

เอกสารแนบ 1

1. เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ 1 พร้อมระบบปฏิบัติการ Windows Server Standard 2012 จำนวน 5 ชุด แต่ละชุดต้องมีคุณลักษณะพื้นฐานที่สำคัญ ดังนี้

- 1.1 มีหน่วยประมวลผลกลาง (CPU) แบบ 6 แกนหลัก (6 core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะ และมีความเร็วสัญญาณนาฬิกาไม่น้อยกว่า 2.0 GHz จำนวนไม่น้อยกว่า 1 หน่วย
- 1.2 CPU รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory ไม่น้อยกว่า 15 MB
- 1.3 มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR3 หรือดีกว่า มีขนาดไม่น้อยกว่า 8 GB
- 1.4 สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1, 5
- 1.5 มีหน่วยจัดเก็บข้อมูล (Hard Disk) แบบ Hot Swap หรือ Hot Plug ชนิด SCSI หรือ SAS หรือ SATA ที่มีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อวินาที หรือ ชนิด Solid State Drives หรือดีกว่า และมีขนาดความจุไม่น้อยกว่า 300 GB จำนวนไม่น้อยกว่า 2 หน่วย
- 1.6 มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวน 1 หน่วย
- 1.7 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-TX หรือ Gigabit Ethernet หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง
- 1.8 มีจอภาพแบบ LCD ขนาดไม่น้อยกว่า 17 นิ้ว จำนวน 1 หน่วย
- 1.9 มี Power Supply แบบ Redundant Power Supply หรือ Hot Swap ขนาดไม่ต่ำกว่า 500 Watt จำนวน 2 หน่วย
- 1.10 มีระบบพัดลมระบายความร้อนภายในเครื่อง (Fan) แบบ Redundant หรือดีกว่า
- 1.11 เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอ ต้องได้รับการรับรองตามมาตรฐาน FCC, UL เป็นอย่างน้อย
- 1.12 ติดตั้งโปรแกรมระบบปฏิบัติการ Windows Server Standard 2012 หรือดีกว่า ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
- 1.13 ต้องมีการรับประกันแบบ On-site Service เป็นระยะเวลาอย่างน้อย 3 ปี

เอกสารแนบ 2

2. อุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (UTM Firewall) จำนวน 5 เครื่อง
แต่ละเครื่องต้องมีคุณลักษณะพื้นฐานที่สำคัญ ดังนี้

- 2.1 เป็นอุปกรณ์ Firewall ชนิด Stateful Inspection firewall แบบ Appliance
- 2.2 มี Throughput ของ Firewall Inspection จำนวนไม่น้อยกว่า 5 Gbps
- 2.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-TX หรือ Gigabit Ethernet หรือดีกว่า จำนวนไม่น้อยกว่า 8 ช่อง
- 2.4 สามารถรองรับ TCP concurrent sessions ได้อย่างน้อย 500,000 Sessions และรองรับ New TCP session rate ได้อย่างน้อย 12,000 (Sessions/sec)
- 2.5 สามารถรองรับการเชื่อมต่อ VPN แบบ IPsec ได้อย่างน้อย 2,000 Tunnels และแบบ SSL ได้อย่างน้อย 55 Tunnels
- 2.6 สามารถรองรับ VPN throughput ได้อย่างน้อย 900 Mbps
- 2.7 มีระบบ Intrusion Detection and Prevention (IDP) ที่สามารถรองรับการ Automatic signature updates จากฐานข้อมูลภายนอกได้อย่างน้อย 1 ปี
- 2.8 มีระบบ Anti-Spam ที่สามารถรองรับการตรวจสอบจากฐานข้อมูลภายนอกได้อย่างน้อย 1 ปี
- 2.9 มีระบบ Anti-Virus ที่สามารถรองรับการ Automatic signature updates จากฐานข้อมูลภายนอกได้อย่างน้อย 1 ปี
- 2.10 มีระบบ Content Filtering ที่สามารถรองรับการตรวจสอบจากฐานข้อมูลภายนอกได้อย่างน้อย 1 ปี
- 2.11 สามารถรองรับ UTM throughput (AV and IDP) ได้อย่างน้อย 500 Mbps
- 2.12 สามารถรองรับระบบ Application intelligence and optimization ได้
- 2.13 สามารถรองรับการทำงานแบบ SSL Inspection ได้
- 2.14 สามารถรองรับการทำงาน WAN load balancing ได้
- 2.15 สามารถรองรับการทำงานแบบ Application Bandwidth Management ได้
- 2.16 สามารถรองรับการทำงาน Authentication แบบ Web Portal โดยสามารถตรวจสอบสิทธิ์จากฐานข้อมูลได้อย่างน้อยดังนี้ Local User Database, Microsoft Windows Active Directory (AD), LDAP, RADIUS
- 2.17 สามารถใช้งานตามมาตรฐาน IPv6 ได้
- 2.18 สามารถทำ Routing Protocol แบบ RIP v1/v2, และ OSPF ได้
- 2.19 สามารถรองรับการส่ง Log เพื่อเก็บลงฐานข้อมูลได้
- 2.20 อุปกรณ์สามารถสรุปรายงานการใช้งานในแต่ละวันได้ (Daily Report)
- 2.21 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

/2.22 มีระบบ...

- 2.22 มีระบบตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ ได้ อย่างน้อยดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoof, IP Address Sweep, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, TCP Fragment, ICMP Fragment เป็นต้น
- 2.23 สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้
- 2.24 สามารถ Routing แบบ Static, Dynamic Routing ได้
- 2.25 สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) โดยเก็บเป็น Syslog ได้
- 2.26 มีการรับประกันอุปกรณ์เป็นเวลาไม่น้อยกว่า 1 ปี

เอกสารแนบ 3

3. อุปกรณ์กระจายสัญญาณ (L2 Switch) ขนาด 24 ช่อง แบบที่ 2 จำนวน 5 ชุด แต่ละชุดต้องมี
คุณลักษณะพื้นฐานที่สำคัญ ดังนี้

- 3.1 มีลักษณะการทำงานไม่น้อยกว่า Layer 2 ของ OSI Model
- 3.2 มีสัญญาณไฟแสดงสถานะของการทำงานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง
- 3.3 สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้
- 3.4 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-TX หรือ Gigabit Ethernet หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง
- 3.5 มี Slot รองรับการเพิ่ม Module แบบ SFP หรือ GBIC จำนวนไม่น้อยกว่า 4 พอร์ต
- 3.6 มีหน่วยความจำแบบ Flash Memory ขนาดไม่น้อยกว่า 32 MB
- 3.7 มีหน่วยความจำหลักในการประมวลผล (SDRAM or DRAM) ขนาดไม่น้อยกว่า 128 MB
- 3.8 มีขนาดของ Switch Capacity ไม่น้อยกว่า 50 Gbps
- 3.9 มี Forwarding Rate ไม่น้อยกว่า 40 Mbps
- 3.10 สามารถรองรับจำนวน MAC Address ได้ ไม่น้อยกว่า 16 K
- 3.11 สามารถทำ Spanning Tree Protocol ได้ ตามมาตรฐาน IEEE802.1d, 802.1w
- 3.12 สามารถทำงานแบบ Link Aggregation ได้ ตามมาตรฐาน IEEE 802.3ad
- 3.13 รองรับ Jumbo Frame ได้ ไม่ต่ำกว่า 10 K
- 3.14 รองรับการกำหนด VLAN ได้ ตามมาตรฐาน IEEE802.1Q
- 3.15 รองรับการกำหนดระบบรักษาความปลอดภัยแบบ ACL, IEEE 802.1x port based and MAC-based, Web authentication, MAC authentication, MAC Filter, DHCP Snooping ได้เป็นอย่างน้อย
- 3.16 ต้องเป็นอุปกรณ์ที่ได้มาตรฐาน FCC Class A, UL เป็นอย่างน้อย
- 3.17 สามารถทำงานที่อุณหภูมิ 0-50 องศาเซลเซียส และความชื้น 10-90 % ได้
- 3.18 สามารถรองรับการบริหารจัดการอุปกรณ์ผ่านทาง Web Management, SNMP v1/v2/v3, CLI ได้
- 3.19 มีการรับประกันอุปกรณ์เป็นเวลาไม่น้อยกว่า 1 ปี

เอกสารแนบ 4

4. เครื่องสำรองไฟฟ้า ขนาด 2 KVA จำนวน 5 เครื่อง แต่ละเครื่องต้องมีคุณลักษณะพื้นฐานที่สำคัญ ดังนี้
- 4.1 ผลิตภัณฑ์ที่เสนอต้องได้รับการรับรองมาตรฐาน มอก. 1291-2545 พร้อมเอกสารยืนยัน
 - 4.2 เป็นเครื่องสำรองไฟระบบ Line Interactive with stabilizer ควบคุมการทำงานด้วยระบบไมโครโปรเซสเซอร์
 - 4.3 เป็นเครื่องสำรองไฟขนาดไม่น้อยกว่า 2 KVA (1,200 Watts) มีแรงดัน Input (VAC) 220 +/-25% หรือดีกว่า และมีแรงดัน Output (VAC) 220 +/-10% หรือดีกว่า
 - 4.4 มีสัญญาณไฟแจ้งการทำงานในสถานะไลน์โหมด, สภาวะสำรองไฟฟ้า, โอเวอร์โวลตและแบตเตอรี่เสื่อม
 - 4.5 มีสัญญาณไฟแสดงปริมาณของโวลตที่ต่อใช้งานและปริมาณประจุแบตเตอรี่
 - 4.6 มีสัญญาณเสียงแจ้งสภาวะสำรองไฟฟ้า, โอเวอร์โวลต และไฟฟ้าขาเข้าไม่อยู่ในช่วง +/- 25 %
 - 4.7 มีปุ่มกดสำหรับทดสอบการสำรองไฟฟ้าและปิดเสียงเตือน
 - 4.8 สามารถสำรองไฟฟ้าที่ Full Load ได้ไม่น้อยกว่า 5 นาที
 - 4.9 มีอุปกรณ์ป้องกันการลัดวงจรทั้ง Input และ Output
 - 4.10 มี Software ในการทดสอบการแสดงสถานะของแบตเตอรี่, บันทึกเหตุการณ์ต่างๆ, แสดงเวลาที่เหลือในการใช้งาน, ตั้งเวลาปิดเครื่องคอมพิวเตอร์ ได้เป็นอย่างน้อย
 - 4.11 รับประกันคุณภาพรวมแบตเตอรี่ และบริการทั่วประเทศ ไม่น้อยกว่า 2 ปี โดยไม่เสียค่าบริการและอะไหล่ใดๆ ทั้งสิ้น

เอกสารแนบ 5

5. แผงวงจรเครื่องคอมพิวเตอร์แม่ข่ายชนิด Blade สำหรับตู้ Enclosure/Chassis แบบที่ 1

จำนวน 4 ชุด แต่ละชุดต้องมีคุณลักษณะพื้นฐานที่สำคัญ ดังนี้

- 5.1 มีหน่วยประมวลผลกลาง (CPU) Intel Xeon ขนาดไม่น้อยกว่า 6 แกนหลัก (6 core) สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะ และมีความเร็วสัญญาณนาฬิกาไม่น้อยกว่า 2.4 GHz จำนวนไม่น้อยกว่า 1 หน่วย
- 5.2 CPU รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory ไม่น้อยกว่า 15 MB ต่อ Processor และมีความเร็วบัสไม่น้อยกว่า 1333 MHz หรือ QPI ไม่น้อยกว่า 7.2 GT/s
- 5.3 แผงวงจรหลักรองรับ CPU ได้รวมกันไม่น้อยกว่า 2 หน่วย
- 5.4 มีหน่วยความจำหลัก (RAM) ชนิด PC3-10600 DDR3 ECC หรือดีกว่า มีขนาดไม่น้อยกว่า 16 GB และสามารถขยายรวมได้ไม่น้อยกว่า 192 GB
- 5.5 มีหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด SAS หรือดีกว่า แบบ SAS Hot-Plug หรือ Hot Swap ที่มีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อวินาที และมีขนาดความจุไม่น้อยกว่า 300 GB จำนวนไม่น้อยกว่า 2 หน่วย
- 5.6 สนับสนุนการทำงาน แบบ RAID ไม่น้อยกว่า RAID 0, 1
- 5.7 มีช่องเชื่อมต่อระบบเครือข่าย แบบ 10/100/1000 Base-t หรือ Gigabit Ethernet หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง
- 5.8 สามารถใช้งาน DVD-ROM, USB device หรือดีกว่า แบบ Virtual Media ได้
- 5.9 มีโปรแกรมสำหรับบริหารจัดการและดูแลเครื่องคอมพิวเตอร์ ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
- 5.10 ติดตั้งซอฟต์แวร์ระบบปฏิบัติการพร้อมใช้งานที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
- 5.11 ต้องสามารถติดตั้งใช้งานร่วมกับตู้ Enclosure/Chassis Blade Center เดิมของ ศทส. (Blade Center H) ได้เป็นอย่างดี และต้องไม่มีค่าใช้จ่ายใดๆ เพิ่มเติมในภายหลัง หากมีค่าใช้จ่ายใดๆ เกิดขึ้นในช่วงติดตั้ง ผู้เสนอราคา ต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด
- 5.12 ต้องมีการรับประกันความบกพร่องหรือชำรุดของอุปกรณ์คอมพิวเตอร์ ทั้งค่าอะไหล่, ค่าบริการ, On-Site เป็นเวลาไม่น้อยกว่า 3 ปี จากเจ้าของผลิตภัณฑ์

เอกสารแนบ 6

6. อุปกรณ์จัดเก็บ Log file ระบบเครือข่าย แบบที่ 2 จำนวน 1 ชุด ต้องมีคุณลักษณะพื้นฐานที่สำคัญ ดังนี้

- 6.1 เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่างๆ, ระบบปฏิบัติการ, ระบบ appliances, ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 5 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้
- 6.2 สามารถจัดเก็บข้อมูลได้ตามหลักเกณฑ์การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- 6.3 เป็นระบบจัดเก็บข้อมูล Log ที่ได้ผ่านการตรวจสอบคุณสมบัติตามมาตรฐาน "ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์" จากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) NECTEC Standard NTS 4003.1-2552 โดยต้องมีเอกสารรายงานผลการทดสอบ
- 6.4 มีความสามารถบริหารจัดการแบบ Web Base Administration เพื่อสามารถเข้าไปบริหารจัดการระบบ log ผ่านเครือข่ายได้
- 6.5 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้
- 6.6 สามารถจัดเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ได้ เช่น Router, Switch, Firewall, VPN, Server เป็นต้น
- 6.7 สามารถรองรับการจัดเก็บ Log ที่ไม่ใช่ Syslog โดยผ่านทาง FTP, sFTP, SNMP Trap ได้เป็นอย่างน้อย
- 6.8 สามารถทำ Archive log และมีการ Compression File เพื่อประหยัดพื้นที่ในการจัดเก็บได้
- 6.9 สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอกได้ เช่น Tape หรือ DVD หรือ External Storage เป็นต้น
- 6.10 มีส่วนของการแสดงผลปริมาณของเหตุการณ์ของ Log ต่อวินาที เพื่อให้ทราบว่ามี Log ส่งเข้ามาจัดเก็บมากน้อยเพียงใด
- 6.11 สามารถเรียกดู Log ที่ส่งเข้ามาต่อประเภทเหตุการณ์ได้แบบ Real Time
- 6.12 ระบบต้องมีส่วนของการแสดงผลข้อมูลทรัพยากรของระบบที่ใช้ไป เช่น ซีพียู, หน่วยความจำ, หน่วยความจำสำรอง, ขนาดพื้นที่จัดเก็บ เป็นต้น
- 6.13 ระบบต้องสามารถระบุชนิดของ Log ที่จะจัดเก็บได้ว่าเป็นประเภทอะไร เช่น ชื่อของระบบ, หมายเลข IP, ประเภทของข้อมูลจราจรคอมพิวเตอร์ เป็นต้น
- 6.14 ระบบต้องสามารถกำหนดค่าระยะเวลาที่ต้องการจัดเก็บ Log ได้ โดยสามารถกำหนดขั้นต่ำ 90 วัน หรือมากกว่าตามต้องการ

/6.15 ระบบต้อง...

- 6.15 ระบบต้องสามารถกำหนดชั้นความลับได้ โดยสามารถกำหนดสิทธิ์ในการเข้าถึง Log File และกำหนดสิทธิ์ในการเข้าถึงฟังก์ชันต่างๆ ของระบบ พร้อมทั้งบันทึกเหตุการณ์การเปลี่ยนแปลงของระบบ เช่น การดาวน์โหลด Log File การเปลี่ยนแปลงคอนฟิกของระบบ การสั่งปิด (Shutdown) เครื่องได้
- 6.16 ระบบต้องมีมาตรการที่ปลอดภัยในการพิสูจน์สิทธิ์ เพื่อเข้าถึงระบบได้ เช่น HTTPS, SSH เป็นต้น
- 6.17 ระบบต้องรองรับการพิสูจน์สิทธิ์ (Authentication) ร่วมกับ Local DB, Active Directory ได้
- 6.18 ระบบต้องสามารถแจ้งเตือนข้อผิดพลาดของระบบในระหว่างการใช้งานได้ เช่น พื้นที่เต็ม, ระบบสำคัญต่างๆ ไม่ทำงาน, มีการ Login เข้าสู่ระบบ เป็นต้น
- 6.19 ระบบต้องมีความสามารถในการทำหน้าที่เป็น Time Server ได้ โดยต้องแสดงค่าสถานะของ Stratum ที่ระบบทำงานอยู่ด้วย
- 6.20 ระบบต้องมีความสามารถในการตรวจสอบความคงสภาพ (Integrity) ของข้อมูล Log ที่จัดเก็บไว้ได้ เพื่อยืนยันว่าข้อมูลที่จัดเก็บนั้นเป็นข้อมูลเดิมที่ไม่มีการเปลี่ยนแปลงหรือแก้ไขใดๆ เช่น การใช้วิธีการเปรียบเทียบค่า MD5 และ SHA-1 หรือที่ดีกว่า
- 6.21 ระบบต้องไม่อนุญาตให้เปลี่ยนแปลงแก้ไขข้อมูล Log ได้ โดยมีระบบการเข้ารหัสข้อมูล Log File โดยเทคโนโลยี 3DES, AES, Blowfish, RSA, หรือ OpenPGP อย่างใดอย่างหนึ่ง
- 6.22 มีระบบ Filtering log ที่สามารถใช้กรอง Log ตามเงื่อนไขต่างๆ ที่กำหนด เพื่อให้สามารถตรวจสอบติดตามผลการแจ้งเตือนเหตุการณ์ทางอีเมล เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่าย โดยสามารถ Filter ตามเงื่อนไขได้ เช่น เลือกตามชื่อ Host , IP, Log (Priority), Keyword เป็นต้น
- 6.23 ระบบค้นหาข้อมูลใน Log File หรือ Log Query จะต้องสามารถระบุเงื่อนไขในการค้นหา และเมื่อได้ผลลัพธ์ที่ต้องการจะต้องสามารถส่งออก (Export) เป็นไฟล์รูปแบบ CSV หรือ PDF ได้
- 6.24 ต้องสามารถส่งต่อ Log ไปยังอุปกรณ์วิเคราะห์ Log (Third Party) ผ่าน Protocol TCP/IP ได้
- 6.25 ระบบต้องรองรับการทำ Network Redundancy ได้ทั้งแบบ Active-Active และ Active-Standby
- 6.26 รองรับการทำงานของ Syslog Agent สำหรับการส่ง Log จาก Windows, IIS, ISA, Exchange, Antivirus log หรือ Server อื่นๆ ที่ไม่รองรับมาตรฐาน Syslog เพื่อให้สามารถส่ง Log นั้นเข้าสู่ Log Server ได้โดยผ่าน Syslog protocol
- 6.27 สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events per Seconds) ได้ไม่น้อยกว่า 4,000 eps
- 6.28 มีสิทธิ์ในการ Upgrade firmware หรือ Software และรับประกันอุปกรณ์เป็นเวลาไม่น้อยกว่า 1 ปี

เอกสารแนบ 7

7. อุปกรณ์ป้องกันเครือข่าย (Firewall) แบบที่ 2 จำนวน 1 ชุด ต้องมีคุณลักษณะพื้นฐานที่สำคัญ ดังนี้

- 7.1 เป็นอุปกรณ์ Firewall ชนิด Stateful Inspection firewall แบบ Appliance มีหน่วยประมวลผลเป็นแบบ ASIC ซึ่งได้รับการออกแบบมาเพื่อทำหน้าที่รักษาความปลอดภัยของเครือข่ายโดยเฉพาะ
- 7.2 มี Network Interface แบบ 10/100/1000 Ethernet (RJ-45) อย่างน้อย 10 พอร์ต
- 7.3 มีอัตราการโอนถ่ายข้อมูล (Throughput) ของ Firewall ได้ ไม่ต่ำกว่า 16 Gbps และได้รับการรับรองตามมาตรฐานของ ICSA ด้าน Firewall
- 7.4 สามารถรองรับการเชื่อมต่อพร้อมๆ กัน (Concurrent Sessions) ได้ ไม่น้อยกว่า 3,000,000 การเชื่อมต่อ (sessions) และรองรับการเชื่อมต่อใหม่ (New Sessions/Second) ได้ ด้วยความเร็ว ไม่ต่ำกว่า 70,000 การเชื่อมต่อ (sessions) ต่อวินาที
- 7.5 สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ ได้ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoof, IP Address Sweep, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, TCP Fragment, ICMP Fragment
- 7.6 สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้
- 7.7 สามารถทำงานลักษณะ Transparent Mode ได้
- 7.8 สามารถ Routing แบบ Static, Dynamic Routing ได้
- 7.9 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย
- 7.10 สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) โดยเก็บเป็น SysLog ได้
- 7.11 มีความสามารถในการตรวจจับและป้องกันไวรัสคอมพิวเตอร์ในโปรโตคอล FTP, HTTP, IMAP, IMAPS, POP3, POP3S, SMTP และ SMTPS และต้องสามารถ update ฐานข้อมูลไวรัส (virus signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอดระยะเวลาของการรับประกันอุปกรณ์
- 7.12 มีความสามารถในการป้องกันการบุกรุก (Intrusion Prevention) โดยสามารถ update ฐานข้อมูลการบุกรุก (attack signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอดระยะเวลาของการรับประกัน
- 7.13 สามารถเข้ารหัสเพื่อการส่งข้อมูลด้วยวิธีการ VPN โดยมีการใช้วิธีการเข้ารหัสแบบ 3DES/AES IPSec และ SSL-VPN เพื่อความปลอดภัยในการติดต่อจากระยะไกลได้ และได้รับการรับรองตามมาตรฐานของ ICSA ด้าน IPSec และ SSL-VPN
- 7.14 มีความเร็วในการทำงาน IPSec VPN ได้ ไม่ต่ำกว่า 8 Gbps
- 7.15 รองรับการทำงานด้วย SSL VPN พร้อมๆ กันได้ ไม่น้อยกว่า 500 users
- 7.16 สามารถทำงานในลักษณะ Content Filtering ได้ โดยสามารถกำหนดให้อุปกรณ์ป้องกันการเข้าถึง URL หรือ Web site ที่ต้องห้ามได้ (URL blocking)

/7.17 สามารถ...