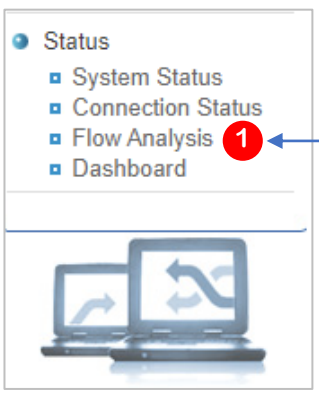
การตรวจสอบความเสี่ยง แรนซัมแวร์ เบื้องต้น

เราทราบกันดีว่า แรนซัมเวร์ จะโจมตีเครื่องคอมพิวเตอร์เรา โดยผ่าน Port เหล่านี้

- TCP/UDP 135
- TCP/UDP 137-139
- TCP/UDP 445
- TCP 3389

การตรวจสอบ แรนซัมแวร์ จะเป็นการตรวจสอบเครื่องคอมพิวเตอร์ภายใน ส่งข้อมูลหรือการเชื่อมต่อสื่อสารกับบุคคลภายนอกด้วย Port ดังกล่าว หรือไม่ สามารถตรวจสอบได้ดังนี้

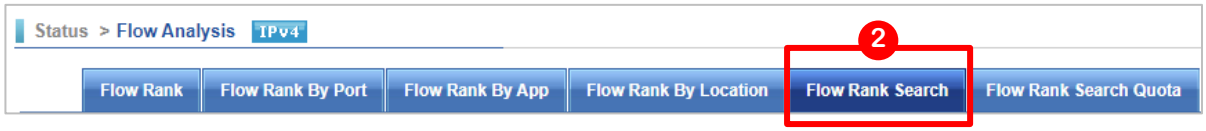
1.เปิดเมนู Status > Flow Analysis



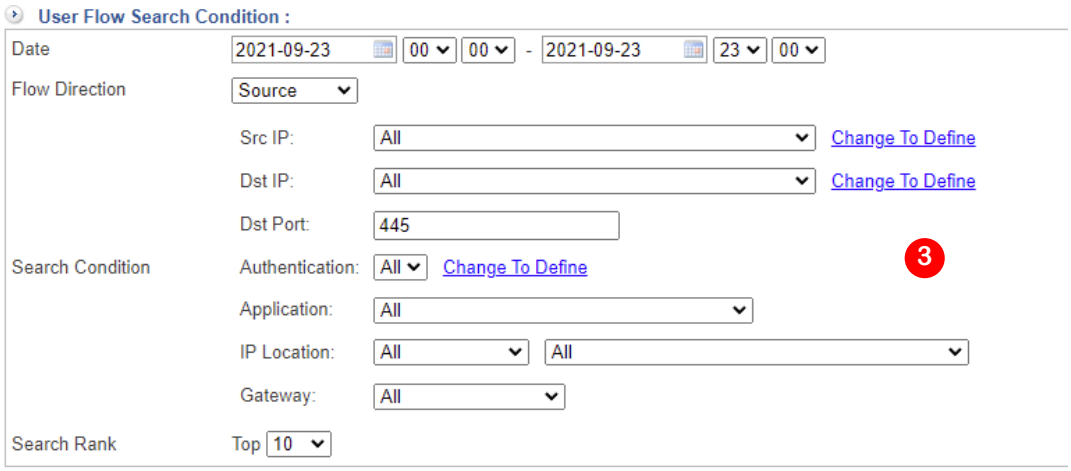
คลิกที่ Flow Analysis

Support : support.th@nit.co.th
Sales : rung@nit.co.th
Mobile : 081=985-6916
Web : www.netinfortech.co.th
Line : nit.sharetech

2.เลือกเมนู Flow Rang Search



3.จะเปิดหน้าจอสำหรับค้นหา



- Date ให้เลือกวันและเวลาที่เราต้องการค้นหา ! ห้ามค้นหาหลายเดือนเพราะจะช้า
- Flow Direction เป็นการเลือกว่าจะค้นหาจากต้นทางหรือเครือข่ายภายใน (Source) หรือจะค้นหาจากเครือข่ายภายนอก (Destination) โดยค่าเริ่มต้นจะเป็น Source
- Src IP: เป็นการกำหนดเงื่อนไขเป็น IP ต้นทาง สามารถเลือกจาก Menu list ถ้าไม่ทราบต้องการหาทั้งหมดให้เลือก All แต่ถ้าเราต้องการค้นหาเฉพาะ IP Address ให้กดที่ข้อความ Change To Define แล้วกรอก IP Address ที่เราต้องการค้นหา
- Dst IP จะเป็นการค้นหา IP ปลายทางการใส่เงื่อนไขจะเหมือนกับ Src IP
- Dst Port เป็น Port ปลายทาง ที่เครื่องคอมพิวเตอร์ภายในเรียกใช้ให้เราใส่ ทีละ port
    - 135
    - 137, 138, 139
    - 445
    - 3389
- Search Condition ไม่ต้องใส่ข้อมูล
- Search Rank ให้เลือกจำนวน Record ที่ต้องการแสดงเช่น 10, 50

4.กดปุ่ม 

ก็จะแสดงข้อมูลจากการค้นหา ถ้าต้องการดูรายละเอียดให้คลิกที่ IP Address