ວິທີການປັບປຸງ SEO ດ້ວຍ HTTPS ແລະ NGINX

ທ່ານຮູ້ບໍ່ວ່າການຮັບປະກັນເວັບໄຊທ໌ຂອງທ່ານດ້ວຍ HTTPS ສາມາດເພີ່ມການຈັດອັນດັບຂອງທ່ານໃນຜົນການຄົ້ນຫາຂອງ Google? Google ປະກາດໃນ [Blog ຄວາມປອດໄພອອນໄລນ໌](https://security.googleblog.com/2014/08/https-as-ranking-signal_6.html) ຂອງ ພວກເຂົາວ່າ algorithm ຄົ້ນຫາຂອງພວກເຂົາໃນປັດຈຸບັນພິຈາລະນາ HTTPS ເປັນສັນຍານການຈັດອັນດັບໃນເວລາທີ່ກັບຄືນຜົນການຄົ້ນຫາ.

[HTTP](https://www.nginx.com/resources/glossary/http/) , Hypertext Transfer Protocol, ແມ່ນພື້ນຖານຂອງການສື່ສານໃນອິນເຕີເນັດ. ຢ່າງໃດກໍຕາມ, ມັນບໍ່ປອດໄພເພາະວ່າການສື່ສານບໍ່ໄດ້ຖືກເຂົ້າລະຫັດ. HTTPS, ເວີຊັນທີ່ປອດໄພຂອງ HTTP, ໃຊ້ SSL ຫຼືໂປຣໂຕຄໍການເຂົ້າລະຫັດ TLS ທີ່ທັນສະໄຫມກວ່າເພື່ອເຂົ້າລະຫັດການໄຫຼເຂົ້າຂອງຂໍ້ມູນ. ບໍລິສັດທີ່ມີສະຕິຄວາມປອດໄພເຊັ່ນ Dropbox ໃຊ້ HTTPS ເພື່ອແກ້ໄຂສິ່ງທ້າທາຍດ້ານຄວາມປອດໄພ ແລະຄວາມເປັນສ່ວນຕົວ.

## **SSL ແລະ TLS ສາມາດສ້າງບັນຫາການປະຕິບັດທີ່ຮ້າຍແຮງ**

ການເພີ່ມປະສິດທິພາບຂອງເຄື່ອງຈັກຊອກຫາ (SEO) ໄດ້ຮັບຜົນປະໂຫຍດຈາກການຮັບປະກັນເວັບໄຊທ໌ຂອງເຈົ້າເປັນທີ່ດຶງດູດແຕ່ສໍາລັບຫຼາຍໆຄົນມັນບໍ່ຫນ້າຕື່ນເຕັ້ນ. ຄວາມເປັນຈິງແລ້ວແມ່ນວ່າແອັບພລິເຄຊັນຈໍານວນຫຼາຍຍັງອີງໃສ່ສະຖາປັດຕະຍະກໍາທີ່ບໍ່ມີປະສິດທິພາບໃນ stacks ຊອບແວຂອງເຂົາເຈົ້າແລະແລ້ວຕໍ່ສູ້ກັບ array ຂອງສິ່ງທ້າທາຍປະສິດທິພາບ. ການເພີ່ມ SSL ຫຼື TLS ສາມາດເຮັດໃຫ້ແອັບພລິເຄຊັນຊ້າລົງ ແລະ ຫິວຊັບພະຍາກອນຫຼາຍຂຶ້ນ.

ການຈັບມື SSL/TLS ທີ່ເຮັດໃຫ້ HTTPS ປອດໄພສາມາດສົ່ງຜົນກະທົບຕໍ່ການປະຕິບັດຢ່າງຫຼວງຫຼາຍ. ການຈັບມືແມ່ນຊຸດການສື່ສານລະຫວ່າງຕົວທ່ອງເວັບແລະເຄື່ອງແມ່ຂ່າຍທີ່ກວດສອບການເຊື່ອມຕໍ່ທີ່ເຊື່ອຖືໄດ້. ມັນເປັນຂະບວນການທີ່ໃຊ້ CPU ຫຼາຍແລະນໍາໄປສູ່ການເດີນທາງຮອບຫຼາຍລະຫວ່າງຜູ້ໃຊ້ແລະເຄື່ອງແມ່ຂ່າຍຂອງທ່ານ.

## **NGINX Solutions**

ໂຊກດີ, ເຄື່ອງແມ່ຂ່າຍເວັບໄຊຕ໌ທີ່ທັນສະໄຫມ, ເຊັ່ນ NGINX ແລະ NGINX Plus, ແກ້ໄຂສິ່ງທ້າທາຍເຫຼົ່ານີ້ແລະອະນຸຍາດໃຫ້ບໍລິສັດສາມາດປັບຂະຫນາດຄໍາຮ້ອງສະຫມັກໄດ້ດີຫຼາຍ. NGINX ແລະ NGINX Plus ສະຫນອງວິທີການຈໍານວນຫນຶ່ງທີ່ທ່ານສາມາດຫຼຸດຜ່ອນຜົນກະທົບດ້ານການປະຕິບັດຂອງ SSL/TLS, ລວມທັງການເກັບຮັກສາເຊດຊັນ, ປີ້ເຊດຊັນຫຼື IDs, OCSP stapling, ແລະອະນຸສັນຍາ SPDY ທົດລອງ.

### **Session Caching**

ເມື່ອທ່ານລວມເອົາ [ssl\_session\_cache](https://nginx.org/en/docs/http/ngx_http_ssl_module.html" \l "ssl_session_cache" \t "_blank)ຄໍາສັ່ງໃນການຕັ້ງຄ່າ, NGINX ແລະ NGINX Plus cache ພາລາມິເຕີຂອງເຊດຊັນທີ່ໃຊ້ເພື່ອສ້າງການເຊື່ອມຕໍ່ SSL/TLS. cache ນີ້, ແບ່ງປັນໃນບັນດາພະນັກງານທັງຫມົດເມື່ອທ່ານລວມເອົາ sharedພາລາມິເຕີ, ປັບປຸງເວລາຕອບສະຫນອງສໍາລັບການຮ້ອງຂໍຕໍ່ໄປຢ່າງຫຼວງຫຼາຍເພາະວ່າຂໍ້ມູນການຕິດຕັ້ງການເຊື່ອມຕໍ່ແມ່ນຮູ້ແລ້ວ. ກຳນົດຊື່ໃສ່ແຄດ ແລະຕັ້ງຂະໜາດຂອງມັນ (ແຄສທີ່ໃຊ້ຮ່ວມກັນ 1-MB ຮອງຮັບປະມານ 4,000 ເຊດຊັນ).

ຄໍາ [ssl\_session\_timeout](https://nginx.org/en/docs/http/ngx_http_ssl_module.html" \l "ssl_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://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_tickets) ເກັບຂໍ້ມູນກ່ຽວກັບເຊດຊັນ SSL/TLS ສະເພາະ. ເມື່ອລູກຄ້າສືບຕໍ່ການໂຕ້ຕອບກັບແອັບພລິເຄຊັນ, ປີ້ເຊດຊັນຈະຖືກນໍາໃຊ້ເພື່ອສືບຕໍ່ເຊດຊັນໂດຍບໍ່ມີການເຈລະຈາຄືນໃຫມ່. Session IDs ເປັນທາງເລືອກ; MD5 hash ຖືກນໍາໃຊ້ເພື່ອແຜນທີ່ກັບກອງປະຊຸມສະເພາະທີ່ເກັບໄວ້ໃນ cache ທີ່ສ້າງໂດຍ ssl\_session\_cacheຄໍາສັ່ງ. ກົນໄກທັງສອງສາມາດໃຊ້ເພື່ອຕັດການຈັບມື SSL/TLS.

ssl\_session\_tickets on;

### **OCSP Stapling**

ອີກວິທີ ໜຶ່ງ ເພື່ອປັບປຸງການປະຕິບັດ HTTPS ແມ່ນດ້ວຍການ [ຍຶດ OCSP](https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling) , ເຊິ່ງເຮັດໃຫ້ເວລາຈັບມື SSL / TLS ຫຼຸດລົງ. ຕາມປະເພນີ, ເມື່ອຜູ້ໃຊ້ເຊື່ອມຕໍ່ກັບແອັບພລິເຄຊັນຫຼືເວັບໄຊທ໌ຂອງເຈົ້າຜ່ານ HTTPS, ຕົວທ່ອງເວັບຈະກວດສອບໃບຢັ້ງຢືນ SSL/TLS ຕໍ່ກັບບັນຊີການຖອນໃບຢັ້ງຢືນ (CRL) ຫຼືໃຊ້ບັນທຶກສະຖານະພາບຂອງໃບຢັ້ງຢືນອອນໄລນ໌ (OCSP) ຈາກອົງການໃບຢັ້ງຢືນ (CA). ການຮ້ອງຂໍເຫຼົ່ານີ້ເພີ່ມເວລາ latency ແລະ CAs ສາມາດບໍ່ຫນ້າເຊື່ອຖື. ດ້ວຍ NGINX ແລະ NGINX Plus ທ່ານສາມາດເກັບການຕອບສະ ໜອງ OCSP ໃຫ້ກັບເຄື່ອງແມ່ຂ່າຍຂອງທ່ານແລະລົບລ້າງຄ່າໃຊ້ຈ່າຍທີ່ແພງເກີນໄປ.

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 – ບາງຄັ້ງກໍເວົ້າໄດ້ວ່າຈະຊ່ວຍເພີ່ມປະສິດທິພາບ. ທ່ານ​ສາ​ມາດ​ນໍາ​ໃຊ້​ການ​ນໍາ​ໃຊ້ [ssl\_prefer\_server\_ciphers](https://nginx.org/en/docs/http/ngx_http_ssl_module.html" \l "ssl_prefer_server_ciphers" \t "_blank)​ຄໍາ​ແນະ​ນໍາ​ສໍາ​ລັບ​ຈຸດ​ປະ​ສົງ​ນີ້​, ແຕ່​ຄວາມ​ເປັນ​ຈິງ​ແມ່ນ​ວ່າ​ການ​ຕັ້ງ​ຄ່າ​ເລີ່ມ​ຕົ້ນ​ແມ່ນ​ດີ​ພຽງ​ພໍ​ສໍາ​ລັບ​ກໍ​ລະ​ນີ​ສ່ວນ​ໃຫຍ່​. ການຕັ້ງຄ່ານີ້, ແລະການປະຕິບັດທີ່ດີທີ່ສຸດ, ເຮັດວຽກໄດ້ດີເທົ່າທຽມກັນສໍາລັບຕົວລະຫັດເກົ່າ, ປັດຈຸບັນ, ແລະ (ຄວາມຫວັງອັນຫນຶ່ງ) ໃນອະນາຄົດ. ພວກເຮົາແນະນໍາໃຫ້ທ່ານເລືອກລະຫັດລັບສະເພາະເພື່ອປະຕິບັດຕາມຄວາມຕ້ອງການຄວາມປອດໄພແລະປະສິດທິພາບໂດຍສະເພາະ.

### **SPDY**

ບັນນາທິການ – SPDY ເປັນພື້ນຖານສໍາລັບ [*ມາດຕະຖານ HTTP/2*](https://tools.ietf.org/html/rfc7540) ທີ່ຕີພິມໃນເດືອນພຶດສະພາ 2015. ການຮອງຮັບ SPDY ໄດ້ຖືກຍົກເລີກ – ແລະ HTTP/2 ໄດ້ຮັບການສະຫນັບສະຫນູນຢ່າງເຕັມສ່ວນ – ໃນ [*NGINX Plus Release 7*](https://www.nginx.com/blog/http2-r7/) ແລະຕໍ່ມາ, ແລະ [*NGINX 1.9.5*](https://www.nginx.com/blog/nginx-1-9-5/) ແລະຕໍ່ມາ.

[SPDY](https://nginx.org/en/docs/http/ngx_http_spdy_module.html) ແມ່ນ ໂປຣໂຕຄໍ ທົດລອງ ທີ່ພະຍາຍາມຫຼຸດຜ່ອນເວລາ latency ແລະເວລາໄປກັບສໍາລັບການຈະລາຈອນ HTTP. ໂປໂຕຄອນສ້າງອຸໂມງລະຫວ່າງຕົວທ່ອງເວັບແລະເຄື່ອງແມ່ຂ່າຍຂອງແອັບພລິເຄຊັນ. ໂດຍຜ່ານ HTTP multiplexing, SPDY ເປີດໃຊ້ການສົ່ງການຈະລາຈອນພ້ອມກັນຜ່ານການເຊື່ອມຕໍ່ TCP ດຽວ, ຫຼຸດຜ່ອນຄວາມຕ້ອງການສໍາລັບການເຊື່ອມຕໍ່ເພີ່ມເຕີມແລະການເຈລະຈາ SSL. ໂປຣໂຕຄໍຍັງບີບອັດສ່ວນຫົວ HTTP ການຮ້ອງຂໍແລະການຕອບສະໜອງ, ສົ່ງຜົນໃຫ້ມີການສົ່ງຜ່ານ bytes ໜ້ອຍລົງ. ມັນເປັນສິ່ງສໍາຄັນທີ່ຈະສັງເກດວ່າ SPDY ສະຫນອງຜົນປະໂຫຍດທີ່ບໍ່ມີຖ້າຫາກວ່າທ່ານກໍາລັງ sharding ໂດເມນ.

listen 443 ssl spdy;

spdy\_headers\_comp 1;

ບັນນາທິການ - ດ້ວຍການສະຫນັບສະຫນູນ HTTP/2, http2 ພາລາມິເຕີຈະປ່ຽນ spdy ພາລາມິເຕີກັບ listen ຄໍາສັ່ງທີ່ສະແດງຢູ່ໃນ snippet ຂ້າງເທິງ. ບໍ່ມີ spdy\_headers\_comp ຄໍາສັ່ງທຽບເທົ່າກັບ HTTP/2.

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

listen 443 ssl http2;

## **ຜົນປະໂຫຍດຂອງການໃຊ້ SSL/TLS ແມ່ນຍິ່ງໃຫຍ່ກວ່າທີ່ເຄີຍມີມາກ່ອນ**

ການເພີ່ມປະສິດທິພາບຂອງເຄື່ອງຈັກຊອກຫາແມ່ນຈຸດສຸມສໍາລັບບໍລິສັດຈໍານວນຫຼາຍທີ່ມີອິນເຕີເນັດ. ໃນຄວາມເປັນຈິງ, Google ອາດຈະເຮັດໃຫ້ HTTPS ເປັນປັດໄຈການຈັດອັນດັບທີ່ມີອິດທິພົນຫຼາຍໃນອະນາຄົດອັນໃກ້ນີ້. ມັນເປັນເລື່ອງທີ່ຫນ້າຕື່ນເຕັ້ນທີ່ມີທາງເລືອກທີ່ມີຢູ່ທີ່ອະນຸຍາດໃຫ້ຜູ້ຄຸ້ມຄອງເວັບໃດກໍ່ຕາມເພື່ອຕອບສະຫນອງຄວາມຕ້ອງການຂອງຄວາມປອດໄພຂອງຜູ້ໃຊ້ຢ່າງມີປະສິດທິພາບໃນຂະນະທີ່ຍັງໃຫ້ຜູ້ຊົມໃຊ້ຮັກແພງ.

ໃນຕອນທ້າຍຂອງມື້, ທ່ານບໍ່ຄວນຮັບປະກັນເວັບໄຊທ໌ຂອງທ່ານ ພຽງແຕ່ ສໍາລັບຜົນປະໂຫຍດ SEO - ແຕ່ມັນເປັນແຮງຈູງໃຈທີ່ດີຈາກ Google ທີ່ພວກເຮົາຫວັງວ່າຈະກະຕຸ້ນໃຫ້ທ່ານພິຈາລະນາຄວາມປອດໄພຂອງຄໍາຮ້ອງສະຫມັກຂອງທ່ານ. ຜູ້ທີ່ບໍ່ຕ້ອງການປັບປຸງປະສົບການແລະຄວາມປອດໄພຂອງຜູ້ໃຊ້ໃນຂະນະທີ່ຍັງໄດ້ຮັບການຊຸກຍູ້ SEO?

ເພື່ອເລີ່ມຕົ້ນ, ແລະຮຽນຮູ້ເພີ່ມເຕີມກ່ຽວກັບວິທີຕັ້ງຄ່າ ແລະປັບປຸງ HTTPS, ໃຫ້ກວດເບິ່ງຄູ່ມືຜູ້ເບິ່ງແຍງລະ [ບົບ NGINX Plus](https://docs.nginx.com/nginx/admin-guide/security-controls/terminating-ssl-http/) .