เอกสารหมายเลข ๒

รายละเอียดคุณลักษณะเฉพาะของอุปกรณ์ที่จัดซื้อ

รายละเอียดคุณลักษณะเฉพาะของอุปกรณ์ที่จัดซื้อ
โครงการเพิ่มประสิทธิภาพระบบบริหารจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง
(Data Center and DR Site Infrastructure Management (DCIM))
และระบบรักษาความปลอดภัยข้อมูล

"คอมพิวเตอร์" ที่กรมสรรพสามิต จัดซื้อในครั้งนี้ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่จะใช้งานได้ทันทีและต้องเป็นรุ่นที่ยังอยู่ในสายการผลิต (Production Line) และจำหน่าย ณ วันยื่นข้อเสนอ โดยคุณลักษณะเฉพาะของ "อุปกรณ์เพิ่มประสิทธิภาพระบบบริหารจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง(Data Center and DR Site Infrastructure Management (DCIM)) และระบบรักษาความปลอดภัยข้อมูล" จะต้องเหมาะสมกับลักษณะงานของกรมสรรพสามิตตามโครงการนี้ และสามารถทำงานร่วมกันและใช้งานร่วมกับระบบงานคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ สะดวกต่อการใช้งาน โดยผู้ประสงค์จะเสนอราคาต้องเสนอระบบเครือข่ายสื่อสารและระบบความปลอดภัยเครือข่ายที่มีคุณลักษณะเฉพาะไม่ต่ำกว่าที่ระบุในเอกสารนี้

เงื่อนไขทั่วไปในการติดตั้ง "คอมพิวเตอร์"

ผู้ชนะการประกวดราคาต้องจัดหาอุปกรณ์หรือซอฟต์แวร์ที่จำเป็นสำหรับการทำงาน ของ "คอมพิวเตอร์" ให้สามารถทำงานได้อย่างสมบูรณ์ โดยไม่คิดมูลค่าเพิ่มเติมจากราคา ที่เสนอ

(๑) ระบบบริหารจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง (Data Center and DR Site Infrastructure Management (DCIM)) จำนวน ๑ ระบบ มีคุณลักษณะดังต่อไปนี้

(๑.๑) โปรแกรมจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง จำนวน ๑ ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้

(๑.๑.๑) มี License ที่สามารถบริหารจัดการตู้จัดเก็บอุปกรณ์ได้ ๑๕๐ License (Rack)

(๑.๑.๒) สามารถทำการแสดงภาพจำลองและข้อมูลรายการอุปกรณ์ที่ถูกติดตั้งภายในตู้จัดเก็บอุปกรณ์ (Rack)

(๑.๑.๓) ระบบบริหารจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง (DC - DR site Infrastructure Management DCIM) โดยสามารถติดตั้งโปรแกรมจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองภายใต้ระบบปฏิบัติการ Windows หรือ Linux Redhat หรือ CentOS ได้

(๑.๑.๔) เป็นโปรแกรมบริหารจัดการเสมือนจริง Graphics แบบ ๓D

(๑.๑.๕) มีระบบ User Authentication โดยสามารถบริหารจัดการผู้ใช้งานได้อย่างน้อยดังนี้

(๑.๑.๕.๑) สามารถ เพิ่ม/ลบ/แก้ไข รายละเอียดผู้ใช้งานและกำหนดสิทธิ์การใช้งานแต่ละผู้ใช้งานได้

(๑.๑.๕.๒) สามารถเชื่อมต่อข้อมูลผู้ใช้งานกับ LDAP หรือ Active Directory Server ได้

(๑.๑.๕.๓) สามารถตั้งกลุ่มของ User หรือ Department เพื่อจำแนกประเภทของ User ได้ไม่น้อยกว่า ๒ กลุ่ม

(๑.๑.๕.๔) สามารถแจ้งเตือนความผิดปกติของอุปกรณ์บนหน้าจอหลักได้ และสามารถบันทึกเหตุการณ์ที่เกิดขึ้นได้ไม่น้อยกว่า ๙๐ วัน

(๑.๑.๖) สามารถสร้างแบบจำลองของห้อง (Layout) ได้ โดยสามารถตั้งชื่อของแต่ละห้องได้และสามารถกำหนดตำแหน่งอุปกรณ์สนับสนุนที่ติดตั้ง ลงในแบบจำลองได้ แต่ละอุปกรณ์สามารถเพิ่ม ลบ และแก้ไขการตั้งค่าได้และสามารถแสดงแบบจำลองในรูปแบบ ๓ มิติ ได้ (โดยมี Object ให้เลือกใช้งาน)

(๑.๑.๗) การแสดงแผนผังศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง ได้อย่างน้อยดังนี้

(๑.๑.๗.๑) ทำการแสดงผลแบบจำลอง Floor Layout ในมุมมองรูปแบบทั้ง ๒ มิติ และ ๓ มิติได้

(๑.๑.๗.๒) ทำการแสดงผลแบบจำลองในมุมมองระดับสูง (Top View)

(๑.๑.๗.๓) ทำการแสดงผลแบบจำลองภาพและข้อมูลรายการอุปกรณ์ที่ถูกติดตั้งภายในตู้จัดเก็บอุปกรณ์ (Rack)

(๑.๑.๘) สามารถคำนวณและแสดงค่า Power usage effectiveness: PUE ได้

(๑.๑.๙) สามารถใส่รายละเอียดข้อมูลต่างๆ ของอุปกรณ์ที่ติดตั้งได้ เช่น ชื่อ เป็นต้น

(๑.๑.๑๐) สามารถจำลองตู้ Rack และเพิ่มลดอุปกรณ์ที่ติดตั้งภายในตู้ Rack ได้จาก Library/Category ที่มีให้เลือก

(๑.๑.๑๑) สามารถค้นหาข้อมูลอุปกรณ์หรือตำแหน่งที่ติดตั้งของอุปกรณ์ในศูนย์ข้อมูลได้

(๑.๑.๑๒) สัญลักษณ์ของอุปกรณ์สนับสนุนที่อยู่ในแบบจำลอง สามารถแสดงข้อมูลเฉพาะของอุปกรณ์นั้นและสามารถเปลี่ยนสีเมื่อเกิดเหตุผิดปกติ

(๑.๑.๑๓) สามารถกำหนดจำนวนชั้น (U) การติดตั้งอุปกรณ์ภายในตู้ Rack ได้

(๑.๑.๑๔) สามารถสร้างรายงานประเภทต่างๆ เช่นพลังงานไฟฟ้า การทำความเย็น จากรูปแบบรายงานที่มีให้เลือกได้จัดการได้

(๑.๑.๑๕) สามารถบริหารจัดการผ่าน web browser หรือ Client ได้

(๑.๑.๑๖) สามารถเชื่อมต่อในมาตรฐานการสื่อสารแบบ TCP/IP, SNMP, Modbus ได้

(๑.๑.๑๗) มี Application หรือ web Browser รองรับการใช้ งานบน SmartPhone ทั้ง Android และ IOS โดยต้องสามารถใช้งานบน SmartPhone พร้อมกันไม่น้อยกว่า ๒๐ ลิขสิทธิ์

(๑.๑.๑๘) สามารถ Generate ค่าอุณหภูมิ ค่าความชื้น และทิศทางลม เป็นแบบแผนภูมิสีได้ (Thermal and Airflow/Velocity Mapping)

(๑.๑.๑๙) สามารถทำ Cable Mapping (การเชื่อมต่อของสาย) ทั้งสายไฟ สาย UTP และ Fiber ได้

(๑.๑.๒๐) สามารถทำการ Import, Export อุปกรณ์ด้วยไฟล์ .CSV หรือจาก Excel ได้

(๑.๑.๒๑) สามารถติดตั้งกับคอมพิวเตอร์แม่ข่ายที่ทางกรมสรรพสามิตจัดหาให้ได้

(๑.๑.๒๒) อุปกรณ์ที่เสนอ ต้องได้รับอนุญาตให้จำหน่ายในประเทศไทยอย่างถูกต้องตามกฎหมาย โดยจะต้องแนบหนังสือรับรองการแต่งตั้ง/หนังสืออนุญาตจากบริษัทผู้ผลิต หรือ ผู้ผลิตที่มีสาขาในประเทศไทยให้จำหน่ายในประเทศไทย โดยหนังสือนั้นต้องมีอายุไม่เกิน ๙๐ วัน นับถัดจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอประกวดราคา แนบไปพร้อมเอกสารการเสนอราคา

(๑.๒) อุปกรณ์ Power Distribution Unit (PDU) จำนวน ๒๐๐ ชุด โดยมีคุณลักษณะดังต่อไปนี้

(๑.๒.๑) สามารถแสดงค่า current, voltage หรือ kWH ตามเวลาจริง จาก Web Browser หรือ Eco Sensors Software Management ได้

(๑.๒.๒) สามารถ สั่งเปิด, ปิด, การจ่ายระบบไฟฟ้าให้เครื่องคอมพิวเตอร์แม่ข่าย ระบบเซิร์ฟเวอร์ หรือ อุปกรณ์ IT ที่เชื่อมต่ออยู่กับ PDU ทั้งหมดหรือเฉพาะบาง Outlet ได้จากระยะไกลผ่านระบบเครือข่าย

(๑.๒.๓) สามารถใช้งานด้วยโปรโตคอล TCP/IP, UDP

(๑.๒.๔) สามารถเข้าใช้งาน PDU ได้ผ่าน Web Browser หรือ Eco Sensors Software Management ได้

(๑.๒.๕) สามารถทำ SNMP V๓ ได้

(๑.๒.๖) สามารถตัดกระแสไฟฟ้าที่เป็นสาเหตุทำให้ใช้ไฟเกินจากปกติได้ (Proactive Overload Protection)

(๑.๒.๗) ตั้งค่าเกณฑ์การแจ้งเตือน ค่า current หรือ voltage ต่ำสุด-สูงสุด ได้

(๑.๒.๘) มีพอร์ตสำหรับการเชื่อมต่ออุปกรณ์ตรวจจับอุณหภูมิ และ ความชื้นไม่น้อยกว่า ๑ พอร์ตพร้อมอุปกรณ์ตรวจจับอุณหภูมิ และความชื้นอย่างน้อย ๑ ชุด

(๑.๒.๙) สามารถรองรับโหลดได้ไม่น้อยกว่า ๓๒A โดยมีระบบป้องกันที่สามารถรีเซ็ตได้

(๑.๒.๑๐) มีช่อง Outlet จำนวนไม่น้อยกว่า ๒๔ ช่อง โดยสามารถใช้งานกับอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายได้

(๑.๒.๑๑) ผลิตภัณฑ์ต้องสามารถทำงานร่วมกับโปรแกรมจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง (ข้อ ๑.๑) ได้อย่างมีประสิทธิภาพ

(๑.๒.๑๒) อุปกรณ์ที่เสนอ ต้องได้รับอนุญาตให้จำหน่ายในประเทศไทยอย่างถูกต้องตามกฎหมาย โดยจะต้องแนบหนังสือรับรองการแต่งตั้ง/หนังสืออนุญาตจากบริษัทผู้ผลิต หรือ ผู้ผลิตที่มีสาขาในประเทศไทยให้จำหน่ายในประเทศไทย โดยหนังสือนั้นต้องมีอายุไม่เกิน ๙๐ วัน นับถัดจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอประกวดราคา แนบไปพร้อมเอกสารการเสนอราคา

(๒) ระบบวิเคราะห์ประสิทธิภาพการทำงานของอุปกรณ์เครือข่าย (Network Performance Monitoring) จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

(๒.๑) มี License สามารถบริหารจัดการจำนวนเครื่องแม่ข่ายและอุปกรณ์ได้ไม่น้อยกว่า ๓,๐๐๐ เครื่อง หรือ ๑๕๐,๐๐๐ interface

(๒.๒) สามารถตรวจสอบสถานภาพและประสิทธิภาพอุปกรณ์โดยใช้โปรโตคอลมาตรฐาน เช่น SNMP, ICMP, Telnet, WMI ได้เป็นอย่างน้อย

(๒.๓) สามารถบริหารจัดการเครื่องแม่ข่ายที่ใช้ระบบปฏิบัติการ Windows, Linux, และ Solaris ในลักษณะ Agentless ได้

(๒.๔) สามารถเรียกดูผ่านทางโปรแกรม Web Browser ได้

(๒.๕) สามารถตรวจสอบสถานะและแสดงผล topology VLAN Diagram

(๒.๖) สามารถกำหนดสิทธิ (Privilege) ให้กับผู้ใช้งานเป็นรายคนได้

(๒.๗) สามารถกำหนดสิทธิ (Privilege) ให้กับกลุ่มผู้ใช้งานโดยกำหนดสิทธิในการเข้าดูแต่ละหน้าได้ในลักษณะ Web Portal สำหรับแต่ละกลุ่มผู้ใช้งาน

(๒.๘) สามารถสร้างรายงาน เป็นแฟ้มข้อมูลแบบ pdf และ MS Excel ได้เป็นอย่างน้อย

(๒.๙) สามารถตรวจสอบการเข้าใช้งานโดยใช้ชื่อและรหัสผ่านเป็นอย่างน้อย และสามารถตรวจสอบชื่อผู้ใช้กับ Active Directory และ LDAP ได้

(๒.๑๐) สามารถตรวจสอบว่า user ใดเข้ามาใช้ในระบบย้อนหลังได้ โดยแสดงวันที่ เวลา และ IP Address ที่ user เข้ามาใช้งานได้

(๒.๑๑) สามารถแสดงสถานภาพ และประสิทธิภาพ ของเครือข่ายแบบ diagram ได้

(๒.๑๒) แสดงสถานภาพของ อุปกรณ์ หรือ พอร์ตเชื่อมต่อเป็นเฉดสีได้

(๒.๑๓) สามารถแสดงข้อมูลของเครื่องแม่ข่าย ได้แก่ Hostname, IP address, OS type, OS version, จำนวน CPU, ขนาดหน่วยความจำ, ขนาด Hard Disk, Up/Down, Uptime, Windows Service status เป็นอย่างน้อย

(๒.๑๔) สามารถแสดงประสิทธิภาพของเครื่องแม่ข่าย ได้แก่ cpu utilization, memory utilization, disk usage, traffic utilization, error rate, discard rate, process utilization เป็นอย่างน้อย และสามารถดูแบบย้อนหลังได้

(๒.๑๕) สามารถเลือกเครื่องแม่ข่าย หรือ process หรือ service หรือ interface หรือ อุปกรณ์ที่ต้องการ monitor และบันทึกเป็น profile เพื่อเรียก monitor ได้ในภายหลัง

(๒.๑๖) สามารถแสดงกราฟ cpu utilization, memory utilization, disk utilization อย่างน้อย ๔๘ ชั่วโมงที่ผ่านมา ของเครื่องแม่ข่ายทุกเครื่องใน profile ที่เลือก โดยเปลี่ยนหน้าจอแบบหมุนภาพตามระยะเวลาที่กำหนด

(๒.๑๗) สามารถแสดงเส้น based line เมื่อ utilization สูงเกิน

(๒.๑๘) สามารถจัดเก็บ Configuration ของอุปกรณ์เป็นรายวันและสามารถเรียกดูย้อนหลังได้

(๒.๑๙) สามารถส่งการแจ้งเตือนไปยังผู้เกี่ยวข้องในกรณีต่างๆ ผ่าน e-mail และ line application และรองรับการส่งแจ้งเตือนผ่าน SMS ได้

(๒.๒๐) สามารถแสดง และจัดทำรายงานในเรื่องต่อไปนี้ได้

(๒.๒๐.๑) CPU, Memory Utilization ของแต่ละอุปกรณ์ โดยกำหนดช่วงวันที่ในรูปแบบตารางและกราฟได้

(๒.๒๐.๒) Host Summary Report แสดง cpu utilization, memory utilization, virtual memory utilization, disk utilization, availability and status change log ของแต่ละเครื่องแม่ข่าย แบบรายวัน รายเดือน

(๒.๒๐.๓) Summary Report แสดง utilization, availability and status change log ของแต่ละ interface แบบรายวัน

(๒.๒๑) บริษัทเจ้าของผลิตภัณฑ์ต้องผ่านการรับรองมาตรฐานในอุตสาหกรรมนั้นๆ ในกรณีซอฟต์แวร์ต้องได้รับรองมาตรฐาน CMMI for Development level ๓ เป็นอย่างน้อย

(๒.๒๒) มี Application รองรับการใช้ งานบน Smartphone ทั้ง Android และ IOS โดยต้องสามารถใช้งานบน Smartphone พร้อมกันไม่น้อยกว่า ๒๐ ลิขสิทธิ์

(๒.๒๓) สามารถติดตั้งกับคอมพิวเตอร์แม่ข่ายที่ทางกรมสรรพสามิตจัดหาให้ได้

(๒.๒๔) อุปกรณ์ที่เสนอ ต้องได้รับอนุญาตให้จำหน่ายในประเทศไทยอย่างถูกต้องตามกฎหมาย โดยจะต้องแนบหนังสือรับรองการแต่งตั้ง/หนังสืออนุญาตจากบริษัทผู้ผลิต หรือ ผู้ผลิตที่มีสาขาในประเทศไทยให้จำหน่ายในประเทศไทย โดหนังสือนั้นต้องมีอายุไม่เกิน ๙๐ วัน นับถัดจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอประกวดราคา แนบไปพร้อมเอกสารการเสนอราคา

(๓) อุปกรณ์ตรวจสอบและบริหารจัดการอุปกรณ์ไฟร์วอลแบบรวมศูนย์ (Centralize Firewall Management and Policy Analysis) จำนวน ๑ ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้

(๓.๑) อุปกรณ์ที่นำเสนอต้องเป็นอุปกรณ์ Appliance ที่ถูกออกแบบมาเพื่อทำหน้าที่วิเคราะห์นโยบายการรักษาความปลอดภัยไฟร์วอลล์บนเครือข่าย (Firewall Analyzer) โดยต้องสามารถบริหารจัดการอุปกรณ์ไฟร์วอลได้จำนวนไม่น้อยกว่า ๒๐ ชุด

(๓.๒) สามารถทำระบบจำลองเพื่อใช้ในการตรวจสอบทราฟฟิค (Traffic Simulation Query) และสามารถค้นหาเส้นทาง Route Lookup จาก Diagram โดยสามารถเลือกจากอุปกรณ์ใน Diagram ได้

(๓.๓) สามารถทำงานร่วมกับผลิตภัณฑ์ Firewall ยี่ห้อ Check Point, PaloAlto, Juniper, Cisco และ Fortinet ได้เป็นอย่างน้อย

(๓.๔) สามารถทำการวิเคราะห์นโยบายการรักษาความปลอดภัยไฟร์วอลล์เพื่อเพิ่มประสิทธิภาพ (Optimize Policy) ได้อย่างน้อย ดังนี้

(๓.๔.๑) นโยบายที่ไม่เคยใช้งาน (Unused rules)

(๓.๔.๒) นโยบายที่มีความซ้ำซ้อนกัน (Covered rules, Redundant special case rules)

(๓.๔.๓) นโยบายที่สามารถรวมกันได้ (Consolidate rules)

(๓.๔.๔) นโยบายที่ไม่อยู่ในช่วงเวลาที่กำหนด (Time-inactive rules)

(๓.๕) สามารถทำการวิเคราะห์เกี่ยวกับนโยบายการรักษาความปลอดภัยไฟร์วอลที่มีความเสี่ยง (Risky Rules) ได้

(๓.๖) สามารถแสดงข้อมูลการแก้ไขเปลี่ยนแปลงนโยบายการรักษาความปลอดภัยไฟร์วอล (Change History) ได้

(๓.๗) สามารถเสนอแนะการปรับปรุงนโยบายให้ดีขึ้น (Intelligent Policy Tuner) ได้

(๓.๘) สามารถสร้างรายงานตามกฎระเบียบมาตรฐาน (Regulatory Compliance) ได้อย่างน้อย ดังนี้

(๓.๘.๑) Payment Card Industry Data Security Standard (PCI DSS) Compliance

(๓.๘.๒) ISO/IEC ๒๗๐๐๑ Compliance

(๓.๘.๓) Financial Instruments and Exchange Law (Japan) Compliance

(๓.๘.๔) Gramm-Leach-Bliley Act (GLBA) Compliance Report

(๓.๘.๕) Health Insurance Portability and Accountability Act (HIPAA)

(๓.๘.๖) General Data Protection Regulation (GDPR)

(๓.๙) ระบบสามารถทำรายงานแบบ Schedule Report และสรุปแบบ รายวัน รายสัปดาห์ และรายเดือน ได้เป็นอย่างน้อย

(๓.๑๐) สามารถทำ Deploy Policy ไปยังอุปกรณ์ Firewall ได้

(๓.๑๑) อุปกรณ์ที่เสนอ ต้องได้รับอนุญาตให้จำหน่ายในประเทศไทยอย่างถูกต้องตามกฎหมาย โดยจะต้องแนบหนังสือรับรองการแต่งตั้ง/หนังสืออนุญาตจากบริษัทผู้ผลิต หรือ ผู้ผลิตที่มีสาขาในประเทศไทยให้จำหน่ายในประเทศไทย โดยหนังสือนั้นต้องมีอายุไม่เกิน ๙๐ วัน นับถัดจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอประกวดราคา แนบไปพร้อมเอกสารการเสนอราคา

(๔) อุปกรณ์บริหารจัดการข้อมูลในระบบเครือข่าย (Network Packet Broker) จำนวน ๑ ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้

(๔.๑) เป็นอุปกรณ์ Appliance ที่ถูกออกแบบมาเพื่อทำหน้าเป็น Aggregator Tap เพื่อรวบรวม Traffic แล้วส่งต่อไปยังเครื่องมือปลายทางที่ต้องการได้

(๔.๒) สามารถประมวลผลไม่น้อยกว่า ๒๐๐ Gbps

(๔.๓) มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑GbE RJ๔๕ จำนวนไม่น้อยกว่า ๒๔ ช่อง และสามารถทำ Fail Open ได้

(๔.๔) มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐GbE SX/SR (๕๐/๑๒๕ µm Multimode) จำนวนไม่น้อยกว่า ๘ ช่องพร้อม Module และสามารถทำ Fail Open ได้

(๔.๕) สามารถทำงานในโหมด Inline และ Out-of-Band ได้

(๔.๖) สามารถทำ Bypass ได้เมื่อตัวอุปกรณ์เกิดขัดข้อง

(๔.๗) สามารถส่งต่อ Traffic ไปยังเครื่องมือปลายทางได้หลายแบบ ดังนี้

(๔.๗.๑) ส่งตามลำดับ (Inline Tools in a Series)

(๔.๗.๒) ส่งแบบกระจาย (Distribution to Multiple Inline Tools)

(๔.๗.๓) ส่งไป Out-of-Band Tools

(๔.๘) สามารถทำการกรองทราฟฟิกที่ต้องการ (Filter Traffic) ก่อนส่งต่อไปยังเครื่องมือปลายทางได้

(๔.๙) สามารถถอดรหัสการรับส่งข้อมูล (SSL Decryption) ในครั้งเดียว และส่งไปยังเครื่องมือปลายทางทั้งแบบ In-line และ Out-of-Band เพื่อการวิเคราะห์เพิ่มเติมได้

(๔.๑๐) สามารถถอดรหัส SSL และ TLS Protocol ดังต่อไปนี้

(๔.๑๐.๑) TLS ๑.๐

(๔.๑๐.๒) TLS ๑.๑

(๔.๑๐.๓) TLS ๑.๒

(๔.๑๐.๔) SSL ๓.๐

(๔.๑๑) สามารถถอดรหัส SSL ที่มี Algorithm หรือ Cipher ดังต่อไปนี้

(๔.๑๑.๑) Encryption algorithms or ciphers: RC๔_๑๒๘, DES_CBC, ๓DES_EDE-CBC, AES_๑๒๘_CBC, AES_๑๒๘_GCM, AES_๒๕๖_CBC, AES_๒๕๖_GCM and Camellia, Chacha๒๐

(๔.๑๑.๒) Message Authentication Code (MAC): MD๕, SHA, SHA๒๕๖, SHA๓๘๔, Poly๑๓๐๕

(๔.๑๑.๓) Key exchange algorithms: RSA, DHE_RSA, ECDHE_RSA, ECDHE_ECDSA

(๔.๑๒) สามารถบริหารจัดการได้ทั้งแบบ CLI และ Web GUI

(๔.๑๓) มี Power Supplies ที่ทำงานแบบ Redundant จำนวน ๒ หน่วย

(๔.๑๔) อุปกรณ์ที่เสนอ ต้องได้รับอนุญาตให้จำหน่ายในประเทศไทยอย่างถูกต้องตามกฎหมาย โดยจะต้องแนบหนังสือรับรองการแต่งตั้ง/หนังสืออนุญาตจากบริษัทผู้ผลิต หรือ ผู้ผลิตที่มีสาขาในประเทศไทยให้จำหน่ายในประเทศไทย โดยหนังสือนั้นต้องมีอายุไม่เกิน ๙๐ วัน นับถัดจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอประกวดราคา แนบไปพร้อมเอกสารการเสนอราคา

(๕) อุปกรณ์บริหารจัดการรหัสผ่านและบริหารจัดการเซสชั่นการใช้งาน Privileged Access Management (PAM) สำหรับผู้ดูแลระบบ จำนวน ๒ ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้

(๕.๑) เป็นอุปกรณ์ Appliance ที่ถูกออกแบบมาเพื่อเป็นระบบ Privileged Account Management

(๕.๒) สามารถบริหารจัดการผ่านทาง Web Browser ในช่องทาง HTTPS

(๕.๓) สามารถทำงานแบบ High Availability ในรูปแบบของ Active/Passive ระหว่างศูนย์หลัก และศูนย์สำรอง (DC – DR) โดยสามารถทำงานทดแทนกันได้ในกรณีที่ระบบที่ศูนย์หลักมีเหตุขัดข้อง โดยสามารถบริหารจัดการอุปกรณ์รวมกันได้ไม่น้อยกว่า ๑,๐๐๐ อุปกรณ์

(๕.๔) สามารถบริหารจัดการรหัสผ่านได้โดยไม่จำเป็นต้องมีการติดตั้ง Software Agent ที่อุปกรณ์ปลายทาง (Agentless)

(๕.๕) สามารถรองรับระบบการ Authentication ผ่านระบบ Active Directory และ LDAP ได้

(๕.๖) สามารถบริหารจัดการ Privileged Account กับอุปกรณ์หรือระบบ อย่างน้อยดังนี้

(๕.๖.๑) Operating System เช่น Windows Server, Linux

(๕.๖.๒) Database Account เช่น SQL Server, Oracle, MySQL

(๕.๖.๓) Network/Security Appliances เช่น Check Point, Juniper, Cisco, Palo Alto, Fortinet

(๕.๗) สามารถกำหนดสิทธิ์ของผู้ใช้งานในการเข้าใช้งานระบบได้อย่างน้อยดังนี้

(๕.๗.๑) ผู้ร้องขอ (Requestor)

(๕.๗.๒) ผู้อนุมัติ (Approver)

(๕.๗.๓) ผู้ร้องขอและผู้อนุมัติ (Approver/Requestor)

(๕.๗.๔) ผู้ดูแลด้าน IS (ISA: Information Security Administrator/System Administrator)

(๕.๗.๕) ผู้ตรวจสอบ (Auditor)

(๕.๘) สามารถควบคุมการขอใช้และกำหนดนโยบายการเปลี่ยนรหัสผ่านได้อย่างน้อยดังนี้

(๕.๘.๑) สามารถกำหนดลักษณะและนโยบายของ Password เช่น ความยาว และองค์ประกอบของ Password ที่มีตัวอักษร ตัวเลข อักขระพิเศษ

(๕.๘.๒) สามารถเปลี่ยนรหัสผ่านเมื่อถึงระยะเวลาที่กำหนดได้

(๕.๘.๓) สามารถเปลี่ยนรหัสผ่านทุกครั้งที่มีการขอใช้งาน

(๕.๘.๔) สามารถตรวจสอบและปรับปรุงรหัสผ่านให้ถูกต้องแบบอัตโนมัติ ในกรณีที่รหัสผ่านในอุปกรณ์ไม่ตรงกับที่เก็บบันทึกอยู่ในระบบ

(๕.๙) สามารถกำหนดให้มี Workflow ในลักษณะ Request – Approve ได้

(๕.๑๐) สามารถกำหนดจำนวนผู้อนุมัติ (Approver) ขั้นต่ำได้

(๕.๑๑) สามารถทำการแจ้งเตือนทางอีเมล์ในกระบวนการร้องขอ (Request) และอนุมัติ (Approve)

(๕.๑๒) สามารถระบุผู้มีสิทธิ์ในการ Approve ให้แตกต่างกันไปตามแต่ละ High Privileged Account Group ได้

(๕.๑๓) สามารถกำหนดสิทธิ์ในการเข้าใช้งาน High Privileged Account ให้แตกต่างกันไปตาม User Group ได้

(๕.๑๔) สามารถทำการ Reset Windows Service Account พร้อมเปลี่ยนรหัสผ่านให้แก่ Service Account ที่ถูกบริหารจัดการโดยระบบ Privileged Account Management ได้

(๕.๑๕) สามารถกำหนดนโยบายการขอเข้าใช้งาน High Privileged Account ให้แตกต่างกันตามช่วงระยะเวลา, วัน และ Network Zone ได้

(๕.๑๖) ผู้ร้องขอ (Requester) สามารถกำหนดนโยบาย ในการเข้าใช้งานได้ อย่างน้อยดังนี้

(๕.๑๖.๑) ช่วงเวลาการเข้าใช้งาน

(๕.๑๖.๒) ระยะเวลาในการขอใช้งาน

(๕.๑๖.๓) ระบบ หรืออุปกรณ์ที่เข้าใช้งาน

(๕.๑๗) สามารถเปิดใช้งาน Session ได้ไม่น้อยกว่า ๓๐๐ Concurrent sessions

(๕.๑๘) สามารถเปิด Session RDP และ SSH ได้โดยไม่จำเป็นต้องมีการติดตั้ง Java ที่เครื่องต้นทาง

(๕.๑๙) สามารถทำการ Monitor Session ที่กำลังถูกใช้งานอยู่ได้แบบ Real-time (Live Session Monitoring)

(๕.๒๐) สามารถทำการควบคุม Session ที่ถูกเปิดใช้งานได้อย่างน้อยดังต่อไปนี้

(๕.๒๐.๑) Lock Screen

(๕.๒๐.๒) Terminate Session

(๕.๒๐.๓) Terminate Session and Cancel Request

(๕.๒๑) สามารถทำ Black-Listing สำหรับ SSH Commands เพื่อป้องกันการรันคำสั่งที่ไม่อนุญาตบนระบบที่ควบคุม

(๕.๒๒) สามารถบันทึกหน้าจอในทุกการกระทำที่เปิดใช้งานผ่าน Session Management โดยบันทึกในรูปแบบของ Video Recording

(๕.๒๓) สามารถบันทึกการพิมพ์ของ Session ที่เปิดใช้งานได้ (Key Stroke Logger)

(๕.๒๔) สามารถค้นหา Session จากคำสั่งที่พิมพ์ และ ชื่อผู้ใช้งาน ได้เป็นอย่างน้อย

(๕.๒๕) สามารถทำงานร่วมกับ Windows Terminal Service ในรูปแบบของการทำ RemoteApp โดยสามารถกำหนด Application ที่จะถูกเปิดใช้งาน พร้อมกรอก Username และ Password ให้โดยอัตโนมัติ (Auto Fill)

(๕.๒๖) สามารถเปิดช่องทางให้ Hardcode Application หรือ Internal Development Application ทำการร้องขอรหัสผ่านได้ผ่านช่องทาง Web API ได้ไม่น้อยกว่า ๒๐๐ applications

(๕.๒๗) สามารถสแกนหาเครื่องแม่ข่าย (Asset Discovery) ที่มีอยู่ในองค์กรเพื่อนำมาบริหารจัดการได้

(๕.๒๘) สามารถสแกนข้อมูลช่องโหว่หรือ Vulnerability Scan เครื่องแม่ข่ายจำนวนไม่น้อยกว่า ๕๐๐ ระบบเพื่อนำข้อมูลที่ได้มาทำการวิเคราะห์ร่วมกับระบบ Privileged Account Management ถึงความเสี่ยงในการเข้าใช้งาน หรือ สามารถเสนอ Software อื่นๆที่มีการทำงานแบบสแกนข้อมูลช่องโหว่หรือ Vulnerability Scan โดยแยกการบริหารจัดการได้

(๕.๒๙) สามารถแสกนข้อมูลของเครื่องแม่ข่ายได้อย่างน้อยดังต่อไปนี้ IP address, DNS name, Hardware detail, Service, Port, Process ได้เป็นอย่างน้อย

(๕.๓๐) สามารถออกรายงานเป็น Schedule Report และรองรับการส่ง Mail ผลรายงานได้

(๕.๓๑) สามารถบันทึกรายงานในรูปแบบของ PDF, Excel, CSV, Word ได้

(๕.๓๒) สามารถทำงานร่วมกับระบบ Log Management ได้

(๕.๓๓) อุปกรณ์ที่เสนอ ต้องได้รับอนุญาตให้จำหน่ายในประเทศไทยอย่างถูกต้องตามกฎหมาย โดยจะต้องแนบหนังสือรับรองการแต่งตั้ง/หนังสืออนุญาตจากบริษัทผู้ผลิต หรือ ผู้ผลิตที่มีสาขา

ในประเทศไทยให้จำหน่ายในประเทศไทย โดยหนังสือนั้นต้องมีอายุไม่เกิน ๙๐ วัน นับถัดจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอประกวดราคา แนบไปพร้อมเอกสารการเสนอราคา

(๖) อุปกรณ์รักษาความปลอดภัยสำหรับเวป (Secure Web Gateway) จำนวน ๑ ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้

(๖.๑) เป็นอุปกรณ์ Appliance สามารถรองรับจำนวนผู้ใช้ได้พร้อมกันไม่น้อยกว่า ๒๕,๐๐๐ ผู้ใช้ (users)

(๖.๒) สามารถตรวจสอบ virus โดยใช้ฐานข้อมูล หรือ signature ของ Symantec, Kaspersky, McAfee หรือ Sophos ได้ และ มีลิขสิทธิ์ในการใช้งานไม่น้อยกว่า ๕,๐๐๐ คน โดยผู้เสนอสามารถเสนออุปกรณ์เพิ่มเติมภายนอกที่มี Internet Bandwidth ๑,๐๐๐ Mbps เพื่อทำคุณลักษณะดังกล่าวได้

(๖.๓) เป็นอุปกรณ์ Appliance ที่ถูกออกแบบมาเพื่อเพิ่มความเร็วการใช้งาน Web application

(๖.๔) Internet Bandwidth ไม่น้อยกว่า ๑,๐๐๐ Mbps

(๖.๕) มีขนาดของ Hard Disk ไม่น้อยกว่า ๑๖ TB

(๖.๖) มีหน่วยความจำ RAM ไม่น้อยกว่า ๑๒๘ GB

(๖.๗) เป็นแบบ Modular หรือ Chassis มีความยืดหยุ่นในการขยายและเปลี่ยนแปลงประเภทของ Network Interface Card ได้ มีจำนวน Slot ไม่น้อยกว่า ๒ Slot

(๖.๘) สามารถรองรับการทำ Link Aggregation ได้ โดยมีพอร์ต ๑๐ GBase-T จำนวนไม่น้อยกว่า ๔ พอร์ต และรองรับการเปลี่ยนเป็นพอร์ตแบบ ๑๐ Gb Fiber ได้ไม่น้อยกว่า ๔ พอร์ต

(๖.๙) มีระบบ Redundant Power Supply

(๖.๑๐) สามารถรองรับโปรโตคอล HTTP, HTTPS, FTP, TCP-Tunnel, และ Socks ได้เป็นอย่างน้อย

(๖.๑๑) สามารถทำ Authentication ร่วมกับ Active Directory (AD), LDAP, NTLM, Radius, Novell และ Local database ได้เป็นอย่างน้อย

(๖.๑๒) สามารถทำ Authentication แบบ Single Sign On หรือ Integrated Windows Authentication ร่วมกับ Active Directory ได้

(๖.๑๓) สามารถทำ VDO Optimization โดยใช้เทคนิค VDO Stream Splitting กับ Windows Media, Real, QuickTime และ โปรโตคอล RTSP ได้เป็นอย่างน้อย และสามารถขยายเพื่อรองรับการทำ VDO Stream Splitting กับโปรโตคอล RTMP และ RTMPE ได้

(๖.๑๔) สามารถทำ Time Quota และ Volume Quota ได้

(๖.๑๕) สามารถทำ Notification Page และ Exception Page ได้ และต้องอนุญาตให้ผู้ดูแลระบบสามารถทำการปรับปรุงเปลี่ยนแปลงข้อความรวมทั้งรูปภาพได้

(๖.๑๖) ระบบ Authentication ต้องสามารถกำหนดให้ผู้ใช้งาน log on ได้เพียงครั้งละ ๑ เครื่องได้ เพื่อป้องกันปัญหาการ share ชื่อล็อกอิน (user account)

(๖.๑๗) สามารถทำ URL/Web filtering ตามคุณลักษณะดังต่อไปนี้ได้เป็นอย่างน้อย

(๖.๑๗.๑) มีลิขสิทธิ์ในการทำ URL/Web filtering สำหรับผู้ใช้ไม่น้อยกว่า ๕,๐๐๐ คน

(๖.๑๗.๒) มีฐานข้อมูลของเว็บไซต์จัดเป็นประเภท (Category) ไม่น้อยกว่า ๘๔ ประเภท

(๖.๑๗.๓) สามารถทำการตรวจวิเคราะห์เว็บไซต์ที่ไม่มีในฐานข้อมูลได้แบบ Real Time โดยใช้เทคนิค Cloud Computing หรือ Cloud service ทำให้สามารถจัดประเภทของเว็บไซต์และตรวจสอบ Web link หรือ Content ที่ไม่ปลอดภัยได้โดยอัตโนมัติ

(๖.๑๗.๔) สามารถควบคุมพฤติกรรมการใช้งานเว็บไซต์ เช่น post message, send email, upload picture , upload video , upload attachment และ download attachment ได้เป็นอย่างน้อย

(๖.๑๘) สามารถแยกประเภทของ VDO บน Youtube (Youtube Categorization)

(๖.๑๙) สามารถรับความรู้ หรือ policy หรือ script จาก Cloud เพื่อทำให้สามารถ cache Web ๒.๐ หรือ Dynamic Web ได้

(๖.๒๐) สามารถทำ Static Code Analysis หรือ Predictive File Analysis ได้

(๖.๒๑) สามารถส่งต่อไฟล์ไปตรวจสอบยังอุปกรณ์ Sandboxing ได้

(๖.๒๒) สามารถทำหน้าที่เป็น Web Application Firewall หรือเสนออุปกรณ์อื่นเพิ่มเติมที่มีคุณลักษณะดังต่อไปนี้ได้

(๖.๒๒.๑) สามารถป้องกันการโจมตี Internal Web server โดยใช้ Signature ได้ (Signature based)

(๖.๒๒.๒) สามารถป้องกันการโจมตี Internal Web server แบบไม่ใช้ Signature ได้ (Signature less)

(๖.๒๒.๓) สามารถป้องกัน Internal Web Server จากภัยคุกคามและการโจมตีต่าง ๆ ตามที่ระบุโดย OWASP Top ๑๐ ได้

(๖.๒๒.๔) สามารถทำตรวจสอบ Virus ของไฟล์ที่จะ Upload ไปยัง Web server ได้

(๖.๒๓) ต้องผ่านการรับรองดังต่อไปนี้ FCC, ICES, RoHS, VCCI, UL, และ EN เป็นอย่างน้อย สามารถจัดทำรายงานได้โดยตัวอุปกรณ์ หรือเป็นโปรแกรมเสริมที่ติดตั้งภายนอกอุปกรณ์ โดยสามารถจัดทำรายงานอย่างน้อยดังนี้

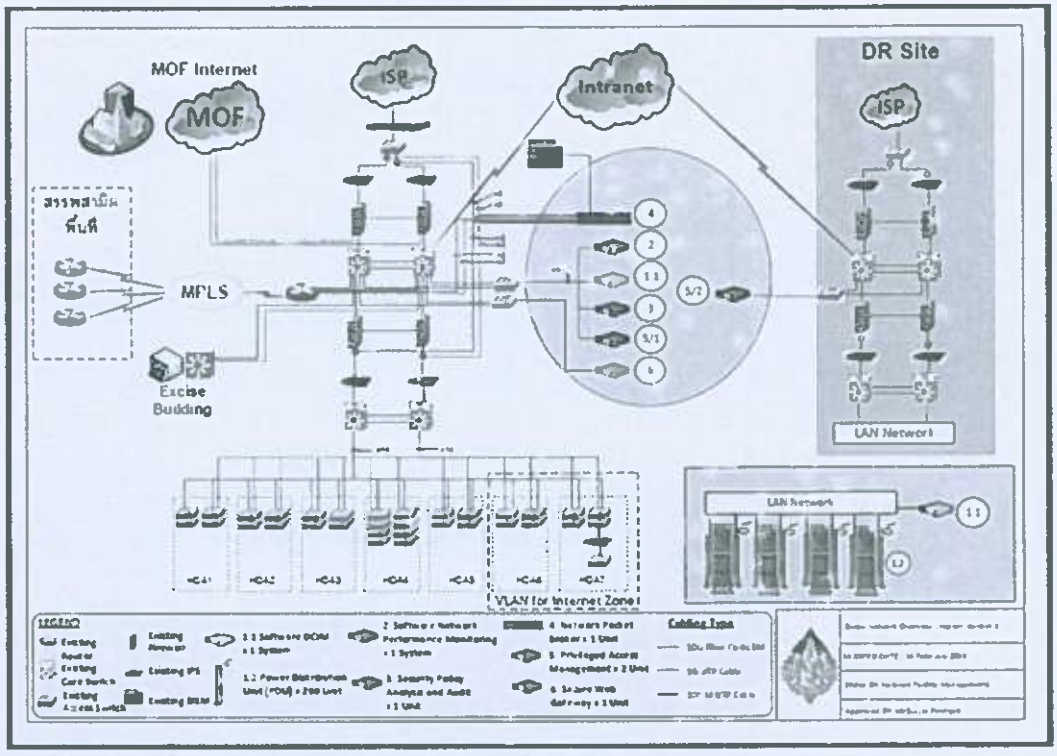
(๖.๒๓.๑) สามารถแสดง Top Users, Top Web Sites และ Top Categories ได้เป็นอย่างน้อย

(๖.๒๓.๒) สามารถกำหนดเวลาในการออกรายงานล่วงหน้า (Scheduling Report) และส่งรายงานผ่าน Email ได้

(๖.๒๔) อุปกรณ์ที่เสนอ ต้องได้รับอนุญาตให้จำหน่ายในประเทศไทยอย่างถูกต้องตามกฎหมาย โดยจะต้องแนบหนังสือรับรองการแต่งตั้ง/หนังสืออนุญาตจากบริษัทผู้ผลิต หรือ ผู้ผลิตที่มีสาขาในประเทศไทยให้จำหน่ายในประเทศไทย โดยหนังสือนั้นต้องมีอายุไม่เกิน ๙๐ วัน นับถัดจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอประกวดราคา แนบไปพร้อมเอกสารการเสนอราคา

๗. การออกแบบและติดตั้งระบบ

ผู้ชนะการประกวดราคาต้องดำเนินการติดตั้งระบบเพิ่มประสิทธิภาพระบบบริหารจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง (Data Center and DR Site Infrastructure Management (DCIM))และระบบรักษาความปลอดภัยข้อมูล และสายสัญญาณคอมพิวเตอร์ ให้ทำงานตามรูปภาพดังนี้



รูปที่ ๑ แสดงการเชื่อมโยงอุปกรณ์เพิ่มประสิทธิภาพระบบบริหารจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง (Data Center and DR Site Infrastructure Management (DCIM))และระบบรักษาความปลอดภัยข้อมูล

(๑) การติดตั้งระบบบริหารจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง (Data Center and DR Site Infrastructure Management (DCIM)) รายการที่ ๑ ให้ดำเนินการดังนี้

(๑.๑) โปรแกรมจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง จำนวน ๑ ชุด

(๑.๑.๑) ต้องติดตั้งโปรแกรมลงบนเครื่องที่กรมสรรพสามิตจัดไว้ให้

(๑.๑.๒) ต้องดำเนินการติดตั้งปรับจูนระบบให้สามารถทำงานได้อย่างมีประสิทธิภาพ

(๑.๑.๓) ต้องจัดทำภาพจำลอง Floor Layout ของกรมมสรรพสามิต ในมุมมองรูปแบบ ๓ มิติ

(๑.๑.๔) ทดสอบการทำงานของโปรแกรมจัดการศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง

(๑.๒) อุปกรณ์ Power Distribution Unit (PDU) จำนวน ๒๐๐ ชุด

(๑.๒.๑) ต้องติดตั้งที่ตู้ Rack ที่กรมสรรพสามิตจัดไว้ให้

(๑.๒.๒) ต้องสามารถทำงานร่วมกับอุปกรณ์เครือข่ายของกรมสรรพสามิตได้อย่างมีประสิทธิภาพ

(๒) ระบบวิเคราะห์ประสิทธิภาพการทำงานของอุปกรณ์เครือข่าย (Network Performance Monitoring) รายการที่ ๒ ให้ดำเนินการดังนี้

(๒.๑) โปรแกรมรายการที่ ๒ จำนวน ๑ ชุด

(๒.๑.๑) ต้องจัดเตรียมระบบเครือข่ายของกรมสรรพสามิต (System Preparation) และจัดเตรียม โดยขอข้อมูลจากลูกค้าดังนี้ Node Information, Zone, Rsc, PoP และขอ SMTP parameter สำหรับกรณีต้องการทำ Alert เพื่อให้เป็นไปตามความต้องการของกรมสรรพสามิต

(๒.๑.๒) ต้องติดตั้งซอฟแวร์ลงบนเครื่องที่กรมสรรพสามิตจัดไว้ให้ โดยพิจารณาการติดตั้งตามจำนวน Node และ Interface ให้สอดคล้องกับระบบเครือข่ายของกรมสรรพสามิต

(๒.๑.๓) ดำเนินการติดตั้งปรับจูนระบบวิเคราะห์ประสิทธิภาพการทำงานของอุปกรณ์เครือข่าย (Network Performance Monitoring)

(๒.๑.๔) ทดสอบการทำงานของซอฟแวร์ระบบวิเคราะห์ประสิทธิภาพการทำงานของอุปกรณ์เครือข่าย (Network Performance Monitoring)

(๓) อุปกรณ์ตรวจสอบและบริหารจัดการอุปกรณ์ไฟร์วอลแบบรวมศูนย์ (Centralize Firewall Management and Policy Analysis) รายการที่ ๓ ให้ดำเนินการดังนี้

(๓.๑) อุปกรณ์รายการที่ ๓ จำนวน ๑ ชุด

(๓.๑.๑) ต้องติดตั้งภายในตู้ Rack ที่กรมสรรพสามิตจัดไว้ให้

(๓.๑.๒) ต้องกำหนดค่าการทำงาน (Configuration) อุปกรณ์ให้สามารถทำงานร่วมกับอุปกรณ์ไฟร์วอลที่มีอยู่เดิมของกรมสรรพสามิตได้

(๓.๑.๓) ต้องทำการนำเข้าค่าการจัดการ (Firewall Policy) อุปกรณ์ไฟร์วอลที่มีอยู่เดิมของกรมสรรพสามิตได้

(๓.๑.๔) ต้องสามารถทำการตรวจสอบและวิเคราะห์อุปกรณ์ไฟร์วอลที่มีอยู่เดิมของกรมสรรพสามิตได้

(๔) อุปกรณ์บริหารจัดการข้อมูลในระบบเครือข่าย (Network Packet Broker) รายการที่ ๔ ให้ดำเนินการดังนี้

(๔.๑) อุปกรณ์รายการที่ ๔ จำนวน ๑ ชุด

(๔.๑.๑) ต้องติดตั้งภายในตู้ Rack ที่กรมสรรพสามิตจัดไว้ให้

(๔.๑.๒) ต้องดำเนินการกำหนดค่าการทำงาน (Configuration) IP Address ให้สามารถบริหารจัดการผ่านทาง Web-GUI และ Command Line Interface

(๔.๑.๓) ต้องเชื่อมโยงเครือข่ายจากอุปกรณ์ Core Switch และ Firewall

(๔.๑.๔) ต้องเชื่อมโยงเครือข่ายจากอุปกรณ์ Network Packet Broker และอุปกรณ์ IPS และ WAF

(๔.๑.๕) ต้องดำเนินกำหนดค่าการทำงาน (Configuration) ให้สามารถทำงานกับอุปกรณ์ IPS และ WAF ได้อย่างมีประสิทธิภาพ

(๔.๑.๖) ต้องดำเนินกำหนดค่าการทำงาน (Configuration) ให้สามารถถอดรหัสการรับส่งข้อมูล (SSL\TLS Decryption) และส่งข้อมูลไปยังอุปกรณ์ IPS และ WAF

(๕)อุปกรณ์บริหารจัดการรหัสผ่านและบริหารจัดการเซสชั่นการใช้งาน Privileged Access Management (PAM) สำหรับผู้ดูแลระบบ รายการที่ ๕ ให้ดำเนินการดังนี้

(๕.๑) อุปกรณ์รายการที่ ๕ จำนวน ๒ ชุด

(๕.๑.๑) ต้องติดตั้งภายในตู้ Rack ที่กรมสรรพสามิตจัดเตรียมไว้ให้

(๕.๑.๒) ต้องดำเนินการกำหนดค่า IP Address หรือค่าการทำงานอื่นๆ ตามที่กรมฯ กำหนด

(๕.๑.๓) ต้องดำเนินการกำหนดค่าการทำงาน (Configuration) ให้ทำงานในลักษณะมีความคงทนสูง (High Availability) ตามรูปแบบที่กำหนด

(๕.๑.๔) ต้องเตรียมการเชื่อมโยงเครือข่ายจากอุปกรณ์ Core Switch หรือจากอุปกรณ์ Distribute Switch เพื่อเชื่อมโยงเครือข่ายไปยังอุปกรณ์เครือข่ายศูนย์คอมพิวเตอร์หลักของกรมฯ และทำการกำหนดค่าการทำงาน (Configuration) ให้สามารถทำงานร่วมกันได้

(๖) อุปกรณ์รักษาความปลอดภัยสำหรับเวป (Secure Web Gateway) รายการที่ ๖ ให้ดำเนินการดังนี้

(๖.๑) อุปกรณ์รายการที่ ๖ จำนวน ๑ ชุด

(๖.๑.๑) ติดตั้งอุปกรณ์ขึ้น Rack พร้อม Configure ระบบเบื้องต้น (Network setting, Firmware upgrade, License installation, Connection testing)

(๖.๑.๒) ทำการอัปเดตฐานข้อมูลของอุปกรณ์ให้เป็นปัจจุบัน

(๖.๑.๓) สร้าง Best practice Policies สำหรับการใช้งานอุปกรณ์เบื้องต้น

(๖.๑.๔) ทดสอบการใช้งานของ User เมื่อเข้าใช้งานเว็บไซต์ผ่านอุปกรณ์

๗. การรับประกัน

๗.๑ ผู้รับจ้างต้องรับประกันความชำรุดบกพร่องของอุปกรณ์และระบบต่างๆ เป็นระยะเวลา ๑ ปี นับจากวันที่กรมสรรพสามิตได้ตรวจรับเป็นที่เรียบร้อยแล้ว

๗.๒ ระหว่างการรับประกันความชำรุดบกพร่อง และซ่อมแซมแก้ไขอุปกรณ์และระบบต่างๆ ผู้รับจ้างต้องรับประกันความชำรุดบกพร่อง และซ่อมแซมแก้ไขอุปกรณ์ดังกล่าว ให้เป็นไปตามมาตรฐานของเจ้าของผลิตภัณฑ์ในลักษณะ On-Site Service (เข้ามาตรวจสอบแก้ไข ณ กรมสรรพสามิตในกรณีที่เกิดการขัดข้องในการใช้งาน) โดยผู้รับจ้างจะต้องนำเสนอแผนและวิธีซ่อมแซมแก้ไขอุปกรณ์ และระบบต่างๆ มาพร้อมกับเอกสารข้อเสนอโครงการในครั้งนี้ด้วยเพื่อประกอบการพิจารณาของกรมสรรพสามิต

๗.๓ กรณีที่ระบบมีปัญหาหรือขัดข้อง ผู้รับจ้างต้องตอบรับทราบต่อการแจ้งเหตุและต้องทำการซ่อมแซมแก้ไขระบบหรือติดตั้งอุปกรณ์/ชิ้นส่วนสำรองมีประสิทธิภาพทัดเทียมกันมาใช้แทนให้อยู่ในสภาพใช้การได้ดีดังเดิม หรือสามารถใช้งานได้ตามปกติไม่เกิน ๔ ชั่วโมง (หลังจากรับแจ้งจากกรมสรรพสามิต)

๗.๔ กรณีผู้รับจ้างดำเนินการซ่อมแซมแก้ไขระบบโดยใช้อุปกรณ์/ชิ้นส่วนทดแทน ซึ่งแตกต่างจากอุปกรณ์เดิมที่นำเสนอ ผู้รับจ้างต้องดำเนินการซ่อมแซมแก้ไขอุปกรณ์/ชิ้นส่วนที่ชำรุดบกพร่องให้แล้วเสร็จภายใน ๗๒ ชั่วโมง ทั้งนี้ เมื่ออุปกรณ์/ชิ้นส่วนที่ชำรุดดังกล่าวได้รับการซ่อมแซมแก้ไขเป็นที่เรียบร้อยแล้ว ผู้รับจ้างต้องนำมาติดตั้งให้สามารถใช้งานได้ดีดังเดิม โดยระยะเวลาที่ใช้สำหรับการติดตั้งหรือเปลี่ยนอุปกรณ์ไม่เกิน ๓ ชั่วโมง