มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

รายละเอียดคุณลักษณะเฉพาะครุภัณฑ์ (Spec.)

ชื่อครุภัณฑ์ อุปกรณ์ป้องกันระบบเครือข่ายระดับสูง Next Generation Firewall **จำนวน** 1 ระบบ

หน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ **วงเงิน** 3,900,000 **บาท**

☐ **เงินงบประมาณรายได้ ประจำปี 2563** ☑ **เงินงบประมาณประจำปี 2563**

ลำดับที่	รายละเอียด	หมายเหตุ
	คุณสมบัติทั่วไป 1. ผู้รับจ้างจะต้องติดตั้งอุปกรณ์ทุกรายการให้สามารถพร้อมใช้งาน 2. ผู้รับจ้างจัดทำเอกสารคู่มือการติดตั้งและคู่มือการใช้งานสำหรับอุปกรณ์และโปรแกรมของระบบที่ติดตั้ง 3. สามารถใช้งานได้เป็นอย่างดีกับระบบไฟฟ้าในประเทศไทย 4. ผลิตภัณฑ์ที่เสนอเป็นอุปกรณ์ใหม่ไม่เคยใช้งานมาก่อนและอยู่ในสายการผลิต ไม่เป็นอุปกรณ์ที่นำมาปรับปรุงสภาพใหม่หรือแปรสภาพ (Reconditioned หรือ Refurbished) 5. ผู้เสนอราคาต้องมีเอกสารรับรองการเป็นตัวแทนจำหน่ายของอุปกรณ์ที่เสนอจากบริษัทผู้ผลิตและต้องมีเอกสารการสนับสนุนทางเทคนิคสำหรับโครงการนี้จากบริษัทผู้ผลิต(เอกสารฉบับจริง) 6. มีการรับประกันแบบ On-Site Service ภายใน 24 ชั่วโมงหลังการแจ้งปัญหาโดยศูนย์บริการของผู้ผลิต เป็นระยะเวลาไม่น้อยกว่า 2 ปี	
1	**อุปกรณ์ป้องกันระบบเครือข่ายระดับสูง Next Generation Firewall จำนวน 1 เครื่อง** มีคุณสมบัติดังนี้ 1.1 เป็นอุปกรณ์แบบ Hardware Appliance ที่ออกแบบมาเพื่อทำหน้าที่ Next Generation Firewall หรือ Next Generation IPS 1.2 อุปกรณ์ถูกออกแบบมาให้สามารถติดตั้งบน Rack 19 นิ้วได้ 1.3 อุปกรณ์ถูกออกแบบมาให้สามารถทำงานได้อย่างต่อเนื่องโดยมี Redundant ของระบบระบายความร้อนแบบพัดลม(Fan Module) และอุปกรณ์แหล่งจ่ายไฟ(Power Supply) เป็นอย่างน้อย 1.4 มีหน่วยความจำหลัก(Memory) ไม่น้อยกว่า 64 GB และมีหน่วยความจำสำรองชนิด SSD ขนาดไม่น้อยกว่า 200 GB.	

ลำดับที่	รายละเอียด	หมายเหตุ
	1.5 รองรับ SFP+ จำนวนไม่น้อยกว่า 8 พอร์ต และสามารถรองรับการเพิ่มขยาย Network Module ขนาด 40 Gigabit ได้สูงสุดไม่น้อยกว่า 4 พอร์ตในอนาคต 1.6 มี SFP+ Module เทียบเท่าหรือดีกว่าแบบ 10 Gigabit Ethernet ชนิด SR พร้อมสาย Patch cord ความยาวไม่น้อยกว่า 3 เมตรชนิดหัวต่อ LC-LC จำนวนไม่น้อยกว่า 4 ชุด 1.7 มี SFP+ Module เทียบเท่าหรือดีกว่าแบบ 10 Gigabit Ethernet ชนิด LR พร้อมสาย Patch cord ความยาวไม่น้อยกว่า 10 เมตรชนิดหัวต่อ LC-LC จำนวนไม่น้อยกว่า 2 ชุด 1.8 มีพอร์ตสำหรับบริหารจัดการอุปกรณ์โดยเฉพาะเทียบเท่าหรือดีกว่า Gigabit Ethernet ชนิด copper พร้อม 1000Base-T SFP Module และพอร์ต Serial Console Port เป็นอย่างน้อย 1.9 มีอุปกรณ์ Line Card ที่นำมาเชื่อมต่อกับอุปกรณ์กระจายสัญญาณหลักของมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัยรุ่น Cisco C9407R หมายเลขครุภัณฑ์ 07-7440-012-0603/2-62 ที่ใช้อยู่ปัจจุบันได้เป็นอย่างดี โดยมีคุณสมบัติเทียบเท่าหรือดีกว่าดังต่อไปนี้ • รองรับ Jumbo Frame 9198 ไบต์ • รองรับ Network Interface Card แบบ SFP+ ได้จำนวนไม่น้อยกว่า 24 พอร์ต • มี SFP+ Module เทียบเท่าหรือดีกว่าแบบ 10 Gigabit Ethernet ชนิด SR พร้อมสาย Patch cord ความยาวไม่น้อยกว่า 5 เมตร หัวต่อชนิด LC-LC จำนวนไม่น้อยกว่า 8 ชุด 1.10 มีความสามารถในการทำงาน(Firewall และ Application Control) สูงสุดไม่น้อยกว่า 13 Gbps โดยรองรับ Application ไม่น้อยกว่า 4,000 applications 1.11 มีความสามารถในการทำงาน(Application Control และ IPS) สูงสุดไม่น้อยกว่า 11 Gbps โดยรองรับการตรวจสอบการโจมตีและควบคุมการใช้งาน Application พร้อมกัน 1.12 รองรับการตรวจสอบเมื่อทำงานในแบบ Application Firewall ได้สูงสุดไม่น้อยกว่า 10 Million Concurrent Sessions และรองรับ New connection per seconds สูงสุดไม่น้อยกว่า 64,000 connections per second 1.13 มี software ในการบริหารจัดการตัวอุปกรณ์รักษาความปลอดภัยติดตั้งเป็น Virtual Machine ซึ่งใช้งานร่วมกับระบบคลาวด์ของมหาวิทยาลัยได้เป็นอย่างดี พร้อม subscription เป็นเวลาไม่น้อยกว่า 3 ปี 1.14 สามารถจัดการนโยบายการเชื่อมต่อ (Access Control Policy) โดยสามารถระบุจากข้อมูลเครือข่าย เช่น IP, Port, Protocol, User, Application และ Geo-Location ได้เป็นอย่างน้อย	

ลำดับที่	รายละเอียด	หมายเหตุ
	1.15 สามารถรับข้อมูลต้องสงสัย(security intelligence) ทั้งในรูปแบบ IP address และ DNS จากเจ้าของผลิตภัณฑ์ เพื่อนำมาใช้ในการติดตาม หรือป้องกันกลุ่ม IP address หรือ DNS ที่ต้องสงสัยได้ 1.16 สามารถแสดงให้เห็นความสัมพันธ์ระหว่าง IP address กับประเทศต้นทาง(geolocation) ได้ 1.17 สามารถตรวจสอบภัยคุกคามที่ผ่านเข้ามาในระบบเครือข่าย โดยสามารถตรวจสอบทั้งการโจมตี และการติดต่อกับเครื่องที่น่าสงสัยภายนอก เช่น Command and Control Server รวมถึงสามารถเก็บข้อมูล packet ที่น่าสงสัย มาตรวจสอบในรูปแบบ pcap format ได้ 1.18 สามารถตรวจสอบข้อมูล DNS (Domain Name Service) และสามารถตอบสนองการเรียกข้อมูลที่ต้องสงสัยได้ เช่น การ drop และ ส่ง IP Sinkhole ได้เป็นอย่างน้อย 1.19 สามารถป้องกันการโจมตีและการบุกรุกเครือข่ายได้อย่างน้อยดังนี้ • ป้องกันการระบาดของ Virus หรือ Worm • ป้องกันการบุกรุกแบบ Vulnerability Exploit, Reconnaissance (port scan/sweep) • ป้องกันเทคนิคการหลบซ่อนการโจมตีแบบ IP Defragmentation, TCP/UDP Stream Segmentation, URL/HTML Obfuscation, HTML Evasion และ FTP Evasion ได้ • ป้องกันเครือข่ายและสามารถตรวจจับวิธีการบุกรุกดังนี้ Overflow, Backdoor Program, Trojan/Spyware 1.20 สามารถแจ้งเตือนและโต้ตอบการโจมตีด้วยวิธีต่อไปนี้ • การ Drop ข้อมูลหรือดีกว่า • สามารถเปลี่ยนสถานะของการป้องกันการโจมตีจาก Drop เป็น Alert หรือ จาก Alert เป็น Drop ตามเงื่อนไขที่กำหนดไว้ • ทำงานร่วมกับอุปกรณ์ภายนอก เช่น อุปกรณ์เครือข่าย หรือไฟร์วอลล์เพื่อป้องกันการโจมตีได้ (external remediation) • สามารถทำงานร่วมได้เป็นอย่างดีกับระบบตรวจสอบตัวตนเพื่อเข้าใช้เครือข่ายในรายการที่ 2 เพื่อเปลี่ยนสถานะของเครื่องที่ต้องสงสัยได้ 1.21 รองรับการตรวจจับ Advance Malware โดยใช้ เทคนิค File analysis และ Sandboxing รวมถึงสามารถตรวจสอบย้อนหลังสำหรับ File ที่เคยผ่านการตรวจสอบเพื่อแจ้งเตือนในกรณีที่ File ดังกล่าวถูกวิเคราะห์ว่าเป็น Malware (Retrospective detection) 1.22 ได้รับมาตรฐาน ความปลอดภัย FCC, UL หรือ CE เป็นอย่างน้อย	

ลำดับที่	รายละเอียด	หมายเหตุ
2	**ซอฟท์แวร์ระบบตรวจสอบตัวตนเพื่อเข้าใช้เครือข่ายคอมพิวเตอร์ จำนวน 1 ชุด** มีคุณสมบัติดังต่อไปนี้ 2.1 ระบบที่เสนอสามารถทำงานแบบ Virtual Machine และใช้งานร่วมกับระบบคลาวด์ของมหาวิทยาลัยได้เป็นดี 2.2 ระบบที่เสนอต้องสามารถรองรับจำนวนอุปกรณ์ที่เข้าสู่การตรวจสอบตัวตนได้สูงสุดไม่น้อยกว่า 18,000 อุปกรณ์ในเวลาเดียวกัน(concurrent) 2.3 สามารถตรวจสอบตัวตนและกำหนดสิทธิ์ในการเข้าใช้งานระบบเครือข่ายขององค์กร ทั้งในรูปแบบของ เครือข่ายชนิดใช้สาย(Wired network) , เครือข่ายไร้สาย(Wireless network) และ เครือข่ายเสมือน(VPN) ได้โดยการบริหารจากส่วนกลาง 2.4 สามารถเข้าบริหารจัดการการเข้าใช้งานระบบเครือข่ายชนิดใช้สาย(Wired) และไร้สาย(Wireless) โดยกำหนดนโยบายตามกลุ่มผู้ใช้, อุปกรณ์ที่เข้าใช้งาน, ทรัพยากรเครือข่ายที่เข้าถึงและ เวลา ได้เป็นอย่างน้อย 2.5 สามารถกำหนด และอนุญาตให้ผู้ใช้งานภายนอก(Guest) เข้าใช้เครือข่าย โดยมีการจำกัดการเข้าถึงทรัพยากรภายใน หรือให้บริการเฉพาะอินเตอร์สำหรับบุคคลภายนอกเท่านั้น และสามารถปรับเปลี่ยนแก้ไขหน้า Web pages ของผู้ใช้งานภายนอกให้เหมาะสมตามความต้องการขององค์กรได้ โดยบริหารจัดการแบบรวมศูนย์ทั้งระบบ 2.6 รองรับการบริหารจัดการอุปกรณ์ที่เข้าใช้ระบบเครือข่าย เช่น IP camera, Printer, IP Phone, Smart Phone, Tablet คอมพิวเตอร์ โดยผู้ดูแลสามารถสร้างกลุ่มของอุปกรณ์ที่มีลักษณะเหมือนกัน และกำจัดการใช้งานของอุปกรณ์ดังกล่าวตามกลุ่มที่กำหนดไว้ได้ โดยบริหารจัดการแบบรวมศูนย์ทั้งระบบ 2.7 ใช้โปรโตคอล มาตรฐาน 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 Active Directory, Generic LDAP, Radius Token OTP	

ลำดับที่	รายละเอียด	หมายเหตุ
	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 รองรับการตรวจสอบสถานะของเครื่องคอมพิวเตอร์ที่เข้าใช้งานระบบเครือข่ายอย่างน้อยดังต่อไปนี้ ● ตรวจสอบระบบ Antivirus และความทันสมัยของระบบ Antivirus ● ตรวจสอบ Microsoft Window Service pack ที่จำเป็น 2.14 รองรับการกักกันเครื่องคอมพิวเตอร์ที่ไม่ผ่านการตรวจสอบตัวตนและสถานะ ให้อยู่ในวงจำกัด 2.15 สามารถบริหารจัดการกลุ่มผู้ใช้ที่เป็นบุคคลภายนอก(Guest Life Cycle Management) ได้ 2.16 สามารถกำหนดติดตั้ง(Configuration and Management) ผ่าน Web Browser ได้และแบ่งกลุ่มผู้ดูแลได้หลายระดับเช่น Operator, Helpdesk, Administrator ได้เป็นอย่างน้อย 2.17 สามารถ Sync Clock กับระบบ NTP server ได้ 2.18 รองรับระบบลงทะเบียนอุปกรณ์ Mobile ใหม่ โดยใช้ Web Redirect ไปยังหน้า Portal เพื่อเข้าสู่ระบบและลงทะเบียนอุปกรณ์เพื่อเข้าสู่ระบบได้ 2.19 มี Dashboard ในการแสดงสถานะภาพรวมของอุปกรณ์ที่เข้าใช้งานระบบเครือข่าย, อุปกรณ์ที่ผ่านการตรวจสอบ, อุปกรณ์ที่ไม่ผ่านการตรวจสอบ เป็นอย่างน้อย 2.20 สามารถส่ง Log ไปยัง Syslog Server ได้ 2.21 อุปกรณ์ที่เสนอต้องรองรับมี Client Software เพื่อใช้เป็น 802.1x Supplicant โดย Software Client มีคุณสมบัติอย่างน้อยดังนี้ ● ใช้งานกับระบบ RADIUS, Microsoft Active Directory, RSA SecureID, LDAP ● รองรับการโปรโตคอล 802.1x สำหรับการตรวจสอบตัวตน (Authentication) และ 802.1AE สำหรับการทำ Encryption ได้เป็นอย่างน้อย ● สามารถใช้งานร่วมกับ Windows 7 (32 bits และ 64 bits), Windows Vista (32 bits และ 64 bits), Window XP (32 bits และ 64 bits), MAC OS 10.5, 10.6.x ได้เป็นอย่างน้อย	

ลำดับที่	รายละเอียด	หมายเหตุ
	• รองรับการใช้งานทั้ง Wired และ Wireless Network • สำหรับ Wireless Encryption ต้องรองรับวิธีต่าง ๆ อย่างน้อยดังต่อไปนี้ Open, Wired Equivalent Policy (WEP), Dynamic WEP, WPA Enterprise, WPA2 Enterprise, WPA Personal, WPA2 Personal	

ผู้ออกรายละเอียด

1. .....

(....นายกิติศักดิ์ วัฒนกุล.....)

2. .....

(.....นายกนกพล เมืองรักษ์.....)

3. .....

(.....นายวัชรินทร์ บุญช่วย.....)