วิธีปรับปรุง SEO ด้วย HTTPS และ NGINX

คุณรู้หรือไม่ว่าการรักษาความปลอดภัยเว็บไซต์ของคุณด้วย HTTPS สามารถเพิ่มอันดับของคุณในผลการค้นหาของ Google Google ประกาศใน[บล็อกความปลอดภัยออนไลน์](https://security.googleblog.com/2014/08/https-as-ranking-signal_6.html)ว่าตอนนี้อัลกอริธึมการค้นหาของพวกเขาถือว่า HTTPS เป็นสัญญาณการจัดอันดับเมื่อส่งคืนผลการค้นหา

[HTTP](https://www.nginx.com/resources/glossary/http/)ซึ่งเป็น Hypertext Transfer Protocol เป็นรากฐานของการสื่อสารบนอินเทอร์เน็ต อย่างไรก็ตาม มันไม่ปลอดภัยเพราะการสื่อสารไม่มีการเข้ารหัส HTTPS ซึ่งเป็นเวอร์ชันที่ปลอดภัยของ HTTP ใช้ SSL หรือโปรโตคอลการเข้ารหัส TLS ที่ทันสมัยกว่าในการเข้ารหัสการไหลของข้อมูล บริษัทที่คำนึงถึงความปลอดภัย เช่น Dropbox ใช้ HTTPS เพื่อจัดการกับความท้าทายด้านความปลอดภัยและความเป็นส่วนตัวที่หลากหลาย

## **SSL และ TLS สามารถสร้างปัญหาด้านประสิทธิภาพที่ร้ายแรงได้**

ประโยชน์ของการเพิ่มประสิทธิภาพกลไกค้นหา (SEO) จากการรักษาความปลอดภัยให้เว็บไซต์ของคุณนั้นน่าดึงดูดใจ แต่สำหรับหลายๆ คน มันไม่ได้น่าตื่นเต้นขนาดนั้น ความจริงก็คือแอปพลิเคชั่นจำนวนมากยังคงพึ่งพาสถาปัตยกรรมที่ไม่มีประสิทธิภาพในซอฟต์แวร์สแต็คและประสบปัญหาด้านประสิทธิภาพมากมาย การเพิ่ม SSL หรือ TLS จะทำให้แอปพลิเคชันทำงานช้าลงและใช้ทรัพยากรมากขึ้น

การจับมือกัน SSL/TLS ที่ทำให้ HTTPS ปลอดภัยสามารถส่งผลกระทบต่อประสิทธิภาพได้อย่างมาก การจับมือกันคือชุดของการสื่อสารระหว่างเว็บเบราว์เซอร์และเซิร์ฟเวอร์ที่ยืนยันว่าการเชื่อมต่อนั้นเชื่อถือได้ เป็นกระบวนการที่ใช้ CPU มาก และนำไปสู่การเดินทางไปกลับระหว่างผู้ใช้และเซิร์ฟเวอร์ของคุณมากขึ้น

## **NGINX Solutions**

โชคดีที่เว็บเซิร์ฟเวอร์สมัยใหม่ เช่น NGINX และ NGINX Plus จัดการกับความท้าทายเหล่านี้และช่วยให้บริษัทต่างๆ สามารถปรับขนาดแอปพลิเคชันได้เป็นอย่างดี NGINX และ NGINX Plus มีหลายวิธีที่คุณสามารถบรรเทาผลกระทบด้านประสิทธิภาพของ SSL/TLS ได้ รวมถึงการแคชเซสชัน ตั๋วเซสชันหรือ ID การเย็บ OCSP และโปรโตคอล SPDY รุ่นทดลอง

### **การแคชเซสชัน**

เมื่อคุณรวม[**ssl\_session\_cache**](https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_cache)คำสั่งในการกำหนดค่า NGINX และ NGINX Plus จะแคชพารามิเตอร์เซสชันที่ใช้เพื่อสร้างการเชื่อมต่อ SSL/TLS แคชนี้ ซึ่งใช้ร่วมกันระหว่างผู้ปฏิบัติงานทั้งหมดเมื่อคุณรวมsharedพารามิเตอร์ ปรับปรุงเวลาตอบสนองอย่างมากสำหรับคำขอที่ตามมาอย่างมาก เนื่องจากทราบข้อมูลการตั้งค่าการเชื่อมต่อแล้ว กำหนดชื่อให้กับแคชและกำหนดขนาด (แคชที่ใช้ร่วมกัน 1‑MB รองรับประมาณ 4,000 เซสชัน)

คำ[**ssl\_session\_timeout**](https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_timeout)สั่งควบคุมระยะเวลาที่ข้อมูลเซสชันยังคงอยู่ในแคช ค่าเริ่มต้นคือ 5 นาที; การเพิ่มเป็นเวลาหลายชั่วโมง (ดังในตัวอย่างต่อไปนี้) ช่วยเพิ่มประสิทธิภาพแต่ต้องการแคชที่ใหญ่ขึ้น

ssl\_session\_cache shared:SSL:20m;

ssl\_session\_timeout 4h;

### **ตั๋วเซสชันและรหัส**

[ตั๋วเซสชัน](https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_tickets)เก็บข้อมูลเกี่ยวกับเซสชัน SSL/TLS เฉพาะ เมื่อลูกค้าดำเนินการโต้ตอบกับแอปพลิเคชันต่อ ตั๋วเซสชันจะใช้เพื่อดำเนินการเซสชันต่อโดยไม่ต้องเจรจาใหม่ รหัสเซสชันเป็นทางเลือก แฮช MD5 ใช้เพื่อแมปกับเซสชันเฉพาะที่เก็บไว้ในแคชที่สร้างโดยssl\_session\_cacheคำสั่ง สามารถใช้กลไกทั้งสองเพื่อช็อตคัต SSL/TLS handshake

ssl\_session\_tickets on;

### **OCSP เย็บเล่ม**

อีกวิธีหนึ่งในการปรับปรุงประสิทธิภาพ HTTPS คือการใช้[OCSP stapling](https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling)ซึ่งลดเวลาของการจับมือ SSL/TLS ตามเนื้อผ้า เมื่อผู้ใช้เชื่อมต่อกับแอปพลิเคชันหรือเว็บไซต์ของคุณผ่าน HTTPS เบราว์เซอร์จะตรวจสอบใบรับรอง SSL/TLS กับรายการเพิกถอนใบรับรอง (CRL) หรือใช้บันทึก Online Certificate Status Protocol (OCSP) จากผู้ออกใบรับรอง (CA) คำขอเหล่านี้เพิ่มเวลาในการตอบสนองและ CA อาจไม่น่าเชื่อถือ ด้วย NGINX และ NGINX Plus คุณสามารถแคชการตอบสนอง OCSP ไปยังเซิร์ฟเวอร์ของคุณและขจัดค่าใช้จ่ายที่มีค่าใช้จ่ายสูง

ssl\_stapling on;

ssl\_stapling\_verify on;

ssl\_trusted\_certificate /etc/nginx/cert/trustchain.crt;

resolver 8.8.8.8 8.8.4.4 valid=300s;

### **ไซเฟอร์ สวีท**

การระบุชุดการเข้ารหัสที่ปรับให้เหมาะสม - อัลกอริธึมที่เข้ารหัสการสื่อสารเครือข่าย - บางครั้งกล่าวเพื่อเพิ่มประสิทธิภาพ คุณสามารถใช้[ssl\_prefer\_server\_ciphers](https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_prefer_server_ciphers)คำสั่งเพื่อจุดประสงค์นี้ได้ แต่ความจริงก็คือการตั้งค่าเริ่มต้นนั้นดีพอสำหรับกรณีส่วนใหญ่ การตั้งค่านี้และแนวปฏิบัติที่ดีที่สุด ใช้ได้ดีกับการเข้ารหัสแบบเก่า ปัจจุบัน และ (ความหวังเดียว) ในอนาคต เราขอแนะนำให้คุณเลือกการเข้ารหัสเฉพาะเพื่อให้เป็นไปตามข้อกำหนดด้านความปลอดภัยและประสิทธิภาพโดยเฉพาะ

### **SPDY**

บรรณาธิการ – SPDY เป็นพื้นฐานสำหรับมาตรฐาน[*HTTP/2*](https://tools.ietf.org/html/rfc7540) ที่ เผยแพร่ในเดือนพฤษภาคม 2015 การรองรับ SPDY เลิกใช้แล้ว และรองรับ HTTP/2 อย่างสมบูรณ์ใน[*NGINX Plus Release 7*](https://www.nginx.com/blog/http2-r7/)ขึ้นไป และ[*NGINX 1.9.5*](https://www.nginx.com/blog/nginx-1-9-5/)ขึ้นไป

[SPDY](https://nginx.org/en/docs/http/ngx_http_spdy_module.html)เป็น โปรโตคอล ทดลองที่พยายามลดเวลาแฝงและเวลาไปกลับสำหรับการรับส่งข้อมูล HTTP โปรโตคอลสร้างช่องสัญญาณระหว่างเว็บเบราว์เซอร์และเซิร์ฟเวอร์แอปพลิเคชัน ผ่านมัลติเพล็กซ์ HTTP ทำให้ SPDY เปิดใช้งานทราฟฟิกสตรีมพร้อมกันผ่านการเชื่อมต่อ TCP เดียว ลดความจำเป็นในการเชื่อมต่อเพิ่มเติมและการเจรจา SSL โปรโตคอลยังบีบอัดคำขอและการตอบสนองส่วนหัว HTTP ส่งผลให้มีการส่งไบต์น้อยลง สิ่งสำคัญที่ควรทราบคือ SPDY ไม่ได้ให้ประโยชน์ใดๆ หากคุณสร้างการแบ่งกลุ่มโดเมน

listen 443 ssl spdy;

spdy\_headers\_comp 1;

ตัวแก้ไข – ด้วยการรองรับ HTTP/2 http2 พารามิเตอร์จะแทนที่ spdy พารามิเตอร์เป็น listen คำสั่งที่แสดงในตัวอย่างด้านบน ไม่มีสิ่งใดเทียบเท่ากับ spdy\_headers\_comp คำสั่งสำหรับ HTTP/2

# In NGINX Plus R7 and later, and NGINX 1.9.5 and later

listen 443 ssl http2;

## **ประโยชน์ของการใช้ SSL/TLS นั้นยิ่งใหญ่กว่าที่เคย**

การเพิ่มประสิทธิภาพกลไกค้นหาเป็นจุดสนใจสำหรับบริษัทจำนวนมากที่มีอินเทอร์เน็ต อันที่จริง Google อาจทำให้ HTTPS เป็นปัจจัยการจัดอันดับที่มีอิทธิพลมากขึ้นในอนาคตอันใกล้นี้ น่าตื่นเต้นที่มีตัวเลือกที่ช่วยให้ผู้ดูแลเว็บสามารถตอบสนองความต้องการของความปลอดภัยของผู้ใช้ได้อย่างมีประสิทธิภาพในขณะที่ยังมอบประสิทธิภาพที่ผู้ใช้ชื่นชอบ

ในท้ายที่สุด คุณไม่ควรรักษาความปลอดภัยให้กับเว็บไซต์ของคุณเพียงเพื่อประโยชน์ด้าน SEO เท่านั้น แต่เป็นแรงจูงใจที่ดีจาก Google ที่เราหวังว่าจะกระตุ้นให้คุณพิจารณาความปลอดภัยของแอปพลิเคชันของคุณอีกครั้ง ใครบ้างที่ไม่ต้องการปรับปรุงประสบการณ์และความปลอดภัยของผู้ใช้ในขณะที่ยังได้รับการส่งเสริม SEO?

ในการเริ่มต้นและเรียนรู้เพิ่มเติมเกี่ยวกับวิธีตั้งค่าและเพิ่มประสิทธิภาพ HTTPS โปรดดูที่ คู่มือ ผู้[ดูแลระบบ NGINX Plus](https://docs.nginx.com/nginx/admin-guide/security-controls/terminating-ssl-http/)