10. ค่าปรับ กรณีที่ผู้ยื่นข้อเสนอ ส่งมอบงานเกินระยะเวลาที่กำหนด ผู้ยื่นข้อเสนอจะต้องชำระค่าปรับเป็นรายวันให้เป็นรายวัน ในอัตราร้อยละ 0.2 นับแต่วันถัดจากวันครบกำหนดตามสัญญา