ขอบเขตของงาน (TERMS OF REFERENCE : TOR)
โครงการเช่าใช้งานบริการระบบรักษาความปลอดภัย Firewall

1. หลักการและเหตุผล/ความเป็นมา

ฝ่ายเทคโนโลยีดิจิทัล สถาบันเทคโนโลยีนิวเคลียร์แห่งชาติ (องค์การมหาชน) เป็นมีหน้าที่รับผิดชอบด้านการให้บริการระบบสารสนเทศ และโครงสร้างพื้นฐานและความมั่นคงปลอดภัยสารสนเทศ ปัจจุบันสถาบันมีการขับเคลื่อนองค์กรโดยใช้เทคโนโลยีดิจิทัล เพื่อสนับสนุนงานการทำงานให้กับเจ้าหน้าที่ภายในสถาบัน ไม่ว่าจะเป็นด้านงานวิจัยและพัฒนา งานถ่ายทอดเทคโนโลยีทางด้านนิวเคลียร์ งานบริการต่างๆ ผ่านระบบอิเล็กทรอนิกส์ ซึ่งปัจจุบันสถาบัน มีระบบรักษาความมั่นคงปลอดภัย Firewall ที่ใช้งานมาเกินระยะเวลา 5 ปีแล้ว มีความเสี่ยงด้านอุปกรณ์ฮาร์ดแวร์อาจจะชำรุดเสียหายแล้ว ยังพบว่าอุปกรณ์ ยี่ห้อ/รุ่น ที่สถาบันใช้งานอยู่กำลังจะสิ้นสุดการสนับสนุนจากเจ้าของผลิตภัณฑ์อีกด้วย หากเกิดเหตุการณ์อุปกรณ์ชำรุด เสียหาย ก็จะทำให้มีผลกระทบต่อการให้บริการด้านเทคโนโลยีดิจิทัล และกระทบด้านความมั่นคงปลอดภัยสารสนเทศของสถาบันอีกด้วย

ดังนั้นเพื่อการให้บริการเทคโนโลยีดิจิทัลของสถาบันมีความต่อเนื่อง และมีความมั่นคงปลอดภัยสารสารสนเทศ ฝ่ายเทคโนโลยีดิจิทัล จึงมีความจำเป็นต้องดำเนินการจัดหาระบบรักษาความปลอดภัย Firewall ใหม่เพื่อทดแทนระบบเดิม โดยจะมีการจัดหาลักษณะแบบเช่าใช้บริการ จำนวน 5 ปี

2. วัตถุประสงค์

2.1 เพื่อทดแทนระบบรักษาความปลอดภัย Firewall เดิม ที่มีอายุการใช้งานเกิน 5 ปี และกำลังจะสิ้นสุดการสนับสนุนจากเจ้าของผลิตภัณฑ์

2.2 เพื่อให้สถาบัน มีระบบรักษาความมั่นคงปลอดภัยสารสนเทศที่ทันสมัย และลดความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ลักษณะภัยคุกคามรูปแบบใหม่ๆ ที่เพิ่มมากขึ้นในปัจจุบัน

2.3 เพื่อให้มีความต่อเนื่องต่อการให้บริการระบบสารสนเทศและโครงสร้างพื้นฐานความมั่นคงปลอดภัยสารสนเทศของสถาบัน

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 คุณสมบัติทั่วไป

3.1.1 มีความสามารถตามกฎหมาย

3.1.2 ไม่เป็นบุคคลล้มละลาย

3.1.3 ไม่อยู่ระหว่างเลิกกิจการ

3.1.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่าย

สารสนเทศของกรมบัญชีกลาง

3.1.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.1.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.1.7 เป็นนิติบุคคลผู้มีอาชีพในงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.1.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่หน่วยงานของรัฐ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.1.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

3.1.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP ของกรมบัญชีกลาง

3.1.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า 3,000,000 บาท

(3) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้าง หรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามสัญญา

(4) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้

ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

(5) กรณีตาม (1) – (4) ยกเว้นสำหรับกรณีดังต่อไปนี้

(5.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(5.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

3.2 คุณสมบัติอื่นๆ

ผู้ยื่นข้อเสนอต้องมีผลงานประเภทการซื้อหรือเช่าระบบรักษาความปลอดภัย Firewall หรือระบบรักษาความปลอดภัยเครือข่าย หรือผลงานอื่นที่เกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัยสารสนเทศ หรือผลงานการเช่าใช้วงจรสื่อสารโทรคมนาคมพร้อมติดตั้งอุปกรณ์รักษาความปลอดภัย กับหน่วยงานราชการหรือรัฐวิสาหกิจหรือเอกชนที่น่าเชื่อถือได้ จำนวนไม่น้อยกว่า 1 ผลงาน ดังนี้

3.2.1 ผลงานการซื้อหรือเช่าต้องมีวงเงินไม่น้อยกว่า 6,000,000 บาท (หกล้านบาทถ้วน) ต่อสัญญา และจะต้องเป็นผลงานที่แล้วเสร็จ ไม่เกิน 3 ปี นับถึงวันยื่นเสนอราคา โดยให้ยื่นหนังสือรับรองผลงานขณะเข้าเสนอราคา

3.2.2 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา

3.2.3 ผู้ยื่นข้อเสนอจะต้องมีบุคลากรผู้เชี่ยวชาญ ในการติดตั้งผลิตภัณฑ์ที่เสนอ พร้อมยื่นเอกสารประกอบคุณสมบัติของบุคลากรขณะเข้าเสนอราคา ดังนี้

3.2.3.1 ประวัติการศึกษา ประสบการณ์การทำงาน ของผู้เชี่ยวชาญ

3.2.3.2 สำเนาหนังสือรับรอง หรือสำเนาประกาศนียบัตร แสดงให้เห็นว่ามีความเชี่ยวชาญในผลิตภัณฑ์ที่เสนอ โดยหนังสือหรือประกาศนียบัตรต้องออกโดยเจ้าของผลิตภัณฑ์เดียวกันกับที่เสนอ

4. รายละเอียดคุณลักษณะทั่วไปหรือขอบเขตของงานจ้าง

ผู้ยื่นข้อเสนอจะต้องดำเนินการตามโครงการเช่าใช้งานระบบรักษาความปลอดภัย Firewall โดยมีรายละเอียด ดังต่อไปนี้

4.1 การเช่าใช้งานระบบรักษาความปลอดภัย Firewall ผู้ยื่นข้อเสนอต้องให้บริการเป็นระยะเวลาจำนวนไม่น้อยกว่า 5 ปี รวมค่าใช้จ่ายซอฟต์แวร์ Subscription และการบำรุงรักษา

4.2 จะต้องดำเนินการประชุมวางแผนการดำเนินการ (Kick off Meeting) โครงการ ที่ระบุถึง ระยะเวลา ขั้นตอนการดำเนินการ ผู้รับผิดชอบดูแลงานในแต่ละขั้นตอน และผลสรุปการประชุมวางแผนการดำเนินการ

4.3 จะต้องดำเนินการศึกษา สำรวจ วิเคราะห์ ออกแบบ และแผนการติดตั้งระบบรักษาความปลอดภัย Firewall พร้อมนำเสนอให้สถาบันทราบและอนุมัติก่อนดำเนินการติดตั้ง

4.4 จะต้องดำเนินการจัดให้มีการอบรมแบบ Onsite หรือ Online ให้กับผู้ดูแลระบบโดยรองรับจำนวนผู้เข้าอบรมไม่น้อยกว่า 3 คน และต้องจัดส่งไฟล์นำเสนอหรือเอกสารอบรมให้กับสถาบันผ่านทางอีเมลก่อนวันอบรมไม่น้อยกว่า 3 วันทำการ

4.5 จะต้องจัดทำคู่มือการใช้งานระบบสำหรับผู้ดูแลระบบเป็นรูปแบบอิเล็กทรอนิกส์ไฟล์ (.PDF) รวมถึงเอกสารอื่นๆ หรือ Configuration files ที่เกี่ยวข้อง จัดเก็บในอุปกรณ์ Flash Drive ให้กับสถาบัน ในวันส่งมอบงาน

4.6 จะต้องจัดให้มีวิศวกรผู้เชี่ยวชาญมาประจำ ณ สถานที่ติดตั้ง จำนวนไม่น้อยกว่า 1 คน สำหรับรองรับการแก้ไขปัญหาที่อาจจะเกิดขึ้นกับการใช้งานระบบใหม่ ในช่วง 5 วันทำการแรก

4.7 จะต้องจัดทำรายงานการตรวจสอบและประเมินระบบอย่างละเอียด เพื่อระบุช่องโหว่และความเสี่ยงต่างๆ ที่อาจถูกโจมตีจากภัยคุกคามไซเบอร์ (Security Assessment Report) ที่ตรวจจับได้จากอุปกรณ์หรือซอฟต์แวร์ที่เสนอ โดยจัดส่งให้สถาบัน ทางอีเมลประจำทุกๆ 3 เดือน

4.8 ผู้ยื่นข้อเสนอต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงการรักษาความลับข้อมูลของสถาบัน

4.9 สถาบัน มีสิทธิ์ในการใช้งานระบบรักษาความปลอดภัย Firewall ทั้งหมดตามระยะเวลาในสัญญาเช่า (ยกเว้นการ Update และ Upgrade เวอร์ชันของซอฟต์แวร์ จะต้องดำเนินการโดยวิศวกรผู้เชี่ยวชาญจากผู้ยื่นข้อเสนอ)

4.10 เมื่อใกล้ครบสัญญาเช่าหรือหมดสัญญาเช่า สถาบัน มีสิทธิ์ในการขอต่อสัญญาเช่าได้ โดยสถาบันจะแจ้งล่วงหน้าเป็นลายลักษณ์อักษรไม่น้อยกว่า 1 เดือน ก่อนหมดสัญญาเช่า

4.11 ผู้ยื่นข้อเสนอจะต้องจัดทำแผนการดำเนินงานติดตั้งและConfig อุปกรณ์ นำเสนอให้กับสถาบันพิจารณา ให้ดำเนินงาน เพื่อให้การติดตั้งใช้งานระบบมีผลกระทบน้อยที่สุด

4.12 ผู้ยื่นข้อเสนอต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศและสัญญารักษาความลับของข้อมูล ของสถาบันเทคโนโลยีนิวเคลียร์แห่งชาติ (องค์การมหาชน)

5. รายละเอียดคุณลักษณะเฉพาะ

5.1 ระบบรักษาความปลอดภัย Firewall ประเภทที่ 1 จำนวน 3 ชุด โดยมีคุณลักษณะพื้นฐานอย่างน้อยดังนี้

5.1.1 เป็นอุปกรณ์ Appliance-Based Firewall (Application Firewall) ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ

5.1.2 เป็นอุปกรณ์ที่ออกแบบมาเป็น Chassis หรือ เป็นอุปกรณ์แบบ Appliance ที่แยกหน่วยประมวลผลสำหรับการบริหารจัดการ (Control Plane หรือ Management Plane) และหน่วยประมวลผลสำหรับการจัดการข้อมูล (Data Plane) ออกจากกันภายในตัวอุปกรณ์

5.1.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) รายละเอียดอย่างน้อยดังนี้

5.1.3.1 ช่องเชื่อมต่อแบบ 10/100/1000 Base-T หรือดีกว่า ไม่น้อยกว่า 8 ช่อง

5.1.3.2 ช่องเชื่อมต่อสำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า 1 ช่อง โดยไม่รวมกับช่องเชื่อมต่อในข้อ 5.1.3.1

5.1.4 มี Firewall Throughput ไม่น้อยกว่า 2.5 Gbps ในแบบ appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

5.1.5 มี Threat Prevention Throughput ไม่น้อยกว่า 1 Gbps ในแบบ appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

5.1.6 มีจำนวนเซสชันสูงสุด (Max Sessions) อย่างน้อย 200,000 sessions และ New Sessions อย่างน้อย 34,000 Sessions ต่อวินาที

5.1.7 สามารถทำงานแบบ L3 หรือ Route Mode, L2, Tap และ Transparent Mode Firewall ได้

5.1.8 สามารถทำ Static Route และ Dynamic Routing Protocol ได้แก่ RIP, OSPF และ BGP ได้เป็นอย่างน้อย

5.1.9 สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย และ SSO แบบ SAML ได้บนตัวอุปกรณ์ หรือเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

5.1.10 สามารถรับ syslog จากอุปกรณ์อื่น เช่น Wireless controller, Proxy Server, และ Network Access Control เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้แต่ละคน (IP address to username mappings) ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้บนตัวอุปกรณ์ หรือเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

5.1.11 สามารถป้องกันภัยคุกคามประเภท Vulnerability, Exploits, C2 และ Spyware ได้โดยสามารถมีการอัพเดท Signature ใหม่แบบอัตโนมัติ

5.1.12 มีระบบตรวจจับ Advanced Malware หรือ Unknown Malware แบบ Cloud-Based และใช้เทคโนโลยีแบบ Sandbox เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้พร้อมทั้งสามารถแสดงรายงาน การทำงานของ Malware ที่ตรวจพบได้จากระบบดังกล่าว รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ

5.1.13 สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category, Block list, Allow list ที่กำหนดได้ และต้องมีการจัด category ให้กับแต่ละ website ไม่น้อยกว่า 2 category (Multi-Category URL Filtering) หรือเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

5.1.14 มีระบบที่สามารถตรวจจับ และป้องกันการเข้าถึง Malicious Domain ภายในองค์กรได้ โดยต้องมีความสามารถอย่างน้อยดังนี้

5.1.14.1 มีระบบ Machine Learning ในการตรวจหาเทคนิคอัลกอริทึม Domain generation algorithms (DGA) เพื่อวิเคราะห์คาดการณ์ ป้องกัน Malicious Domain ที่ไม่เคยพบมาก่อนได้

5.1.14.2 สามารถตรวจจับและป้องกัน DNS Tunneling เพื่อป้องกันการขโมยข้อมูลในองค์กร ผ่านช่องทาง DNS

5.1.14.3 สามารถตรวจจับและป้องกันผ่าน DNS Services เช่น Fast Flux Domains, DNS Rebinding Attack ได้เป็นอย่างน้อย

5.1.14.4 ทำงานแบบ Real time และไม่มีข้อจำกัดรองรับปริมาณ Malicious Domain ที่เพิ่มขึ้นในอนาคต โดยตรวจจับผ่านทาง DNS และต้องไม่ส่งผลกระทบกับ Performance ของตัวอุปกรณ์

5.1.14.5 สามารถเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถใช้งานได้ตามข้อกำหนดข้อ 1.14

5.1.15 สามารถทำงานในลักษณะ SD-WAN เพื่อควบคุมเส้นทางของ Traffic ด้วยคุณภาพของการเชื่อมต่ออินเทอร์เน็ต เช่น Latency, Jitter, Package Loss ได้เป็นอย่างน้อย

5.1.16 อุปกรณ์รองรับผู้ใช้งานระบบ VPN Client ไม่น้อยกว่า 1,000 ผู้ใช้งานและสามารถเชื่อมต่อกับระบบ Active Directory (AD) ของ สถาบัน และสามารถใช้บนระบบปฏิบัติการ Windows 11, MAC OS ได้เป็นอย่างน้อย

5.1.17 รองรับการติดตั้งแบบ HA (High Availability) ในรูปแบบ Active/Active หรือ Active/Passive

5.1.18 รองรับแหล่งจ่ายไฟฟ้า (Power Supply) แบบ Redundant

5.1.19 ต้องได้รับการรับรองมาตรฐาน FCC และ VCCI เป็นอย่างน้อย

5.1.20 ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Network Firewalls ปี 2022 หรือปีล่าสุด

5.1.21 เป็นอุปกรณ์ใหม่ไม่เคยติดตั้งใช้งานที่อื่นมาก่อน

5.2 ระบบรักษาความปลอดภัย Firewall ประเภทที่ 2 จำนวน 2 ชุด โดยมีคุณลักษณะพื้นฐานอย่างน้อยดังนี้

5.2.1 เป็นอุปกรณ์ Appliance-Based Firewall ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ (Application Firewall)

5.2.2 เป็นอุปกรณ์ที่ออกแบบมาเป็น Chassis หรือ เป็นอุปกรณ์แบบ Appliance ที่แยกหน่วยประมวลผลสำหรับการบริหารจัดการ (Control Plane หรือ Management Plane) และหน่วยประมวลผลสำหรับการจัดการข้อมูล (Data Plane) ออกจากกันภายในตัวอุปกรณ์

5.2.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) รายละเอียดอย่างน้อยดังนี้

5.2.3.1 ช่องเชื่อมต่อแบบ 10/100/1000 RJ-45 หรือดีกว่า ไม่น้อยกว่า 4 พอร์ต

5.2.3.2 ช่องเชื่อมต่อแบบ 1G/2.5G/5G หรือดีกว่า ไม่น้อยกว่า 8 พอร์ต

5.2.3.3 ช่องเชื่อมต่อแบบ 1G SFP หรือดีกว่า ไม่น้อยกว่า 2 พอร์ต

5.2.3.4 ช่องเชื่อมต่อแบบ 1G/10G SFP/SFP+ หรือดีกว่า ไม่น้อยกว่า 8 พอร์ต

5.2.4 มี Interface HA แบบ 10/100/1000 หรือดีกว่าไม่น้อยกว่า 2 พอร์ท, 10G SFP+ ไม่น้อยกว่า 1 พอร์ท และมี Interface แบบ 10/100/1000 หรือดีกว่าสำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า 1 พอร์ต โดยทั้งหมดไม่นับรวมกับ interface จากข้อที่ 5.2.3

5.2.5 มี Firewall Throughput ไม่น้อยกว่า 9.5 Gbps ในแบบ appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

5.2.6 มี Threat Prevention Throughput ไม่น้อยกว่า 6 Gbps ในแบบ appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

5.2.7 มีจำนวนเซสชันสูงสุด (Max Sessions) ไม่น้อยกว่า 1,400,000 sessions และ New Sessions ไม่น้อยกว่า 140,000 Sessions ต่อวินาที

5.2.8 มี storage ชนิด SSD สำหรับจัดเก็บข้อมูลระบบ (System Storage) ขนาดไม่ต่ำกว่า 240 GB หรือดีกว่า

5.2.9 สามารถทำงานแบบ L3 หรือ Route Mode, L2, Tap และ Transparent Mode Firewall ได้

5.2.10 สามารถทำ Routing แบบ Static, RIP, BGP, OSPF, Multicast และ Policy Based Forwarding หรือ Policy based Routing ได้เป็นอย่างน้อย

5.2.11 สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย และ SSO แบบ SAML ได้บนตัวอุปกรณ์ หรือเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

5.2.12 สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound) รวมทั้งการทำ decryption mirroring

5.2.13 สามารถรับ syslog จากอุปกรณ์อื่น เช่น Wireless controller, Proxy Server, และ Network Access Control เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้แต่ละคน (IP address to username mappings) ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้บนตัวอุปกรณ์ หรือเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

5.2.14 สามารถป้องกันภัยคุกคามประเภท Vulnerability, Virus และ Spyware ได้โดยสามารถมีการอัพเดท Signature ใหม่แบบอัตโนมัติ

5.2.15 มีระบบตรวจจับ Advanced Malware หรือ Unknown Malware แบบ Cloud-Based และใช้เทคโนโลยีแบบ Sandbox เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้พร้อมทั้งสามารถแสดงรายงาน การทำงานของ Malware ที่

ตรวจพบได้จากระบบดังกล่าว รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ

5.2.16 สามารถตรวจจับ และ ป้องกัน การเข้าถึง Malicious Domain ภายในองค์กรได้ โดยต้องมีความสามารถอย่างน้อย ดังนี้

5.2.16.1 มีระบบ Machine Learning ในการตรวจหาเทคนิคอัลกอริทึม Domain generation algorithms (DGA) เพื่อวิเคราะห์คาดการณ์ ป้องกัน Malicious Domain ที่ไม่เคยพบมาก่อนได้

5.2.16.2 สามารถตรวจจับและป้องกัน DNS Tunneling ได้ เพื่อป้องกันการขโมยข้อมูลในองค์กร ผ่านช่องทาง DNS

5.2.16.3 สามารถตรวจจับและป้องกันผ่าน DNS Services เช่น Fast Flux Domains, DNS Rebinding Attack ได้เป็นอย่างน้อย

5.2.16.4 ทำงานแบบ Real time และไม่มีข้อจำกัดรองรับปริมาณ Malicious Domain ที่เพิ่มขึ้นในอนาคต โดยตรวจจับผ่านทาง DNS และต้องไม่ส่งผลกระทบกับ Performance ของตัวอุปกรณ์

5.2.16.5 สามารถเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

5.2.17 สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category, Block list, Allow list ที่กำหนดได้ และต้องมีการจัด category ให้กับแต่ละ website ไม่น้อยกว่า 2 category (Multi-Category URL Filtering) หรือเสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

5.2.18 สามารถทำงานในลักษณะ SD-WAN เพื่อควบคุมเส้นทางของ Traffic ด้วยคุณภาพของการเชื่อมต่ออินเทอร์เน็ต เช่น Latency, Jitter, Package Loss ได้เป็นอย่างน้อย

5.2.19 อุปกรณ์รองรับผู้ใช้งานระบบ VPN Client ไม่น้อยกว่า 1,000 ผู้ใช้งานและสามารถเชื่อมต่อกับระบบ Active Directory (AD) ของ สถาบัน และสามารถใช้บนระบบปฏิบัติการ Windows 11, MAC OS ได้เป็นอย่างน้อย

5.2.20 รองรับการติดตั้งแบบ HA (High Availability) ในรูปแบบ Active/Active หรือ Active/Passive

5.2.21 มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ redundant

5.2.22 ต้องได้รับการรับรองมาตรฐาน FCC และ VCCI เป็นอย่างน้อย

5.2.23 ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Network Firewalls ปี 2022 หรือปีล่าสุด

5.2.24 เป็นอุปกรณ์ใหม่ไม่เคยติดตั้งใช้งานที่อื่นมาก่อน

5.3 ระบบบริหารจัดการอุปกรณ์รักษาความปลอดภัยระดับแอปพลิเคชันแบบรวมศูนย์ จำนวน 1 ชุด โดยแต่ละชุดมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.3.1 เป็นอุปกรณ์สำหรับการบริหารจัดการอุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์แบบรวมศูนย์ (Centralized Management) ในรูปแบบของ Software Appliance และต้องเป็นผลิตภัณฑ์แบรนด์เดียวกับอุปกรณ์ Firewall

5.3.2 สามารถสร้าง Configuration Template ได้จากจุดเดียวและกำหนดให้ทำการปรับปรุง (Deploy) ไปยังอุปกรณ์รักษาความปลอดภัยระดับแอปพลิเคชัน (Application Firewall) ที่ใช้งานในระบบได้ รวมทั้งสามารถรับ log เพื่อทำการ Traffic Monitoring, Analysis, Reporting and Forensics

5.3.3 ระบบสามารถบริหารจัดการอุปกรณ์รักษาความปลอดภัยระดับแอปพลิเคชัน (Application Firewall) ได้ไม่น้อยกว่า 25 หน่วย

5.3.4 สามารถเชื่อมต่อกับอุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ลูกข่ายที่นำเสนอผ่านโปรโตคอล SSL

5.3.5 ระบบสามารถทำการบริหารจัดการผ่านทาง Web Interface และ SSH ได้เป็นอย่างน้อย

5.3.6 สามารถดูสรุป General Information, Top Application, Interface Status, Threat Logs, Data Filtering Logs, URL Filtering Logs, System Logs, High Availability และ Resource Information ในส่วนของ Dashboard ได้

5.3.7 สามารถเรียกดูสรุปข้อมูลของ Applications, URL Categories, Threats และ Data ในรูปแบบของกราฟฟิกได้

5.3.8 สามารถปรับแต่งรายงานตามความต้องการ (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลา ส่งรายงานผ่านทาง Email แบบอัตโนมัติได้ และสามารถทำรายงานต่างๆ อย่างน้อยดังนี้

5.3.8.1 Top Application, Application Category

5.3.8.2 Top Source, User, Destination

5.3.8.3 Top Threats, Attackers and Victims

5.3.8.4 User activity report

5.3.9 รองรับการติดตั้งบนระบบเครื่องแม่ข่ายเสมือน VMware หรือ Nutanix ได้เป็นอย่างน้อย

6. กำหนดส่งมอบ

ระยะเวลาการเช่า 5 ปี โดยผู้ให้เช่าจะต้องส่งมอบระบบรักษาความปลอดภัย Firewall ภายใน 90 วัน นับถัดจากวันที่ได้ลงนามในสัญญาเช่าใช้ระบบ โดยส่งมอบที่สถาบันเทคโนโลยีนิวเคลียร์แห่งชาติ (องค์การมหาชน) องครักษ์

7. วงเงินในการจัดหา

วงเงินงบประมาณ 15,000,000 บาท (สิบห้าล้านบาทถ้วน)

8. การชำระค่าเช่า

แบ่งชำระเป็น 20 งวด งวดละ 3 เดือน จำนวนเงินงวดละเท่าๆ

9. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

พิจารณาข้อเสนอโดยใช้เกณฑ์ราคา

10. อัตราค่าปรับ

กรณีที่ผู้ให้เช่าไม่สามารถดำเนินการตามเวลาที่กำหนดได้ ผู้ให้เช่าจะต้องเสียค่าปรับให้แก่สถาบันเทคโนโลยีนิวเคลียร์แห่งชาติ (องค์การมหาชน) เป็นรายวันในอัตราร้อยละ 0.20 ของราคาพัสดุที่ยังไม่ได้ส่งมอบ นับถัดจากวันครบกำหนดจนถึงวันที่ผู้ให้เช่าปฏิบัติตามสัญญาถูกต้องครบถ้วนและสถาบันได้ตรวจรับงานแล้ว

11. การรับประกันความชำรุดบกพร่องของงาน

11.1 ผู้ยื่นข้อเสนอจะต้องจัดให้มีการรับประกันผลงาน และการบริการบำรุงรักษาระบบรักษาความปลอดภัย Firewall เป็นระยะเวลา 5 ปี หรือตามระยะสัญญาเช่า ณ สถานที่ติดตั้ง ในเวลาทำการแบบ 24 x 7 (24 ชั่วโมง x 7 วัน) นับตั้งแต่ที่ระบบได้ใช้งานจริง (Production)

11.2 การบำรุงรักษาและซ่อมแซมแก้ไขภายในกำหนดเวลารับประกันผลงานผู้ยื่นข้อเสนอจะต้องบำรุงรักษาระบบโดยไม่คิดค่าใช้จ่ายใด ๆ

11.3 การบำรุงรักษาแบบป้องกัน (Preventive Maintenance) ไม่น้อยกว่า 6 เดือนต่อครั้ง

11.4 การบำรุงรักษาแบบแก้ไข (Corrective Maintenance) เมื่อเกิดข้อผิดพลาดของอุปกรณ์ หรือซอฟต์แวร์ที่เสนอ หรือขัดข้องอันเนื่องจากการใช้งานตามปกติ ผู้ยื่นข้อเสนอจะต้องรับจัดการซ่อมแซมแก้ไขภายใน 24 ชั่วโมงเพื่อให้สามารถใช้งานได้ชั่วคราว และแก้ไขให้ใช้งานได้ปกติภายใน 5 วันทำการนับแต่เวลาที่ได้รับแจ้งจากผู้ดูแลระบบของสถาบัน ไม่ว่าด้วยวาจาหรือเป็นลายลักษณ์อักษร

11.5 กรณีที่อุปกรณ์ หรือซอฟต์แวร์เกิดความเสียหาย และไม่สามารถดำเนินการแก้ไขให้กลับมาใช้งานได้ ผู้ยื่นข้อเสนอต้องนำอุปกรณ์หรือซอฟต์แวร์สำรองมาเปลี่ยนให้ใหม่ หรือเปลี่ยนเป็นอุปกรณ์หรือซอฟต์แวร์ใหม่ ที่มีคุณลักษณะเดียวกันหรือดีกว่า เพื่อให้ระบบสามารถกลับมาใช้งานได้ตามปกติ

11.6 ผู้ยื่นข้อเสนอจัดให้มีเจ้าหน้าที่ สำหรับรับข้อปัญหาและแจ้งตอบวิธีแก้ปัญหาที่เกิดขึ้น ทางโทรศัพท์ อีเมล หรือ ไลน์แอพลิเคชั่น ทุกวันในเวลาราชการ ตลอดเวลาการรับประกัน

ผู้สนใจสามารถ วิจารณ์ เสนอข้อคิดเห็น และข้อเสนอแนะเกี่ยวกับร่างขอบเขตการจัดซื้อวัสดุดังกล่าว ด้วยวิธีการดำเนินโครงการ e-bidding สามารถแจ้งให้ความเห็นทาง e-mail ที่ suphachai@tint.or.th, danai

@tint.or.th หรือ udomsak@tint.or.th และส่ง e-mail โดยระบุชื่อ ที่อยู่ และหมายเลขโทรศัพท์ที่สามารถติดต่อได้

(ลงชื่อ).....ประธานกรรมการ

(นายศุภชัย โรยแก้ว)

(ลงชื่อ).....กรรมการ

(นายดนัย วงษ์เนตร)

(ลงชื่อ).....กรรมการ

(นายอุดมศักดิ์ สุขสวัสดิ์)