# STG

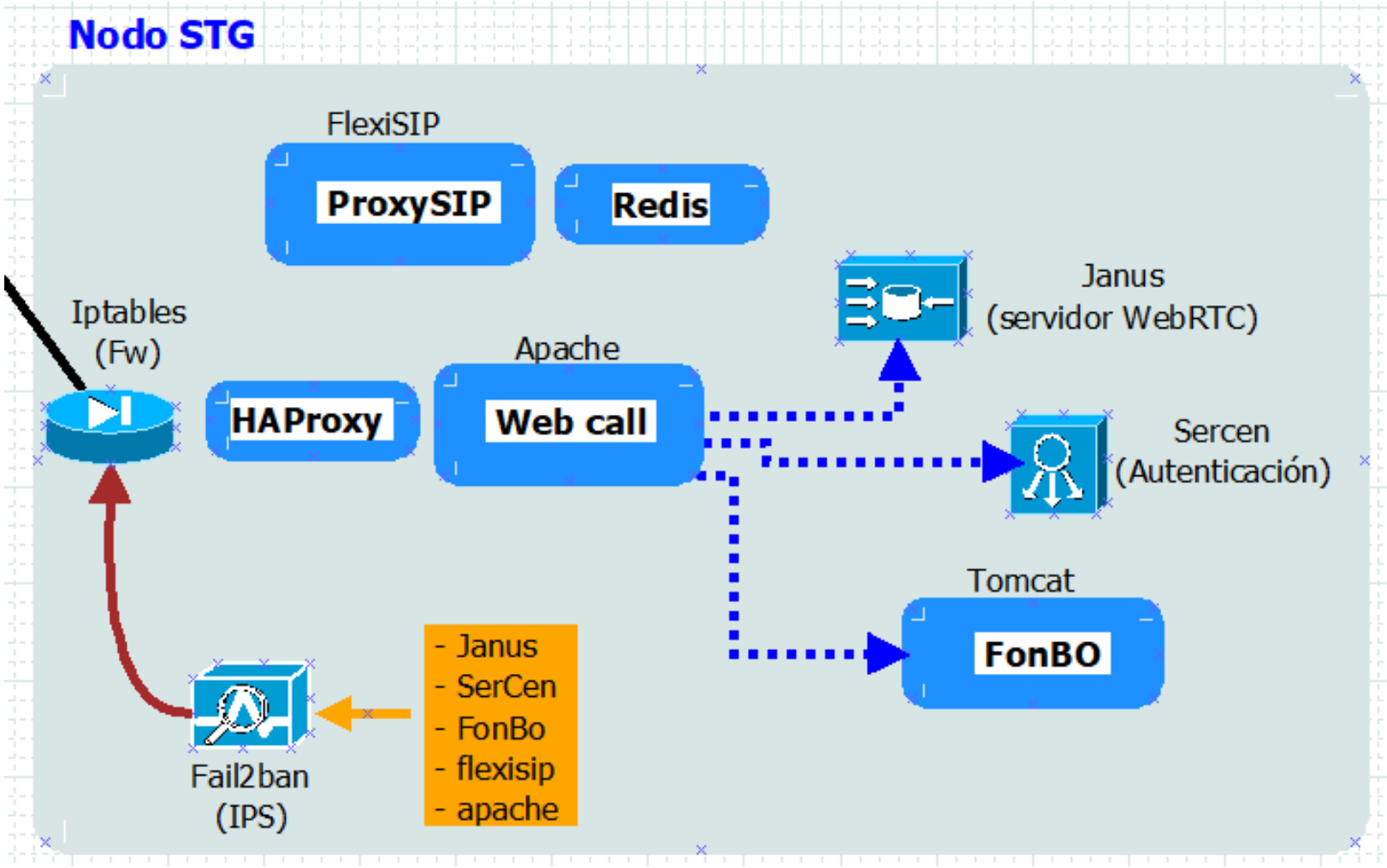
*... beyond limit ...*

*www.mdtel.es*

# Nodo STG
# Web RTC + FlexiSip

# Nodo STG

## Esquema nodo STG

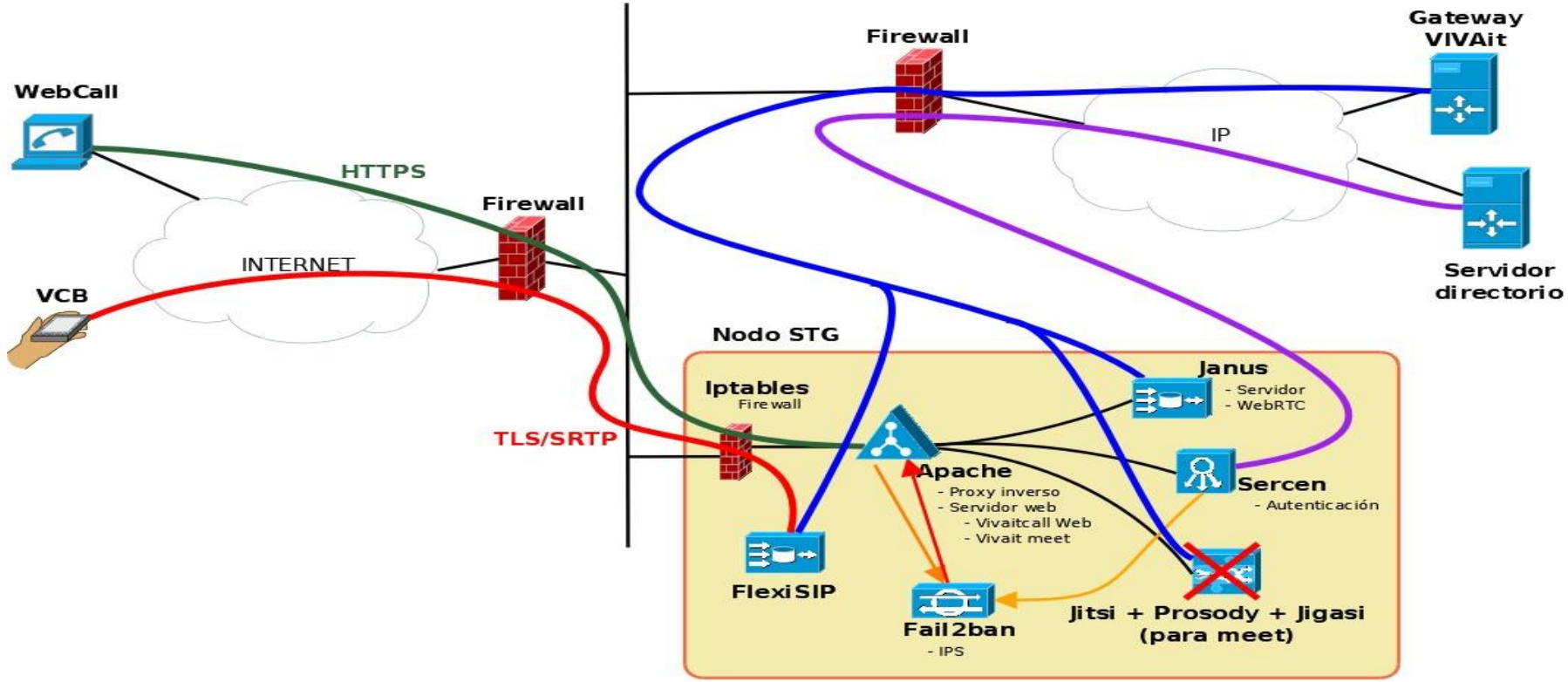


# Nodo STG

Para minimizar el area de exposición de VIVAit a redes inseguras (internet), se han concentrado las funciones que requieren conectividad con dichas redes en el nodo STG Las conexiones vía internet de Web Call, APP ***VIVA***it Call Business y otros (p.ej hardphone en internet) serán terminadas y controladas en este nodo.

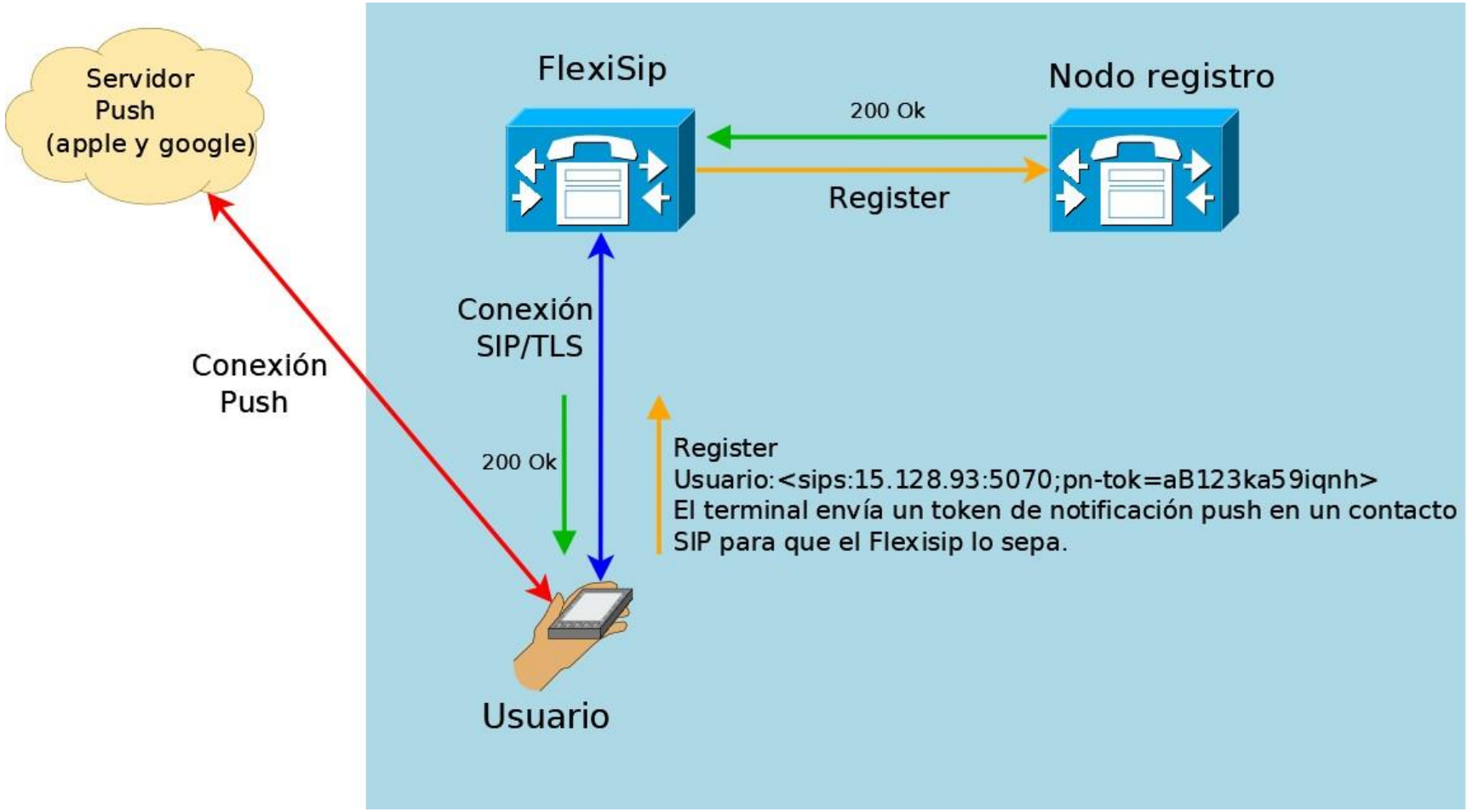
Se han definido mecanismos de balanceo de carga y alta disponibilidad (Pacemaker, Haproxy, Redis, DNS).

Mecanismos específicos de seguridad para asegurar el funcionamiento de los bloqueos incluso en cluster

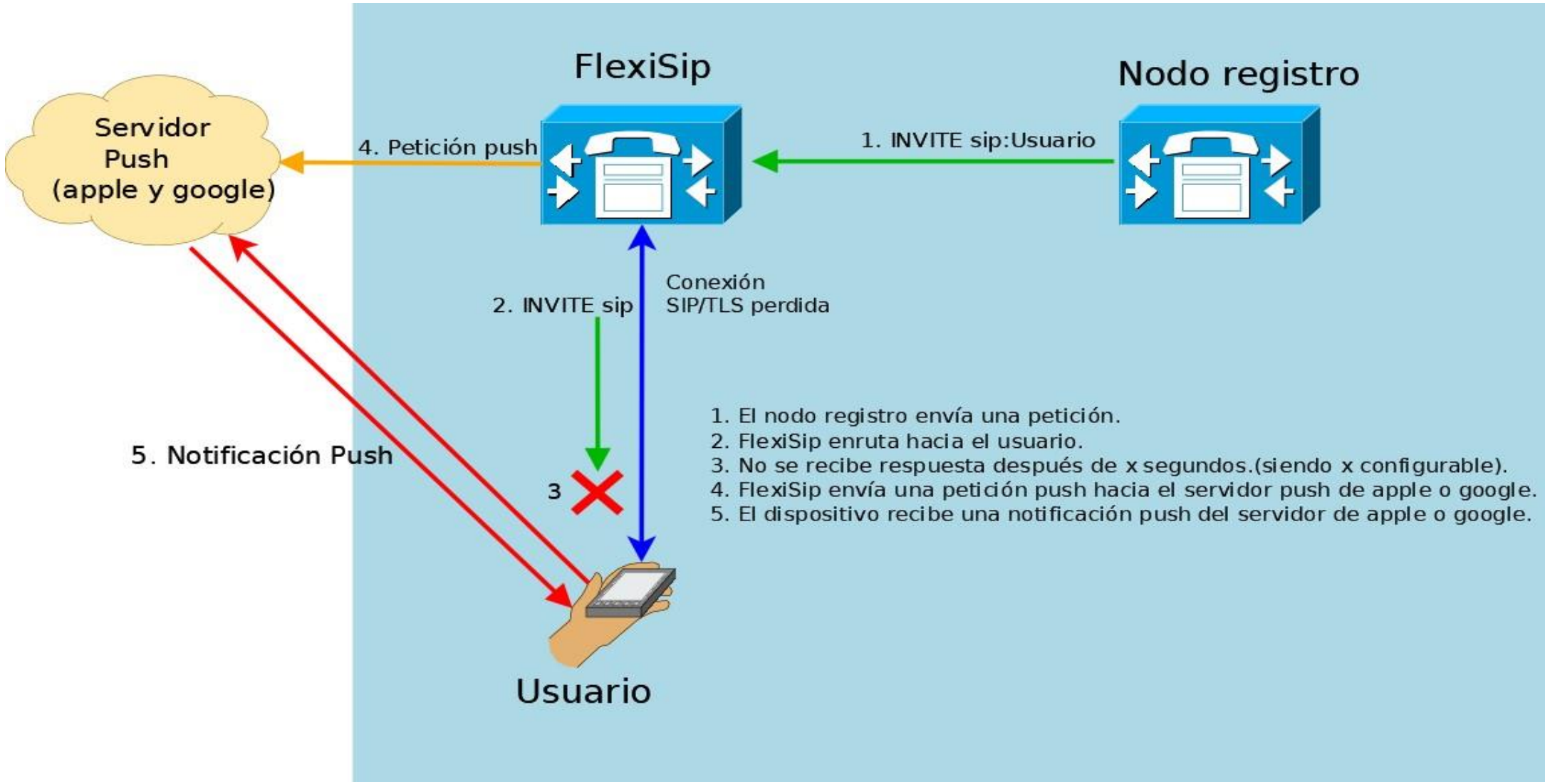


# Nodo STG

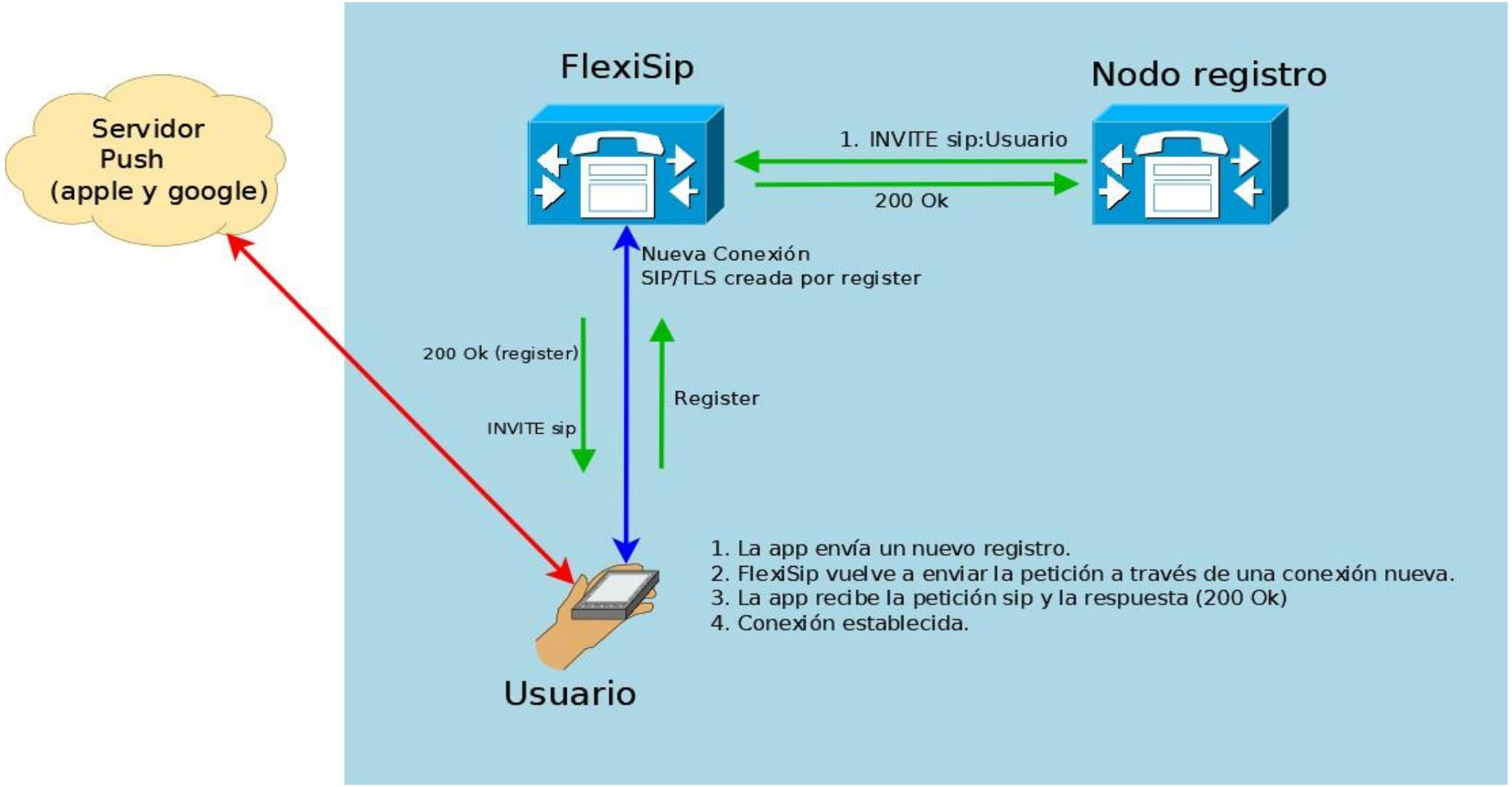
El nodo STG/FlexiSIP tiene un servicio push. Este servicio sirve para enviar llamadas entrantes SIP o mensajes de texto en el dispositivo móvil del usuario, ya que se requieren notificaciones push para recibir información cuando la aplicación de **Viva**it Business no está activa en primer plano. FlexiSIp actúa como proxy en el registro de los terminales.



# Establecimiento de llamada vía push (1/2)



# Establecimiento de llamada vía push (2/2)



# Nodo STG

## INSTALACION FlexiSIP (proxy sip)

- mkdir /var/log/flexisip
- apt install gpg redis
- Paquete proporcionado por MDtel
  - bc-flexisip_2.3.0-0.alpha.100+df47b191_amd64.deb
    - apt install bc-flexisip_2.3.0-0.alpha.100+df47b191_amd64.deb
- flexisip-logrotate: Para copiar en /etc/logrotate.d
- **Fichero de configuracion**
  - flexisip.conf: Para copiar en /etc/flexisip
    - Comprobar todos los **REVISAR**
- flexisip_desplegar.sh: Script para instalar servicio
- systemctl enable flexisip-proxy
- systemctl start flexisip-proxy

- **Ficheros de logs**
  - /var/log/flexisip/flexisip-proxy.log

# Nodo STG

## Comprobaciones tras instalación

| Elemento | Que pruebo | Como lanzo la prueba | Donde reviso | Que reviso | Resultado esperado |
|---|---|---|---|---|---|
| General | Nmap de TCP | nmap -sS -sV -p 0- -T4 -A -v A.B.C.D | Resultados Nmap | | Puertos abiertos 443 y 80 |
| General | Nmap de UDP | nmap -sU -T4 -v --max-rtt-timeout 100ms --initial-rtt-timeout 100ms --max-retries 1 A.B.C.D | Resultados Nmap | | Puertos abiertos ninguno o solo entre 30000 a 30999 |
| HTTPS<br>Portal usuario<br>Portal WebCall | Clave incorrecta (una vez) | Acceso a URL, clave incorrecta una vez | Navegador<br><br>Log Sercen<br><br>Log Fail2ban | Navegador<br><br>Logs:<br>tail -f /var/log/serCen/serCen.log \| grep TRUCO<br><br>tail -f /var/log/fail2ban.log \| grep 'filter\|actions' | Navegador:<br>Usuario o clave incorrectos<br>Sercen:<br>Aparecen entradas TRUCO_KO<br>Fail2ban:<br>Aparece entrada fail2ban.filter |
| HTTPS<br>Portal usuario<br>Portal WebCall | Clave incorrecta (mas de diez veces) | Acceso a URL, clave incorrecta, más de 10 veces | Navegador<br><br>Syslog<br><br>fail2ban<br><br>Iptables | Navegador<br><br>Logs:<br>tail -f /var/log/syslog \| grep TRUCO<br><br>tail -f /var/log/fail2ban.log \| grep 'filter\|actions'<br><br>Iptables -L \| grep X.X.X.X | Navegador:<br>Usuario o clave incorrectos<br>Timeout<br><br>**EN TODOS LOS SERVIDORES DEL CLUSTER**<br>syslog:<br>Aparece entrada TRUCO_KO<br>fail2ban:<br>Aparecen entradas fail2ban.filter<br>Aparece entradas fail2ban.actions<br>iptables:<br>DROP all -- X.X.X.X anywhere |
| HTTPS<br>Otras URL | Acceso a URL solo accesible desde dentro | Acceder a urlcliente/sercen/getautenticacionapache | Navegador | Respuesta en navegador | Forbidden |
| HTTPS<br>Otras URL | Acceso a URL solo accesible desde dentro<br>URL de Fonbo una vez | script FONBO | Log fonbo | Log:<br>tail -f /var/log/tomcat9/Vivait-FonBO.log \| grep TRUCO | Fonbo:<br>TRUCO_KO [X.X.X.X] token invalido |
| HTTPS<br>Otras URL | Acceso a URL solo accesible desde dentro<br>URL de Fonbo mas de diez veces | script FONBO | Syslog | Syslog: tail -f \| grep TRUCO | EN TODOS LOS SERVIDORES DEL CLUSTER<br>aparecen entrada de TRUCO en Syslog<br>aparece entrada en IPTables para IP origen |
| HTTPS<br>Otras URL | URL mas corta (una vez) | Acceder a urlcliente/sercen/ | Navegador (timeout) | Error 404 | |
| HTTPS<br>Otras URL | URL mas corta (mas de cien veces) | Script Acceso | Navegador | Syslog: tail -f \| grep TRUCO | EN TODOS LOS SERVIDORES DEL CLUSTER<br>aparecen entrada de TRUCO en Syslog<br>aparece entrada en IPTables para IP origen |
| HTTPS<br>Otras URL | URL mas corta | Acceder a urlcliente | Navegador | Redirección | Redirige a lo configurado en index.html |
| HTTP<br>Otras URL | URL mas corta | Acceder a urlcliente | Navegador | Destino | index.html con Forbidden |
| HTTP<br>Otras URL | URL's Webfon/portal | Acceder a URL en http | Navegador (no accede, no da error) | Respuesta en navegador | Not found |
| IP | Acceder a URL por IP | Acceder a url Webfon/portal cambiando urlcliente por la IP | Navegador<br>Fail2ban.log | Respuesta en navegador<br>Log de fail2ban | En navegador "Not found"<br>En log de fail2ban aparece un intento |
| SSH | Acceso SSH desde IP fuera de mdtel | Cliente SSH desde un PC no conectado a red mdtel (por ejemplo vía WiFi con un movil) | Cliente SSH | Conectividad | Timeout |
| FlexiSIP | Clave incorrecta (una vez) | Conectar VCB con clave de cuenta SIP incorrecta | VCB<br>flexisip-proxy.log | VCB conectiidad<br>tail -f log \| grep TRUCO | VCB no conecta<br>aparece entrada TRUCO |
| FlexiSIP | Clave incorrecta (mas de diez veces) | Conectar VCB con clave de cuenta SIP incorrecta, mas de 10 veces | VCB<br>Syslog<br>Iptables | | VCB no conecta<br>EN TODOS LOS SERVIDORES DEL CLUSTER<br>- aparecen entrada de TRUCO en Syslog<br>- aparece entrada en IPTables para IP origen |
| ntp | | | | ntpq -p | |

# Nodo STG

## Maneja 2 tipos de base de datos

- Mysql
- Redis
  - Almacén de estructura de datos de valores de clave en memoria rápido y de código abierto.
  - Almacena los terminales registrados, asi como las direcciones ips reales de los terminales que se conectan a través de internet, asi como si UID.
  - redis-cli keys * -> devuelve todas las 'claves' almacenada en redis. Útil para diagnósticos.
  - redis-cli hgetall <clave> -> devuelve toda la informacion de una 'clave'. Útil para diagnósticos.

# Nodo STG

## Maneja 2 tipos de base de datos

- Ejemplo:

```
root@mdlinux25:~/docs# redis-cli keys \*
 1) "fs:6109*01@sips.mdtel.es"
 2) "fs:6170*01@sips.mdtel.es"
 3) "fs:40702*01@sips.mdtel.es"
 4) "fs:conference-factory@192.168.0.29"
 5) "fs:40107*02@sips.mdtel.es"
 6) "fs:40709*01@sips.mdtel.es"
 7) "fs:40107*01@sips.mdtel.es"
 8) "fs:6177*01@sips.mdtel.es"
 9) "fs:40902*01@sips.mdtel.es"
10) "fs:40401*01@sips.mdtel.es"
11) "fs:40516*01@sips.mdtel.es"
12) "fs:40004*01@sips.mdtel.es"
13) "fs:40518*01@sips.mdtel.es"
14) "fs:40521*01@sips.mdtel.es"
15) "fs:40300*01@sips.mdtel.es"
16) "fs:40710*01@sips.mdtel.es"
17) "fs:40519*01@sips.mdtel.es"\

root@mdlinux25:~/docs# redis-cli hgetall "fs:40004*01@sips.mdtel.es"
1) "\"<urn:uuid:f39520e5-83ef-005c-b7e8-989617e6d730>\""
2) "\"JAC\" <sip:40004*01@79.146.86.86:33030;pn-prid=d6kkm6jJQx6Q0zwqP2WkFI:APA91bEF_QjbKKiEc1qZ3X6ofEkrW9GgMRCAk_ez9iJuZ-avP3ws-
zN0WGlGl3N0MbjIwzM1rcCFI6md3_eXD4oe6eR-UNWVRlvzK8YXzr30f8Uu3G-j4I-SfPZJDaEoFf01tZfbskRm;pn-provider=fcm;pn-param=917288118967;pn-silent=1;pn-
timeout=0;transport=tls;fs-conn-
id=ee1a796332c7cc1a;callid=iZZ9Nq8ars;expires=36000;cseq=21;updatedAt=1697711736;alias=no;usedAsRoute=no?path=%3Csip%3A89.140.51.149%3A5556%3Btransport%3Dtcp%3Bf
s-proxy-id%3D26378b0194d4162e%3Blr%3E%2C%3Csips%3A89.140.51.149%3A5554%3Blr%3E&accept=application/sdp%2Ctext/plain%2Capplication/vnd.gsma.rcs-ft-http+xml&user-
agent=LinphoneAndroid/5.2.0-alpha.18+ae92b030c%20(realme%208%205G)%20LinphoneSDK/5.3.0-alpha.310+1616072%20(master)>;+sip.instance=\"<urn:uuid:f39520e5-83ef-005c-
b7e8-989617e6d730>\";+org.linphone.specs=\"ephemeral/1.1,groupchat/1.2,lime\";pub-gruu=\"sip:40004*01@sips.mdtel.es;gr=urn:uuid:f39520e5-83ef-005c-b7e8-989617e6d730\""
```

# Nodo STG

## Configurar correctamente el dominio

- Campo C_DOMINIO_INTERNET en la tabla COM_CONFIGURACION

## Posibles diagnosticos

- Revisar archivo de log
- Comprobar conectividad desde internet al puerto 5554
  - nc NOMBRE_DOMINIO 5554 –vn
    Ejemplo:
    nc sips.mdtel.es 5554 -nv
    Connection to 172.25.0.25 5554 port [tcp/*] succeeded!

- Comprobar conectividad desde nodo STG a nodos asterisk
  - nc ips_asterisk 5060 –vn
    Ejemplo:
    nc 172.25.128.251 5060 -nv
    Connection to 172.25.128.251 5060 port [tcp/*] succeeded!

# Nodo STG

**Alta disponibilidad**

https://wiki.linphone.org/xwiki/wiki/public/view/Flexisip/HOWTOs/High%20availability/

## HAProxy

Proporciona un equilibrador de carga de alta disponibilidad, balanceo y un proxy inverso para aplicaciones basadas en TCP y HTTP que distribuye solicitudes entre varios servidores.

**Instalacion**

- apt install haproxy

**Fichero de configuracion**

- /etc/haproxy/haproxy.cfg

**Arranque del servicio**

- systemctl start haproxy.service

**Logs**

- /var/log/haproxy.log

# Nodo STG

## Fichero de configuracion HAProxy

```
# REVISAR direcciones ip en backend
#
global
    log /dev/log local0
    log /dev/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin expose-fd listeners
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log global
    mode http
    # option httplog
    option dontlognull
    timeout connect 5000
    timeout client  50000
    timeout server  50000
    errorfile 400 /etc/haproxy/errors/400.http
    errorfile 403 /etc/haproxy/errors/403.http
    errorfile 408 /etc/haproxy/errors/408.http
    errorfile 500 /etc/haproxy/errors/500.http
    errorfile 502 /etc/haproxy/errors/502.http
    errorfile 503 /etc/haproxy/errors/503.http
    errorfile 504 /etc/haproxy/errors/504.http

frontend test_kb
    bind 0.0.0.0:443 ssl crt /etc/apache2/ssl/ApacheCert.pem
    option forwardfor
    default_backend apache_webservers

backend apache_webservers
    mode http
    balance source
    server websvr1 10.53.27.72:80 source 10.53.27.72 check inter 30s
    server websvr1 10.53.27.73:80 source 10.53.27.73 check inter 30s

listen stats
    bind :8800
    mode http
    option httpclose
    stats enable
    stats uri /
    stats hide-version
    stats auth haproxy:ALIcates
```

## Cambios en apache

Debido a la introducción del HAProxy se ha modificado la configuración de apache para hacerlo más estándar:

Nuevos ficheros en /etc/apache2/sites-availables/

- 100-SIN-HAproxy.conf
- 200-CON-HAproxy.con
- 300-Portales.conf
- 900-CON-HAproxy-saml2.conf

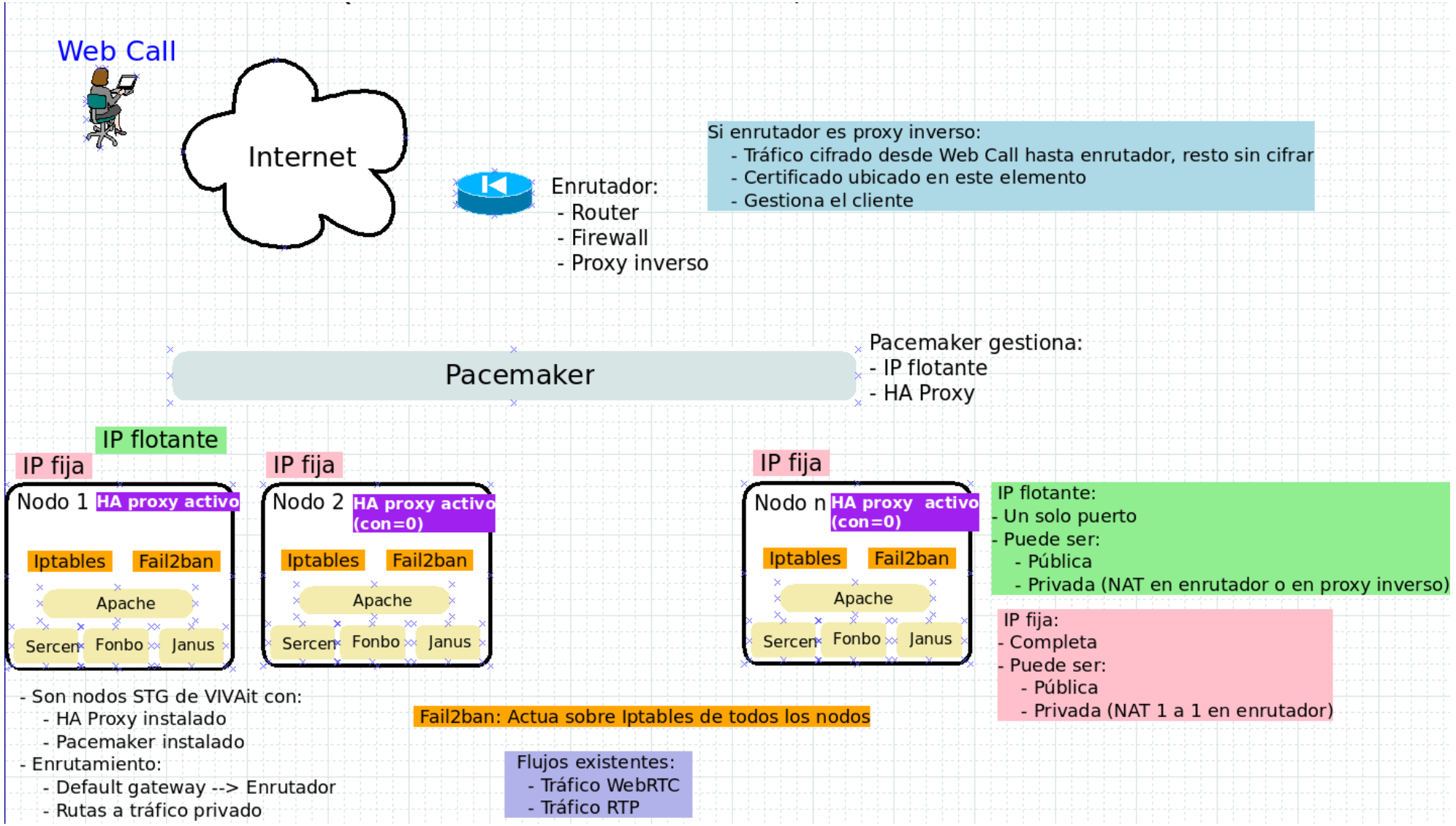
Solo debéis poner el enlace simbólico apropiado a vuestra maquina en /etc/apache2/sites-enabled/

Ejemplo:

Maquina STG -> **200-CON-HAproxy.conf -> ../sites-available/200-CON-HAproxy.conf**
Maquina Gestión -> **300-Portales.conf -> ../sites-available/300-Portales.conf**

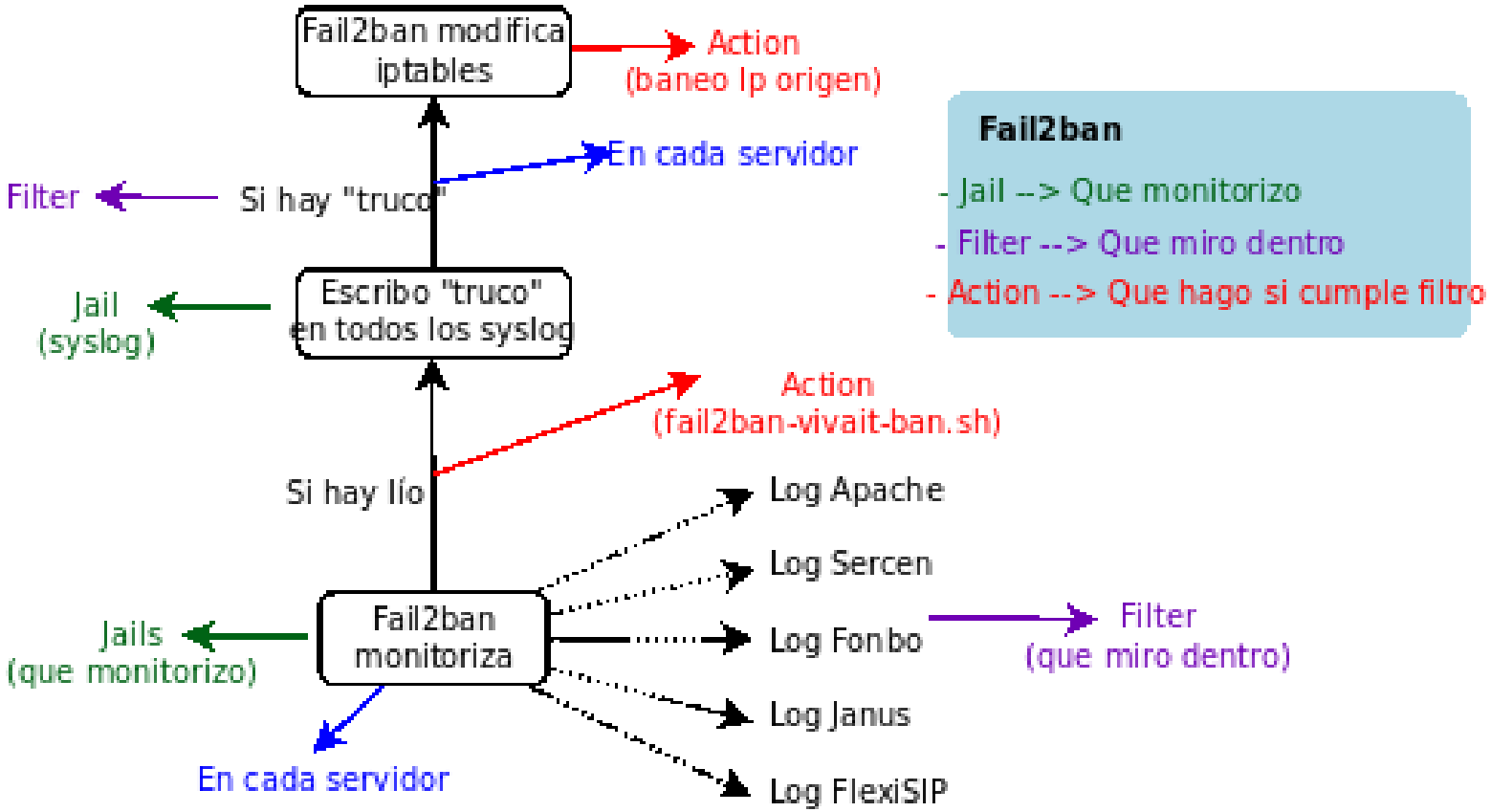
# Nodo STG

## Alta disponibilidad WebCall



## Cambios en fail2ban

Provocado por la introducción del HAProxy (alta disponibilidad y balanceo)



# Nodo STG

## Cambios en fail2ban

- /etc/fail2ban/jail.d/vivait.local
  - Fichero donde indicamos que es lo que vamos a "mirar"
    - FonBo, apache, flexisip, sercen...

- /etc/fail2ban/jail.local
  - Fichero donde se configurar listado de IPs en los que ignoraremos las reglas del fail2ban

- /etc/fail2ban/filter.d/vivait-apache.local
  - Se especifica la cadena a buscar en el archivo de logs

- /etc/fail2ban/filter.d/vivait-truco.local
  - Se indica la cadena "TRUCO_KO Seguido de la IP a buscar en los archivos de logs

- /etc/fail2ban/action.d/vivait-ban.local
  - Acción a ejecutar cuando se cumple el filtro
    - Se ejecuta el script /usr/local/sbin/fail2ban-vivait-ban.sh "<name>" "<ip>"

## Cambios en fail2ban

```
#!/bin/bash

#
# REVISAR lineas 'ban_*' del final
#

JAIL="$1"
IP="$2"
HORA="$(/usr/bin/date +%H:%M:%S.%N)"

function ban_local {
  /usr/bin/logger -d -t vivait "TRUCO_KO [$IP] fail2ban $JAIL $HORA"
}

function ban_remoto {
  /usr/bin/logger -n $1 -d -t vivait "TRUCO_KO [$IP] fail2ban $JAIL $HORA"
}

ban_local
#ban_remoto 10.53.27.73
```


*… eso es todo amigos …*