ວິທີການປັບປຸງ SEO ດ້ວຍ HTTPS in NGINX

[HTTP](https://www-nginx-com.translate.goog/resources/glossary/http/?_x_tr_sl=en&_x_tr_tl=lo&_x_tr_hl=th&_x_tr_pto=wapp) ເປັນ Hypertext Transfer Protocol, ແມ່ນພື້ນຖານຂອງການສື່ສານໃນອິນເຕີເນັດ. ສາມາດເພີ່ມອັນດັບຂອງການຄົ້ນຫາຂອງ Google ປະກາດໃນ blog ຄວາມປອດໄພອອນໄລນ໌ວ່າ algorithm ຄົ້ນຫາຂອງພວກເຂົາໃນປັດຈຸບັນປະຕິບັດ HTTPS ເປັນສັນຍານການຈັດອັນດັບໃນເວລາທີ່ກັບຄືນຜົນການຄົ້ນຫາ.

**Session Caching**

ເມື່ອທ່ານລວມເອົາ [ssl\_session\_cache](https://translate.google.com/website?sl=en&tl=lo&client=webapp&u=https://nginx.org/en/docs/http/ngx_http_ssl_module.html%23ssl_session_cache" \t "_blank)ຄໍາສັ່ງໃນການຕັ້ງຄ່າ, NGINX ແລະ NGINX Plus cache ພາລາມິເຕີຂອງເຊດຊັນທີ່ໃຊ້ເພື່ອສ້າງການເຊື່ອມຕໍ່ SSL/TLS. cache ນີ້, ແບ່ງປັນໃນບັນດາພະນັກງານທັງຫມົດເມື່ອທ່ານລວມເອົາ sharedພາລາມິເຕີ, ປັບປຸງເວລາຕອບສະຫນອງສໍາລັບການຮ້ອງຂໍຕໍ່ໄປຢ່າງຫຼວງຫຼາຍເພາະວ່າຂໍ້ມູນການຕິດຕັ້ງການເຊື່ອມຕໍ່ແມ່ນຮູ້ແລ້ວ. ກໍານົດຊື່ໃສ່ແຄດແລະກໍານົດຂະຫນາດຂອງມັນ (ແຄດທີ່ໃຊ້ຮ່ວມກັນ 1-MB ຮອງຮັບປະມານ 4,000 ເຊດຊັນ).

ຄໍາ [ssl\_session\_timeout](https://translate.google.com/website?sl=en&tl=lo&client=webapp&u=https://nginx.org/en/docs/http/ngx_http_ssl_module.html%23ssl_session_timeout" \t "_blank)ສັ່ງຄວບຄຸມໄລຍະເວລາທີ່ຂໍ້ມູນຂອງເຊດຊັນຍັງຄົງຢູ່ໃນ cache. ຄ່າເລີ່ມຕົ້ນແມ່ນ 5 ນາທີ; ເພີ່ມຂຶ້ນເປັນຫຼາຍຊົ່ວໂມງ (ໃນຕົວຢ່າງຕໍ່ໄປນີ້) ປັບປຸງປະສິດທິພາບແຕ່ຕ້ອງການ cache ຂະຫນາດໃຫຍ່.

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

ssl\_session\_timeout 4h;

**ປີ້ Session ແລະ IDs**

[ປີ້ Session](https://translate.google.com/website?sl=en&tl=lo&client=webapp&u=https://nginx.org/en/docs/http/ngx_http_ssl_module.html%23ssl_session_tickets) ເກັບຂໍ້ມູນກ່ຽວກັບເຊດຊັນ SSL/TLS ສະເພາະ. ເມື່ອລູກຄ້າສືບຕໍ່ການໂຕ້ຕອບກັບແອັບພລິເຄຊັນ, ປີ້ເຊດຊັນຈະຖືກນໍາໃຊ້ເພື່ອສືບຕໍ່ເຊດຊັນໂດຍບໍ່ມີການເຈລະຈາຄືນໃຫມ່. Session IDs ເປັນທາງເລືອກ; MD5 hash ຖືກນໍາໃຊ້ເພື່ອ map ກັບ Session ສະເພາະທີ່ເກັບໄວ້ໃນ cache ທີ່ສ້າງໂດຍ ssl\_session\_cacheຄໍາສັ່ງ. ກົນໄກທັງສອງສາມາດໃຊ້ເພື່ອຕັດການຈັບມື SSL/TLS.

ssl\_session\_tickets on;

**OCSP Stapling**

อีกวิธีหนึ่งในการปรับปรุงประสิทธิภาพ HTTPS คือการใช้[OCSP stapling](https://translate.google.com/website?sl=en&tl=th&client=webapp&u=https://nginx.org/en/docs/http/ngx_http_ssl_module.html%23ssl_stapling)ซึ่งลดเวลาของการจับมือ SSL/TLS  เมื่อผู้ใช้เชื่อมต่อกับแอปพลิเคชันหรือเว็บไซต์ของคุณผ่าน HTTPS เบราว์เซอร์จะตรวจสอบใบรับรอง SSL/TLS กับรายการเพิกถอนใบรับรอง (CRL) หรือใช้บันทึก Online Certificate Status Protocol (OCSP) จากผู้ออกใบรับรอง (CA) คำขอเหล่านี้เพิ่มเวลาในการตอบสนอง ด้วย NGINX และ NGINX Plus สามารถแคชการตอบสนอง 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;

Cipher Suites

ການລະບຸຊຸດລະຫັດລັບທີ່ຖືກປັບປຸງໃຫ້ເໝາະສົມ – ສູດການຄິດໄລ່ທີ່ເຂົ້າລະຫັດການສື່ສານໃນເຄືອຂ່າຍ – ບາງຄັ້ງກໍເວົ້າໄດ້ວ່າເພີ່ມປະສິດທິພາບ. ທ່ານ​ສາ​ມາດ​ນໍາ​ໃຊ້​ການ​ນໍາ​ໃຊ້ [ssl\_prefer\_server\_ciphers](https://translate.google.com/website?sl=en&tl=lo&client=webapp&u=https://nginx.org/en/docs/http/ngx_http_ssl_module.html%23ssl_prefer_server_ciphers" \t "_blank)​ຄໍາ​ສັ່ງ​ສໍາ​ລັບ​ຈຸດ​ປະ​ສົງ​ນີ້ໄດ້​, ແຕ່​​ຄວາມຈີງກໍຄື​ການ​ຕັ້ງ​ຄ່າ​ເລີ່ມ​ຕົ້ນ​ແມ່ນ​ດີ​​ພໍ​ສໍາ​ລັບ​ກໍ​ລະ​ນີ​ສ່ອນໄຫ່ຍ.  ພວກເຮົາແນະນໍາໃຫ້ທ່ານເລືອກລະຫັດລັບສະເພາະເພື່ອປະຕິບັດຕາມຄວາມຕ້ອງການຄວາມປອດໄພແລະປະສິດທິພາບໂດຍສະເພາະ.

SPDY

[SPDY](https://translate.google.com/website?sl=en&tl=lo&client=webapp&u=https://nginx.org/en/docs/http/ngx_http_spdy_module.html) ແມ່ນ ໂປຣໂຕຄໍ ທົດລອງ ເວລາໄປກັບສໍາລັບການຮັບສົ່ງຂໍ້ຄວາມ HTTP. ໂປໂຕຄອນສ້າງຊ່ວງສັນຍາລະຫວ່າງ​​ browser ແລະ Server ຂອງແອັບພລິເຄຊັນ. ໂດຍຜ່ານ HTTP multiplexing, SPDY ເປີດໃຊ້ການສົ່ງຕໍ່ການຈະລາຈອນພ້ອມກັນຜ່ານການເຊື່ອມຕໍ່ TCP ດຽວ, ຫຼຸດຜ່ອນຄວາມຈຳເປັນໃນການເຊື່ອມຕໍ່ເພີ່ມເຕີມແລະການເຈລະຈາ SSL. ໂປຣໂຕຄໍຍັງບີບອັດສ່ວນຫົວ HTTP ການຮ້ອງຂໍ ແລະຕອບສະໜອງ, ສົ່ງຜົນໃຫ້ມີການສົ່ງຜ່ານ bytes ໜ້ອຍລົງ. ມັນເປັນສິ່ງ ສຳ ຄັນທີ່ຈະຕ້ອງສັງເກດວ່າ SPDY ບໍ່ໄດ້ໃຫ້ຜົນປະໂຫຍດໃດໆຖ້າທ່ານກໍາລັງແບ່ງປັນໂດເມນ.

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;

ຜົນປະໂຫຍດຂອງການໃຊ້ SSL/TLS ແມ່ນຍິ່ງໃຫຍ່ກວ່າທີ່ເຄີຍມີມາກ່ອນ

ການເພີ່ມປະສິດທິພາບຂອງເຄື່ອງຈັກຊອກຫາຈຸດເປັນຈູຸດສົມໃຈສໍາລັບບໍລິສັດຈໍານວນຫຼາຍທີ່ມີອິນເຕີເນັດ. ໃນຄວາມເປັນຈິງ, Google ອາດຈະເຮັດໃຫ້ HTTPS ເປັນປັດໄຈການຈັດອັນດັບທີ່ມີອິດທິພົນຫຼາຍໃນອະນາຄົດ.