cgc-eu

DOCUMENTO TÉCNICO

ARQUITECTURA DE CENTRALITA VIRTUAL

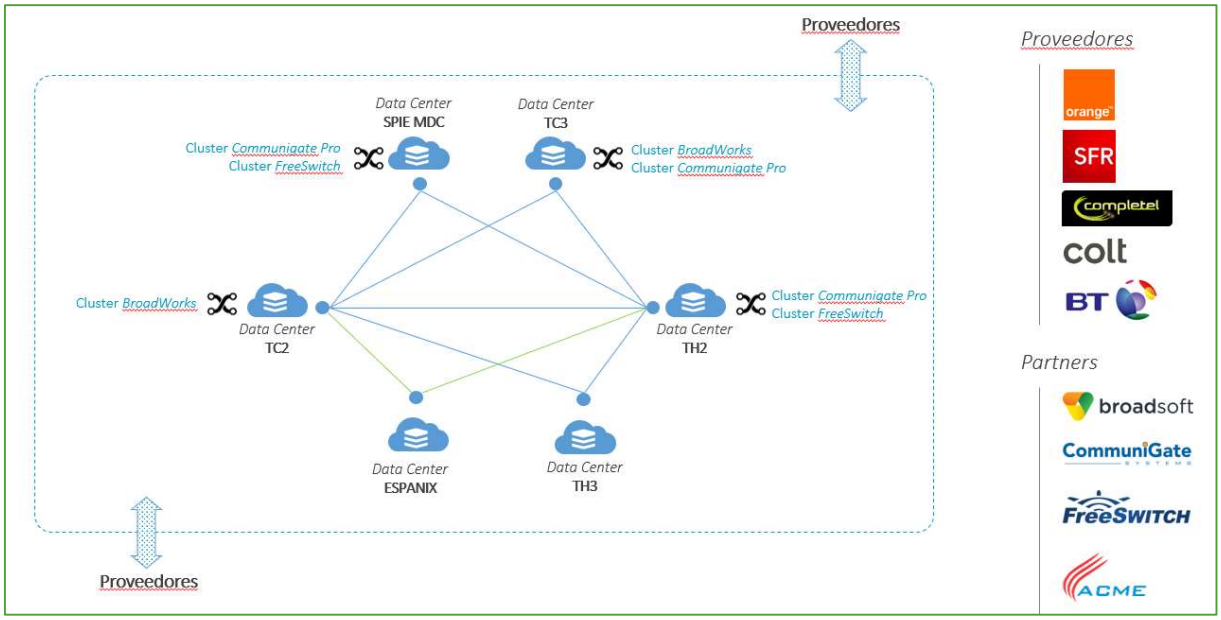
ANEXO 1: ARQUITECTURA Y PROVEEDORES DE LA CENTRALITA VIRTUAL

CGC ha construido una arquitectura basada en múltiples Datacenter remotos para responder a las necesidades de alojamiento y seguridad más exigentes de sus clientes.

Estos Datacenter están interconectados por fibras ópticas oscuras multi-operador, iluminadas por CGC a 10GB/s, con el objetivo de garantizar el transporte correcto de los flujos de datos de clientes. Las infraestructuras se duplican por grupos de dos Datacenter en modo espejo, permitiendo así garantizar la continuidad del servicio de Centralita Virtual.

Todos los centros de alojamiento forman parte de una misma red extensa, permitiendo así disponer de una solución altamente disponible, paliando eficazmente cualquier indisponibilidad de un componente técnico. Además, esta arquitectura facilita el despliegue de los clientes.

Los centros de alojamiento están organizados según el siguiente esquema:



SERVICIO

Distribuida en 5 centros de datos, la red central de CGC es totalmente redundante.

Basado en una implementación de múltiples clústeres, los servicios son resistentes (SLA> 99,99%)

SEGURIDAD

La red central está totalmente protegido contra ataques (D DoS Y hacking) y todos los equipos están protegidos por elementos de seguridad (Firewall, Load-Balancer F5, SBC Acme)

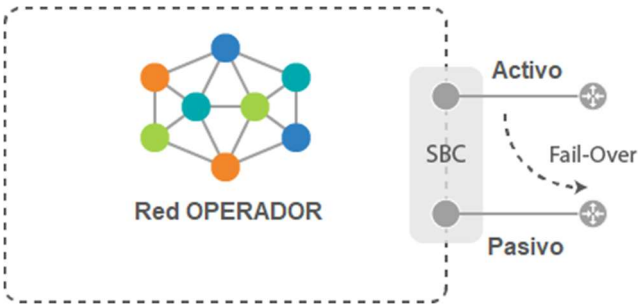
MANTENIMIENTO

Asegurado por el departamento I-D y el equipo de gestión de los centros de datos, CGC proporciona todo el mantenimiento de acuerdo con las restricciones del cliente (HNO, período de aviso)

ANEXO 2: REDUNDANCIA DEL TRUNK SIP

Modo «Global & Help»

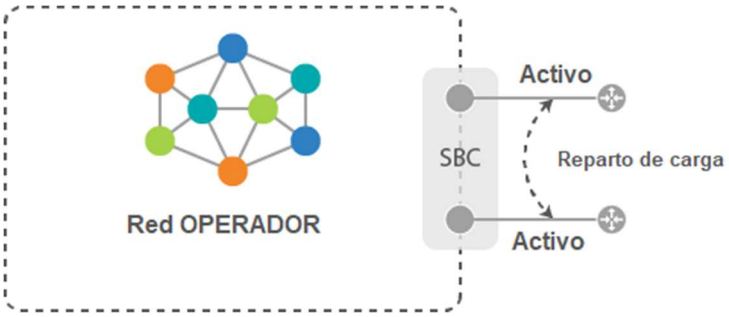
El sitio cliente se conecta mediante dos conexiones en tecnología mixta: una conexión «activa», utilizada en función global y una conexión «pasiva» utilizada en rescate, para asegurar un funcionamiento óptimo, incluso en modo degradado.



La transición– o «Fail-Over» de una conexión hacia la otra se efectúa en menos de 90 segundos. En caso de cambio de conexión, se interrumpen las conversaciones con el exterior. Las conversaciones internas al sitio pueden continuar.

Modo «Reparto de Carga»

El sitio cliente está también conectado con dos conexiones de tecnología mixta, pero las dos conexiones están «activas». CGC preconiza este tipo de seguridad para los sitios que deben estar en todo momento operativos, y gestionar la distribución y la gestión del tráfico.



El tráfico se reparte entre las conexiones de acceso. En caso de fallo de una conexión o de un equipo distante, el SBC CGC detecta el error y dirige la totalidad del tráfico hacia la conexión que permanece operativa.

ANEXO 3: DISPOSITIVOS DE SEGURIDAD

Confidencialidad

Los flujos entre nuestras infraestructuras y nuestros transportistas utilizan interconexiones físicas directas, sin pasar por la Internet pública. Por otro lado, nuestras propias infraestructuras, como se indica en el párrafo precedente, responden a criterios de seguridad de muy alto nivel, y están en conformidad con las certificaciones y particularmente con el RGS.

Desde un punto de vista legal, nosotros garantizamos en toda la cadena de las comunicaciones la conservación de las identidades reales de todas las llamadas que pasan por nuestra red, incluidas las llamadas anónimas y las que presentan identidades falsas.

Autentificación de las comunicaciones

Desde un punto de vista protocolario SIP ofrecemos dos soluciones de autentificación:

- Nuestros sistemas conocen las direcciones IP de los equipos de interconexión de los clientes (los dos pares de SBC ACME) y rechazan las llamadas procedentes de una fuente desconocida mediante el posicionamiento de normas de firewall (IP ACL).
- Además, los intercambios pueden ser igualmente autentificados por parejas usuario/contraseña, que permiten verificar los intercambios SIP. Este método está a menudo reservado para los equipos móviles, que deben poder unirse a nuestras infraestructuras, desde cualquier dirección originaria.