[NW004] หลักสูตร Cisco Routers & Switches Hardening and Security (Workshop)

เนื้อหาหลักสูตรถูกออกแบบมาเพื่อให้ผู้ที่มีอาชีพ ติดตั้งและจัดคอนฟิก Router และ Switch ของค่าย Cisco ซึ่งต้องให้บริการ Support ลูกค้าภาคปฏิบัติซึ่งเน้นด้านความปลอดภัย (Security) โดยตรง เริ่มต้นตั้งแต่การตั้งค่าความปลอดภัยในการ Access เข้ามาที่ตัวอุปกรณ์ การกำหนดค่าต่างๆ ที่เกี่ยวข้องกับความปลอดภัยบน Router และ Switch ของค่าย Cisco การกำหนดค่าให้ Router ของ Cisco ทำหน้าที่เสมือนเป็น Firewall ด้วยความสามารถของ IOS Firewall ไปจนถึงวิธีการในการเข้ารหัส (Encryption) สำหรับการส่งและรับข้อมูลผ่านเครือข่าย (IPsec VPN) รวมทั้งการกำหนดค่าความปลอดภัยบน Layer 3 Switch ของ Cisco ดังนั้นจึงรับประกันได้ว่า
ท่านที่ผ่านการอบรมหลักสูตรนี้แล้วจะสามารถนำความรู้และทักษะที่ได้รับไปประกอบอาชีพเกี่ยวกับการดูแลรักษา, การติดตั้ง และการแก้ไขปัญหาโดยมุ่งเน้นด้านความปลอดภัยของเครือข่าย ที่ใช้อุปกรณ์ Router และ Switch ของค่าย Cisco ได้อย่างแน่นอน

หลักสูตรนี้เหมาะสมกับ

- ผู้ดูแลติดตั้งอุปกรณ์ Router และ Switch ของค่าย Cisco โดยมุ่งเน้นด้านความปลอดภัย (Security)
- ผู้บริหารจัดการระบบเครือข่าย (Network Administrator)
- วิศวกรติดตั้งระบบเครือข่าย (Network Engineer)
- กลุ่มสายงาน Network Planner และ Network Operator
- ผู้สนใจระบบการทำงานของเครือข่ายโดยเน้นด้านความปลอดภัย (Security)
- ผู้ที่ต้องการปูพื้นฐานความรู้เพื่อเตรียมตัวสอบ Cert. CCNA และ CCNP ที่เน้นสายงาน Security โดยตรง

พื้นฐานผู้เข้าอบรม

- เคยผ่านการอบรมหลักสูตร CCNA Routing and Switching มาแล้ว หรือ เคยทำงานกับอุปกรณ์ Network ที่เป็น Router และ Switch ของ ค่าย Cisco มาบ้างแล้วแต่ต้องการปรับปรุงให้มีความปลอดภัยมากขึ้น

กำหนดเวลาอบรม

เวลา 09:30 น. – 17:30 น.

<u>วันที่ 1</u>

การควบคุมการเข้าถึงเพื่อบริหารจัดการ Router และ Switch

- การกำหนดค่า และ เข้ารหัส Password ทั้งหมดในระบบ
- กำหนดค่า Banner เพื่อแจ้งเตือนการเข้าสู่ระบบ

- การกำหนดค่าการรักษาความปลอดภัยโดยการสร้างบัญชีผู้ใช้
- การกำหนดค่าการรักษาความปลอดภัยในการเข้ามาจากระยะไกล
- กำหนดค่า SSH เซิร์ฟเวอร์บน Router และ Switch
- กำหนดค่า SSH ทางฝั่งไคลเอนต์ และ ตรวจสอบการเชื่อมต่อ

กำหนดค่าบทบาท และ สิทธิ์ในการเข้ามาบริหารจัดการ

- สร้างมุมมองบทบาทที่หลากหลาย และ ให้สิทธิ์ที่แตกต่างกัน
- ตรวจสอบบทบาท และ ระดับสิทธิ์ที่ได้รับที่แตกต่างกัน

กำหนดค่า Cisco IOS ให้ทนทานต่อความล้มเหลว และ รายงานผลการจัดการ

- การรักษาความปลอดภัยของ Cisco IOS และ การตั้งค่าไฟล์จัดตั้ง
- กำหนดค่า Router และ Switch ตรงกับแหล่งเวลาที่ใช้ NTP เซิร์ฟเวอร์
- การกำหนดค่า Syslog บน Router และ Switch
- การจัดตั้ง Syslog เซิร์ฟเวอร์บนเครื่องพีซี และ การเปิดใช้งาน
- การกำหนดค่าการรายงานบน Router และ Switch ที่ใช้ SNMP

การกำหนดค่าการรับรองพิสูจสิทธิ์ที่ใช้ AAA

- การกำหนดค่าผู้ใช้การเข้าถึงสำหรับคอนโซล และ ทางระยะไกล
- ทดสอบการกำหนดค่าการรับรองพิสูจสิทธิ์ที่ใช้ AAA

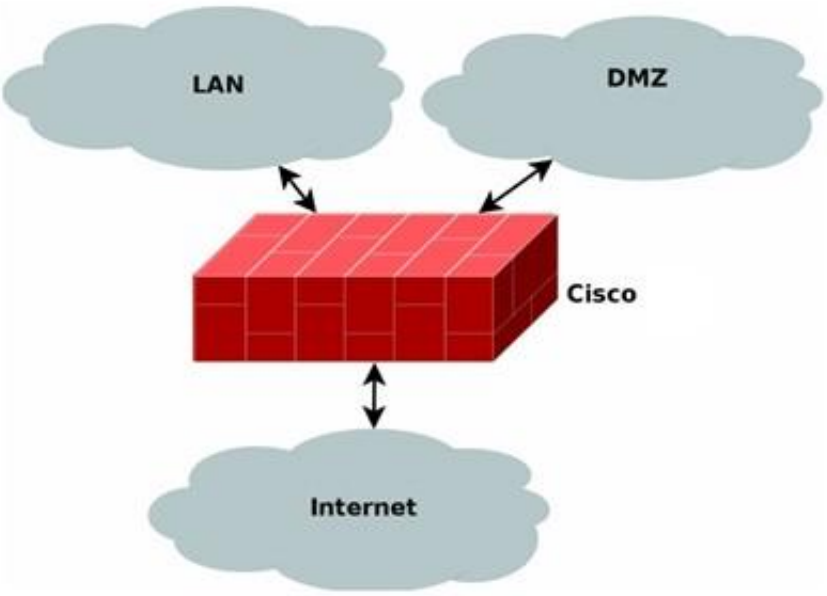
การกำหนดค่าการรับรองพิสูจสิทธิ์ที่ใช้ AAA และ Radius เซิร์ฟเวอร์

- การติดตั้ง RADIUS เซิร์ฟเวอร์บนคอมพิวเตอร์
- การกำหนดค่าผู้ใช้บน RADIUS เซิร์ฟเวอร์
- การกำหนดค่า AAA บน Router และ Switch เข้าถึง RADIUS เซิร์ฟเวอร์
- ทดสอบการกำหนดค่า AAA ทำงานร่วมกับ RADIUS เซิร์ฟเวอร์

วันที่ 2

การกำหนดค่าใช้งาน Cisco IOS ไฟร์วอลล์เพื่อปกป้องเครือข่าย

- เข้าใจหลักการทำงานของเทคโนโลยีไฟร์วอลล์
- การใช้ ACL ในการสร้างตัวกรองแพ็คเก็ตแบบคงที่
- การใช้ไฟร์วอลล์กำหนดนโยบาย Cisco IOS ในการจัดโซน



การจัดสร้าง IPSec VPN เชื่อมต่อระหว่างสาขา

- หลักการความเข้าใจพื้นฐานเกี่ยวกับ IPSec VPN
- การจัดตั้ง IPSec VPN เชื่อมต่อระหว่างสาขา
- การใช้ Cisco SDM กำหนดค่า IPSec VPN เชื่อมต่อระหว่างสาขา

การกำหนดค่า VPN จากการเข้าถึงระยะไกล

- การใช้ Cisco SDM ในการกำหนดค่า VPN เซิร์ฟเวอร์ที่ง่ายกว่า
- การใช้ Cisco VPN ไคลเอนต์เพื่อทดสอบการเข้าถึง VPN จากระยะไกล

<u>วันที่ 3</u>

ความเข้าใจการรักษาความปลอดภัยบนอุปกรณ์ Switch

- อธิบายการรักษาความปลอดภัยบน Switch เป็นส่วนหนึ่งของแผนการรักษาความปลอดภัยเครือข่ายโดยรวม
- อธิบายวิธีการรักษาความปลอดภัยพอร์ต Switch ที่มีการใช้งาน
- อธิบายการตรวจสอบพอร์ตโดยใช้มาตรฐาน 802.1x

การกำหนดค่าการรักษาความปลอดภัย Trunk และ Access พอร์ต

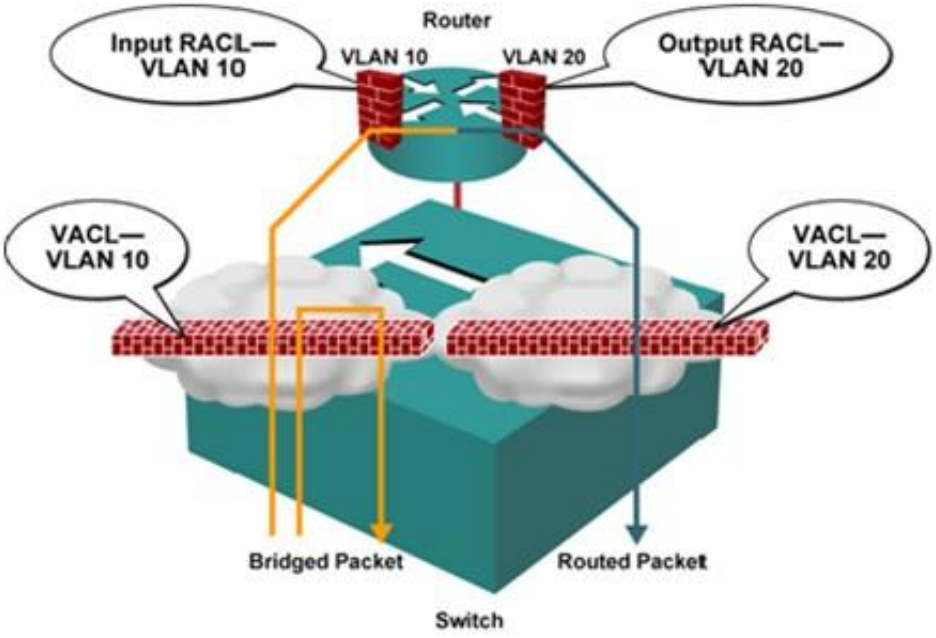
- โหมดการตั้งค่าคอนฟิก Trunk พอร์ต
- การเปลี่ยน Native VLAN สำหรับ Trunk พอร์ต
- ตรวจสอบการกำหนดค่า Trunk พอร์ต
- การกำหนดค่า Access พอร์ต
- การจัดตั้งค่ารักษาความปลอดภัยบน Access พอร์ต
- ตรวจสอบความปลอดภัยของ Access พอร์ต
- ทำการปิดการใช้งานพอร์ตที่ไม่ได้ใช้
- เปิดการใช้งาน PortFast และ BPDU guard
- ตรวจสอบการทำงานของ BPDU guard
- เปิดการใช้งาน Root guard
- เปิดการใช้งาน Loop guard และ UDLD

รูปแบบ และ บริการของ Cisco Switch ในการรักษาความปลอดภัย

- การกำหนดค่า และ ตรวจสอบ DHCP Snooping
- การกำหนดค่า DAI เพื่อป้องกันการปลอม ARP
- กำหนดค่า IP Source Guard เพื่อป้องกันการปลอม IP
- ปิดโปรโตคอลในการค้นหาอุปกรณ์เพื่อนบ้าน
- การกำหนดค่า SSH และ HTTPS บน Switch

การตั้งค่าความปลอดภัยบน Multilayer Switch

- อธิบายการรักษาความปลอดภัยบน Multilayer Switch
- การรักษาความปลอดภัยโดยใช้การจัดตั้งค่า VACL
- การกำหนดค่า Private VLANs และ Protected พอร์ต



สิ่งที่ผู้เข้ารับการอบรมจะได้รับ

- อบรมโดยวิทยากรที่มี Cert. ระดับ CCNA, CCDA, CCNP, CCDP และ CCIP
- เรียนรู้กับอุปกรณ์ Router, Switch ของค่าย Cisco ที่เป็นอุปกรณ์จริงทุก LAB
- แผ่น DVD-ROM โปรแกรม, Tools ต่างๆ สำหรับจัดการกับ Router และ Switch
- Video Training อุปกรณ์ Router และ Switch ของค่าย Cisco จากต่างประเทศ
- E-Book พร้อมกับแนวข้อสอบวิชา CCNA Security ซึ่ง Update ล่าสุด
- เอกสารประกอบการอบรมสามารถนำไปใช้ในการทำงานจริงได้ทันที
- สามารถเข้ามาทบทวนซ้ำได้ฟรีภายในระยะเวลา 1 ปี หลังจากที่เรียนจบไปแล้ว
- ใบรับรองผ่านการอบรมจากสถาบัน ITC Training Center Co., Ltd. ซึ่งเป็นที่ยอมรับขององค์กรทุกระดับ ทั้งหน่วยงานภาครัฐ และ เอกชน มามากกว่า 10 ปี

ระยะเวลาอบรม 3 วัน (21 ชั่วโมง)
เวลา 09:30 - 17:30 น.

ค่าอบรม 7500 บาท (ยังไม่รวมภาษี 7%)

หลักสูตรอื่นๆที่เกี่ยวข้อง

ถ้าท่านใดสนใจ สามารถติดต่อสอบถามรายละเอียดหลักสูตรและโปรโมชั่นเพิ่มเติมได้ที่
คุณจันทร์ทิพย์ (เก่) เบอร์โทร. 02-001-8200, 089-892-3246 ,Line ID : @itcert2005