SSL/TLS pour le web

Pourquoi ? Comment ?

PLUG — 6 février 2015

Internet

un truc de hippies

des protocoles ouverts

HTTP, FTP, SMTP, POP, IMAP, DNS, NTP, etc.

inter-opérabilité

texte clair

```
→ telnet en.wikipedia.org 80
Trying 91.198.174.192...
Connected to en.wikipedia.org.
Escape character is '^]'.
GET /wiki/Main_Page http/1.1
Host: en.wikipedia.org

HTTP/1.1 200 OK
Server: Apache
Last-Modified: Tue, 03 Feb 2015 20:59:47 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 03 Feb 2015 21:15:22 GMT
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate

<!DOCTYPE html>
<html lang="en" dir="ltr" class="client-nojs">
…
```

clarté & simplicité

vs.

aucune garantie

aucune garantie

1. identité du serveur
2. confidentialité des données
3. intégrité des données

🔒 HTTPS


SSLv1
SSLv2
SSLv3
TLSv1.0
TLSv1.1
TLSv1.2
TLSv1.3

évolutions

- sécurité
- performance
- fonctionnalités

la cryptographie

garantie la confidentialité et l'intégrité

les certificats

garantissent l'identité


Safari utilise une connexion chiffrée à www.wikipedia.org.
Le chiffrement avec un certificat numérique garantit la confidentialité des données lors de l'envoi et la réception depuis le site web https www.wikipedia.org.
GlobalSign Root CA
GlobalSign Organization Validation CA - SHA256 - G2
*.wikipedia.org
Certificate
Standard
*.wikipedia.org
Délivré par: GlobalSign Organization Validation CA - SHA256 - G2
Expire le dimanche 22 novembre 2015 19:06:02 heure normale d'Europe centrale
Ce certificat est valide
Se fier
Détails

Objectif concret

Certificat SSL Gandi avec Nginx sur Linux

Niveaux de recommandation

mozilla

modern

Firefox 27, Chrome 22, IE 11, Opera 14, Safari 7, Android 4.4, Java 8

intermediate

Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7

old

Windows XP IE6, Java 6

Certificat wildcard SHA-2

HTTP Strict Transport Security

Perfect Forward Secrecy

En pratique

Création du certificat

```
→ openssl req -nodes -newkey rsa:2048 -sha256 \
-keyout wildcard_example_com.key.pem \
-out wildcard_example_com.csr.pem
```

-----BEGIN CERTIFICATE REQUEST-----
MIICzzCCAbcCAQAwgYkxCzAJBgNVBAYTAkZSMRMwEQYDVQQIEwpTb21lLVN0YXRl
MRIwEAYDVQQHEwlNYXJzZWlsbGUxFTATBgNVBAoTDEV4YW1wbGUgSW5jLjEWMBQG
A1UEAxQNKi5leGFtcGxlLmNvbTEiMCAGCSqGSIb3DQEJARYTY29udGFjdEBleGFt
cGxlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKO13wEpS2Ka
unLpJVLF2AqYVZV4OK7p7OG4IfVhkK5wP/kh8KYxyOHZZDx+rGfJE1UA8dJQd+EV
xST0tdN2tw0Dv0jSv6SjXoQO1inTbDf+qixxAj/RxAVmn8AuWC3g/YtI7Wikb3PO
+h81Ezb7i4rkZGYoFleDOpprQvxZEKVXOyU9bumKJRY3YO7xmwdV1pVt+vwgyR+8
sI1R7OCglPwdYlRD9R0ZFEzpPYkDmY7qkx9Jk+TJNewSyS4wy6qg6Neguxg+hYaD
MLY5kXmhmRBHlTaOznbi8m/lEIszH9/r+4weDjt66DPEmM0vUEl3p8dZUb2Nkn7n
gBOCM4/mdhcCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQAri8Gtz2SkiBMXb4Me
ICL/exVrM6q03wcrFSOE9XJbcyOOA1gP8+zWNcNlMyfd/MpB5lNRPdzKT01zb17z
kiteEDTSvGMTwklWJN08hJDXPXs2POnQDZau/FEAvLM8jWheq+UzSsIsuSju1MUJ
ra8d/3FH25J5eRCvy63tPpje9qk+EoHxO5g22QCcgXIc2CANicLNjTKkECG+TRN1
WMmir+a2+raBgNZCrE5N87SsfHnhPZEJExXL5AuKTAOH3FcBb0G1f4KcKPgULbrE
aH9rpFywuEMgnkp3eRoxtPs7UuTVTaNIjCJX+Q5oY2eT6cH1UVwn8qnJe1j8S6Mx
CGi7
-----END CERTIFICATE REQUEST-----

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAo7XfASlLYpq6cuklUsXYCphVlXg4runs4bgh9WGQrnA/+SHw
pjHI4dlkPH6sZ8kTVQDx0lB34RXFJPS103a3DQO/SNK/pKNehA7WKdNsN/6qLHEC
P9HEBWafwC5YLeD9i0jtaKRvc876HzUTNvuLiuRkZigWV4M6mmtC/FkQpVc7JT1u
6YolFjdg7vGbB1XWlW36/CDJH7ywjVHs4KCU/B1iVEP1HRkUTOk9iQOZjuqTH0mT
5Mk17BLJLjDLqqDo16C7GD6FhoMwtjmReaGZEEeVNo7OduLyb+UQizMf3+v7jB4O
O3roM8SYzS9QSXenx1lRvY2SfueAE4Izj+Z2FwIDAQABAoIBAQCO7LlEykiGTY95
wxJSsWdr2JLfa5YRHykv5xG+qO8nW9h+KKNwdQZsJt7b8buS4HmAPNLiSl5epCL5
…
z2dKswESYgUYHe+qfjc0ICXzjT5To6nyUxjh+VnwxsUBg5m4qkTBxkl3HCzIz5gK
t2OvCQblfTf94nRBvcclZGjtVyYJVt8PULmj9ncJSR/p2GGWNNhb+SM1Zry07nzR
KABin0qxF3A6Ch8lxTntsAECgYEAvVWR9lYXsZ4YUzHK67pmNrpRc7gfFQ2Yn9Lj
deduvlZdizsbh5++UrXIhlGZ6J75OZbNzGh2cSW7U1jweJ+HrRXFV1Ybpe0uDiQA
8BmnxQh7X+t0skEytBadYUMp3sa3QdUWhBiDvFLK7LNwUlpCJtZqAjWYZjzjqLsI
Emtg1/0CgYA214z3XCLXqenPDcJuYHoKaDNY7hBJpcMx+PC/djHa5lbFCYzfhg7h
A+sH/qFmLTkb3Ha+S4uRTWlEfMk7iliwAGfGhYBTCjUQiqdLdwSkO6YBey0nXZLJ
E0pV7+shRPoK7jguy6zzSHK1ygWnqTSn8TePgtIXOoVcZoH6jQBfcA==
-----END RSA PRIVATE KEY-----

Config du serveur

```
user www-data;
worker_processes 32;
pid /var/run/nginx.pid;

events {
  worker_connections 768;
}

http {
  sendfile on;
  tcp_nopush on;
  tcp_nodelay on;
  keepalive_timeout 65;

  include /etc/nginx/mime.types;
  default_type application/octet-stream;

  access_log /var/log/nginx/access.log;
  error_log /var/log/nginx/error.log;

  include /etc/nginx/sites-enabled/*;
}
```

```
server {
  listen 80;
  rewrite ^ https://$host$request_uri? permanent;
}
server {
  listen 443 ssl;

  server_name www.example.com;

  include /etc/nginx/wildcard_example_com.ssl.conf;
  add_header Strict-Transport-Security max-age=31536000;

  root /var/www/example;
  index index.htm index.html;
}
```

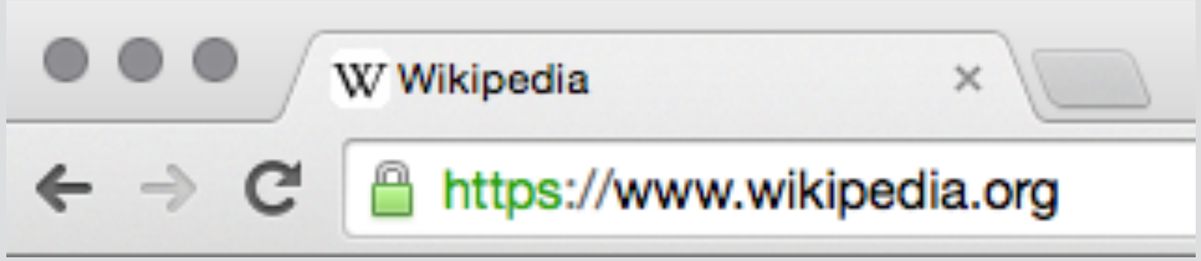
```
ssl_certificate /etc/ssl/certs/wildcard_example_com.chain.pem;
ssl_certificate_key /etc/ssl/private/wildcard_example_com.key.pem;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:
            CAMELLIA:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:
            !PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:
            !KRB5-DES-CBC3-SHA';
ssl_prefer_server_ciphers on;

ssl_session_timeout 24h;
ssl_session_cache shared:SSL:10m;

ssl_dhparam /etc/ssl/dhparam.pem;

ssl_stapling on;
ssl_stapling_verify on;
ssl_trusted_certificate /etc/ssl/certs/gandi-standardssl-2.chain.pem;

resolver 127.0.0.1;
```

Vérifications

dans les logs Nginx

```
→ tail -f /var/log/nginx/error.log
```

dans un navigateur



avec CipherScan

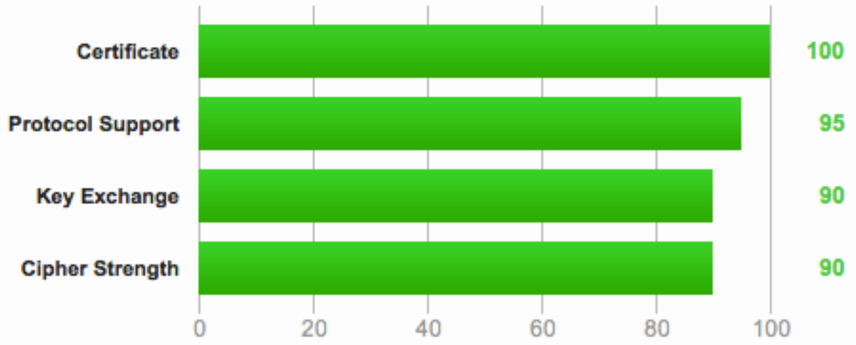
```
→ cipherscan/analyze.py -t www.example.com

www.example.com:443 has intermediate ssl/tls
and complies with the 'intermediate' level
```

QUALYS® SSL LABS

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

Ressources

jlecour.github.io/ssl-gandi-nginx-debian

wiki.mozilla.org/Security/Server_Side_TLS

istlsfastyet.com

jeveuxhttps.fr

how2ssl.com

trac.evolix.net/infogerance/wiki/HowtoSSL

Merci

envoyez les questions

Jérémy Lecour

HÔTEL À PARIS .com

jeremy@lecour.fr

@jlecour

jeremy.wordpress.com

github.com/jlecour