Secure CryptoTunnel

Generalidades

7 Layers International (7L) es una empresa independiente, de propiedad privada, registrada en el ReinoUnido, dedicada al diseño, desarrollo y producción de soluciones de alto nivel en Tecnolog´as deInformación y Comunicación. 7L también presta servicios de consultor´a y apoyo para la implementaciónde infraestructuras completas, incluidas infraestructuras de nube privadas. 7L ha estado suministrando soluciones a clientes en varios pa´ses del mundo. Todas las soluciones de seguridad de 7L se basan enSecure CryptoTunnel (SCT), una arquitectura de seguridad única basada en tecnolog´a de punta, queproporciona un nivel muy alto de seguridad, integridad y disponibilidad, cumpliendo con las últimas normasinternacionales y salvaguardando toda la información transmitida durante la comunicación y elalmacenamiento. SCT se desarrolla enteramente por 7L en la Unión Europea. Consiste en una serie demódulos interconectados que proporcionan conjuntamente una valla de seguridad alrededor de toda lainformación sensible transmitida y almacenada. Sus componentes incluyen los siguientes módulos:

- Claves de cifrado generadas por herramientas de generación de claves verdaderamente aleatorias, almacenadas en módulos de seguridad de hardware (HSM)
- Diseño de hardware basado en Linux
- Algoritmo de cifrado de clave simétrica AES256-bit
- Control total del cliente de los procedimientos administrativos

Los clientes incluyen organizaciones gubernamentales e internacionales, as´ como una gama de organizaciones no gubernamentales, instituciones financieras, de transporte, de hospitalidad y empresas industriales.

RESUMEN

7L SCT proporciona una solución segura que satisface la creciente necesidad de privacidad y confidencialidad dentro de las comunicaciones móviles gubernamentales y militares. 7L SCT está garantizado para la confidencialidad y la privacidad.

Entregamos una solución móvil con encriptación de extremo a extremo y en tiempo real de todas las comunicaciones de voz, chat, SMS, correo electrónico, fotos y archivos de datos utilizando criptograf´a de curva el´ptica de confianza encima de un sistema operativo endurecido y funcionando con una alta calidad (smartphone, tableta o portátil) con modernas funciones de seguridad de hardware .

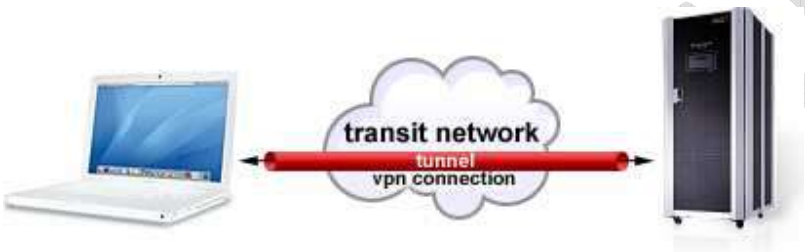
7L SCT ha sido construido pensando en la seguridad y utiliza la última tecnolog´a. La seguridad de 7L gira en torno a cuatro bloques de construcción básicos:

1) Dispositivo móvil seguro
2) Sistema operativo endurecido: Fácil de usar Android - ROM personalizada (y / o Win / iOS para Tablets, Notebooks) sin acceso a la tienda de aplicaciones.
3) Criptograf´a avanzada: criptograf´a AES256
4) Control de clientes: Infraestructura instalada en los equipos del cliente (opción alojada)

7L SCT y su infraestructura es llave en mano, con todos los componentes de software entregados, instalados, aprovisionados y mantenidos junto con el apoyo del administrador y del usuario final.
El hardware puede ser suministrado por el cliente o entregado por 7L (opcional)

1 7L CryptoTunnel

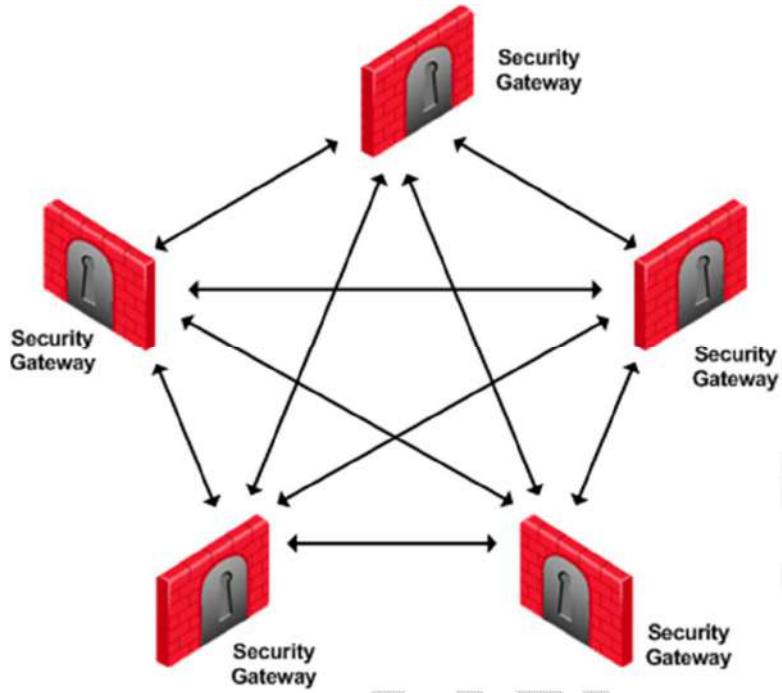
El 7L CryptoTunnel crea túneles de red altamente seguros a través de Internet o cualquier otra red privada (red de tránsito). Utilizando este tipo de túnel, cualquier tipo de transmisión puede serseguro, protegiéndolo de cualquier tipo de intentos de robar la información transmitida.



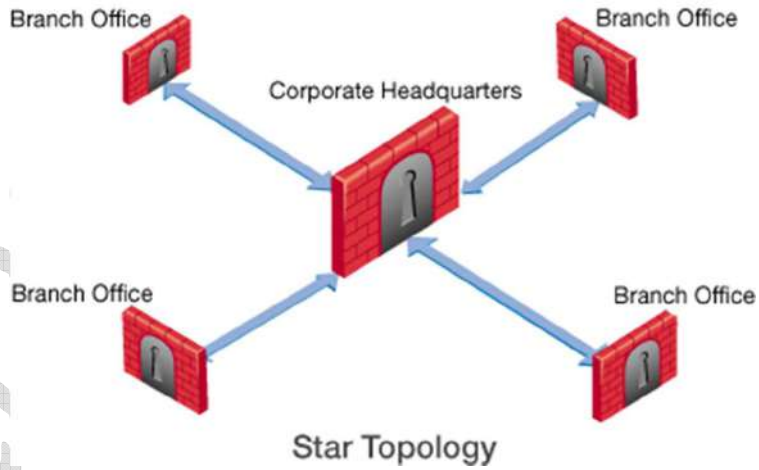
1.1 CryptoTunnel Modos

1.1.1 Crypto Tunnel Sitio a Sitio

En este modo, se pueden conectar 2 o más sitios remotos a través de múltiples CryptoTunnels de 7L en cualquier parte del mundo. Cada 7L CryptoTunnel puede ser independiente y operar aislado de los otros túneles de la red del cliente, como se muestra en la imagen siguiente:



También se pueden conectar múltiples sitios a través del sitio principal (sede), como se muestra en el siguiente diagrama:



1.1.2 Dispositivo a dispositivo / sitio CryptoTunnel

El 7L CryptoTunnel soporta la conectividad de dispositivos bajo múltiples plataformas. Actualmente, son compatibles las siguientes plataformas:

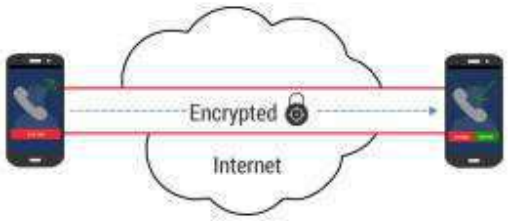
Microsoft Windows hasta la versión de Windows 10

- Desktops
- Laptops
- Tablets

Android
Smartphones y Tablets

Smartphones y Tablets de Apple (iPhone / iPad)

Cualesquiera Dos (2) o más dispositivos conectados a 7L CryptoTunnel, por ejemplo, en la Sede del Cliente será capaz de comunicarse con seguridad entre s´.



Los siguientes tipos de comunicaciones se pueden realizar de forma segura:
-Enviar y recibir correos electrónicos de forma segura
-Enviar y recibir mensajes instantáneos de forma segura
-Realizar y recibir llamadas de forma segura

1.2 7L CryptoTunnel Seguridad

La seguridad del CryptoTunnel 7L está garantizada en múltiples niveles, utilizando el Securosys Primus X-Series o HSM (Hardware Security Module) para lo siguiente:
-Generación de claves
-Especificación de cifrado
-Código fuente

Debido a su arquitectura dinámica, nuestro cifrado está preparado para ordenadores cuánticos. Si los ordenadores cuánticos hacen que cualquiera de los algoritmos soportados se vuelvan obsoletos, entonces se puede instalar un algoritmo que sea seguro para ordenadores cuánticos. Toda la información, incluida la comunicación de voz realizada a través del 7L CryptoTunnel, se digitaliza y encripta en tiempo real antes de ser transmitida. Escuchar en cualquier parte de la cadena de comunicación de la red no dará ninguna información útil. Como resultado, el 7L CryptoTunnel es infdiferente en cuanto a qué conectividad o red se utiliza para la transmisión, 3G / 4G, Wi-Fi o cable Puesto que todas las comunicaciones de datos están cifradas antes de la transmisión, el método de transmisión no afecta la seguridad de la comunicación. Para Smartphones, sólo se recomienda una conexión 3G / 4G para mayor seguridad. La solución de 7L CryptoTunnel Smartphone es completa, incluyendo un sistema operativo, software, algoritmo y servidor endurecidos con hardware y software relevantes. Para mayor seguridad, el Smartphone está cargado con un firewall "codificado", bloqueando cualquier comunicación que no esté relacionada con el Smartphone y el Servidor.

Constituye una atmósfera segura que permite al cliente encriptar todo tipo de comunicaciones de datos. El cliente tiene el control total de la infraestructura y la arquitectura del sistema y del servidor.

1.2.1 Generar Claves

Las claves de cifrado son una parte fundamental de la seguridad de la solución. Un módulo de seguridad de hardware diseñado espec´ficamente para la generación de claves, la administración de claves y la protección de claves se utiliza en una caja f´sicamente separada, reforzada y resistente a manipulaciones y en un almacén de claves inviolable. Las claves de encriptación de entrop´a alta se generan en módulos de hardware separados de generación de números aleatorios (TRNG).

1.2.2 Especificaciones de Cifrado

La encriptación se ejecuta sólo en AES de 256 bits y las claves no son estáticas, por lo cual se están rotando lo que hace imposible descifrar la comunicación. El intercambio de claves se realiza con Diffie-Hellman habilitado, proporcionando secreto hacia adelante por el uso de la criptograf´a de curva el´ptica.

- Arquitectura de seguridad de grado militar
- Encriptacion / Autenticacion
    - 128/192/256 bit AES (GCM, CTR, ECB, CBC, MAC modes)
    - 128, 192 and 256-bit Camellia (GCM, CTR, ECB, CBC, MAC modes)
    - RSA 2048 - 8192 with PKCS, PSS and OEAP modes
    - ECDSA 256 (mod-p curves, etc.), DSA 2048 - 4096
    - ECDH 256, DH 2048 - 4096
    - SHA-2, SHA-3 (224 - 512)
    - oActualizable a los algoritmos de seguridad informatica cuantica
- Generacion de Claves
    - o Dos generadores de verdaderos numeros aleatorios de hardware de entrop a
- Gestion de claves
    - Capacidad de la llave: mas de 1'000'000 llaves de 2048 bits
    - Boveda ultra segura para claves y certificados a largo plazo
- Multi-Cliente - Usuario - Capacidad de particion
    - Mas de 100 particiones
- Mecanismos anti-manipulacion
    - Varios sensores para detectar accesos no autorizados
    - Habilitado para destruir todo el material clave y datos sensibles
    - Transporte y proteccion contra manipulaciones durante varios anos
- Firmware
    - Actualizacion de firmware de manera local y / o remota
- Funciones de seguridad
    - Multiples oficiales de seguridad (n de m)
    - oIdentificacion basada en tarjeta inteligente y PIN

1.2.3 Infraestructura

Sitio a Sitio CryptoTunnel

7L SCT requiere una infraestructura que se compone de un "Gateway de seguridad" en cada sitio interconectado. Este "Security Gateway" está compuesto por un "Servidor VPN", un "Servidor de Aplicaciones" y un "Firewall". El Nodo Central también incluirá un Módulo de Seguridad del Hardware (HSM) para generar y almacenar las claves criptográficas

Dispositivo a dispositivo / sitio CryptoTunnel

7L SCT requiere una infraestructura que se compone de un "Security Gateway" en un nodo central . Este "Security Gateway" está compuesto por un "Servidor VPN", un Servidor de Aplicaciones "y un" Firewall ". El nodo central también incluirá un módulo de seguridad de hardware (HSM) para generar y almacenar las claves criptográficas. Todos los dispositivos se comunican entre s´ a través del Nodo Central, a través de un túnel VPN seguro (7L SCT - Secure CryptoTunnel) que se establece entre el dispositivo y el Nodo Central

Componentes de la Infraestrucura

Las "Puertas de enlace de seguridad" son las mismas para ambos modos CryptoTunnel, "Sitio a sitio" y "Dispositivo a dispositivo / sitio". Los servidores se basan en Dell (o equivalente) y pueden venir en forma de dispositivos listos para usar. El firewall de red se basa en Cisco (o equivalente) y también puede venir con una configuración lista para usar que rechaza las conexiones no autorizadas y registra los intentos de ataques. Todos los componentes de hardware son opcionales y pueden ser reemplazados con diferentes componentes de acuerdo con las especificaciones y requisitos del cliente. El servidor SCT para voz y mensajer´a es el "servidor de aplicaciones" que actúa como un conmutador de voz, conectando a los usuarios. Está ejecutando nuestro software propietario SCT encima de un endurecido sistema operativo Linux. El protocolo de comunicación implementado en la solución entre el servidor SCT y los dispositivos móviles está optimizado para proporcionar un mayor rendimiento en redes de bajo ancho de banda. Para la transmisión de voz se utiliza la VPN encapsulada UDP / TCP. Utiliza codecs modernos para proporcionar una gran calidad de audio incluso en situaciones de bajo ancho de banda y está optimizado para reducir el consumo de energ´a. El servidor SCT también maneja mensajes instantáneos de texto y archivos enviados entre dispositivos móviles 7L. El servidor env´a los mensajes sin tocar el contenido del mensaje. El 7L VPN Server proporciona un túnel seguro entre todos los dispositivos en el campo y la infraestructura segura. Todo el tráfico de datos de los dispositivos pasa por el servidor 7L VPN. Los dispositivos que pueden conectarse al Nodo Central pueden ser PCs, Notebooks, Tablets o smartphones, como se mencionó anteriormente. Dependiendo de las necesidades del cliente, 7L puede recomendar una gama de dispositivos diferentes que pueden ser compatibles.

Los servidores son Dell (o equivalente) y tienen las siguientes especificaciones:

Hardware del servidor

Processor: Quad Core XEON with AES-NI 2.5GHz+

Memory: 32GB RAM

Disk: 2 x 120GB SSD for Operating System

Firewall

Memory: 4GB
SSD: 50GB mSata
IO: 8 x 1 Gigabit Ethernet
Maximum stateful-inspection throughput: 750Mbps
Maximum AVC throughput: 250 Mbps
Maximum AVC + IPS throughput: 125 Mbps

HSM

El HSM utilizado por 7L para esta tarea realiza una amplia gama de operaciones. Genera claves de cifrado, almacena estas claves y administra la distribución de estas claves. Además de la administración de claves, también realiza tareas de autenticación y cifrado. Múltiples HSM se pueden agrupar para soportar la redundancia y el equilibrio de carga. Cada HSM también se puede particionar para múltiples usuarios. Soporta algoritmos criptográficos simétricos (AES, 3DES), asimétricos (RSA, ECC, Diffie-Hellman) y hashing (SHA-2, SHA-3).

Las claves de encriptación de entrop´a alta se generan en módulos separados de generación de verdaderos números aleatorios (TRNG) basados en diferentes mecanismos de ruido f´sico. El HSM también contiene una bóveda ultra segura implementada dentro de un chip de seguridad dedicado. Debido a su arquitectura dinámica, el HSM está listo para la computación cuántica. Si las computadoras cuánticas hacen que cualquiera de los algoritmos soportados se vuelvan obsoletos, entonces se puede instalar un algoritmo de seguridad computacional cuántica a través de una actualización de firmware / software.

Smartphone Seguro

Los teléfonos inteligentes seguros funcionarán en el modo "Dispositivo a dispositivo / sitio" y requerirán la infraestructura pertinente descrita anteriormente. La solución consiste en Secure Mobile Core System (Servidor VPN, Servidor de Aplicaciones, Firewall y HSM) incluyendo los sistemas de comunicación y gestión necesarios y el Teléfono Móvil Seguro. La versión actual es compatible con los teléfonos inteligentes LG Nexus5X y Huawei Nexus 6P. Es un sistema de encriptación seguro, aplicable en todo el mundo, para proteger las comunicaciones de voz. El teléfono móvil seguro equipado con 7L SCT es un teléfono móvil con un sistema operativo endurecido basado en Android, para garantizar la máxima seguridad, combinado con la facilidad de uso. La solución permite a los gobiernos, organizaciones y empresas comunicarse globalmente a través de redes móviles e inalámbricas (WiFi es opcional) con la mayor seguridad. 7L Secure Mobile Phone viene con un sistema operativo basado en Android. Se han eliminado todos los servicios innecesarios y no seguros. Incluye arranque seguro que garantiza que sólo se ejecute el software apropiado y original. Además, el teléfono tiene otras caracter´sticas de seguridad únicas e importantes, incorporadas en su endurecido sistema operativo basado en Android.

El software 7L SCT Communication Suite ofrece voz encriptada, video, datos, chat, mensajer´a y uso compartido de archivos de extremo a extremo y en tiempo real. La gama de aplicaciones se puede personalizar de acuerdo a los requisitos, a partir de sólo voz y mensajer´a y la expansión de acuerdo a las necesidades. Utiliza el cifrado de última generación con almacenamiento seguro de claves en el teléfono móvil seguro 7L. Estas son las especificaciones técnicas del teléfono móvil seguro 7L, el teléfono móvil LG Nexus 5X (alternativa Huawei Nexus 6P):

1.2.4 Especificaciones de hardware del movil

- Qualcomm® Snapdragon™ 808 processor, 1.8 GHz hexa-core 64-bit
- Hexa-core (4x1.4 GHz Cortex-A53 & 2x1.8 GHz Cortex-A57)
- Adreno 418 3D graphics accelerator
- Operating system: Android™ v7.1.1 (Nougat)
- 5.2” HD (1080 x 1920 pixels) LCD touchscreen
- 2 GB RAM
- Memory: 16/32 GB

1.2.5 Imagen y Video

- Principal: 12.3 MP, f/2.0, 26mm, laser autofocus, dual-LED (dual tone) flash h
- Secundaria: 5 MP, f/2.0, 1/4" sensor size, 1.4 µm pixel size, HDR
- Video: 2160p@30fps, 1080p@30fps, 720p@120fps, HDR

1.2.6 Audio

- Altavoces de Alto rendimiento
- Microfono: supresion de ruido con microfono dedicado
- Auriculares y microfono
- 3.5mm el conector

1.2.7 Posicionamiento (opcional)

- A-GPS
- GLONAS

1.2.8 Interfaces

- v2.0, Type-C 1.0 reversible connector

1.2.9 Conectividada Inalámbrica

- 4G Bands: LTE band 1(2100), 2(1900), 3(1800), 4(1700/2100), 5(850), 7(2600), 8(900), 9(1800), 17(700), 18(800), 19(800), 20(800), 26(850), 28(700), 38(2600), 40(2300), 41(2500) - Global model
- 3G Bands: HSDPA 800 / 850 / 900 / 1700(AWS) / 1800 / 1900 / 2100 - Global model
- GPRS/EDGE: Class 12
- HSPA 42.2/5.76 Mbps, LTE-A Cat6 300/50 Mbpsy
- Wi-Fi: 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, DLNA, hotspot (optional)
- Bluetooth v4.2, A2DP (optional)

- NFC (optional)

1.2.10 Mecanica

- Tamaño 147 x 72.6 x 7.9 mm
- Peso 136 g
- Proteccion de Pantalla: Corning Gorilla Glass 3, oleophobic coating
- Sensores: Fingerprint (rear-mounted), accelerometer, gyro, proximity, compass, barometer

1.2.11 Bater a y Rendimiento

- Battery Life 60h
- Non-removable Li-Po 2700 mAh battery

Sistema operativo endurecido

El sistema operativo Android tiene una serie de funciones de seguridad obligatorias y opcionales que un fabricante de teléfonos inteligentes puede habilitar para proteger su producto. 7L activa todas las funciones de seguridad opcionales y las incrementa con seguridad adicional utilizando AOSP, para limitar el daño que podr´a causar el código malicioso y los atacantes. Muchas de las caracter´sticas respaldadas por hardware de 7L protegen contra actos malintencionados que normalmente no están protegidos contra otros smartphones con Android. Full Disk Encryption en la capa del sistema de archivos, cubriendo todos los datos (AES-256-XTS) y metadatos (AES-256-CBC + CTS). La clave de cifrado es generada aleatoriamente por el HSM y luego cifrada con una clave de cifrado clave. Arranque completamente verificado, que cubre todas las particiones del firmware y del sistema operativo. Las particiones no verificadas que contienen datos de usuario se borran mediante un restablecimiento de fábrica. Aislamiento de la aplicación de l´nea de base a través de pares uid / gid únicos para cada aplicación.