การเลือกใช้งาน **SSL Method** บน **F5** จะเลือกใช้งานอย่างไร

F5 LTM: SSL Offload, SSL Pass-Through และ **Full SSL Proxy**

Content นี้จะช่วยท่านผู้อ่านได้เข้าใจไม่มากก็น้อย เพราะฟังก์ชั่น SSL นี่เป็นที่นิยมใช้งานบน Web Application Server เป็นจำนวนมาก

แต่ปัญหาที่จะพบได้น้อยคือ Web Site ที่เรามีการใช้งานอยู่ ไม่สามารถ Turn On - SSL/TLS ขึ้นมาได้ แต่ถ้าหากท่านผู้อ่านกำลังเจอปัญหาส่วนน้อยนี้แล้ว ผมว่าบทความนี้มีประโยชน์ต่อการเลือกงานแน่นอน

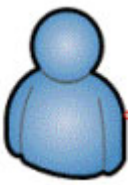
ปัจจัยสำคัญของอุปกรณ์ Server Load Balance ในปัจจุบันคือการ Handle SSL Traffic ก่อนที่จะกระจายโหลดไปยัง Server ปลายทาง ดังนั้นการทำงานของ SSL Configure จึงมีอยู่ 3 รูปแบบในการกำนดการทำงานนี้คือ

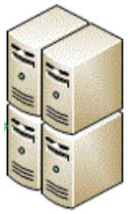
1. SSL Offloading
2. SSL Passthrough
3. Full SSL Proxy หรือ SSL Re-Encryption หรือ SSL Bridging หรือ SSL Terminations (หลายชื่อมาก แล้วแต่ใครจะเรียกชื่อไหน)

ก่อนที่เราจะทำความเข้าใจในการกำหนดหรือเลือกใช้ SSL Method อยากให้ท่านผู้อ่านเข้าใจการกำหนด SSL Profile ของ F5 กันก่อน เพราะใน Object Configuration Profile ของ F5 จะประกอบไปด้วย Virtual Server, Client SSL profile และ Server SSL profile

ซึ่ง Flow SSL Traffic ที่เกิดขึ้นจะเป็นตามด้านล่าง

Client ---> **BIG-IP VIP** ----> **Servers**



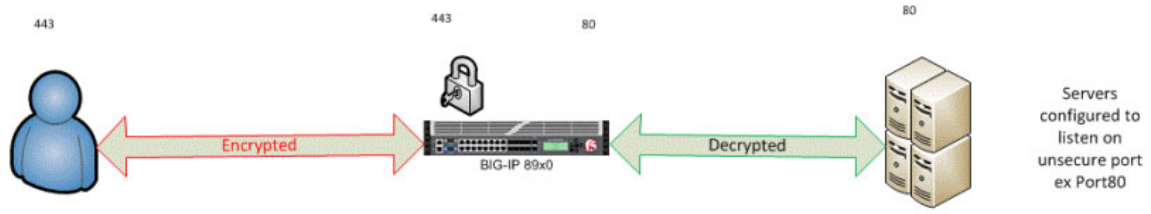


ในการเลือกใช้ SSL Method จึงเป็นตามด้านล่าง

SSL Offloading - ใน SSL Method นี้ Client จะทำการส่ง SSL Traffic (Encryption) ด้วย HTTPS (443) มาที่ F5 LTM หลังจากนั้น F5 LTM จะถอดรหัส (Decryption) SSL Traffic นี้ ซึ่งในเหตุการณ์นี้ Administrator จะต้องทำการ Import Certificate และ Private Key เข้าไปบน F5 LTM แล้วด้วยนะ

หลังจาก F5 LTM ถอดรหัส SSL Traffic จะนำส่งไปยัง Server ด้วย Clear text หรือ HTTP (80) เมื่อ Server ได้รับก็จะ HTTP Response กลับมาที่ F5 LTM

เมื่อ F5 LTM ได้รับ HTTP Response จาก Server, F5 LTM จะทำการ Response/Return ผ่าน Encryption กลับไปยัง Client ดังรูปด้านล่าง



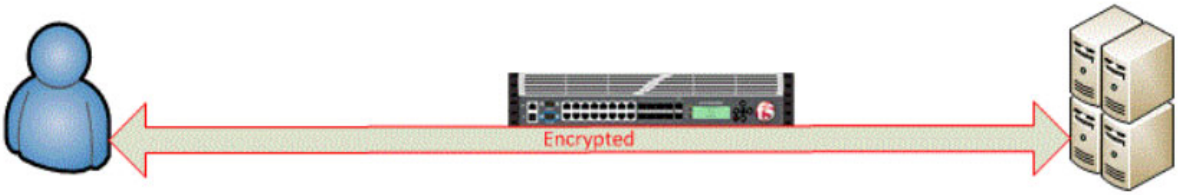
เพิ่มเติม

เนื่องจาก F5 LTM สามารถถอดรหัส HTTP Traffic ได้จะทำให้สามารถอ่านเนื้อหาอื่นได้ (Header, txt, cookies, ฯลฯ) และสามารถใช้ตัวเลือกการทำ Persistent ได้เช่น Source address, Destination address, Cookies, SSL, SIP, Universal, MSRDP

ข้อดีของการทำงานในรูปแบบนี้

1. Server มี Listener แค่ 80 หรือ HTTP
2. Server ไม่ต้อง Handle SSL Traffic
3. Server จะไม่เสีย Resource หรือ Performance ในการทำ Decryption Traffic ที่ Client ส่งออกมาให้
4. ได้รับ Performance ที่สูง F5 Hardware จะมี Hardware SSL Acceleration ในการประมวลผล SSL Traffic แยกออกมาโดยไม่ใช้งาน CPU หลัก
5. สามารถมองเห็นข้อมูลที่ถูกเข้ารหัสมาจาก Client และสามารถตรวจสอบความถูกต้องหรือเป็น injection ด้วย Advance WAF ของ F5 เพื่อทำการ Protection ได้

SSL Pass through - ในการทำงานของ SSL Method นี้ เป็นการทำงานโดยการ pass traffic จาก Client ไป Server ปลายทาง ซึ่งการทำงานลักษณะนี้จะเป็นการทำ forwarding SSL Handshake และ connection จะ Direct ตรงไปถึง Server โดยไม่ถูก Terminate ระหว่างทางเลย ดังรูปด้านล่าง



ข้อดีของการทำงานในรูปแบบนี้

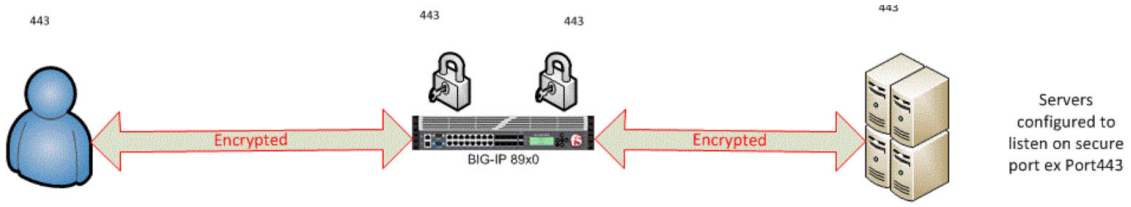
ข้อมูลที่ถูกส่งจาก Client ถึง Server เป็น Encrypted Communicate

ข้อเสียของการทำงานในรูปแบบนี้

1. ในกรณีที่ต้องการทำ Revoke Certificate ต้องทำบน Real Server ทุกเครื่อง
2. Server จะเสีย Resource หรือ Performance ในการทำ Decryption Traffic ที่ Client ส่งออกมาให้
3. ไม่สามารถมองเห็นข้อมูลที่ถูกเข้ารหัสมาจาก Client และไม่สามารถตรวจสอบความถูกต้องก่อนส่งไปยัง Server ปลายทางได้

SSL Full-Proxy – ใน SSL Method นี้มีหลายชื่อที่จะคุ้นหูเช่น SSL Re-Encryption, SSL Terminate หรือ SSL Bridging ซึ่งการทำงานใน Method นี้คือการที่ F5 LTM จะทำการ Re-Encryption Traffic ก่อนส่งไปยัง Server ปลายทาง

โดยการทำงานในลักษณะนี้ Client จะส่ง Encrypted traffic มาที่ F5 LTM ก่อน และ F5 จะทำการ Decrypted SSL Traffic หรือ SSL Terminate ก่อนที่จะส่งไปยัง Resource Pool Member หลังจากนั้นจะทำการ Re-encrypted อีกครั้ง และส่งไปยัง Server ด้วย Encryption Traffic เมื่อ Server ได้รับก็จะทำการ Decryption อีกครั้ง ดังรูปด้านล่าง



จากรูปจะเห็นได้ว่า Traffic ระหว่าง Client ถึง F5 LTM และ F5 LTM ถึง Server จะเป็น Encrypted traffic ทั้งหมด

ข้อดีของการทำงานในรูปแบบนี้

1. Communication ระหว่าง Client ถึง F5 และ F5 ถึง Server จะเป็น Secure ทั้งหมด
2. Server จะต้องมี Listener HTTPS (443) และมีการ Decryption SS Traffic ซึ่งสามารถปรับลด Size ของ Private Key จาก 2K ลงมา 1K หรือ 512 ก็ได้
3. Certificate บน Server สามารถเลือกใช้งานเป็น Self Cert หรือ CSA (CA) ได้
4. F5 LTM สามารถถอดรหัส HTTP Traffic ได้จะทำให้สามารถอ่านเนื้อหาอื่นได้ (Header, txt, cookies, ฯลฯ) และสามารถใช้ตัวเลือกการทำ Persistent ได้เช่น Source address, Destination address, Cookies, SSL, SIP, Universal, MSRDP
5. สามารถมองเห็นข้อมูลที่ถูกเข้ารหัสมาจาก Client และสามารถตรวจสอบความถูกต้องหรือเป็น injection ด้วย Advance WAF ของ F5 เพื่อทำการ Protection ได้

สำหรับเนื้อหาในเรื่องของ SSL Method เพื่อให้เราสามารถเลือกใช้งาน Encryption Traffic แบบไหนมาใช้งานให้เหมาะสมกับระบบ หรือ Server ที่มีอยู่

ท่านผู้อ่านสามารถอ่านข้อมูลเพิ่มเติมได้ที่นี่ https://support.f5.com/csp/article/K65271370