UTN – Facultad Regional Santa Fe

PROYECTO FINAL DE CARRERA

Diseño e implementación de solución WIFI para Municipalidad de la Ciudad de Santa Fe

Alumno: Juan Ignacio Vanney
Director: Ing. Gabriel Filippa

2020

1. Introducción 3

1.1. La organización 3

1.2. Necesidad 3

1.3. Ámbito 4

1.4. Aportes 4

1.5. Objetivos Generales 5

1.6. Objetivos Específicos 5

1.7. Alcance 5

2. Metodología 6

2.1. Recursos Asignados 6

2.2. Cronograma 7

3. Relevamiento 9

3.1. Relevamiento de documentación 9

3.2. Relevamiento del equipamiento y cableado existente 9

3.3. Relevamiento de requerimientos por piso 10

3.4. Aspectos destacados 11

3.5. Mediciones de la situación actual y proyección a futuro 11

4. Selección de tecnologías y estándares 16

4.1. Wireless Controller 16

4.2. Solución de Firewall 18

4.3. Solución como un todo 20

4.4. Solución DHCP 20

4.5. Solución DNS 20

4.6. Solución de monitoreo 21

4.7. Otras Herramientas 22

4.8. Estándares y protocolos destacados 23

5. Diseño de la solución 28

5.1. Santafeciudad 29

5.2. Redmuni 33

5.3. Diseño físico de la solución 37

6. Implementación de la solución. 45

6.1. Cableado e instalación física de dispositivos. 45

6.2. Puesta en marcha de equipos y servicios 47

7. Transferencia y resultados 66

7.1. Ajuste de canales y potencias 66

7.2. Ajuste sobre el uso del espectro 67

7.3. Monitoreo de uso de enlace y cantidad de usuarios y autorización 69

7.4. Testeo de calidad del servicio 71

7.5. Notificaciones 72

7.6. Reportes de equipos 73

7.7. Capacitación 74

7.8. Transferencia y soporte 75

8. Conclusiones 76

9. Glosario 78

10. Bibliografia 83

11. Anexos 85

Costos de equipamiento y cableado 86

12. Anexo Implementación de la solución. 87

12.1. Cableado e instalación física de dispositivos 87

12.1.1. Ejemplo reporte de certificación de cableado 87

12.2. Puesta en marcha de equipos y servicios 89

12.2.1. Instalación del servidor Wireless controller y Certificado Wildcard 89

12.2.2. Archivos de configuración para el servidor DNS 90

12.2.3. Instalación y configuración de Webmin 92

12.2.4. Archivos de configuración para el servidor DHCP 92

12.2.5. Archivo de configuración switch de distribución 98

12.2.6. Archivo de configuración switch en centro de cableado y Datacenter 100

1. Introducción

En este capítulo introductorio, se presenta el análisis de la problemática y su contexto, los fundamentos, alcances y objetivos del presente proyecto final de carrera además de los principales sus principales aportes.

1.1. La organización

La Municipalidad de la ciudad de Santa Fe, es la organización que se encarga de la administración local en la ciudad y la población que habita la misma. Su misión consiste en promover políticas de transparencia y acceso a la información, para poder proporcionar de manera eficiente lo solicitado por los ciudadanos a fin de transparentar la gestión municipal y lograr el desarrollo de un modelo de gestión de calidad así como de rendición de cuentas que propicie la participación ciudadana.

En este marco se encuentra el área de infraestructura, la misma depende del departamento de informática.

El presente proyecto involucró principalmente al área de infraestructura, encargada de brindar servicios a toda la organización.

A nivel emplazamiento físico, la solución como tal va a ser puesta en marcha en el edificio del correspondiente palacio municipal situado en la calle Salta 2951, Santa Fe.

1.2. Necesidad

El principal motor que origina los requerimientos para este proyecto radica en la limitada cobertura de conectividad inalámbrica actualmente disponible dentro del palacio municipal. Esto surge debido a la existencia de soluciones parciales siendo las mismas implementadas bajo demanda y con equipos de uso doméstico (no adecuados para el entorno mencionado).

El constante crecimiento del uso de dispositivos móviles y de prácticas como "bring your own device", hacen que las implementaciones de redes inalámbricas se vuelvan cruciales para el funcionamiento en la gran mayoría de las organizaciones. Dada la naturaleza de las soluciones inalámbricas se debe prestar atención especial a las cuestiones de seguridad.

Además, se busca que este tipo de soluciones sean capaces de atender a una gran cantidad de dispositivos y usuarios, ofreciendo una experiencia lo más parecida al uso de la red cableada tradicional.

El correcto diseño e implementación de la solución WiFi, permitiría ofrecer un servicio acorde a las necesidades actuales, homogeneizando el servicio existente y, además, constituiría una base a nivel infraestructura para la implementación futura de diversos servicios adicionales.

1.3. Ámbito

El proyecto como tal, se realizará en el marco del llamado proyecto final de carrera, por lo cual se ven afectadas, tanto la materia del mismo nombre como el Departamento de Sistemas de Información.

Además, dado que este proyecto aborda una problemática particular planteada por la entidad administrativa, se verá afectado parte del personal del municipio en diversos estamentos y áreas. Por otro lado, el proyecto como tal va a ser ejecutado en la organización ICOP Santa Fe S.R.L. por lo que involucra también a parte del personal de la misma.

El proyecto se va a ejecutar tanto en las oficinas de ICOP Santa Fe S.R.L como en el Palacio Municipal de la ciudad de Santa Fe.

1.4. Aportes

Con la realización de este proyecto se espera aportar al Municipio y la comunidad un conjunto de servicios que les permita a sus usuarios desarrollar de manera eficiente sus tareas de recepción, creación y transmisión de información, logrando así, la comunicación de diversos dispositivos de manera inalámbrica. Desde un punto de vista del crecimiento personal de quien lleva a cabo el proyecto, se espera que el mismo constituya parte importante de la formación como Ingeniero en Sistemas de Información. Además se espera que permita afianzar, aplicar y llevar a la práctica muchos de los conocimientos adquiridos durante el cursado de la carrera. Otro punto importante es la intención de aprovechar la oportunidad para conocer y aprender tanto nuevas herramientas como tecnologías las cuales podrían ser útiles para otros proyectos futuros.

1.5. Objetivos Generales

Diseñar, implementar y probar una solución de conectividad inalámbrica para dar servicio a todo el palacio municipal.

1.6. Objetivos Específicos

- Relevar e identificar dificultades inherentes a la infraestructura actual.
- Investigar tecnologías que mejor se adecuen al contexto del problema para llegar a una solución acorde.
- Implementar la solución como tal, generando el mínimo impacto posible para los usuarios.
- Implementar herramientas que permitan el monitoreo y seguimiento de la solución planteada.
- Realizar la transferencia de conocimientos necesaria para que el departamento de sistemas pueda administrar la solución.

1.7. Alcance

Se incluye dentro del alcance del presente proyecto, la adecuación física y lógica en la infraestructura actual para brindar el servicio, junto con la puesta en marcha de los servicios asociados requeridos tanto para garantizar su funcionamiento como para su realizar el mantenimiento.

2. Metodología

La metodología a ser utilizada corresponde a una metodología ad-hoc, ya que las tareas fueron diagramadas exclusivamente para este proyecto.

Las partes interesadas realizaron reuniones periódicas para definir la metodología de trabajo y un cronograma acorde. De dichas reuniones se definieron las etapas del proyecto y las tareas para concretar dichas etapas.

Las etapas definidas fueron las siguientes:

- Etapa 1: Relevamiento.
- Etapa 2: Diseño de la Solución.
- Etapa 3: Implementación de la solución.
- Etapa 4: Transferencia y monitoreo.

Para más detalle se puede consultar la planificación incluida en una sección posterior.

NOTA: Las estimaciones de esfuerzo requerido para cada tarea, fueron obtenidas en base a experiencia en proyectos realizados con anterioridad.

2.1. Recursos Asignados

Los recursos humanos involucrados en el proyecto son:

- Vanney, Juan Ignacio en el rol de Diseñador e Implementador.
- Personal del área de Instalaciones de ICOP Santa Fe SRL.
- Ing. Gabriel Filippa en el rol de Director del Proyecto.

Además en el rol de cliente/interesado incluimos a:

- Alejandro Temporelli – Jefe Dpto. Infraestructura de Redes de la Municipalidad de la ciudad de Santa Fe.

La disponibilidad de los involucrados es la siguiente:

- Vanney, Juan Ignacio: 20 horas semanales.
- Director de proyecto: 2 horas semanales.
- Cliente: 5 horas semanales.

2.2. Cronograma

Nombre de tarea	Duración	Comienzo	Fin
Proyecto	**162 días**	**lun 05/11/18**	**mar 18/06/19**
Inicio	0 días	lun 05/11/18	lun 05/11/18
Etapa 1: Relevamiento	**40 días**	**lun 05/11/18**	**vie 28/12/18**
Relevamiento de equipamiento y cableado existente	15 días	lun 05/11/18	vie 23/11/18
Relevamiento de necesidades por área/piso	5 días	lun 26/11/18	vie 30/11/18
Relevamiento de planos y documentación	10 días	lun 03/12/18	vie 14/12/18
Investigación de tecnologías y estándares	10 días	lun 17/12/18	vie 28/12/18
Etapa 2: Diseño de la solución	**21 días**	**lun 31/12/18**	**lun 28/01/19**
Diseño lógico de la solución	**6 días**	**lun 31/12/18**	**lun 07/01/19**
Diseño lógico de la solución red MCSF	3 días	lun 31/12/18	mié 02/01/19
Diseño lógico de la solución red Santafeciudad	3 días	jue 03/01/19	lun 07/01/19
Diseño físico de la solución	**6 días**	**mar 08/01/19**	**mar 15/01/19**
Ubicación de los Activos	3 días	mar 08/01/19	jue 10/01/19
Diseño del cableado estructurado	3 días	vie 11/01/19	mar 15/01/19
Requerimientos de hardware y software	6 días	mié 16/01/19	mié 23/01/19
Presentación y aceptación de la solución	3 días	jue 24/01/19	lun 28/01/19
Etapa 3: Implementación de la solución	**81 días**	**mar 29/01/19**	**mar 21/05/19**
Cableado e Instalación física de dispositivos e interconexiones.	20 días	mar 29/01/19	lun 25/02/19
Instalación y configuración de equipos y servicios	**44 días**	**mar 26/02/19**	**vie 26/04/19**
Configuración de Access Point	3 días	mar 26/02/19	jue 28/02/19
Configuración de switch y dispositivos involucrados	10 días	vie 01/03/19	jue 14/03/19
Instalación y Configuración del Servidor Wireless Controller	6 días	vie 15/03/19	vie 22/03/19
Configuración de Gateway/Firewall	12 días	lun 25/03/19	mar 09/04/19
Configuraciones adicionales	**10 días**	**mié 10/04/19**	**mar 23/04/19**
Configuración de perfiles de acceso y uso de recursos	2 días	mié 10/04/19	jue 11/04/19
Servidor de Monitoreo	10 días	mié 10/04/19	mar 23/04/19
Aspectos de Seguridad	**3 días**	**mié 24/04/19**	**vie 26/04/19**
Configuración de perfiles de acceso y uso de recursos	2 días	mié 24/04/19	jue 25/04/19
Configuración de acceso por lista blanca	1 día	vie 26/04/19	vie 26/04/19
Puesta en marcha	**5 días**	**lun 29/04/19**	**vie 03/05/19**
Publicar las redes y comunicar las claves.	2 días	lun 29/04/19	mar 30/04/19
Eliminación de redes inalámbricas que no correspondan a la solución	5 días	lun 29/04/19	vie 03/05/19
Monitoreo y correcciones	**12 días**	**lun 06/05/19**	**mar 21/05/19**
Ajuste de canales y potencias de los Access Point	5 días	lun 06/05/19	vie 10/05/19
Monitoreo de uso de enlace y cantidad de usuarios	4 días	lun 13/05/19	jue 16/05/19

Encuestas informales sobre calidad del servicio	3 días	vie 17/05/19	mar 21/05/19
Etapa 4: Transferencia y monitoreo	**20 días**	**mié 22/05/19**	**mar 18/06/19**
Resultados	**7 días**	**mié 22/05/19**	**jue 30/05/19**
Revisión de Documentación	2 días	mié 22/05/19	jue 23/05/19
Generación de Reportes	5 días	vie 24/05/19	jue 30/05/19
Transferencia	**13 días**	**vie 31/05/19**	**mar 18/06/19**
Capacitación para personal de Área	3 días	vie 31/05/19	mar 04/06/19
Transferencia de la solución y soporte	10 días	mié 05/06/19	mar 18/06/19
Fin	0 días	mar 18/06/19	mar 18/06/19

3. Relevamiento

En este capítulo, se van a desarrollar las metodologías y tareas llevadas a cabo para abordar el relevamiento de la situación actual en lo que respecta a cableado, facilidades o restricciones para realizar tendido del mismo, activos involucrados y todo lo referente a necesidades de cobertura del servicio a ser brindado.

Si bien la reestructuración del cableado y la conectividad entre el data center y los centros de cableado correspondientes a los pisos se encuentra fuera del alcance de este proyecto, es un punto clave a considerar para trabajos futuros y poder asegurar una calidad de servicio acorde tanto a usuarios cableados como a usuarios de las redes inalámbricas. Además, en ocasiones, se pueden reutilizar metodologías de cableado tales como bandejas y cable canales.

3.1. Relevamiento de documentación

Habiendo solicitado al personal e la Municipalidad de Santa Fe toda la documentación asociada, se obtuvo lo siguiente:

- Planos arquitectónicos de todo el edificio.
- Documentación relacionada a equipamiento tanto en los centros de cableado como en el data center.
- Diagramas y planos de cableado.
- Nomenclaturas actualmente utilizadas.

3.2. Relevamiento del equipamiento y cableado existente

Para cumplimentar con este punto, se procedió a realizar un recorrido por todo el edificio visitando cada centro de cableado, empezando por el data center ubicado en el octavo piso del edificio. Para esta tarea fue necesario un trabajo conjunto con el personal del área de infraestructura de la municipalidad para obtener acceso a los racks de cada piso.

Los puntos a ser considerados fueron:

- Uplinks a distribuidores de piso desde el data center (Switch de core).
- Uplinks entre dispositivos en el distribuidor de piso.

- Routers y access point que se encuentren en funcionamiento y sus características (los mismos pueden estar ubicados dentro de los centros de cableado o distribuidos dentro de la planta).
- Disponibilidad de puertos en switch, así como las direcciones IP de todos los activos.
- Aspectos de conflicto para la implementación (dispositivos no administrables, equipos domésticos, inexistencia de puertos disponibles, activos no accesibles, etc).

Como se puede esperar, dicho relevamiento implica un recorrido minucioso por cada planta. Además, es necesario considerar que la documentación suministrada por el personal de la Municipalidad puede encontrarse inexacta o desactualizada.

A modo de resumen, se procede mencionar algunos aspectos considerados de importancia obtenidos del relevamiento realizado:

- Switch de Core.
- Otros switch intermedios y sus interfaces disponibles.
- Puerta de enlace de la red interna y hardware que realiza las veces de firewall.
- Servidores y equipos que prestan servicios de DHCP y DNS.
- Puertos que brindan conectividad hacia cada distribuidor de piso.
- Disponibilidad de espacio físico y tomas eléctricas para la instalación de equipos adicionales.
- Sistemas de manejo de cableado de rack y etiquetado.
- Disponibilidad de recursos en hosts de virtualización para nuevas máquinas virtuales.
- Utilización de VLAN para otros propósitos.

3.3. Relevamiento de requerimientos por piso

En lo que refiere a la cantidad de usuarios y sus requerimientos típicos, se interactuó con referentes de cada área para familiarizarse con el tipo de trabajo que se realiza tanto de forma cotidiana como de forma excepcional para así considerar dichas necesidades para la implementación.

La tarea antes mencionada se ejecutó en paralelo al relevamiento de cableado y equipamiento, además se hicieron estimaciones de cantidad de usuarios inalámbricos.

3.4. Aspectos destacados

En cada piso se visitó la ubicación del rack distribuidor de piso donde se encontró gran variedad en lo que respecta a tipos de racks y dispositivos dentro de los mismos.

Por otro lado, debido a la disparidad en el número de usuarios en cada piso y los requisitos particulares de cada área, cada planta cuenta con uno o más switches con capacidad para atender a todas las estaciones de trabajo junto otros dispositivos del piso y las equivalentes de bocas en las respectivas patcheras. Los switches mencionados presentan características dispares, como por ejemplo:

- Switches de 24 o 48 puertos.
- Switches con puertos de velocidades 10/100/1000 y 10/100.
- Switches con interfaces SFP y sin interfaces SFP.
- Switches de diversas marcas (Allied tellesis, Dell, 3Com, HP, etc).

Además, como para el caso anterior se identificaron:

- Switch cabecera de piso (El que cuenta con el uplink de fibra desde el data center).
- Otros switches en cascada y los puertos involucrados en la cascada.
- Disponibilidad de puertos en los switches.
- Disponibilidad de espacio físico y tomas eléctricas para la instalación de equipos adicionales.
- Sistemas de manejo de cableado dentro del rack.

Otra tarea consistió en la realización inspecciones visuales en toda la planta para evaluar tendido de cableado estructurado existente que da servicio a las estaciones de trabajo y la disponibilidad de cable canal, bandejas, pasos de muro, etc. Dicha inspección permitirá posteriormente realizar el diseño del cableado de nuevos equipos.

3.5. Mediciones de la situación actual y proyección a futuro

Las siguientes estimaciones fueron realizadas en base a la información obtenida de equipos en producción, además de contar con aportes brindados por personal del área

de informática de la Municipalidad de Santa Fe. Cabe aclarar que los datos obtenidos han sido ajustados en base a experiencia adquirida en diversos proyectos realizados con anterioridad.

Dicho esto, se partió de la información suministrada por el firewall de core. Dicho equipo actualmente realiza, además de sus tareas inherentes, el balanceo de enlaces a internet y "failover", filtrado de contenido web y aplicaciones. Al mismo se conectan 3 enlaces de 2 ISP distintos, las capacidades de los mismos son las siguientes:

ISP 1 Enlace 1: Bajada 45 / Subida 15.

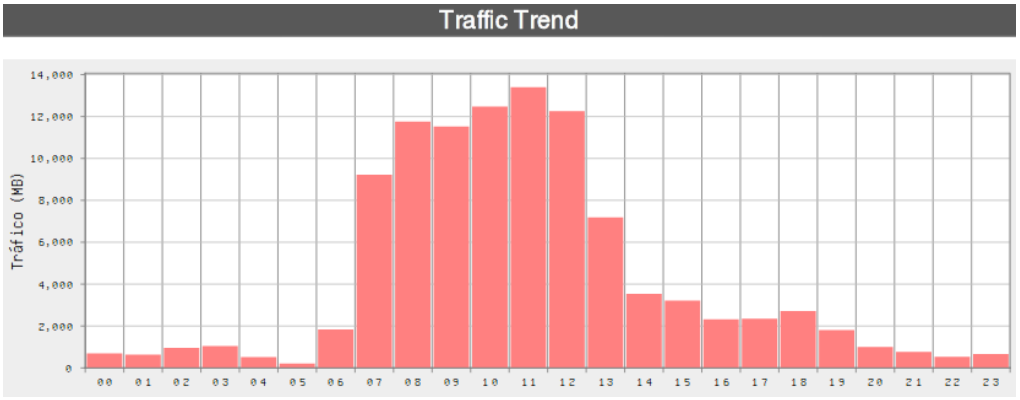
ISP 1 Enlace 2: Bajada 45 / Subida 15.

ISP 2 Enlace 1: Bajada 20 / Subida 15.

Tanto el firewall como los enlaces conectados a él, dan servicios a toda área administrativa del palacio tanto cableada como inalámbrica.

Actualmente existen unos 2000 activos en el palacio municipal, de los cuales se consideran unos 1250 en forma simultánea (habiendo previamente exceptuado impresoras, controles de acceso y dispositivos similares).

En la siguiente imagen, se puede apreciar que el máximo durante un día elegido arbitrariamente.



Como podemos ver, entre las 11:00 hs. y las 12:00 hs, se produce el mayor consumo. Casi llegando casi a un total de 14 MB (112 Mbps). Partiendo de esto, planteamos el siguiente promedio.

Usuarios	Ancho de Banda Acumulado en horario pico	Ancho de Banda estimado por usuario
1250	112 Mbps	0,0896 Mbps

Las estimaciones presentadas a continuación, según los lineamientos del proyecto, fueron divididas en dos apartados:

- Estimaciones para la LAN de trabajo "Red Muni".
- Estimaciones para la red de invitados "santafeciudad".

Estimaciones para la LAN de trabajo "Red Muni"

Para este caso, los dispositivos que serían utilizados de forma inalámbrica, ya son parte de los 1250 considerados en cálculos anteriores y las actividades que se realizan con los mismos, no difiere del promedio de uso.

Además sería coherente considerar la cantidad de dispositivos inalámbricos esperados. La municipalidad cuenta actualmente, en números aproximados, con:

- 149 Notebook
- 31 PCs con placas WIFI
- 78 Teléfonos celulares
- 28 Tablets

Se estima que hay un uso de entre 30 y 40 dispositivos en forma simultánea al día de hoy. Además, se espera que muchos de los dispositivos con capacidades inalámbricas que al día de hoy son utilizado de forma cableada, empiezan a ser utilizados de manera inalámbrica.

Partiendo de estos supuestos se plantean 2 escenarios.

	Descripción del Caso	Cantidad de usuarios conectados	Usuarios Considerados en el calculo	Ancho de banda por usuario	Ancho de banda total
Caso Promedio	Tomando un promedio del uso total máximo de enlaces entre la cantidad total de usuarios.	40	40	89,6 Kbps	3584 Kbps
Caso Extremo	Tomando 30 usuarios que consuman simultáneamente video Full HD.	60	30	870 Kbps	26100 Kbps

Estimaciones para la red de invitados

Respecto a la nueva red para invitados, no existe actualmente el servicio, ni tampoco otro de similares características. Se esperan alrededor de 300 usuarios simultáneos, con sus respectivas restricciones de ancho de banda. Además picos de hasta 500 usuarios en eventos u ocasiones especiales.

Dado que los pisos inferiores van a ser los que absorban la mayor parte de la carga (debido a su tamaño, cantidad de personal municipal y acceso al ciudadano promedio) se considera como requerimiento que los Access Point de dichos pisos sean capaces de atender al menos 150 usuarios cada uno.

Nuevamente, partiendo de estos supuestos, se plantearon 4 escenarios. Los mismos se diferencian por los factores de cantidad de usuarios totales y cantidad de usuarios considerados.

Como se mencionó anteriormente, para este caso se van a aplicar restricciones de ancho de banda por cliente para así mantener equidad entre los clientes y evitar los consumos excesivos.

A continuación, se presenta un cuadro comparativo entre los escenarios mencionados:

	Descripción del Caso	Cantidad de usuarios conectados	Usuarios Considerados en el calculo	Ancho de Banda por usuario	Ancho de banda total
Caso Promedio concurrente	Tomando un caso promedio, utilizando los valores calculados para "Red Muni" y considerando un uso concurrente de todos los usuarios.	300	300	86,6 Kbps	25980 Kbps

Caso Promedio	Tomando un caso promedio, utilizando los valores calculados para "Red Muni", considerando que los usuarios de esta red, en la mayoría de los casos, no hacen uso continuo de la misma. Consideramos que el 30% de los usuarios hace uso del ancho de banda en un momento determinado.	300	100	86,6 Kbps	8660 Kbps
Caso Extremo concurrente	Caso solo teórico, el ancho de banda total va a ser consumido. No hay que asegurar el servicio, si bien es deseable.	500	500	86,6 Kbps	43300 Kbps
Caso extremo	Mismo razonamiento que para el caso promedio, pero considerando una gran cantidad de usuarios.	500	170	86,6 Kbps	14772 Kbps

4. Selección de tecnologías y estándares

En este capítulo se pretende realizar un análisis de los aspectos que deberían ser cubiertos por la solución, seguidos por el análisis de las tecnologías y estándares a ser utilizados. En algunos apartados, además, se ha realizado la comparativa de herramientas y/o productos que se podrían haber abordado.

En base a los objetivos planteados, se procede a detallar los aspectos de la problemática que la solución debería cubrir para funcionar como un todo:

- Wireless Controller
- Access Point y conectividad
- Solución de Firewall
- Solución DNS
- Solución DHCP
- Solución de Monitoreo de activos
- Estándares de Cableado
- Protocolos y estándares de Red

Otro aspecto condicionante, es el acceso a equipos, experiencias en implementaciones previas y además las restricciones presupuestarias.

4.1. Wireless Controller

El primer aspecto a considerar es la selección del Wireless controller ya que dicha decisión condiciona las subsecuentes. Las tecnologías contempladas para este apartado fueron las siguientes:

- Fortinet con su producto Fortigate.
- Ubiquiti Networks con su producto UniFi Controller

Las mismas fueron tenidas en cuenta dados los requisitos del cliente y su disponibilidad presupuestaria (como se dijo anteriormente, la elección de una tecnología por sobre la otra implica no sólo la elección del controlador, sino también

condiciona la adquisición de los access point y el resto de la infraestructura que le da soporte a la red inalámbrica).

A continuación, se realiza una breve descripción de ambas tecnologías y sus respectivas soluciones para la problemática planteada:

- *Fortinet:* Es una organización dedicada a comercialización de software, dispositivos y servicios de ciberseguridad como firewalls, antivirus, prevención de intrusiones y seguridad en dispositivos de usuario. Comercializa soluciones conocidas como NGFW (de la sigla en inglés firewall de nueva generación) las cuales combinan las funcionalidades de firewall, VPN, prevención de intrusiones entre otras.

  Los equipos denominados "Fortigate" corresponden a dispositivos tanto físicos como virtuales que proveen diversas funcionalidades de seguridad (firewall, IPS, filtrado web, etc), además poseen posibilidad de funcionar como wireless controller pudiendo ser combinado únicamente con los access point de la marca Fortinet y así disponer de una gran variedad de opciones para la gestión y monitoreo tanto activos de la infraestructura como clientes WiFi. Algo a destacar es la posibilidad de mantener visibilidad y seguridad a lo largo de toda la red en un solo panel de administración y un solo equipo.

- *Ubiquiti Networks:* Es una organización principalmente dedicada al diseño de hardware de redes inalámbricas, tanto para la comunicación a largas distancias, como para el despliegue de redes WiFi, priorizando la innovación y el alto rendimiento a un bajo coste.

  La línea de productos a ser considerados son los denominados "UniFi", los mismos corresponden a dispositivos WiFi tanto de interior como exterior para edificios o pequeños espacios abiertos. Una vez más, los dispositivos UniFi, son administrados por un wireless controller del mismo nombre (UniFi Controller), el mismo puede actuar en un entorno mixto (combinando productos de la marca con otros).

  Para implementar esta solución, es requisito disponer de un servidor que pueda ejecutar el UniFi Controller (funcionando sobre Linux, Windows o Mac OS). Además, es necesario considerar la adquisición de un equipo que funcione a modo de gateway ya que el controlador por sí mismo no contempla dicha funcionalidad.

Tabla comparativa de los access point:

	Fortinet (Fortigate 100E y FAP 211E)	Ubiquit (UniFi AC pro)
Capacidad para 802.11ac	Si, Wave 2	Si, Wave 1
Control de aplicaciones	Si	Si
Selección de canal automático y potencias	Si	Si
Gestión de Roamming	Si	SI
Portal cautivo	SI	SI
Band Steering	Si	Si
Deteccion de Rogue AP	Si	Si
Multiples WLAN por radio	Hasta 8 por radio	Hasta 8 por radio
Alimentacion PoE	802.3af	802.3af/802.3at
Complejidad de implementación y mantenimiento	Baja	Media
Administración basada en web	Si	Si
Apto para uso exterior	No	Si
Mesh	Si	Si
Max tx power	2,4 GHz: 23 dBm 5 GHz: 24 dBm	2,4 GHz: 22 dBm 5 GHz: 22 dBm
Antenas	4 intenas + 1 Bluethoot	3 internas
Clientes concurrentes	512	250+
Control sobre Usuarios/Dispositivos	Si	Si

4.2. Solución de Firewall

En lo que respecta a solución de firewall y filtrado, los tres proveedores considerados para formar parte (importante) de la solución fueron:

- Mikrotik
- Sophos
- Fortinet

Dado que las soluciones consideradas difieren bastante tanto en funcionalidades como en el costo a considerar para su implementación, se limitó a hacer una breve

descripción de cada una. Siendo las mismas presentadas al cliente con sus respectivos costos y sus beneficios en lo que respecta a características y administración. En base a los requisitos previstos para el proyecto, el cliente puede volcarse por una de ellas siendo la solución acorde al presupuesto con el que se dispone.

- *Mikrotik:* Como la solución más económica, pero a su vez la más difícil de administrar y con menor capacidad de filtrado en lo que respecta a aplicaciones y contenido web. No se requiere licencia para su funcionamiento.

  Mikrotik es una compañía proveedora de hardware y software para la creación de redes. La compañía dispone de un sistema operativo basado en el núcleo de Linux conocido como RouterOS. Dicho sistema operativo puede correr tanto en una PC como en placas dedicadas, y provee una gran versatilidad en lo que respecta a configuraciones. RouterOS cuenta con una amplia comunidad y diversos foros dedicados.

- *Sophos:* Como la solución intermedia, se requiere licencia paga para mantener los servicios activos de filtrado web y de aplicaciones. Su costo es moderado respecto al de otras soluciones.

  Sophos es una compañía de hardware y software de seguridad, se dedica a desarrollar productos para seguridad en la red, seguridad para dispositivos móviles, encriptación y manejo unificado de amenazas. La línea de productos a ser considerada para este proyecto corresponde a la llamada "XG Firewall" (Next Generation Firewall).

- *Fortinet:* Como la solución más completa (y la más costosa), en la sección anterior ya se introdujo a Fortinet como solución integrada, en la cual se cubren los requisitos propuestos para este proyecto. La desventaja es que requiere contrato de mantenimiento de equipo y servicios de filtrado web/aplicaciones, como para el uso de servicios adicionales.

  La línea de productos a considerar sería la antes mencionada "Fortigate" por lo que estaríamos hablando de un equipo que unifique las tareas de firewall y seguridad con las de wireless controller.

4.3. Solución como un todo

- En el caso de seleccionar a Fortigate como wireless controller, toda la solución debería ser orientada a los equipos Fortinet teniendo que considerar tanto los access point como el firewall que incluye entre sus funcionalidades el wireless controller.
- En el caso de seleccionar a UniFi como wireless controller, en lo que respecta a solución de gateway o firewall estarían las siguientes opciones:
    - Mikrotik
    - Sophos

Si bien se podrían hacer combinaciones que incluyan Fortinet en combinación con UniFi, como ya se mencionó, no es recomendable debido a las condiciones de ecosistema entre productos Fortinet.

4.4. Solución DHCP

Los servidores DHCP pueden ser implementados tanto en los equipos de firewall (cualquiera de los antes mencionados), dentro del servidor/wireless controller o disponer de un servidor DHCP dedicado (Basado en Windows o Linux)

Para el caso de utilizar un servidor dedicado, si bien existen varias posibilidades, todos ellos brindan funcionalidades muy parecidas y solo difieren en aspectos de su configuración. La opción más conocida y utilizada es DHCPD.

DHCPD, de las siglas en inglés (Dynamic Host Configuration Protocol Daemon), consiste en una implementación de servidor DHCP desarrollada por la organización sin fines de lucro ISC (Internet System Consortium) para sistemas operativos BSD, Linux y Solaris. La misma es una de las primeras implementaciones y se encuentra disponible desde el año 1999.

4.5. Solución DNS

Al igual que para el caso del apartado anterior, el/los servidores DNS pueden ser implementados en equipos de propósito general o en servidores dedicados. Se optó por utilizar la herramienta BIND.

BIND: Es un servidor DNS open source ampliamente utilizado en sistemas Unix y provee todas las funcionalidades requeridas para la mayor parte de las

implementaciones DNS, entre ellas el uso de caché, balanceo de carga y notificaciones, entre otros. Se presenta como una solución estable, multiplataforma y con una amplia comunidad.

4.6. Solución de monitoreo

A la hora de abordar las posibilidades en lo que respecta a una solución de monitoreo se limitó al análisis de dos de las más utilizadas:

- Zabbix
- Nagios

Zabbix: Es un sistema de monitorización de redes que permite registrar el estado de servicios de red, servidores y hardware de red. Entre sus características ofrece:

- Chequeos simples que pueden verificar la disponibilidad y el nivel de respuesta de servicios como SMTP o HTTP, sin necesidad de instalar ningún software sobre el host a monitorear.
- Un agente Zabbix que puede ser instalado tanto en Linux como en Windows, para monitorizar diversas variables.
- Soporte para monitorización vía protocolos SNMP, TCP, ICMP, IPMI, JMX, SSH, telnet, entre otros.
- Soporta gran variedad de mecanismos de notificación en tiempo real.

Funcionalidades destacadas:

- Alto rendimiento y capacidad de monitorear una extensa cantidad de dispositivos.
- Auto descubrimiento de servidores y dispositivos de red.
- Monitorización distribuida (a través de agentes) y una administración web centralizada.
- Agentes nativos en múltiples plataformas.
- Posibilidad de monitorización sin agentes.
- Una interfaz web con gran poder para dar visibilidad de todos los equipos/servicios monitoreados.

Nagios: Es un sistema de monitorización de redes de código abierto, permite realizar monitoreo tanto sobre equipos como servicios. Es ampliamente utilizado y

proporciona gran versatilidad de uso, generación de alertas y envío de las mismas. Entre sus características ofrece:

- Monitorización remota a través de túneles SSL cifrados o SSH.
- Diseño simple de plugins, lo que permite al usuario desarrollar los propios acorde a sus necesidades para el monitoreo de servicios.
- Chequeo de servicios paralizados
- Posibilidad de definir jerarquías de red (para distinguir entre host caídos y hosts inaccesibles).
- Amplia integración con servicios de notificaciones a usuarios ante caídas de servicios.
- Soporte para monitorización a través de SMTP, POP3, HTTP, NNTP, ICMP y SNMP.
- Disponibilidad de plugins de monitoreo de hardware para varios sistemas operativos.
- Posibilidad de definir disparadores que ejecuten tareas frente a eventos registrados.
- Soporte para la rotación automática de registros.
- Interfaz web con posibilidad de mostrar gráficas, eventos y reportes de los mismos.

4.7. Otras Herramientas

Webmin: Es una interface web para administradores de sistemas basados en Unix la cual presenta gran variedad de configuraciones, desde gestión de cuentas de usuario, gestión de servidores Apache, DNS, archivos compartidos entre otros. Utilizando esta interfaz se elimina (en la mayoría de los casos) la necesidad de editar de forma manual los archivos de configuración. Herramienta tenida en cuenta en vista de un posterior mantenimiento de la solución por personal de la Municipalidad, por su interfaz intuitiva y poderosa. Permite administrar tanto el servidor DHCP como el servidor DNS que se requiere para la solución.

Ubuntu: Es un sistema operativo de código abierto para computadoras, consiste en una distribución de Linux basada en Debian. Es patrocinado por la empresa Canonical, manteniendo el sistema operativo de manera gratuita y siendo financiada por servicios relacionados como soporte sobre el sistema operativo. La comunidad de Ubuntu participa activamente escribiendo código, solucionando fallas, probando versiones inestables del sistema, etc. Además existen diversos mecanismos para que los propios usuarios puedan proponer y votar ideas a ser desarrolladas a futuro. Existen versiones pensadas para funcionar en servidores, en las que se dispone de diversas funcionalidades preinstaladas.

4.8. Estándares y protocolos destacados

Para este apartado, se propone una breve descripción de los estándares y protocolos a ser utilizados. Cabe aclarar que de los mencionados se desprenden muchos otros que, para esta sección, no se van a detallar.

ANSI/TIA/EIA-568: Es un estándar que tiene como objetivo permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información sobre los productos de telecomunicaciones que posteriormente se instalarán. La norma tiene como objetivo garantizar que los sistemas que se ejecuten sobre la instalación soportarán todas las aplicaciones de telecomunicaciones presentes y futuras por al menos 10 años. Además define:

- Requerimientos mínimos para el cableado.
- Topología a ser utilizada.
- Distancia máxima de los cables.
- Rendimiento de los componentes.
- Tomas y conectores de telecomunicaciones.

IEEE 802.1Q: Es el protocolo de red que implementa mecanismos de VLAN. VLAN es un acrónimo de "LAN virtual" y corresponde a un método para poder crear diversas redes lógicas sobre una misma red física. Las VLAN son utilizadas para reducir los dominios de colisión de las redes, aumentando la eficiencia y escalabilidad de la misma. 802.1Q se basa en añadir una etiqueta a las tramas Ethernet con la que se diferencia el tráfico; cuando una trama etiquetada llega a un conmutador con soporte

para VLAN, este utiliza el ID de VLAN como un índice de tabla para averiguar a cuáles puertos se debe enviar la trama.

Los motivos que llevan a querer implementar 802.1Q para el problema planteado son los siguientes:

- Aspectos de seguridad, como la necesidad de mantener el tráfico separado entre las distintas redes (tanto inalámbricas como cableadas).
- Aspectos de administración de redes, permitiendo el monitoreo y administración de equipos separado del tráfico de usuario.
- Flexibilidad y relativa simplicidad para implementación de nuevos servicios sobre la infraestructura existente.

IEEE 802.11: Corresponde a la familia de estándares que define las redes de área local inalámbricas o WLAN (por sus siglas en inglés Wireless Local Area Network). Las especificaciones que contiene esta familia de estándares proporcionan la base para los productos que hacen uso de la marca Wi-Fi.

Dado que parte de la problemática planteada consiste en proveer una solución sobre la tecnología Wi-Fi, resulta imperativo la utilización de la familia 802.11.

Los estándares que pertenecen a la familia 802.11 se caracterizan por estar basados en una serie de técnicas de modulación por medio del aire utilizando un mismo protocolo básico. Dichos estándares se pueden agrupar según la banda del espectro electromagnético en la que funcionan (2,4 GHz y 5 GHz). Cada banda posee variedad de protocolos asociados y los mismos poseen sus restricciones en lo que respecta a velocidades teóricas, amplitud del espectro que utiliza, amplitud de canales, alcance, etc.

A continuación se incluye una tabla comparativa entre las dos bandas mencionadas

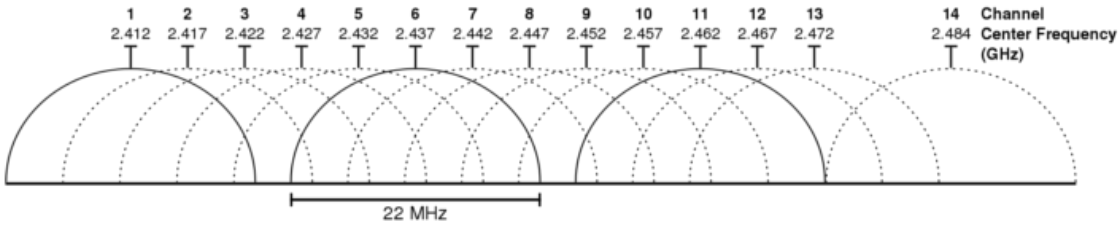
	Banda 2,4 GHz	Banda 5 GHz
Canales no superpuestos	3	21
Dispositivos compatibles	Solo los más modernos	La gran mayoría
Interferencia	Mucha (Telefonía inalámbrica, dispositivos	Poca (Banda poco poblada)

	Bluethoot, Hornos de microondas)	
Velocidad Máxima	Hasta 150 Mbps (300 Mbps teóricos)	Hasta 1 Gps (1,7 Gps teóricos)
Rango	Amplio rango	Rango limitado
Estándares	IEEE 802.11b, 802.11g, 802.11n (B, G y N)	IEEE 802.11a, 802.11n, 802.11ac (A, N, AC)

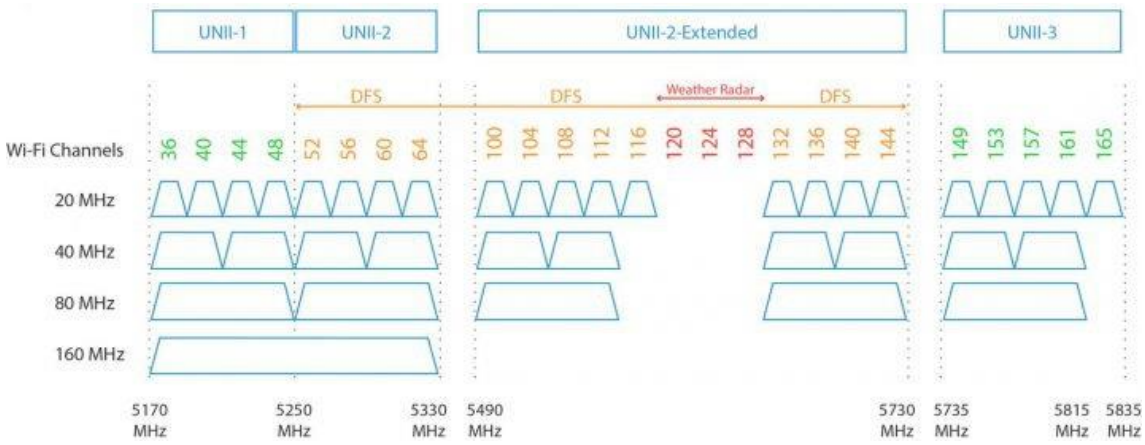
Canales no superpuestos:

Para el caso de la banda de 2,4 GHz, hay definidos un total de 11 canales utilizables (ancho de banda de 22 MHz por canal). De los 11 canales, no todos se encuentran completamente independientes, sino que muchos de ellos se encuentran solapados por lo que se interfieren mutuamente. Para evitar esta superposición, se debe dejar 5 canales de separación entre ellos, lo que deja un total de 3 canales completamente independientes. Por convención se utilizan los canales 1, 6 y 11.

En el siguiente diagrama se pueden ver los canales correspondientes a la banda de 2,4 GHz, siendo resaltados los canales 1, 6 y 11 antes mencionados.



Para el caso de la banda de 5 GHz, hay definidos 21 canales sin superposición alguna (de 20 MHz de ancho de banda) como se puede apreciar en la siguiente imagen:



IPSEC: Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre IP autenticando y/o certificando cada paquete en un flujo de datos. También incluye protocolos para el establecimiento de claves de cifrado. Los protocolos IPsec actúan en la capa de red del modelo OSI.

IPSEC consta de tres protocolos:

- Authentication Header (AH): Permite la autenticación del remitente, la integridad de los datos y la protección contra el reenvío.
- Encapsulating Security Payload (ESP): Permite el cifrado de datos para garantizar la confidencialidad de los mismos.
- Security Association (SA): Permite definir un conjunto de políticas y claves para establecer y proteger la conexión.

Existen dos modos básicos de operación para IPSec, modo túnel y modo transporte.

En el funcionamiento en modo túnel, todo el paquete IP (carga útil y cabecera) es cifrado y autenticado, siendo encapsulado en un nuevo paquete para ser enrutado. Este modo es utilizado para comunicaciones red a red permitiendo implementar VPN. Gran cantidad de enrutadores de borde (por no decir todos), soportan la utilización de VPN a través de IPSec.

SNMP: Protocolo simple de administración de red o por sus siglas en inglés (Simple Network Management Protocol) corresponde a un protocolo de capa de aplicación, diseñado para facilitar el intercambio de información de administración entre dispositivos de red.

SNMP presenta las siguientes características de funcionamiento:

- Uno o más equipos administrativos (gerentes) tienen la tarea de supervisión o gestión de un grupo de host o dispositivos.
- En cada sistema gestionado se ejecuta un componente llamado agente, el cual es el encargado de reportar la información a través de SNMP al gerente.
- Las variables accesibles a través de SNMP presentan una organización jerárquica, tanto su información como su ubicación dentro de la jerarquía se encuentran definidos por bases de datos de gestión (MIB).

5. Diseño de la solución

En este capítulo se pretende detallar los aspectos inherentes al diseño de la solución tanto desde un punto de vista lógico, como desde el físico. Por otro lado, se incluye un apartado en el cual se detalla los requerimientos adicionales en hardware y software para poder realizar la implementación. Una vez formalizada la solución la misma debe ser presentada al cliente para ser aprobada.

Debido a que se pretende realizar el despliegue de dos redes inalámbricas (WLAN) totalmente independientes, con uso y objetivos muy diferentes, se requiere individualizar el planteo para cada una de ellas. Las mismas son:

- RedMuni
- Santafeciudad

El punto principal a definir corresponde a la elección del wireless controller, ya que seleccionando una tecnología por sobre otra, se condicionan gran parte de los factores involucrados para el desarrollo de la solución.

Dicho esto, se optó por utilizar el producto de Ubiquiti (analizado en detalle en el capítulo anterior), siendo un factor determinante para su elección el costo total de la solución.

Consideraciones de la solución:

- Se requiere configurar VLAN en todos los switch que sean o vayan a ser parte de la infraestructura dedicada a la solución (los mismos deben ser compatibles con el protocolo IEEE 802.1Q)
- Disponer de recursos de hardware para virtualizar los servidores, para este caso es necesario un servidor UniFi (utilizado como software de base Ubuntu Server).
- Adquirir tanto access point como switch de la marca Ubiquiti.

Requerimientos asociados:

- Realizar el montaje y cableado a cada uno de los access point.
- Disponer de un medio para alimentar los access point (utilizando tanto switch PoE como Inyectores PoE)

A continuación se procede a indicar los componentes a considerar en las dos WLAN mencionadas. Para cada una de ellas, se realiza un detalle de los aspectos relacionados con:

- Networking y aspectos generales
- Aspectos de ruteo
- Solución de Firewall
- Servidor DHCP
- Servidor DNS
- Aspectos de Seguridad
- Perfiles de usuario

5.1. Santafeciudad

Para este caso, hay que considerar el despliegue completo de la solución, junto con todos los servicios asociados para su funcionamiento.

Networking y aspectos generales: Se propone la utilización de VLAN para mantener independiente el tráfico correspondiente a la red "pública", haciendo uso de la infraestructura de la municipalidad. El tráfico de esta red, corresponde a una nueva LAN, incorporando de forma independiente los servicios de DHCP, DNS, Firewall, entre otros.

Aspectos de ruteo: Para esta red, se utilizará un firewall en un esquema de alta disponibilidad haciendo las veces de enrutador. Se debe considerar tanto el ruteo hacia internet, como hacia el wireless controller (el mismo va a estar disponible en la red de administración atendiendo peticiones).

Solución de Firewall: Para este apartado, se propone la utilización de dos equipos de la marca Sophos como firewall de borde en un esquema de alta disponibilidad, permitiendo gestionar reglas de navegación, perfiles de aplicaciones y filtros web para los dispositivos de la red "pública". A dicho firewall se conectarán 2 enlaces de diferentes proveedores en un esquema de balanceo de carga y a prueba de fallos. Este equipo además debe llevar una interfaz en la red de administración para permitir el acceso a servicios del wireless controller.

Servidor DHCP: El servidor DHCP va a ser implementado dentro del Firewall mencionado debido a que el equipo brinda este servicio y su implementación es relativamente simple. Se pretende que el equipo pueda proveer una gran cantidad de direcciones IP de manera dinámica y con una persistencia (conocida como "lease time") de no más de una hora.

Servidor DNS: El servidor DNS va a ser implementado dentro del servidor wireless controller. Donde las peticiones que no se puedan resolver, serán reenviadas a otro servidor DNS externo. Cabe aclarar que la dirección del servidor DNS será difundida por el servidor DHCP al momento de responder una petición de asignación de IP.

Seguridad de acceso: El SSID correspondiente, se va a encontrar visible (Difundido) y sin protección por contraseña para facilitar el acceso a cualquier usuario que así lo requiera. Será requisito para su uso la aceptación de los términos y condiciones presentados en el portal cautivo.

Perfil de usuario: Se pretende mantener restricciones en lo que respecta a ancho de banda disponible por usuario. Esto puede implementado tanto a nivel firewall, como a nivel wireless controller. Para este caso, se considera más adecuada la implementación a través del wireless controller fijando en principio un límite de 1024 Kbps de bajada y 512 Kbps de subida por usuario. Otro detalle es que, utilizando el portal cautivo antes mencionado, se puede restringir el tiempo que un usuario se encuentra conectado al servicio y consumiendo ancho de banda. Una vez vencido el plazo preestablecido (1 Hora), el usuario deberá pasar nuevamente por el portal cautivo y aceptar los términos y condiciones.

Otras consideraciones:

- El diseño planteado contempla la utilización de una VLAN dedicada al manejo del todo el tráfico de navegación de la red santafeciudad, dicha VLAN debe ser trasladada desde el equipo de firewall por todos los switch de la infraestructura hasta llegar a los access point. Aprovechando esta tarea, se propone además, realizar la configuración de algunas VLAN adicionales para una rápida puesta en marcha de servicios nuevos (similares a los que incluye este proyecto).
- Se propone la instalación de un certificado SSL en el servidor, ya que el mismo permite comprobar la autenticidad del servidor web que presenta el portal cautivo.

Diagrama de conectividad para santafeciudad

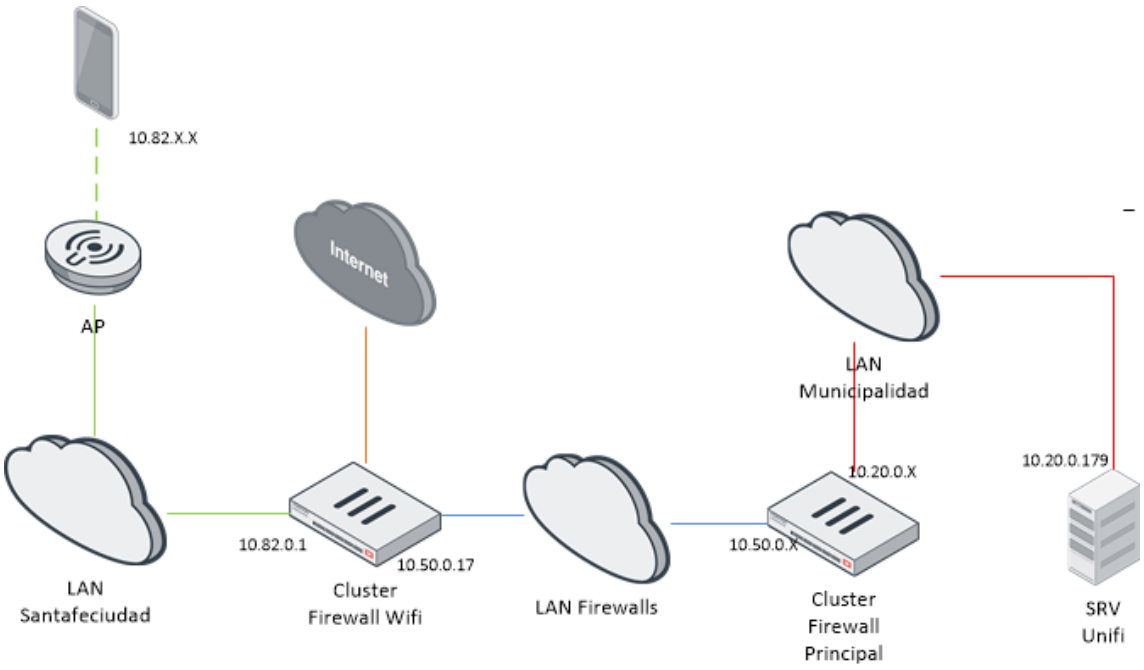
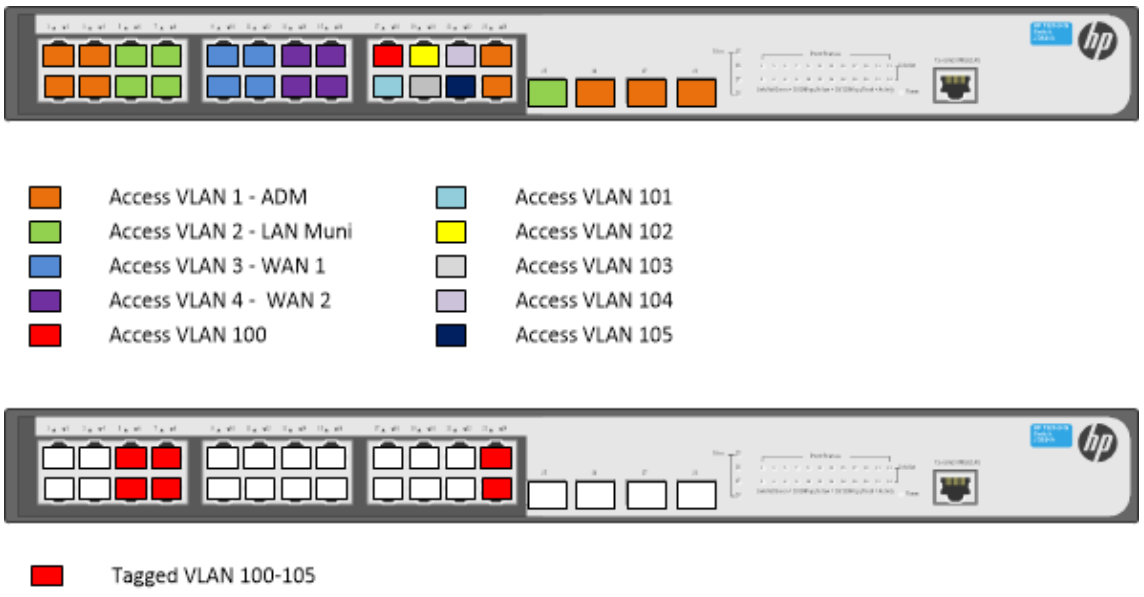
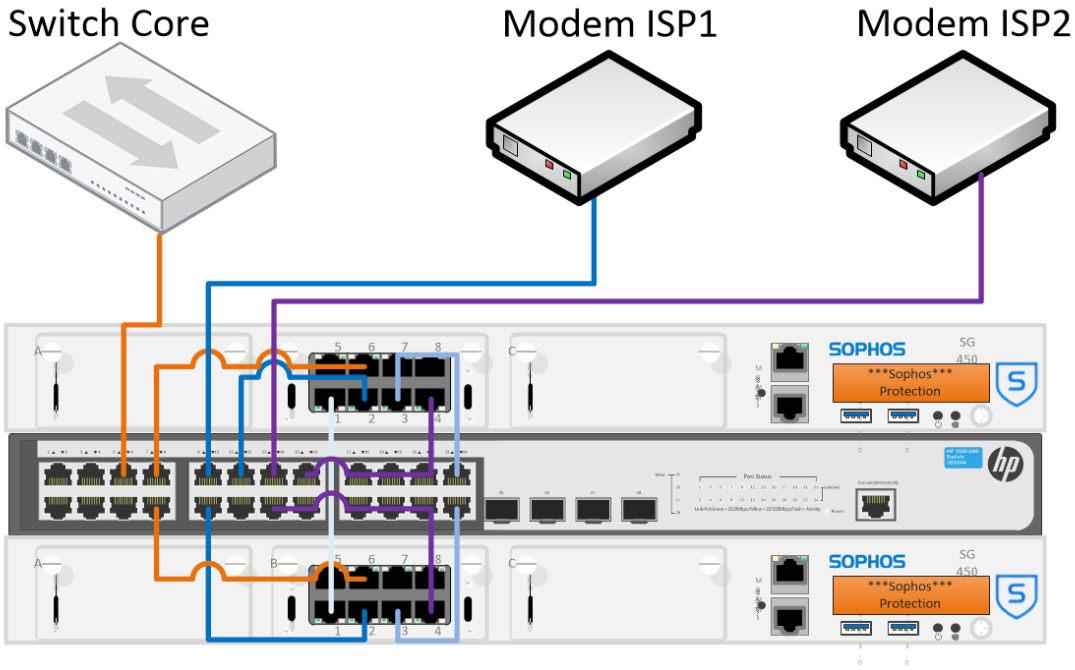


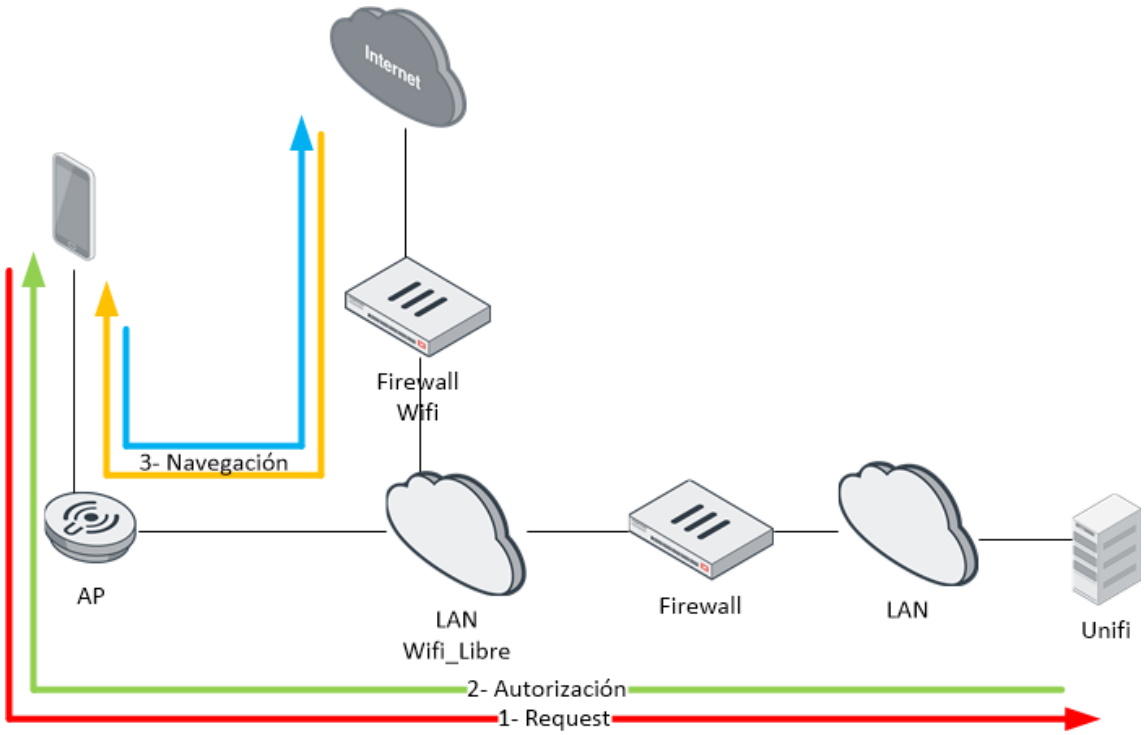
Diagrama de VLAN para switch HA



Conectividad simplificada para el Cluster Firewall



Funcionamiento del portal cautivo



Diseño DHCP

Para el diseño del servidor DHCP, se consideraron cubrir los usuarios estimados, pero además permitir que se pueda escalar la solución en iteraciones futuras sin realizar mayores cambios.

Dada la naturaleza cambiante del usuario promedio de esta red, se propone un tiempo cesión de direccionamiento de 1 hora, considerando el mismo coincidente con el tiempo de autorización que otorga el antes mencionado portal cautivo.

Dirección de Red	10.82.0.0
Rango IP usable	10.82.0.1 - 10.82.63.254
Dirección de Difusión	10.82.63.255
Mascara de subred	255.255.192.0
Número de direcciones usables	16382

5.2. Redmuni

Debido a que esta red debe ser una extensión de la LAN cableada actualmente desplegada, se propone escalar los servicios ya utilizados tales como servidores DHCP y servidores DNS además de respetar los equipos que realicen el ruteo, sirvan de puerta de enlace predeterminadas así como los servicios que proveen internet a la LAN realizando las modificaciones pertinentes para que sean funcionales a los dispositivos WiFi (IEE 802.11) que así lo requieran.

Networking: Por cuestiones de minimizar la complejidad para la administración, se optó por mantener las subredes preexistentes. Los access point, switch y wireless controller, se encuentran todos en una subred de administración, la cual agrupa el acceso a las interfaces IP de administración de los dispositivos pertenecientes a la LAN.

Ruteo: Para esta red, se mantienen las condiciones de la LAN, por lo que el encargado de enrutar esta red es el switch de core.

Firewall: La red cuenta con dos equipos marca Fortinet como firewall de borde en un esquema de alta disponibilidad. Dichos equipos van a ser utilizados para la solución, siendo necesaria la creación de reglas de navegación, perfiles de aplicaciones y perfiles de filtros web para los dispositivos WiFi. A dicho firewall se encuentran conectados 3 enlaces de 2 proveedores distintos funcionando en un esquema de balanceo de carga (además de implementar tolerancia a fallos). Este equipo, también permite el acceso a la DMZ desde la LAN, ofreciendo acceso a diversos servidores y servicios (Aplicativos, Servidores web, Servicios de Mail, etc.)

Servidor DHCP: El esquema actual presenta un solo servidor Ubuntu virtualizado corriendo DHCPD y siendo el mismo administrado a través de la interfaz web llamada webmin. Se propone implementar un segundo servidor DHCP bajo el mismo esquema, funcionando el mismo en el caso que falle el primario. Dicho servidor debería ser desplegado en un host diferente que el primario. La metodología actual consiste en una asignación DHCP estática para todos los host, por lo que cada host debe ser dado de alta con su dirección física (MAC) para poder recibir su dirección IP desde el servidor.

Servidor DNS: El esquema actual presenta un único servidor DNS funcionando en el Firewall de borde, se propone la implementación de un servidor DNS adicional y dedicado, en principio, a los dispositivos WiFi. Nuevamente, utilizando un servidor Ubuntu virtualizado y corriendo BIND DNS. No se prevé un esquema de replicación para este servidor DNS.

Seguridad en el acceso:

- Difusión de SSID: Debido a requerimientos del cliente, se va a realizar la difusión del SSID mencionado.

  Ventajas: Permite una conexión simple para los clientes y evita que los administradores, en la mayoría de los casos, deban agregar manualmente la información del SSID en cada dispositivo que requiera conectarse.

  Desventajas: Ocultar el SSID, puede considerarse un elemento que refuerza la seguridad de la red, ya que el común de los dispositivos no intentará conectarse a la red de manera automática.

Nota: Cabe aclarar, que un atacante con conocimiento, que se lo proponga, puede a través de herramientas llamadas "Wireless Sniffer", obtener la información oculta del SSID.

- Protección de acceso: Utilización de WPA2 (AES/CCMP)

  Ventajas: WPA2 provee un aspecto de seguridad extra a los usuarios WiFi otorgando acceso a través de una clave compartida, además, WPA2 posee amplia compatibilidad con los dispositivos.

  Desventajas: No hace un uso de red completamente eficiente (se genera una carga extra en las tareas de cifrar y descifrar). Por otro lado, recientemente se ha descubierto una vulnerabilidad sobre este protocolo por lo cual es necesario mantener actualizados los activos involucrados.

  Nota: Se podría considerar que la opción más adecuada para este apartado sería utilizar WPA2-Enterprise autenticando a cada dispositivo contra un servidor RADIUS. Para este caso particular existen las siguientes restricciones a la hora de implementar WPA2-Enterprise:

  - El cliente no posee un servidor RADIUS en producción.
  - Si bien el cliente posee un servidor LDAP (servidor Zimbra que da servicios de correo electrónico), el mismo no permite realizar las modificaciones para integrar un servidor RADIUS.
  - El cliente no desea tener que mantener un servidor RADIUS dedicado al servicio de WiFi.

- Filtrado MAC: Se propone la utilización del filtrado por MAC que provee el servidor UniFi, donde se debe mantener una lista blanca de dispositivos autorizados.

  Ventajas: Solo los dispositivos listados tendrán acceso al servicio y constituye un mecanismo para reforzar la seguridad en la red.

  Desventajas: Se requiere cierto trabajo por parte del administrador, ya que debe cargar cada dispositivo.

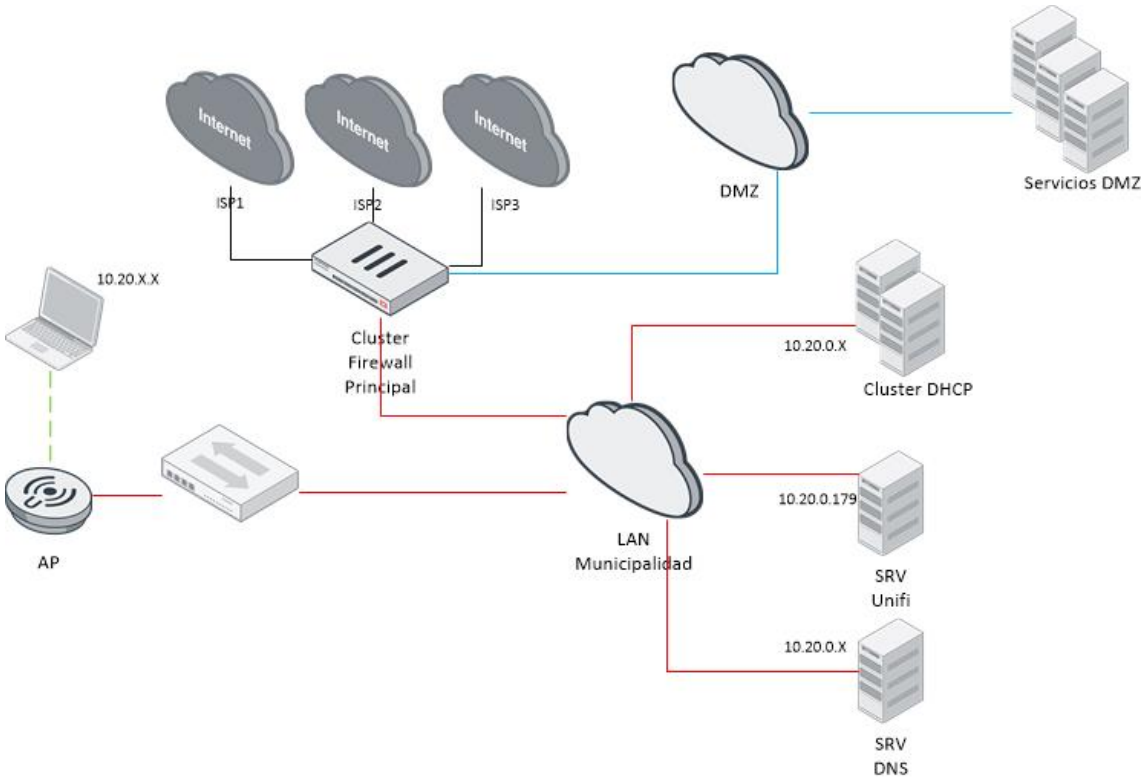
Nota: Otro punto negativo es que un atacante podría realizar un clonado de una MAC autorizada y así lograr acceder a la red con un dispositivo fraudulento, evitando este mecanismo de seguridad.

Perfil de usuario: Se propone, en principio, no definir restricciones de ancho de banda para esta red inalámbrica para así permitir el acceso correcto a los servicios internos y entre equipos de la LAN. Cabe aclarar que probablemente se realicen restricciones de acceso a internet (a través del firewall Fortinet mencionando en puntos anteriores), manteniendo el esquema de perfiles y permisos ya existente para usuarios cableados.

Otras consideraciones:

Se plantea un esquema de backup, el mismo contempla respaldos periódicos de la configuración de todos los servicios disponibles, siendo los mismos almacenados en unidades o servidores totalmente independientes.

Diagrama de conectividad RedMuni



5.3. Diseño físico de la solución

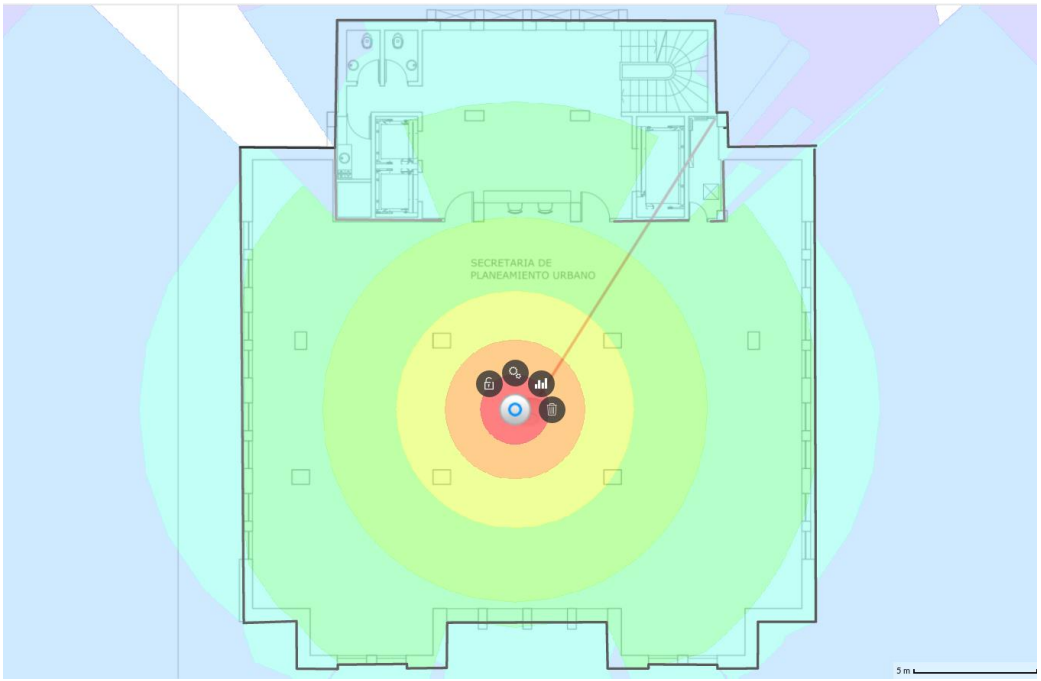
Partiendo de la información obtenida en la fase de relevamiento, se procedió a realizar una propuesta de despliegue físico.

Los principales factores a ser tenidos en cuenta son:

- Densidad de usuarios por área/piso, para poder cubrir las necesidades de cada uno de los ellos.
- Minimizar la cantidad de activos (mantener el espectro lo más limpio posible).
- Maximizar el área de cobertura dentro del edificio.
- Mantener la infraestructura simple evitando arreglos del tipo "mesh", dicho tipo de arreglos consiste en que al menos un access point, no se encuentre cableado a un activo y se comunique de manera inalámbrica con otro access point, dedicando ambos equipos, uno de sus radios para tal fin.
- Ubicar los equipos de manera que sean visibles para tareas de diagnóstico
- Reutilizar los elementos de manejo de cableado existentes tales como bandejas, cable canales, etc.
- Para pisos extensos, minimizar las distancias de cableado estructurado y mantener balanceados la carga al switch que alimenten los access point.

Como herramienta de apoyo al diseño físico se utilizó un módulo del software UniFi que permite realizar estimaciones sobre el área de cobertura considerando las atenuaciones generadas por factores edilicios. Con esta herramienta se puede ir variando la posición de los access point para obtener mejores resultados en lo que respecta a cobertura en las áreas de interés.

A continuación se incluye un ejemplo de la interfaz del módulo mencionado y la estimación de cobertura para una planta.



Como se puede apreciar en la imagen, cada access point es localizado en el plano de una planta, habiendo previamente definido la escala a utilizar junto con todas las paredes y divisiones (tales como vidrio, durlock, etc) con sus correspondientes atenuaciones ya provistas por la herramienta. El software se encarga de realizar la simulación de cobertura para una potencia de funcionamiento seleccionada.

Aclaraciones:

- Si bien se pretende utilizar las dos bandas disponibles (2.4 GHz y 5 GHz), para realizar este cálculo se considera únicamente la frecuencia de 2,4 GHz debido a su mayor compatibilidad con dispositivos y su mayor área de cobertura siendo dicha cobertura la que el servicio como tal puede abarcar.
- Se realizaron estas simulaciones para cada planta, haciendo los ajustes necesarios sobre la ubicación de los Access Point (por supuesto, siendo coherentes con la cercanía a los centros de cableado y la potencia a utilizar para cada access point).
- Un factor a considerar una vez resuelta la ubicación física de los access point es, tanto las posibilidades de montaje del equipo, como su cableado desde el centro de cableado más cercano.

- Otro aspecto para tener una solución que funcione correctamente es considerar la utilización del espectro, ya que si dos access point cercanos se encuentran en el mismo canal, los mismos interferirán entre sí.

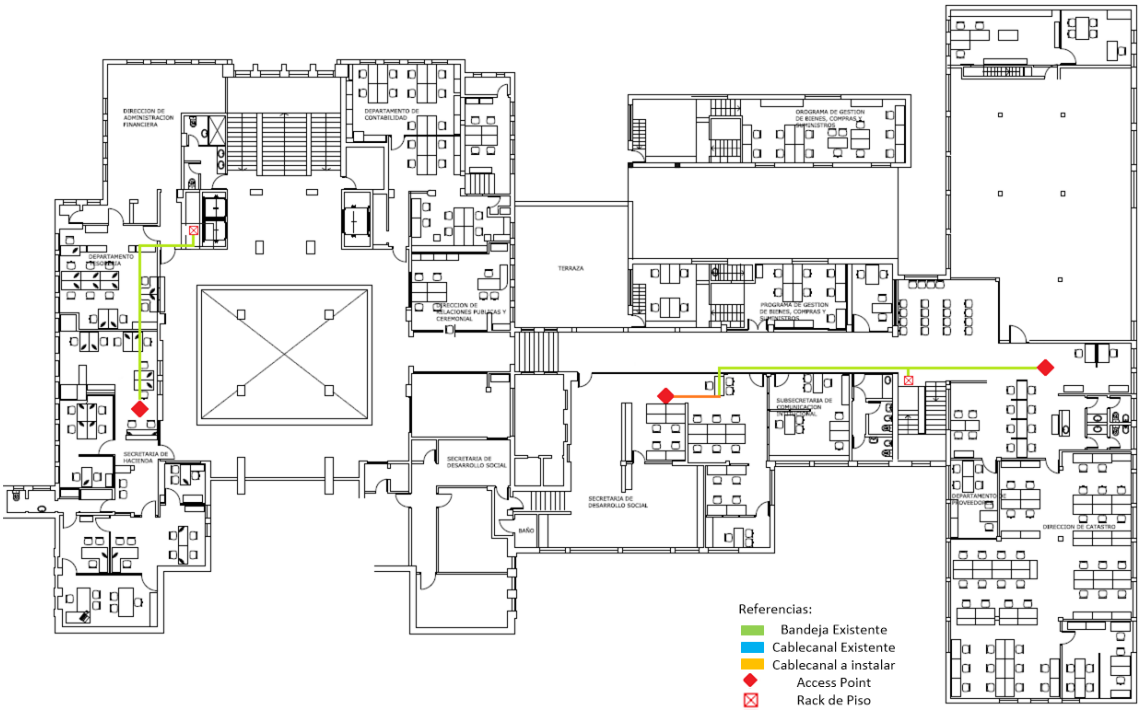
Finalizada esta etapa, se determinó la ubicación de los demás activos requeridos, entre ellos, switch e inyectores PoE. Para ello se partió de la premisa de incluir switch PoE únicamente en los centros de cableado en los que converjan al menos dos access point, dejando para los restantes el uso de los inyectores PoE.

Del relevamiento se sabe que existe espacio físico en todos los racks al menos para poder ubicar un switch, inyector PoE, unidades para agregar patchera o espacio en patcheras descargadas existentes. Además se sabe, se encuentran adecuadas las condiciones de tendido eléctrico para la instalación de los nuevos equipos.

Las premisas para realizar el tendido de cableado estructurado fueron:

- Partiendo del rack distribuidor de piso, se realizará la instalación de una patchera descargada (se añadirán patcheras sólo en el caso de ser necesarias).
- La canalización y ductería a utilizar, siempre que se pueda, corresponde con las bandejas para datos preexistentes
- Para los últimos metros antes del access point se utilizará cable canal autoadhesivo (el mismo será fijado además con tornillos a la superficie).
- El tendido de UTP Cat 6, tendrá como terminaciones para el extremo del distribuidor de piso un jack Cat 6.
- El tendido de UTP Cat 6, tendrá en el extremo del access point una roseta Cat 6.

Se incluye a modo de ejemplo, la planificación del cableado para uno de los pisos.



Utilización de canales:

Este apartado es de crucial interés para las bandas de 2.4 GHz, ya que existen solo 3 canales sin solapamiento por lo que hay que diseñar el uso de los mismos para que no existan interferencias significativas entre los equipos de la solución que afecten la performance del servicio.

A continuación se presenta de forma tabular la distribución de canales para los access point requeridos, considerando tanto las interferencias que puedan existir entre dispositivos del mismo piso como las posibles interferencias entre dos pisos adyacentes. En otra columna se detalla, además la potencia requerida para cada Access Point.

Tabla de canales

Nombre	Dirección IP	Canal	Potencia
AP-Piso13	10.20.1.165	1	Media
AP-Piso12	10.20.1.166	6	Media
AP-Piso11	10.20.1.164	11	Media
AP-Piso10	10.20.1.161	1	Media
AP-Piso9	10.20.1.163	6	Media
AP-Piso8	10.20.1.160	11	Media
AP-Piso7	10.20.1.167	1	Media
AP-Piso6	10.20.1.168	6	Media
AP-Piso5	10.20.1.169	11	Media
AP-Piso4	10.20.1.162	1	Media
AP-Piso3	10.20.1.173	6	Media
AP-Piso2-Este	10.20.1.170	11	Baja
AP-Piso2-Centro	10.20.1.171	1	Baja
AP-Piso2-Oeste	10.20.1.172	6	Baja
AP-Piso1-Este	10.20.1.174	11	Media
AP-Piso1-Centro	10.20.1.175	6	Media
AP-Piso1-Oeste	10.20.1.176	1	Baja
AP-PB-Centro	10.20.1.177	1	Media
AP-PB-Oeste-Sur	10.20.1.178	6	Baja
AP-PB-Oeste-Norte	10.20.1.179	11	Baja

Nomenclatura para el cableado estructurado

Este apartado es crucial para un trabajo prolijo. El correcto etiquetado va a permitir identificar los dispositivos y permitir diagnósticos futuros. Dicha nomenclatura debe ser coherente con la utilizada hasta el momento en todo el edificio.

Se optó por utilizar la siguiente nomenclatura para el etiquetado de rosetas y bocas en patcheras:

[ID PISO]-R[ID RACK]-PP[ID PATCH PANEL]-B[ID BOCA]

- [ID PISO]: Corresponde al número de piso en dos dígitos.
- [ID RACK]: Corresponde al número de rack referido
- [ID PATCH PANEL] Corresponde al número de patch panel
- [ID BOCA]: Corresponde al número de boca

A modo de ejemplo, a continuación se detalla el etiquetado que llevaría la roseta correspondiente al access point del piso 12:

"12-R1-P02-B01"

Requerimientos de Hardware y Software

Una vez estructurada la propuesta de solución, se procede a detallar qué aspectos adicionales de hardware y software son necesarios.

Instalación de servidor virtualizado Ubuntu server 16.04 LTS:

Requisitos mínimos:

CPU: 1 GHz

Memoria RAM: 512 MB

Disco: 2.5 GB

Referencia: help.ubuntu.com/lts/serverguide/preparing-to-install.html

UniFi Controller (Mínimos para su funcionamiento):

Sistema operativo: Ubuntu Desktop/Server 14.04 o 16.04

CPU: Procesador con Arquitectura x86-64 (Intel o AMD)

Memoria RAM: 2GB.

Red: 100Mbps Ethernet

Disco: 10GB libres (20GB o más, preferentemente)

Referencia: help.ubnt.com/hc/en-us/articles/360012282453#2

UniFi Controller (Recomendados para esta solución):

Sistema operativo: Ubuntu Server 16.04

CPU: 2 Virtual CPU.

Memoria RAM: 5 GB

Red: 1000Mbps Ethernet

Disco: 50GB

Servidor DNS y Secundario de DHCP

Ubuntu Server 16.04 LTS

CPU: 1 GHz

Memoria RAM: 512 MB

Disco: 2.5 GB

Servidor de Monitoreo:

Ubuntu Server 16.04 LTS

CPU: 2 CPU Cores

Memoria RAM: 2 GB

Referencia: www.zabbix.com/documentation/4.2/manual/installation

Contratación de servicios a ISP:

Es necesario contratar un enlace con las siguientes características:

Bajada: 100 Mbps

Subida: 15 Mbps

De preferencia, realizar la contratación de dos enlaces de diferentes ISP, para aprovechar la posibilidad de equipos de funcionar en modo balanceo de carga y a prueba de fallas.

Requerimientos de Hardware y cableado:

Ver anexo "Costos de equipamiento y cableado"

6. Implementación de la solución.

6.1. Cableado e instalación física de dispositivos.

Una cuadrilla de personal de cableado realizó las siguientes tareas avanzando de piso en piso:

- Tendido de cableado estructurado, según planimetría y realizando las terminaciones de los mismos (pachera o roseta según corresponda).
- Instalación de los soportes requeridos para la fijación de los access point al techo del edificio.
- Comprobación del cableado a través de tester de red.
- Instalación y alimentación eléctrica de switch o inyectores PoE en cada rack de piso.
- Instalación de los access point y conexión a través de un patchcord con la roseta disponible.
- Etiquetado de dispositivos, rosetas y parcheras.
- Certificación del cableado a través de herramienta Fluke
- Alimentación de todos los activos en cada rack.

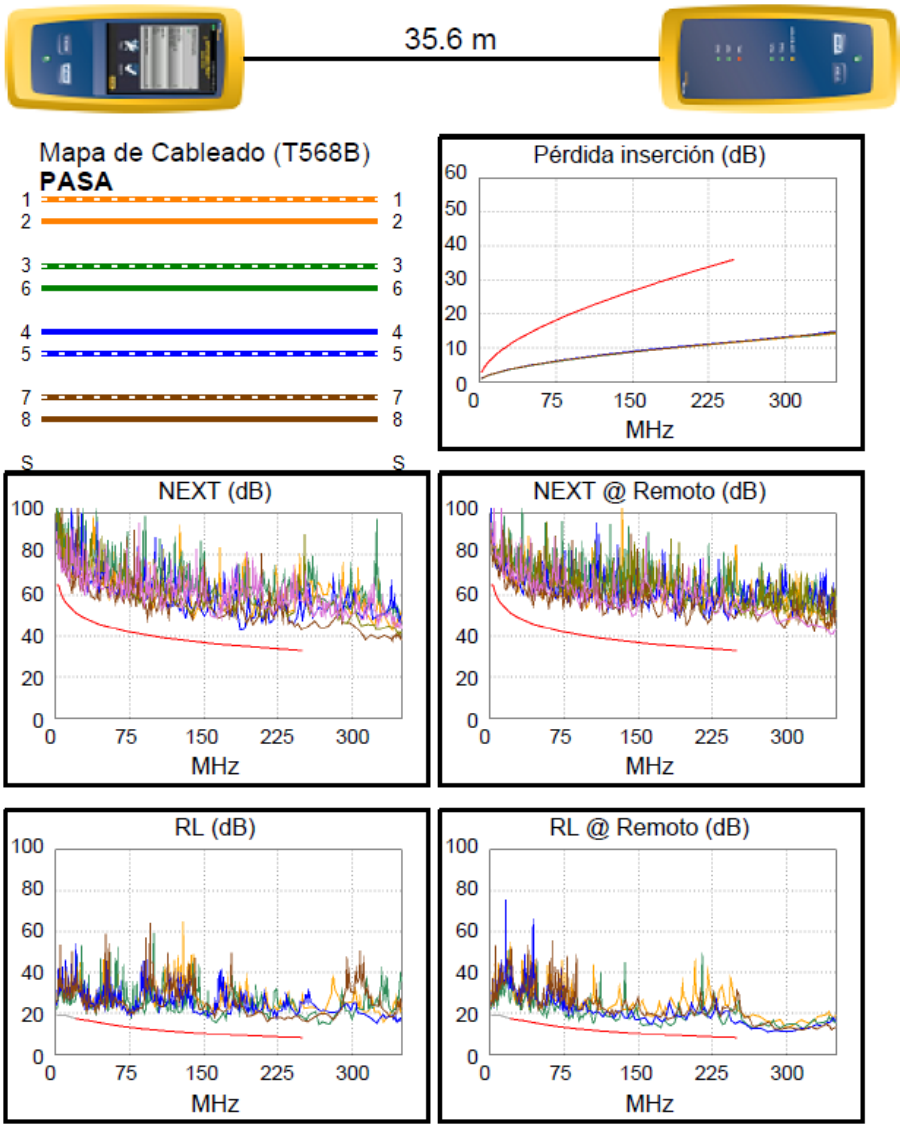
Para la certificación de cableado mencionada, se utilizó un equipo de la marca Fluke, particularmente el modelo DTX-5000; la tarea de certificar consiste en verificar que una instalación de cableado estructurado cumpla con los estándares esperados en diversos aspectos, entre ellos, el rendimiento en la transmisión. Realizando esta certificación, se demuestra tanto la calidad de los componentes involucrados, como de su correcta instalación.

Entre las pruebas que se realizan para determinar si el cableado pasa o no pasa la certificación se encuentran:

- Relevamiento de información sobre longitud del cableado
- Mapa del cableado, donde se verifican aspectos de continuidad, existencias de cortocircuitos, pares cruzados o invertidos, etc.

- Perdida por inserción donde se mide la atenuación de la señal, y se verifica que la pérdida total de señal extremo a extremo no supere el límite impuesto por la norma.
- Diafonía de extremo cercano también conocida como "NEXT", donde se mide la cantidad de ruido que se crea de un par a otro en el total de frecuencias de operación.
- Perdida de Retorno: se miden todas las reflexiones causadas por los desajustes de impedancia en todas las ubicaciones a lo largo del cableado (aspecto esencial- para la implementación de Gigabit Ethernet)

A continuación se incluye un extracto de una certificación para ilustrar las pruebas mencionadas, el informe completo de certificación para dicho cableado se encuentra disponible en el anexo "Implementación de la solución".



Como consideración general para los gráficos expuestos, es necesario remarcar que en ellos se puede apreciar una curva en color rojo, la misma representa el límite impuesto por el estándar por debajo (o por encima según corresponda) de la cual el cableado no pasa la prueba.

6.2. Puesta en marcha de equipos y servicios

Servicios de Internet

El ISP fue el encargado de llegar físicamente al data center ubicado en el piso 8, y realizar la instalación de los activos que requeridos (PON/Cablemodem) además de realizar las configuraciones pertinentes para proveer el servicio.

Instalación y configuración del servidor Wireless Controller:

Para realizar la instalación del servidor UniFi, fue necesario descargar e instalar los paquetes de la última versión disponible de dicho software, para luego acceder a través de la interfaz web y continuar con la configuración del mismo.

Ingresando a la interfaz web del servidor, fue necesario completar la configuración brindando información de región, aspectos para la automatización de respaldos y datos para la creación de un usuario administrador.

Instalación de certificado SSL

Una vez puesto en marcha el servidor wireless controller, debimos realizar la instalación del certificado SSL del tipo Wildcard, el cual nos puso a disposición el cliente. La implementación de este certificado evita inconvenientes a la hora de mostrar el portal cautivo previsto para el servicio de WiFi Santafeciudad (los dispositivos podrían considerar al portal como un sitio riesgoso y bloquear su acceso).

Para la correcta instalación de un certificado SSL en el servidor UniFi, fueron requeridos los siguientes archivos:

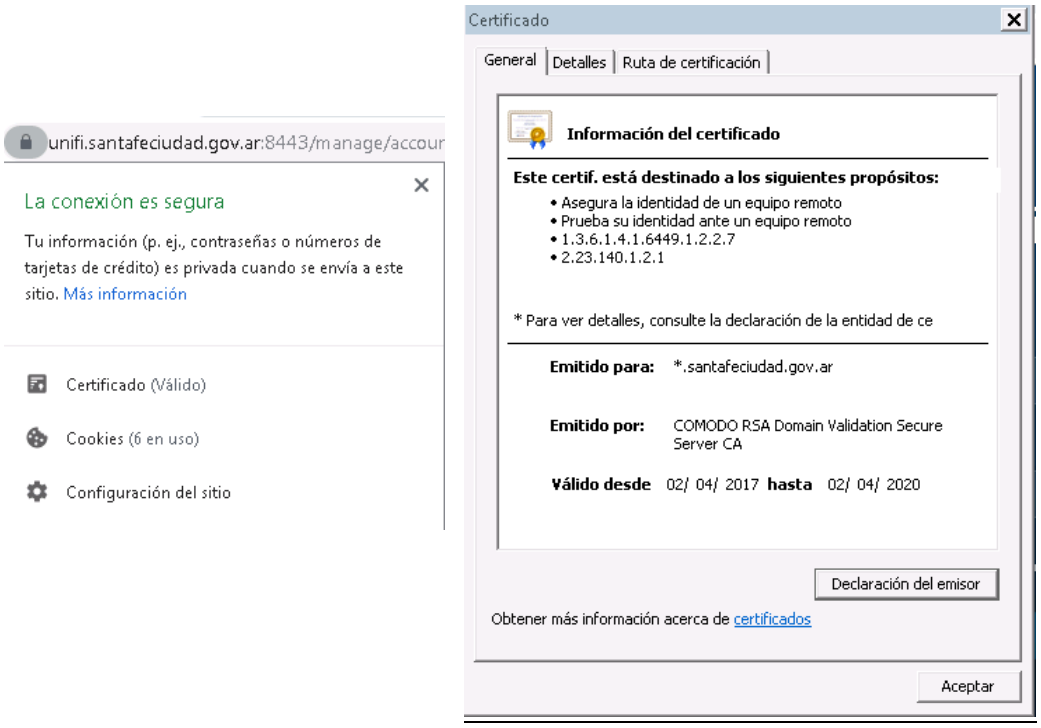
- Commercial.key: Corresponde a la clave privada del servidor en el cual fue generado el csr a la hora de solicitar el certificado.
- Bundle.crt: Corresponde al conjunto de certificados que componen la cadena de certificación.

El procedimiento para la implementación del certificado mencionado difiere bastante de la implementación para un servidor web convencional. El primer paso, consistió en la concatenación de los diferentes certificados que componen la cadena de certificación

Luego, fue necesario el uso de las utilidades openssl y keytool para finalizar el proceso:

- OpenSSL: es una herramienta que se utiliza para exportar los múltiples certificados a un único archivo.
- Keytool: es una herramienta que se utiliza para importar el archivo generado anteriormente al almacén de claves.

Una vez realizada la importación del certificado, solo fue necesario reiniciar el servicio de UniFi y comprobar la correcta instalación del certificado, como se puede apreciar en las siguientes imágenes:



Para un mayor detalle del procedimiento utilizado para la implementación del certificado SSL, ver el anexo "Implementación de la solución"

Configuración de los parámetros desde la interfaz web del servidor.

A continuación se detallan los aspectos mas relevantes configurados en el servidor.

Usuarios administradores:

- Incluyendo nombre de los respectivos usuarios, dirección de e-mail, perfil de administrador y contraseña.
- Los perfiles de administrador incluyen los permisos aplicables a cada usuario.

Redes WiFi:

- Nombre/SSID: Corresponde al nombre representativo de la red, es el identificador único por el cual el usuario va a poder detectar y conectarse a la red inalambrica. De manera intependiente, se definieron las redes inalambricas RedMuni y Santafeciudad.
- Seguridad inalambrica: Como se mencionó durante el diseño de la solución, se pretente utilizar diferentes arreglos de seguridad para cada una de las redes definidas, por lo que se detalla para cada caso:
    - Santafeciudad: Seguridad de tipo "Open", lo cual significa que no existe encriptacion por clave compartida para la misma y no se requiere una contraseña para conectarse a la red.
    - Redmuni: Seguridad de tipo "WPA Personal" donde se utiliza una encriptación por clave compartida y se requiere una contraseña para conectarse a la red.
- Clave de seguridad: Solo para el caso de Redmuni, se definió una clave de seguridad, la misma será utilizada al momento de conectarse a la red mencionada y pueden contener entre 8 a 63 caracteres.
- Politica de Invitado: Solo para el caso de Santafeciudad, habilitamos la opción "Guest Policy", esta funcionalidad permite que la red haga uso del portal cautivo antes mencionado.

Opciones avanzadas:

- Bloqueo de multicast y broadcast: Habilitando esta opcion, se previene el uso inecesario de la red inalambrica debido a trafico de este tipo.
- Utilización de VLAN: Solo para el caso de Santafeciudad, habilitamos la opcion "Use VLAN" y detallamos la VLAN correspondiente (para este caso VLAN 101)

- Grupo de usuario: Este apartado corresponde a la calidad de servicio y restricciones sobre el ancho de banda que se van a aplicar a cada usuario. Nuevamente, nos encontramos con dos configuraciones diferentes para cada una de las redes:
    - Santafeciudad: Utiliza el perfil de usuario default (limitado)
    - RedMuni: Utiliza el perfil GRP-Redmuni el cual se encuentra ilimitado a nivel ancho de banda disponible.

Filtrado por dirección MAC:

- Únicamente este apartado aplica a RedMuni, donde se habilita el filtrado mencionado, operando el mismo en modo "Lista blanca" donde solo se va a permitir acceso a aquellos dispositivos que hayan sido dados de alta en la lista mencionada.

Declaración de redes y VLAN para el uso en switch UniFi:

- Fue necesario realizar la declaración de las VLAN a ser utilizadas para la solución desde el controlador, de esta manera se le informa a los equipos UniFi que VLAN y tráfico asociado deben permitir. Para esta etapa de la implementacion, nos limitamos a definir la VLAN 101 correspondiente a la red Santafeciudad.

Politicas de Invitado:

- En este apartado definimos las configuraciones a ser aplicadas para las redes WLAN que posean habilitada la politica de invitado antes mencionada.
- Tipo de autenticación: Para esta aplicación, y según el diseño realizado, se configuró utilizando la opcion "Sin atuenticacion", la cual permite que el usuario se conecte a la red sin ningun tipo de usuario/contraseña o voucher.
- Tiempo de expriación: El tiempo de expiración seleccionado es de 1 hora.
- Configuraciones sobre la redirección una vez autorizado el usuario por el portal. Dentro de estas opciones se incluye la redirección a la pagina originalmente solicitada o a la pagina oficial de la municipalidad de Santa Fe.
- Personalización de portal: En este apartado se configuraron parametros tales como:
    - Título del portal y mensaje de bienvenida.

- Términos de servicio definidos por el cliente .
- Logo de la entidad y paleta de colores a ser utilizada.

A continuación se puede apreciar como se va a mostrar el portal cautivo personalizado.

- Sitios a los que se tiene acceso sin que el usuario deba pasar por el portal, para este caso se limita a la pagina oficial de la entidad y el portal propiamente dicho publicado dentro del servidor.

Grupos de usuario:

- Se definieron, para esta etapa, solo dos grupos de usuarios a ser utilizados por las redes planificadas:
  - Default: A ser utilizado, en principio por la red “Santafeciudad” con las restricciones de 1024 Kbps de bajada y 512 Kbps de subida.
  - GRP-RedMuni: A ser utilizado, por la red “RedMuni” sin restricciones de ancho de banda.
  - Estas restricciones mencionadas son a nivel wireless controller, por lo que puede que se implementen otras restricciones a nivel firewall, por ejemplo.

Configuración de servidor DNS

Con el objetivo de simplificar esta sección, únicamente nos vamos a centrar en las configuraciones generales del servidor, junto con su puesta en marcha y de la zona “santafeciudad.gov.ar” (y su correspondiente zona reversa para su eventual uso).

Archivos de configuración a tener en cuenta:

Named.conf: Corresponde a la configuración general del servidor, contiene las rutas de los demás archivos requeridos.

Named.conf.options: En este archivo se definen los servidores de reenvío. Los servidores de reenvío se utilizan para el caso de que el servidor BIND no disponga de entradas en su base de datos que correspondan a una petición, ni que la misma se encuentre en la cache del servidor.

Named.conf.local: En este archivo se definen cada una de las zonas (y sus correspondientes zonas reversas) junto con las características de las mismas.

for.santafeciudad.gov.ar: Corresponde al archivo para la zona santafeciudad.gov.ar y contiene los parámetros para dicha zona junto con cada una de las entradas asociadas.

rev.santafeciudad.gov.ar: Corresponde al archivo para la zona reversa de santafeciudad.gov.ar.

Para mayor detalle respecto a los archivos mencionados, ver el apartado correspondiente en el anexo "Implementación de la solución".

Una vez que se concluyó con la configuración del servidor BIND, se procedió a realizar pruebas de funcionamiento a través de la utilidad dig. Dicho comando permite realizar consultas DNS a un servidor particular, obteniendo tanto la resolución DNS, como información relevante para llevar a cabo todo tipo de diagnósticos.

A continuación se deja un extracto de las pruebas realizadas para este caso, incluyendo únicamente el fragmento de la salida relevante.

Resolución zona santafeciuidad.gov.ar DNS LAN

```
root@unifi:/# dig mail.santafeciudad.gov.ar @10.20.0.122

; <<>> DiG 9.10.3-P4-Ubuntu <<>> mail.santafeciudad.gov.ar
@10.20.0.122
[…]
;; ANSWER SECTION:
mail.santafeciudad.gov.ar. 86400 IN     A       X.X.X.X

;; Query time: 0 msec
;; SERVER: 10.20.0.122#53(10.20.0.122)
;; WHEN: Wed Oct 30 18:24:13 -03 2019
;; MSG SIZE  rcvd: 104
```

Resolución externa DNS LAN

```
root@unifi:/# dig www.frsf.utn.edu.ar @10.20.0.122


; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.frsf.utn.edu.ar
@10.20.0.122
```

```
[…]
;; ANSWER SECTION:
www.frsf.utn.edu.ar.    14400   IN      CNAME
pino.frsf.utn.edu.ar.
pino.frsf.utn.edu.ar.   3599    IN      A       190.183.255.40
pino.frsf.utn.edu.ar.   3599    IN      A       190.114.206.142

[…]
;; Query time: 667 msec
;; SERVER: 10.20.0.122#53(10.20.0.122)
;; WHEN: Wed Oct 30 18:28:31 -03 2019
;; MSG SIZE  rcvd: 483
```

Webmin: Como se mencionó anteriormente, esta herramienta permite la visualización y modificación de los archivos ya mencionados. A través de su interfaz web, se puede visualizar de manera intuitiva la base de datos del servidor con cada una de sus zonas y entradas DNS.

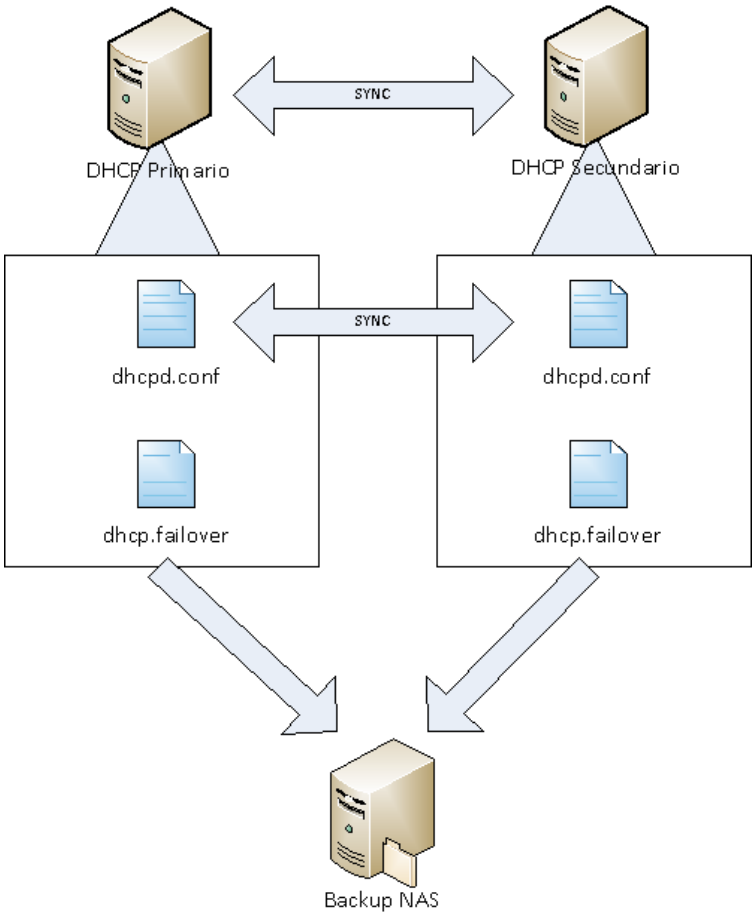
Configuración de DHCPD en Ubuntu

Este servidor fue concebido a partir de la necesidad de contar con un servidor secundario para el uso dentro de Redmuni.

Nuevamente, nos vamos a limitar a mencionar los archivos de configuración más relevantes para la puesta en marcha del DHCP. Dado que este servidor va a funcionar como parte de un esquema de failover, se requiere la configuración de dos archivos independientes:

- Dhcpd.conf: Corresponde al archivo principal de configuración del servidor
- Dhcpd.failover: Corresponde a un archivo auxiliar referenciado en el archivo principal de configuración, el mismo contiene la información particular para este nodo del esquema. Este esquema permite aislar de la sincronización parte de la configuración evitando así ser sobrescrita.

Esquema de replicación:



Se crearon tareas del tipo Cron en el servidor con el objetivo de permitir la sincronía entre ambos miembros del cluster DHCP, esto conlleva la ejecución de un script de manera periódica utilizando una herramienta llamada Rsync.

Webmin:

Nuevamente, Webmin se utiliza para gestionar de forma gráfica los archivos de configuración del servidor, principalmente para aspectos relacionados a la asignación de IP de manera estática.

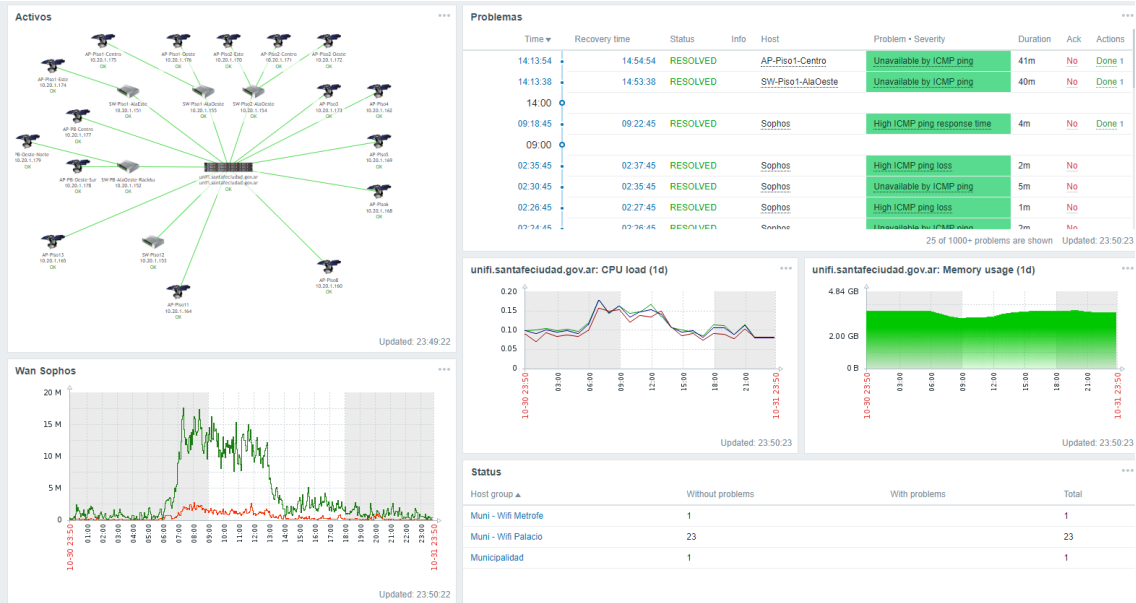
Instalación y configuración de zabbix

Una vez instalado Zabbix y teniendo acceso a la interfaz web del servidor (ver anexo "Implementación de la solución"), fue necesario abordar las siguientes actividades:

- Creación de usuarios con sus respectivos permisos para administrar, visualizar y editar las configuraciones del servidor de monitoreo. Este paso contempla,

además, la creación de usuario administrador por defecto, un usuario para ICOP, y por último, un usuario para el responsable asignado al monitoreo de la solución.

- Instalación y configuración del Agente Zabbix en servidores a ser monitoreados. El proceso de instalación mencionado se detalla en el anexo "Implementación de la solución".
    - Importar/Crear plantillas para el monitoreo según el dispositivo en cuestión. Para este caso se descargaron plantillas SNMP de repositorios propios de Zabbix. Cada plantilla incluye como componente principal las MIB que permiten acceder a información específica para cada dispositivo a monitorear y administrar.
- Creación de hosts desde la interfaz web de servidor Zabbix
    - Especificar la dirección IP o DNS y el tipo de monitoreo que se desea realizar (SNMP, Basado en agente o basado extensiones).
    - Asignar el host a un grupo de monitoreo.
    - Asignar una plantilla de monitoreo (la misma incluye los disparadores, gráficos y aplicaciones).
- Creación de tableros acordes a los usuarios previamente identificados. Los tableros incluyen una vista en una única pantalla de los aspectos relevantes de la solución, pudiendo combinar información de diversos host en diversos formatos. A continuación se muestra un ejemplo de un tablero creado para un usuario administrador.



- Configuración de disparadores y perfiles de notificación: Se especifican los perfiles para envío de notificaciones (en este caso por medio de email). En resumen, se define bajo qué condiciones se enviarán notificaciones a los usuarios interesados. Adicionalmente, se define la plantilla para los mismos, pudiendo incluir los valores asociados a de variables de interés como parte del mensaje.

Configuración de Backups

Dada la variedad de servidores y servicios implementados como parte de esta solución, fueron necesarios diversos esquemas para permitir respaldo de las configuraciones realizadas. Se destacan tres enfoques bastante diferentes:

- Implementación a través de funcionalidades previstas por las aplicaciones y equipos instalados como parte de la solución particular (como fue el caso para el servidor UniFi y el firewall Sophos)
- Implementación a través de la instalación de herramientas adicionales, en este caso Webmin (como en el caso de servidores DHCP y servidor DNS).
- Implementación a través de Script (implementado para el servidor Zabbix).

Para un mayor detalle de los esquemas mencionados, ver anexo “Implementación de la solución”.

Configuración de Access Point

Partiendo de las direcciones IP definidas en la subred de administración, se procedió a realizar la configuración de los access point a través de su interfaz web. Para esta etapa, es únicamente requerido configurar:

- Dirección IP para administración.
- Mascara de subred.
- Puerta de enlace predeterminada.
- Servidor DNS.
- Realizar cambios en usuario y contraseña para su administración.

Adopción de los access point y switch

Este apartado resulta muy simple, ya que teniendo los dispositivos previamente configurados y correctamente conectados a la red, fue cuestión de simplemente detectarlos desde la interfaz del servidor UniFi y adoptarlos por el mismo. Una vez adoptados tanto los access point como los swtich pasan a ser administrados de manera centralizada por el servidor UniFi. En las siguientes imágenes se puede ver, tanto los access point como los switch ya adoptados por el Wireless Controller.

DEVICE NAME ↑	IP ADDRESS	STATUS
AP-Piso3	10.20.1.173	CONNECTED
AP-Piso4	10.20.1.162	CONNECTED
AP-Piso5	10.20.1.169	CONNECTED
AP-Piso6	10.20.1.168	CONNECTED (100 FDX)
AP-Piso7	10.20.1.167	CONNECTED
AP-Piso8	10.20.1.160	CONNECTED
AP-Piso9	10.20.1.163	CONNECTED
SW-PB-AlaOeste-Rack6u	10.20.1.152	CONNECTED
SW-Piso1-AlaEste	10.20.1.151	CONNECTED
SW-Piso1-AlaOeste	10.20.1.155	CONNECTED (100 FDX)
SW-Piso12	10.20.1.153	CONNECTED
SW-Piso2-AlaOeste	10.20.1.154	CONNECTED

DEVICE NAME ↑	IP ADDRESS	STATUS
AP-PB-Centro	10.20.1.177	CONNECTED
AP-PB-Oeste-Norte	10.20.1.179	CONNECTED
AP-PB-Oeste-Sur	10.20.1.178	CONNECTED
AP-Piso1-Centro	10.20.1.175	CONNECTED
AP-Piso1-Este	10.20.1.174	CONNECTED
AP-Piso1-Oeste	10.20.1.176	CONNECTED
AP-Piso10	10.20.1.161	CONNECTED
AP-Piso11	10.20.1.164	CONNECTED (100 FDX)
AP-Piso12	10.20.1.166	CONNECTED
AP-Piso13	10.20.1.165	CONNECTED
AP-Piso2-Centro	10.20.1.171	CONNECTED
AP-Piso2-Este	10.20.1.170	CONNECTED
AP-Piso2-Oeste	10.20.1.172	CONNECTED

Configuración inicial del firewall para santafeciudad:

Las tareas requeridas fueron las siguientes:

- Registrar el firewall en el portal de soporte de la marca: Dicho registro, permite acceder al soporte y además dar de alta los servicios adicionales tales como filtro de contenido web y filtro de aplicaciones.
- Configuración de HA: A continuación se muestra un diagrama para ilustrar el esquema de HA. En dicho diagrama podemos ver, entre otros aspectos, el puerto dedicado para HA que conecta de forma directa ambos miembros del clúster. Esta interconexión, permite que ambos equipos escuchen los latidos del miembro restante.

- Configuración de usuario administrador: Se crean los usuarios correspondientes para poder administrar el equipo, además de realizar el cambio de contraseña para el usuario admin pre-existente.
- Configuración de IP en principales interfaces: Para este caso es necesario tener configurada la interfaz que va a ser utilizada como WAN, pero también las interfaces del tipo VLAN que van a dar servicios a las distintas redes WLAN.
- Modo de funcionamiento del equipo: El equipo es configurado en modo Gateway.
- Configuración de servidor DNS a utilizar por el equipo.
- Selección de política por defecto: Por el momento, se permitió todo el tráfico desde las VLAN/LAN hacia la WAN.
- Configuración SMTP: Se configura según los parámetros del servidor de correo del cliente para que los equipos puedan enviar email permitiendo notificar distintos eventos.

- NTP: Configuración del servidor NTP para mantener los equipos en hora y permitir que la búsqueda dentro de registros sea eficiente.

Una vez finalizada la configuración inicial del cluster, resta ajustar cada uno de los siguientes aspectos:

- Servidor DHCP

  Dar de alta el servidor DHCP para la red Santafeciudad, y según diseño configuramos:

  - Nombre del servidor DHCP.
  - Interfaz en la cual va a prestar servicio el servidor.
  - Rango de direccionamiento para las concesiones (según diseño).
  - Asignación estática de direcciones (En principio, no aplicable para este servidor, salvo casos particulares a analizar en un futuro).
  - Selección de puerta de enlace para la subred, en este caso corresponde a la dirección IP de la interfaz en la VLAN correspondiente.
  - Tiempo de concesión de direccionamiento, coherente con los parámetros del servicio Santafeciudad.
  - Selección de servidor DNS primario, según diseño.

- Aspectos de filtrado

  Para este caso, el firewall mencionado cuenta con una serie de categorías de navegación, las cuales se pueden permitir o bloquear según corresponda.

  Cabe aclarar que el proveedor del servicio, Sophos, se encarga de mantener las bases de datos actualizadas y mantener bajo la lupa la categorización de las páginas web. El equipo descarga periódicamente definiciones para estas categorías para poder realizar de manera eficiente el filtrado mencionado.

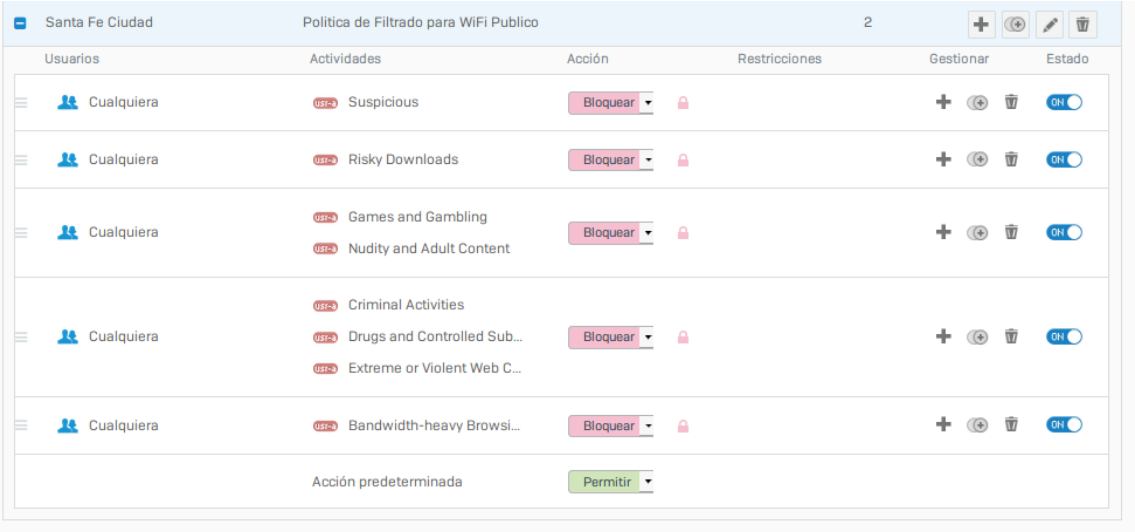
  Según requerimientos, la red santafeciudad debe contar con un filtrado sencillo basado en categorías, donde se declara el bloqueo para:

  - Páginas Web consideradas como sospechosas.
  - Descargas Riesgosas.
  - Juegos y apuestas.

- Desnudos y contenido para adultos.
- Actividades criminales.
- Drogas.
- Contenido violento.
- Contenido de alto consumo de ancho de banda.
- Acción por defecto.

Se aplica una política de Aceptar por defecto en la presente implementación.

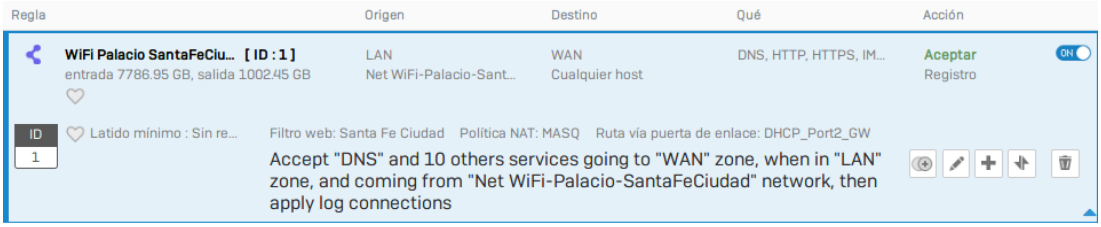
A continuación, se puede ver una captura de la interfaz web del firewall Sophos en el que se muestra el perfil de filtrado mencionado.



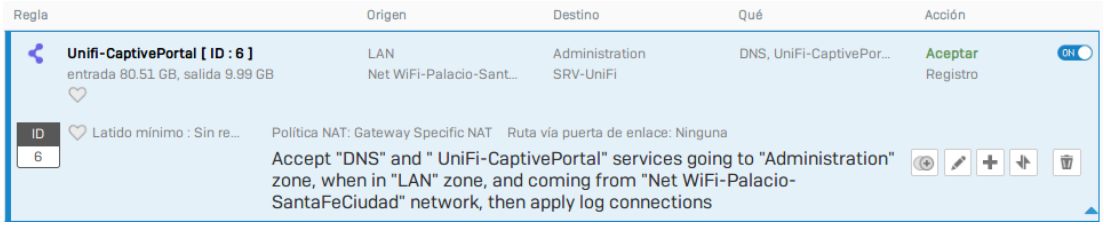
- Rutas
  - Se declaró la puerta de enlace predeterminada para que se pueda navegar a través del equipo.
  - La puerta de enlace asignada corresponde a la provista por el ISP en una de las interfaces destinadas a funcionar como WAN.
- Políticas de Firewall

  A nivel políticas de firewall, las más relevantes a considerar son:
  - Política que permite la navegación de dispositivos pertenecientes a la red de WiFi Santafeciudad, permitiendo a cualquier dispositivo de la LAN mencionada acceder a cualquier destino de internet a través de los puertos por defecto de navegación, así como también los puertos destinados a

servicios de email. Cabe aclarar que además, en un análisis posterior del tráfico por parte del equipo, el mismo aplica las políticas de filtrado web definidas en el apartado "Aspectos de filtrado". La política se puede ver en la siguiente imagen:



- Política que permite el acceso a dispositivos pertenecientes a la LAN WiFi Santafeciudad al portal cautivo (disponible en la LAN de la municipalidad) puertos TCP/8880 y TCP/8843. Dicha política se puede apreciar en la siguiente imagen.



Configuración del switch de distribución según diseño

Entre las configuraciones que se realizaron en el switch de distribución se incluye:

- Configuraciones iniciales:
  - Información de identificación del dispositivo.
  - Creación de usuarios y contraseña para su administración.
  - Configuración de fecha/hora y servidor NTP.
- Declaración de las VLAN mencionadas en el diseño.
- Creación de las VLAN interface, para actividades de depuración y administración.
- Configuración de cada puerto declarando:
  - Tipo de funcionamiento.
  - ID de VLAN.
  - VLAN en access (untagged).

- VLAN en tagged.

Para un detalle de los comandos utilizados y un extracto del archivo de configuración del dispositivo ver el anexo "Implementación de la solución"

Configuración switch en centros de cableado

En cada uno de los switch involucrados se realiza la declaración las VLAN a utilizar, y luego el estado de cada uno de los puertos requeridos en relación a las VLAN.

Dichas configuraciones fueron realizadas en los equipos a través de interfaces de consola, acceso a través de telnet o acceso SSH, corroborando luego a través de interfaces web la correcta configuración de los equipos.

La configuración es particular para cada switch, pero comparten la particularidad que tanto para los switch intermedios como para los switch a los que se encuentra conectado un switch UniFi PoE o un access point, las correspondientes VLAN son declaradas como tagged. Para un detalle de los comandos utilizados en cada marca de switch, ver anexo "Implementación de la solución".

Prueba de funcionamiento:

Una vez configurados todos los switch, trasladando las VLAN correspondientes por todos ellos hasta el access point, la prueba del correcto funcionamiento, consistió simplemente en conectarse a la red inalámbrica Santafeciudad y corroborar que el servidor DHCP (ubicado en el firewall Sophos) nos asigne una dirección IP en el rango esperado.

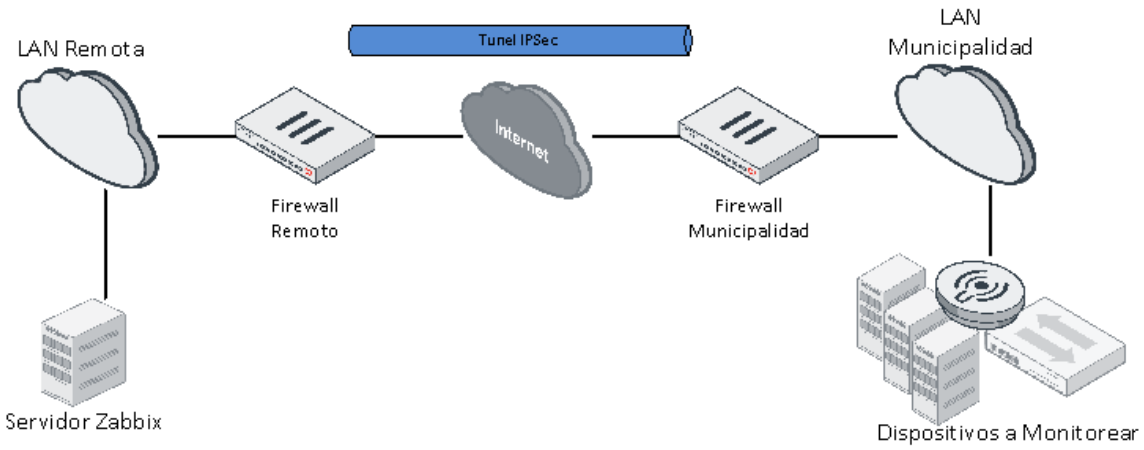
El hecho de que no se reciba una IP correctamente, implica que existe algún problema en al menos uno de los equipos intermedios involucrados.

Una vez obtenida la dirección IP, automáticamente se muestra una notificación indicando que la red a la que el dispositivo se encuentra conectado, requiere autenticación.

Implementación de VPN

La implementación de una VPN IPSec tiene como objetivo dar conectividad de manera segura desde un servidor de monitoreo dedicado en una ubicación remota hacia la infraestructura WiFi.

Para este caso, en ambos extremos nos encontramos con dispositivos de la marca Fortigate con capacidad de realizar túneles IPSec. En el siguiente diagrama se puede ver un esquema de cómo ha implementado.



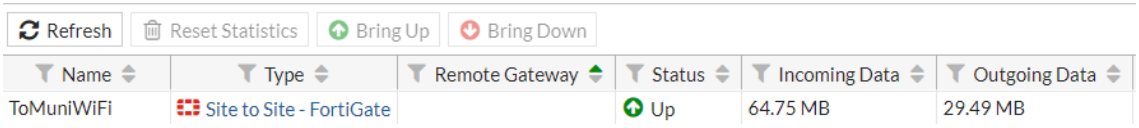
Para la puesta en marcha de la VPN IPSec, es necesario realizar la declaración de 2 fases en cada extremo

- Declaración de la fase1:
    - Gateway remoto: Corresponde a la dirección IP publica del equipo remoto con capacidad de negociar la conexión IPSec, también se puede utilizar un DDNS para el caso de no contar con una IP publica fija.
    - Proposal: Consiste en el/los algoritmo/s que van a ser utilizados en la negociación de la primera fase de IPSec.
    - Diffe Hellamn Group: Grupo IKE para el intercambio claves para la fase 1
    - Preshared key: es una clave compartida entre los dos extremos de la VPN
- Declaración de la fase2:
    - Proposal: Mismo objetivo que para la fase 1,
    - Diffe Hellman Group: Grupo IKE para el intercambio claves para la fase 2
    - Subred local: Corresponde a la declaración de que subred local será utilizada para la VPN.
    - Subred remota: Corresponde a la declaración de la subred remota que será utilizada para la VPN.

- Rutas estáticas para la VPN: Se deben declarar las políticas estáticas en ambos extremos para poder realizar enrutamiento de las subredes declaradas. La denominada “blackhole” corresponde a una ruta de uso exclusivo para el caso de que la VPN se encuentre caída. Esto evita que tráfico que, se supone debería ser ruteado y encriptado a través dela VPN, sea enviado a través de la ruta por defecto (un ISP).

Una vez definida y levantada la VPN, es necesario crear las políticas a nivel firewall que permitan el tráfico para realizar el monitoreo de los servidores y demás activos.

Las políticas mencionadas son configuradas en ambos extremos de la VPN, e incluyen como origen o destino tanto las interfaces preexistentes como las creadas a la hora de configurar el túnel IPSec. Fuera de este aspecto, el funcionamiento de las mismas, es el tradicional.



Para un mayor detalle de la configuración del túnel IPSec visitar el anexo “Implementación de la solución”.

7. Transferencia y resultados

7.1. Ajuste de canales y potencias

Con la solución puesta en marcha, se procedió a realizar mediciones de cobertura para ejecutar un ajuste fino sobre las potencias y canales utilizados por cada uno de los access point.

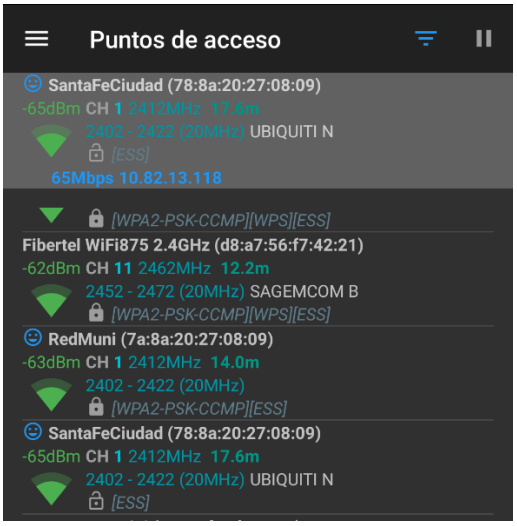
Para ello, se hizo uso la herramienta “WiFi Analyzer”, disponible para dispositivos Android. Empleando un dispositivo móvil equipado con dicha herramienta, se procedió a realizar un escaneo en tiempo real de la intensidad de señal disponible para toda el área de cobertura esperada. Además, se definieron los valores de potencia mínima aceptable para dar como correcta la cobertura del servicio.

El umbral de aceptación fue ubicado en los -65 dBm en la banda de 2,4 GHz, bajo el cual la herramienta procede a categorizar la intensidad de la señal como media y siendo mostrada en color amarillo en lugar de verde.

Cabe aclarar que para el indicador de intensidad de señal recibida, cuanto menor (más negativo) sea el valor, el mismo representa una mayor pérdida de señal.

A continuación se muestra una captura tomada desde la herramienta mencionada, evidenciando, entre otros detalles:

- La red SantaFeCiudad con una potencia acorde a los valores definidos y por lo tanto, aceptable.
- La red RedMuni con una potencia acorde a los valores definidos, con una intensidad de señal recibida aún mejor.



Nota: El dispositivo utilizado durante toda la prueba corresponde a un teléfono inteligente marca Motorola, modelo "G4 Plus". De esto surge la aclaración que las mediciones están ligadas directamente al dispositivo utilizado, principalmente variando según la calidad y ubicación de las antenas disponibles en el equipo.

7.2. *Ajuste sobre el uso del espectro*

Del Relevamiento se sabe de la existencia de diversos activos utilizando las mismas frecuencias que la solución implementada. De los identificados, solo algunos pudieron ser apagados y reemplazados por activos de la presente solución. Los demás, o son administrados de manera independiente por algunas áreas y no pueden ser modificados, o se tratan de equipos que por defecto poseen difusión de redes WiFi para su administración y deben ser desactivados.

La herramienta UniFi Controller, provee una funcionalidad que permite identificar las redes WiFi cercanas a los dispositivos administrados por el controlador, junto con su canal de operación y el porcentaje de interferencia con cada access point de UniFi. A continuacion se puede ver un extracto de la funcionalidad mencionada.

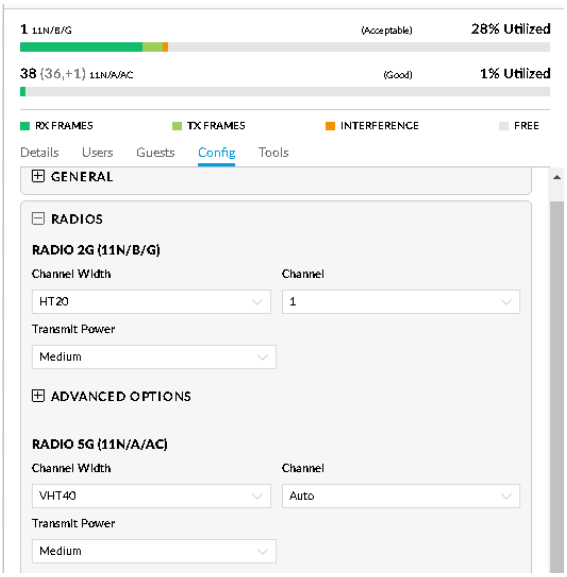
	NAME/SSID	CHANNEL	BW [MHz]	SECURITY	LOCATION	SIGNAL ↓
1	SETUP	11 (ng)	20	Open (Ad-Hoc)	Near AP-Piso2-Este	99% (-41 dBm)
1	DIRECT-e6-HP M180 LaserJet	6 (ng)	20	WPA2 (AES/CCMP)	Near AP-Piso2-Oeste	94% (-52 dBm)
4	REDMUNI	3 (ng)	20	WPA/WPA2 (TKIP/AES/CCMP)	Near AP-PB-Centro Near AP-Piso2-Centro Near AP-Piso2-Oeste Near AP-PB-Oeste-Sur	92% (-53 dBm) 35% (-76 dBm)
1	DIRECT-yKM262x 282x Series	11 (ng)	20	WPA2 (AES/CCMP)	Near AP-Piso4	77% (-59 dBm)
1	HP-Print-FB-LaserJet 1102	6 (na)	20	Open	Near AP-Piso8	74% (-60 dBm)
1	PISO_4	3 (ng)	20	WPA/WPA2 (AES/CCMP)	Near AP-Piso2-Centro	69% (-62 dBm)
1	Portthru	11 (ng)	20	Open (Ad-Hoc)	Near AP-Piso2-Este	69% (-62 dBm)
1	DIRECT-EtCLP-360 Series	11 (ng)	20	WPA2 (AES/CCMP)	Near AP-Piso4	67% (-63 dBm)

Como se puede apreciar, existe diversidad de redes trabajando en el espectro de interés. Dichas redes pueden ser pertenecientes a dispositivos tales como impresoras, televisores y acondicionadores de aire. Por lo general, estas redes corresponden a servicios destinados a realizar las configuraciones iniciales de dichos dispositivos y, actualmente, se encuentran sin utilidad. De ser posible, deben ser desactivadas.

Para resolver este aspecto, utilizado la información suministrada por el wireless controller y con ayuda, nuevamente, de la herramienta WiFi Analyzer, se procedió a identificar la fuente de las redes y proceder a desactivarlas.

Dado que se pudieron desactivar gran cantidad de redes en desuso, no fue necesario realizar ajustes sobre canales de funcionamiento para los dispositivos de la solución.

A continuación se puede ver un ejemplo correspondiente a un Access Point y su utilización del canal.



- Verde Oscuro: Corresponde a la utilización del canal para tramas recibidas
- Verde Claro: Corresponde a la utilización del canal para tramas enviadas
- Anaranjado: Corresponde a la interferencia externa en el canal.

Por otro lado, se puede ver un extracto de la configuración correspondiente al ancho de banda del canal a utilizar, el canal propiamente dicho y la potencia de transmisión a utilizar en ambos radios (2,4 GHz y 5GHz).

Fue necesario realizar estos ajustes, a pesar de haber realizado simulaciones en la etapa de diseño, debido a que no todas las variables que pueden interferir son simples de medir. No hay que olvidar que el medio a utilizar es compartido y posee una naturaleza cambiante para este tipo de aplicaciones, algunas fuera del control del administrador de la red.

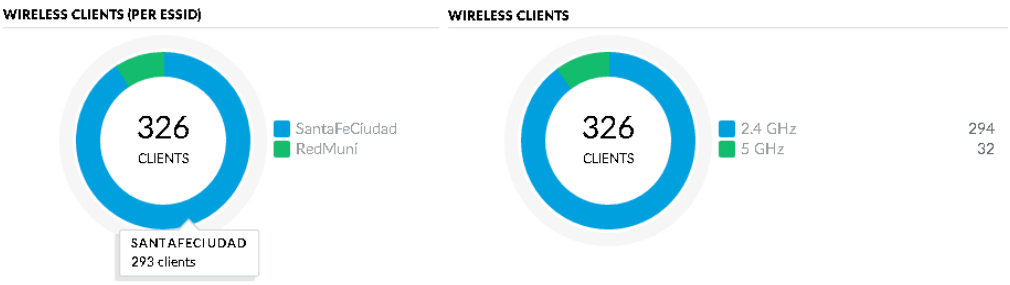
7.3. Monitoreo de uso de enlace y cantidad de usuarios y autorización

En esta sección se mostrarán los aspectos relacionados al monitoreo de la cantidad de usuarios, dicha información es obtenida tanto del wireless controller, como del servidor de monitoreo. Podemos apreciar información en tiempo real así como también en gráficas que muestran la evolución de las diferentes variables en el tiempo.

Todas las imágenes son a modo ilustrativo de las capacidades de monitoreo, por lo que se trató de visibilizar, al menos, las más relevantes para las tareas diarias, realización de estimaciones, diagnósticos y mediciones varias.

Desde el wireless controller podemos ver, por ejemplo:

- Cantidad de usuarios por red inalámbrica y por radio en tiempo real

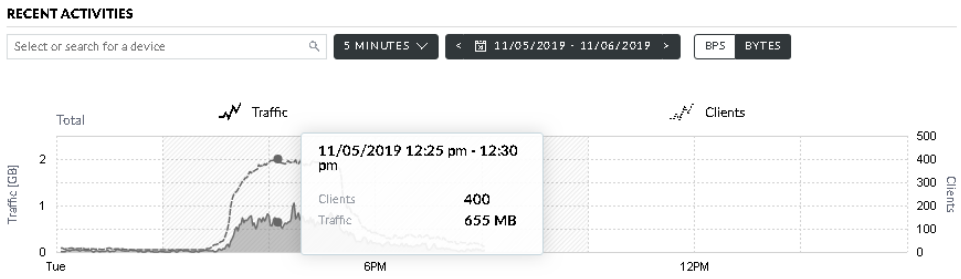


- Cantidad de usuarios en los access point de mayor uso, desagregando los mismos por la banda a la que se encuentran conectados.

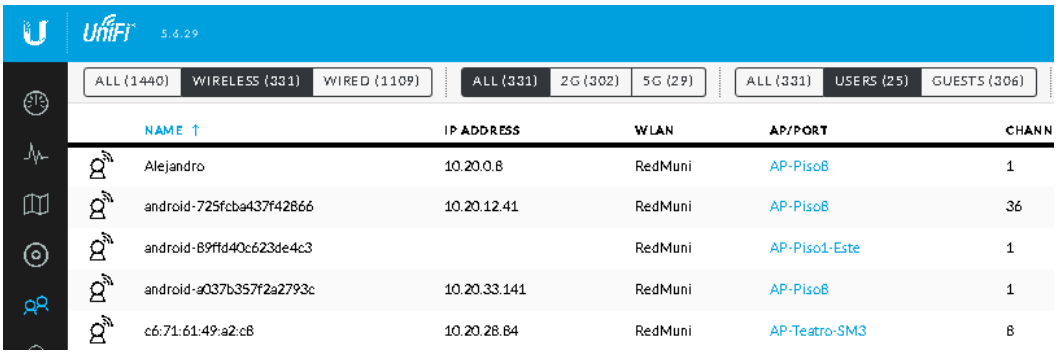
TOP CLIENTS

NAME	5 GHZ CLIENTS	TOTAL CLIENTS
AP-Piso8	10	49
AP-PB-Centro	7	42
AP-PB-Oeste-Norte	5	53
AP-Piso6	4	30
AP-Piso1-Este	4	22

- Gráficos (por access point o totalizados) de usuarios conectados y tráfico durante períodos configurables.

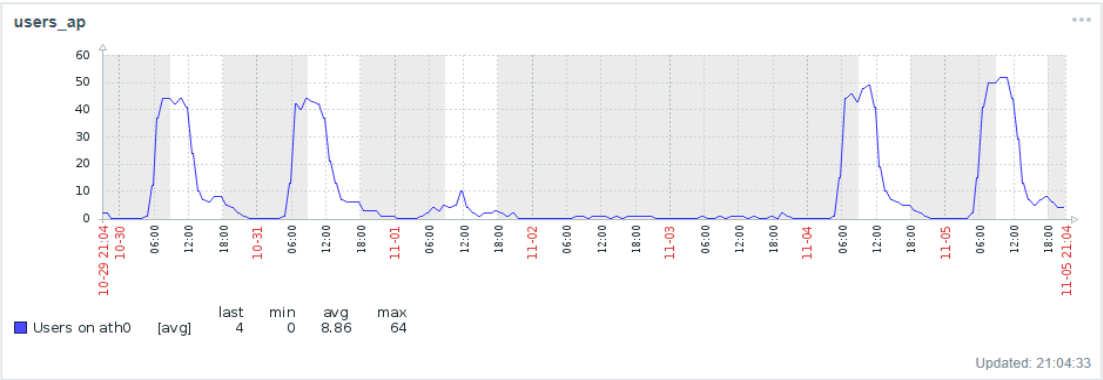


- Estado de los dispositivos, posibilidad de administración y gestión de los usuarios.

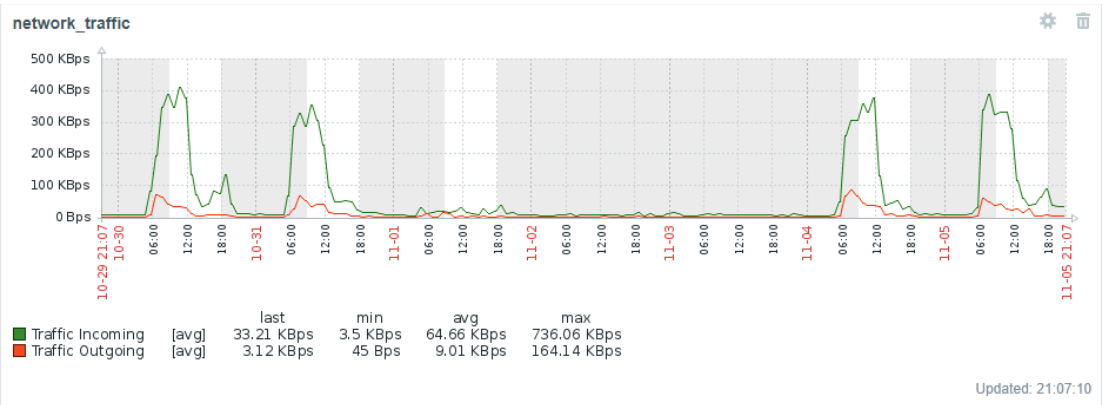


Desde el monitoreo de Zabbix podemos ver, por ejemplo:

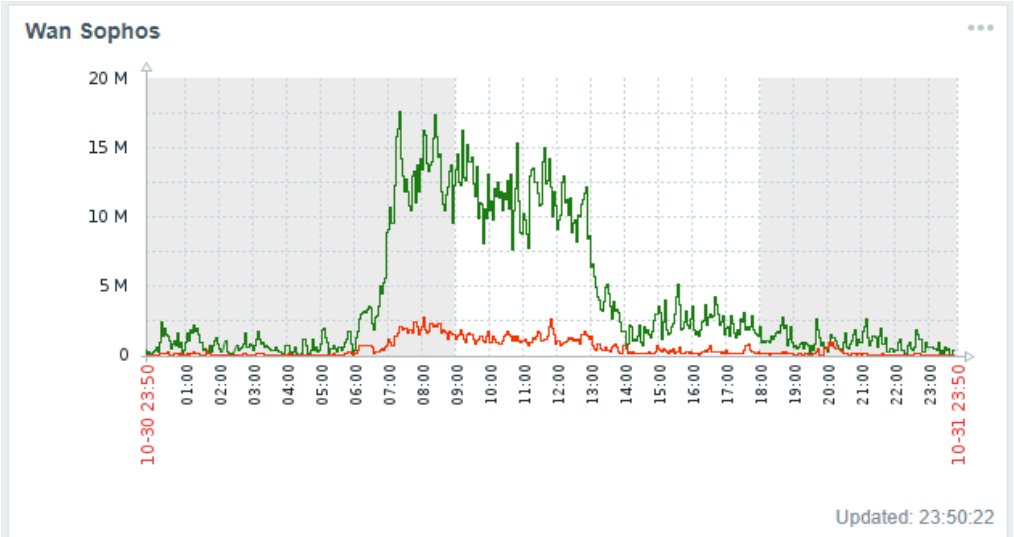
- Gráficos de cantidad de usuarios por access point a lo largo del tiempo



- Gráficos del tráfico por access point a lo largo del tiempo



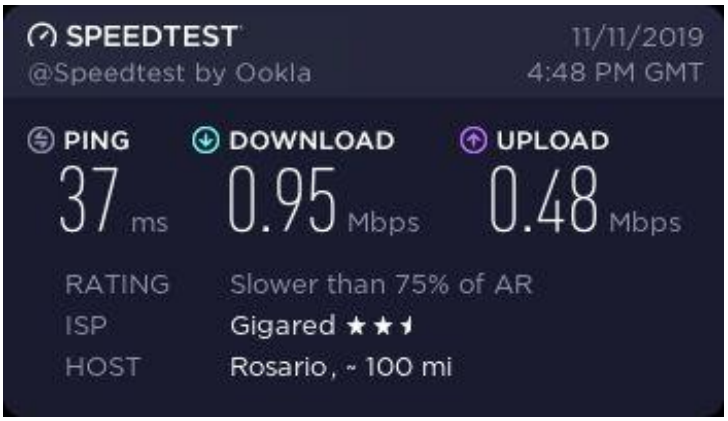
- Gráficos del tráfico en las respectivas interfaces del firewall Sophos, en este caso, una interfaz WAN.



7.4. *Testeo de calidad del servicio*

Para realizar el test de la calidad de servicio, se utilizó la aplicación web Speedtest, dicha aplicación permite realizar una prueba de ancho de banda disponible tanto de bajada como de subida contra un servidor remoto.

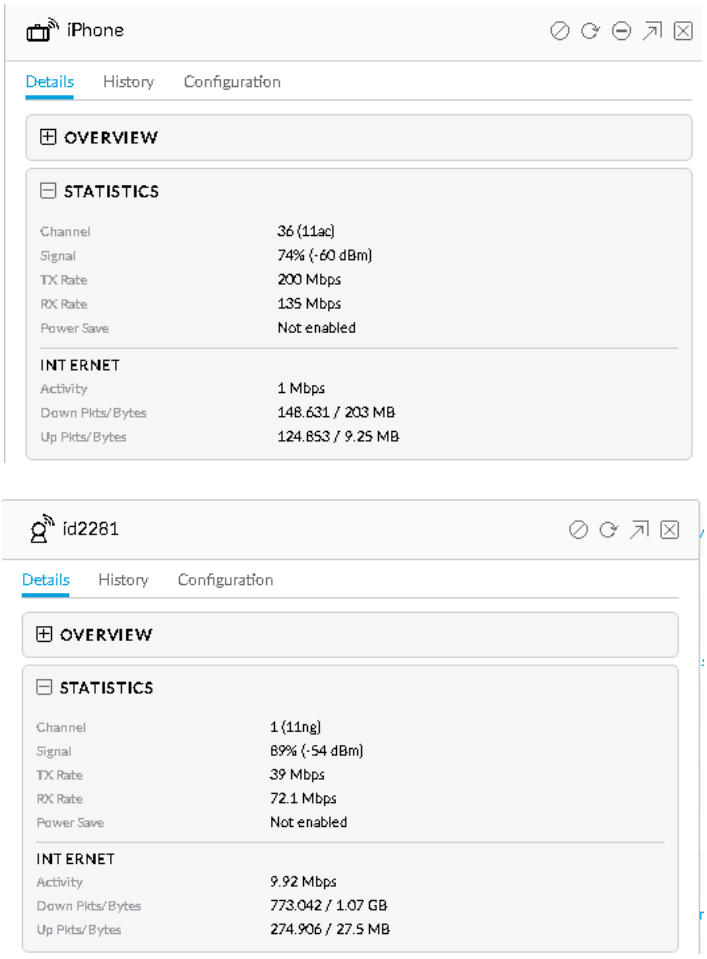
Como se puede apreciar en la imagen, para el servicio de Santafeciudad, se respetan las restricciones de ancho de banda impuestas en el Wireless Controller.



Otro aspecto a analizar y tener en cuenta a la hora de determinar la correcta utilización del servicio es la información para un cliente en particular. Dentro del panel del Wireless Controller se puede acceder a:

- Estadísticas: Estas incluyen el canal de operación, potencia de señal y tasas de transferencias
- Aspectos referidos al uso de internet: Estas incluyen uso de ancho de banda, cantidad de bytes descargados y cantidad de bytes subidos.

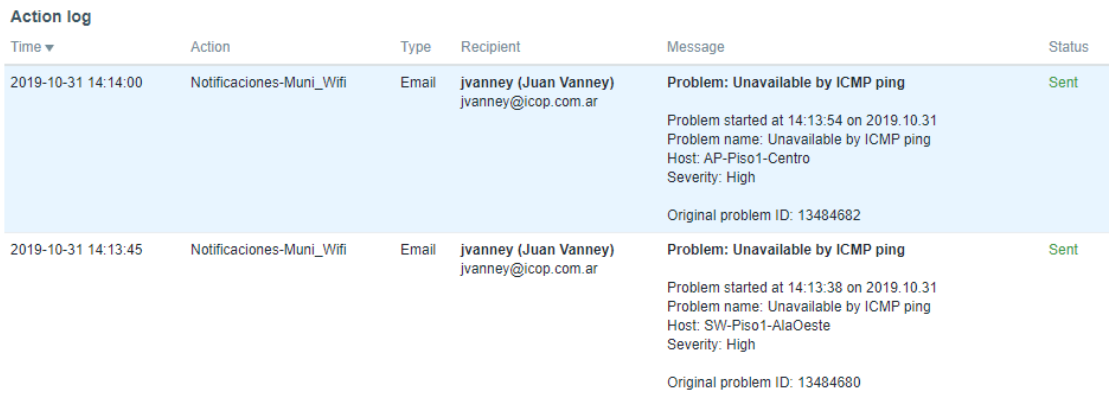
Para ejemplificar estos apartados mencionados, se muestran dos capturas, la primera correspondiente a un usuario de Santafeciudad en la banda de 5 GHz (y la correspondiente restricción de uso de ancho de banda), y la segunda correspondiente a un usuario de Redmuni con en la banda de 2,4 GHz.



7.5. *Notificaciones*

Otro aspecto muy importante es la recepción de notificaciones. A continuación se incluyen algunas capturas de las notificaciones recibidas en forma de correo electrónico según los perfiles definidos anteriormente.

La siguiente imagen corresponde a la visualización a través del panel personalizado de Zabbix, donde se puede ver las notificaciones, su mensaje y destinatario, además del estado de cada notificación.



Action log

Time ▾	Action	Type	Recipient	Message	Status
2019-10-31 14:14:00	Notificaciones-Muni_Wifi	Email	**jvanney (Juan Vanney)** jvanney@icop.com.ar	**Problem: Unavailable by ICMP ping** Problem started at 14:13:54 on 2019.10.31 Problem name: Unavailable by ICMP ping Host: AP-Piso1-Centro Severity: High Original problem ID: 13484682	Sent
2019-10-31 14:13:45	Notificaciones-Muni_Wifi	Email	**jvanney (Juan Vanney)** jvanney@icop.com.ar	**Problem: Unavailable by ICMP ping** Problem started at 14:13:38 on 2019.10.31 Problem name: Unavailable by ICMP ping Host: SW-Piso1-AlaOeste Severity: High Original problem ID: 13484680	Sent

En relación a lo mencionado, se muestra a continuación un correo recibido en una cuenta de correo de ICOP con la notificación correspondiente (en este caso la pérdida de conectividad ICMP contra un access point).

Problem: Unavailable by ICMP ping 1 mensaje

De: monitoreo@icop.com.ar 31 de Octubre 2019 14:14

Para: Juan Ignacio Vanney

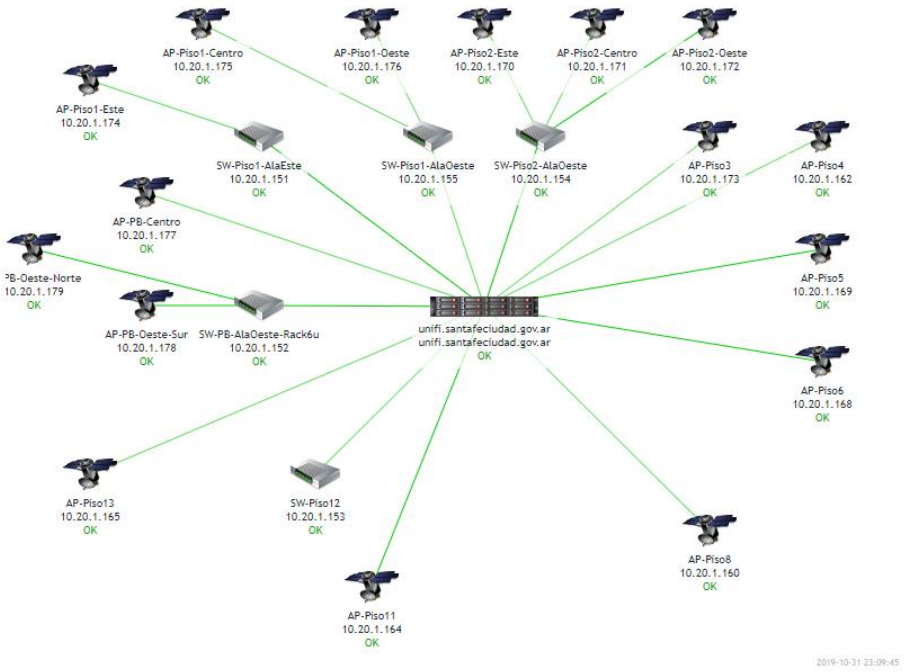
```
Problem started at 14:13:54 on 2019.10.31
Problem name: Unavailable by ICMP ping
Host: AP-Piso1-Centro
Severity: High

Original problem ID: 13484682
```

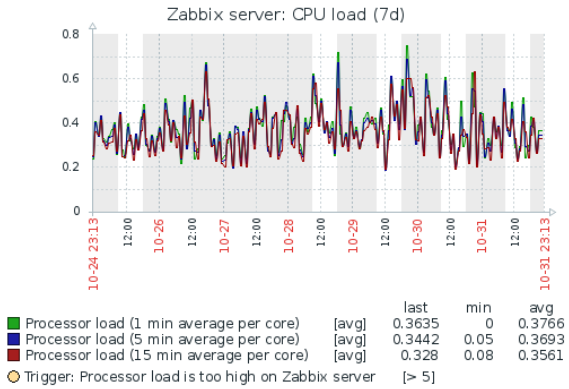
7.6. *Reportes de equipos*

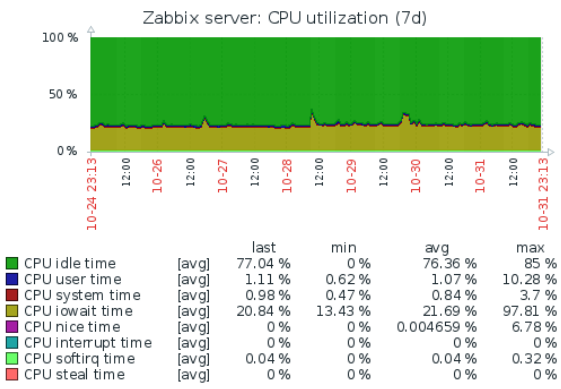
Otro aspecto que podemos visualizar a través de las herramientas de monitoreo corresponde al estado de cada uno de los dispositivos involucrados en la solución en forma de mapa.

Para ejemplificar este caso se tomaron únicamente los activos de la solución UniFi. En la imagen que se muestra a continuación se pueden ver cada uno de los dispositivos con un nombre descriptivo, su dirección IP, su conectividad física (enlaces entre los mismos) y su estado a nivel conectividad.



Además, para los servidores de la solución, podemos apreciar información de su utilización de recursos, incluyendo uso de sus interfaces de red, utilización de disco, utilización de memoria RAM, utilización de CPU, entre otros.





7.7. Capacitación

Esta etapa consistió en realizar la transferencia de conocimiento asociada a la solución implementada. Si bien, durante la implementación parte del equipo del área de infraestructura de la Muncipalidad de Santa Fe fue involucrada, a modo de cierre de la capacitación se planificó una presentación donde se explicaron los diagramas y documentación generada durante la etapa de diseño, y los ajustes realizados durante la implementación.

Por otro lado se realizó un recorrido por las interfaces gráficas de los equipos y servidores involucrados en la solución, haciendo hincapié en los que signifiquen un uso frecuente.

Luego de la presentación mencionada, se procedió a evacuar todas las consultas que hayan surgido o aspectos que no hayan quedado claros, dejando a disposición diversas vías de comunicación para realizar consultas.

7.8. Transferencia y soporte

Una vez finalizada la etapa de capacitación y entregada la documentación generada, la solución pasó a etapa de soporte.

La metodología aplicada para esta etapa, consiste en atender a los reclamos que el personal del área no pueda resolver, evacuar todas las dudas que surjan durante la operación de la solución y realizar los ajustes que se sean necesarios mientras la solución se encuentra en producción.

Por otro lado, las notificaciones frente a eventos en los dispositivos o servicios son enviadas tanto a área de ingeniería de ICOP como a personal del área de infraestructura de la Municipalidad de Santa Fe, lo que permite un seguimiento desde ambos frentes ante sucesos que afecten el servicio.

8. Conclusiones

Tecnologías utilizadas y su integración

La ejecución de este proyecto constituyó un gran desafío debido a la complejidad de herramientas y tecnologías abordadas, junto con la integración de las mismas. El uso e integración de dichos elementos, supusieron el aprendizaje tanto de aspectos conceptuales como también aspectos prácticos inherentes a cada tecnología abordada.

Aportes para el cliente

La solución implementada constituye una mejora sustancial en la calidad de servicios prestados, por lo que el cliente quedó muy conforme e interesado en hacer extensiva la solución a sus demás dependencias en un futuro. Al día de hoy, los diferentes aspectos que fueron parte de este proyecto, son herramienta fundamental para el trabajo diario de gran parte del personal municipal. Además, el servicio prestado al ciudadano posee un correcto funcionamiento acorde a sus objetivos.

Experiencia personal

El desarrollo del presente proyecto constituyó un gran aprendizaje en lo que respecta, principalmente, a aspectos relacionados a la gestión de proyecto y gestión de los recursos asignados al mismo. Además, fue necesario recurrir a diversos conocimientos adquiridos a lo largo de la carrera y en algunos casos retomar bibliografía utilizada durante el cursado de la misma.

El lugar de responsabilidad asumido para este proyecto constituyo otro gran desafío, pudiendo superar los obstáculos presentados para la conclusión del mismo en tiempo y forma.

Dada la importancia de un entendimiento amplio del problema a resolver así como los aspectos condicionantes para la solución, fue crucial la retroalimentación recibida por parte del personal municipal involucrado, así como también los aportes brindados por diversos departamentos de ICOP Santa Fe los cuales ayudaron a resolver aspectos que excedían los alcances del área.

Principales dificultades enfrentadas

- Documentación desactualizada: lo cual trajo dificultades a la hora de realizar configuraciones de equipos. Una vez detectado este problema, se procedió a

normalizar la documentación antes de continuar con la implementación (esto provocó algunos retrasos en la planificación planteada).

- Cambios en el cronograma: durante la etapa de implementación, el cliente requirió adelantar la fecha de puesta en marcha de la solución, por lo que se debió duplicar el esfuerzo para el proyecto, dejando resentidos otros de los abordados en simultáneo por la empresa.
- Restricciones organizacionales: en algunos casos por restricciones de este tipo, no fue posible la implementación de las mejores herramientas, protocolos o estándares para la situación considerada de manera aislada y se debieron realizar las negociaciones para que la solución sea acorde a lo planteado por el cliente.
- Aspectos pasados por alto por inexperiencia: el abordaje de nuevas herramientas y tecnologías hizo que en algunos casos no se hayan considerado variables sustanciales.

9. Glosario

A

Access Point (Punto de acceso inalámbrico): es un equipamiento de red que interconecta diversos dispositivos de comunicación inalámbricos para formar una red inalámbrica.

Alta Disponibilidad (HA): Es una característica de los sistemas, cuyo objetivo es garantizar un nivel acordado de rendimiento operativo, generalmente se refiere al tiempo de actividad.

C

Centro de cableado (o IDF): Corresponde a la sala donde convergen todas las conexiones del cableado horizontal de un piso. En dicho recinto se ubican los activos que conectan el cableado horizontal mencionado con el resto del edificio.

Certificado Wildcard: Es un certificado SSL (Secure Sockets Layer) mediante el cual se proporciona autenticación y privacidad de la información entre los extremos gracias al uso de criptografía. Se conoce como Wilcard (comodín) al certificado emitido para todo un dominio, pudiendo ser utilizado para todo subdominio del mismo.

Cron: En los sistemas Linux, es un administrador regular de demonios (procesos en segundo plano) que ejecuta tareas a intervalos regulares. Es un método de programar y automatizar tareas.

D

Data Center: Corresponde al espacio físico donde se concentran los recursos necesarios para el procesamiento de la información de una organización. Incluye un recinto debidamente acondicionado donde se emplazan servidores y poder de cómputo junto con dispositivos de comunicación y redes.

DDNS: es un servicio que permite la actualización en tiempo real de la información sobre nombres de dominio en un servidor de nombres. Se utiliza generalmente para permitir la asignación de un nombre de dominio (DNS) a un dispositivo con dirección IP dinámica.

DHCP: Por las siglas en Inglés "Dynamic Host Configuration Protocol", es un protocolo de configuración dinámica de host, el cual funciona bajo una arquitectura de cliente servidor. El servidor asigna dinámicamente una dirección IP, junto con otros parámetros asociados a la red para que los dispositivos puedan comunicarse.

Dig (Domain information Groper): es un comando disponible en sistemas Linux y puede ser utilizado en la gestión de redes permitiendo hacer peticiones DNS.

Dirección IP: Es una etiqueta numérica asignada a cada dispositivo conectado a una red de computadoras, siempre y cuando la se utilice el protocolo de internet para su comunicación.

Dirección MAC: Es un identificador único asociado a una tarjeta o dispositivo de red, el mismo está compuesto por 48 bits (6 bloques de dos caracteres hexadecimales). También es conocida como "Dirección física" y entre dispositivos del mismo fabricante se comparten los primeros caracteres.

DNS: La sigla DNS proviene del Inglés "Domain Name System" (Sistema de nombres de dominio) y consiste en un sistema de nomenclatura jerárquica descentralizado para dispositivos conectados a redes IP. Su función consiste en traducir nombres entendibles por las personas a identificadores binarios asociados a los equipos conectados a la red, y de esta manera, se puede direccionar y localizar a los equipos tanto de forma local como hacia internet. En resumen, un servidor DNS contesta las peticiones de clientes, y en el caso de no disponer de la dirección solicitada, los mismos re envían la petición a otro servidor.

F

Firewall: Es una pieza de hardware o software diseñada para bloquear acceso no autorizado y, al mismo tiempo, permitir el acceso autorizado. Suelen ser utilizados para evitar que los usuarios de internet (no autorizados), tengan acceso a redes privadas conectadas a internet. Todo el tráfico que entre o salga de la red privada, pasa por el firewall, y el mismo examina cada mensaje y bloquea aquellos que no cumplen con criterios de seguridad especificados.

I

IKE (Internet Key Exchange): Consiste en un protocolo utilizado para establecer los atributos de seguridad compartidos entre dos entidades de red para permitir una comunicación segura.

ISP: (del inglés "Internet service provider") o proveedor de servicio de internet, que es la empresa que brinda conexión de internet a sus clientes a través de variadas tecnologías.

L

Lease time: Dentro de un esquema de DHCP, el lease time corresponde al tiempo durante el cual una asignación de dirección IP es válida para el sistema.

O

OSI: Es un modelo de referencia para la representación de sistemas abiertos a la comunicación con otros sistemas. Está basado en una propuesta de ISO (Organización internacional de estándares) y se compone por siete capas, cada una con objetivos definidos.

P

PoE (Alimentación a través de Ethernet): Es una tecnología que incorpora alimentación eléctrica en una infraestructura LAN. Permite que la alimentación de un dispositivo utilizando el mismo cable de red que se utiliza para datos, lo que elimina la necesidad de utilizar cableado adicional para alimentar dispositivos, o acceso a tomacorrientes en la ubicación del dispositivo. PoE es regulado por la norma IEEE 802.3af.

Portal Cautivo: Es un programa que vigila el tráfico correspondiente a navegación web y fuerza a los usuarios a pasar por una página web especial que constituye un requisito para poder navegar por internet de forma normal. Es una herramienta que permite controlar el tiempo que dura la sesión de un determinado dispositivo.

Puerto SFP: Son puertos de switch particulares que brindan la posibilidad de conectarse a través de gran variedad de cables de fibra óptica y Ethernet para extender el funcionamiento a través de la red. La sigla SFP proviene del inglés por "small form-factor pluggable".

R

Rack: Estructura generalmente metálica destinada a alojar equipamiento electrónico, informático y de comunicaciones.

Router (enrutador) es un dispositivo que reenvía paquetes de datos entre redes de computadoras.

Rsync: Es una aplicación que ofrece transmisión eficiente de datos incrementales, permitiendo además la compresión y cifrado de los mismos. Se utiliza mayormente para sincronizar archivos y directorios entre dos máquinas de una red.

S

SSH (del Inglés Secure Shell): es un protocolo de red que implementa acceso remoto a un equipo por medio de un canal seguro en el que toda la información enviada y recibida se encuentra cifrada.

SSID (Service Set Identifier): Es un identificador único de una red inalámbrica, consiste en un código de hasta 32 caracteres, normalmente alfanuméricos. Todos los paquetes de una red inalámbrica incluyen la información de SSID al que pertenecen.

Switch de core: Es un dispositivo de conmutación ubicado en el núcleo de la estructura de red. Para dicho dispositivo se requieren altas velocidades de conmutación y capacidades adicionales como manejo de VLAN, protocolos de ruteo, entre otros.

T

Telnet: (del ingles Telecommunication Network) es un protocolo de red para acceder a un equipo y manejarlo remotamente de manera similar a estar frente al mismo.

Trama: Es una unidad de envío de datos, consiste en una serie sucesiva de bits organizados en forma cíclica que transportan información y permiten extraer dicha información por parte del receptor.

U

Uplink: Corresponde al enlace de comunicación entre dos equipos.

W

Wireless controller: Es una solución de software dedicada a administrar y optimizar los recursos de una solución WiFi con los objetivos de dar visibilidad y mantener calidad en el servicio ofrecido.

WLAN: Red inalámbrica local (Wireless local area network por sus siglas en inglés) es una red informática inalámbrica que conecta dos o más dispositivos con dicha tecnología, dentro de un área limitada. Ofrece a los usuarios la capacidad de moverse dentro del área sin desconectarse de la red. La mayoría de las WLAN modernas se basan en los estándares IEEE 802.11.

WPA2 (WiFi Protected Access 2): Es un sistema para proteger las redes inalámbricas, y constituye una evolución del protocolo WPA. WPA permite la autenticación por clave pre-compartida.

10. Bibliografia

[1] Sommerville, Ian – "Ingeniería del software" – Séptima Edición 2005

[2] Pressman, Roger S. – "Ingeniería del software. Un enfoque práctico" – Séptima Edición 2010

[3] Fairley, Richard E. – "Managing and Leading Software Projects" – 2009

[4] Ordoñez Luque, Javier – "Comunicaciones Unificadas: Integracion y convergencia de las comunicaciones coorporativas" – 2009

[5] Tanenbaum, Andrew S. – "Redes de Computadoras" – Cuartas Edición 2009

[6] Vincent Ferrer – Certificador de Redes – https://vicentferrer.com/certificador-de-redes/

[7] Install and configure DNS server in Ubuntu 16.04 LTS - https://www.ostechnix.com/install-and-configure-dns-server-ubuntu-16-04-lts/

[8] Alejandro Alcalde – Cómo configurar un servidor DNS - https://elbauldelprogramador.com/como-configurar-un-servidor-dns/

[9] Sophos XG Firewall: How to configure High Availability - https://community.sophos.com/kb/en-us/123174

[10] How to Install & Upgrade the UniFi Network Controller Software - https://help.ubnt.com/hc/en-us/articles/360012282453-UniFi-How-to-Install-Upgrade-the-UniFi-Network-Controller-Software

[11] How to install Ubuntu server 16.04 and the Webmin GUI - https://www.techrepublic.com/article/how-to-install-ubuntu-server-16-04-and-the-web-based-admin-tool-webmin/

[12] How To Install Webmin on Ubuntu 16.04 - https://www.digitalocean.com/community/tutorials/how-to-install-webmin-on-ubuntu-16-04

[13] Instalar y configurar zabbix - https://www.programadornovato.com/2017/12/instalar-y-configurar-zabbix.html

[14] Use of Black hole route in site to site IPsec VPN scenarios - https://kb.fortinet.com/kb/documentLink.do?externalID=FD36695

[15] Articulos consultados en Wikipedia:

https://en.wikipedia.org/wiki/WPA2

https://en.wikipedia.org/wiki/Wireless_LAN

https://es.wikipedia.org/wiki/Trama_de_red

https://en.wikipedia.org/wiki/Telnet

https://es.wikipedia.org/wiki/SSID

https://en.wikipedia.org/wiki/Secure_Shell

https://en.wikipedia.org/wiki/Rsync

https://es.wikipedia.org/wiki/Power_over_Ethernet

https://es.wikipedia.org/wiki/Internet_key_exchange

https://en.wikipedia.org/wiki/Dig_(command)

https://en.wikipedia.org/wiki/Dynamic_DNS

https://en.wikipedia.org/wiki/Cron

https://en.wikipedia.org/wiki/Wireless_access_point

11. Anexos

Costos de equipamiento y cableado

Item	Cant.	Costo U.	Costo T.	Subtotal
Datos				
Puestos Nuevos	**20**			$ 73.554,00
Cable UTP Cat 6 Furukawa x Caja	2	$ 8.800,00	$ 17.600,00	
PLUG Cat 6, Furukawa	50	$ 48,00	$ 2.400,00	
Frente de Patchera Descargado	9	$ 2.544,00	$ 22.896,00	
Jack Cat 6	32	$ 350,00	$ 11.200,00	
Roseta 2 port	32	$ 125,00	$ 4.000,00	
Patchcord UTP Cat 6 de 0,5 mts, Furukawa	28	$ 275,00	$ 7.700,00	
Patchcord UTP Cat 6 de 1,0mts, Furukawa	33	$ 226,00	$ 7.458,00	
Certificacion y Etiquetado	20	$ 15,00	$ 300,00	
Ductos				$ 7.000,00
CABLECANAL 18X 21 MM C/ADHES BLANCO	100	$ 67,00	$ 6.700,00	
Accesorios	50	$ 6,00	$ 300,00	
Mano de Obra				$ 35.250,00
Mano de Obra Cableado	80	$ 300,00	$ 24.000,00	
Mano de Obrado de Instalación.	20	$ 300,00	$ 6.000,00	
Ferretería Cableado	1	$ 5.250,00	$ 5.250,00	
Activos				
				$ 366.290,00
UniFi AC PRO	19	$ 8.223,00	$ 156.237,00	
Switch POE	13	$ 7.349,00	$ 95.537,00	
Firewall Sophos XG310	2	$ 51.034,00	$ 102.068,00	
Switch HPE 1920S-24G	1	$ 12.448,00	$ 12.448,00	

TOTAL	$ 482.094,00

12. Anexo Implementación de la solución.

12.1. Cableado e instalación física de dispositivos.

12.1.1. Ejemplo reporte de certificación de cableado

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: 10-R1-P02-B01
Fecha / Hora: 28/09/2018 01:03:01 PM
Paso Libre 6.1 dB (NEXT 1,2-7,8)
Limite de Prueba: TIA Cat 6 Channel (+All)
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: Vanney, Juan Ignacio
Versión de Software: V5.2 Build 1
Version de Limites: V6.1
Calibración fecha de inicio:
Principal (Modulo): 13/06/2018
Remoto (Modulo): 13/06/2018

Sumario de Pruebas: PASA
Modelo: DSX-5000
Principal N/S: 17350088
Remoto N/S: 17350085
Adaptador Principal: DSX-CHA004
Adaptador Remoto: DSX-CHA004

Longitud (m), Lím. 100.0	[Par 3,6]	35.6
Tiempo de Prop. (ns), Lím. 555	[Par 4,5]	180
Diferencia Retardo (ns), Lím. 50	[Par 4,5]	8
Resistencia (ohm.)		N/A
Pérdida inserción Margen (dB)	[Par 4,5]	24.0
Frecuencia (MHz)	[Par 4,5]	250.0
Límite (dB)	[Par 4,5]	35.9

35.6 m

Mapa de Cableado (T568B)
PASA

Pérdida inserción (dB)

Margen de Peor Caso / Valor de Peor Valor

PASA	MAIN	SR	MAIN	SR
Peor Par	1,2-7,8	3,6-4,5	1,2-7,8	3,6-4,5
NEXT (dB)	6.1	8.9	6.1	10.7
Frec. (MHz)	188.5	43.8	188.5	199.0
Límite (dB)	35.2	46.0	35.2	34.8
Peor Par	7,8	3,6	7,8	3,6
PS NEXT (dB)	8.9	10.3	8.9	12.9
Frec. (MHz)	188.5	43.8	188.5	199.0
Límite (dB)	32.3	43.2	32.3	31.9

NEXT (dB) | NEXT @ Remoto (dB)

PASA	MAIN	SR	MAIN	SR
Peor Par	3,6-4,5	4,5-3,6	3,6-4,5	4,5-3,6
ACR-F (dB)	11.6	12.0	11.6	12.0
Frec. (MHz)	250.0	250.0	250.0	250.0
Límite (dB)	15.3	15.3	15.3	15.3
Peor Par	4,5	4,5	4,5	4,5
PS ACR-F (dB)	14.0	13.9	14.2	14.7
Frec. (MHz)	1.3	1.1	250.0	250.0
Límite (dB)	58.3	59.2	12.3	12.3

ACR-F (dB) | ACR-F @ Remoto (dB)

N/A	MAIN	SR	MAIN	SR
Peor Par	3,6-4,5	3,6-4,5	3,6-4,5	3,6-4,5
ACR-N (dB)	13.8	12.9	33.1	31.5
Frec. (MHz)	15.9	3.0	248.5	199.0
Límite (dB)	45.3	61.5	-2.7	3.4
Peor Par	3,6	3,6	4,5	4,5
PS ACR-N (dB)	15.8	14.7	35.8	39.0
Frec. (MHz)	15.9	3.0	248.5	241.5
Límite (dB)	42.6	58.5	-5.6	-4.8

ACR-N (dB) | ACR-N @ Remoto (dB)

PASA	MAIN	SR	MAIN	SR
Peor Par	3,6	3,6	7,8	3,6
RL (dB)	3.6	3.1	7.2	3.2
Frec. (MHz)	40.5	171.5	232.5	172.0
Límite (dB)	15.9	9.7	8.3	9.6

RL (dB) | RL @ Remoto (dB)

Estándares de Red Compatibles:
10BASE-T 100BASE-TX 100BASE-T4
1000BASE-T 2.5GBASE-T 5GBASE-T
ATM-25 ATM-51 ATM-155
100VG-AnyLan TR-4 TR-16 Active
TR-16 Passive

LinkWare™ PC Versión 10.3

Proyecto: Wifi Palacio Municipal
Edificio: Municipalidad de la Ciudad de Santa Fe
Rack: N°_1

Wifi Palacio Municipal.flw
Piso: _ 10mo

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: 10-R1-P02-B01

Sumario de Pruebas: PASA

Fecha / Hora: 28/09/2018 01:03:01 PM
Paso Libre 6.1 dB (NEXT 1,2-7,8)
Limite de Prueba: TIA Cat 6 Channel (+All)
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: Vanney, Juan Ignacio
Versión de Software: V5.2 Build 1
Version de Limites: V6.1
Calibración fecha de inicio:
Principal (Modulo): 13/06/2018
Remoto (Modulo): 13/06/2018

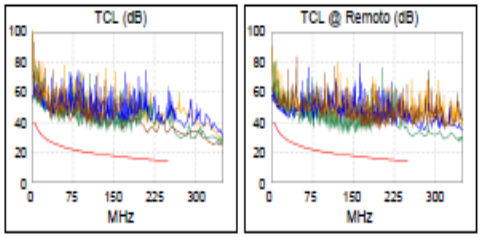
Modelo: DSX-5000
Principal N/S: 17350088
Remoto N/S: 17350085
Adaptador Principal: DSX-CHA004
Adaptador Remoto: DSX-CHA004

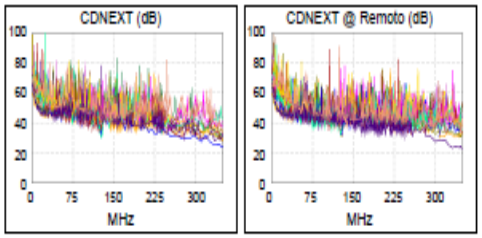
	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	3,6	4,5	7,8	3,6
TCL (dB)	13.5	12.9	17.2	16.1
Frec. (MHz)	1.3	4.8	247.0	154.0
Límite (dB)	40.0	39.8	14.1	17.2

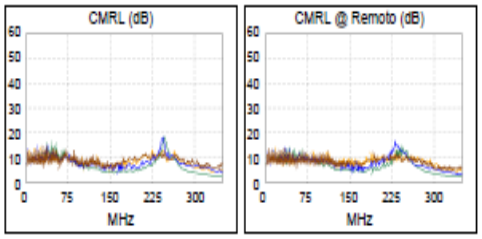
N/A	MAIN	SR	MAIN	SR
Peor Par			1,2-7,8	7,8-3,6
CDNEXT (dB)			23.7	22.6
Frec. (MHz)			350.0	350.0
Límite (dB)				

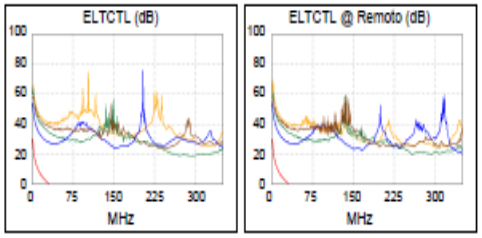
N/A	MAIN	SR	MAIN	SR
Peor Par			3,6	3,6
CMRL (dB)			2.4	2.3
Frec. (MHz)			338.0	331.0
Límite (dB)				

PASA	MAIN	SR	MAIN	SR
Peor Par	4,5	4,5	4,5	4,5
ELTCTL (dB)	23.9	23.8	27.2	27.0
Frec. (MHz)	1.3	1.3	30.0	30.0
Límite (dB)	28.1	28.1	0.5	0.5









LinkWare™ PC Versión 10.3

Proyecto: Wifi Palacio Municipal
Página 2
Piso: ._ 10mo

Wifi Palacio Municipal.flw
Edificio: Municipalidad de la Ciudad de Santa Fe
Rack: N°_1

FLUKE networks

12.2. Puesta en marcha de equipos y servicios

12.2.1. Instalación del servidor Wireless controller y Certificado Wildcard

Para la puesta en marcha del UniFi Controller en un servidor Ubuntu, primero debemos descargar e instalar los paquetes requeridos.

```
wget http://dl.ubnt.com/unifi/5.6.29/unifi_sysvinit_all.deb
dpkg -i unifi_sysvinit_all.deb
apt-get -f install
```

Una vez finalizada la instalación se puede acceder a la interfaz web de UniFi Controller a través de la siguiente dirección:

```
https://ip_servidor:8443
```

Instalación de certificado SSL

Concatenación de los diferentes certificados que componen la cadena de certificación

```
cat COMODORSAAddTrustCA.crt
COMODORSADomainValidationSecureServerCA.crt
AddTrustExternalCARoot.crt > commercial_ca.crt
```

Utilizando las herramientas openssl y keytool:

```
openssl pkcs12 -export -in
/tmp/STAR_santafeciudad_gov_ar/STAR_santafeciudad_gov_ar.crt -
inkey /tmp/STAR_santafeciudad_gov_ar/commercial.key -certfile
/tmp/STAR_santafeciudad_gov_ar/commercial_ca.crt -out UniFi.p12
-name "*.santafeciudad.gov.ar" -password pass:password


keytool -importkeystore -srckeystore UniFi.p12 -srcstoretype
PKCS12 -srcstorepass password -destkeystore
/usr/lib/UniFi/data/keystore -storepass password
```

Para luego reiniciar el servicio con el siguiente comando:

```
/etc/init.d/UniFi restart
```

12.2.2. Archivos de configuración para el servidor DNS

Instalación de Bind en servidor Ubuntu.

```
sudo apt-get update
sudo apt-get install bind9 bind9utils bind9-doc
```

Fragmento relevante del archivo named.conf:

```
[…]
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
[…]
```

Fragmento relevante del archivo named.conf.options:

```
[…]
options {
      directory "/var/cache/bind";
      forwarders {
            8.8.8.8;
            8.8.4.4;
      };
------------------------
};
[…]
```

Fragmento relevante del archivo named.conf.local:

```
[…]
zone "santafeciudad.gov.ar" {
        type master;
        file "/etc/bind/for.santafeciudad.gov.ar";
};
zone "0.20.10.in-addr.arpa" {
        type master;
        file "/etc/bind/rev.santafeciudad.gov.ar";
 };
[…]
```

Fragmento relevante del archivo for.santafeciudad.gov.ar:

```
$TTL 86400
@     IN    SOA   pri.santafeciudad.gov.ar.
root.santafeciudad.gov.ar. (
                  2018042638
                  3600
                  1800
                  604800
                  86400 )
@           IN  NS      pri
@                 IN    MX    10    mail.santafeciudad.gov.ar
santafeciudad.gov.ar.   IN    A     X.X.X.X


pri               IN    A     10.20.0.122
mail        IN    A     X.X.X.X
muniweb1    IN    A     X.X.X.X
muniweb2    IN    A     X.X.X.X
munisvn           IN    A     X.X.X.X
munired01   IN    A     X.X.X.X
[…]
```

Fragmento relevante del archivo rev.santafeciudad.gov.ar:

```
$TTL 86400
@     IN    SOA   pri.santafeciudad.gov.ar.
root.santafeciudad.gov.ar. (
                  2011071031
                  3600
                  1800
                  604800
                  86400 )
@       IN  NS          pri.santafeciudad.gov.ar
@       IN  PTR         santafeciudad.gov.ar.
pri     IN  A           10.20.0.122
79      IN  PTR         pri.santafeciudad.gov.ar
pri.santafeciudad.gov.ar IN A 10.20.0.122
158.0.20.10.in-addr.arpa.     IN    PTR
      portaldatos.santafeciudad.gov.ar.
52.0.20.10.in-addr.arpa.      IN    PTR
      websat2.santafeciudad.gov.ar.
65.0.20.10.in-addr.arpa.      IN    PTR
      pg11pro.santafeciudad.gov.ar.
120.0.20.10.in-addr.arpa.     IN    PTR
      pg9pro.santafeciudad.gov.ar.
[…]
```

Una vez realizadas las configuraciones, verificamos que los archivos de configuración sean correctos en su estructura para luego reiniciar el servicio.

```
named-checkconf /etc/bind/named.conf
named-checkconf /etc/bind/named.conf.local
named-checkconf /etc/bind/named.conf.options
named-checkconf /etc/bind/for.santafeciudad.gov.ar
named-checkconf /etc/bind/rev.santafeciudad.gov.ar


systemctl restart bind9
```

12.2.3. Instalación y configuración de Webmin

Instalación de webmin en el servidor Ubuntu:

```
wget http://www.webmin.com/jcameron-key.asc
apt-key add jcameron-key.asc
sudo apt-get update
apt-get install webmin
```

Una vez finalizada la instalación se puede acceder a la interfaz web de Webmin a través de la siguiente dirección:

```
http://ip_servidor:10000
```

12.2.4. Archivos de configuración para el servidor DHCP

Instalación de DHCPD en servidor Ubuntu:

```
sudo apt-get update
sudo apt-get install isc-dhcp-server –y
```

Fragmento relevante del archivo dhcpd.failover:

```
failover peer "mcsf" {
         primary;
         address 10.20.X.X;
         port 647;
         peer address 10.20.X.Y;
         peer port 647;
         max-response-delay 5;
         max-unacked-updates 10;
         mclt 3600;
         split 128;
```

```
         load balance max seconds 3;
        }
```

Fragmento relevante del archivo dhcpd.conf:

```
option T150 code 150 = string;
ddns-update-style interim;
ddns-updates off;
allow client-updates;
one-lease-per-client false;
allow bootp;
#option wpad-url code 252 = string;
authoritative;
log-facility local5;
option x-display-manager 10.20.0.X;
option tftp-server-name "10.20.0.X";
include "/etc/dhcpd.failover";


# Red Municipalidad de la Ciudad de Santa fe
shared-network Municipalidad {



      # INFRAESTRUCTURA
      subnet 10.20.0.0 netmask 255.255.252.0 {
            option routers 10.20.0.X;
            option subnet-mask 255.255.252.0;
            option domain-name-servers 10.20.X.X;
            option time-offset -18000;
            max-lease-time 86400;
            default-lease-time 43200;
            pool {
                  failover peer "mcsf";
                  range 10.20.0.X 10.20.0.Y;
                  deny dynamic bootp clients;
                  deny unknown-clients;
                  }


            # Grupo de APs IPS
            group {
            # Ubiquiti - UniFi AP AC Pro - 8vo Piso
            host UnifiAPACPro8voPiso {
                  hardware ethernet f0:9f:c2:c8:f0:e7;
                  fixed-address 10.20.1.160;
                  }
            # Ubiquiti - Unifi AP AC Pro - 10mo Piso
            host UnifiAPACPro10moPiso {
                  hardware ethernet 78:8a:20:26:08:7b;
                  fixed-address 10.20.1.161;
                  }
            [...]
            }
      [...]
      }
```

```
[...]
}
```

Sincronización entre servidor primario y secundario:

```
rsync -avz backup@10.X.X.X:/etc/dhcp/dhcpd.conf /etc/dhcp
```

Este comando se ejecuta en el servidor secundario, una vez sincronizado el archivo, el script reinicia el servicio correspondiente.

```
service dhcpd restart
```

Instalación y configuración de Zabbix

El primer paso es instalar todos los paquetes necesarios

```
sudo apt-get update
sudo apt-get install php7.0-xml php7.0-bcmath php7.0-mbstring
wget http://repo.zabbix.com/zabbix/3.2/ubuntu/pool/main/z/zabbix
-release/zabbix-release_3.2-1+xenial_all.deb


sudo dpkg -i zabbix-release_3.2-1+xenial_all.deb
sudo apt-get update
sudo apt-get install zabbix-server-mysql zabbix-frontend-php
```

Una vez instalados los paquetes, debemos hacer las configuraciones correspondientes a la base de datos, para ello debemos iniciar sesión en mysql.

```
mysql -uroot –p
```

Una vez dentro, es necesario crear una base de datos para Zabbix y darle los privilegios a un usuario zabbix.

```
mysql> create database zabbix character set utf8 collate
utf8_bin;
mysql> grant all privileges on zabbix.* to zabbix@localhost
identified by 'password';
mysql> flush privileges;
mysql> quit;
```

Luego, procedemos importar el esquema inicial para la base de datos de Zabbix desde la plantilla disponible.

```
zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -
uzabbix -p zabbix
```

Modificando el archivo /etc/zabbix/zabbix_server.conf.

```
LogFile=/var/log/zabbix/zabbix_server.log
LogFileSize=0
PidFile=/var/run/zabbix/zabbix_server.pid
DBName=zabbix
DBUser=zabbix
DBPassword=password
StartPollers=50
StartPingers=5
Timeout=4
AlertScriptsPath=/usr/lib/zabbix/alertscripts
ExternalScripts=/usr/lib/zabbix/externalscripts
FpingLocation=/usr/bin/fping
Fping6Location=/usr/bin/fping6
LogSlowQueries=3000
```

Y el archivo /etc/zabbix/apache.conf.

```
    <IfModule mod_php7.c>
        php_value max_execution_time 300
        php_value memory_limit 128M
        php_value post_max_size 16M
        php_value upload_max_filesize 2M
        php_value max_input_time 300
        php_value always_populate_raw_post_data -1
        php_value date.timezone America/Argentina/Buenos_Aires
    </IfModule>
```

Solo resta reiniciar los servicios.

```
sudo systemctl restart apache2
sudo systemctl start zabbix-server
sudo systemctl enable zabbix-server
```

Instalación y configuración del Agente Zabbix en servidor Ubuntu

```
sudo apt-get update
wget http://repo.zabbix.com/zabbix/3.2/ubuntu/pool/main/z/zabbix
-release/zabbix-release_3.2-1+xenial_all.deb
sudo dpkg -i zabbix-release_3.2-1+xenial_all.deb
sudo apt-get update
sudo apt-get install zabbix-agent
```

Configurando el archivo /etc/zabbix/zabbix_agentd.conf según los datos que siguen:

```
LogFile=/var/log/zabbix/zabbix_agentd.log
LogFileSize=0
Server=10.20.0.179,127.0.0.1,::/0
ServerActive=127.0.0.1
Hostname=unifi.santafeciudad.gov.ar
Include=/etc/zabbix/zabbix_agentd.d/*.conf
```

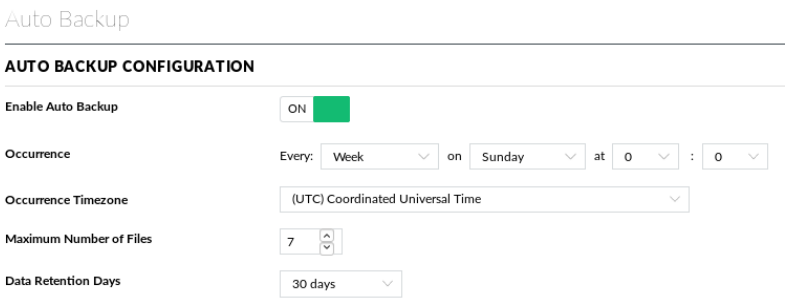
Solo resta establecer el inicio automático del agente e iniciar el servicio manualmente.

```
sudo systemctl enable zabbix-agent
sudo systemctl start zabbix-agent
```

Configuración de Backups

- Backup Servidor UniFi:

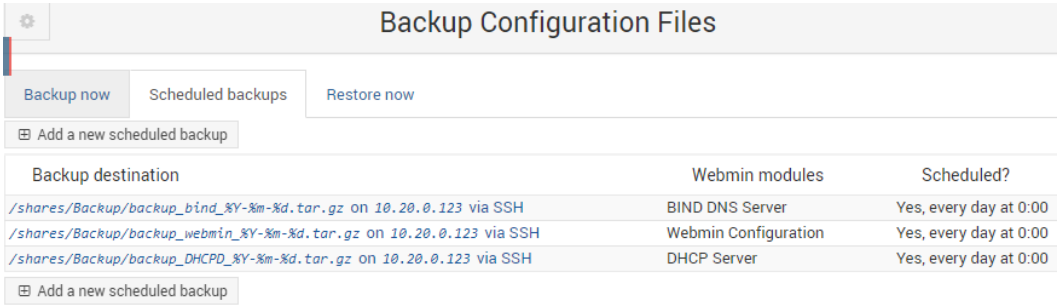
  Se configuró un backup automático desde la funcionalidad que provee UniFi, el mismo se realiza semanalmente. A continuación se muestra una captura de la implementación mencionada.



- Backup Servidor DHCPD y Bind

  En ambos servidores fue instalada la herramienta Webmin, dicha herramienta permite automatizar las tareas de backup de diversos módulos, para este caso se

programaron tareas de respaldo diarias para las configuraciones requeridas. A continuación se puede ver un ejemplo de la programación mencionada.



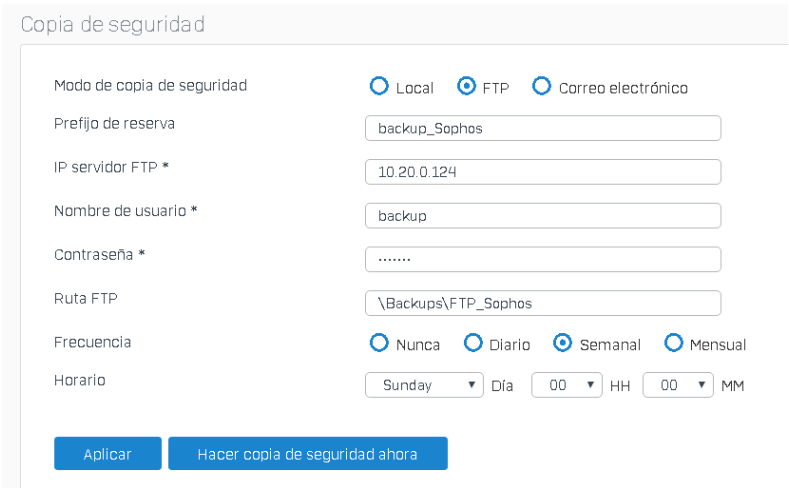
- Backup base de datos Zabbix

  Para este caso se utilizó un script, el mismo realiza un backup de la base de datos utilizando el la utilidad "dump", la misma permite generar un archivo de texto con la información necesaria para restablecer/migrar la base de datos desde cero.

  El script completo se puede obtener del siguiente enlace:

  https://github.com/bbrendon/zabbixzone/blob/master/zabbix-mysql-backupconf.sh

- Backup de Firewall Sophos: Nuevamente se hizo uso de las herramientas automatizadas provistas por el equipo. A continuación se deja una captura de la configuración del mismo para realizar los backup de manera semanal.



Cabe aclarar, que todas las máquinas virtuales creadas para este proyecto, fueron incluidas en el esquema de replicación y backup que posee la toda la infraestructura virtualizada de la Municipalidad de Santa Fe. Dicha replicación se maneja de manera

automatizada con herramientas provistas por el Hypervisor utilizado, quedando fuera del alcance de este proyecto.

12.2.5. Archivo de configuración switch de distribución

Fragmento relevante de la configuración del switch de distribución de la solución:

```
vlan 1
 description VLAN 0001 - Adm MetroFe
vlan 2
 description VLAN 0002 - LAN Muni
vlan 3
 description VLAN 0003 - WAN 1
vlan 4
 description VLAN 0004 - WAN 2
vlan 100
 description VLAN 0100
vlan 101
 description VLAN 0101
vlan 102
 description VLAN 0102
vlan 103
 description VLAN 0103
vlan 104
 description VLAN 0104
vlan 105
 description VLAN 0105
#
interface Vlan-interface1
 ip address 10.50.0.20 255.255.255.248
interface Vlan-interface101
 ip address 10.82.0.249 255.255.192.0



#
interface GigabitEthernet1/0/5
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 100 to 105 tagged
 port hybrid vlan 2 untagged
 port hybrid pvid vlan 2


interface GigabitEthernet1/0/6
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 100 to 105 tagged
 port hybrid vlan 2 untagged
 port hybrid pvid vlan 2


interface GigabitEthernet1/0/7
 port link-type hybrid
 undo port hybrid vlan 1
```

```
 port hybrid vlan 100 to 105 tagged
 port hybrid vlan 2 untagged
 port hybrid pvid vlan 2
```

```
interface GigabitEthernet1/0/8
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 100 to 105 tagged
 port hybrid vlan 2 untagged
 port hybrid pvid vlan 2

interface GigabitEthernet1/0/9
 port access vlan 3

interface GigabitEthernet1/0/10
 port access vlan 3

interface GigabitEthernet1/0/11
 port access vlan 3

interface GigabitEthernet1/0/12
 port access vlan 3

interface GigabitEthernet1/0/13
 port access vlan 4

interface GigabitEthernet1/0/14
 port access vlan 4

interface GigabitEthernet1/0/15
 port access vlan 4

interface GigabitEthernet1/0/16
 port access vlan 4

interface GigabitEthernet1/0/17
 port access vlan 100

interface GigabitEthernet1/0/18
 port access vlan 101

interface GigabitEthernet1/0/19
 port access vlan 102

interface GigabitEthernet1/0/20
 port access vlan 103

interface GigabitEthernet1/0/21
 port access vlan 104

interface GigabitEthernet1/0/22
 port access vlan 105

interface GigabitEthernet1/0/23
 port link-type hybrid
 port hybrid vlan 1 untagged
 port hybrid vlan 100 to 105 tagged
 port hybrid pvid vlan 1

interface GigabitEthernet1/0/24
```

```
 port link-type hybrid
 port hybrid vlan 1 untagged
 port hybrid vlan 100 to 105 tagged
 port hybrid pvid vlan 1
interface GigabitEthernet1/0/25
 port access vlan 3
```

12.2.6. Archivo de configuración switch en centro de cableado y Datacenter

A continuación se muestra un ejemplo los comandos utilizados en los switch ubicados en el datacenter y los centros de cableado.

Switch de Core (Chasis de la marca Allied Telesis):

```
#
# VLAN general configuration
#
create vlan="WiFi-RedMuni" vid=100
create vlan="WiFi-SantaFeCiudad" vid=101
create vlan="WiFi-Invitado" vid=102
create vlan="WiFi-Evento1" vid=103
create vlan="WiFi-Evento2" vid=104
create vlan="WiFi-Evento3" vid=105

#
# VLAN port configuration
#
add vlan="101" port=3.2
add vlan="100" port=1.1-1.2,1.4-1.8,2.1-2.7,3.1 frame=tagged
add vlan="101" port=1.1-1.2,1.4-1.8,2.1-2.7,3.1 frame=tagged
add vlan="102" port=1.1-1.2,1.5-1.8,2.2-2.7,3.1 frame=tagged
add vlan="103" port=1.1-1.2,1.5-1.8,2.2-2.7,3.1 frame=tagged
add vlan="104" port=1.1-1.2,1.5-1.8,2.2-2.7,3.1 frame=tagged
add vlan="105" port=1.1-1.2,1.5-1.8,2.2-2.7,3.1 frame=tagged

#
# IP configuration
#
enable ip
add ip int=vlan1-0 ip=10.20.X.X mask=255.255.252.0
add ip dns prim=10.40.X.X
```

Switch cabecera del 8° Piso (Switch de la marca HP):

```
interface ethernet g21
description Uplink-Core
exit

vlan database
vlan 55,80-81,100-105
exit
interface range ethernet g(2,10,13,20-24)
switchport trunk allowed vlan add 100
```

```
exit
interface range ethernet g(2,10,13,20-24)
switchport trunk allowed vlan add 101
exit
interface range ethernet g(2,10,13,20-24)
switchport trunk allowed vlan add 102
exit
interface range ethernet g(2,10,13,20-24)
switchport trunk allowed vlan add 103
exit
interface range ethernet g(2,10,13,20-24)
switchport trunk allowed vlan add 104
exit
interface range ethernet g(2,10,13,20-24)
switchport trunk allowed vlan add 105
exit

interface vlan 100
name WiFi-RedMuni
exit
interface vlan 101
name WiFi-SantaFeCiudad
exit
interface vlan 102
name WiFi-Invitado
exit
interface vlan 103
name WiFi-Evento1
exit
interface vlan 104
name WiFi-Evento2
exit
interface vlan 105
name WiFi-Evento3
interface vlan 1
ip address 10.20.X.X 255.255.252.0
exit
ip default-gateway 10.20.X.X
hostname "Cabecera Piso8"
```

Switch Dell en centro de cableado:

```
interface ethernet g3
switchport mode trunk
exit

interface ethernet g4
switchport mode trunk
exit

vlan database
vlan 100-105
exit
interface ethernet g3
switchport trunk allowed vlan add 100
exit
interface ethernet g3
switchport trunk allowed vlan add 101
exit
```

```
interface ethernet g3
switchport trunk allowed vlan add 102
exit
interface ethernet g3
switchport trunk allowed vlan add 103
exit
interface ethernet g3
switchport trunk allowed vlan add 104
exit
interface ethernet g3
switchport trunk allowed vlan add 105
exit
interface ethernet g4
switchport trunk allowed vlan add 100
exit
interface ethernet g4
switchport trunk allowed vlan add 101
exit
interface ethernet g4
switchport trunk allowed vlan add 102
exit
interface ethernet g4
switchport trunk allowed vlan add 103
exit
interface ethernet g4
switchport trunk allowed vlan add 104
exit
interface ethernet g4
switchport trunk allowed vlan add 105
exit

interface vlan 100
name WiFi-RedMuni
exit
interface vlan 101
name WiFi-SantaFeCiudad
exit
interface vlan 102
name WiFi-Invitado
exit
interface vlan 103
name WiFi-Evento1
exit
interface vlan 104
name WiFi-Evento2
exit
interface vlan 105
name WiFi-Evento3
exit
```

Switch Allied telesis en centro de cableado:

```
interface ethernet g1
switchport mode trunk
exit
interface ethernet g2
switchport mode trunk
exit
vlan database
```

```
vlan 100-105
exit
interface ethernet g1
switchport trunk allowed vlan add 100
exit
interface ethernet g1
switchport trunk allowed vlan add 101
exit
interface ethernet g1
switchport trunk allowed vlan add 102
exit
interface ethernet g1
switchport trunk allowed vlan add 103
exit
interface ethernet g1
switchport trunk allowed vlan add 104
exit
interface ethernet g1
switchport trunk allowed vlan add 105
exit

interface ethernet g2
switchport trunk allowed vlan add 100
exit
interface ethernet g2
switchport trunk allowed vlan add 101
exit
interface ethernet g2
switchport trunk allowed vlan add 102
exit
interface ethernet g2
switchport trunk allowed vlan add 103
exit
interface ethernet g2
switchport trunk allowed vlan add 104
exit
interface ethernet g2
switchport trunk allowed vlan add 105
exit

interface vlan 100
name WiFi-RedMuni
exit
interface vlan 101
name WiFi-SantaFeCiudad
exit
interface vlan 102
name WiFi-Invitado
exit
interface vlan 103
name WiFi-Evento1
exit
interface vlan 104
name WiFi-Evento2
exit
interface vlan 105
name WiFi-Evento3
```

Switch HP en centro de cableado:

```
# configure

(config)# interface vlan 100
(config)# name WiFi-RedMuni
(config)# exit
(config)# interface vlan 101
(config)# name WiFi-SantaFeCiudad
(config)# exit
(config)# interface vlan 102
(config)# name Wifi-Evento1
(config)# exit
(config)# interface vlan 103
(config)# name Wifi-Evento2
(config)# exit
(config)# interface vlan 104
(config)# name Wifi-Evento3
(config)# exit
(config)# interface vlan 105
(config)# name Wifi-Evento5
(config)# exit

# configure
(config)# interface ethernet g20
(config)# switchport mode trunk
(config)# switchport trunk allowed vlan add 100
(config)# switchport trunk allowed vlan add 101
(config)# switchport trunk allowed vlan add 102
(config)# switchport trunk allowed vlan add 103
(config)# switchport trunk allowed vlan add 104
(config)# switchport trunk allowed vlan add 105

(config-if)# end

(config)# interface ethernet g21
(config)# switchport mode trunk
(config)# switchport trunk allowed vlan add 100
(config)# switchport trunk allowed vlan add 101
(config)# switchport trunk allowed vlan add 102
(config)# switchport trunk allowed vlan add 103
(config)# switchport trunk allowed vlan add 104
(config)# switchport trunk allowed vlan add 105

# copy running-config startup-config

(config-if)# end
```

Implementación de VPN

A continuación se detallan los comandos más relevantes para la creación de la VPN mencionada, se realizaron simplificaciones para únicamente manifestar acceso al servidor Wireless Controller

- Extremo Municipalidad:

```
config vpn ipsec phase1-interface
```

```
    edit "To_Monitoreo"
        set interface "port4"
        set comments "VPN: To_Monitoreo"
        set proposal 3des-sha1
        set dhgrp 5
        set remote-gw 190.X.X.X
        set psksecret "password"
    next
end
config vpn ipsec phase2-interface
    edit " To_Monitoreo"
        set phase1name "To_Monitoreo"
        set comments "VPN: To_Monitoreo"
        set proposal 3des-sha1
        set dhgrp 5
        set src-subnet 10.20.0.179 255.255.255.255
        set dst-subnet 172.16.11.66 255.255.255.255
    next
end
config router static
    edit 28
        set dst 172.16.11.66 255.255.255.255
        set device " To_Monitoreo "
        set comment "VPN: To_Monitoreo"
    next
end
```

- Extremo Monitoreo

```
config vpn ipsec phase1-interface
      edit "ToMuniWiFi"
        set type ddns
        set interface "wan1"
        set peertype any
        set comments "VPN: ToMuniWiFi"
        set proposal 3des-sha1
        set dhgrp 5
        set remotegw-ddns "monitoreo.santafeciudad.gov.ar"
        set psksecret "password"
    next
config vpn ipsec phase2-interface
    edit "ToMuniWiFi"
        set phase1name "ToMuniWiFi"
        set comments "VPN: ToMuniWiFi"
        set proposal 3des-sha1
        set dhgrp 5
        set src-addr-type name
        set dst-addr-type name
        set src-name "ToMuniWiFi_local"
        set dst-name "ToMuniWiFi_remote"
    next
end
config router static
    edit 17
        set distance 254
        set comment "VPN: ToMuniWiFi Backhole"
        set blackhole enable
        set dstaddr "ToMuniWiFi_remote"
    next
```

```
    edit 19
        set dst 172.16.16.0 255.255.255.0
        set distance 254
        set comment "VPN: ToMuniWiFi"
        set blackhole enable
    next
end
```

Políticas de Firewall que permiten el tráfico

- Extremo Municipalidad

```
config firewall policy
    edit 220
        set srcintf "port3"
        set dstintf "To_Icop"
        set srcaddr "SRV Unifi - LAN 10.20.0.179"
        set dstaddr "SRV Zabbix - ICOP"
        set action accept
        set schedule "always"
        set service "ZABBIX 10051"
        set logtraffic all
        set comment "Monitoreo a traves de Agente Zabbix"
    next
    edit 221
        set srcintf "To_Icop"
        set dstintf "port3"
        set srcaddr "SRV Zabbix - ICOP"
        set dstaddr "SRV Unifi - LAN 10.20.0.179"
        set action accept
        set schedule "always"
        set service "SNMP"
        set logtraffic all
        set comment "Monitoreo a traves de SNMP"
    next
end
```

- Extremo Monitoreo

```
config firewall policy
    edit 65
        set srcintf "ToMuniWiFi"
        set dstintf "internal"
        set srcaddr "SRV Unifi - Muni"
        set dstaddr "SRV Zabbix"
        set action accept
        set schedule "always"
        set service "Zabbix 10051"
        set logtraffic all
        set comment "Monitoreo a traves de Agente Zabbix"
    next
edit 60
        set srcintf "internal"
        set dstintf "ToMuniWiFi"
        set srcaddr "SRV Zabbix"
        set dstaddr "SRV Unifi - Muni"
        set action accept
```

```
        set schedule "always"
        set service "SNMP"
        set logtraffic all
        set comments "Monitoreo a traves de SNMP)"
    next
end
```

A continuación, se muestra un fragmento del log de uno de los equipos Fortinet donde se puede apreciar cada registro de la negociación y el éxito de la misma

VPN Tunnel: ToMuniWiFi | Add Filter | Details

#	Date/Time	Level	Action	Status	Message	VPN Tunnel
1	21:24:22		tunnel-stats		IPsec tunnel statistics	ToMuniWiFi
2	21:20:08		negotiate	success	negotiate IPsec phase 2	ToMuniWiFi
3	21:20:08		negotiate	success	progress IPsec phase 2	ToMuniWiFi
4	21:20:08		negotiate	success	progress IPsec phase 2	ToMuniWiFi
5	21:20:08		install_sa		install IPsec SA	ToMuniWiFi
6	21:19:44		negotiate	success	negotiate IPsec phase 2	ToMuniWiFi
7	21:19:44		negotiate	success	progress IPsec phase 2	ToMuniWiFi
8	21:19:44		negotiate	success	progress IPsec phase 2	ToMuniWiFi
9	21:19:44		phase2-up		IPsec phase 2 status change	ToMuniWiFi
10	21:19:44		install_sa		install IPsec SA	ToMuniWiFi