

[FW001] หลักสูตร FortiGate Firewall Security

หลักสูตรนี้ท่านจะได้เรียนรู้วิธีการติดตั้ง FortiGate Firewall กำหนดค่าการทำงานเบื้องต้น, การนำ Firewall เชื่อมต่ออินเทอร์เน็ต, การกำหนดค่า Policy ให้ได้อย่างที่ต้องการ โดยเน้นการทำความเข้าใจเพื่อให้สามารถนำไปประยุกต์ใช้ในงานจริงได้, การเชื่อมต่อเครือข่ายที่อยู่ต่างวงแลนและตรวจสอบช่องโหว่ที่มาจากเครือข่ายภายนอกด้วย Firewall ได้, การป้องกันภัยคุกคามจากเครือข่ายอินเทอร์เน็ต เช่น ไวรัส Hacker และช่องโหว่ของโปรแกรมต่างๆ, การกรองเนื้อหาจากเว็บไซต์ต่างๆ เพื่อควบคุมและให้เข้าถึงเนื้อหาต่างๆ บนอินเทอร์เน็ตให้เหมาะสม, การเชื่อมต่อเครือข่ายของแต่ละสาขาให้ปลอดภัยด้วย IPSec VPN การกำหนดค่า Virtual IP เพื่อลดความเสี่ยงของเว็บไซต์ภายในองค์กรที่ถูกโจมตีจากช่องโหว่ต่างๆของ Hacker ตลอดจนการแก้ไขปัญหาที่เกิดจากการละเมิดความปลอดภัย สามารถนำความรู้ ทักษะที่ได้รับ ทั้งภาคทฤษฎี และ ภาคปฏิบัติ ไปใช้วางระบบทำงานจริงได้กับทุกองค์กรในประเทศไทย



หลักสูตรนี้เหมาะสำหรับ

- ท่านที่ผ่านการอบรมหลักสูตร Basic Network หรือ เคยทำงานกับระบบ Network มาบ้างแล้ว
- ท่านที่ต้องการทำงานในสายงานด้าน Network Admin โดยใช้ระบบ FortiGate Firewall
- ท่านที่ต้องการรับผิดชอบติดตั้ง, วางระบบ Network ที่เน้น Solutions ด้านความปลอดภัย
- ท่านที่สนใจระบบการทำงานในสาย Network Admin โดยเน้นระบบ Firewall

พื้นฐานผู้เข้าอบรม

เคยผ่านการอบรมหลักสูตร Basic Network มาแล้ว หรือ เคยทำงานกับระบบ Network มาบ้างแล้ว
หลักสูตรแนะนำก่อนหน้า : [Basic Network Installation and Troubleshooting](#)

หลังจบหลักสูตรนี้ ผู้เข้าอบรมจะสามารถ

- เข้าใจแนวคิดพื้นฐานของ Firewall และการทำงานของ FortiGate Firewall
- ติดตั้งและตั้งค่าพื้นฐานของอุปกรณ์ FortiGate Firewall ได้
- จัดการ Policy เพื่อควบคุมการเข้า-ออกของข้อมูลในองค์กรได้
- ใช้งาน Feature สำคัญ เช่น NAT, Security Profiles, และการ Monitor Traffic

เนื้อหาหลักสูตร

1. แนะนำพื้นฐาน Firewall และ Fortigate

- แนวคิดของ Firewall คืออะไร
- ประเภทของ Firewall (Packet Filtering, Stateful, NGFW)
- โครงสร้างและหน้าที่ของ Fortigate Firewall
- รู้จัก Interface, Zone, Policy, และ Session

2. ทำความรู้จักกับ Fortigate Device

- ภาพรวมหน้าตาอุปกรณ์และพอร์ตต่าง ๆ
- การเชื่อมต่อเข้า Fortigate (Console, Web GUI, SSH)
- การตั้งค่าเริ่มต้น (Initial Setup Wizard)

- การกำหนด IP, Default Gateway, และ DNS

3. การจัดการเบื้องต้นผ่าน Web GUI

- โครงสร้างหน้า Dashboard และเมนูหลัก
- ตรวจสอบสถานะระบบ (CPU, Memory, Interface Status)
- สำรองและกู้คืนค่ากำหนด (Backup & Restore Configuration)

4. การสร้าง Firewall Policy

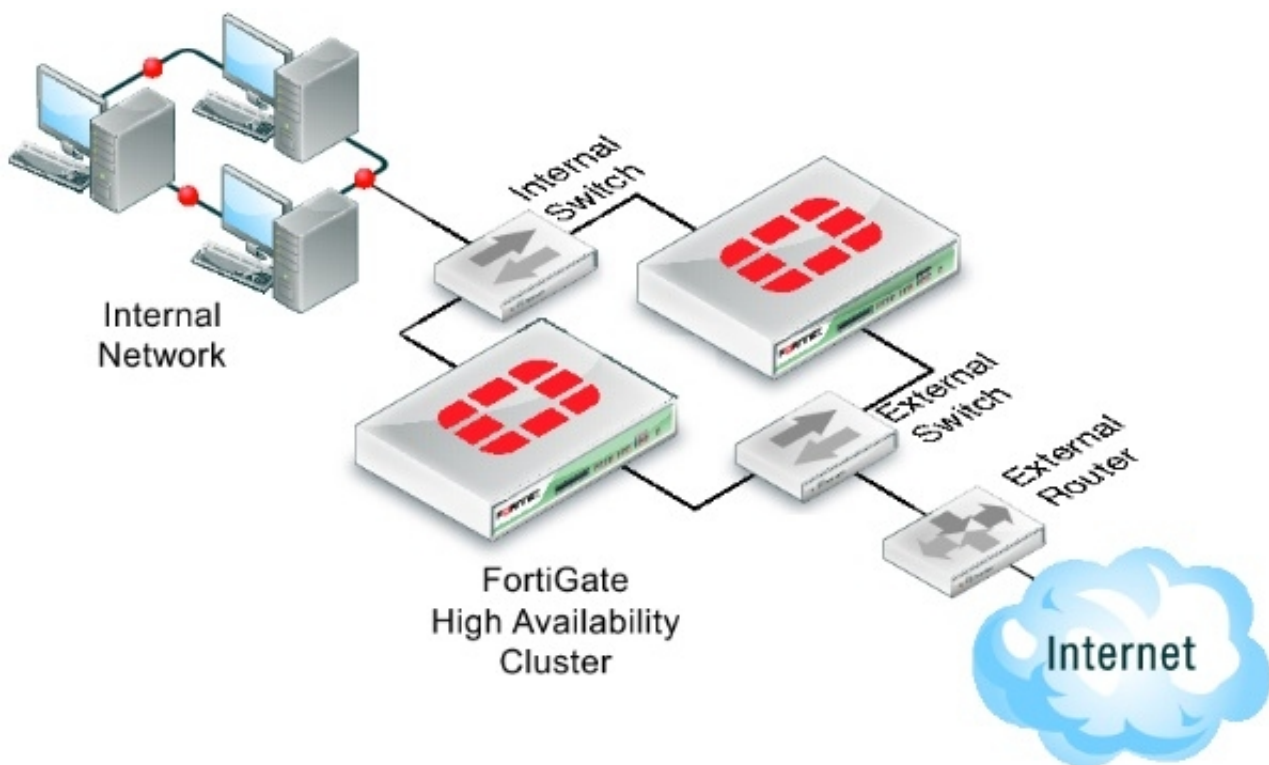
- ความหมายของ Policy และลำดับการทำงาน (Policy Order)
- การสร้าง Allow/Deny Policy
- การกำหนด Source, Destination, Service และ Action
- การทดสอบการทำงานของ Policy

5. การตั้งค่า NAT (Network Address Translation)

- แนวคิด NAT คืออะไร
- การสร้าง Policy พร้อม NAT สำหรับการออกอินเทอร์เน็ต
- การตั้งค่า Virtual IP (Port Forwarding) เพื่อให้เข้าจากภายนอกได้

6. การเปิดใช้ Security Feature เบื้องต้น

- การใช้ Web Filter เพื่อบล็อกเว็บไซต์ไม่เหมาะสม
- การเปิดใช้ Application Control และ Antivirus
- การตรวจสอบ Log และ Event



สิ่งที่ผู้เข้ารับการอบรมจะได้รับ

- อบรมโดยวิทยากรที่มีประสบการณ์ทำงานด้านระบบ Network & Security มามากกว่า 10 ปี และมีใบ Certificated รับรองความสามารถโดยตรง
- เอกสารประกอบการบรรยายอย่างละเอียดซึ่งสามารถนำไปใช้ประกอบการทำงานจริงได้ทันที

- มีการทดสอบทำ LAB (Workshop) สำหรับแบบฝึกหัดแต่ละหัวข้อ เพื่อความเข้าใจ และ ฝึกฝนให้ชำนาญก่อนนำไปใช้วางระบบทำงานจริง
- สามารถเข้ามาทบทวนซ้ำได้ฟรีภายในระยะเวลา 1 ปี หลังจากที่เรียนจบไปแล้ว
- ใบรับรองผ่านการอบรมเป็น e-Certificate จากสถาบัน ITC Training Center Co., Ltd. ซึ่งเป็นที่ยอมรับ ขององค์กรทุกระดับ ทั้งหน่วยงานทางภาครัฐ และภาคเอกชน ตลอดระยะเวลามากกว่า 20 ปี

ระยะเวลาอบรม 1 วัน (7 ชั่วโมง)

เวลา 09:30 - 17:30 น.

ค่าอบรม 3800 บาท (ยังไม่รวมภาษี 7%)

รอบวันอบรม

1. วันธรรมดา 12 มิถุนายน 2569 
2. วันธรรมดา 26 มิถุนายน 2569 
3. วันธรรมดา 8 กรกฎาคม 2569
4. วันธรรมดา 28 สิงหาคม 2569
5. วันธรรมดา 25 กันยายน 2569
6. วันธรรมดา 20 ตุลาคม 2569
7. วันหยุด 25 ตุลาคม 2569
8. วันธรรมดา 6 พฤศจิกายน 2569
9. วันธรรมดา 18 ธันวาคม 2569

หลักสูตรอื่นๆที่เกี่ยวข้อง

ถ้าท่านใดสนใจ สามารถติดต่อสอบถามรายละเอียดหลักสูตรและโปรโมชั่นเพิ่มเติมได้ที่
เบอร์โทร. 02-001-8200, 063-337-1483, 061-658-8288 ,Line ID : @itcert2005