Overcome the Challenges of SSL Everywhere

KEY BENEFITS

Improve SSL processing performance

Strengthen security by gaining visibility into SSL traffic

Deploy forward secrecy without creating blind spots

Maximize existing security investments

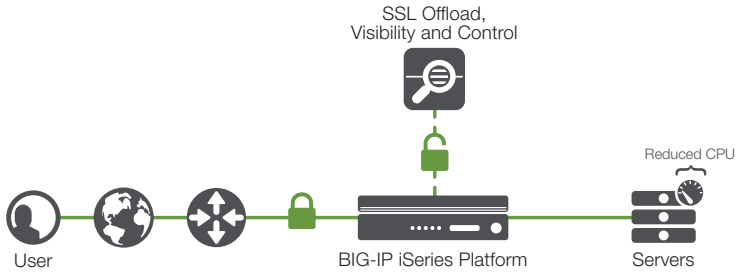
As network attacks become more frequent and costly, enterprises have begun to enforce a policy of encrypting all traffic at all times. Known as SSL Everywhere, this approach introduces its own risks and costs, including decreased performance, security blind spots, and SSL certificate management. The new F5® BIG-IP® iSeries delivers hardware-accelerated SSL decryption and re-encryption and central certificate management to overcome the risks imposed by widespread SSL adoption.

Challenge

Cryptographic processing is far more complex than processing unencrypted traffic, and both the client and the server shoulder the burdens of encrypting and decrypting bidirectional traffic. As a result, SSL Everywhere can significantly degrade the user experience. In addition, crypto processing in software on a general-purpose CPU may lead to unpredictable performance due to the processing load of the CPU at that moment in time.

The purpose of encryption is to conceal information traversing two endpoints, but concealing traffic cuts both ways. While ensuring that malicious parties cannot see the information, SSL Everywhere eliminates organizational visibility into the traffic, hindering security inspections. Standard security processes and appliances become blind to the encrypted traffic, an unfortunate side effect known as the SSL blind spot.

In particular, SSL encryption methodologies continue to evolve, with forward secrecy ciphers, specifically the Elliptical Curve Diffie-Hellman Ephemeral (ECDHE) cipher, quickly becoming the standard. Traditional RSA ciphers enabled anyone with the private key to read all traffic, which meant that an administrator could copy the private key to a supporting security appliance to enable SSL monitoring. Unfortunately, if that private key became exposed through poor design, human error, or implementation bugs, all traffic ever encrypted with that key, including previously recorded traffic, could be decrypted. While ECDHE forward secrecy offers better protection against future traffic decryption, to eliminate the SSL blind spot the network architecture must include an SSL proxy that decrypts all SSL traffic for inspection by security devices.



Traffic inspection via SSL proxy

SSL Everywhere also adds an administrative burden in the form of certificate management. All certificates must be cataloged, maintained, and regularly renewed, as well as updated to address any compromised certificates. With most enterprises managing 500 or more applications, certificate management and related server configuration can be time-consuming and costly.

Solution

Software solutions to the SSL blind spot aren't practical. For organizations using forward secrecy, hardware accelerated decryption and encryption is required to deliver the processing capacity and speed needed to avoid performance degradation. The new BIG-IP iSeries provides the high performance and predictable speed necessary as firms drive toward SSL Everywhere. BIG-IP iSeries hardware, positioned at a strategic control point in the network, can decrypt all SSL traffic for inspection by the organization's existing security solutions and then re-encrypt that traffic without consuming CPU resources or incurring the latency of software decryption. In addition, this solution enables the organization to maximize the return on its existing security infrastructure, including intrusion prevention systems (IPS), sandbox systems, or next-generation firewalls. The BIG-IP platform provides visibility into inbound and outbound traffic so that existing security appliances can do what they were designed to do, without blind spots. Unencrypted traffic can then flow to application servers or, for maximum security, be re-encrypted by the BIG-IP appliance first.

Beyond hardware acceleration, the BIG-IP iSeries provides centralized SSL certificate and private key management, and streamlined configuration for SSL Labs A+ grade SSL rating.

SSL Everywhere and forward secrecy penalize application performance, introduce blind spots that impede traffic inspection, and make certificate management difficult to scale. The BIG-IP iSeries overcomes these challenges while improving performance by creating an inspection zone where all security appliances can inspect unencrypted network traffic at maximum speed. This comprehensive solution eliminates encryption blind spots, improves performance across a range of ciphers, simplifies SSL management, and maximizes existing security investments.

Learn more about addressing the challenges of SSL Everywhere at f5.com/products/big-ip.