Trabajo Integrador AyG

Cadena de Restaurantes

ZAMUDIO FABIAN LEG 108932
Fabian.zamudio.89@gmail.com

índice

Aspectos globales y comunes

Topología global 3

Asignación de IP 4

SLAs de conectividad 4

Configuración de monitoreo 5

Notificaciones y TRAPS 5

Prioridad de tráfico 6

Seguridad y control 7

Disponibilidad y tolerancia a fallas 8

Detalle sede CENTRAL

Topología lógica sede CENTRAL 9

Asignación de IP 10

Equipamiento de interconectividad 10

Especificaciones de servidores 11

Seguridad y control 12

Disponibilidad y tolerancia a fallas 15

Detalle sede común

Topología lógica sede común 16

Asignación de IP 16

Equipamiento de interconectividad 17

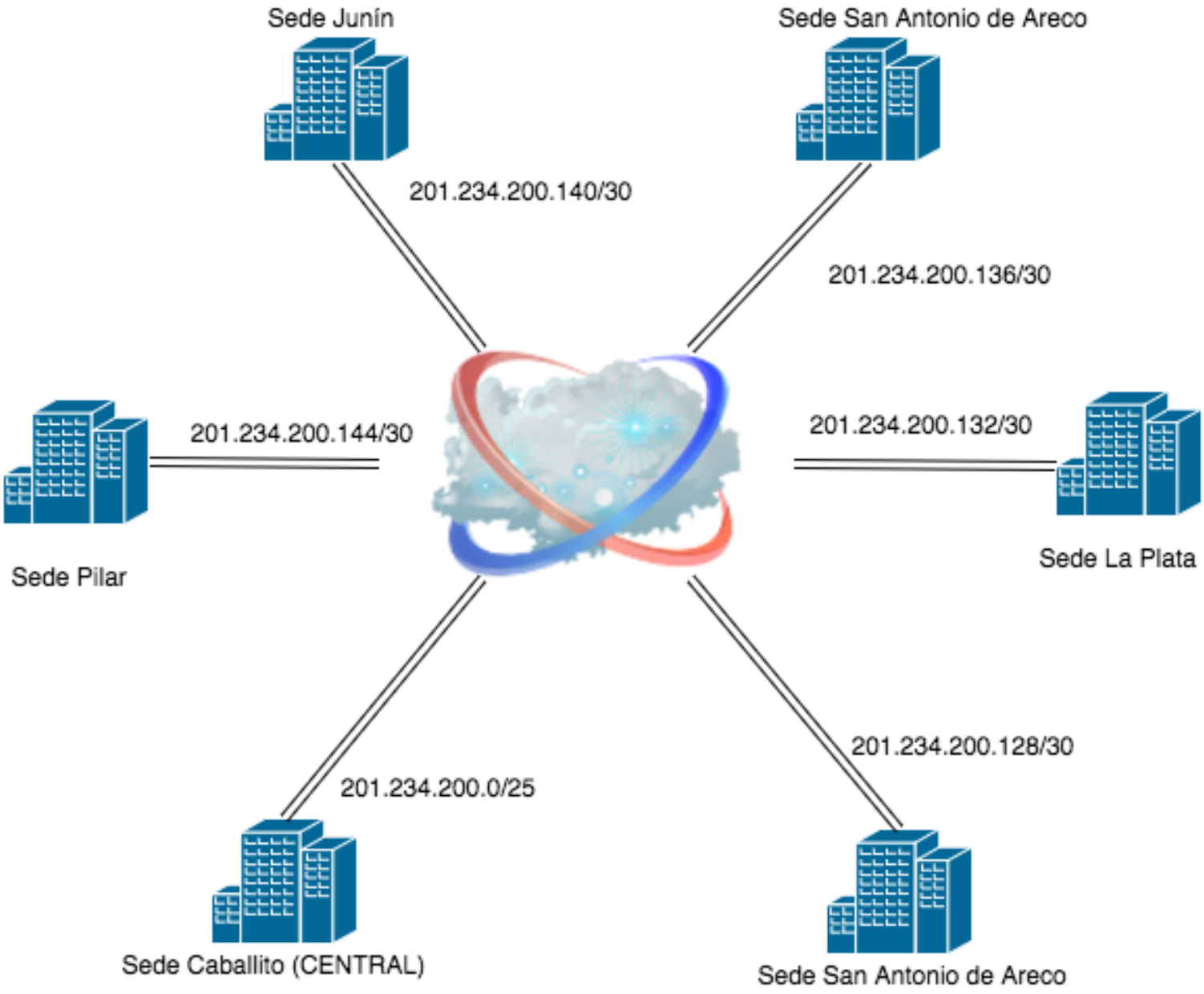
Especificaciones de servidores 17

Seguridad y control 18

Aspectos globales y comunes

En este apartado se específica toda configuración, característica, conexiones y restricción globales y comunes , entendiendo como global a todas las sedes en su conjunto. Se encontrara la topología entre las sedes y hacia internet, las direcciones IP y mascaras asignada a cada una, SLAs pretendida para asegurar un optimo uso de la red, configuración de monitoreo mínima, notificaciones para el administrador ante eventos,, prioridad de tráfico y seguridad y control.
Se hizo una reserva del bloque IP 201.234.200.0/24 y se asigno a la sede central el bloque 201.234.200.0/25 y se dividió el bloque restante en partes iguales de mascara /30 permitiendo la escalabilidad a futuras sedes.

Topología lógica



Asignación de IP

Sede	IP	Mascara
Caballito	201.234.200.0	/25
Pilar	201.234.200.128	/30
La Plata	201.234.200.128	/30
San Antonio de Areco	201.234.200.128	/30
Junín	201.234.200.128	/30

Conectividad SLAs

Se especifica una conexión de cada sucursal hacia internet

- Máximo RTT: 150ms (se toma como referencia www.google.com.ar).
- Máximo Jitter: 25%.
- Ancho de banda 6Mbps simétrico
- Tiempo sin disponibilidad de conexión mensual 3hs. Máximo tiempo continuo de indisponibilidad de 2hs.
- Tiempo sin disponibilidad de servicio mensual 6hs.
- Asistencia técnica 24X7 y respuesta ante errores dentro de las 6hs siguientes al registro del ticket.
- Perdida de paquete 1 de 800 paquetes transmitidos.
- IP estática anteriormente mencionadas.
- Para trafico VoIP se debe mantener la secuencia.

Se especifica una conexión de cada sucursal (excepto CENTRAL) hacia la sede CENTRAL. (Opcional)

- Máximo RTT: 100ms (se toma como referencia www.google.com.ar).
- Máximo Jitter: 10%.
- Ancho de banda 10Mbps simétrico
- Tiempo sin disponibilidad de conexión mensual 3hs. Máximo tiempo continuo de indisponibilidad de 2hs.
- Tiempo sin disponibilidad de servicio mensual 4hs.
- Asistencia técnica 24X7 y respuesta ante errores dentro de las 6hs siguientes al registro del ticket.
- Enlace de fibra óptica
- Perdida de paquete 1 de 1000 paquetes transmitidos.
- IP estática anteriormente mencionadas
- Para trafico VoIP se debe mantener la secuencia.

Configuración de monitoreo

Se listan a continuación los dispositivos a monitorear con algunos puntos sensibles a monitorear:

- Router: Cambios en el estado operacional, resultados del negativos del test POST al iniciar, notificaciones de anomalías en el tráfico analizado.

- Servidor Web: Consultas periódicas automáticas de respuesta del servidor, umbral de espacio en memoria ram disponible, umbral de espacio de disco rigido , umbral de porcentaje de uso del procesador, puertos en escucha, Test de Estrés con diferentes herramientas de benchmarking.

- Switch: Cambios en el estado operacional, resultados del negativos del test POST al iniciar, puertos en escucha, control de conteo de tags VLANs.

- Servidor DNS: Consultas periódicas automáticas de respuesta del servidor, umbral de espacio en memoria ram disponible.

- Servidor de Mail: Consultas periódicas automáticas de respuesta del servidor, umbral de espacio en disco disponible.

- Servidor de base de datos: Consultas periódicas automáticas de respuesta del servidor, umbral de espacio en disco disponible, backup semanal .

- Servidor VoIP: Consultas periódicas automáticas de respuesta del servidor.

- Servidor de aplicaciones: Consultas periódicas automáticas de respuesta del servidor, umbral de porcentaje de uso del procesador, umbral de espacio en memoria ram disponible, umbral de espacio en disco disponible.

- Red general: Se utilizaran herramientas como Iptraf, VnStat, NMap, Ntop, Ping para controles mensuales o semanales de la red. En los enlaces hacia internet y dedicado se agregara IPerf para conocer el (throughput).

Notificaciones y TRAPS

Mediante el uso de SNMP se crearan TRAPS que notificaran al administrador de posibles errores, ataques, fallas. Ante la falta de suministro eléctrico se encenderán las UPS y se avisara al administrador mediante un email del evento, si se agotara el suministro de la UPS se

encenderá el segundo conjunto de UPS de respaldo, enviando nuevamente un email al administrador.

En el caso que los componentes monitorizados superen umbrales establecidos se enviaran notificaciones al administrador.

Recurso	Umbral	Envió de email
Uso de disco rigido en cada servidor	40% Uso	NO
Uso de disco rigido en cada servidor	70% Uso	NO
Uso de disco rigido en cada servidor	80% Uso	SI
Uso de disco rigido en cada servidor	90% Uso	SI
Uso de disco rigido en cada servidor	95% Uso	SI
No respuesta de dispositivo	10 intentos	
No respuesta de dispositivo	20 intentos	SI
Uso de red de una sola IP	60%	SI
Cambio de topología	1	
Cierre de interfaces VPN		SI

Todos los informes y logs generados serán almacenados para futuros controles. Semanalmente se tiene que enviar un email al administrador con las estadísticas relevantes de la semana caducada.

Todas las redes de todas las sedes deben poder ser administradas por SNMP desde la red de Administración o desde la red de Administración de la sede central mediante VPN o SSH.

Prioridades de tráfico

Se listan las prioridades y requisitos mínimos y máximos para cada servicio y/o tipo de tráfico, donde se especifica numero de prioridad siendo 1 el más alto y 7 el más bajo, ancho de banda máximo y mínimo.
Cualquier tipo de trafico no puede superar el uso de más del 80% del ancho de banda total. Para esta instancia se utiliza Traffic Shaping

Tráfico de VoIP

- Prioridad: 1.
- Ancho de banda máximo: 8Mbps.
- Ancho de banda mínimo: 4Mbps.

Tráfico Web

- Prioridad: 2.
- Ancho de banda máximo: 8Mbps.
- Ancho de banda mínimo: 1Mbps.

Tráfico de DNS

- Prioridad: 3.
- Ancho de banda máximo: 3Mbps.
- Ancho de banda mínimo: 1Mbps.

Tráfico hacia el servidor de aplicaciones

- Prioridad: 4.
- Ancho de banda máximo: 5Mbps.
- Ancho de banda mínimo: 1Mbps.

Tráfico de consultas a la base de datos

- Prioridad: 5.
- Ancho de banda máximo: 4Mbps.
- Ancho de banda mínimo: 1Mbps.

Tráfico de correo

- Prioridad: 6.
- Ancho de banda máximo: 2Mbps.
- Ancho de banda mínimo: 1Mbps.

Default

- Ancho de banda máximo: 2Mbps.
- Ancho de banda mínimo: 1Mbps.

Seguridad y control

Para la seguridad ante ataques se implementa un Firewall perteneciente al router el cual aplica filtrado de paquetes según políticas definidas.
Para mayor seguridad se implementa un sistema de detección de intrusos (IDS) en donde analiza el tráfico y lo compara tanto con firmas de ataques conocidos, como con parámetros definidos por el administrador. Aunque no se toma en cuenta su uso en este caso se sugiere el uso de IPS y en lo posible UTM para mejor eficiencia en la administración y protección.

Se cree conveniente el uso de VLANs para separar distintos tipos de servicios como:

- Servidores para evitar tráfico innecesario y posible congestión en la red.
- Telefonía IP para aumentar la QoS y priorización de la misma.
- Protocolo SNMP para administración de dispositivos.

El router principal tiene la función de RSA de las conexiones VPN entre las diferentes sedes, preferentemente montar la conexión VPN en el enlace dedicado y transmitir el tráfico VoIP por el miso.

Se sugiere que se permita el uso de control remoto SSH mediante el uso de clave publica y en su defecto usuario y contraseña.

Los servidores utilizaran certificados, se listan una serie de autoridades certificantes:

- letsencrypt.org
- identrust.com
- entrust.com
- geotrust.com
- globalsign.es

Disponibilidad y tolerancia a fallas

Los servidores de aplicación para la toma de pedidos de los mozos tendrá dos caminos de distribución de energía simultáneos para todos los servidores con dispositivos UPS (dos por servidor) conectados al servidor para prevención en caso de cortes del suministro eléctrico.

El router aplicara NAT hacia internet desde las redes de administración, red de aplicación de mozos y clientes. No se elimino la posibilidad de que la red de mozos pueda acceder a internet para posibilitar futuros cambios en la organización, aunque solo bastaría con una regla más en la política de seguridad para eliminar estos permisos.

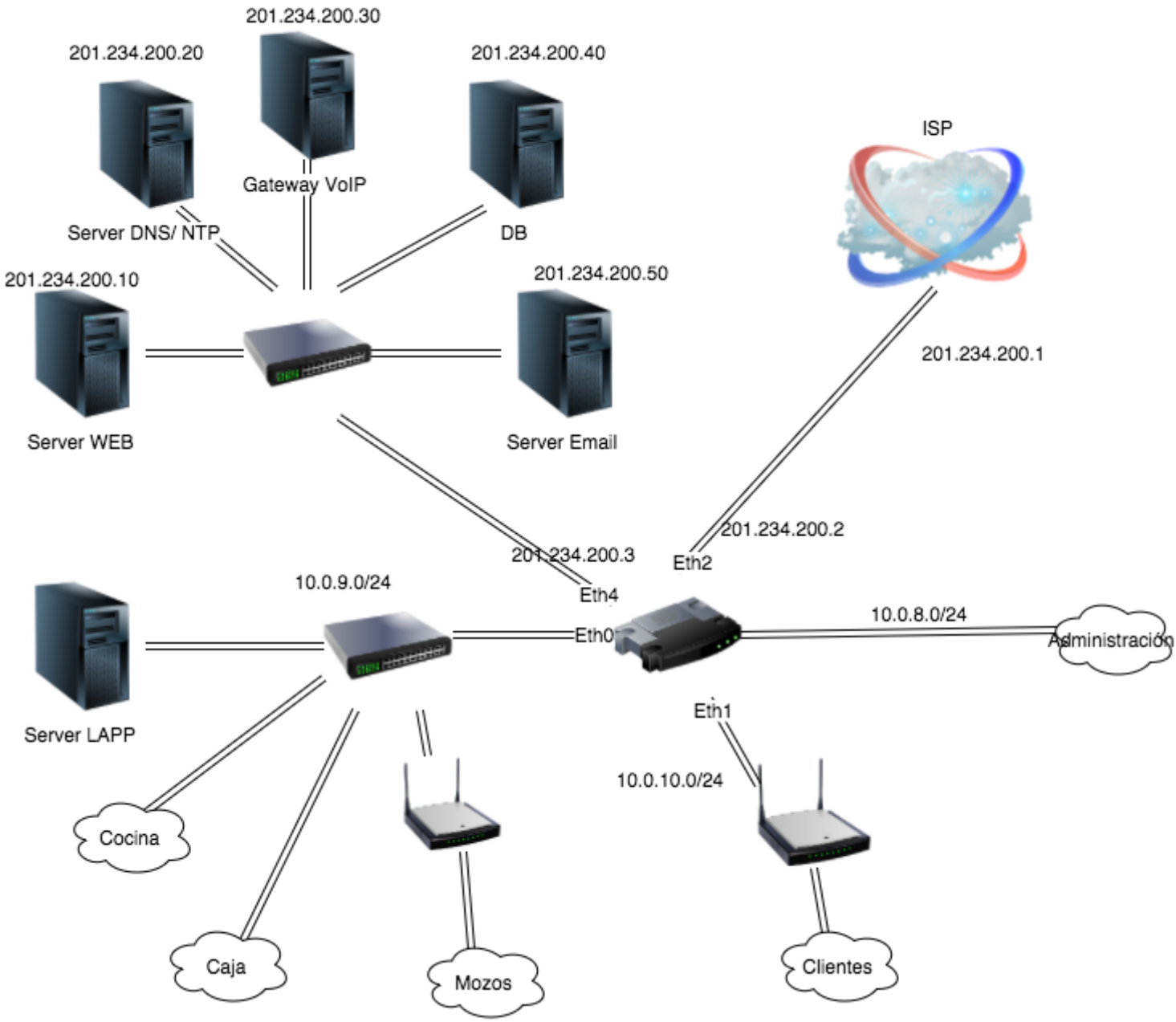
El túnel VPN será configurado site to site con un posible uso de certificados creados a partir de las CA mencionadas en los servidores web. Se utilizara el enlace dedicado para establecer la conexión y en el caso de falla se iniciara en el enlace hacia internet.

Toda transmisión VoIP pasara por el Gateway tanto SIP como RTP para un mayor control, administración y contabilidad de uso de este servicio.

El acceso a la red tanto por el switch wireless de clientes y mozos tendrán contraseñas distintas WPA2. Se tiene que considerar el uso de la red de mozos filtrada por MAC de los dispositivos.

Sede central

Topología lógica



Asignación de IP

Red/Dispositivo	IP	Mascara	Cantidad
Administración	**10.0.8.0**	**/24**	**255**
Desktop	10.0.8.1-10.0.8.24	-	24
Telefonía IP	10.0.8.25-10.0.8.36	-	12
Aplicación pedidos	**10.0.9.0**	**/24**	**255**
Mozos	10.0.9.1-10.0.9.12		12
Telefonía IP Mozos	10.0.9.13-10.0.9.24		12
Cocina	10.0.9.25 – 10.0.9.29		5
Telefonía IP Cocina	10.0.9.30		1
Caja	10.0.9.31 – 10.0.9.32		2
Telefonía IP Cocina	10.0.9.33		1
Clientes	**10.0.10.0**	**/24**	**255**

Equipamiento de interconectividad

Equipo	Cantidad
Switch wireless 1 Gbps SNMP v2c compatible etiquetado 802.1	2
Switch 48 puertos 1Gbps SNMP v2c compatible etiquetado 802.1	2
Switch 12 puertos 1Gbps SNMP v2c compatible etiquetado 802.1	1
Servidor Aplicación mozos: Servidor S.O. Windows Server 2012 R2 - Procesador i7 x64 (preferentemente i7-6920HQ) - 8GB de memoria ram - 2 discos rígidos de 1TB	1
Servidor DNS: Servidor S.O. DEBIAN - Procesador i7 x64 (preferentemente i7-6920HQ) - 8GB de memoria ram - 3 discos rígidos de 1TB (RAID 5) para el servicio Web	1
Servidor Email: Servidor S.O. DEBIAN - Procesador i7 x64 (preferentemente i7-6920HQ) - 8GB de memoria ram - 3 discos rígidos de 1TB (RAID 5) para el servicio Web	1
Servidor DB: Servidor S.O. DEBIAN - Procesador i7 x64 (preferentemente i7-6920HQ) - 8GB de memoria ram - 3 discos rígidos de 1TB (RAID 5) para el servicio Web	1
Gateway VOIP: SS7 Media Gateway - SVI_MG8000	1
Servidor WEB: Servidor S.O. DEBIAN - Procesador i7 x64 (preferentemente i7-6920HQ) - 8GB de memoria ram - 3 discos rígidos de 1TB (RAID 5) para el servicio Web	1

UPS 800w 800va mínimo SNMPv2c compatible	12
Router VPN, NAT, Firewall, protocolo SNMPv2c compatible – 1Gbps.	1
Teléfono IP	14
Tablet wifi compatible 7''	12
Cable UTP categoría 5e	-
PC escritorio 2GB ram – microprocesador i3 – 250GB disco rigido	31

Especificaciones de servidores

Servidor Web

- Apache
  - Código abierto
  - Gratuito
  - Portabilidad
  - Soporte

- Nginx (Alternativa)
  - Código abierto
  - Gratuito

Servidor de Mail

- Exim: Es un agente de transferencia de mensajes (MTA) desarrollado en la Universidad de Cambridge para su uso en sistemas Unix conectados a Internet . Es libremente disponible bajo los términos de la Licencia Pública General GNU . En el estilo es similar a Smail 3 , pero sus instalaciones son más generales. Hay una gran flexibilidad en la manera que el correo puede ser encaminado.

- PostFix (Alternativa)

Servidor DNS:

- Bind9: Incluye entre otras características importantes: TSIG, notificación DNS, nsupdate, IPv6, rndc flush, vistas, procesamiento en paralelo, y una arquitectura mejorada en cuanto a portabilidad.

- PowerDNS (Alternativa).

Servidor de base de datos

- Postgres: Es un sistema de gestión de bases de datos objeto-relacional, distribuido bajo licencia BSD y con su código fuente disponible libremente. Es el sistema de gestión de bases de datos de código abierto más potente del mercado. PostgreSQL utiliza un modelo cliente/servidor y usa *multiprocesos* en vez de *multihilos* para garantizar la estabilidad del sistema. Un fallo en uno de los procesos no afectará el resto y el sistema continuará funcionando.

- Firebird (Alternativa).

Servidor de Aplicaciones

- Apache Tomcat 8.0: El servidor Tomcat ha sido desarrollado por "Apache Software Foundation" Esta comunidad tiene tal importancia que quizás sea la responsable del éxito de java. Tiene muchos proyectos interesantes pero sin duda el que más significativo es y será Tomcat.

- Apache Geronimo (Alternativa)

Central VoIP

- Elastix: Es un software de código abierto para el establecimiento comunicaciones unificadas. Pensando en este concepto el objetivo de Elastix es el de incorporar en una única solución todos los medios y alternativas de comunicación existentes en el ámbito empresarial.

- Asterik PBX (Alternativa)

Seguridad y control

Se presenta un script para la política de seguridad para implementar en el firewall.

```
#########################################################################
# Políticas por defecto
# Denegar todo el tráfico que no se habilite de manera específica
#########################################################################

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#########################################################################
# Eliminar todas las reglas existentes
#########################################################################

iptables -F
iptables -X
iptables -Z

#########################################################################
  Permitir al firewall enviar/recibir tráfico de servicios básicos
#########################################################################

## DNS
```

```
iptables -A OUTPUT -d  201.234.200.20 -p udp -dport 53 -j ACCEPT
iptables -A OUTPUT  -d  201.234.200.20 -p tcp -dport 53 --syn -j ACCEPT
iptables -A INPUT -s   201.234.200.20 -p udp -sport 53 -j ACCEPT

## NTP

iptables -A OUTPUT -d  201.234.200.20 -p udp -dport 123 -j ACCEPT
iptables -A INPUT -s  201.234.200.20 -p udp -sport 123 -j ACCEPT



## SMTP  Correo electrónico saliente

iptables -A OUTPUT -d 201.234.200.50 -p tcp -dport 25 --syn -j ACCEPT

## Aceptar paquetes de conexiones ya establecidas

iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

## Aceptar conexiones locales

iptables -A INPUT -i lo -j ACCEPT


#########################################################################
#  Paquetes en tránsito (tráfico que se rutea)
#########################################################################


## Permitir paquetes pertenecientes a conexiones ya establecidas

iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT


#####################################################################
#  Accedo desde red privada a servicios en servidores corporativos
#####################################################################

## Acceso a servidor de correo electrónico

iptables -A FORWARD  -s 10.0.0.0/8 -p tcp -d 201.234.200.50 -m multiport  -
dports 25,110,143 --syn -j ACCEPT

## Acceso a servidor dns y ntp

iptables -A FORWARD  -s 10.0.0.0/8 -d 201.234.200.20 -p udp -dport 53 -
j  ACCEPT
iptables -A FORWARD  -s 10.0.0.0/8 -d 201.234.200.20 -p tcp -dport 53 syn  -
j ACCEPT
iptables -A FORWARD  -s 10.0.0.0/8 -d 201.234.200.20 -p udp -dport 123 -
j  ACCEPT

## Acceso a servidor web
```

```
iptables -A FORWARD -s 10.0.0.0/8 -d 201.234.200.10 -p tcp -m multiport  -
dports 80,443 --syn -j ACCEPT

## Acceso a base de datos únicamente desde administración y su propia red

iptables -A FORWARD -s 10.0.8.0/24 -d 201.234.200.40 -p tcp -m multiport  -
dports 5432--syn -j ACCEPT

## Acceso a Gateway Voip de redes privadas excepto clientes33

## SIP

iptables -A FORWARD -s 10.0.8.0/24 -d 201.234.200.30 -p tcp -
m multiport  -dports 5060,5061--syn -j ACCEPT
iptables -A FORWARD -s 10.0.9.0/24 -d 201.234.200.30 -p tcp -
m multiport  -dports 5060,5061 --syn -j ACCEPT
iptables -A FORWARD -d 10.0.8.0/24 -s 201.234.200.30 -p tcp -
m multiport  -dports 5060,5061--syn -j ACCEPT
iptables -A FORWARD -d 10.0.9.0/24 -s 201.234.200.30 -p tcp  -
m multiport  -dports 5060,5061 --syn -j ACCEPT


## RTP

iptables -A FORWARD –d 201.234.200.30 -p udp -sport 10000:20000 -s 200.10.45.4 -j
ACCEPT
iptables -A FORWARD  –s 201.234.200.30 -p udp -dport 10000:20000 -d 200.10.45.4 -j
ACCEPT

## Acceso SNMP desde red de administración

iptables -A OUTPUT -d 10.0.8.0/24 -p udp -m multiport –dports 161,162 -j ACCEPT
iptables -A INPUT -s 10.0.8.0/24  -p udp -m multiport –sports 161,162 -j ACCEPT
iptables -A FORDWARD -s 10.0.8.0/24 -p udp m multiport –sports 161,162 -j ACCEPT



#####################################################################
# Desde Internet es posible acceder al servidor web de la empresa.
#####################################################################

iptables -A FORWARD -i eth2 -d 201.234.200.10 -p tcp -m multiport -
dports 80,443 --syn -j ACCEPT

#####################################################################
# Desde Internet es posible enviar correo electrónico al servidor de correo  #
corporativo.
#####################################################################

iptables A FORWARD -i eth2 -d 201.234.200.50 -p tcp  -dport 25 --syn -j ACCEPT
```

```
#####################################################################
# Desde Internet es posible realizar consultas DNS al servidor de nombres de #
dominio  de la organización.
#####################################################################

iptables -A FORWARD -i eth2 -d 201.234.200.20 -p udp -dport 53 -j ACCEPT
iptables -A FORWARD -i eth2 -d 201.234.200.20 -p tcp -dport 53 --syn -j ACCEPT

#####################################################################
# El servidor de nombres de dominio debe sincronizarse con otros servidores N#
TP  accesibles a través de Internet.
#####################################################################

iptables -A FORWARD -i eth4 -s 201.234.200.20 -p udp -dport 123 -j ACCEPT

#####################################################################
# El Gateway debe ser accesido desde internet.
#####################################################################

iptables -A FORWARD -i eth2 -d 201.234.200.30 -p tcp -dports 5060,5061 --
syn  -j ACCEPT
iptables -A FORWARD -o eth2 -s 201.234.200.30 -p tcp -dports 5060,5061 --
syn  -j ACCEPT
```

Disponibilidad y tolerancia a fallas

Sistema de refrigeración redundante en la sala de servidores, los cuales se intercalan con cierta periodicidad para reducir la carga de trabajo en el tiempo. Se programa un mantenimiento preventivo mensual de los equipos y canales.
Dos caminos de distribución de energía simultáneos para todos los servidores con dispositivos UPS (dos por cada servidor) conectados a los servidores para prevención en caso de cortes del suministro eléctrico.

Los servidores poseen discos para formar RAIDs que anteriormente se especificaron según el servicio que presta y lo crítico de su falla. Copias de seguridad semanales y almacenadas en servidores de BackUp Online (sugerencia de DropBox business o IDrive Enterprise).

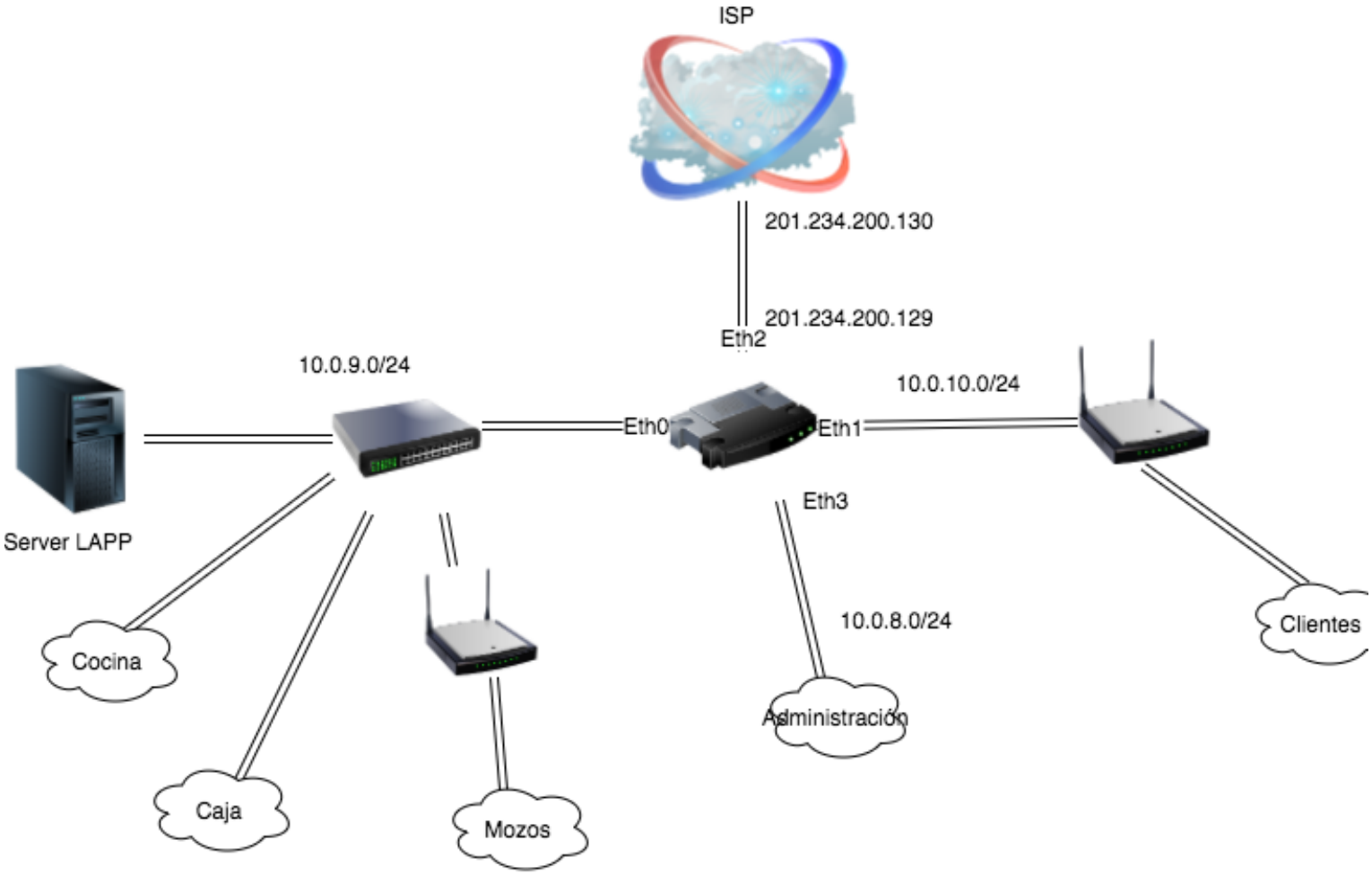
Los servidores de BD solo son accesibles desde la administración de la sede principal y desde la propia red de servidores de la organización.

Toda transmisión VoIP pasara por el Gateway tanto SIP como RTP para un mayor control y administración y contabilidad de uso de este servicio.

Detalle sede común

Para el desarrollo de este punto se toma el caso de San Antonio de Areco, pero se debe replicar en cada una de las demás sedes a excepción de la sede CENTRAL (Caballito) cambiando las IP públicas por las especificadas en la sección de "Aspectos globales y comunes".

Topología lógica



Asignación de IP

Red/Dispositivo	IP	Mascara	Cantidad
Administración	**10.0.8.0**	**/24**	**255**
Desktop	10.0.8.1-10.0.8.2	-	2
Telefonía IP	10.0.8.3-10.0.8.4	-	2
Aplicación pedidos	**10.0.9.0**	**/24**	**255**
Mozos	10.0.9.1-10.0.9.12		12
Telefonía IP	10.0.9.13-10.0.9.24		12

	Mozos			
	Cocina	10.0.9.25 – 10.0.9.29		5
	Telefonía IP Cocina	10.0.9.30		1
	Caja	10.0.9.31 – 10.0.9.32		2
	Telefonía IP Cocina	10.0.9.33		1
Clientes		**10.0.10.0**	**/24**	**255**

Equipamiento de interconectividad

Equipo	Cantidad
Switch wireless 1 Gbps SNMP compatible	2
Switch 48 puertos 1Gbps SNMP compatible	2
Switch 12 puertos 1Gbps SNMP compatible etiquetado 802.1	1
Servidor S.O. Windows Server 2012 R2 - Procesador i7 x64 (preferentemente i7-6920HQ) - 8GB de memoria ram - 2 discos rígidos de 1TB para el servicio Web	1
UPS 800w 800va mínimo SNMP compatible	2
Router VPN, NAT, Firewall, protocolo SNMP compatible - 1Gbps.	1
Teléfono IP	4
Tablet wifi compatible 7''	12
Cable UTP categoría 5e	-
PC escritorio 2GB ram – microprocesador i3 – 250GB disco rigido	9

Especificaciones de servidores

Servidor de Aplicaciones

- Apache Tomcat 8.0: El servidor Tomcat ha sido desarrollado por "Apache Software Foundation" Esta comunidad tiene tal importancia que quizás sea la responsable del éxito de java. Tiene muchos proyectos interesantes pero sin duda el que más significativo es y será Tomcat.

- Apache Geronimo (Alternativa)

```
#########################################################################
# Políticas por defecto
# Denegar todo el tráfico que no se habilite de manera específica
#########################################################################

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#########################################################################
# Eliminar todas las reglas existentes
#########################################################################

iptables -F
iptables -X
iptables -Z

#########################################################################
   Permitir al firewall enviar/recibir tráfico de servicios básicos
#########################################################################

## DNS

iptables -A OUTPUT -d  201.234.200.20 -p udp -dport 53 -j ACCEPT
iptables -A OUTPUT  -d  201.234.200.20 -p tcp -dport 53 --syn -j ACCEPT
iptables -A INPUT -s   201.234.200.20 -p udp -sport 53 -j ACCEPT

## NTP

iptables -A OUTPUT -d  201.234.200.20 -p udp -dport 123 -j ACCEPT
iptables -A INPUT -s  201.234.200.20 -p udp -sport 123 -j ACCEPT



## SMTP  Correo electrónico saliente

iptables -A OUTPUT -d 201.234.200.50 -p tcp -dport 25 --syn -j ACCEPT

## Aceptar paquetes de conexiones ya establecidas

iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

## Aceptar conexiones locales

iptables -A INPUT -i lo -j ACCEPT


#########################################################################
```

```
#  Paquetes en tránsito (tráfico que se rutea)
#########################################################################


## Permitir paquetes pertenecientes a conexiones ya establecidas

iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT


#################################################################
#  Accedo desde red privada a servicios en servidores corporativos
#################################################################

## Acceso a servidor de correo electrónico

iptables -A FORWARD  -s 10.0.0.0/8 -p tcp -d 201.234.200.50 -m multiport  -
dports 25,110,143 --syn -j ACCEPT

## Acceso a servidor dns y ntp

iptables -A FORWARD  -s 10.0.0.0/8 -d 201.234.200.20 -p udp -dport 53 -
j  ACCEPT
iptables -A FORWARD  -s 10.0.0.0/8 -d 201.234.200.20 -p tcp -dport 53 syn  -
j ACCEPT
iptables -A FORWARD  -s 10.0.0.0/8 -d 201.234.200.20 -p udp -dport 123 -
j  ACCEPT

## Acceso a servidor web

iptables -A FORWARD -s 10.0.0.0/8 -d 201.234.200.10 -p tcp -m multiport  -
dports 80,443 --syn -j ACCEPT

## Acceso a base de datos únicamente desde administración y su propia red

iptables -A FORWARD -s 10.0.8.0/24 -d 201.234.200.40 -p tcp -m multiport  -
dports 5432--syn -j ACCEPT

## Acceso a Gateway Voip de redes privadas excepto clientes33
## SIP

iptables -A FORWARD -s 10.0.8.0/24 -d 201.234.200.30 -p tcp -
m multiport  -dports 5060,5061--syn -j ACCEPT
iptables -A FORWARD -s 10.0.9.0/24 -d 201.234.200.30 -p tcp -
m multiport  -dports 5060,5061 --syn -j ACCEPT
iptables -A FORWARD -d 10.0.8.0/24 -s 201.234.200.30 -p tcp -
m multiport  -dports 5060,5061--syn -j ACCEPT
iptables -A FORWARD -d 10.0.9.0/24 -s 201.234.200.30 -p tcp  -
m multiport  -dports 5060,5061 --syn -j ACCEPT
```

```
## RTP

iptables -A FORWARD –d 201.234.200.30 -p udp -sport 10000:20000 -s 200.10.45.4 -j
ACCEPT
iptables -A FORWARD  –s 201.234.200.30 -p udp -dport 10000:20000 -d 200.10.45.4 -
j ACCEPT

## Acceso SNMP desde red de administración

iptables -A OUTPUT -d 10.0.8.0/24 -p udp -m multiport –dports 161,162 -j ACCEPT
iptables -A INPUT -s 10.0.8.0/24  -p udp -m multiport –sports 161,162 -j ACCEPT
iptables -A FORDWARD -s 10.0.8.0/24 -p udp m multiport –sports 161,162 -j ACCEPT
```