บริษัท จีเนียสย์ ดีเวลลอป จำกัด
เลขที่ 98/29 ถนนโพธิ์แก้ว แขวงนวมินทร์ เขตบึงกุ่ม กรุงเทพฯ 10240
โทร. 02-5096715 มือถือ 082-5674413, 086-4133928 Mail : contact@ez-admin.com, ezgenius54@gmail.com

หลักสูตร Network Firewall and Security Engineer (เน้นภาคปฏิบัติและติดตั้งใช้งานจริง)

(หลักสูตรการบริหารจัดการ Firewall เพื่อสร้างระบบความปลอดภัยให้กับเครือข่ายคอมพิวเตอร์)

หลักสูตร Network Firewall and Security Engineer เป็นหลักสูตรที่นำมาใช้ในการจัดการระบบ Firewall เพื่อสร้างระบบป้องกันความปลอดภัย ให้กับระบบเครือข่ายให้มีประสิทธิภาพ ซึ่งผู้ที่เข้ารับการฝึกอบรมจะสามารถเข้าใจระบบ OSI Model ทั้ง 7 เลเยอร์, กำหนดค่าการทำงานเบื้องต้นของ Firewall ด้วยคำสั่งต่างๆ และหน้ากราฟิกได้, กำหนดค่าการ Routing ด้วย Firewall ได้, กำหนดค่า Policy ของ Firewall, กำหนดค่าการทำงานของ Firewall แบบครบวงจร (UTM Firewall) เช่น การป้องกันไวรัส การกรองเนื้อหาเว็บไซต์ การควบคุมและป้องกันการโจมตีจากโปรแกรมต่างๆ ได้อย่างมีประสิทธิภาพ, สามารถกำหนดค่าการทำ IPSec VPN แบบ Site to Site, สามารถกำหนดค่า Virtual IP ด้วย Firewall, สามารถตรวจสอบและออกรายงานบันทึกข้อมูลการทำงานของ Firewall ด้วย Syslog รวมทั้งสามารถสำรองและการเรียกคืนข้อมูลกลับได้ เป็นต้น

รายละเอียดการอบรม

1. พื้นฐาน OSI Model 7 Layer
   - ชั้นที่ 7 Application Layer
   - ชั้นที่ 6 Presentation Layer
   - ชั้นที่ 5 Session Layer
   - ชั้นที่ 4 Transport Layer
   - ชั้นที่ 3 Network Layer
   - ชั้นที่ 2 Data Link Layer
   - ชั้นที่ 1 Physical Layer
2. รู้จัก Fortigate Firewall และการกำหนดค่าการทำงานเบื้องต้น
   - Firewall คืออะไร
   - รู้จัก Firewall Fortigate
   - กำหนด IP ให้กับ Fortigate และเครื่อง Client
   - กำหนดรหัสผ่านของ Admin
   - อัปเกรด Firmware
   - การ Backup และ Restore ค่าคอนฟิก
   - การทำ Factory Default
   - Restart และ Shutdown
3. กำหนดค่าการทำงานของ DHCP Server
   - การกำหนดค่าการทำงานของ DHCP Server
   - กำหนดค่าให้แจก IP แบบ Reserve
4. กำหนดค่าเชื่อมต่อเครือข่ายอินเทอร์เน็ต
   - กำหนดให้ Fortigate เชื่อมต่ออินเทอร์เน็ต
   - กำหนด Policy เพื่อให้เครือข่ายในออกอินเทอร์เน็ตได้

- กำหนด Policy ให้เครื่อง Client สามารถ ping ออกอินเทอร์เน็ตได้
- ให้ Fortigate เก็บ Log การใช้งานอินเทอร์เน็ต

5. กำหนดกลุ่มผู้ใช้เพื่อจำกัดการใช้งานอินเทอร์เน็ต
   - กำหนดกลุ่มของ VIP ให้สามารถใช้งานอินเทอร์เน็ตได้ไม่จำกัด
   - กำหนดกลุ่ม IP ของ User เพื่อจำกัดการใช้งานอินเทอร์เน็ต
   - ทดสอบการสร้างกลุ่ม Policy ที่กำหนด
6. การทำ User Authen เพื่อจำกัด Bandwidth การใช้งานอินเทอร์เน็ต
   - การสร้างกลุ่มของ VIP ที่ใช้งาน Bandwidth ไม่จำกัด
   - การสร้างกลุ่มของ User ที่ถูกจำกัดการใช้งาน Bandwidth
7. การบล็อกเว็บไซต์และเนื้อหาต่างๆ ที่ไม่เหมาะสมบนอินเทอร์เน็ต
   - การบล็อกเว็บไซต์หรือคำไม่เหมาะที่กำหนดเอง
   - การบล็อกเนื้อหาที่ไม่เหมาะสมจากเว็บไซต์ต่างๆ
   - การใช้ IPS ช่วยป้องกันการโจมตีจากภายนอก
8. การทำ Routing ระหว่าง Fortigate
9. การเชื่อมต่อเครือข่ายระหว่างสาขาด้วย VPN แบบ Site to Site
   - กำหนดค่า VPN ที่ Site 1
   - กำหนดค่า VPN ที่ Site 2
10. การทำ Virtual IP ให้กับเครื่อง Server เพื่อป้องกันการโจมตีโดยตรงจากภายนอก