

THINK APP SECURITY FIRST

SSL/TLS ORCHESTRATION

TLS 1.3: ARE YOU READY?

IT'S OFFICIAL

TLS 1.3 has been approved by the Internet Engineering Task Force (IETF), and it contains “major improvements in the areas of security, performance, and privacy.” And unlike with TLS 1.2, there appears to be some built-in motivation to upgrade. TLS 1.3 offers a performance boost, which in itself will perk up the ears of more than just security folks.

The benefits offered by TLS 1.3 are substantial, but more comprehensive encryption also makes it tougher to spot malicious traffic and defend against attacks hidden in that encrypted traffic. You may need to take a new approach to get the visibility you need while simultaneously preserving your performance gain realized by the updated protocol.



THE BENEFITS OFFERED BY TLS 1.3 ARE SUBSTANTIAL, BUT MORE COMPREHENSIVE ENCRYPTION ALSO MAKES IT TOUGHER TO SPOT MALICIOUS TRAFFIC.

WHAT'S NEW IN TLS 1.3?

TLS 1.3 offers some great improvements over TLS 1.2. Vulnerable optional parts of the protocol have been removed, there's support for stronger ciphers required to implement perfect forward secrecy (PFS), and the handshake process has been significantly shortened.

In addition, implementing TLS 1.3 should be relatively simple. You can use the same keys you used for TLS 1.2. Clients and servers will automatically negotiate a TLS 1.3 handshake when they both support it, and Google Chrome and Mozilla Firefox already do it by default.

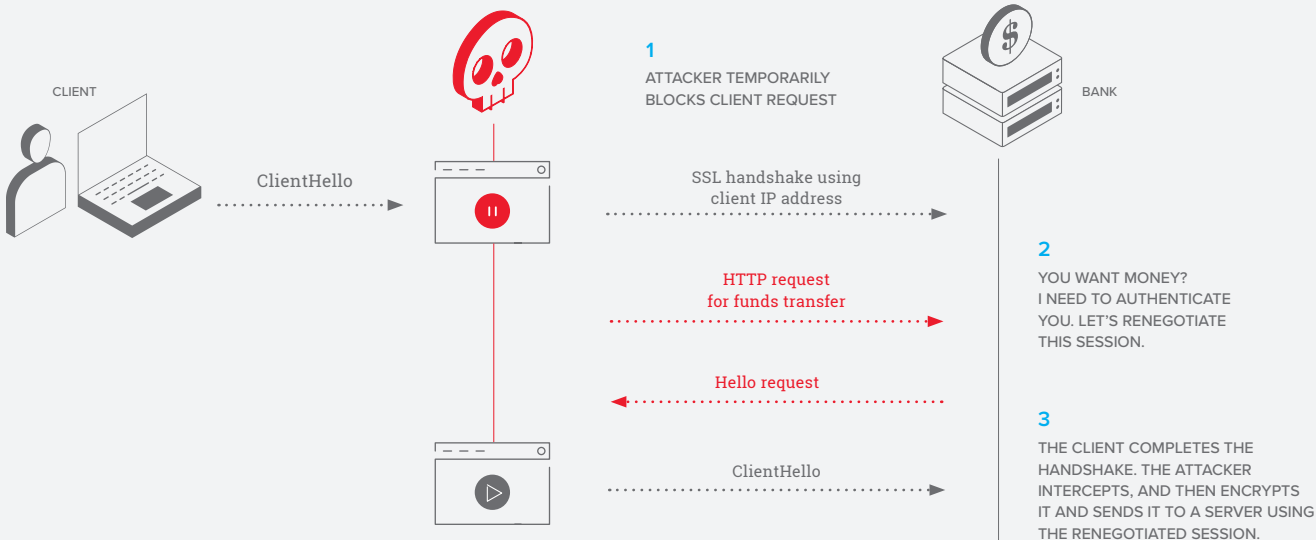
Security benefits

Although TLS 1.2 can still be deployed securely, several high-profile vulnerabilities have exploited optional parts of the protocol and outdated ciphers. TLS 1.3 removes many of these problematic options and only includes support for algorithms with no known vulnerabilities (at this time).

The IETF chose to remove all ciphers that do not support PFS from TLS connections. These include DES, AES-CBC, RC4, and other ciphers less commonly used. They also removed the ability to perform what’s known as “renegotiation,” which allows a client and server that already have a TLS connection to negotiate new parameters, generate new keys, etc. Eliminating renegotiation closes a window of opportunity for an attack.

RENEGOTIATION ATTACK

The renegotiation attack is an example of a threat that is no longer possible in TLS 1.3.



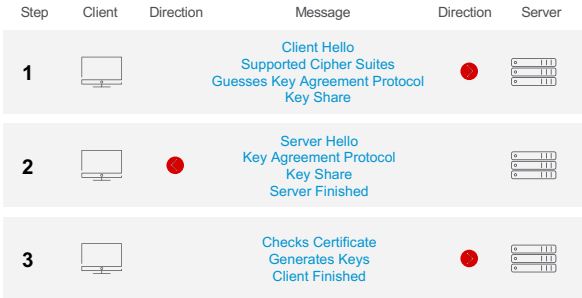
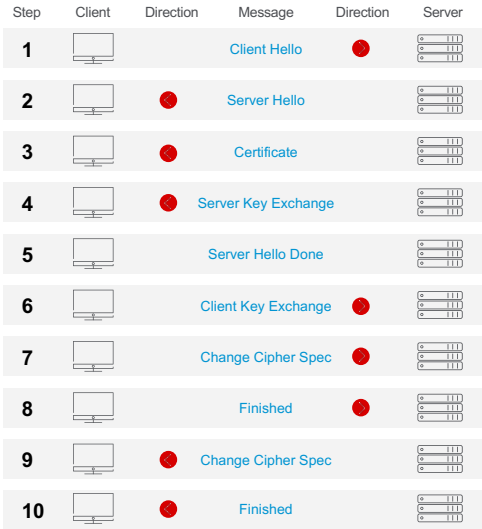
Privacy benefits

TLS 1.3 also enables PFS by default. This cryptographic technique adds another layer of confidentiality to an encrypted session, ensuring that only the two endpoints can decrypt the traffic. With PFS, even if a third party were to record an encrypted session, and later gain access to the server private key, they could not use that key to decrypt the session.

Performance benefits

With respect to performance, TLS 1.3 shaves an entire round trip from the connection establishment handshake, which cuts the encryption latency in half. Another advantage is when accessing a site you have previously visited, you can now send data on the first message to the server. This is called a “zero round trip time” (0-RTT). These enhancements—coupled with efficient modern cryptographic algorithms—can make TLS 1.3 faster than TLS 1.2.

TLS 1.2 HANDSHAKE AND TLS 1.3 COMPARISON



Sounds great: what’s the catch?

With all these benefits, what could possibly be a problem? So glad you asked! With PFS, only the endpoints (the web user and the application server), can decrypt the traffic. However, it’s likely that you have one or more solutions—like a next-gen firewall, an intrusion detection system (IDS), or a malware sandbox—designed to spot malicious traffic egressing your network. Or you may have a web application firewall, IDS, or an analytics solution in front of an application that you host. All these solutions sit between a user and the application or website they are connected to, so they are blind to the encrypted traffic.

Another issue certainly worth mentioning is the 0-RTT feature with TLS 1.3 has some security experts up in arms because of the potential for replay attacks. And without 0-RTT enabled within the TLS configuration, you may lose most of the performance boost that motivated you to implement in the first place.

Is it time to enable TLS 1.3?

The decision to implement TLS 1.3 at this point will depend on your requirements and motivations. There are mainstream browsers that do not support 1.3, and those that do support it currently have it disabled by default. Additionally, if you take out potentially vulnerable features like renegotiation and use PFS for your applications’ TLS 1.2 configuration, you get all the same security and privacy benefits as TLS 1.3. As far as a potential performance boost, you should perform thorough testing to see if this is true for your application as it may not be worth the effort with 0-RTT disabled.

Whatever your decision, it doesn’t mean that previous versions of TLS are going away anytime soon. Google has just recently announced that they will deprecate TLS 1.0 and 1.1 by 2020, so TLS 1.2 will continue to be around for quite a while. And with the exception of some point-to-point API connections, you will need to continue support for TLS 1.2 (and possibly 1.0 and 1.1) for some time to ensure you do not break users’ connections to your applications.

POLICY-BASED TRAFFIC STEERING

By orchestrating your SSL/TLS traffic, you can maximize the efficiency of your security solutions while optimizing the performance of critical applications.



Don't be blind to encrypted threats

Regardless of your TLS version, you need to have visibility into encrypted threats to protect your business. SSL/TLS based-decryption devices that allow for packet inspection can help you regain visibility into your traffic. These devices intercept encrypted traffic, decode, inspect, and re-encrypt untrusted TLS traffic entering or leaving the network. This provides visibility into malicious traffic, but that's not quite enough.

SSL/TLS BASED-DECRYPTION DEVICES THAT ALLOW FOR PACKET INSPECTION CAN INTERCEPT ENCRYPTED TRAFFIC, DECODE, INSPECT, AND RE-ENCRYPT UNTRUSTED TLS TRAFFIC ENTERING OR LEAVING THE NETWORK—BUT THAT'S NOT QUITE ENOUGH.

Security teams and network operations have found that setting up decryption zones is not easy. They often have to resort to manual daisy-chaining or tedious configuration to manage decryption/encryption across the entire security stack. And then they find that exceptions abound.

F5 **SSL Orchestrator** delivers visibility but differentiates itself from the pack with orchestration, which provides policy-based traffic steering to a service chain based on risk and dynamic network conditions. Because it functions as a full proxy for both SSL/TLS and HTTP, SSL Orchestrator can make intelligent decisions to steer inbound and outbound traffic to service chains within the security stack.

No matter how complicated your inbound and outbound encryption requirements are, SSL Orchestrator can bring visibility back to your inspection solutions, which helps keep your network—and your apps—more secure.

Learn more at
f5.com/security.

