OpenSSL - s_server

Serveur SSL/TLS

OPTIONS

-accept port Port TCP d'écoute (défaut : 4433)

-context id ID de Context SSL. Peut être une valeur chaîne.

-cert certname Certificat à utiliser.

-certform PEM|DER Format du certificat

-key keyfile Clé privée à utiliser

-keyform PEM|DER Format de la clé privée

-pass arg Source du mot de passe de la clé privée

-dcert filename, -dkey keyname Certificat et clé privée additionnel

-dcertform format, -dkeyform format, -dpass arg Le format du certificat et de la clé privée supplémentaire, et la source du mot de passe.

-nocert Ne pas utiliser de certificat. Restreint la suite de chiffrements à anonymous DH.

-dhparam filename Fichier de paramètres DH à utiliser

-no_dhe Ne charge aucun paramètre DH et désactive les suites de chiffrement ephemeral DH.

-no_tmp_rsa Pour les suites utilisant une clé RSA temporaire, désactive la génération d'une telle clé.

-verify depth, -Verify depth Spécifie la longueur max de la chaîne de certificat client et force le serveur à demander le certificat du client. -verifie, le client n'a pas à fournir de certificat, -Verify l'oblige.

-crl_check, -crl_check_all Vérifie la CRL. Les crl sont ajoutés au fichier de certificat.

-CApath directory Répertoire contenant les certificats de la CA au 'hash format'

-CAfile file Un fichier contenant les certificats de confiance

-state Affiche l'état de session SSL

-debug Affiche des informations de débogage incluant un dump hexa de tout le trafic

-msg Affiche tous les messages de protocoles avec dump hexa

-nbio_test Tests IO non bloquant

-nbio Active l'I/O non bloquant

-crlf Traduit un line feed depuis le terminal en CR+LF

-quiet Inhibe l'affichage de session et des informations de certificat

-psk_hint hint Utilise l'identité PSK en utilisant la suite de chiffrement PSK.

-psk key Utilise la clé PSK spécifié. La clé est donnée en hexa sans 0x, exemple : 1a2b3c4d

-ssl2, -ssl3, -tls1, -no_ssl2, -no_ssl3, -no_tls1 Désactive l'utilisation de certains protocoles SSL ou TLS. Par défaut, le handshake utilise une méthode qui devrait être compatible avec tous les serveurs et permet d'utiliser SSLv3, SSLv2 ou TLS.

-bugs Il y'a de nombreux bugs connus dans les implémentations SSL et TLS. Cette option autorise diverses solutions.

-hack Active une solution de contournement pour certaines anciennes versions de Netscape SSL.

-cipher cipherlist Permet de modifier la liste des chiffrements utilisés par le serveur.

-tlsextdebug Affiche un dump hexa des extensions TLS reçue

-no_ticket Désactive le support de ticket de session RFC4507bis

-www Envoie un message de statut au client quand il se connecte. Inclus beaucoup d'informations sur les chiffrements utilisé et divers paramètres de session, la sortie est au format HTML.

-WWW Emule un serveur web simple. Les pages chargées sont relatives au répertoire courant. (Ex : https ://myhost/page.html charge ./page.html)

-HTTP idem, mais les pages chargée contiennent une réponse HTTP complète et correcte.

-engine id s_server va tenter d'obtenir une référence fonctionnelle du moteur spécifié.

-id_prefix arg Génère un ID de session SSL/TLS préfixé par arg.

-rand file(s) Le(s) fichier(s) contenant les données aléatoire utilisé par le générateur de nombre aléatoire.

Commandes connectées

Si une connexion est établie avec un client SSL et ni -www ni -WWW n'est utilisé, les données du client sont affichées et l'appuie sur une touche sera envoyé au client :

q Termine la connexion SSL courante, mais accepte les nouvelles connections

Q Termine la connexion SSL courante et quitte.

r Renégocie la session SSL

R Renégocie la session SSL et demande un certificat client

P Envoie un texte en clair à la connexion TCP : devrait forcer le client à se déconnecter dû à une violation de protocole.

S Affiche les informations de statut du cache de session

Notes

s_server peut être utilisé pour débugger les clients SSL. Pour accepter les connections depuis un navigateur web :
openssl s_server -accept 443 -www
Beaucoup de navigateurs ne supportent que les suites de chiffrement RSA. Les paramètres de session peuvent être imprimés avec sess_id.