

- 7.17 สามารถป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้ โดยมีสิทธิ์ในการเข้าตรวจสอบฐานข้อมูลประเภทของ Web site ได้ตลอดระยะเวลาของการรับประกัน
- 7.18 รองรับการตรวจสอบผู้ใช้ (User Authentication) กับฐานข้อมูลผู้ใช้ภายในตัวอุปกรณ์, ผู้ใช้ใน RADIUS, ใน LDAP และ Windows Active Directory ได้เป็นอย่างดี
- 7.19 สามารถเก็บข้อมูลจราจรดังต่อไปนี้ ได้เป็นอย่างดี
- IP address ต้นทาง (source IP address)
 - IP address ปลายทาง (destination IP address)
 - Service port ปลายทาง (destination port)
 - วันและเวลาของการเชื่อมต่อ
 - ชื่อของผู้ใช้งาน เมื่อมีการระบุตัวบุคคล (authentication)
- 7.20 รองรับในการทำ High Availability (HA) แบบ Active-Active โดยไม่ต้องเสียค่าใช้จ่ายเพิ่ม
- 7.21 สามารถใช้งานตามมาตรฐาน IPv6 ได้
- 7.22 มีอุปกรณ์จ่ายไฟฟ้า (Power Supply) แบบ Redundant
- 7.23 สามารถส่งข้อมูลจราจรไปจัดเก็บ วิเคราะห์ข้อมูล และออกรายงานร่วมกับอุปกรณ์จัดเก็บและวิเคราะห์ข้อมูลระบบเครือข่ายที่ ศทส. ใช้งานได้เป็นอย่างดี
- 7.24 มีสิทธิ์ในการ Upgrade firmware และรับประกันอุปกรณ์เป็นเวลาไม่น้อยกว่า 1 ปี

เอกสารแนบ 8

8. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน 1 เครื่อง ต้องมีคุณลักษณะพื้นฐานที่สำคัญ ดังนี้

- 8.1 เป็นอุปกรณ์ที่ทำหน้าที่ในการป้องกันด้าน Web Application หรือ Web Service โดยเฉพาะ สามารถติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด 19 นิ้ว ได้
- 8.2 ได้รับการรับรองมาตรฐาน Web Application Firewall (WAF) จาก ICSA
- 8.3 มีความสามารถในการทำงานและปกป้อง Web Application ต่างๆ ได้ โดยรองรับ HTTPS ได้เป็นอย่างดี
- 8.4 รองรับการส่งผ่านข้อมูลได้อย่างน้อย 10,000 HTTP ต่อวินาที หรือ 10,000 Transactions ต่อวินาที หรือดีกว่า
- 8.5 อุปกรณ์ต้องมีหน่วยประมวลผลที่ทำงาน SSL โดยเฉพาะ (SSL offload) เพื่อเพิ่มประสิทธิภาพในการตรวจสอบข้อมูล
- 8.6 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 3 ช่อง
- 8.7 มีความจุรวมของหน่วยเก็บข้อมูล (Harddisk) ไม่ต่ำกว่า 1 TB
- 8.8 มี Throughput อย่างน้อย 100 Mbps
- 8.9 สามารถตรวจจับพฤติกรรมการใช้งาน Web Application ของผู้ที่เข้ามาใช้บริการ Web Application บนเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ได้
- 8.10 อุปกรณ์ที่นำเสนอจะต้องสามารถทำงานแบบ In-Line (Bridge), Reverse Proxy หรือ Transparent และ Spanmode (Monitor) สำหรับตรวจสอบพฤติกรรม ได้เป็นอย่างดี
- 8.11 รองรับการป้องกันการถูกโจมตีด้วยวิธีต่างๆ ได้อย่างน้อย ดังนี้
 - Cross-site Scripting/Cross-site Request Forgery
 - Cookie Poisoning/Cookie Tampering
 - Buffer Overflow
 - SQL infection/Injection
 - HTTP request smuggling
 - Encoding attacks
 - Remote file inclusion
 - Forms Tampering
 - Schema Poisoning
 - XML Parameter Tampering/Intrusion Prevention

/8.12 สามารถ...

- 8.12 สามารถป้องกันการถูกเปลี่ยนข้อมูลบน Website ได้ (Anti Web Defacement)
- 8.13 สามารถตรวจสอบหาช่องโหว่ที่มีความเสี่ยงต่อการถูกโจมตีได้ (Web Application Vulnerability Assessments หรือ Vulnerability Scan)
- 8.14 อุปกรณ์ต้องสามารถเก็บ log ไว้ในตัวอุปกรณ์เอง และสามารถส่งข้อมูล Log File แบบ Syslog ได้ เป็นอย่างน้อย
- 8.15 สามารถสร้าง admin Profile เพื่อให้สิทธิ์ในการเข้าถึงที่ไม่เท่ากันสำหรับผู้ดูแลระบบ
- 8.16 สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser หรือ CLI ได้ เป็นอย่างน้อย
- 8.17 สามารถปรับเทียบเวลา (Sync) กับอุปกรณ์ภายนอกได้
- 8.18 สามารถทำรายงานการถูกโจมตีได้ในรูปแบบ HTML หรือ PDF หรือ XLS หรือดีกว่า
- 8.19 สามารถใช้งานตามมาตรฐาน IPv6 ได้
- 8.20 มีสิทธิ์ในการ Upgrade firmware และรับประกันอุปกรณ์เป็นเวลาไม่น้อยกว่า 1 ปี

เอกสารแนบ 9

9. อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ 2

จำนวน 1 เครื่อง ต้องมีคุณลักษณะพื้นฐานที่สำคัญ ดังนี้

- 9.1 เป็นอุปกรณ์ (Hardware Appliance) ที่ออกแบบมาเพื่อป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System) โดยเฉพาะ
- 9.2 สามารถทำงานได้ในโหมด Passive และ In-line หรือดีกว่า
- 9.3 สามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้อย่างน้อย ดังนี้ Signature matching, Protocol / Packet Anomalies, Statistical anomalies หรือ Application anomalies, Overflow, Worm, Virus, Backdoor Program, Trojan Horse, Port Scanning, Spy ware, Packet Analysis, DoS, DDoS
- 9.4 สามารถทำงานได้อย่างน้อย 3 segments ใน IPS mode
- 9.5 มีความสามารถในการตรวจจับ (Throughput) ไม่น้อยกว่า 1 Gbps และอุปกรณ์สามารถรองรับ Concurrent Connections ไม่น้อยกว่า 2,000,000 Concurrent Connections
- 9.6 มี Network Interface แบบ Gigabit Ethernet ไม่น้อยกว่า 8 พอร์ต
- 9.7 เมื่ออุปกรณ์เกิดปัญหาสามารถทำงานได้อย่างต่อเนื่อง (Bypass Traffic) โดยช่องสัญญาณ In-Line Mode สามารถรับส่งข้อมูลได้ตามปกติ
- 9.8 สามารถป้องกันการโจมตีและการบุกรุกเครือข่ายได้อย่างน้อย ดังนี้
 - ป้องกันการระบาดของ Virus และ Worm ได้
 - ป้องกันการโจมตีแบบ Denial of Server (DoS) Attack และ DDoS ได้
 - ป้องกันการบุกรุกแบบ Vulnerability Exploit, Reconnaissance (port scan/sweep) ได้
 - ป้องกันเทคนิคการหลบซ่อนการโจมตีแบบ IP Defragmentation, TCP Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, HTML Evasion และ FTP Evasion ได้
 - ป้องกันเครือข่ายและสามารถตรวจจับวิธีการบุกรุก ดังนี้ Overflow, Backdoor Program, Trojan Horse และ Spy ware ได้
- 9.9 สามารถแจ้งเตือนและโต้ตอบการโจมตีด้วยวิธี Drop เมื่อเกิดเหตุการณ์ถึงจำนวนที่ตั้งไว้ (Threshold) ได้
- 9.10 อุปกรณ์ IPS จะต้องถูกออกแบบมาให้มีความน่าเชื่อถือสูง โดยจะต้องมีระบบ Redundant Power Supply จำนวนไม่น้อยกว่า 2 ชุด โดยสามารถถอดเปลี่ยนแบบ Hot-Swap ได้ และใช้อุปกรณ์ เช่น SSD แทนฮาร์ดดิสก์ในการเก็บข้อมูล
- 9.11 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้ เป็นอย่างน้อย

/9.12 สามารถ...

9.12 สามารถบริหารจัดการอุปกรณ์ผ่าน Command-line หรือ GUI ได้ โดยผ่านเว็บแบบ HTTPS และมีระบบบริหารจัดการจากศูนย์กลาง เพื่อจัดการอุปกรณ์ โดยมีความสามารถอย่างน้อย ดังต่อไปนี้

- สามารถบริหารจัดการ การจัดเก็บและส่ง Log ไปที่ระบบจัดเก็บ Log ศูนย์กลาง (Centralized Log Management) ได้
- สามารถแสดงสถานะการทำงานของอุปกรณ์ (Dashboard) ได้ โดยแสดงถึงสถานะการถูกโจมตีของระบบเครือข่าย และเลือกแสดงในระดับความรุนแรงที่สนใจ โดยสามารถเลือกแสดงเฉพาะการโจมตีที่มีผลกระทบอย่างรุนแรงกับเครือข่ายที่กำหนดได้
- สามารถปรับแต่งการแสดงผลของ Dashboard โดยกำหนดเงื่อนไขที่ต้องการแสดง (search criteria) ได้เอง รวมถึงสามารถปรับช่วงเวลาการแสดงผลข้อมูลได้ออย่างน้อยเป็นชั่วโมง หรือ วัน
- สามารถกำหนดให้มีการดึงข้อมูล signature/rule จากผู้ผลิตได้อัตโนมัติ
- อนุญาตให้ผู้ใช้สามารถสร้างรูปแบบการตรวจสอบเองได้ (custom signature/rule) โดยมีเครื่องมือ หรือ GUI เพื่อช่วยในการสร้าง
- สามารถนำเสนอข้อมูลผ่านระบบแอปพลิเคชัน ทั้งในลักษณะจำนวน flow หรือปริมาณข้อมูล (KB/s) ได้
- สามารถจัดเก็บข้อมูลที่มีการโจมตี (Packet Capture) และสามารถเรียกดูได้โดยตรงจากอุปกรณ์บริหารจัดการ
- สามารถแสดงข้อมูลตำแหน่ง (Geolocation) ผ่านระบบได้

9.13 ระบบจะต้องสามารถให้คำแนะนำและปรับแต่งนโยบายเรื่องความปลอดภัยได้อย่างอัตโนมัติ โดยอาศัยข้อมูล ทั้งจากการทำ Passive Scan หรือ Active Scan

9.14 สามารถใช้งานมาตรฐาน IPv6 ทั้งการจัดการ IPS และการตรวจสอบข้อมูลการโจมตี โดยผ่านการทดสอบจากหน่วยงานที่น่าเชื่อถือ เช่น ICSA หรือ USGv6

9.15 ได้รับการรับรองมาตรฐาน FCC, UL หรือ CE เป็นอย่างน้อย

9.16 ได้รับการรับรองมาตรฐานจาก ICSA หรือ NSS Labs หรือ Common Criteria เป็นอย่างน้อย

9.17 มีสิทธิ์ในการ Upgrade firmware และรับประกันอุปกรณ์เป็นเวลาไม่น้อยกว่า 1 ปี

รายชื่อสำนักงานพัฒนาสังคมและความมั่นคงของมนุษย์จังหวัด (สนง.พมจ.) 5 จังหวัด
ที่ได้รับการจัดสรรครุภัณฑ์คอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย
ทดแทนเครื่องเดิมที่หมดอายุการใช้งาน ประจำปี 2558

ครุภัณฑ์คอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย สำหรับสนง.พมจ. 5 จังหวัด
จำนวน 4 รายการ 20 หน่วย ประกอบด้วย

- ① เครื่องคอมพิวเตอร์แม่ข่ายสำหรับงานประมวลผล แบบที่ 1
- ② อุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (UTM Firewall)
- ③ อุปกรณ์กระจายสัญญาณ (L2 Switch) ขนาด 24 ช่อง
- ④ เครื่องสำรองไฟฟ้า ขนาด 2 KVA

ที่	หน่วยงาน	จำนวนเครื่อง/ชุด				สถานที่ตั้งหน่วยงาน
		①	②	③	④	
1	ตาก	1	1	1	1	ศาลากลางจังหวัดตาก (หลังเก่า) ถนนพหลโยธิน ตำบลระแหง อำเภอเมือง จังหวัดตาก 63000
2	นครนายก	1	1	1	1	ศาลากลางจังหวัดนครนายก ตำบลท่าช้าง อำเภอเมือง จังหวัดนครนายก 26000
3	นครปฐม	1	1	1	1	ศาลากลางจังหวัดนครปฐม อำเภอเมือง จังหวัดนครปฐม 73000
4	เพชรบุรี	1	1	1	1	ศาลากลางจังหวัดเพชรบุรี ชั้น 1 ถนนราชวิถี อำเภอเมือง จังหวัดเพชรบุรี 76000
5	ราชบุรี	1	1	1	1	ศาลากลางจังหวัดราชบุรี อำเภอเมือง จังหวัดราชบุรี 70000