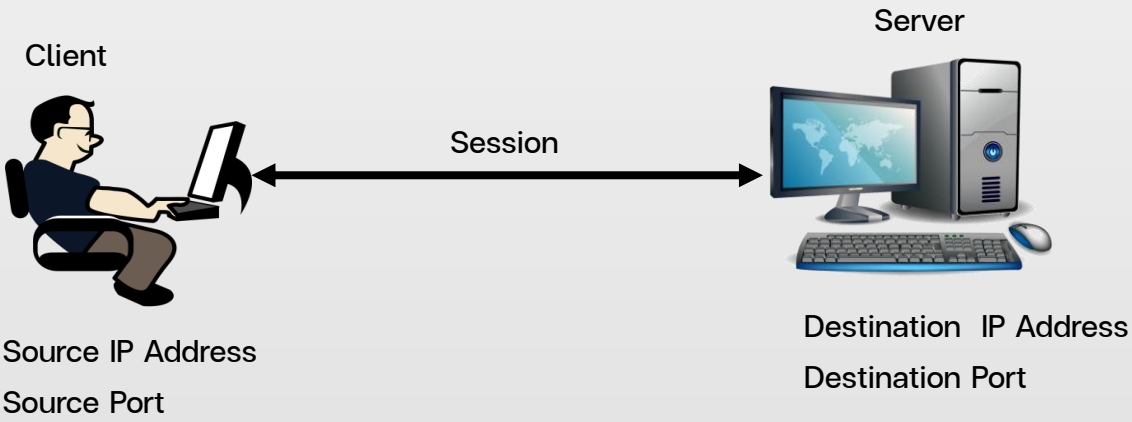
NetinforTech
Internet Security Specialists

Session

มาตารฐานการวิเคราะห์ Session



Session คือ การติดต่อสื่อสารกันระหว่าง Client กับ Server โดย 1 Session จะประกอบด้วย Source IP Address, Source Port, Destination IP Address, Destination Port ที่ไม่ซ้ำกัน อย่างใดอย่างหนึ่ง ก็นับเป็น 1 Session

ต.ย Client เปิด Browser และเรียกเวป www.google.co.th จะถือว่าเป็น 1 Session เมื่อ Client เปิดหน้า Google ได้ที่ Browser ถือว่าจบ 1 Session แต่ถ้าในขณะเปิด Browser และคงเรียก Google ไว้ และ Google สลับ IP Address เป็น IP Address อื่นจากตอนติดต่อครั้งจะนับเป็น 1 Session

Next Gen Firewall ทั่วไปจะกำหนดมาตารฐานของ Session ไว้ดังนี้

- 1-100 Session เป็นการใช้งานที่ปกติ
- 101-200 Session เป็นการใช้งานกลุ่ม Steaming, SQL
- 201-300 Session มีความเป็นไปได้เกิดจาก Malware, Trojan, ฯลฯ แต่บางครั้งจะพบจากการใช้งาน Voice/Steaming/File transfer
- 301 up Session จะถือว่าเป็นไวรัส (แต่อาจจะมีผลมาจากการเขียนโปรแกรม Connect DB ค้าง) และอุปกรณ์พวก AP, Switch, Network มีการ Broadcast สูง แต่ที่เห็นบ่อยๆคือ Client ร้องขอ DNS (UDP 53) เป็นปริมาณสูง (DNS Attack)

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