รายละเอียดคุณลักษณะเฉพาะพัสดุ

ครุภัณฑ์สำหรับระบบป้องกันเครือข่ายและระบบป้องกันการโจมตีแอพพลิเคชั่น จำนวน 1 ระบบ ประกอบด้วย

1. ระบบป้องกันการบุกรุกระบบเครือข่าย จำนวน ๑ ระบบ
2. ระบบตรวจสอบตัวตนเพื่อเข้าใช้เครือข่ายคอมพิวเตอร์ จำนวน ๑ ระบบ
3. ระบบป้องกันการโจมตีแอพพลิเคชั่น จำนวน ๑ ชุด
4. เครื่องคอมพิวเตอร์แม่ข่ายประมวลผลรองรับระบบ Virtualization จำนวน ๑ ชุด
5. อุปกรณ์กระจายสัญญาณไร้สาย จำนวน ๑๐ ชุด
6. ระบบควบคุมการทำงานอุปกรณ์กระจายสัญญาณไร้สาย จำนวน ๑ ชุด

1. ระบบป้องกันการบุกรุกระบบเครือข่าย จำนวน 1 ระบบ มีคุณสมบัติดังต่อไปนี้

1.1 เป็นอุปกรณ์แบบ Hardware Appliance ที่ออกแบบมาเพื่อทำหน้าที่ Next Generation Firewall หรือ Next Generation IPS

1.2 มีความสามารถในการทำงานเป็น Next Generation Firewall พร้อมด้วยการทำ Application Visibility Control Throughput ไม่น้อยกว่า 12 Gbps

1.3 มีความสามารถในการทำงาน Next Generation Firewall (Application Visibility Control) และเปิดใช้งาน IPS พร้อมกันแล้วมี Throughput ไม่น้อยกว่า 10 Gbps

1.4 มีพอร์ตแบบ 10 Gigabit Ethernet ไม่น้อยกว่า 8 พอร์ตและมี slot สำหรับ Network Module ได้ไม่น้อยกว่า 2 slot โดยรองรับแบบ 10 Gigabit Ethernet SPF+ อย่างน้อย 8 พอร์ต และแบบ 40 Gigabit Ethernet Quad SFP+ อย่างน้อย 2 พอร์ต

1.5 รองรับการตรวจสอบเมื่อทำงานในแบบ Application Firewall ได้สูงสุดไม่น้อยกว่า 9,000,000 Concurrent Sessions และรองรับ New connection per seconds สูงสุดไม่น้อยกว่า 68,000 New Connections per second.

1.6 มีพอร์ตสำหรับบริหารจัดการอุปกรณ์โดยเฉพาะแบบ Gigabit Ethernet ชนิด copper และพอร์ต Serial Console Port

1.7 สามารถจัดการ กำหนด Security Policy โดยสามารถระบุจากข้อมูลเครือข่าย เช่น IP, Port, Protocol, User, Application และตำแหน่งประเทศตาม Geo-Location ได้เป็นอย่างน้อย

1.8 สามารถตรวจสอบข้อมูลต้องสงสัย (Threat security intelligence) ทั้งในรูปแบบ IP address และ DNS จากเจ้าของผลิตภัณฑ์ เพื่อนำมาใช้ในการติดตาม หรือป้องกันกลุ่ม IP address หรือ DNS ที่ต้องสงสัยได้

1.9 สามารถแสดงข้อมูลหมายเลข IP address และชื่อประเทศเจ้าของหมายเลข IP address จากการโจมตีระหว่างเครื่องของเครือข่ายภายในและเครือข่ายภายนอกได้

1.10 สามารถตรวจสอบภัยคุกคามที่ผ่านเข้ามาในระบบเครือข่าย โดยสามารถตรวจสอบทั้งการโจมตี และการติดต่อกับเครื่องที่น่าสงสัยภายนอก เช่น Command and Control Server รวมถึงสามารถเก็บข้อมูล packet ที่น่าสงสัย มาตรวจสอบในรูปแบบ pcap format ได้

1.11 สามารถกำหนดให้ถอดรหัสข้อมูลที่อยู่ในรูปแบบ SSL (Secure Socket Layer) ทั้งข้อมูลขาออก (จากผู้ใช้ไปสู่ เครือข่ายอินเทอร์เน็ต) และขาเข้า (จากเครือข่ายอินเทอร์เน็ตมายังเครื่องแม่ข่ายภายใน) รวมถึงสามารถกำหนดให้หยุดการติดต่อที่เข้ารหัสที่ไม่ปลอดภัยได้ เช่น มีการใช้ self-sign certificate.

1.12 สามารถตรวจสอบข้อมูล DNS (Domain Name Service) และสามารถตอบสนองการเรียกข้อมูลที่ต้องสงสัยได้ เช่น การ drop และ ส่ง IP Sinkhole

1.13 สามารถป้องกันการโจมตีและการบุกรุกเครือข่ายได้อย่างน้อย ดังนี้

1.13.1 ป้องกันการระบาดของ Virus หรือ Worm

1.13.2 ป้องกันการบุกรุกแบบ Vulnerability Exploit, Reconnaissance (port scan/sweep)

1.13.3 ป้องกันเทคนิคการหลบซ่อนการโจมตีแบบ IP Defragmentation, TCP/UDP Stream Segmentation, URL/HTML Obfuscation, HTML Evasion และ FTP Evasion ได้

1.13.4 ป้องกันเครือข่ายและสามารถตรวจจับวิธีการบุกรุกดังนี้ Overflow, Backdoor Program, Trojan/Spy ware.

1.14 สามารถแจ้งเตือนและโต้ตอบการโจมตีด้วยวิธีต่อไปนี้

1.14.1 Drop Traffic หรือ Drop Packet

1.14.2 สามารถเปลี่ยนสถานะของการป้องกันการโจมตีจาก Drop เป็น Alert หรือ จาก Alert เป็น Drop ตามเงื่อนไขที่กำหนดไว้

1.14.3 ทำงานร่วมกับอุปกรณ์ภายนอก เช่น อุปกรณ์เครือข่ายหรือไฟร์วอลล์เพื่อป้องกันการโจมตีได้ (external remediation)

1.15 สามารถทำงานร่วมกับระบบพิสูจน์ตัวตนการใช้งานเครือข่ายได้

1.16 รองรับทำงาน URL Filtering โดยมี categories ไม่น้อยกว่า 80 กลุ่ม

1.17 รองรับการตรวจจับ Malware โดยใช้ เทคนิค File analysis และ Sandboxing รวมถึงสามารถตรวจสอบย้อนหลังสำหรับ File ที่เคยผ่านการตรวจสอบเพื่อแจ้งเตือนในกรณีที่ File ดังกล่าวถูกวิเคราะห์ว่าเป็น Malware (Retrospective detection)

1.18 มีฟังชั่นป้องกันการโจมตี IPS, Anti Malware, URL Filtering Subscription มาพร้อมโดยมีระยะเวลาของ Subscription ไม่น้อยกว่า 3 ปี

1.19 มีโปรแกรมสำหรับบริหารจัดการการทำงานของอุปกรณ์ระบบรักษาความปลอดภัย

1.19.1 สามารถติดตั้งแบบ Virtual Machine หรือดีกว่าได้

1.19.2 ทำหน้าที่ในการบริหารจัดการระบบ Next Generation Firewall ที่นำเสนอ รองรับการบริหารจัดการอุปกรณ์ได้ผ่าน Graphic User Interface โดยผ่านเว็บแบบ HTTPS

1.19.3 สามารถบริหารจัดการอุปกรณ์ NGFW ได้สูงสุดไม่น้อยกว่า 2 อุปกรณ์พร้อม License ที่ถูกต้อง

1.19.4 สามารถใช้งานมาตรฐาน IPv6 ทั้งการจัดการอุปกรณ์ และการตรวจสอบข้อมูลการโจมตี

1.19.5 สามารถจัดการจัดเก็บ Log และสามารถส่ง Log ไปที่ระบบ
จัดเก็บ Log ศูนย์กลาง (Centralized Log Management) โดยรองรับการจัดส่งข้อมูลแบบเข้ารหัส (SSL/TCP) โดยสามารถเก็บข้อมูลได้ไม่น้อยกว่า 10,000,000 เหตุการณ์

1.19.6 สามารถบริหารจัดการนโยบายเรื่องควบคุมรักษาความมั่นคงปลอดภัยเครือข่าย (Next Generation Firewall Policy) และสามารถรองรับการกำหนดนโยบายโดย Application ซึ่งรองรับจำนวน Application ได้ไม่น้อยกว่า 4,000 Applications

1.19.7 สามารถบริหารจัดการนโยบายเรื่องการป้องกันเครือข่าย (Threat Prevention Policy) และนโยบายการป้องกัน ตรวจสอบ Advance Malware อยู่ในกลุ่ม Policy ชุดเดียวกัน เพื่อง่ายต่อการบริหารจัดการนโยบาย

1.19.8 สามารถปรับแต่งการแสดงผลของ Dashboard โดยกำหนดเงื่อนไขที่ต้องการแสดง (search criteria) ได้เอง รวมถึงสามารถปรับช่วงเวลาการแสดงข้อมูลได้อย่างน้อยเป็น ชั่วโมง หรือ วัน

1.19.9 สามารถสร้างรายงานที่ปรับแต่งได้ทั้งหมด ตั้งแต่ ข้อมูลที่สนใจ กราฟ สารบัญ และการสรุป โดยสามารถสร้าง และนำไปใช้กำหนดให้สร้างตามช่วงเวลาที่ต้องการได้

1.19.10 รองรับการเชื่อมต่อจากระบบภายนอกเพื่อดึงข้อมูลการโจมตีจากระบบภายนอก (3rd Party Threat Feed) ได้

1.19.11 สามารถแสดงข้อมูลของ Application ที่ใช้งานผ่านอุปกรณ์ทั้งในลักษณะจำนวน flow หรือปริมาณข้อมูลที่มีหน่วยเป็น kilobit per second (KB/s) ได้

1.19.12 สามารถจัดเก็บข้อมูลที่มีการโจมตี (Packet Capture) และ สามารถเรียกดูได้

1.19.13 สามารถแสดงชื่อผู้ใช้งานบนระบบเครือข่ายได้ โดยสามารถทำงานร่วมกับระบบไดเรกตอรี เช่น LDAP และสามารถกำหนดให้ตรวจสอบชื่อผู้ใช้จากโปรโตคอลที่ไม่มีการเข้ารหัสเช่น POP3 ได้

1.19.14 ระบบจัดการจะต้องทำงานอยู่บนระบบปฏิบัติการที่ได้รับการดูแล และอัปเดต โดยผู้ผลิต ได้ตลอดระยะรับประกัน

1.19.15 รองรับการรับข้อมูลจากอุปกรณ์ภายนอก เช่นระบบ Vulnerability Management เพื่อนำมาใช้ในการประเมินความเสี่ยงของระบบได้

1.20 ได้รับมาตรฐาน ความปลอดภัย FCC , UL หรือ CE เป็นอย่างน้อย

1.21 อุปกรณ์ที่นำเสนอจะต้องเป็นผลิตภัณฑ์ที่อยู่ในสายการผลิตไม่ตกรุ่น และเป็นสินค้าใหม่ ไม่เคยผ่านการใช้งานมาก่อน และพร้อมรับรองการบริการหลังการขาย หากในกรณีที่สินค้ายกเลิกการผลิต บริษัทฯ เจ้าของผลิตภัณฑ์จะต้องให้บริการทั้งด้าน Hardware และด้าน Software ต่อเนื่องอีกไม่น้อยกว่า 5 ปี เป็นสินค้าที่นำเข้าถูกต้องตามกฎหมายโดยต้องมีหนังสือรับรองสำหรับโครงการนี้จากบริษัทเจ้าของผลิตภัณฑ์สาขาประจำประเทศไทยยื่นต่อกรรมการพิจารณาโดยอ้างอิงเลขที่ประกาศและชื่อหน่วยงานอย่างชัดเจน

1.22 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งตัวแทนจำหน่ายโดยตรงจากบริษัทเจ้าของผลิตภัณฑ์สาขาประจำประเทศไทย

2. ระบบตรวจสอบตัวตนเพื่อเข้าใช้เครือข่ายคอมพิวเตอร์ จำนวน 1 ระบบ มีคุณสมบัติดังต่อไปนี้

2.1 สามารถติดตั้งใช้งานแบบ Virtual Appliance รองรับระบบปฏิบัติการ VMware ESX/ESXi หรือ ดีกว่า

2.2 ระบบที่เสนอต้องสามารถรองรับจำนวนอุปกรณ์ที่เข้าถึงระบบพร้อมกันได้ไม่น้อยกว่า 1,500 อุปกรณ์

2.3 สามารถตรวจสอบตัวตนและกำหนดสิทธิ์ในการเข้าใช้งานระบบเครือข่ายขององค์กร ทั้งในรูปแบบของเครือข่ายชนิดใช้สาย (Wired network), เครือข่ายไร้สาย (Wireless network) และ เครือข่ายเสมือน (VPN) ได้โดยการบริหารจากส่วนกลาง

2.4 สามารถเข้าบริหารจัดการการเข้าใช้งานระบบเครือข่ายชนิดใช้สาย (Wired) และไร้สาย (Wireless) โดยกำหนดนโยบายตาม กลุ่มผู้ใช้, ทรัพยากรเครือข่ายที่เข้าถึง, อุปกรณ์ที่เข้าใช้งาน, ได้เป็นอย่างน้อย

2.5 สามารถกำหนด และอนุญาตให้ผู้ใช้งานภายนอก (Guest) เข้าใช้เครือข่าย โดยมีการจำกัดการเข้าถึงทรัพยากรภายในบริษัท หรือให้บริการเฉพาะอินเตอร์สำหรับบุคคลภายนอกเท่านั้นและสามารถปรับเปลี่ยนแก้ไขหน้า Web pages ของผู้ใช้งานภายนอกให้เหมาะสมตามความต้องการขององค์กรได้โดยบริหารจัดการแบบรวมศูนย์ทั้งระบบ

2.6 รองรับการบริหารจัดการอุปกรณ์ที่เข้าใช้ระบบเครือข่าย เช่น IP camera, Printer, IP Phone, Smart Phone, Tablet และ คอมพิวเตอร์ โดยผู้ดูแลสามารถสร้างกลุ่มของอุปกรณ์ที่มีลักษณะเหมือนกัน และจำกัดการใช้งานของอุปกรณ์ดังกล่าวตามกลุ่มที่กำหนดไว้ได้ โดยบริหารจัดการแบบรวมศูนย์ทั้งระบบ

2.7 ใช้โปรโตคอลมาตรฐาน RADIUS (Remote Access Dial-In User Service)ในการทำ Authentication, Authorization และ Accounting (AAA) ได้

2.8 รองรับการตรวจสอบตัวตนด้วย โปรโตคอล PAP, MS-CHAP, EAP-MD5, PEAP, EAP-FAST, EAP-TLS เป็นอย่างน้อย

2.9 มีความสามารถในการทำ VLAN Assignment, Downloadable ACLs และ URL-Redirection ในการทำ Rule-based Policy ซึ่งทำงานร่วมกับอุปกรณ์เครือข่ายแบบไร้สายและแบบมีสายเดิมได้

2.10 สามารถเชื่อมต่อกับฐานข้อมูลของผู้ใช้งานจากภายนอก (External User Databases) ดังต่อไปนี้ได้ ActiveDirectory, Generic LDAP, Radius Token OTP

2.11 สามารถสร้างกลุ่มผู้ใช้ที่เป็นบุคคลภายนอก (Guest) โดยกำหนดเวลาที่สามารถใช้งาน ทั้งเวลาเริ่มต้นและสิ้นสุดของการใช้งานได้

2.12 รองรับการตรวจสอบอุปกรณ์ที่เข้าใช้งานระบบเครือข่ายโดยใช้การ Scanning ซึ่งช่วยในการบ่งบอก OS information, Open ports, SNMP variablesได้ และรองรับการรับข้อมูลของอุปกรณ์ที่เข้าใช้งานระบบเครือข่ายจากการใช้งาน Protocol CDP, LLDP, DHCP โดยรับข้อมูลผ่านทาง RADIUS attribute ที่ใช้ในการตรวจสอบตัวตนในการใช้งานได้

2.13 รองรับบริหารจัดการกลุ่มผู้ใช้ที่เป็นบุคคลภายนอก (Guest Life Cycle Management) ได้

2.14 สามารถกำหนดติดตั้ง ได้และแบ่งกลุ่ม Web Browser ผ่าน (Configuration and Management) ผู้ดูแลได้หลายระดับเช่น Operator, Helpdesk, Administrator ได้เป็นอย่างน้อย

2.15 สามารถ Sync Clock กับระบบ NTP server ได้

2.16 รองรับระบบลงทะเบียนอุปกรณ์ Mobile ใหม่โดยใช้ Web Redirect ไปยังหน้า Portal เพื่อเข้าสู่ระบบและลงทะเบียนอุปกรณ์เพื่อเข้าสู่ระบบได้

2.17 มี Dashboard ในการแสดงสถานะภาพรวมของอุปกรณ์ที่เข้าใช้งานระบบเครือข่าย ทั้งอุปกรณ์ที่ผ่านและอุปกรณ์ที่ไม่ผ่านการตรวจสอบ

2.18 สามารถส่ง Log ไปยัง Syslog Server ได้

2.19 อุปกรณ์ที่เสนอต้องรองรับ Client Software เพื่อใช้เป็น 802.1x Supplicant โดย Software Client มีคุณสมบัติอย่างน้อย ดังนี้

2.19.1 ใช้งานกับระบบ RADIUS, Microsoft Active Directory, RSA, LDAP

2.19.2 รองรับการโปรโตคอล 802.1x สำหรับการตรวจสอบตัวตน (Authentication) และ 802.1AE สำหรับการทำ Encryption ได้เป็นอย่างน้อย

2.19.3 สามารถใช้งานร่วมกับ Windows OS (32 bits และ 64 bits), MAC OS 10.5 ได้เป็นอย่างน้อย

2.19.4 รองรับการใช้งานทั้ง Wired และ Wireless Network

2.19.5 สำหรับ Wireless Encryption ต้องรองรับวิธีต่าง ๆ อย่างน้อยดังต่อไปนี้ Open, Wired Equivalent Policy (WEP), Dynamic WEP, WPA Enterprise, WPA2 Enterprise, WPA Personal, WPA2 Personal

2.20 ผลิตภัณฑ์ที่นำเสนอจะต้องเป็นผลิตภัณฑ์ที่อยู่ในสายการผลิตไม่ตกรุ่น และเป็นสินค้าใหม่ ไม่เคยผ่านการใช้งานมาก่อน และพร้อมรับรองการบริการหลังการขายหากในกรณีที่สินค้ายกเลิกการผลิต บริษัทฯเจ้าของผลิตภัณฑ์จะต้องให้บริการด้าน Software ต่อเนื่องอีกไม่น้อยกว่า 5 ปี เป็นสินค้าที่นำเข้าถูกต้องตามกฎหมายโดยต้องมีหนังสือรับรองสำหรับโครงการนี้จากบริษัทเจ้าของผลิตภัณฑ์สาขาประจำประเทศไทยยื่นต่อกรรมการพิจารณาโดยอ้างอิงเลขที่ประกาศและชื่อหน่วยงานอย่างชัดเจน

2.21 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งตัวแทนจำหน่ายโดยตรงจากบริษัทเจ้าของผลิตภัณฑ์สาขาประจำประเทศไทย

3. ระบบป้องกันการโจมตีแอพพลิเคชั่น จำนวน 1 ชุด มีคุณสมบัติดังต่อไปนี้

3.1 เป็นอุปกรณ์ที่ออกแบบมาเพื่อใช้งานเป็น Web Application Firewall โดยสามารถป้องกันการโจมตี Web Applications ได้

3.2 มีระบบ Power Supply จำนวนไม่น้อยกว่า 2 ชุด

3.3 มี Throughput ไม่น้อยกว่า 10 Gbps

3.4 มีพอร์ตการเชื่อมต่อ 1 Gigabit แบบ SFP ไม่น้อยกว่า 4 พอร์ต

3.5 มีพอร์ตการเชื่อมต่อ 10 Gigabit แบบ SFP+ ไม่น้อยกว่า 2 พอร์ต

3.6 สามารถรับการเชื่อมต่อแบบ L7 Request per Second ไม่น้อยกว่า 350,000 ต่อวินาทีและ L4 Concurrent Connections ที่ 14,000,000 Connections

3.7 สามารถทำงานในรูปแบบ Reverse Proxy Mode หรือ In-Line Bridge หรือ Transparent ได้เป็นอย่างน้อย

3.8 ผลิตภัณฑ์ต้องได้รับการรับรองมาตรฐานจาก ICSA Lab

3.9 ผลิตภัณฑ์ที่นำเสนอผ่านการทดสอบมาตรฐานจาก NSS Labs ตามเอกสาร WEB APPLICATION FIREWALL COMPARATIVE ANALYSIS ในส่วนของ Overall Rating ในระดับ Recommended

3.10 ผลิตภัณฑ์ที่นำเสนออยู่ในกลุ่ม Leaders หรือ Challengers ของ Gartner Magic Quadrant ด้าน Web Application Firewalls ในการจัดลำดับครั้งล่าสุดในวันที่ยื่นเสนอราคา

3.11 สามารถป้องกันการโจมตีเว็บไซต์ที่ได้มาตรฐานตาม OWASP Top 10 เป็นอย่างน้อย

3.12 สามารถทำงานร่วมกับ Vulnerability Scan Tool เช่น Qualys, IBM App Scan, HP Web Inspectเป็นต้นโดยนำผลการ Scan มาทำ Policy ได้

3.13 สามารถทำการ Update Signature แบบ Manual และ Automatic Update ได้

3.14 สามารถทำรายงานการถูกโจมตีในรูปแบบ HTML หรือ PDF ได้

3.15 อุปกรณ์รองรับการทำงานแบบ High Availability ในการทำงานแบบ Active-Passive หรือ Active-Active ได้

3.16 สามารถทำ Data Guard ป้องกันการรั่วไหลของข้อมูลได้ เช่น Credit Card Numbers และ Custom Pattern และสามารถตรวจสอบไฟล์ประเภท MS Office, PDF และ ELF ได้เป็นอย่างน้อย

3.17 สามารถป้องกันการโจมตีจาก BOT โดยวิธีการส่ง CAPTCHA Challenges ได้

3.18 อุปกรณ์รองรับการป้องกันการโจมตีแบบ DDos Attacks ได้

3.19 สามารถทำงานร่วมกับ ICAP Server ได้

3.20 สามารถทำ SSL Offload ได้

3.21 อุปกรณ์สามารถส่ง Log ในแบบ Syslog ได้

3.22 สามารถรองรับการทำงาน Load Balancing เพื่อกระจายโหลด Server ในอนาคตได้อย่างน้อย ดังนี้ Round Robin, Ratio, Fastest, Least Connections, Weighted Least Connections, Observed, Predictive และ Least Sessions

3.23 สามารถรองรับการทำ Session persistence ในอนาคตได้โดยดูจาก Cookie, Destination Address, Hash, Microsoft Remote Desktop, SIP, Source Address, SSL และ Universal

3.24 รองรับการทำ SSL Connection and Session Mirroring ได้ เพื่อช่วยรักษา SSL Connection เมื่อเกิด Fail-Over ขึ้น

3.25 ผู้เสนอราคาต้องได้รับการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิต โดยแสดงเอกสารรับรองการสนับสนุนที่ระบุชื่อโครงการนี้ ว่าให้การสนับสนุนทางเทคนิคแก่ผู้เสนอราคา และรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ที่ยังอยู่ในสายการผลิตนับถึงวันที่เสนอราคาเป็นของใหม่ที่ยังไม่ได้ทำการติดตั้งใช้งาน ณ ที่ใดมาก่อน และไม่เป็นเครื่องที่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt)

4. เครื่องคอมพิวเตอร์แม่ข่ายประมวลผลรองรับระบบ Virtualization จำนวน 1 ชุด มีคุณสมบัติดังต่อไปนี้

4.1 หน่วยประมวลผลกลางไม่น้อยกว่า 8 Core หรือดีกว่า ความเร็วไม่ต่ำกว่า 2.1 GHz โดยมี Cache ขนาดไม่น้อยกว่า 10MB Cache จำนวน 2 หน่วย

4.2 หน่วยความจำ แบบ ECC DDR4 หรือดีกว่าขนาดไม่น้อยกว่า 192 GB

4.3 หน่วยควบคุม Hard Disk Controller ที่สนับสนุนการทำ RAID 0, 1, 5 ได้หรือดีกว่า

4.4 มี Hard Disk แบบ SATA หรือดีกว่า ความจุไม่น้อยกว่า 600 GB จำนวนไม่น้อยกว่า 2 หน่วยและมี Hard Disk แบบ SSD ขนาด 450 GB ไม่น้อยกว่า 1 หน่วย

4.5 มีส่วนเชื่อมต่อกับระบบเครือข่าย การใช้งานแบบ 10 Gigabit Ethernet SFP หรือ SFP+ จำนวนไม่น้อยกว่า 2 พอร์ต ติดตั้ง Transceiver มาพร้อมใช้งาน

4.6 มีระบบจ่ายไฟ Power Supply 750 วัตต์ จำนวน 2 หน่วยสามารถทำงานแบบ Redundant Power Supply และ Hot-Pluggable ได้

4.7 เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่ได้รับการออกแบบสำหรับติดตั้งกับตู้ Rack ขนาด 19 นิ้วพร้อมอุปกรณ์การติดตั้งใน Rack

4.8 ผ่านมาตรฐาน FCC, UL, EN และ CE เป็นอย่างน้อย

5. อุปกรณ์กระจายสัญญาณไร้สาย จำนวน 10 ชุด มีคุณสมบัติดังต่อไปนี้

5.1 Access Point ที่สามารถทำงานร่วมกับ WLAN Controller ที่มหาวิทยาลัยทำการติดตั้งไว้แล้วได้อย่างมีประสิทธิภาพ

5.2 สามารถรับส่งข้อมูลที่ย่านความถี่ 2.4 GHz และ 5 GHz ได้พร้อมกัน

5.3 อุปกรณ์ต้องมีเสาอากาศแบบภายใน ชนิด internal horizontal beamwidth 360°

5.4 มีหน่วยความจำแบบ DRAM ไม่น้อยกว่า 1 GB และ Flash 256 MB เป็นอย่างน้อย

5.5 เสาอากาศภายในสามารถใช้งานย่านความถี่ 2.4 GHz ที่ 3dBi และ 5 GHz ที่ 5dBi โดยที่อุปกรณ์รองรับการทำงานแบบ MIMO 3Tx และ 3Rx ได้ และสามารถส่งข้อมูลได้ 2 Spatial Stream ซึ่งสามารถทำให้รองรับความเร็วสูงสุดได้ 867 Mbps IEEE802.11ac เป็นอย่างน้อย

5.6 สนับสนุนการทำงานตามมาตรฐาน IEEE802.11a, IEEE802.11b/g, IEEE802.11n และ IEEE802.11ac Wave 2

5.7 สนับสนุนการทำ Dynamic Frequency Selection (DFS) ได้

5.8 สนับสนุนการทำ Cyclic shift diversity (CSD) ได้

5.9 สนับสนุนความปลอดภัยของระบบเครือข่ายไร้สายแบบ 802.11i, Wi-Fi Protected Access 2 (WPA2), Wi-Fi Protected Access (WPA), 802.1x, Advanced Encryption Standard (AES)

5.10 สนับสนุนการทำงาน Multiuser MIMO และ Transmit beamforming เทคโนโลยีได้เป็นอย่างน้อย

5.11 มีพอร์ต Gigabit Ethernet 1000 Base-Tx ที่รองรับ PoE ตามมาตรฐาน 802.3af, 802.3at ได้

5.12 มีไฟแสดงสถานการณ์ทำงานของอุปกรณ์

5.13 มีพอร์ต Console แบบ RJ45 และ USB เป็นอย่างน้อย

5.14 อุปกรณ์สามารถทำงานตามสภาวะแวดล้อมได้ที่อุณหภูมิ 0 - 40 องศาเซลเซียส

5.15 ได้รับการรับรองข้อกำหนดตามมาตรฐาน UL, EN, IEC และ FCC ที่เกี่ยวข้อง

5.16 เพื่อเป็นการรับประกันการให้บริการหลังการขาย ผู้เสนอราคาต้องได้รับการแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ในประเทศไทยสำหรับโครงการนี้ และรับรองว่าเป็นสินค้าใหม่ไม่เป็นสินค้าลอกเลียนแบบ ประกอบสำเร็จจากโรงงานผลิต และยังอยู่ในสายการผลิตปัจจุบัน

6. ระบบควบคุมการทำงานอุปกรณ์กระจายสัญญาณไร้สาย จำนวน 1 ชุด มีคุณสมบัติ ดังต่อไปนี้

6.1 อุปกรณ์ต้องเป็น Appliance ที่ออกแบบมาสำหรับใช้ควบคุมอุปกรณ์ Wireless Access Point โดยเฉพาะ

6.2 มี Slot สำหรับ 10GBase-X SFP อย่างน้อย 2 ช่อง

6.3 มี Management Controller port แบบ10/100/1000 Ethernet (RJ-45) จำนวน 1 พอร์ท และมี Console port แบบ Serial port (RJ-45) จำนวน 1 พอร์ท

6.4 สามารถควบคุม Access Point ได้ไม่น้อยกว่า 1,300 เครื่องและสามารถขยายได้สูงสุด 1,500 เครื่องภายในอุปกรณ์ตัวเดียว และสามารถรองรับเครื่องลูกข่ายได้ไม่น้อยกว่า 20,000 เครื่อง

6.5 สามารถควบคุม Remote Access Point โดยใช้ในการทำงานแบบ ได้ Office Extended

6.6 สามารถทำงานได้ตามมาตรฐาน IEEE802.11a, 802.11b, IEEE 802.11g และ IEEE 802.11ac Wave1 and Wave2

6.7 สามารถรองรับการทำ VLAN ได้ตามมาตรฐาน IEEE 802.1QVLAN tagging

6.8 สามารถเชื่อมต่อกับ Access Point ได้ตาม Control and Provisioning of Wireless Access Points Protocol (CAPWAP)ตามรูปแบบ DTLS(RFC 5416)ได้

6.9 มีระบบรักษาความปลอดภัยตามมาตรฐาน Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2) และ HMAC: Keyed Hashing for Message Authentication

6.10 สามารถเข้ารหัสข้อมูลได้ตามมาตรฐาน TKIP และ AES

6.11 สามารถทำการตรวจสอบผู้ใช้งานตามมาตรฐาน IEEE802.1x ดังต่อไปนี้ LAEP, PEAP, EAP-TLS, EAP-TTLS

6.12 สามารถเปลี่ยน Channel ของ Access point ได้ตามสภาพแวดล้อม (Dynamic Channel Assignment)

6.13 มีระบบตรวจจับการกวนของสัญญาณและสามารถปรับปรุงให้ดีขึ้นได้ (Interference Detection & Avoidance)

6.14 สามารถตรวจหาจุดที่ไม่มีสัญญาณและแก้ไขได้โดยอัตโนมัติ (Coverage hole detection & correction)

6.15 สามารถตรวจวัดและควบคุมระดับความแรงในการส่งสัญญาณของอุปกรณ์ Access Point แต่ละตัวได้

6.16 สามารถกระจายผู้ใช้งานไปยัง Access Point ที่อยู่โดยรอบได้โดยอัตโนมัติ (Client Load Balancing)

6.17 สามารถบริการจัดการในระดับแอพลิเคชันได้ (Application visibility and control)

6.18 สามารถทำการ Roaming ทั้งในลักษณะ Layer 2 และ Layer 3 ได้

6.19 สามารถทำการตรวจจับและป้องกัน Access Point แปลกปลอมได้ (Rogue Detection and Containment)

6.20 มีระบบ Wireless Intrusion Detectionเพื่อตรวจสอบและป้องกันการโจมตีบนเครือข่ายไร้สาย

6.21 สามารถทำงานในรูปแบบ Enterprise Mesh ตามมาตรฐาน 802.11n ได้

6.22 สามารถป้องกันการโจมตี Management Frame ได้ด้วย Management Frame Protection (MFP)

6.23 สามารถควบคุม Quality of Service (QoS) ได้แบบ Bandwidth contract, traffic shaping, RF Utilization เป็นอย่างน้อย

6.24 สามารถรองรับการใช้กับระบบ Radius Server ภายนอกได้

6.25 สามารถทำการ Authenticate ผู้ใช้งานผ่านทาง Web - based ได้

6.26 สามารถทำ Access Control List ได้

6.27 สามารถบริหารจัดการอุปกรณ์ผ่าน HTTP, HTTPS, Telnet, SSH และ Console Port ได้

6.28 สามารถบริหารผ่านโปรโตคอล SNMPV1, V2c, V3 และ CDP over Air

6.29 อุปกรณ์ต้องผ่านมาตรฐานความปลอดภัย FCC, EN และ UL เป็นอย่างน้อย

6.30 อุปกรณ์ที่นำเสนอจะต้องเป็นผลิตภัณฑ์ที่อยู่ในสายการผลิตไม่ตกรุ่น และเป็นสินค้าใหม่ ไม่เคยผ่านการใช้งานมาก่อน และพร้อมรับรองการบริการหลังการขายหากในกรณีที่สินค้ายกเลิกการผลิต บริษัทฯเจ้าของผลิตภัณฑ์จะต้องให้บริการทั้งด้าน Hardware และด้าน Software ต่อเนื่องอีกไม่น้อยกว่า 5 ปี เป็นสินค้าที่นำเข้าถูกต้องตามกฎหมายโดยต้องมีหนังสือรับรองสำหรับโครงการนี้จากบริษัทเจ้าของผลิตภัณฑ์สาขาประจำประเทศไทยยื่นต่อกรรมการพิจารณาโดยอ้างอิงเลขที่ประกาศและชื่อหน่วยงานอย่างชัดเจน

6.31 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งตัวแทนจำหน่ายโดยตรงจากบริษัทเจ้าของผลิตภัณฑ์สาขาประจำประเทศไทย

7. เงื่อนไขอื่น ๆ

7.1 ผู้เสนอราคาต้องมีช่องทางรับแจ้งปัญหาต่าง ๆ ที่อาจเกิดขึ้น เช่น โทรศัพท์ โทรสาร e - Mail หรือช่องทางอื่น ๆ ที่สามารถติดต่อได้

7.2 ผู้เสนอราคาจะต้องรับประกันคุณภาพสินค้าทุกรายการเป็นเวลา 1 ปี และต้องรับประกันจากผู้ผลิตเป็นระยะเวลา 3 ปี นับถัดจากวันที่ผู้ซื้อได้รับมอบสิ่งของทั้งหมดไว้โดยถูกต้องครบถ้วนตามสัญญา โดยไม่คิดค่าแรง ค่าอะไหล่ ค่าเดินทาง ค่าน้ำมันเชื้อเพลิง ค่าที่พัก ฯลฯ และในช่วงรับประกัน หากอุปกรณ์ที่ใช้ใด ๆ เกิดความเสียหายใช้งานได้ไม่ได้ จะต้องนำอุปกรณ์ที่มีคุณสมบัติเทียบเท่าหรือดีกว่า มาทดแทนภายในระยะเวลาไม่เกิน 48 ชั่วโมง (ไม่รวมวันหยุดนักขัตฤกษ์) นับจากได้รับแจ้งจากทางมหาวิทยาลัย ทุกช่องทาง เช่น โทรศัพท์ โทรสาร e – Mail หรือช่องทางอื่น ๆ ที่สามารถติดต่อได้

7.3 ต้องทำการติดตั้งและปรับตั้งค่าของอุปกรณ์ทุกรายการ รวมถึงจัดหาวัสดุ และอุปกรณ์ประกอบจนสามารถใช้งานได้เป็นอย่างดี