ประกาศสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
เรื่อง การกำหนดหัวข้อร่างขอบเขตของงาน (Term of Reference: TOR)
โครงการจัดซื้อลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์
(Intrusion Prevention System)
มหาวิทยาลัยเชียงใหม่

1. หลักการและเหตุผล

ในการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์นั้นมีภัยคุกคามต่างๆ มากมายในหลากหลายรูปแบบ ทั้งจากภายในระบบเครือข่ายอินทราเน็ตขององค์กรเอง และจากระบบเครือข่ายอินเทอร์เน็ตภายนอกองค์กร ซึ่งมักจะประสบกับปัญหาในเรื่องของไวรัส มัลแวร์ ฟิชชิ่ง การโจมตีช่องโหว่ รวมถึงการที่อาจจะถูกเจาะระบบโดยผู้ไม่ประสงค์ดี ซึ่งนับวันยิ่งจะมีมากขึ้นและมีความรุนแรงสูงขึ้น มหาวิทยาลัยเชียงใหม่ก็เป็นหน่วยงานหนึ่งที่มีการเชื่อมต่อเข้าสู่ระบบเครือข่ายอินเทอร์เน็ต เพื่อใช้ประโยชน์ในด้านการเรียนการสอน การวิจัย และการบริหารงาน ซึ่งเชื่อมโยงผ่านระบบเครือข่ายหลักของมหาวิทยาลัยเชียงใหม่ (CMU-NET) ไปยังหน่วยงานต่างๆ ภายในมหาวิทยาลัย จึงทำให้ต้องมีการตระหนักถึงภัยคุกคามต่างๆ ดังกล่าวที่อาจเข้าสู่ระบบเครือข่ายหลักของมหาวิทยาลัยได้ ทั้งนี้เพื่อประโยชน์ของผู้ใช้งานภายในมหาวิทยาลัยที่จะใช้งานระบบเครือข่ายคอมพิวเตอร์ให้มีความปลอดภัยมากยิ่งขึ้น ซึ่งมีความจำเป็นอย่างยิ่งที่จะต้องมีระบบที่ช่วยในการกรองและป้องกันการโจมตีข้อมูลต่างๆ ที่เชื่อมต่อเข้าสู่ระบบอินเทอร์เน็ตให้มีความปลอดภัย โดยอาศัยระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) ซึ่งจะเป็นระบบที่ช่วยในการเฝ้าระวังภัยคุกคามต่างๆ ผ่านระบบเครือข่ายฯ อีกทั้งเมื่อสามารถตรวจจับภัยคุกคามต่างๆ ได้แล้วก็จะทำหน้าที่ป้องกันไม่ให้ภัยคุกคามเหล่านั้นเข้าสู่ระบบเครือข่ายหลักของมหาวิทยาลัยเชียงใหม่ได้อีกด้วย โดยได้ทำการติดตั้งซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) บนอุปกรณ์รักษาความปลอดภัย (Firewall) ให้มีความสามารถเพิ่มเติมในการป้องกันการรักษาความปลอดภัยและป้องกันการโจมตีระบบเครือข่ายในลักษณะแบบ Intrusion Prevention System เพื่อทำให้ระบบเครือข่ายคอมพิวเตอร์หลัก เครื่องคอมพิวเตอร์แม่ข่าย และข้อมูลสารสนเทศที่สำคัญของมหาวิทยาลัยมีความมั่นคงปลอดภัยมากยิ่งขึ้น แล้วแต่สิทธิ์การใช้งาน (License) กำลังจะหมดอายุการใช้งานลง ซึ่งจะส่งผลกระทบต่อความมั่นคงปลอดภัยของสารสนเทศต่างๆ ที่สำคัญของมหาวิทยาลัยได้

ดังนั้นสำนักฯ จึงมีความต้องการซื้อลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายเครือคอมพิวเตอร์ (Intrusion Prevention System) บนอุปกรณ์รักษาความปลอดภัย (Firewall) ของมหาวิทยาลัยเชียงใหม่ เพื่อทำให้ระบบเครือข่ายคอมพิวเตอร์หลัก เครื่องคอมพิวเตอร์แม่ข่าย และข้อมูลสารสนเทศที่สำคัญของมหาวิทยาลัยยังคงมีเสถียรภาพและมีความมั่นคงปลอดภัยอย่างต่อเนื่องต่อไป

2. วัตถุประสงค์

2.1 เพื่อให้ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) สามารถทำงานได้ด้วยความมั่นคงปลอดภัย และมีประสิทธิภาพอย่างต่อเนื่อง

2.2 เพื่อให้หน่วยงานภายใน นักศึกษา และบุคลากรของมหาวิทยาลัยมีความพึงพอใจและเกิดความเชื่อมั่นในการใช้งานระบบเครื่องคอมพิวเตอร์และระบบเครือข่ายของมหาวิทยาลัย

3. ผู้มีสิทธิเสนอราคาจะต้องมีคุณสมบัติ ดังต่อไปนี้

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคล ผู้มีอาชีพให้ขายพัสดุที่ประกวดราคาซื้อด้วยวิธีอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอราคาได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

3.11 เป็นนิติบุคคลที่จดทะเบียนในประเทศไทยและประกอบธุรกิจทางด้านระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์มาแล้วไม่น้อยกว่า 2 ปี ณ วันที่ยื่นซอง และมีเงินทุนจดทะเบียนไม่น้อยกว่า 1 ล้านบาท

3.12 ผู้เสนอราคาจะต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทยโดยให้ยื่นขณะเข้าเสนอราคา

4. การพิจารณาทางเทคนิค

4.1 มหาวิทยาลัยเชียงใหม่จะพิจารณาราคาเฉพาะของผู้เข้าประกวดราคาที่ผ่านข้อเสนอทางเทคนิคและผ่านข้อกำหนดเกี่ยวกับคุณสมบัติเท่านั้น นอกจากนี้มหาวิทยาลัยเชียงใหม่ยังขอสงวนสิทธิ์ในการพิจารณาลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) และอุปกรณ์ประกอบอื่น ๆ (ถ้ามี) ที่ผู้เข้าประกวดราคาเสนอซึ่งมีคุณสมบัติอื่นที่นอกเหนือไปจากคุณสมบัติที่จำเป็นและคุณสมบัติที่ควรมี และมหาวิทยาลัยสงวนสิทธิ์ที่จะพิจารณาผู้เข้าประกวดราคารายที่เสนอราคาอยู่ในวงเงิน และให้ประโยชน์แก่มหาวิทยาลัยมากที่สุดก่อน

4.2 ผู้เข้าประกวดราคามีหน้าที่แสดงเอกสารต่าง ๆ เพื่อยืนยันหรือแสดงให้เห็นถึงคุณสมบัติต่าง ๆ ที่จะต้องเป็นไปตามข้อกำหนดหรือมีคุณสมบัติที่ดีกว่าข้อกำหนด โดยเอกสารที่นำมาแสดงจะต้องเป็นเอกสารหรือเป็นเอกสารสำเนาที่เป็นทางการ สามารถเชื่อถือได้ และเป็นที่ยอมรับโดยทั่วไป ซึ่งผู้เข้าประกวดราคามีหน้าที่จะต้องเปรียบเทียบข้อกำหนดที่มหาวิทยาลัยกำหนดในแต่ละข้อกับคุณสมบัติของตนเองและของอุปกรณ์ต่าง ๆ ที่เสนอ โดยจะต้องระบุให้ชัดเจนว่าเอกสารที่นำมาเสนอ ข้อความในประโยคใดที่ใช้ยืนยันข้อกำหนดหมายเลขใดของมหาวิทยาลัย โดยผู้เข้าประกวดราคามีหน้าที่ทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน ได้แก่ การขีดเส้นใต้ หรือ การระบายสี พร้อมระบุหมายเลขลำดับของข้อกำหนดที่จะทำการยืนยันให้เห็นชัดเจน ซึ่งหากผู้เข้าประกวดราคาขาดเอกสารยืนยัน หรือขาดการทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน หรือแสดงเอกสารไม่ชัดเจนทำให้ขาดข้อกำหนดหนึ่งใดในข้อกำหนดของมหาวิทยาลัย ให้ถือว่าผู้เข้าประกวดราคาไม่ผ่านการพิจารณาทางด้านเทคนิค

4.3 ให้จัดทำรายละเอียดข้อเสนอด้านเทคนิคของระบบงานที่เสนอ ในรูปแบบดังต่อไปนี้

หัวข้อ	คุณลักษณะที่กำหนด	คุณลักษณะที่เสนอ	เอกสารอ้างอิง (หน้า, ข้อ)
ระบุหัวข้อให้ตรงกับที่กำหนดในเอกสารนี้	ให้คัดลอกจากข้อกำหนดที่กำหนดในเอกสารนี้	ให้ระบุความสามารถหรือคุณลักษณะเฉพาะของระบบที่เสนอ	ให้ระบุหรืออ้างอิงถึงเอกสารในข้อเสนอที่เกี่ยวข้อง และทำสัญลักษณ์แสดงข้อความในประโยคของเอกสารหรือในแคตตาล็อกนั้นให้ชัดเจน

4.4 ผู้เข้าประกวดราคาจะต้องเสนอลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) และอุปกรณ์อื่น ๆ (ถ้ามี) ตามที่มหาวิทยาลัยกำหนดเท่านั้น ซึ่งหากผู้เข้าประกวดราคาได้เสนอรายการรายละเอียดอื่นใดที่นอกเหนือไปจากข้อกำหนดดังกล่าว มหาวิทยาลัยขอสงวนสิทธิ์ในการเปลี่ยนแปลงรายการอุปกรณ์และระบบที่เสนอดังกล่าวได้ในภายหลัง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพ

5. กำหนดระยะเวลาการดำเนินการ

ผู้ชนะการประกวดราคาต้องทำการติดตั้งและส่งมอบลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) รวมถึงจะต้องบำรุงรักษาระบบและรับประกันให้สามารถใช้งานได้อย่างมีประสิทธิภาพตามคุณลักษณะและสิทธิ์ของการใช้งานดังกล่าว เป็นเวลา 12 เดือน นับจากวันที่หมดอายุสิทธิ์การใช้งานระบบป้องกันภัยเครือข่ายคอมพิวเตอร์เดิม ภายในระยะเวลา 60 วัน นับจากวันลงนามในสัญญาซื้อ ซึ่งหากเกินกว่าระยะเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราร้อยละ 0.2 ต่อวันของวงเงินที่ประมูลได้

6. ขอบเขตลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์

ลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) จะต้องเป็นไปตามข้อกำหนด ของ TOR ให้ครบตามข้อกำหนด

7. ข้อกำหนดการดำเนินการ

7.1 ก่อนที่ผู้ชนะการประกวดราคาจะเข้าดำเนินการใด ๆ ผู้ชนะการประกวดราคาจะต้องทำจดหมายแจ้งให้กับมหาวิทยาลัยรับทราบก่อนจะเข้าดำเนินการจริงอย่างน้อย 5 วันทำการ และจะต้องรอให้ได้รับการอนุมัติจากมหาวิทยาลัยก่อน จึงจะสามารถดำเนินการใด ๆ ได้ ซึ่งหากผู้ชนะการประกวดราคาเข้าทำการติดตั้งระบบใด ๆ โดยไม่ได้รับการอนุมัติจากมหาวิทยาลัย มหาวิทยาลัยมีสิทธิที่จะให้บริษัทดำเนินการรื้อถอนระบบต่าง ๆ ที่ได้ติดตั้งไปแล้ว โดยให้ถือเป็นความผิดและความรับผิดชอบของผู้ชนะการประกวดราคา

7.2 ผู้ชนะการประกวดราคาต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น เนื่องจากการติดตั้งอุปกรณ์หรือความเสียหายใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็วและยินยอมชดใช้ค่าเสียหายที่เกิดขึ้นให้กับมหาวิทยาลัย

7.3 การติดตั้งและส่งมอบลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) และอุปกรณ์ประกอบอื่น ๆ (ถ้ามี) ที่ผู้ชนะการประกวดราคาได้เสนอหรือติดตั้งอุปกรณ์และระบบอื่นใดเพิ่มเติม ซึ่งหากไม่ได้ระบุไว้ในข้อกำหนดของมหาวิทยาลัยให้อยู่ในดุลยพินิจของมหาวิทยาลัยที่จะเป็นผู้กำหนดลักษณะและรูปแบบของการติดตั้ง โดยขึ้นอยู่กับความจำเป็นและสภาพการใช้งานจริง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพเป็นสำคัญ

8. รายการที่มหาวิทยาลัยต้องการ

มหาวิทยาลัยเชียงใหม่มีความต้องการจะซื้อลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) บนอุปกรณ์รักษาความปลอดภัย (Firewall) เดิมของมหาวิทยาลัย ยี่ห้อ Palo Alto Networks ซึ่งมีหมายเลขเครื่อง (Serial Number) 013101000928 โดยจะต้องบำรุงรักษาและต่ออายุสิทธิ์การใช้งาน (License) เป็นเวลา 12 เดือน นับจากวันที่หมดอายุสิทธิ์การใช้งานของเดิม

9 การตรวจรับการบำรุงรักษา

9.1 ผู้ชนะการประกวดราคาต้องจัดเตรียมเอกสารต่าง ๆ สำหรับการส่งมอบและการตรวจรับอย่างเหมาะสมให้กับทางมหาวิทยาลัยเชียงใหม่พิจารณา โดยจะต้องมีหลักฐานแสดงการส่งมอบและใช้สิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) ของมหาวิทยาลัยเชียงใหม่เป็นเวลา 12 เดือน

9.2 ผู้ชนะการประกวดราคาต้องทำหนังสือแจ้งการส่งมอบงานเพื่อตรวจรับ ให้ทางมหาวิทยาลัยเชียงใหม่ทราบอย่างน้อย 5 วันทำการ ก่อนการส่งมอบ ผู้ชนะการประกวดราคาต้องจัดทำเอกสารระบุอุปกรณ์ คู่มือ หรือสิ่งอื่นใดที่จะทำการตรวจรับ โดยระบุ ชนิด ยี่ห้อ รุ่น หมายเลขประจำอุปกรณ์ (Serial Number) สถานที่ติดตั้งหรือรายละเอียดอื่นใดที่จำเป็นในการตรวจรับให้มหาวิทยาลัยเชียงใหม่ทราบ

10. การดูแลรักษาและการรับประกัน

10.1 เมื่อผู้ชนะการประกวดราคาส่งมอบลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) และตรวจรับเป็นที่เรียบร้อยแล้ว ผู้ชนะการประกวดราคาจะต้องบำรุงรักษาระบบและรับประกันให้สามารถใช้งานได้อย่างมีประสิทธิภาพตามคุณลักษณะและสิทธิ์ของการใช้งานดังกล่าว จนถึงวันสิ้นสุดอายุสิทธิ์การใช้งานของระบบ

10.2 ผู้ชนะการประกวดราคาจะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ และกฎระเบียบต่าง ๆ ด้านความมั่นคงปลอดภัยสารสนเทศของสำนักบริการเทคโนโลยีสารสนเทศอย่างเคร่งครัด

10.3 ผู้ชนะการประกวดราคาจะต้องปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ ที่เกี่ยวข้อง เช่น พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พรบ.ลิขสิทธิ์ พรบ.คุ้มครองข้อมูลส่วนบุคคล พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

10.4 ผู้ชนะการประกวดราคาจะต้องไม่เปิดเผยหรือเผยแพร่ข้อมูลที่สำคัญต่าง ๆ เช่น การตั้งค่าของระบบ (Configuration) รหัสผ่าน (Password) แผนผังของระบบ (Diagram) เป็นต้น ให้บุคคลอื่นทราบโดยไม่ได้รับอนุญาต อนึ่งไม่ว่าเวลาใด แม้สิ้นสุดสัญญาก็ตาม การรักษาข้อมูลที่สำคัญต่างๆ ยังคงมีผลผูกพันกับคู่สัญญาต่อไป มิฉะนั้นมหาวิทยาลัยจะดำเนินการเรียกร้องค่าเสียหายโดยถือเป็นความผิดของผู้ชนะการประกวดราคา

11. ระยะเวลาส่งมอบ 60 วัน

12. วงเงินในการจัดซื้อจัดจ้าง 1,500,000 บาท (หนึ่งล้านห้าแสนบาทถ้วน)

13. สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติมหรือเสนอแนะวิจารณ์หรือแสดงความคิดเห็นโดยเปิดเผยตัว

สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
เลขที่ 239 ถนนห้วยแก้ว ตำบลสุเทพ อำเภอเมือง จังหวัดเชียงใหม่ 50200
โทรศัพท์ 053-94-3807
โทรสาร 053-94-3825
E-mail : sudruethai.j@cmu.ac.th, sajja.t@cmu.ac.th

14. หน่วยงานที่รับผิดชอบ

สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่

(ลงชื่อ).....รัฐสิทธิ์ สุขะหุต.....ประธานคณะกรรมการ
(รองศาสตราจารย์ ดร.รัฐสิทธิ์ สุขะหุต)
ผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศ

(ลงชื่อ).....สัจจะ ตันจันทร์พงศ์.....กรรมการ
(นายสัจจะ ตันจันทร์พงศ์)

(ลงชื่อ).....โอภาส หมื่นแสน.....กรรมการ
(นายโอภาส หมื่นแสน)

(ลงชื่อ).....ศุภวิทย์ วรรณภิละ.....กรรมการ
(นายศุภวิทย์ วรรณภิละ)

(ลงชื่อ).....สุภาพ สิทธิพานิช.....เลขานุการ
(นางสุภาพ สิทธิพานิช)

ภาคผนวก ก

คุณสมบัติของลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) ที่มหาวิทยาลัยต้องการ ซึ่งทั้งหมดจะต้องมีคุณสมบัติดังต่อไปนี้เป็นอย่างน้อย ประกอบด้วย

1. ลิขสิทธิ์ซอฟต์แวร์ระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) จำนวน 1 ปี

    1.1 สามารถติดตั้งใช้งานบนอุปกรณ์รักษาความปลอดภัย (Firewall) ของมหาวิทยาลัยได้
    1.2 มีความสามารถทำ Threat prevention หรือ Intrusion Prevention โดยมี Throughput ไม่น้อยกว่า 20 Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix และรองรับจำนวน Max Sessions ได้ไม่น้อยกว่า 8,000,000 sessions และ New Sessions ไม่น้อยกว่า 290,000 ต่อวินาที
    1.3 สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound) รวมทั้งการทำ SSL Decryption Broker ได้
    1.4 สามารถทำการตรวจจับ และป้องกันการโจมตีได้ ด้วยการตรวจสอบแบบ Stream-based ได้
    1.5 สามารถป้องกันภัยคุกคามประเภท Vulnerability และ Spyware ได้โดยสามารถมีการอัพเดท Signature ใหม่แบบอัตโนมัติได้
    1.6 สามารถตรวจจับและป้องกัน Buffer Overflow, DoS/DDoS, Non-RFC compliant protocol, Port scans, Host sweeps, Malformed Packets, IP/Protocol defragmentation และ TCP reassembly ได้เป็นอย่างน้อย รวมทั้งสามารถปรับแต่งรูปแบบของภัยคุกคาม (Custom signatures) ได้ตามความต้องการ
    1.7 สามารถป้องกันทราฟฟิกที่จะมีการติดต่อสื่อสาร (Command and Control) กลับไปยัง Malicious Domain พร้อมทั้งระบุเครื่องที่ติด malware ดังกล่าวได้ หรือสามารถกำหนด IP ภายในขึ้นมาเพื่อทำหน้าที่ในการป้องกันการติดต่อสื่อสารกลับไปยัง Malicious Domain ได้ (DNS Sinkhole)
    1.8 สามารถตรวจจับการโจมตีที่แอบแฝงเข้ามาผ่าน compressed files และ web content ได้
    1.9 สามารถตรวจจับการโจมตีที่แอบแฝงเข้ามาผ่าน payload ของไฟล์ประเภทต่างๆ อาทิ Microsoft Office Document หรือ PDF ได้
    1.10 สามารถป้องกันการ Download Malware โดยไม่ได้ตั้งใจ (Drive-by Download Protection) โดยสามารถแจ้งเตือนผู้ใช้งาน เพื่อให้ผู้ใช้งานสามารถยืนยันการ Download ไฟล์ดังกล่าวได้
    1.11 สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้