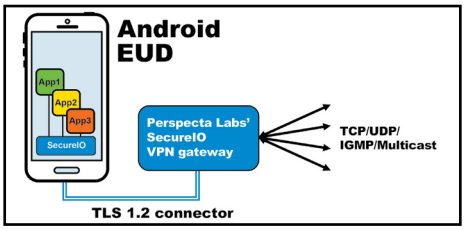
perspecta LABS

SecureIO

Accelerate fielding of CSfC Android end-user device apps by offloading TLS encryption functionality



The challenge

The National Security Agency's Mobile Access Capability Package (MACP) requirements stipulate that each Commercial Solutions for Classified (CSfC) app implementing Transport Layer Security (TLS) must be individually tested and approved by the National Information Assurance Partnership (NIAP). Since Android CSfC end-user devices (EUDs) typically use TLS-encrypted app traffic inside an IPSec tunnel, each Android CSfC app that uses TLS is subject to NIAP testing and NSA review. NIAP certification can be a long and expensive process, representing a high barrier to entry for new Android CSfC apps, especially government off-the-shelf apps. The time required to approve, test and field TLS apps for CSfC-compliant Android devices needs to be dramatically reduced in order to help ensure that warfighters have the best technology in their hands as soon as possible.

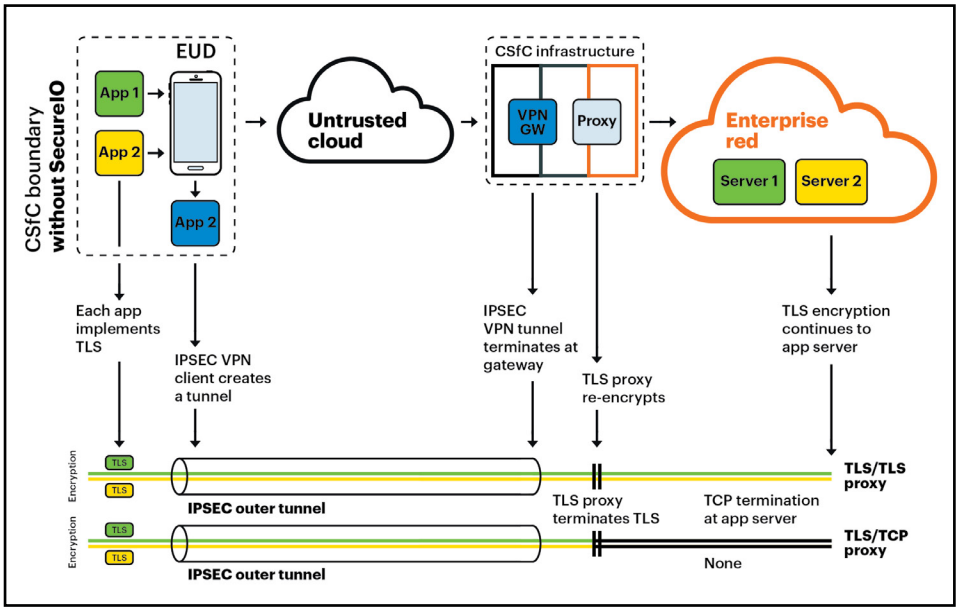
The solution

The Perspecta Labs SecureIO suite provides a NIAP-approved common, shared TLS encryption function that can be used by every TLS app running on Android CSfC EUDs. The SecureIO Android services eliminate the need for CSfC apps to implement their own transport security, enabling a wide variety of new apps to be quickly deployed on MACP-compliant Android EUDs. Since the SecureIO suite is separate from upper layers, new upper layers can be added or existing upper layers can be modified without requiring SecureIO suite modification or re-approval. An application programming interface for applications makes integration straightforward and painless.

perspecta LABS

SecureIO features – Android components

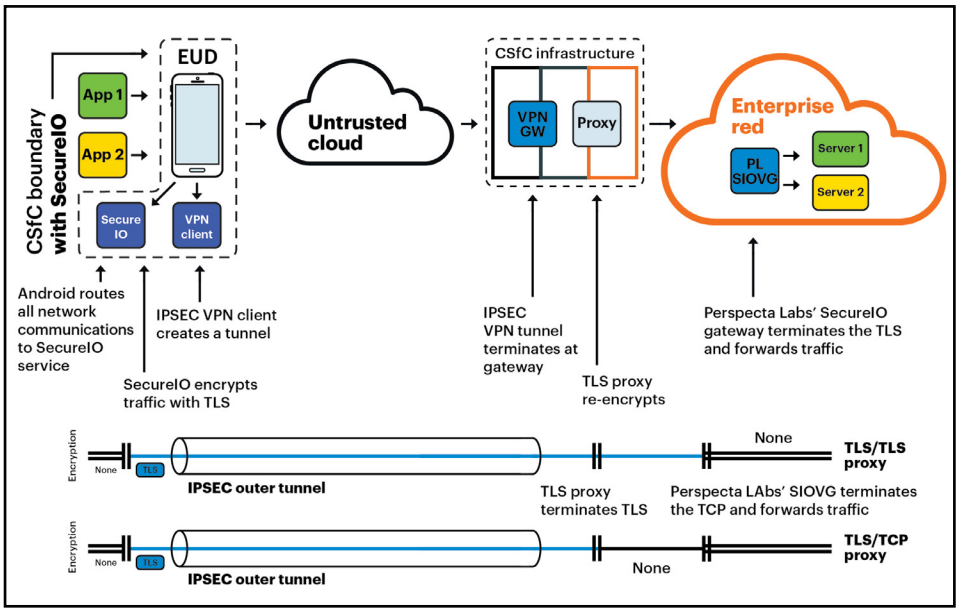
- Standard Android software, compliant with VPN framework
- Implements Android VPN API
- Implements KNOX Extensions
- Exposes a standard TUN interface when configured as a VPN
- Offers UDP, TCP, IGMP and Multicast interfaces
- Imports certificates from Android Key Chain and grants access
- Creates TLS or Websocket+TLS profiles
- Manages cipher suites
- Performs SAN/SNI checks using TLS server hostname
- Performs certificate validation, OCSP, and CRL checking
- Provides a statistics manager
- Monitors activity
- Runs as a service, auto-started by upper layer
- Requires no user interaction



Without SecureIO: Apps are within the CSfC boundary. Each app must implement TLS and be tested and approved for NIAP compliance

SecureIO VPN Gateway (SIOVG) features

- Provides the anchor point for secure services
- Allows Android connection termination in TCP, or TLS, or Websocket
- Provides IP Forwarding Services for UDP, TCP, Multicast and IGMP
- Provides a DHCP pool, route setting and ARP Proxy for Android TLV TUN
- Uses 4.15.12 custom kernel on CentOS 7.4.1708 (Core) with upgrades for 32768 tunnel interfaces (instead of 32)
- Can reside on a VM (on a Type-1 cluster)



With SecureIO: Apps are outside the CSfC boundary and communicate locally with SecureIO, which encrypts all communications with TLS

perspectalabs.com | info@perspectalabs.com
150 Mount Airy Road
Basking Ridge, NJ 07920