คุณลักษณะเฉพาะ

ชื่ออุปกรณ์ ระบบรักษาความปลอดภัยเครือข่ายแบบเอนกประสงค์

จำนวน 2 ระบบ

วัตถุประสงค์ เป็นอุปกรณ์รักษาความปลอดภัยให้กับเครือข่ายคอมพิวเตอร์ระบบ MMIS และระบบ Internet ทดแทนอุปกรณ์เดิมที่ใช้งานมาแล้ว 7 ปี

งบประมาณ 10,800,000 บาท

คุณลักษณะเฉพาะ

1. เป็นอุปกรณ์ที่ได้รับการออกแบบมา เพื่อทำหน้าที่รักษาความปลอดภัยของเครือข่ายโดยเฉพาะ โดยมีหน่วยประมวลผลด้านความปลอดภัยโดยเฉพาะ (Security Processing Unit)
2. มีความสามารถในการทำงานเป็น Stateful Inspection Firewall
3. มีความสามารถในการป้องกันการบุกรุก (Intrusion Prevention) โดยสามารถตรวจจับการบุกรุกได้ด้วยวิธีการตรวจสอบด้วย signature และ Anomaly detection เป็นอย่างน้อย
4. คุณสมบัติด้านพอร์ตเชื่อมต่อเครือข่าย
   - 4.1. มีพอร์ตแบบ RJ45 10GE ports จำนวนไม่น้อยกว่า 8 ports
   - 4.2. มีพอร์ตแบบ SFP+ 10GE พร้อมติดตั้ง Transceivers (LR) ขนาด 10G จำนวน 8 ชิ้น
   - 4.3. มีพอร์ตแบบ QSFP28 100GbE พร้อมติดตั้ง Transceivers (LR) ขนาด 100G จำนวน 2 ชิ้น
   - 4.4. รองรับมาตรฐาน IEEE 802.1q (VLAN tagging)
   - 4.5. รองรับการทำ NAT (Network Address Translation), VIP (Virtual IP) ได้เป็นอย่างน้อย
5. คุณสมบัติด้านประสิทธิภาพ
   - 5.1. ความสามารถในการรองรับการเชื่อมต่อพร้อมกัน (Concurrent sessions) ได้ไม่น้อยกว่า 7,5000,000 การเชื่อมต่อวินาที และ รองรับการเชื่อมต่อใหม่ (New sessions) ไม่น้อยกว่า 650,000 การเชื่อมต่อต่อวินาที
   - 5.2. สนับสนุน IPv4 Firewall Throughput สำหรับการรับส่งข้อมูลแบบ UDP ที่ 1518 Byte ได้ไม่น้อยกว่า 198 Gbps
   - 5.3. สนับสนุนการตรวจสอบและป้องกันการโจมตีโดยมี IPS Throughput ไม่น้อยกว่า 19 Gbps, Threat Protection Throughput ไม่น้อยกว่า 13 Gbps และ Next Generation Firewall Throughput ไม่น้อยกว่า 15 Gbps
   - 5.4. สนับสนุนการทำ IPsec VPN และ SSL VPN โดยมี Throughput ไม่น้อยกว่า 55 Gbps และ 5.3 Gbps ตามลำดับ
6. คุณสมบัติด้านการบริหารจัดการ
   - 6.1. สามารถทำงานร่วมกับฐานข้อมูลผู้ใช้แบบ LDAP, RADIUS, Active Directory ได้
   - 6.2. สามารถบริหารจัดการอุปกรณ์ได้ทั้งทาง Web GUI (HTTP หรือ HTTPS), SSH, SNMP (v1, v2c, v3)

6.3. สามารสร้างบัญชีผู้ใช้บนตัวอุปกรณ์เอง (Local Database) ได้

6.4. สามารถส่ง Syslog มาเก็บไว้ยัง Syslog Server ได้

6.5. สามารถทำการแจ้งเตือนผู้ดูแลระบบด้วยอีเมล์ (Email notification) ในกรณีที่ตรวจพบไวรัส และการโจมตี

7. คุณสมบัติด้านการป้องกันการโจมตีผ่าน Web/Mail

7.1. สามารถทำงานในลักษณะ Content Filtering ได้ โดยสามารถกำหนดให้อุปกรณ์ป้องกันการเข้าถึง URL หรือ Web site ที่ต้องห้ามได้ (URL blocking)

7.2. สามารถกำหนดให้อุปกรณ์ป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้

7.3. สามารถกำหนดให้ป้องกัน Java applet, Cookies และ Active X ได้ และมีความสามารถในการตรวจจับและหยุดการทำงานของ Malware, Phishing หรือ Pharming ได้

7.4. สามารถป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้

7.5. สามารถป้องกัน Spam mail ได้ โดยสามารถตรวจสอบ Spam mail จาก MIME header, คำหรือวลีในเนื้อหาของ e-mail และ e-mail Address ได้

7.6. สามารถตรวจสอบ Spam mail จากคำหรือวลีในเนื้อหาของ e-mail ที่เป็นตัวอักษรภาษาไทยและภาษาอังกฤษได้เป็นอย่างน้อย

7.7. สามารถตรวจสอบ Spam mail จากฐานข้อมูลของผู้ผลิตผ่านเครือข่าย Internet ได้

7.8. สามารถทำการแจ้งเตือนผู้ดูแลระบบด้วย e-mail หรือเตือนผ่าน SNMP ไปยังซอฟต์แวร์จัดการระบบได้

7.9. สามารถทำการแจ้งเตือนผู้ดูแลระบบด้วย e-mail ในกรณีที่ตรวจพบ ไวรัส (Virus) และ การโจมตี (attacks) ได้

8. คุณสมบัติด้านการป้องกันไวรัส และการบุกรุก

8.1. มี Antivirus ที่สนับสนุนโปรโตคอล HTTP, FTP, SMTP, POP3, IMAP และช่องทาง VPN

8.2. มีความสามารถในการป้องกันการบุกรุก (Intrusion Prevention) โดยสามารถตรวจจับการบุกรุกได้ด้วยวิธีการตรวจสอบด้วย signature และ Anomaly detection เป็นอย่างน้อย

8.3. สามารถป้องกันการแพร่ของหนอนคอมพิวเตอร์ได้

8.4. ผู้ดูแลระบบสามารถทำการสร้างฐานข้อมูลรูปแบบการบุกรุกได้ด้วยตนเอง (Custom attack signature)

8.5. สามารถ update ฐานข้อมูลการบุกรุก (attack signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติ

8.6. อุปกรณ์ต้องสามารถ update ฐานข้อมูลไวรัสฯ (virus signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติ

9. ความสามารถด้านการจัดการ Bandwidth

9.1. มีความสามารถในการทำ Traffic Management แบบ Guarantee/Max/Priority bandwidth หรือเทียบเท่า ได้

9.2. สามารถควบคุมการเชื่อมโยงและจำกัดการใช้งาน Bandwidth ให้แก่โปรแกรมประเภท peer-to-peer ได้

9.3. สามารถกำหนดช่วงเวลาในการเข้าใช้งาน หรือไม่ใช้งาน (Time-based policies) ของแต่ละผู้ใช้งานได้

10. สามารถระบุชนิดและควบคุมการใช้งาน Application ต่าง ๆ ได้ไม่น้อยกว่า 2,900 Application

11. สามารถแสดงสถิติการทำงานของระบบต่างๆ ในตัวอุปกรณ์ หรือ Bandwidth ที่ใช้งานของระบบ

12. สนับสนุนการทำงานร่วมกับระบบวิเคราะห์ Log ของทางคณะได้

13. อุปกรณ์ได้รับการรับรองมาตรฐาน FCC, USGv6/IPv6, VCCI และ CE

14. มีการรับประกันอุปกรณ์ พร้อมสิทธิ์การ Update ข้อมูลทุกชนิดอย่างน้อย 5 ปี นับตั้งแต่วันที่คณะกรรมการตรวจรับ

15. เป็นของใหม่ไม่เคยใช้งานมาก่อน

16. ผู้ขายจะต้องทำการติดตั้งและอบรมการใช้งานให้กับเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ให้สามารถใช้งานอุปกรณ์และ แก้ไขปัญหาเบื้องต้นได้

17. ผู้เสนอราคาต้องเป็นบริษัทที่ได้รับหนังสือแต่งตั้งให้เป็นตัวแทนจำหน่ายจากบริษัทสาขาของผู้ผลิตในประเทศไทยหรือเจ้าของผลิตภัณฑ์

กำหนดส่งมอบ

กำหนดเวลาการส่งมอบพัสดุ หรือให้งานแล้วเสร็จภายใน ๙๐ วัน นับถัดจากวันที่ได้รับแจ้งจากคณะแพทยศาสตร์

เงื่อนไขการซ่อมครุภัณฑ์ในระยะประกัน

- รับประกันคุณภาพ 5 ปี นับจากวันที่ตรวจรับ
- หากครุภัณฑ์ชำรุดบกพร่องผู้ขายต้องดำเนินการแก้ไขให้ใช้งานได้ภายใน 7 วัน โดยนับจากวันที่คณะแพทยศาสตร์แจ้งให้ทราบทางโทรศัพท์หรือโทรสาร ก่อนเวลา 12.00 น. นับเป็นวันที่ 1 หาก หลัง 12.00 น. ให้นับวันถัดไปเป็นวันที่ 1
- หากผู้ขายซ่อมเกิน 7 วัน ผู้ขายต้องชำระค่าปรับวันละ 0.2% ของราคาเครื่อง/วัน จนกว่าจะซ่อมเสร็จให้ดี ดังเดิม โดยชำระค่าปรับภายในกำหนดเวลาที่คณะแพทยศาสตร์มีหนังสือแจ้ง หรือไม่ต้องชำระค่าปรับหาก มีเครื่องสำรองให้ใช้ทดแทนระหว่างดำเนินการซ่อม
- นอกเหนือจากการปรับข้างต้น หากในระยะประกันครุภัณฑ์ชำรุดและต้องใช้เวลาซ่อมให้ดีดังเดิมมากกว่า 7วัน เกิน 3 ครั้ง/ปี ผู้ขายต้องเปลี่ยนเครื่องใหม่ ให้คณะแพทยศาสตร์ ภายใน 60 วัน นับจากวันที่ คณะแพทยศาสตร์มีหนังสือแจ้งให้เปลี่ยน โดยครุภัณฑ์ใหม่ต้องเป็นเครื่องใหม่ที่มีคุณภาพไม่ต่ำกว่าครุภัณฑ์เดิม