เอกสารหมายเลข ๒

รายละเอียดคุณลักษณะเฉพาะของอุปกรณ์ที่จัดซื้อ

รายละเอียดคุณลักษณะเฉพาะของอุปกรณ์ที่จัดซื้อ
โครงการเพิ่มประสิทธิภาพระบบป้องกันภัยคุกคามแบบต่อเนื่องขั้นสูง
สำหรับอาคารศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต

การจัดซื้อในครั้งนี้ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่จะใช้งานได้ทันทีและต้องเป็นรุ่นที่ยังอยู่ในสายการผลิต (Production Line) และจำหน่าย ณ วันยื่นข้อเสนอ โดยคุณลักษณะเฉพาะของ "ระบบป้องกันภัยคุกคามแบบต่อเนื่องขั้นสูงสำหรับอาคารศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต" จะต้องเหมาะสมกับลักษณะงานของกรมสรรพสามิตตามโครงการนี้ และสามารถทำงานร่วมกันและใช้งานร่วมกับระบบงานคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ สะดวกต่อการใช้งาน โดยผู้ประสงค์จะเสนอราคาต้องเสนอระบบเครือข่ายสื่อสารและระบบความปลอดภัยเครือข่ายที่มีคุณลักษณะเฉพาะไม่ต่ำกว่าที่ระบุในเอกสารนี้

เงื่อนไขทั่วไปในการติดตั้ง

ผู้ชนะการประกวดราคาต้องจัดหาอุปกรณ์หรือซอฟต์แวร์ที่จำเป็นสำหรับการทำงาน ให้สามารถทำงานได้อย่างสมบูรณ์ โดยไม่คิดมูลค่าเพิ่มเติมจากราคา ที่เสนอ

(๑) ระบบป้องกันเครือข่ายขั้นสูง จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

(๑.๑) อุปกรณ์ป้องกันเครือข่าย (Security Gateway) จำนวน ๒ ชุด โดยมีคุณลักษณะ อย่างน้อยดังนี้

(๑.๑.๑) เป็น Firewall Appliance ที่ใช้เทคโนโลยีแบบ Stateful Inspection และมี Firewall Throughput ไม่น้อยกว่า ๕๐ Gbps

(๑.๑.๒) มีThreat prevention throughput ๕ Gbps

(๑.๑.๓) สามารถรองรับ Concurrent Connections อย่างน้อย ๖,๔๐๐,๐๐๐ Connections และ New sessions/connection per second ไม่น้อยกว่า ๓๐๐,๐๐๐ sessions per second

(๑.๑.๔) มีพอร์ตแบบ ๑๐/๑๐๐/๑๐๐๐ Base-T จำนวนไม่น้อยกว่า ๘ พอร์ต และแบบ ๑๐Base-F SFP+ จำนวนไม่น้อยกว่า ๔ พอร์ต พร้อมเสนอโมดูล SR Transceiver จำนวน ๔ โมดูล

(๑.๑.๕) มี Storage บนตัวอุปกรณ์ไม่น้อยกว่า ๔๐๐ GB และหน่วยความจำไม่น้อยกว่า ๑๖ GB

(๑.๑.๖) สามารถตรวจสอบและควบคุม Applications ได้อย่างน้อย ๒,๐๐๐ Applications

(๑.๑.๗) สามารถกำหนด Security Policy ตาม User, User Group ด้วยการ Integrate เข้ากับ Active Directory ได้โดยไม่ต้องติดตั้งซอฟต์แวร์ (Agent) เพิ่มเติมบน Domain Controller หรือเครื่องของผู้ใช้งานรวมทั้งสามารถทำการ Authentication ผ่าน Browser ได้สำหรับผู้ใช้งานที่ไม่ได้อยู่ใน Domain ขององค์กร

(๑.๑.๘) สามารถใช้งาน Routing แบบ Dynamic Routing ได้แก่ OSPF, BGP, RIP v๑/๒, IGMP และ PIM ได้เป็นอย่างน้อย

(๑.๑.๙) สามารถทำงานตามมาตรฐาน IPv ๖ ได้

(๑.๑.๑๐) สามารถทำงานในลักษณะ Link Redundancy ได้ทั้งแบบ Primary/Backup และ Load Sharing โดยสามารถใช้ประสิทธิภาพของ Link เป็นตัวกำหนด หรือสามารถนำเสนออุปกรณ์อื่นเพิ่มเติมเพื่อทำงานได้ตามข้อกำหนด

(๑.๑.๑๑) สามารถทำงานเป็น Intrusion Prevention System (IPS) ได้โดยจะต้องมีพื้นฐานการทำงานในการป้องกันภัยคุกคามได้แก่ Known exploit, vulnerability, outbound malware communication เป็นอย่างน้อย

(๑.๑.๑๒) สามารถตรวจจับ Virus โดยป้องกันการดาวโหลดไฟล์ที่มีมัลแวร์และตรวจสอบไฟล์ที่มีการมีการย่อขนาดไฟล์ได้อย่างน้อยดังนี้ zip,gzip,rar และ tar

(๑.๑.๑๓) สามารถตรวจจับ Bot โดยวิธีการตรวจสอบจาก C&C address หรือ website ได้เป็นอย่างน้อย

(๑.๑.๑๔) สามารถป้องกัน Spam ที่มาในรูปแบบของ Email ผ่านโปรโตคอล POP๓ และ SMTP และสามารถป้องกันโดยใช้รูปแบบ IP reputation anti-spam และ Block list anti-spam ได้ หรือสามารถนำเสนออุปกรณ์อื่นเพิ่มเติมเพื่อทำงานได้ตามข้อกำหนด

(๑.๑.๑๕) สามารถตรวจจับและป้องกันภัยคุกคามแบบ Zero-day โดยสามารถทำงานร่วมกับอุปกรณ์แบบ on premise หรือ local Sandboxing หรือ local emulation appliance ที่นำเสนอในโครงการได้

(๑.๑.๑๖) สามารถทำ High Availability แบบ active/passive หรือ active/active ได้เป็นอย่างน้อย

(๑.๑.๑๗) สามารถจัดการแบบศูนย์กลาง (Centralized Management) ผ่านระบบบริหารจัดการแยกต่างหากจากอุปกรณ์ป้องกันเครือข่าย Security Gateway ที่นำเสนอได้

(๑.๑.๑๘) สามารถจัดการระบบผ่านทาง SSH หรือ Application GUI หรือ Web-based ได้

(๑.๑.๑๙) มีแหล่งจ่ายไฟจำนวนไม่น้อยกว่า ๒ หน่วย แบบ Redundant Hot-Swappable

(๑.๑.๒๐) อุปกรณ์ที่นำเสนอต้องผ่านมาตรฐาน FCC และ UL

(๑.๒) อุปกรณ์ป้องกันภัยคุกคามขั้นสูงแบบต่อเนื่อง (Sandbox) จำนวน ๑ ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้

(๑.๒.๑) ต้องเป็นแบบ Hardware Appliance ที่ออกแบบมาเพื่อทำหน้าที่ป้องกันภัยคุกคามแบบ Zero-Day ได้

(๑.๒.๒) ต้องมี Throughput ไม่น้อยกว่า ๔ Gbps หรือสามารถตรวจสอบไฟล์บน VM ของ Sandbox จำนวนไม่น้อยกว่า ๓,๓๐๐ ไฟล์ต่อชั่วโมง หรือสามารถเสนออุปกรณ์มากกว่า ๑ ชุดเพื่อรองรับจำนวนไฟล์ได้ตามที่กำหนด

(๑.๒.๓) ต้องมี Interface แบบ ๑๐/๑๐๐/๑๐๐๐Base-T จำนวนไม่น้อยกว่า ๔ พอร์ต

(๑.๒.๔) สามารถทำงานตามมาตรฐาน IPV ๖ ได้

(๑.๒.๕) ต้องมีหน่วยจัดเก็บข้อมูล (Hard disk) ขนาดรวมไม่น้อยกว่า ๒ TB หลังจากการทำ RAID ๑๐ (ใช้สำหรับการคำนวณขนาด Storage เท่านั้น)

(๑.๒.๖) สามารถตรวจสอบไฟล์บนระบบที่ทำงานในลักษณะ Virtual Execution หรือ Virtual Machine ที่ไม่ใช่ VMWare และ Microsoft Adapter ได้ไม่น้อยกว่า ๔๐ ชุดพร้อม ๆ กัน หรือสามารถนำเสนออุปกรณ์มากกว่า ๑ ชุดเพื่อรองรับจำนวน virtual machine ที่กำหนดได้

(๑.๒.๗) ระบบ Virtual Execution หรือ Virtual Machine สามารถทำงานบนระบบปฏิบัติการได้แก่ Windows ๗ หรือ Windows ๘.๑ หรือ Windows ๑๐ ได้เป็นอย่างน้อย ทั้งนี้ต้องมีระบบปฏิบัติการที่มีลิขสิทธิ์ ถูกต้องตามกฎหมายสำหรับ Virtual Machine ที่ใช้ในการตรวจสอบไฟล์มาพร้อมกับระบบที่นำเสนอ

(๑.๒.๘) สามารถตรวจสอบไฟล์ที่ส่งผ่านโปรโตคอล HTTP, SMTP ได้เป็นอย่างน้อย

(๑.๒.๙) สามารถตรวจสอบไฟล์ในรูปแบบ (File Types) ดังต่อไปนี้ได้เป็นอย่างน้อย

๑) Microsoft Office ได้แก่ DOC, DOCX, XLS, XLSX, PPT และ PPTX

๒) PDF (Adobe Acrobat Document)

๓) EXE (Executable File)

๔) HTML (Hyper Text Mark Language)

๕) RTF (Rich Text Format File)

๖) SWF (Flash Player File)

๗) JAR (Java Archive File)

(๑.๒.๑๐) สามารถตรวจจับพฤติกรรมของเครื่องที่ติด Bot และป้องกันความเสียหายที่อาจเกิดขึ้นจากการติดต่อระหว่างเครื่องของผู้ใช้งานที่ติด Bot ไปยัง Command & Control Server ได้

(๑.๒.๑๑) กรณีตรวจสอบพบไฟล์ที่ผิดปกติซึ่งเป็น unknown attack แล้วสามารถสร้าง Signature ขึ้นมาใหม่และ อัพเดทบนระบบฐานข้อมูลได้

(๑.๒.๑๒) สามารถออกรายงาน (Report) เมื่อตรวจพบไฟล์ที่มีพฤติกรรมผิดปกติ (Malicious) โดยในรายงานต้องมีรายละเอียดอย่างน้อยดังนี้

๑) File Details

๒) Abnormal Activity หรือ Threat by Host

(๑.๒.๑๓) สามารถสร้าง Signature สำหรับ malware ใหม่ ที่ยังไม่เคยถูกค้นพบ (Zero-day malware) ได้แบบอัตโนมัติจากอุปกรณ์ที่นำเสนอไปยังอุปกรณ์เครือข่าย (Security Gateway)

(๑.๒.๑๔) สามารถบริหารจัดการผ่านระบบจัดการแบบศูนย์กลาง (Centralize Management) ที่นำเสนอ ได้หรือสามารถบริหารจัดการผ่านตัวอุปกรณ์ได้

(๑.๒.๑๕) มีแหล่งจ่ายไฟจำนวนไม่น้อยกว่า ๒ หน่วย แบบ Redundant Hot-Swappable

(๑.๒.๑๖) อุปกรณ์ที่นำเสนอต้องผ่านมาตรฐาน FCC และ UL

(๑.๓) ระบบจัดการแบบศูนย์กลาง (Centralize Management) สำหรับระบบป้องกันเครือข่ายชั้นสูง จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

(๑.๓.๑) เป็นซอฟต์แวร์ระบบบริหารจัดการที่มีระบบปฏิบัติการแบบเฉพาะที่ทำการ Hardening เรียบร้อยแล้ว

(๑.๓.๒) สามารถบริหารจัดการอุปกรณ์ Security Gateway ได้อย่างน้อย ๕ Gateways

(๑.๓.๓) สามารถกำหนดสิทธิ์และระดับความสำคัญให้กับผู้ดูแลระบบที่จะเข้ามาใช้งานอุปกรณ์ได้

(๑.๓.๔) สามารถใช้งาน Search Logging ได้

(๑.๓.๕) สามารถแสดงสถิติการใช้งาน (Hit Count Statistic) ของแต่ละ Policy ได้

(๑.๓.๖) สามารถจัดการ security policy ต่าง ๆ และจัดเก็บ Log ได้ทั้งแบบ real time และตรวจสอบย้อนหลัง

(๑.๓.๗) สามารถแสดงข้อมูลจากการวิเคราะห์เหตุการณ์ต่าง ๆ ในลักษณะของ Timelines หรือ Charts หรือ Maps ได้ เป็นอย่างน้อย

(๑.๓.๘) สามารถจัดทำรายงานแบบ Predefined Report ได้แก่รายงานประเภท Virus Report, Application และ URL Filtering Report ได้เป็นอย่างน้อย หรือสามารถปรับแต่ง (customize) รายงานเพิ่มเติมได้

(๑.๓.๙) สามารถกำหนดช่วงเวลาที่ต้องการให้สร้างและแสดงผลรายงานได้ (scheduled report) และกำหนดให้ส่งรายงานผ่านทาง Email ได้เป็นอย่างน้อย

(๑.๓.๑๐) สามารถติดตั้งกับคอมพิวเตอร์แม่ข่ายที่ทางกรมสรรพสามิตจัดหาให้ได้

(๑.๔) โปรแกรมรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์ผู้ใช้งาน (Next Generation Endpoint Security) จำนวน ๑ ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้

(๑.๔.๑) สามารถติดตั้ง (Agent) บนระบบปฏิบัติการ เช่น Windows ๗, Windows ๘, Windows ๑๐ ทั้งแบบ ๓๒ บิต และ ๖๔ บิต และ Mac OS

(๑.๔.๒) มีลิขสิทธิ์ (License) ที่จะสามารถนำไปใช้ติดตั้งใช้งานได้ไม่น้อยกว่า ๖,๐๐๐ เครื่อง โดยมีเอกสารรับรองจากเจ้าของผลิตภัณฑ์และสามารถ Update Signature ได้ตลอดระยะเวลา ๑ ปี

(๑.๔.๓) มีระบบบริหารจัดการนโยบายจากส่วนกลาง (Policy Management) ผ่าน web console หรือ GUI ได้ และสามารถทำรายงานสรุปให้ผู้ดูแลระบบและผู้บริหารได้

(๑.๔.๔) สามารถกำหนดสิทธิ์ของผู้ดูแลระบบในระดับที่แตกต่างกันด้วยสิทธิ์ที่ต่างกันได้ (Role-based Administration)

(๑.๔.๕) รองรับการตรวจสอบไฟล์ผ่านระบบ Sandbox ที่นำเสนอได้

(๑.๔.๖) สามารถตรวจสอบและป้องกันการทำงานของโปรแกรมไม่พึงประสงค์ (Malware) บนเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint) โดยมีคุณลักษณะดังนี้

๑) การโจมตีของมัลแวร์ที่ยังไม่เป็นที่รู้จัก (Zero-day attack)

๒) การโจมตีผ่านทาง memory เช่น buffer overflow

๓) การโจมตีผ่านทาง Power shell หรือ script attacks

(๑.๔.๗) สามารถป้องกันการโจมตี application ที่มีใช้งานบนเครื่องคอมพิวเตอร์

(๑.๔.๘) สามารถทำ host quarantine เมื่อตรวจพบ suspicious และ Compromised บนเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint) ได้

(๒.) ระบบรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์แม่ข่าย จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

(๒.๑) โปรแกรมตรวจจับและป้องกันการโจมตีผ่านช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่าย จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

(๒.๑.๑) สามารถทำงานบนระบบปฏิบัติการ ได้เป็นอย่างน้อยดังนี้

๑) Microsoft Windows Server ๒๐๐๘ R๒

๒) Microsoft Windows Server ๒๐๑๒

๓) Microsoft Windows Server ๒๐๑๖

๔) Solaris

๕) Linux

(๒.๑.๒) มีลิขสิทธิ์ (License) ที่จะสามารถนำไปใช้ติดตั้งใช้งานได้ไม่น้อยกว่า ๓๐๐ เครื่อง/VM โดยมีเอกสารรับรองจากเจ้าของผลิตภัณฑ์ และสามารถ Update Signature ได้ตลอดระยะเวลา ๑ ปี

(๒.๑.๓) รองรับการติดตั้งแบบ Virtual บน VMware, Citrix และ Microsoft HyperV

(๒.๑.๔) สามารถป้องกัน Virtual machines จากภัยคุกคามต่าง ๆ ได้อย่างน้อยดังนี้ Virus, Malware, Spyware, Bots, Key loggers, Root kits, Dialers, Adware, Trojans, Worm และ advanced threats ได้

(๒.๑.๕) สามารถทำงานรักษาความปลอดภัยในลักษณะ Firewall เพื่อป้องกันการโจมตีมายังเครื่องพิวเตอร์แม่ข่าย โดยการบริหารจัดการ policy จากระบบจัดการแบบศูนย์กลาง (Centralize Management)

(๒.๑.๖) มีระบบ Intrusion Prevention สำหรับป้องกัน unknown หรือ zero day หรือ vulnerability exploits ได้

(๒.๑.๗) ป้องกันการโจมตีในรูปแบบของ TCP/IP, DDoS Attacks และ Botnet ได้

(๒.๑.๘) สามารถตรวจจับ, ป้องกัน และแจ้งเตือนอันตรายจากภัยต่าง ๆ จากโปรแกรมไม่พึงประสงค์ (Malware) โดยใช้เทคนิค

๑) Signature Base

๒) Behavior base

๓) Machine-learning

(๒.๑.๙) สามารถสแกนไฟล์ในรูปแบบ Compressed (zip ,gzip ,rar และ tar) ,Executable files, JavaScript, VBScript และ Macro ได้

(๒.๒) ระบบจัดการแบบศูนย์กลาง (Centralize Management) สำหรับระบบรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์แม่ข่าย จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

(๒.๒.๑) สามารถติดตั้งบนระบบปฏิบัติการ Windows Server ๒๐๑๒ หรือ Windows Server ๒๐๑๒ R๒ หรือ Windows Server ๒๐๑๖ ได้

(๒.๒.๒) สามารถการทำงานร่วมกับ Database ของ Microsoft SQL Server ๒๐๑๒ หรือ ๒๐๑๒R๒ ได้ หรือ Database อื่นที่ใช้ในการเก็บข้อมูลในระบบได้

(๒.๒.๓) มีความสามารถในการบริหารและจัดการลิขสิทธิ์ (License)

(๒.๒.๔) สามารถทำการแจ้งเตือนผู้ดูแลระบบในกรณีที่ตรวจพบปัญหาด้วย email ได้เป็นอย่างน้อย

(๒.๒.๕) มีระบบการจัดการจากส่วนกลางเป็นแบบ Web-Base Management ด้วยมาตรฐาน HTTPS

(๒.๒.๖) สามารถติดตั้งตั้งโปรแกรมไปยังเครื่องแม่ข่ายได้ ด้วยวิธี Remote Install หรือ Client Package หรือ URL Install

(๒.๒.๗) สามารถแสดงข้อมูลจากการวิเคราะห์เหตุการณ์ต่าง ๆ และแนวโน้มของเหตุการณ์ ในลักษณะของ Timelines หรือ Charts หรือ Maps ได้ เป็นอย่างน้อย

(๒.๒.๘) สามารถสร้างรายงานได้ในรูปแบบ PDF, CSV หรือ HTML ได้เป็นอย่างน้อย รวมทั้งสามารถปรับแต่ง (customize) รายงานเพิ่มเติมได้

(๒.๒.๙) สามารถกำหนดช่วงเวลาที่ต้องการให้สร้างและแสดงผลรายงานได้ (scheduled report) และกำหนดให้ส่งรายงานผ่านทาง Email ได้เป็นอย่างน้อย

(๒.๒.๑๐) สามารถติดตั้งกับคอมพิวเตอร์แม่ข่ายที่ทางกรมสรรพสามิตจัดหาให้ได้

(๓) อุปกรณ์ DWDM สำหรับติดตั้งเชื่อมโยงระบบเครือข่ายระหว่าง DC กับ DR จำนวน ๒ ชุด โดยมีคุณลักษณะอย่างน้อย ดังนี้

(๓.๑) สามารถเชื่อมต่อ และส่งผ่านสัญญาณผ่านสายใยแก้วนำแสง ระหว่างศูนย์ข้อมูล และศูนย์สำรอง จำนวน ๒ เส้นทางอย่างมีประสิทธิภาพ

(๓.๒) มีลักษณะเป็น Modular Chassis มีจำนวน Service Slot ไม่น้อยกว่า ๖ Slots และ สามารถติดตั้งบน RACK ขนาด ๑๙ นิ้วได้

(๓.๓) ต้องมี Wavelength ในการใช้งานเป็นจำนวนไม่น้อยกว่า ๘ Wavelength ในแบบ Protection และ ๑๖ Wavelength ในแบบ Un-Protection และต้องสามารถขยายได้ไม่น้อยกว่า ๔๐ Wavelength

(๓.๔) ต้องมีพอร์ตที่สามารถเชื่อมต่อกับอินเตอร์เฟซได้เป็นอย่างน้อยดังนี้

๑) Gigabit Ethernet แบบ ๑๐GE จำนวนไม่น้อยกว่า ๔ พอร์ต

๒) Fiber Channel แบบ ๑๖G Fiber Channel Single Mode จำนวนไม่น้อยกว่า ๒ พอร์ต

(๓.๕) ต้องสามารถทำ Wavelength Tunable ได้

(๓.๖) ต้องมีระบบ Path Protection โดยสามารถ สลับจาก Main Path ในกรณี ที่ Fiber ขาดไปสู่ Protection Path ได้ภายใน ๕๐ ms

(๓.๗) ต้องรองรับ Reconfigurable OADM Technology ได้

(๓.๘) ต้องมี Optical Supervisory Channel สำหรับเป็นช่องทางในการสื่อสารระหว่าง Node

(๓.๙) ต้องเสนออุปกรณ์ Amplifier มาด้วย โดยอุปกรณ์ Amplifier ที่นำเสนอจะต้องสามารถใส่อยู่ใน Chassis เดียวกันได้

(๓.๑๐) ต้องสามารถทำ Hot Swap ในอุปกรณ์ที่ใช้ในการส่งสัญญาณ และควบคุมการส่งสัญญาณได้โดยไม่ต้องหยุดการทำงาน

(๓.๑๑) ต้องสามารถปิดการทำงานของเลเซอร์ได้โดยอัตโนมัติ (Automatic Laser Shutdown ALS) เมื่อเกิดเหตุขัดข้อง เนื่องจากสายสัญญาณ

(๓.๑๒) ในกรณีที่มีการเพิ่ม Wavelength เข้าไปในระบบ หรือสายใยแก้วนำแสงขาด อุปกรณ์จะต้องทำการควบคุม Optical Power ได้เองโดยอัตโนมัติ

(๓.๑๓) สามารถทำงานภายใต้อุณหภูมิระหว่าง ๐ ถึง๔๐ องสาเซลเซียส และความชื้นสัมพัทธระหว่าง ๕ ถึง ๘๕% ได้ดี

(๓.๑๔) มีแหล่งจ่ายไฟจำนวนไม่น้อยกว่า ๒ หน่วย แบบ Redundant Hot-Swappable

(๓.๑๕) ต้องผ่านการรับรองมาตรฐานคุณภาพดังต่อไปนี้

(๓.๑๕.๑) รองรับมาตรฐานความปลอดภัย UL ๑๙๕๐ และ IEC ๖๐๙๕๐

(๓.๑๕.๒) รองรับมาตรฐานการป้องกันการรบกวนของคลื่นแม่เหล็กไฟฟ้า EN๕๕๐๒๒

(๓.๑๕.๓) ต้องมีระยะห่างระหว่าง Wavelength ตามมาตรฐาน ITU-T Standard (ITU Grid Channels Spacing)

(๓.๑๖) ต้องสามารถเชื่อมโยงข้อมูลได้ระยะทางไม่น้อยกว่า ๘๐ กิโลเมตร

(๓.๑๗) ถ้าต้องมีอุปกรณ์เพิ่มสำหรับการขยายสัญญาณ จะต้องเสนอมาด้วย

(๔) วงจรเช่าคู่สาย Fiber Optic (Dark Fiber) เชื่อมโยงระบบเครือข่ายระหว่าง DC กับ DR จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

(๔.๑) คู่สาย Fiber Optic (Dark Fiber) เชื่อมโยงระหว่าง DC – DR ของกรมสรรพสามิต จำนวน ๒ เส้นทาง ที่มีเส้นทางการเดินสาย Fiber Optic ต่างกันอย่างชัดเจนรองรับการทำ Active/Standby

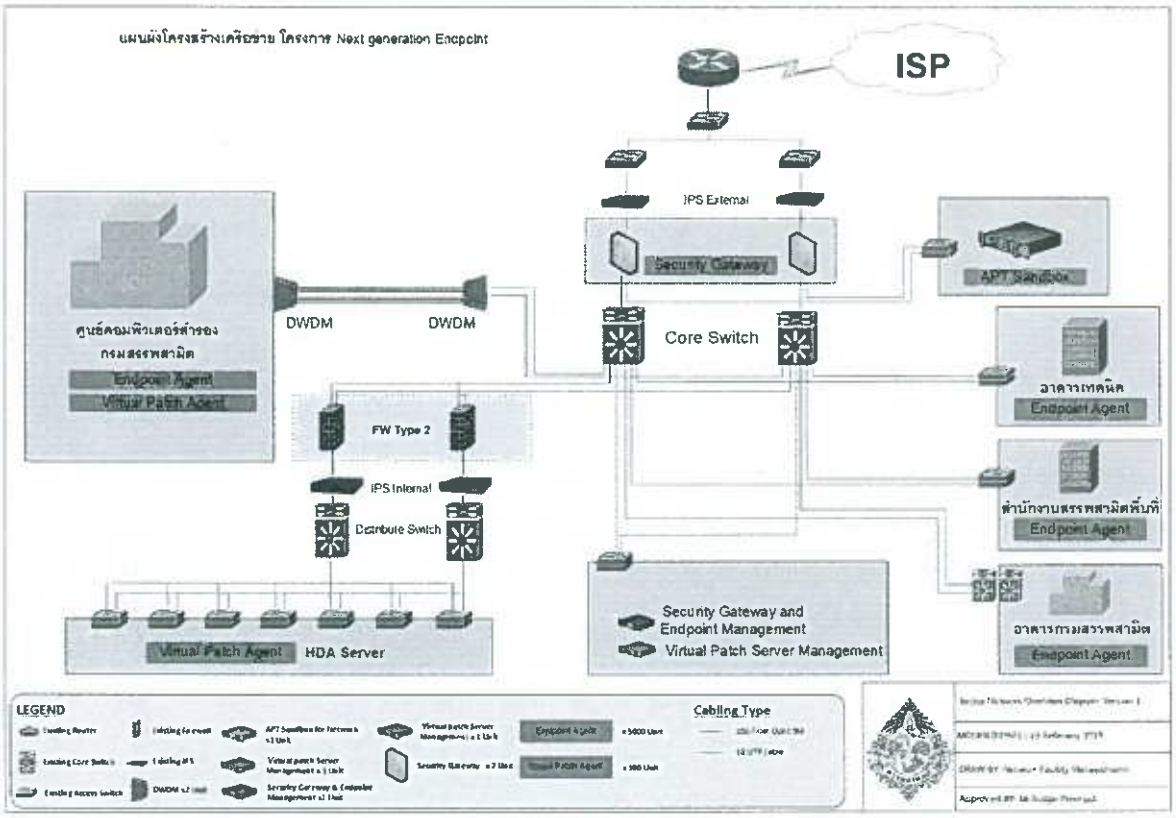
(๔.๒) สาย Fiber optic ที่ใช้ติดตั้ง เป็นสายชนิด Single Mode ความต้องการใช้งาน ๒ แกนต่อ ๑ เส้นทาง

(๔.๓) สามารถเชื่อมต่อกับอุปกรณ์ DWDM ที่นำเสนอมาได้

(๔.๔) ระยะเวลาในการเช่า ๑ ปี

๗. การออกแบบและติดตั้งระบบ

ผู้ชนะการประกวดราคาต้องดำเนินการติดตั้งระบบป้องกันภัยคุกคามแบบต่อเนื่องขั้นสูง สำหรับอาคารศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต และสายสัญญาณคอมพิวเตอร์ ให้ทำงานตามรูปภาพดังนี้



รูปที่ ๑ แสดงแนวคิดของการเชื่อมโยงในโครงการเพิ่มประสิทธิภาพระบบป้องกันภัยคุกคามแบบต่อเนื่องขั้นสูง สำหรับอาคารศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต

(๑) ระบบป้องกันเครือข่ายขั้นสูง จำนวน ๑ ระบบ รายการที่ ๑ ให้ดำเนินการดังนี้

(๑.๑) กำหนดค่า Configuration ตั้งต้น ซึ่งรวมถึงแผนผัง Diagram, Port Interface, VLAN, IP Address, Route, Policy, Authentication และค่าสำคัญในการเชื่อมอุปกรณ์ใหม่และอุปกรณ์ปัจจุบันของกรมฯ

(๑.๒) ประชุมชี้แจงแผนงานการเข้าติดตั้งอุปกรณ์, การกำหนดค่า Configuration, การทดสอบ และเอกสารของงานติดตั้ง หรือส่งแผนงานให้กรมฯ อนุมัติ

(๑.๓) ดำเนินการติดตั้ง เชื่อมโยงอุปกรณ์ และทดสอบ

(๑.๔) ตรวจสอบการใช้งานจากข้อมูลรับส่งบนอุปกรณ์ และปรับแต่งนโยบายการทำงานต่าง ๆ ให้เป็นไปตามความต้องการของทางกรมสรรพสามิต

(๒) ระบบรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์แม่ข่าย จำนวน ๑ ระบบ รายการที่ ๒ ให้ดำเนินการดังนี้

(๒.๑) กำหนดค่า Configuration ตั้งต้น ซึ่งรวมถึงแผนผัง Diagram, Port Interface, VLAN, IP Address และค่าสำคัญของอุปกรณ์

(๒.๒) ประชุมชี้แจงแผนงานการเข้าติดตั้งอุปกรณ์, การกำหนดค่า Configuration, การทดสอบ หรือส่งแผนงานให้กรมฯ อนุมัติ

(๒.๓) ดำเนินการติดตั้ง, เพิ่ม Sever เข้าระบบจัดการ และทดสอบ

(๓) อุปกรณ์ DWDM สำหรับติดตั้งเชื่อมโยงระบบเครือข่ายระหว่าง DC กับ DR จำนวน ๒ ชุด รายการที่ ๓ ให้ดำเนินการดังนี้

(๓.๑) ส่งมอบพร้อมติดตั้ง

(๓.๒) ปรับแต่งอุปกรณ์

(๓.๓) ทดสอบประสิทธิภาพร่วมกับสายนำส่งสัญญาณใยแก้วนำแสง

(๔) วงจรเช่าคู่สาย Fiber Optic (Dark Fiber) เชื่อมโยงระบบเครือข่ายระหว่าง DC กับ DR จำนวน ๑ ระบบ ชุด รายการที่ ๓ ให้ส่งมอบ และทดสอบระบบสัญญาณ

(๕) ผู้เสนอราคาจะต้องจัดหาเครื่องคอมพิวเตอร์แม่ข่ายพร้อมซอฟต์แวร์ลิขสิทธิ์ (OS และ DBMs) ที่มีคุณลักษณะตามคำแนะนำ (recommendation) ของผู้ผลิต เพื่อใช้ในการทดสอบการใช้งานของ Centralize Management ของรายการ (๑.๓) และ (๒.๒) จนจบโครงการฯ

๗. การรับประกัน

๗.๑ ผู้รับจ้างต้องรับประกันความชำรุดบกพร่องของอุปกรณ์และระบบต่าง ๆ เป็นระยะเวลา ๑ ปี นับจากวันที่กรมสรรพสามิตได้ตรวจรับเป็นที่เรียบร้อยแล้ว

๗.๒ ระหว่างการรับประกันความชำรุดบกพร่อง และซ่อมแซมแก้ไขอุปกรณ์และระบบต่าง ๆ ผู้รับจ้างต้องรับประกันความชำรุดบกพร่อง และซ่อมแซมแก้ไขอุปกรณ์ดังกล่าว ให้เป็นไปตามมาตรฐานของเจ้าของผลิตภัณฑ์ในการเข้ามาดำเนินการแก้ไขซ่อมแซมอุปกรณ์ (On-site Service) (เข้ามาตรวจสอบแก้ไข ณ กรมสรรพสามิตในกรณีที่เกิดการขัดข้องในการใช้งาน) โดยผู้รับจ้างจะต้องนำเสนอแผนและวิธีซ่อมแซมแก้ไขอุปกรณ์ และระบบต่าง ๆ มาพร้อมกับเอกสารข้อเสนอโครงการในครั้งนี้ด้วยเพื่อประกอบการพิจารณาของกรมสรรพสามิต

๗.๓ กรณีที่ระบบมีปัญหาหรือขัดข้อง ผู้รับจ้างต้องตอบรับทราบต่อการแจ้งเหตุและต้องทำการซ่อมแซมแก้ไขระบบหรือติดตั้งอุปกรณ์/ชิ้นส่วนสำรองมีประสิทธิภาพทัดเทียมกันมาใช้แทนให้อยู่ในสภาพใช้การได้ดีดังเดิม หรือสามารถใช้งานได้ตามปกติไม่เกิน ๔ ชั่วโมง (หลังจากรับแจ้ง จากกรมสรรพสามิต)

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