อุปกรณ์รักษาความปลอดภัยระดับสูง (Next Generation Firewall) จำนวน 1 ระบบ
สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

รายละเอียดคุณลักษณะเฉพาะ

1. เป็นอุปกรณ์ Appliance-Based Firewall ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ (Application Firewall) และใช้โครงสร้างสถาปัตยกรรมแบบ Single Pass Software
2. มี Network Interface แบบ 10/100/1000 ไม่น้อยกว่า 12 พอร์ท และรองรับ 1G/10G SFP+ ไม่น้อยกว่า 8 พอร์ท และรองรับ 40G QSFP+ ไม่น้อยกว่า 4 port
3. มี Transceiver แบบ 10G Base LR ไม่น้อยกว่า 2 อัน และ มี 10G Base-T ไม่น้อยกว่า 2 อัน
4. รองรับ Application Firewall Throughput ได้ไม่น้อยกว่า 9 Gbps (appmix) และจำนวนเซสชันสูงสุด (Max Sessions) ได้ไม่น้อยกว่า 3,000,000 sessions และ (New Sessions) ไม่น้อยกว่า 100,000 Sessions ต่อวินาที
5. รองรับการทำ Virtual Systems ได้อย่างน้อย 6 Systems
6. สามารถทำ Routing แบบ Static, RIP, BGP, OSPF, Multicast และ Policy Based Forwarding ได้เป็นอย่างน้อย
7. สามารถทำ NAT (Network Address Translation) / PAT (Port Address Translation) , DHCP Servers และ DHCP Relay ได้
8. สามารถกำหนดนโยบายรักษาความปลอดภัยเพื่อควบคุมการเข้าถึงระบบเครือข่ายจาก Application, User และ Content ได้
9. สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส ด้วยการทำ SSL (ทั้ง Inbound และ Outbound) และ SSH Decryption ได้
10. สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP, eDirectory และ Microsoft Terminal Services เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย
11. สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตนของ user ที่ใช้งานโดยรองรับทั้ง User login และ user logout ได้
12. สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ดาวน์โหลดและอัพโหลดบนแต่ละ Application ได้ รวมทั้งสามารถป้องกันการรั่วไหลของข้อมูล (Data Filtering) ออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต ได้ตามความต้องการ
13. สามารถปรับแต่ง Response Page แจ้งไปยังผู้ใช้งาน กรณีที่มีการบล็อกทราฟฟิคเกิดขึ้น รวมไปถึงหน้าลงทะเบียนเข้าใช้ระบบครือข่ายของ Captive Portal และ Client VPN ได้
14. มีระบบป้องกันภัยคุกคาม (Threat Prevention) โดยมี Throughput ไม่น้อยกว่า 4.4 Gbps (appmix)

15. มีระบบการกรอง URL (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category และกำหนด Black list, White list รวมทั้งสามารถปรับแต่ง Category ได้ตามต้องการ
16. อุปกรณ์ที่นำเสนอต้องสามารถทำ IPsec VPN (Site to Site) โดยมี IPSec VPN Throughput ได้ไม่น้อยกว่า 4.8 Gbps
17. อุปกรณ์ที่นำเสนอต้องสามารถทำ Client VPN (Remote Access) บนโปรโตคอล IPSec และ SSL ได้
18. มีระบบจัดการคุณภาพการให้บริการ (Quality of Service) โดยสามารถกำหนดนโยบายเพื่อจัดการแบนวิธด์ของทราฟฟิคตาม Application, User, Source, Destination, Interface และ IPSec VPN Tunnel ได้เป็นอย่างน้อย
19. ผู้ยื่นข้อเสนอจะต้องมีหนังสือแสดงการเป็นผู้มีสิทธิจำหน่ายผลิตภัณฑ์ที่เสนอจากผู้ผลิตหรือจากสาขาของผู้ผลิตในประเทศไทย
20. รับประกัน 3 ปี แบบ onsite service
21. ติดตั้งที่ อาคารเรียนรวม องครักษ์ ชั้น 3 สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

.....