ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจัดหาอุปกรณ์ Firewall สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server Farm Zone)**

   /หน่วยงานเจ้าของโครงการ **ฝ่ายเทคโนโลยีสารสนเทศ**

2. วงเงินงบประมาณที่ได้รับจัดสรร 1,995,000.- บาท **(หนึ่งล้านเก้าแสนเก้าหมื่นห้าพันบาทถ้วน)**

3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 20 ต.ค. 2557

   เป็นเงิน 1,995,000.- บาท (หนึ่งล้านเก้าแสนเก้าหมื่นห้าพันบาทถ้วน)

   ราคา/หน่วย (ถ้ามี) - บาท

4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   ใช้ราคาที่สืบจากตัวแทนจำหน่ายอุปกรณ์ Firewall จำนวน 3 ราย

   4.1 บริษัท ดาต้าโปร คอมพิวเตอร์ ซิสเต็มส์ จำกัด

   4.2 บริษัท เมโทรซิสเต็มส์ คอร์ปอเรชั่น จำกัด (มหาชน)

   4.3 บริษัท คอมเทรดดิ้ง จำกัด

5. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

   5.1 นายบุญลักษณ์ ฉวีวงศ์วิวัฒน์ ผู้ช่วยผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ

   5.2 นางสาวกนกวรรณ มหิวรรณ ผู้ช่วยผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ

   5.3 นางอุรสา พงษ์เสรี ผู้บริหารส่วนจัดซื้อ ฝ่ายธุรการ

ผนวก 1

คุณลักษณะด้านเทคนิคขั้นต่ำ/ขอบเขตงาน

การจัดหาอุปกรณ์ Firewall สำหรับ Server Farm Zone

---

1. **ข้อกำหนดความต้องการทั่วไป**

1.1 ต้องเสนอราคาอุปกรณ์ Firewall รวมการติดตั้ง การทดสอบ การรับประกันความชำรุดบกพร่อง การฝึกอบรม คู่มือและเอกสารสนับสนุนการใช้งานที่เกี่ยวข้องตามขอบเขตที่กำหนด

1.2 อุปกรณ์ Firewall ที่เสนอต้องสามารถทำงานร่วมกับระบบสารสนเทศหลักของธนาคารที่มีอยู่เดิม ประกอบด้วย ระบบเครือข่าย (Network) ระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบจัดเก็บข้อมูล (SAN) ระบบการสำรองข้อมูล (Backup) และระบบการรักษาความปลอดภัยของระบบสารสนเทศ (Security) ได้อย่างมีประสิทธิภาพ

1.3 ต้องเสนอ Configuration Design ของอุปกรณ์ Firewall ทั้งระบบส่งให้กับธนาคาร โดยต้องให้รายละเอียดของอุปกรณ์ ตลอดจนรูปแบบและวิธีการเชื่อมต่อของอุปกรณ์ทั้งโครงการ

2. **ข้อกำหนดเกี่ยวกับคุณลักษณะเฉพาะ (Specification)**

อุปกรณ์ Firewall สำหรับ Server Farm Zone จำนวน 2 ชุด ต้องมีคุณสมบัติขั้นต่ำดังต่อไปนี้

2.1 เป็นอุปกรณ์ที่ออกแบบเฉพาะ (Appliance) เพื่อทำหน้าที่เป็น Application Firewall

2.2 สามารถทำ High Availability (HA) แบบ Active/Passive และ Active/Active และต้องเสนออุปกรณ์ที่ใช้ประกอบร่วมมาให้ครบ

2.3 มี Network port ดังต่อไปนี้

2.3.1 แบบ 10/100/1000 จำนวนไม่น้อยกว่า 12 port

2.3.2 แบบ Gigabit SFP จำนวนไม่น้อยกว่า 8 port

2.4 มี Hard disk ขนาดความจุไม่น้อยกว่า 120 GB

2.5 สามารถทำงานแบบ Application Firewall (Layer 7) ที่ Throughput ไม่น้อยกว่า 4 Gbps

2.6 สามารถทำงานแบบ IPSec VPN ที่ Throughput ไม่น้อยกว่า 500 Mbps

2.7 สามารถทำงานแบบ SSL VPN ได้โดยรองรับ Concurrent Users ได้ไม่น้อยกว่า 2,000 ผู้ใช้งาน

2.8 มี Maximum Session ไม่น้อยกว่า 500,000 Sessions และสามารถรับ Session ใหม่ไม่น้อยกว่า 50,000 Sessions ต่อวินาที

2.9 สามารถเข้ารหัส (Encryption) แบบ 3DES, AES (128 bit , 192 bit , 256 bit) และรองรับการ Authentication แบบ MD5, SHA เป็นอย่างน้อย

2.10 สามารถตรวจสอบ Traffic ที่มีการเข้ารหัสแบบ SSL (Inbound และ Outbound) และ SSH

2.11 รองรับมาตรฐานการทำงานต่างๆ ดังต่อไปนี้

2.11.1 VLAN (802.1q)

2.11.2 NAT

2.11.3 DHCP Relay

2.11.4 Dynamic Routing (OSPF , RIP และ BGP)

2.11.5 Multicast Routing (PIM-SM, PIM-SSM และ IGMP)

2.11.6 Syslog (TCP, UDP และ SSL)

2.11.7 SNMP (Version 2 และVersion 3)

2.12 สามารถกำหนดเงื่อนไขการทำงานเพื่อให้รองรับการทำงานในระดับของ Layer 2, Layer 3, Transparent และ Tap Mode

2.13 สามารถตรวจสอบผู้ใช้งาน (User Authentication/Identification) ร่วมกับระบบ Microsoft Active Directory, LDAP และ RADIUS

2.14 สามารถควบคุมการใช้งานโดยจำแนก Application ไม่น้อยกว่า 1,700 ชนิด

2.15 สามารถควบคุมการใช้งานด้าน Application อย่างน้อยดังต่อไปนี้

2.15.1 Application Files Transfer

2.15.2 Tunnel Application (เช่น การ encrypted-tunnel)

2.15.3 Instant Messaging

2.15.4 Internet Conferencing

2.15.5 P2P

2.16 สามารถทำ QoS แบบ Guaranteed, Maximum และ Priority Bandwidth

2.17 สามารถกำหนดเงื่อนไขการทำ QoS (Traffic shaping policy) อย่างน้อยดังต่อไปนี้

2.17.1 Application

2.17.2 User and User Group

2.17.3 Source

2.17.4 Destination

2.17.5 Interface

2.17.6 IPSec VPN Tunnel

2.18 มี Throughput ไม่น้อยกว่า 2 Gbps เมื่อเปิดใช้งาน IPS ร่วมกับ Firewall

2.19 มีระบบป้องกันภัยคุกคาม (Threat Prevention) อย่างน้อยดังต่อไปนี้

2.19.1 Vulnerability exploits

2.19.2 buffer overflows

2.19.3 DoS attacks

2.19.4 Port scans

2.19.5 Malformed packets

2.19.6 IP defragmentation

2.19.7 TCP reassembly

2.20 สามารถใช้งานในรูปแบบของ Antivirus และ Antispyware อย่างน้อยดังต่อไปนี้

2.20.1 Malware

2.20.2 Viruses

2.20.3 Spywares

2.20.4 Bot-net

2.20.5 Trojans

2.20.6 การ download malware แบบอัตโนมัติ

2.21 มีระบบตรวจสอบ Malware หรือ Threat ที่ยังไม่ปรากฏอยู่ในฐานข้อมูล (Unknown Malwares หรือ Threat) โดยใช้ระบบ Cloud-based Engine

2.22 สามารถระงับการทำงาน (Block) ตามประเภทของไฟล์(Extension file type) อย่างน้อยดังต่อไปนี้

2.22.1 exe

2.22.2 dll

2.22.3 mp3

2.22.4 iso

2.22.5 gzip

2.22.6 tar

2.22.7 docx

2.22.8 xlsx

2.23 สามารถป้องกันการรั่วไหลของข้อมูล (Data Filtering) ออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต และสามารถกำหนดสร้างรูปแบบตามต้องการ (Custom Pattern)

2.24 มี Console Port อย่างน้อย 1 พอร์ต

2.25 มี Port แบบ Gigabit สำหรับบริหารจัดการอุปกรณ์โดยเฉพาะ (Out of Band Management) อย่างน้อย 1 พอร์ตแยกต่างหากจาก Network Port ปกติ

2.26 สามารถบริหารจัดการอุปกรณ์แบบ GUI (Web-based หรือ Software Management) และ Command Line Interface

2.27 สามารถเก็บข้อมูลการใช้งาน (Logging)

2.28 สามารถสร้างรายงาน (Report) อย่างน้อยดังต่อไปนี้

2.28.1 User Activity

2.28.2 Application

2.28.3 Threat/Attack

2.28.4 Bot-net

2.28.5 AntiVirus

2.29 สามารถทำการปรับแต่งรายงาน (Custom Report) และนำออก (Export) ในรูปแบบ PDF หรือ CSV

2.30 สามารถติดตั้งในตู้เก็บอุปกรณ์ขนาดมาตรฐาน 19 นิ้ว

2.31 ผลิตภัณฑ์ที่นำเสนอต้องอยู่ใน Gartner Leader Quadrant ด้าน Enterprise Network Firewalls ปี 2013 หรือใหม่กว่า

2.32 ต้องรับประกันคุณภาพแบบ On Site Service (24x7) เป็นระยะเวลา 1 ปี นับจากวันที่ธนาคารได้ทำการตรวจรับการส่งมอบงาน โดยถูกต้องครบถ้วนทั้งหมดเป็นที่เรียบร้อยแล้ว

3. การให้บริการสนับสนุนระหว่างการรับประกัน (Support)

3.1 ผู้เสนอราคาจะต้องจัดให้มีเจ้าหน้าที่ประสานงานและเบอร์โทรศัพท์ที่สามารถรับแจ้งเหตุขัดข้อง และให้คำปรึกษา หรือแก้ไขปัญหาขั้นต้นทางโทรศัพท์เกี่ยวกับการใช้งานตลอดจนดำเนินการติดตั้งและปรับปรุงแก้ไขให้แล้วเสร็จสมบูรณ์ ทุกวันตลอด 24 ชั่วโมง

3.2 ต้องดำเนินการติดต่อกลับธนาคารภายใน 4 ชั่วโมง นับจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร

3.3 ในกรณีที่ไม่สามารถแก้ไขปัญหาผ่านทางโทรศัพท์ หรือช่องทางอื่นได้ ต้องจัดส่งพนักงานเข้ามายังสถานที่ติดตั้ง เพื่อแก้ไขเหตุขัดข้องหรือความชำรุดบกพร่อง เพื่อให้อุปกรณ์สามารถใช้งานได้เป็นปกติภายใน 8 ชั่วโมง นับจากที่ได้รับแจ้งเหตุขัดข้อง หรือความชำรุดบกพร่องจากธนาคาร

3.4 ต้องจัดทำรายละเอียดและขั้นตอนการแก้ไขปัญหาหรือเหตุขัดข้อง หรือความชำรุดบกพร่องหรือการบำรุงรักษาอุปกรณ์ Firewall โดยละเอียดให้แก่ผู้ว่าจ้างในทันทีที่สามารถดำเนินการได้

3.5 ต้องเข้ามาตรวจสอบ และบำรุงรักษาอุปกรณ์ Firewall ณ สถานที่ติดตั้ง อย่างน้อย 4 ครั้ง ตามระยะเวลาที่ได้ตกลงร่วมกัน โดยก่อนเข้าดำเนินการต้องทำหนังสือแจ้งให้ธนาคารทราบล่วงหน้าก่อนเข้าดำเนินการอย่างน้อย 5 วันทำการ

4. **ขอบเขตงาน**

ผู้เสนอราคาที่ได้รับการคัดเลือกต้องดำเนินการตามขอบเขตงานที่กำหนดอย่างน้อย ดังต่อไปนี้

4.1 จัดทำแผนการดำเนินงานโดยละเอียดตั้งแต่เริ่มดำเนินการ กระบวนการติดตั้ง การทดสอบการใช้งาน การฝึกอบรมการใช้งาน จนถึงการส่งมอบงานที่แล้วเสร็จสมบูรณ์ให้ธนาคารพิจารณาเห็นชอบก่อนเริ่มดำเนินโครงการ

4.2 จัดทำคู่มือการใช้งานอย่างน้อยรายการละ 1 ชุด ดังต่อไปนี้

4.2.1 คู่มือการ Configure

4.2.2 คู่มือการ Backup/Restore

4.2.3 คู่มือการใช้งาน

4.3 ดำเนินการติดตั้งอุปกรณ์และทดสอบการใช้งาน

4.4 ดำเนินการฝึกอบรม พร้อมจัดทำเอกสารที่เกี่ยวข้องกับการใช้งานอุปกรณ์ Firewall ให้กับเจ้าหน้าที่ผู้ดูแลระบบของธนาคาร โดยรองรับผู้เข้ารับการฝึกอบรมได้ไม่น้อยกว่า 3 คน