SSL Report: gmail.com (2607:f8b0:4005:80a:0:0:0:2005)

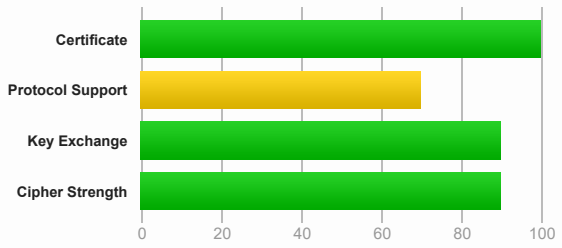
Assessed on: Fri, 22 Oct 2021 19:15:35 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



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

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Static Public Key Pinning observed for this server.

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: EC 256 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	gmail.com Fingerprint SHA256: 6e751c6d93f87ffbefd1913ef29f695565562ca17b18cd5d1c904727386d145c Pin SHA256: LRjFYPLl/t7ZlujkWb+LuPuKd/cRbH6Sf4sg32MIAwQ=
Common names	gmail.com
Alternative names	gmail.com *.gmail.com
Serial Number	55a53dedcd5d71e80a0000000108ad7c
Valid from	Mon, 04 Oct 2021 02:11:47 UTC
Valid until	Mon, 27 Dec 2021 02:11:46 UTC (expires in 2 months and 4 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	GTS CA 1C3 AIA: http://pki.goog/repo/certs/gts1c3.der
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl OCSP: http://ocsp.pki.goog/gts1c3
Revocation status	Good (not revoked)

Server Key and Certificate #1

DNS CAA	**Yes** policy host: gmail.com issue: pki.goog flags:0
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (3982 bytes)
Chain issues	None

#2

Subject	GTS CA 1C3 Fingerprint SHA256: 23ecb03eec17338c4e33a6b48a41dc3cda12281bbc3ff813c0589d6cc2387522 Pin SHA256: zCTnfLwLKbS9S2sbp+uFz4KZOocFvXxkV06Ce9O5M2w=
Valid until	Thu, 30 Sep 2027 00:00:42 UTC (expires in 5 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	GTS Root R1
Signature algorithm	SHA256withRSA

#3

Subject	GTS Root R1 Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5 Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
Valid until	Fri, 28 Jan 2028 00:00:42 UTC (expires in 6 years and 3 months)
Key	RSA 4096 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI

Click here to expand

Certificate #3: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	gmail.com Fingerprint SHA256: 438a6c749d2ffa40ab7262a29dffb3e3fcfbb2207b4676fac11125eb7ebc79b0 Pin SHA256: hs2SWbuItKUMyAJb75uHW6uBv9QXJgWMZv1j5GRmtgs=
Common names	gmail.com
Alternative names	gmail.com *.gmail.com
Serial Number	221b2aaca488c4a50a0000000108ad79
Valid from	Mon, 04 Oct 2021 02:11:39 UTC
Valid until	Mon, 27 Dec 2021 02:11:38 UTC (expires in 2 months and 4 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GTS CA 1C3 AIA: http://pki.goog/repo/certs/gts1c3.der

Server Key and Certificate #1

Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl OCSP: http://ocsp.pki.goog/gts1c3
Revocation status	Good (not revoked)
DNS CAA	**Yes** policy host: gmail.com issue: pki.goog flags:0
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (4186 bytes)
Chain issues	None

#2

Subject	GTS CA 1C3 Fingerprint SHA256: 23ecb03eec17338c4e33a6b48a41dc3cda12281bbc3ff813c0589d6cc2387522 Pin SHA256: zCTnfLwLKbS9S2sbp+uFz4KZOocFvXxkV06Ce9O5M2w=
Valid until	Thu, 30 Sep 2027 00:00:42 UTC (expires in 5 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	GTS Root R1
Signature algorithm	SHA256withRSA

#3

Subject	GTS Root R1 Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5 Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
Valid until	Fri, 28 Jan 2028 00:00:42 UTC (expires in 6 years and 3 months)
Key	RSA 4096 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	Yes
TLS 1.0	Yes*
SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

Cipher Suites

TLS 1.3 (server has no preference)

TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112

TLS 1.1 (suites in server-preferred order)

TLS 1.0 (suites in server-preferred order)

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

Handshake Simulation

Android 2.3.7 No SNI [2]	Incorrect certificate because this client doesn't support SNI RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA		
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.3	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 5.0.0	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Baidu Jan 2015	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS

Handshake Simulation

Googlebot Feb 2018	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
IE 7 / Vista	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 8 / XP No FS [1] No SNI [2]	Incorrect certificate because this client doesn't support SNI RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_3DES_EDE_CBC_SHA		
IE 8-10 / Win 7 R	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 10 / Win Phone 8.0	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 16 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 18 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 13 / Win Phone 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 6u45 No SNI [2]	Incorrect certificate because this client doesn't support SNI RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA		
Java 7u25	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u161	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 1.0.1l R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.0k R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Apple ATS 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)

IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc009
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc009
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc009
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc009
Sleeping POODLE	No (more info) TLS 1.2 : 0xc009
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	Yes h2 http/1.1
NPN	Yes grpc-exp h2 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	**Chrome Edge Firefox IE**
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	**Yes** includeSubDomains: false report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbDAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YZPgTZ+woNCCCIW3LH2CxQeLzB/1m42QcCTBSdgayjs= pin-sha256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc= pin-sha256: Vfd95BwDeSQo+NUYxVEEIlvkOlWY2SalKK1lPhzOx78= pin-sha256: QXnt2YHvdHR3tJYmQIr0Paosp6t/nggsEGD4QJZ3Q0g= pin-sha256: mEflZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpiOjYQ0c= pin-sha256: iie1VXtL7HzAMF+/PVPR9xzT80kQxdZeJ+zduCB3uj0= pin-sha256: hxrRCWblJB5FGRZv++qAms7uX69qFC45aBhVpeGclco= (Forbidden) pin-sha256: SG/sBoMJc9IgJ8+dGgIHyTLvz7wyVBio7lMoDanPuRk= (Forbidden) pin-sha256: LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A= (Forbidden)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1 (server preferred order)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

HTTP Requests

1 **https://gmail.com/** (HTTP/1.1 301 Moved Permanently)

Miscellaneous

Test date	Fri, 22 Oct 2021 19:12:06 UTC
Test duration	104.320 seconds
HTTP status code	301
HTTP forwarding	https://www.google.com
HTTP server signature	sffe
Server hostname	sfo07s17-in-x05.1e100.net

SSL Report v2.1.8