Cómo hacer llamadas de Voz y Chat que no puedan grabarse.

MTIA Guillermo Canchola; Solution Architect Latin America

ShoreTel
Brilliantly simple™

Agenda

Notas Curiosas

- Algunos casos recordados por la historia
- En México

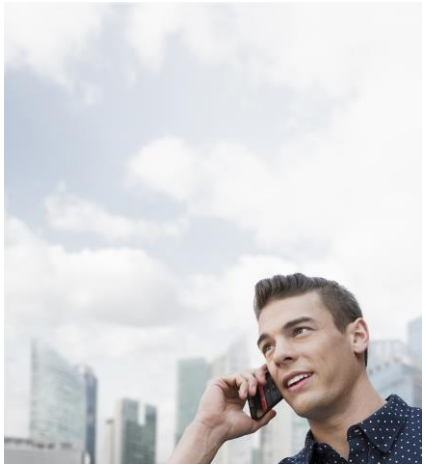
El origen del problema

La solución:

- Autenticación
- Encripción
- Encapsulación

Seguridad vs Privacidad

Preguntas

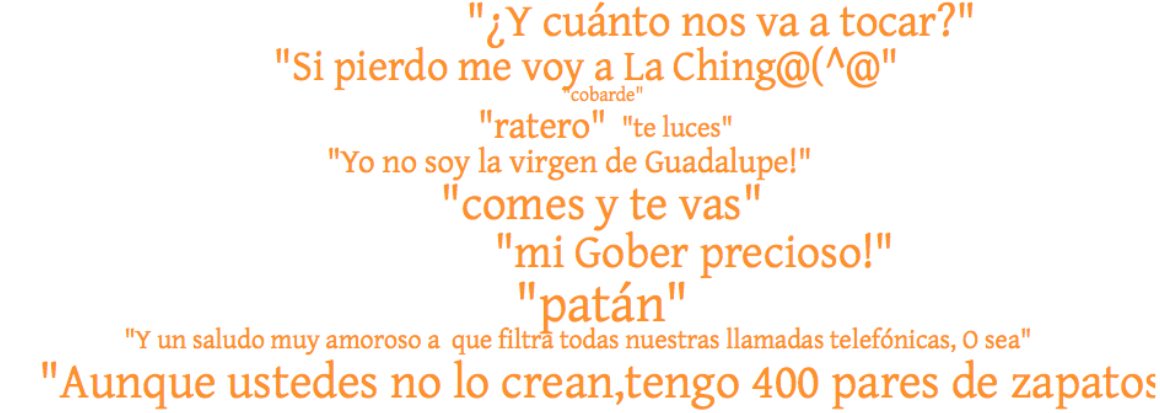


Algunas notas curiosas

Algunos casos recordados por la historia

- Edward Snowden hace publicos los programas de vigilancia masiva de la NSA (Agencia de seguridad Nacional). Junio de 2013
- Voicemail de Donald Trump ’hackeado’ por Anonymous.- 31 de Marzo, 2016.
- Conversación entre Dilma Rousseff y Lula da Silva .- 16 de Marzo, 2016.
- Mensajes entre Kate del Castillo y Joaquín Guzmán .- 12 de Enero 2016
- Whatsapp prohibido en Brasil por 24 horas.-17 diciembre 2015
- Whatsapp libera encripción mundial.- 5 Abril 2016

En México

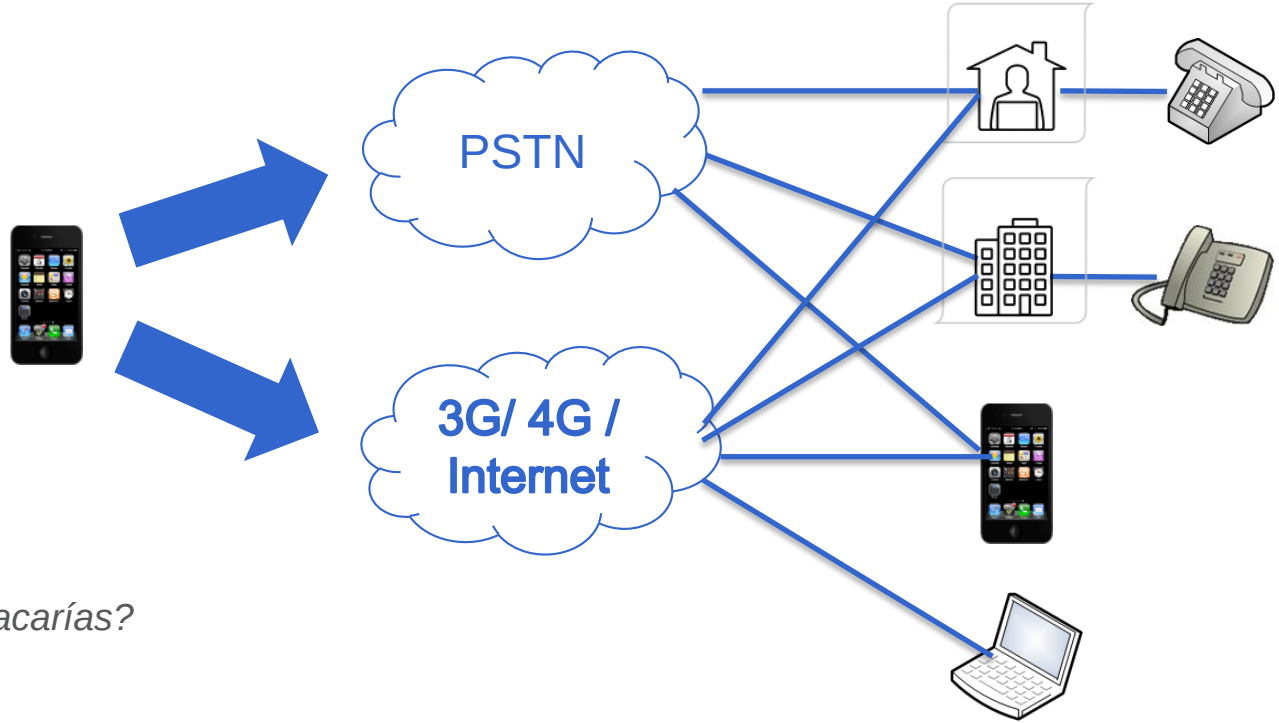


El delito de intervención de comunicaciones privadas está previsto y sancionado en el artículo 177 del Código Penal Federal: “A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones **de 6 a 12 años de prisión y de 300 a 600 días de multa”.**

De acuerdo a la ley, **sólo el CISEN y la PGR** pueden realizar intervenciones telefónicas mediante un permiso otorgado por un juez. Para ello **tienen que argumentar que se trata de casos de seguridad nacional o de investigaciones relacionadas con la delincuencia organizada.**

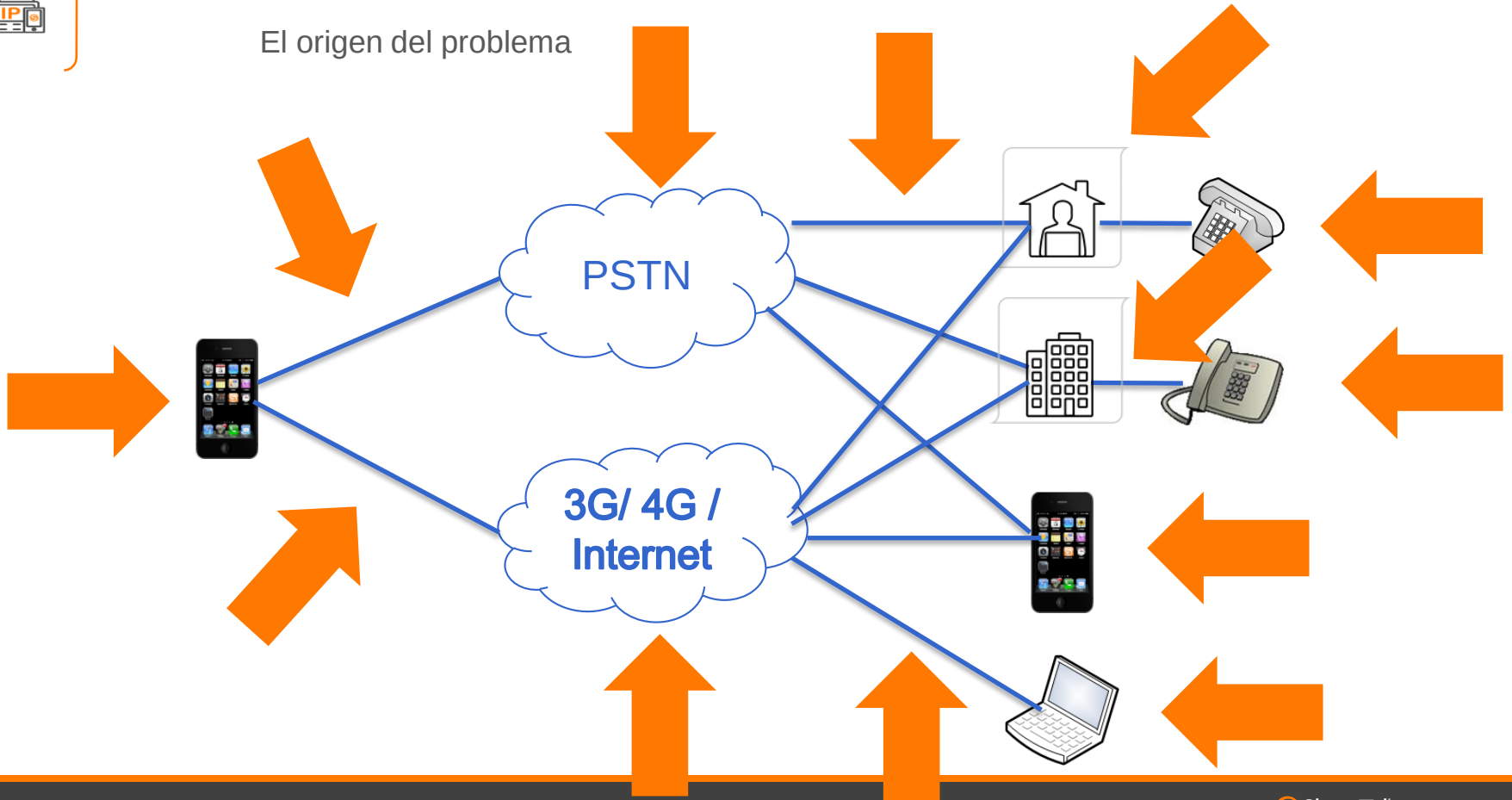
El Origen del problema

El origen del problema



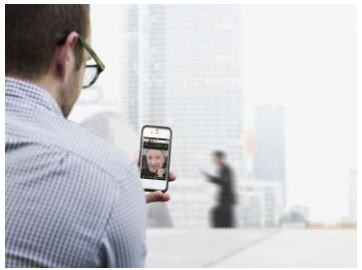
En dónde atacarías?

El origen del problema



Amenazas en cualquier punto involucrado en la conversación.

Dispositivo móvil	Red celular (3G/4G)	Red Publica (PSTN)	Tel. de escritorio
Pérdida o robo del dispositivo Virus, Malware, Botnet, Hoaxes, Spam, Rootkit. Suplantación de identidad o ‘spoofing’. Acceso a información confidencial, archivos, conversaciones, imágenes.	Intrusiones tipo “hombre en medio” (Man in the middle). Suplantar a la red o “IMSI Catcher”. Localización Geográfica Negación de servicio. Downgrade selectivo. Malware, Botnet, Suplantación.	Intrusiones tipo “hombre en medio” (Man in the middle). Suplantar a la red o “IMSI Catcher”. Negación de servicio. “Phreaking”.	Malware, Botnet, Rootkit. Suplantación de identidad o ‘spoofing’.



Mecanismos de seguridad

1. Autentica

2. Encripció

3. Encapsu

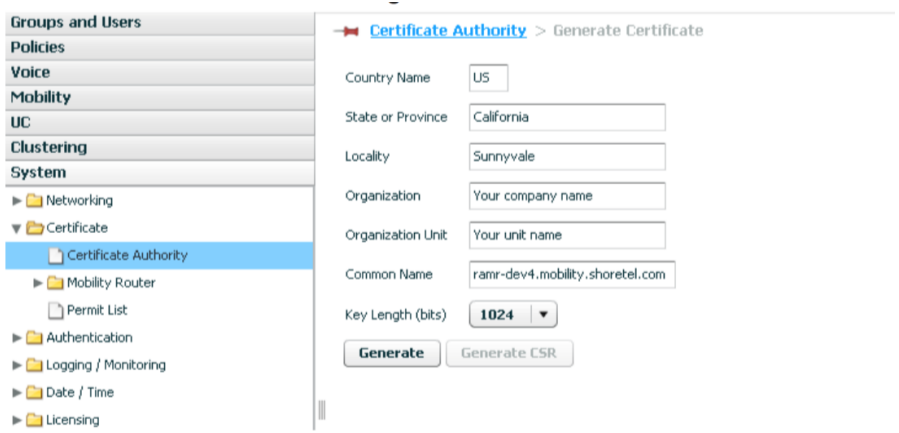
Solución de ShoreTel

ShoreTel
Brilliantly simple™

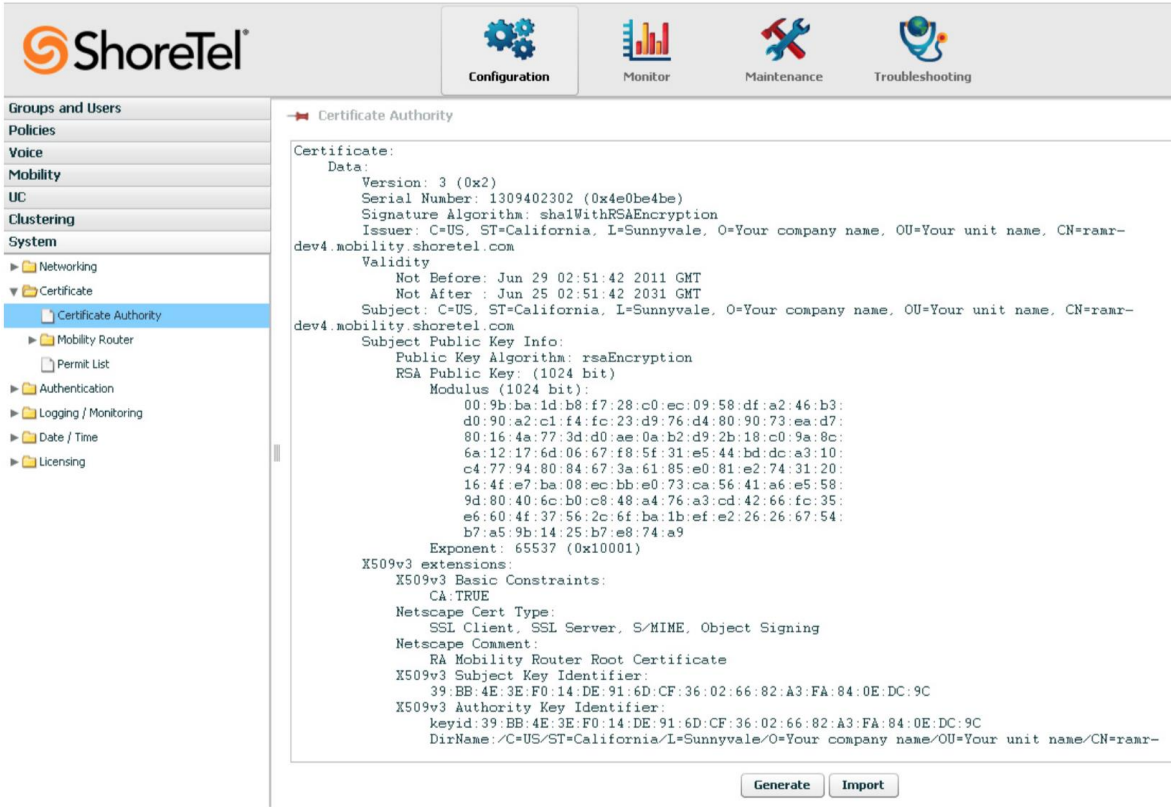
Autenticación en ShoreTel

- Corroborar la identidad de un usuario representa más mecanismos que simplemente un usuario y password, por ejemplo: certificados cliente/servidor, identificación de dispositivos y controles de acceso.
- MAAGTICSI y la Estrategia Digital Nacional obliga a las Instituciones a instrumentar servicios de TIC con autenticación de certificados.

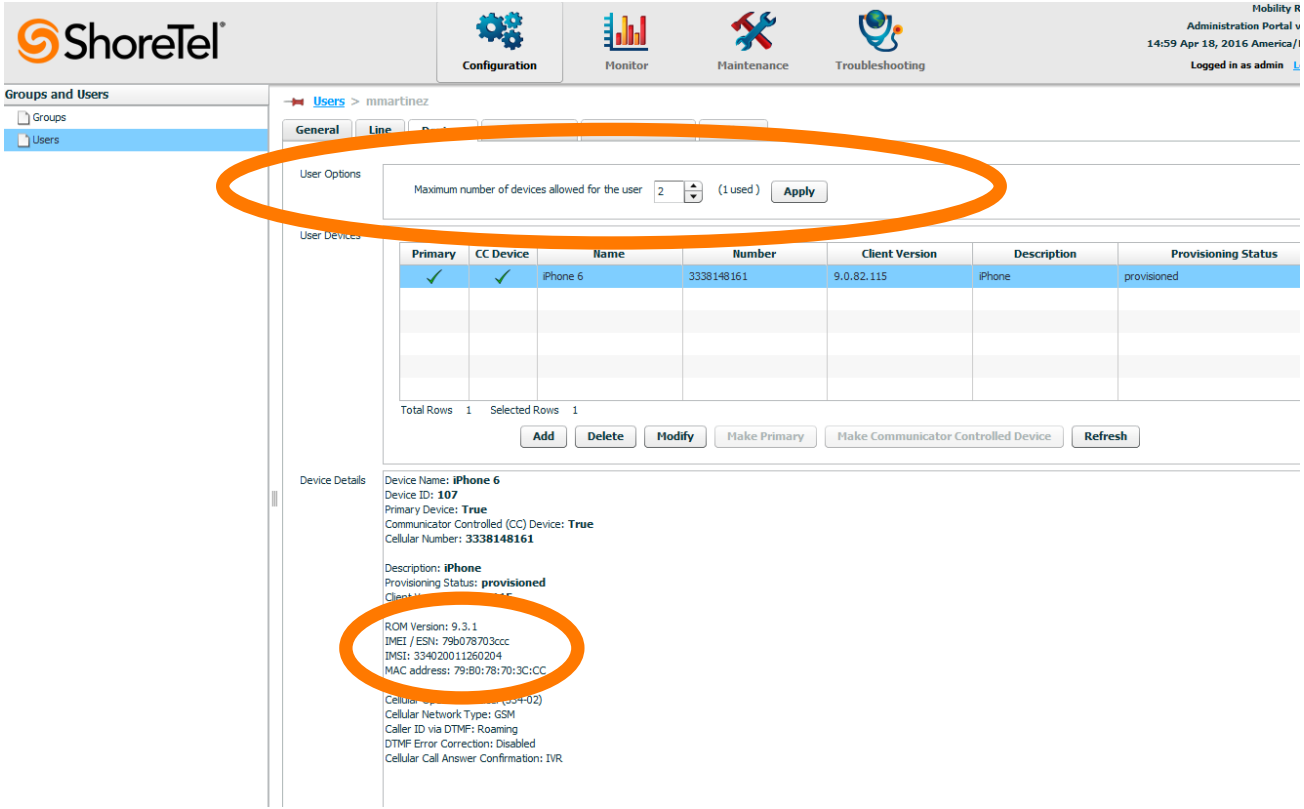
Generando un certificado en ShoreTel:



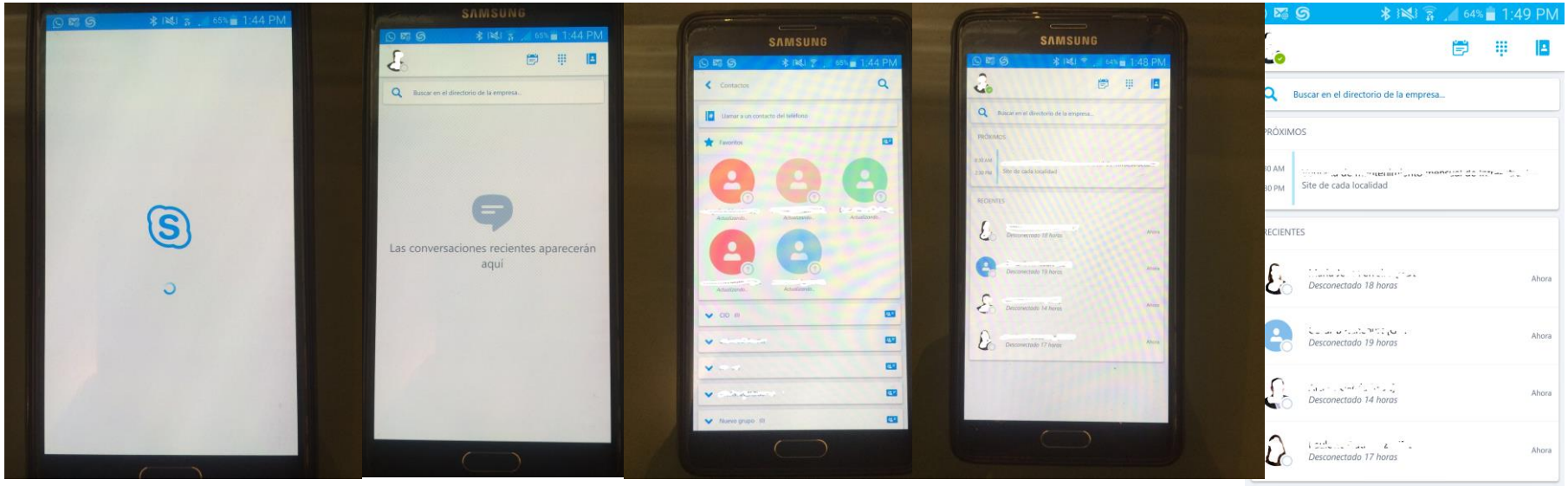
Autenticación en ShoreTel



Autenticación en ShoreTel



Una configuración mal aplicada…

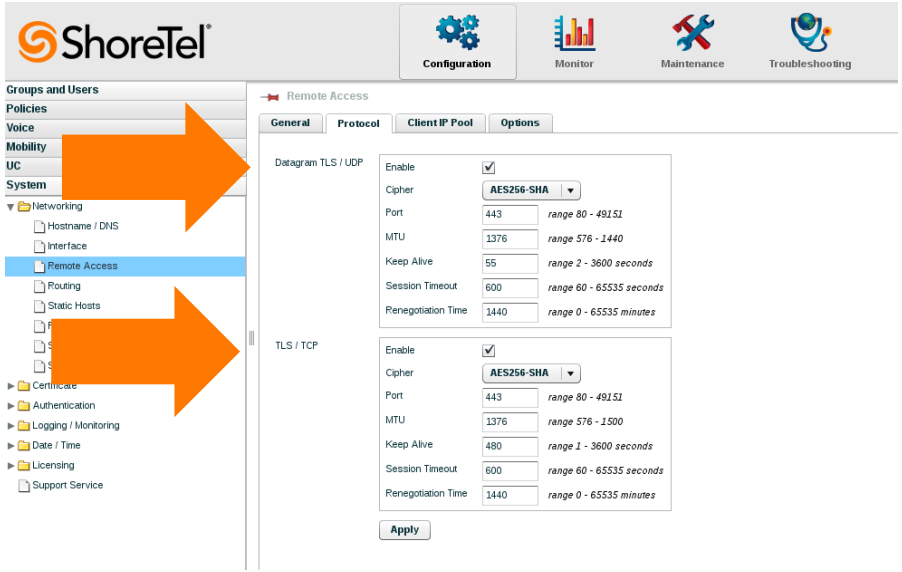


Intercambiamos nuestros usuarios / passwords?

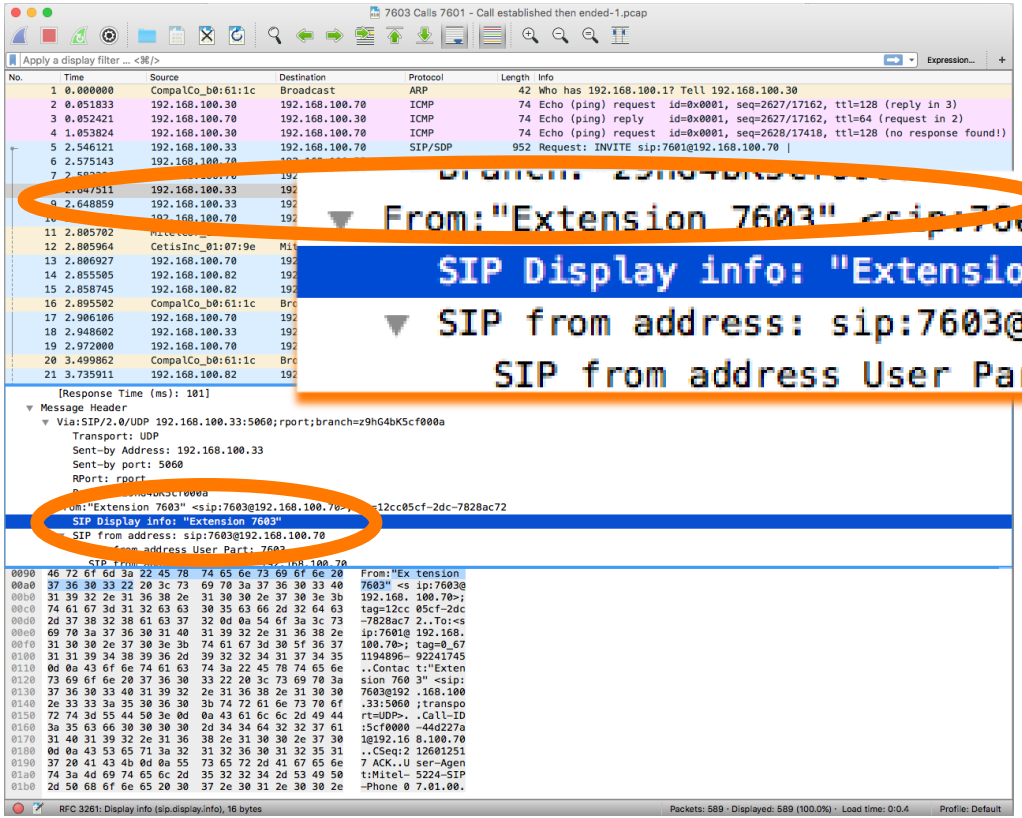
Cifrado en ShoreTel

- Existen diferencias entre cifrado de señalización y cifrado de contenido.
- MAAGTICSI y la Estrategia Digital Nacional obliga a las Instituciones a utilizar cifrado a 256 bits .

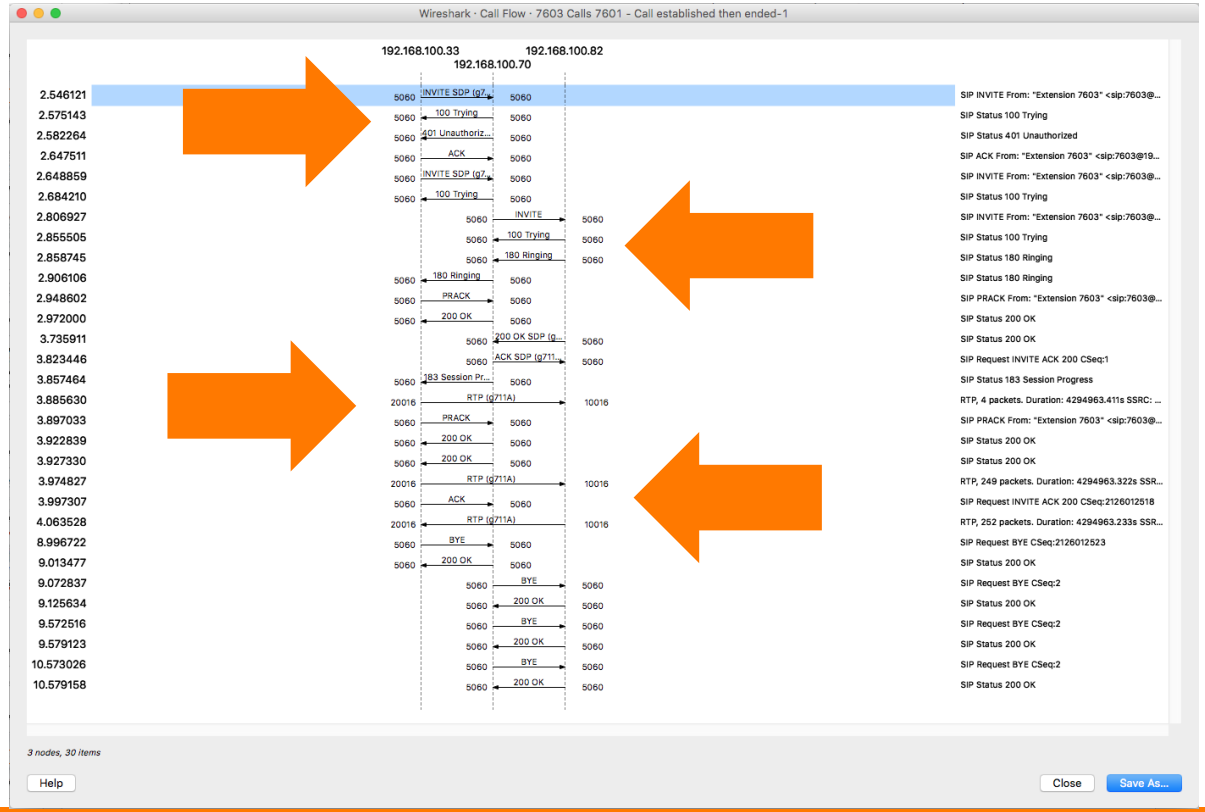
Habilitando cifrado en ShoreTel:



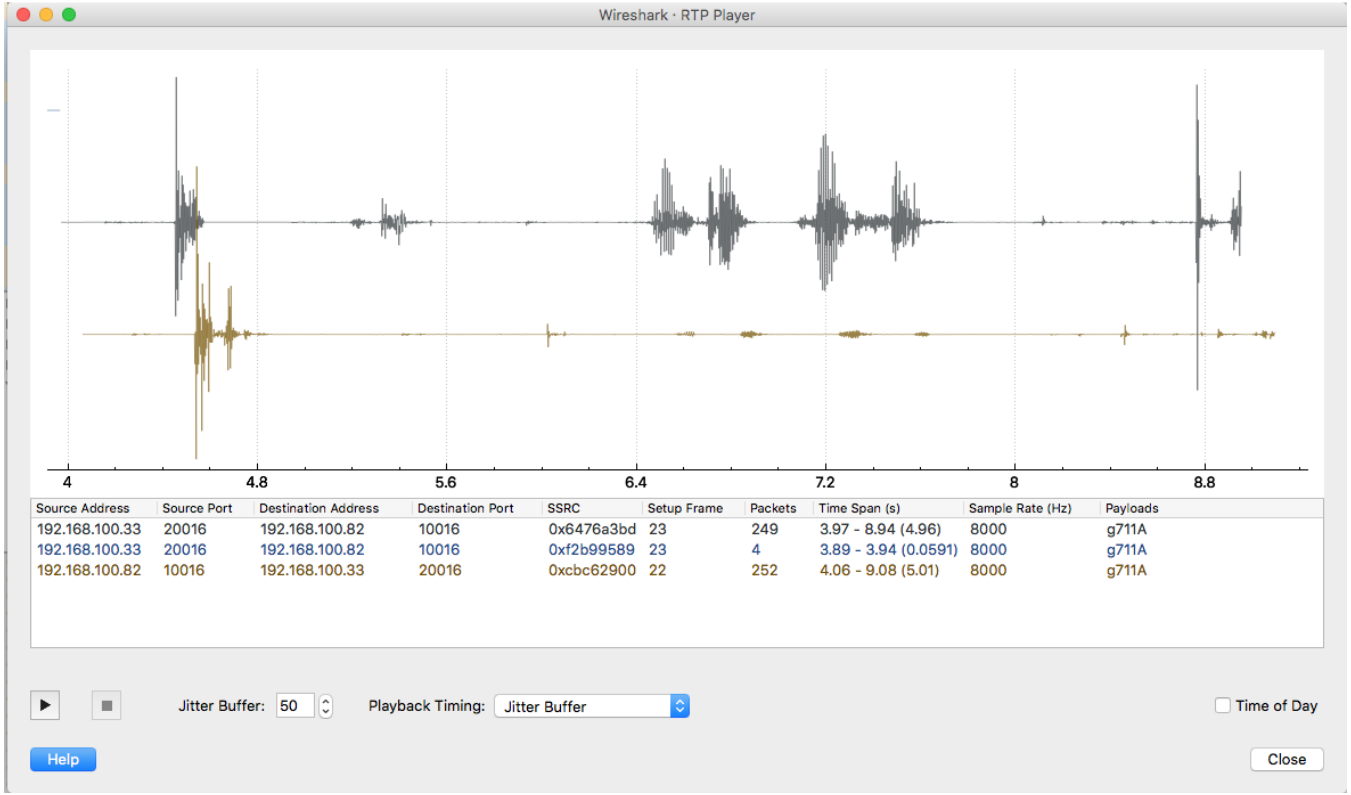
Una configuración mal aplicada…



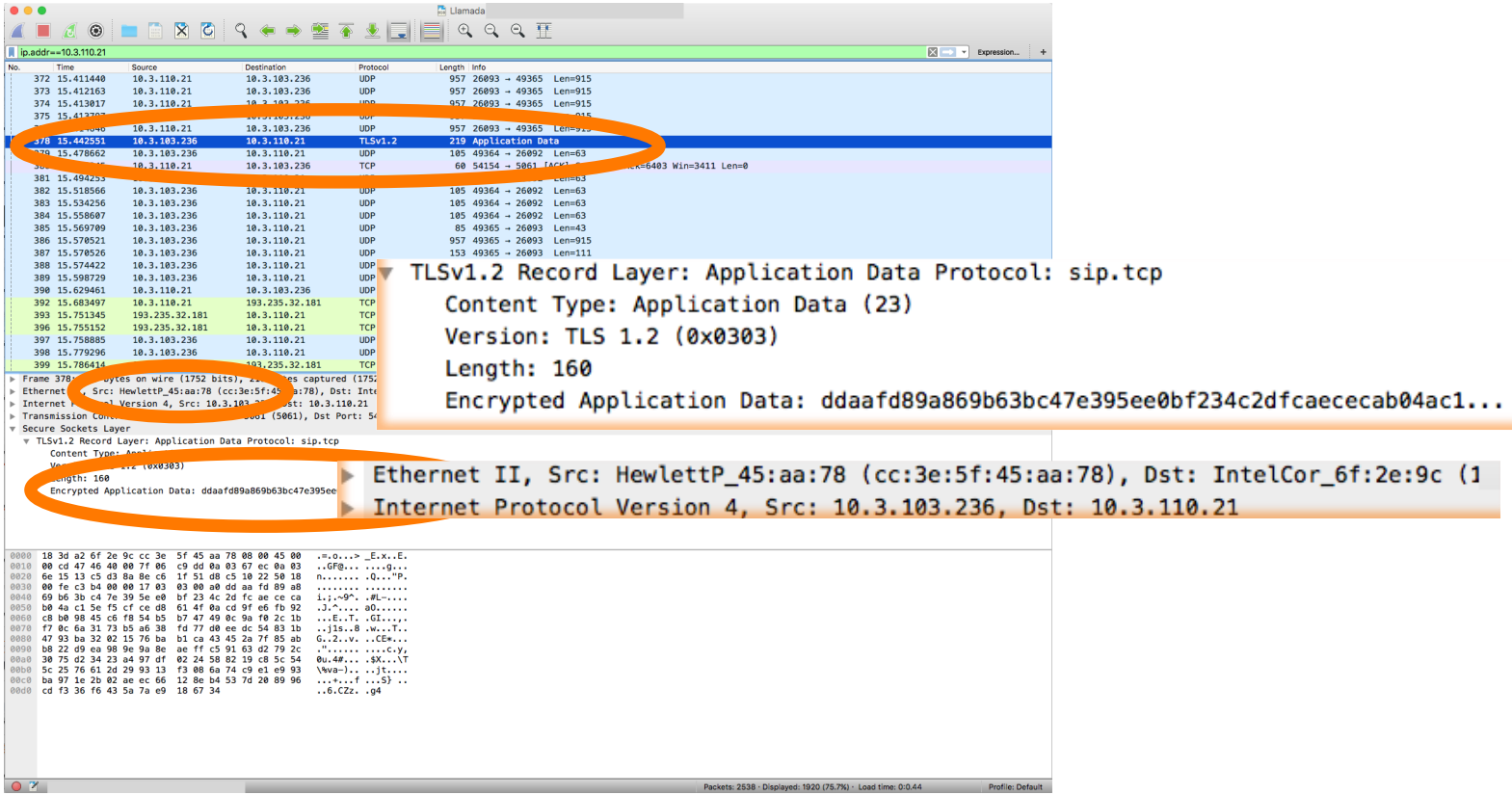
Una configuración mal aplicada…



Una configuración mal aplicada…



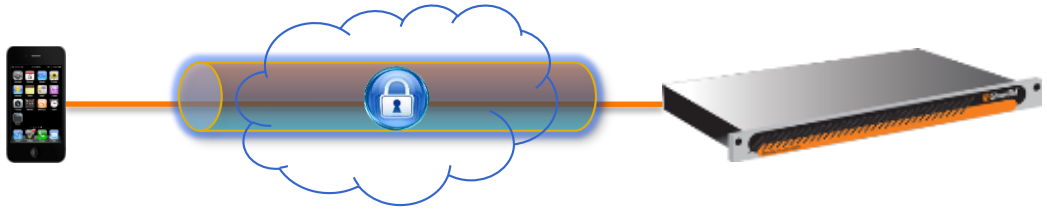
Una llamada encriptada



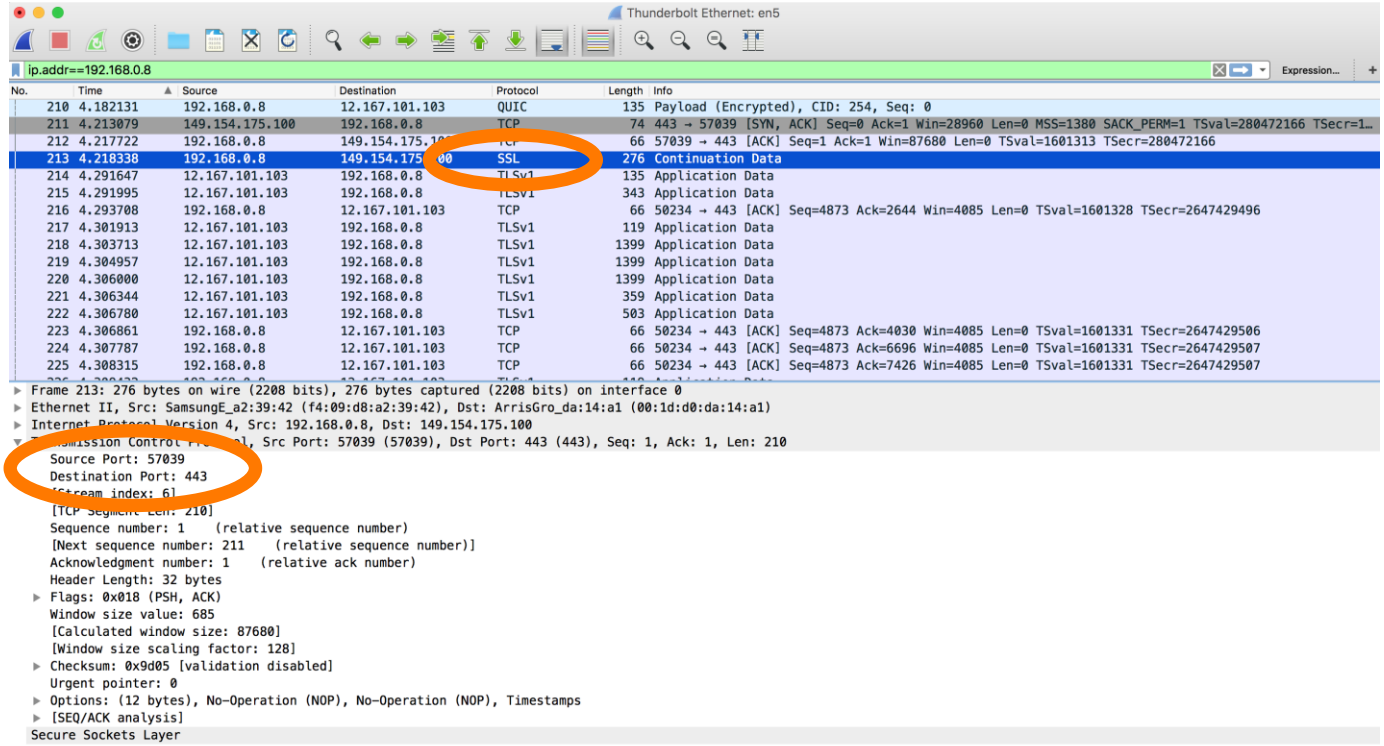
Encapsulación

- Un túnel SSL es utilizado para asegurar la comunicación entre el SMR y los dispositivos móviles, los servicios empresariales (IM, directorio, etc.) también se encuentran dentro del túnel.

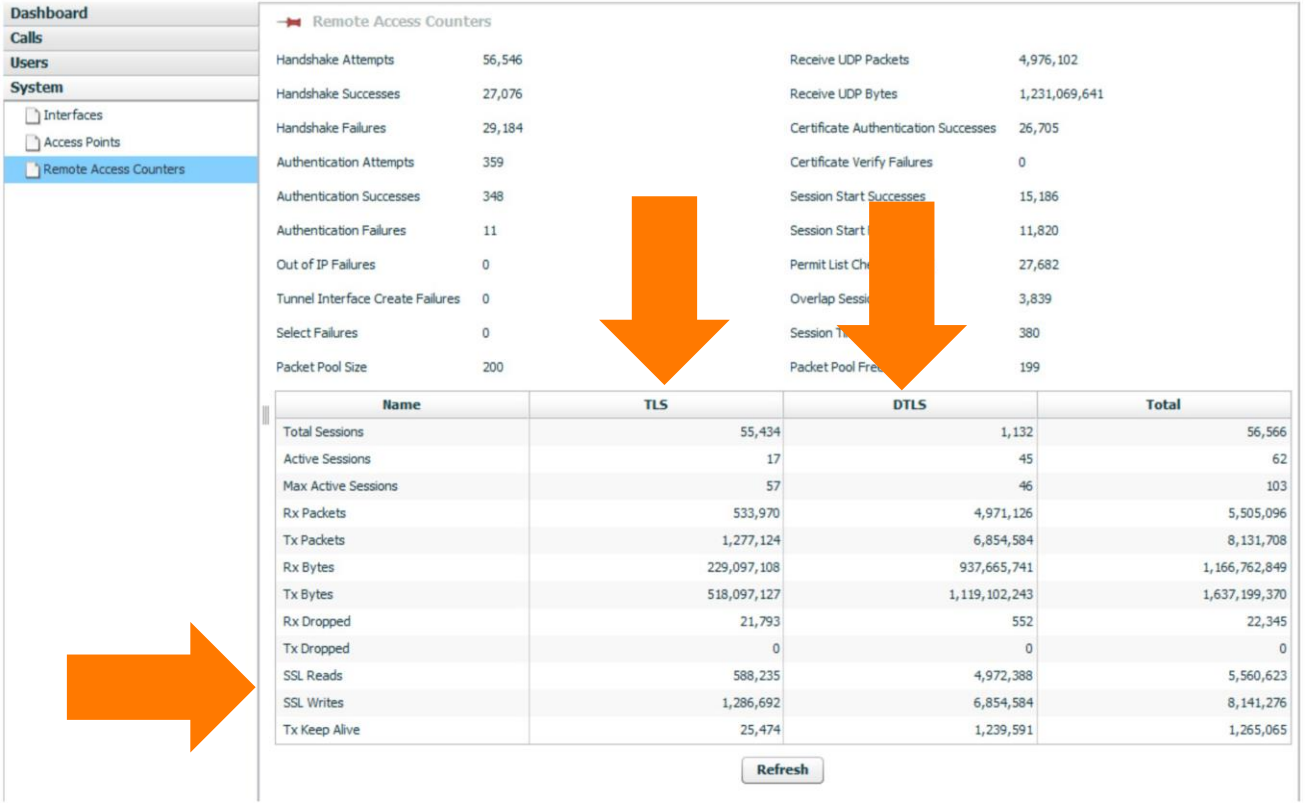
Generando una VPN con SSL en ShoreTel:



Una llamada en un tunel VPN



Una llamada en un tunel VPN



Name	TLS	DTLS	Total
Total Sessions	55,434	1,132	56,566
Active Sessions	17	45	62
Max Active Sessions	57	46	103
Rx Packets	533,970	4,971,126	5,505,096
Tx Packets	1,277,124	6,854,584	8,131,708
Rx Bytes	229,097,108	937,665,741	1,166,762,849
Tx Bytes	518,097,127	1,119,102,243	1,637,199,370
Rx Dropped	21,793	552	22,345
Tx Dropped	0	0	0
SSL Reads	588,235	4,972,388	5,560,623
SSL Writes	1,286,692	6,854,584	8,141,276
Tx Keep Alive	25,474	1,239,591	1,265,065

ShoreTel Mobility Router

ShoreTel Mobility Router

Scaling:

- 2000 Series:10 - 100 users
- 4000 Series:10 - 1,000 users

(Stackable for additional scaling)

- Virtual SMR – 1000 users

Core Functions:

- PBX and UC integration
- Security integration
- App layer security
- Policy management
- Reporting/trending

ShoreTel Mobility Client

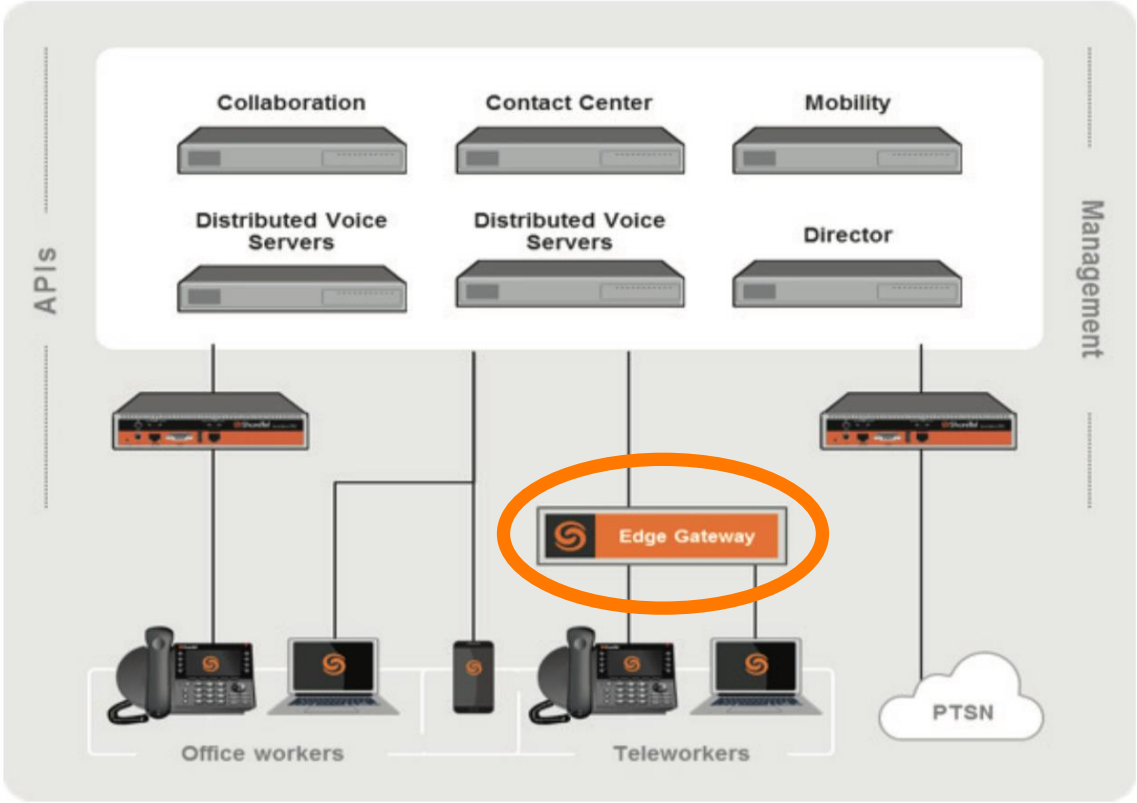
Key Features:

- Video Conferencing
- Desk phones and UC capabilities
- Integrated security
- Business and personal identities
- Calendar integration

Phone Types:

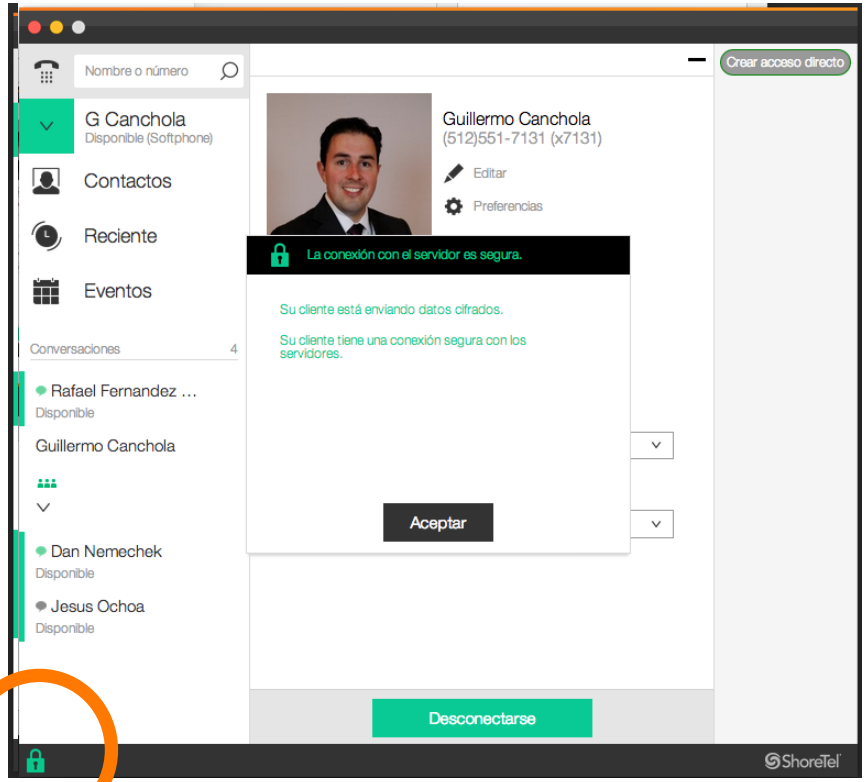
- Android
- Apple iOS
- Blackberry OS

Que pasa con los teléfonos de escritorio? Edge Gateway

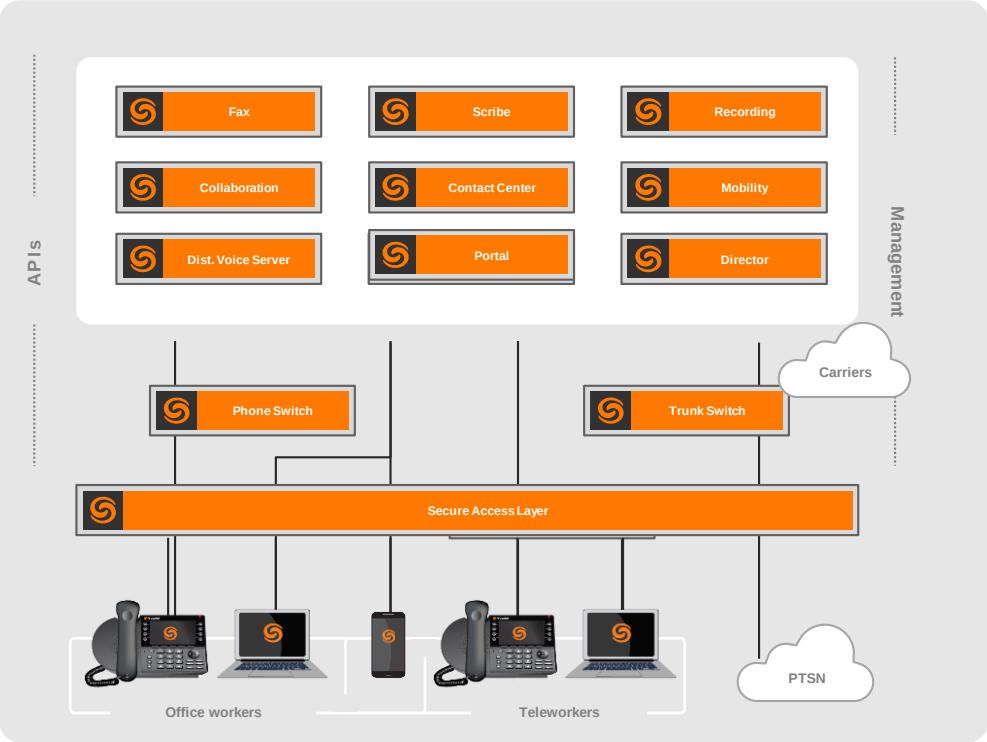


Edge Gateway

Edge Gateway



Que pasa con el video y otros servicios de comunicaciones?



Todas las comunicaciones entre los usuarios **dentro de tu red** ahora están seguras.

Seguridad VS Privacidad

c. [redacted] Not Encrypted End-to-End. Calls made through the [redacted] service are decrypted at [redacted] servers and are then routed without encryption through the public switched telephone network (PSTN) to their intended termination points. Calls made via [redacted] may be subject to lawful interception at the point where they are decrypted and at any point on the public telephone network. Member to member calls are fully encrypted end-to-end.

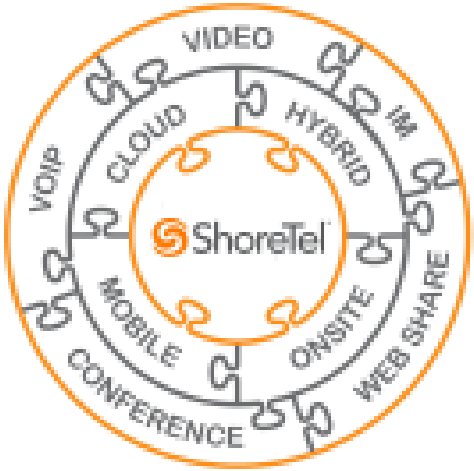
Log File Information: When you use the [redacted], our servers automatically record certain information that your web browser sends whenever you visit any website. These server logs may include information such as your web request, Internet Protocol ("IP") address, browser type, browser language, referring / exit pages and URLs, platform type, number of clicks, domain names, landing pages, pages viewed and the order of those pages, the amount of time spent on particular pages, the date and time of your request, one or more cookies that may uniquely identify your browser, your phone number, phone number you are requesting the status of and various status information. When you use the [redacted] Service, our servers log certain general information that our application sends whenever a message is sent or received, or if you update or request any status information, including time and date stamps and the mobile phone numbers the messages were sent from and to.

[redacted] If you do not agree to our practices, please do not use the [redacted] Service.

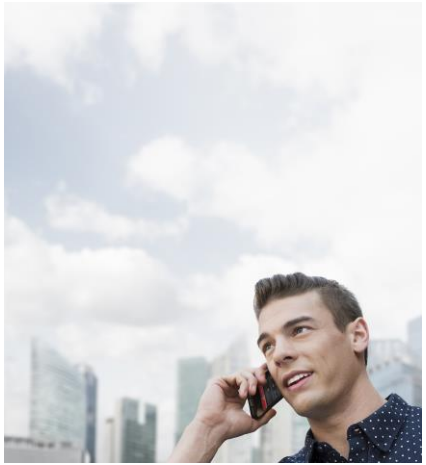
you. You are responsible for all activity that occurs under your Account, and you agree to maintain the security and secrecy of your Account username and password at all times. Unless otherwise permitted by [redacted] writing, you may only possess one Account.

[redacted] may, in [redacted] sole discretion, permit you from time to time to submit, upload, publish or otherwise make available to [redacted] through the Services textual, audio, and/or visual content and information, including commentary and feedback related to the Services, initiation of support requests, and submission of entries for competitions and promotions ("*User Content*"). Any User Content provided by you remains your property. However, by providing User Content to [redacted] you grant [redacted] a worldwide, perpetual, irrevocable, transferrable, royalty-free license, with the right to sublicense, to use, copy, modify, create derivative works of, distribute, publicly display, publicly perform, and otherwise exploit in any manner such User Content in all formats and distribution channels now known or hereafter devised (including in connection with the Services and [redacted] business and on third-party sites and services), without further notice to or consent from you, and without the requirement of payment to you or any other person or entity.

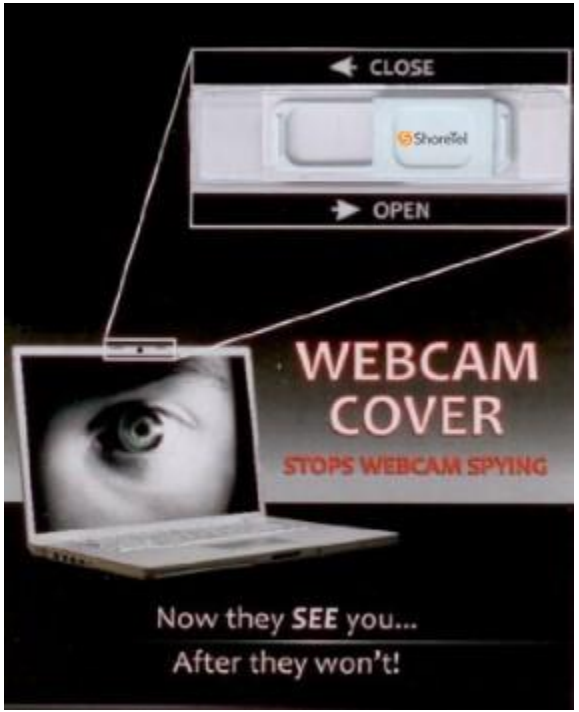
Preguntas?



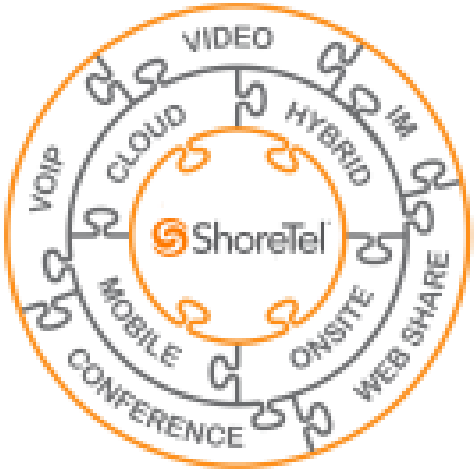
Contacto: gcanchola@shoretel.com
@MemoCancholaR
www.shoretel.com



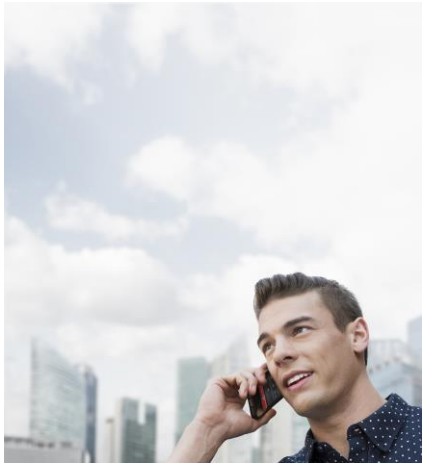
La mejor seguridad para el video…….



GRACIAS!!!!!!!!!



Contacto: gcanchola@shoretel.com
@MemoCancholaR
www.shoretel.com



Cálculo de ancho de banda

Bandwidth Calculator for Secure Remote Voice		Device Type	Android
Codec	G.711 u-law	Sample Size	20
Transport Type	UDP	Encryption	AES-SHA

ETHERNET	14	
IP	20	
UDP	8	
DTLS	13	
AES-SHA	40	
RAST	16	
RTP	12	
Tunneled UDP	8	
Tunneled IP	20	
G.711	160	
Total bytes	311	
Packet per sec	50	
Data Rate (one-way)	124.4	kbps