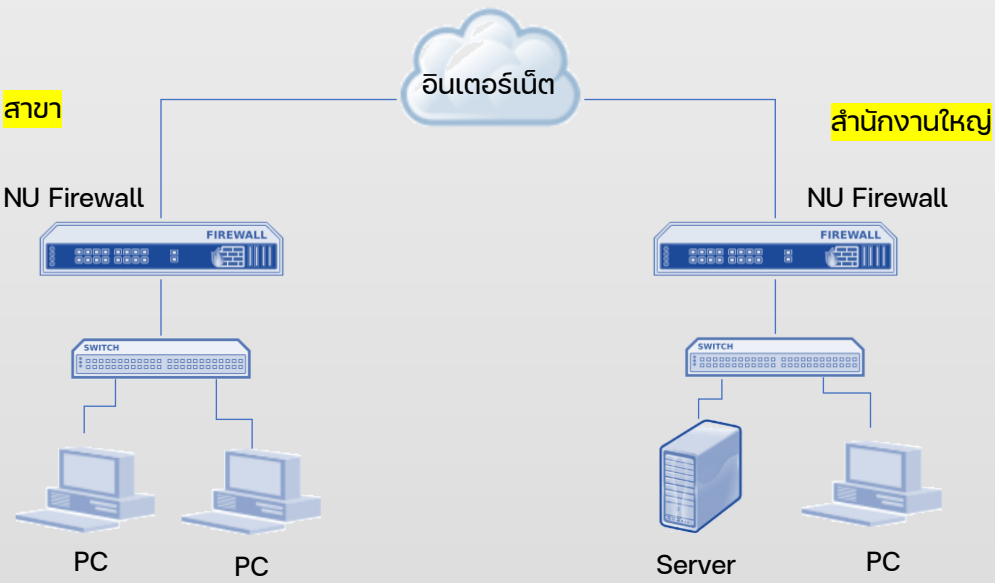
NetinforTech
Internet Security Specialists

IPSec VPN (Site to Site)

การเชื่อมต่อเครือข่ายระหว่างสำนักงานใหญ่กับสาขาด้วย VPN

Network Diagram สำหรับการเชื่อมต่อระหว่าง สำนักงานใหญ่ กับ สาขา



วัตถุประสงค์ในการทำ IPSec VPN Site to Site เพื่อให้ทั้งสาขาและสำนักงานใหญ่ สามารถเรียกใช้ทรัพยากรกันได้ผ่านเครือข่ายอินเตอร์เน็ต อย่างปลอดภัย จะมีการ Setup ดังนี้

(1).เปิดเมนู [VPN / IPSec Tunnel]
(2).กดปุ่ม 

(3).กรอกข้อมูลในหน้าจอที่ปรากฏ ให้กรอกข้อมูลสำหรับสร้าง Tunnel

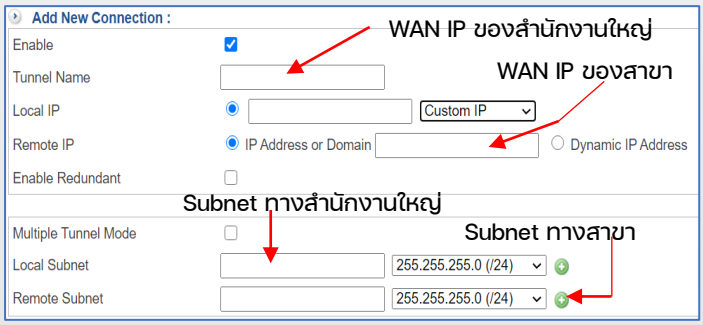
www.netinfortech.co.th rung@nit.co.th 0819856916

NetinforTech
Internet Security Specialists

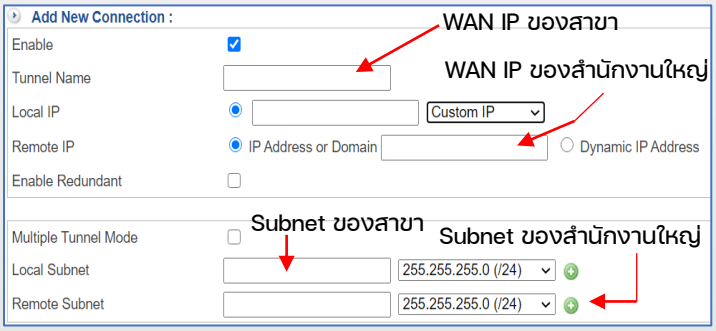
IPSec VPN (Site to Site)

การเชื่อมต่อเครือข่ายระหว่างสำนักงานใหญ่กับสาขาด้วย VPN

สำนักงานใหญ่



สาขา



- Enable ให้กดเครื่องหมายถูกเพื่อเปิดใช้งาน IPSec VPN
- Tunnel name ให้ใส่ชื่อของ Tunnel ที่สื่อความหมายเช่น HQ-TO-BRANCH
- Local IP ให้เลือกจาก Menu list Custom IP ว่าเราจะใช้ Link/IP Address ไหนสำหรับเชื่อมต่อ VPN
- Remote IP มีให้เลือกอยู่สองแบบ
  - IP Address or Domain ให้ใส่ WAN IP Address ทางฝั่งสาขา ถ้าสาขามี WAN IP Address เป็นแบบ Fix IP Address
  - Dynamic IP Address ใช้ก็ต่อเมื่อทางฝั่งสาขามี IP Address เป็นแบบ Dynamic IP หรือ IP Address เปลี่ยนไปตามการ Connect ของ Router

  ! ทางสามาขาต้อง Setup Bridge Mode บน Router เท่านั้น

-Enable Redundant จะใช้ในกรณีถ้า Link เสียให้สลับไปใช้ Link สำรองในการเชื่อมต่อ VPN แต่แนะนำว่า Function นี้ควรมี Link สำรองที่ความเร็วเท่า Link หลัก และ Fix IP Address ด้วย

-Multiple Tunnel Mode ก่อนการจะเชื่อมต่อจะต้องมีการพิสูนจ์ว่าเป็นตัวตนจริงมั้ยที่จะทำการเชื่อมต่อ ในการพิสูจน์จะใช้สองวิธีคือ IP Address กับ Domain name ฉะนั้นในหัวข้อนี้สามารถให้เราเลือกวิธีพิสูจน์ได้สองอย่างใน Tunnel เดียวกันได้ แต่โดยปกติเราจะไม่ใช้งานในหัวข้อนี้

- Local Subnet ให้ใส่ Subnet ทางฝั่งสำนักงานใหญ่ที่ต้องการให้สาขา เรียกใช้งาน ต.ย 192.168.10.0/24

  ! ถ้ามีมากกว่า 1 Subnet ให้กดเครื่องหมาย + แล้วใส่ Subnet ที่ต้องการ

- Remote Subnet ให้ใส่ Subnet ทางฝั่งสาขา ต.ย 192.168.20.0/24

  ! ถ้ามีมากกว่า 1 Subnet ให้กดเครื่องหมาย + แล้วใส่ Subnet ที่ต้องการ

www.netinfortech.co.th rung@nit.co.th 0819856916

NetinforTech
Internet Security Specialists

IPSec VPN (Site to Site)

การเชื่อมต่อเครือข่ายระหว่างสำนักงานใหญ่กับสาขาด้วย VPN

สำนักงานใหญ่

IKE Setting (Phase1)						
IKE	v1 v2					
Connection Type	Main Aggressive					
Preshare Key						
ISAKMP	des	md5	DH Group 1	Auto Matching		
Local ID	IP Address Domain Name @					
Remote ID	IP Address Domain Name @					
IKE SA Lifetime	3 Hour(s)					
IPSec Setting (Phase 2)						
IPSec	des	md5	Auto Matching			
Perfect Forward Secrecy (PFS)	No Yes					
IPSec SA Lifetime	3 Hour(s)					
Dead Peer Detection	hold	Delay 10 Seconds	Time out 60 Seconds			
Drop SMB Protocol						

สาขา

IKE Setting (Phase1)						
IKE	v1 v2					
Connection Type	Main Aggressive					
Preshare Key						
ISAKMP	des	md5	DH Group 1	Auto Matching		
Local ID	IP Address Domain Name @					
Remote ID	IP Address Domain Name @					
IKE SA Lifetime	3 Hour(s)					
IPSec Setting (Phase 2)						
IPSec	des	md5	Auto Matching			
Perfect Forward Secrecy (PFS)	No Yes					
IPSec SA Lifetime	3 Hour(s)					
Dead Peer Detection	hold	Delay 10 Seconds	Time out 60 Second			
Drop SMB Protocol						

- IKE Setting (Phase 1) เป็นขั้นตอนในการพิสูจน์ตัวตน และเป็นการแลกเปลี่ยนคีย์ เพื่อใช้ในการสร้าง Tunnel
  - IKE ให้เลือก v1
  - Connection Type ให้เลือก Main
  - Preshare Key คือ Password ที่ใช้ในการพิสูจน์ให้ใส่ อะไรก็ได้เช่น 123456789
    หมายเหตุ : Preshare Key ต้องเหมือนกันทั้ง สำนักงานใหญ่และสาขา
  - ISAKMP ให้เลือกตามความเหมาะสมถ้าต้องการความปลอดภัยสูงให้เลือก 3DES/DES แต่จะช้า แต่ถ้าต้องการความไวให้เลือก AES/SHA1
  - Local ID/Remote ID ให้เลือก IP Address
  - IKE SA Lifetime ให้เลือกจำนวนชั่วโมงว่าจะให้มีการตรวจสอบสิทธิ์ใหม่กี่ชั่วโมง
    หมายเหตุ : ตอนตรวจสอบสิทธิ์หรือพิสูจน์ตัวตนจะทำให้ Tunnel หลุดหรือ IPSec VPN หลุด

-IPSec Setting (Phase 2) เป็นการขั้นตอนของการเข้ารหัสข้อมูลให้เลือกเหมือนกับ Phase 1

- Dead Peer Detection มีให้เลือก
  - hold ถ้า Link down จะให้ hold IPSec connect คอยไว้กี่วินาทีถึงจะเชื่อมต่อใหม่ ถ้า Link เป็นปกติ IPSec VPN ก็จะคง session ไว้เหมือนเดิมและ App ยังทำงานต่อไปได้
  - restart ถ้า Link down ให้ restart IPSec service ใหม่ จะดำเนินการใหม่หมด
    หมายเหตุ : เหมาะสำหรับฝั่งใดฝั่งหนึ่งมี IP Address เป็นแบบ Dynamic IP หรือเปลี่ยนไปตลอด
  - clear คือถ้า Link down จะเคลีย์ session แล้วสร้าง tunnel ใหม่

-Time out ถ้าระบบ IPSec VPN มีการเช็ค Link และมี Timeout มากกว่า 60วินาทีจะถือว่า Link Down ก็จะเข้าสู่ Mode ของ Dead Peer Detection

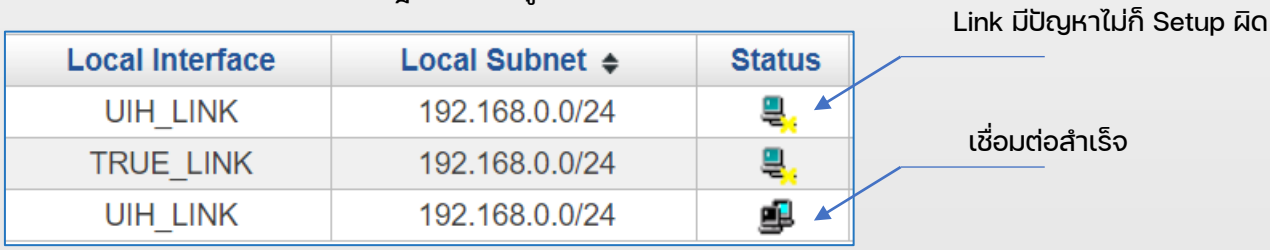
www.netinfortech.co.th rung@nit.co.th 0819856916

NetinforTech
Internet Security Specialists

IPSec VPN (Site to Site)

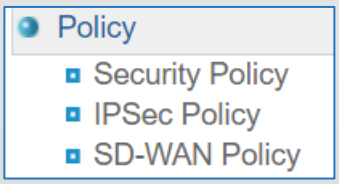
การเชื่อมต่อเครือข่ายระหว่างสำนักงานใหญ่กับสาขาด้วย VPN

(4).เมื่อสร้าง Tunnel เสร็จแล้วจะปรากฏหน้าจอดังรูป

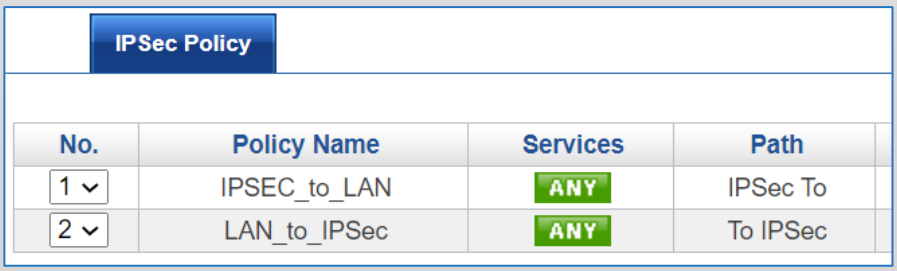


- ถ้าแสดงรูปคอมพิวเตอร์กระพริบแสดงว่าเชื่อมต่อสำเร็จแต่ถ้าเป็นกากบาทสีเหลือแสดงว่า Link มีปัญหา

(5).เพื่อให้สาขาสามารถเรียกใช้งานเครือข่ายทางสำนักงานใหญ่ได้จะต้องสร้าง Policy อนุญาติ ด้วยให้เข้าเมนู [Policy] และ [IPSec Policy]



- ต้องสร้าง 2 Policy
  - Policy แรกให้อนุญาติจาก IPSEC หา LAN
  - Policy สองให้อนุญาติจาก LAN ไป IPSec



(6).ทดสอบ Ping ข้ามวงถ้า ping ได้ก็จบขั้นตอนการ Setup