TRABAJO FIN DE MÁSTER

ANÁLISIS DE IMPLANTACIÓN DE LA TECNOLOGÍA SD-WAN EN CENTROS SANITARIOS DE ATENCIÓN PRIMARIA DEL SESCAM.

AUTORES

Alvaro Espinosa Muñoz

Alejandro Fernández Prendes

Isidro Merayo Castellano

TUTOR

Jose Manuel Morales Pastora

Fecha: 10/11/2021

Master en Dirección de Sistemas y TIC de la Salud y en Digitalización Sanitaria 2020-2021

Resumen

El presente trabajo pretende realizar un análisis que refleje las ventajas e inconvenientes de la tecnología SD-WAN en un entorno sanitario teniendo en cuenta la criticidad que requiere este sector. El modo de trabajo desde sedes remotas, hace imprescindible que las organizaciones evolucionen sus sistemas de comunicaciones buscando rendimiento, control, gestión, automatización, aumento de ancho de banda, disponibilidad, seguridad, visibilidad, monitorización, optimización y eficiencia.

La tecnología SD-WAN resuelve esta demanda de requerimientos o necesidades y da un paso más allá, llegando incluso a tener visibilidad del endpoint.

Para ello se abordará:

- Una descripción de la red actual que da servicio a los Centros de Salud de atención primaria del Servicio de Salud de Castilla-La Mancha, exponiendo ciertas deficiencias actuales.
- Una descripción de la tecnología SD-WAN.
- Un análisis de la integración de esta tecnología en el entorno sanitario, contemplando coste/beneficio así como los inconvenientes que puede presentar.

Referencias al Temario Del Máster

En este trabajo de fin de máster hemos tratado de aplicar los conceptos aprendidos a lo largo del curso, de los siguientes temas:

- Tema 2.1 La planificación TIC. Aspectos generales. La planificación estratégica. Articulación con la planificación operativa. La gobernanza TI.
- Tema 2.3 La planificación operativa. Planes directores. Planes de sistemas. La gestión del cambio. Oficinas técnicas de proyectos. Acuerdos de nivel de servicios. Planes de garantía de calidad.
- Tema 2.5 La seguridad TIC. Legislación aplicable. Aplicación del Reglamento General de Protección de Datos. El papel del Delegado de Protección de Datos. Auditorías. Metodologías / Herramientas de Seguridad MAGERIT. SGSI. PILAR.
- Tema 2.6 Infraestructuras LAN. WAN, WLAN. NAS / SAN. SERVICIOS @-LAN. Seguridad en redes.
- Tema 2.8 Cloud Computing. BIG DATA. Infraestructuras Centralizadas, CPD´s. Servicios de Housing, Hosting. Centros de backup.
- Tema 2.10 La gestión presupuestaria / del gasto. La gestión de RRHH. Los contratos de servicios para entornos de desarrollo, consultoría, sistemas o comunicaciones.

Introducción

El ámbito de aplicación del presente trabajo es la Comunidad de Castilla-La Mancha, en concreto en los centros de salud de atención primaria de su servicio sanitario, a continuación, se describen a grandes rasgos, características a tener en cuenta tanto de la Comunidad como de su Servicio Sanitario y se expondrán los motivos de orientar la aplicación de la tecnología SD-WAN en dichos centros.

Castilla-La Mancha

La comunidad es la tercera autonomía más extensa de España, con una superficie de 79.409 km², que representa el 15,7 % del total peninsular, contando con una población a 1 de enero de 2020 de 2.045.221 habitantes, habiendo experimentado un importante aumento en los últimos años. La esperanza de vida alcanzó de media los 82,88 años, superior a la media nacional.

Según los datos oficiales del INE a 1 de enero de 2020, Castilla-La Mancha consta de 919 municipios, repartidos por las cinco provincias, lo que supone el 11,3 % de todos los municipios de España. De ellos, 525 tienen menos de 500 habitantes, 214 entre 501 y 2000 habitantes, 144 entre 2001 y 10 000 habitantes y solo 36 poblaciones tienen más de 10 000 habitantes. La organización de los núcleos de población es muy dispar, siendo pequeños y numerosos en el norte, y de mayor entidad y menor número en el sur de la Comunidad, consecuencia ésta de la geografía regional y de los distintos modos de repoblación que se emplearon durante la Reconquista.

Los municipios se reparten de forma desigual, siendo la provincia de Guadalajara la que cuenta con un mayor número (288), seguido de la provincia de Cuenca (238), Toledo (204), Ciudad Real (102) y Albacete (87).

En virtud del artículo 29 del Estatuto de Autonomía los municipios y provincias gozan de autonomía para la gestión de sus respectivos intereses. El máximo órgano municipal es el ayuntamiento, que realiza el gobierno en el territorio municipal a través del alcalde y los concejales.

Distribución por tamaño de los municipios

La población se concentra en las grandes ciudades de la Comunidad Autónoma. En los 36 municipios con más de 10 000 habitantes reside el 55,6% de la población, mientras que sólo reside el 7,9% en municipios de menos de 1000 habitantes.

La gran extensión de la Comunidad y la dispersión de la población exigen un mayor esfuerzo inversor por parte del Gobierno regional para abordar la demanda de infraestructuras, dotar de equipamientos y acercar los servicios públicos a los ciudadanos.

Sanidad en Castilla-La Mancha

El Servicio de Salud de Castilla-La Mancha (SESCAM) pone a disposición de los ciudadanos una atención sanitaria de calidad constituida por profesionales altamente cualificados y una extensa red asistencial integrada por 18 hospitales, 11 centros de especialidades, diagnóstico y tratamiento, 204 centros de salud y 1.116 consultorios locales, donde se desarrollan actividades relacionadas con la atención sanitaria, investigación, curación y rehabilitación, así como la prevención de la enfermedad y promoción de la salud, teniendo como prioridad la salud y el bienestar del paciente contemplando una extensa cartera de servicios.

Las funciones del Servicio Sanitario, así como su creación, naturaleza y objetivos se contemplan en algunos de los artículos de la ***Ley 8/2000, de 30 de noviembre, de Ordenación Sanitaria de Castilla-La Mancha,*** en concreto:

Artículo 67. Creación y objeto.

Se crea el Servicio de Salud de Castilla-La Mancha con el fin de proveer los servicios y gestionar los centros y establecimientos destinados a la atención sanitaria que le sean asignados, así como desarrollar los programas de salud que se le encomienden con el objetivo final de proteger y mejorar el nivel de salud de la población.

Artículo 68. Naturaleza jurídica.

1. El Servicio de Salud de Castilla-La Mancha es un organismo autónomo dotado de personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines.

2. El Servicio de Salud de Castilla-La Mancha queda adscrito a la Consejería competente en materia de sanidad.

3. El Servicio de Salud de Castilla-La Mancha podrá gestionar los siguientes centros, servicios y establecimientos sanitarios:

a) Los de asistencia sanitaria a la población propios de la Administración Regional.

b) Los de asistencia sanitaria a la población de la Seguridad Social, cuya gestión sea transferida a la Comunidad Autónoma.

c) Los centros dependientes en la actualidad de las Corporaciones Locales en virtud de los acuerdos que se establezcan.

d) Todos los que se integren en el futuro, no contemplados en los apartados anteriores.

Las funciones del Servicio de Salud de Castilla-La Mancha se recogen en el ***Artículo 69,*** algunas de ellas son:

1. La ejecución y gestión de las prestaciones sanitarias, que le sean asignadas, mediante las actuaciones de Promoción de la Salud, Prevención de la Enfermedad, Asistencia Sanitaria y Rehabilitación.

2. La adecuada gestión, conservación y mantenimiento de los centros, servicios y establecimientos sanitarios que le sean asignados, teniendo en cuenta las características socioeconómicas, geográficas, sanitarias y poblacionales de Castilla-La Mancha.

3. La óptima distribución de los medios económicos afectos a la financiación de los servicios y prestaciones sanitarias asistenciales que le asigne el Sistema Sanitario de Castilla-La Mancha.

Artículo 74. De las Gerencias.

1. Las Gerencias son los órganos periféricos territoriales del Servicio de Salud de Castilla-La Mancha a quienes corresponde optimizar la gestión de los servicios y dirigir los recursos y centros que se le asignen, bajo la dependencia de la Dirección-Gerencia del Servicio de Salud de Castilla-La Mancha.

2. Las Gerencias actuarán bajo los principios de autonomía y desconcentración de la gestión.

3. Cada Gerencia convendrá con la Dirección-Gerencia el contrato de gestión de los servicios, centros y establecimientos a su cargo, el cual fijará los objetivos sanitarios, la dotación de recursos necesarios, el plazo para su cumplimiento y su evaluación.

4. Las personas al cargo de las Gerencias serán designadas y cesadas por quien esté al frente de la Dirección-Gerencia del Servicio, de quien dependerán jerárquicamente.

5. Reglamentariamente se establecerá la estructura, organización y funcionamiento de las Gerencias, y se garantizará la participación de sus profesionales y de su personal.

El SESCAM representa uno de los mayores Servicios Regionales de Salud del país, con una amplia red de centros de asistencia primaria y especializada y con un total de 25.000 profesionales aproximadamente.

Centros de Salud de Atención Primaria del SESCAM

El centro de salud y el consultorio local constituyen el primer nivel asistencial sanitario disponible a la población para acceder a la atención sanitaria. Un equipo multidisciplinar de profesionales del Equipo de Atención Primaria (médico de familia, pediatra, enfermero, matrona, fisioterapeuta, odontólogo, trabajador social y auxiliares administrativos) ofrecen una atención integral en el centro de salud o consultorio local de cada Zona Básica de Salud.

En la actualidad, el Sistema Sanitario de Castilla-La Mancha queda configurado territorialmente por las demarcaciones geográficas denominadas Áreas de Salud y cada una de ellas está integrada por diversas Zonas Básicas de Salud.

El Equipo de Atención Primaria desarrolla funciones de promoción de la salud, prevención de la enfermedad, asistencia, rehabilitación, investigación y docencia, en coordinación con Atención Especializada.

En caso de precisar atención sanitaria urgente, en horario diferente al de su centro de salud, existe un Punto de Atención Continuada (PAC) ubicado en unas instalaciones sanitarias integradas en el centro sanitario.

La Ley 8/2000, de 30 de noviembre, de Ordenación Sanitaria de Castilla-La Mancha, contempla la configuración de los centros sanitarios de atención primaria:

Artículo 44. Áreas de Salud.

1. El Sistema Sanitario de Castilla-La Mancha queda configurado territorialmente por las demarcaciones geográficas denominadas Áreas de Salud.

2. El Consejo de Gobierno de Castilla-La Mancha, a propuesta del titular de la Consejería competente en materia de sanidad, aprobará la delimitación territorial de las Áreas de Salud teniendo en cuenta

los factores geográficos, socioeconómicos, demográficos, laborales, epidemiológicos, culturales, climatológicos, las vías y medios de comunicación, así como las instalaciones sanitarias existentes.

3. El Área de Salud constituye el marco fundamental para el desarrollo de los programas de promoción de la salud y prevención de la enfermedad y en tal condición asegurará la organización y ejecución de las distintas disposiciones y medidas que adopta la Administración Sanitaria de la Comunidad Autónoma.

4. Cada Área de Salud estará integrada por Zonas Básicas de Salud.

Con independencia de lo anterior, en el ámbito de cada Área de Salud se podrá establecer la ordenación territorial que resulte necesaria en función de cada circunstancia geográfica y, en su caso, para cada tipología de prestaciones y servicios sanitarios.

Artículo 49. De la Atención Primaria.

1. La Atención Primaria constituye el nivel de acceso ordinario de la población al Sistema Sanitario y se caracteriza por prestar atención integral a la salud mediante el trabajo del colectivo de profesionales del Equipo de Atención Primaria que desarrollan su actividad en la Zona Básica de Salud correspondiente.

2. Las Zonas Básicas de Salud constituyen la demarcación geográfica y poblacional que sirve de marco territorial a la Atención Primaria de Salud.

3. No obstante lo establecido anteriormente, cuando las especiales condiciones socio-económicas demográficas y de comunicaciones dificulten la creación de Zonas Básicas de Salud, podrán constituirse Zonas Especiales de Salud.

4. Los Centros de Salud y los Consultorios Locales constituyen las estructuras físicas de las Zonas Básicas de Salud, donde presta servicio el conjunto de profesionales que integran los Equipos de Atención Primaria.

5. La delimitación de las Zonas Básicas de Salud se regulará mediante Orden de la Consejería competente en materia de sanidad.

En relación a la atención especializada la misma Ley contempla coordinación entre primaria y especializada:

Artículo 50. De la Atención Especializada.

1. La Atención Especializada, en tanto que atención que se realiza una vez superadas las posibilidades de diagnóstico y tratamiento de la Atención Primaria, se prestará en los hospitales, así como en otros Centros Especializados de Diagnóstico y Tratamiento, constituyendo el segundo nivel de asistencia.

2. El hospital es la estructura sanitaria responsable de la Atención Especializada, programada y urgente, tanto en régimen de internamiento, como ambulatorio y domiciliario de la población de su ámbito territorial. Desarrolla además las funciones de promoción de salud, prevención de la enfermedad, asistencia, rehabilitación, investigación y docencia, en coordinación con la Atención Primaria, de acuerdo con las directrices establecidas por los órganos superiores del Sistema Sanitario de Castilla-La Mancha.

3. Los centros hospitalarios y los Centros Especializados de Diagnóstico y Tratamiento integrados en el Sistema Sanitario constituirán la red hospitalaria pública integrada de Castilla-La Mancha.

6. Cada Área de Salud dispondrá, al menos, de un centro hospitalario, que ofertará los servicios adecuados a las necesidades de la población.

7. Se garantizará la interrelación entre los diferentes niveles asistenciales.

8. Reglamentariamente se establecerán las normas de estructura, organización y funcionamiento de los centros y servicios de atención especializada y se garantizará la participación del colectivo de los profesionales en la gestión de los mismos.

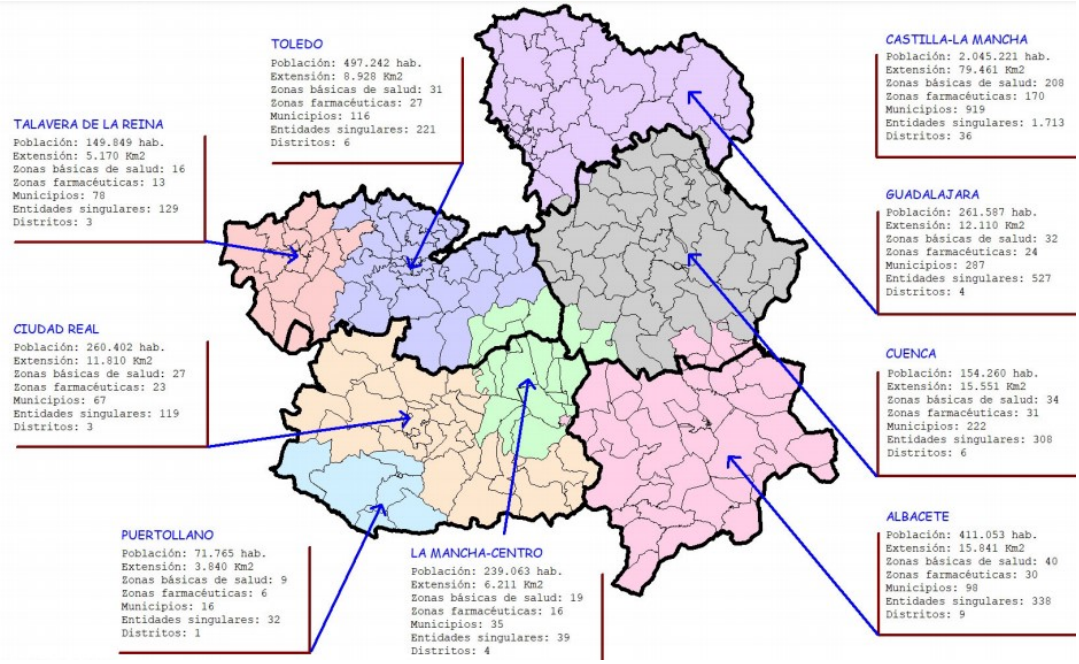
El Mapa Sanitario de Castilla-La Mancha se regula por el Decreto 13/1994, de Ordenación Territorial de la Sanidad en Castilla-La Mancha y mediante la Orden de 201/2018 de 27 de diciembre, por la que se determina el Mapa Sanitario de Castilla-La Mancha.

La Ordenación territorial de la Sanidad en Castilla-La Mancha se estructura en:

- Áreas de Salud: Albacete, La Mancha-Centro, Ciudad Real, Cuenca, Guadalajara, Talavera de la Reina, Toledo y Puertollano.
- Distritos de Salud: prestan servicios de apoyo en Salud Pública a las Zonas Básicas de Salud.
- Zonas Básicas de Salud (ZBS): unidades territoriales básicas de la atención primaria de la salud, en ellas desarrollan su actividad los Equipos de Atención Primaria dentro del centro de salud y los consultorios locales.

El Visor del Mapa Sanitario de Castilla-La Mancha es un proyecto desarrollado por la Consejería de Sanidad y la Consejería de Fomento, en el que se muestra, de forma rápida y sencilla, la información geográfica de las distintas áreas que conforman la ordenación territorial y funcional de la atención a la salud en la región, así como la ubicación espacial de los distintos recursos (Hospitales, CEDT, Centros de Salud, PAP, Consultorios, Farmacias y Botiquines).

En el visor no aparecen las ZBS no funcionantes; es decir, aquéllas creadas mediante Orden de la Consejería de Sanidad pero que no disponen, hasta el momento, de centro de salud, por lo que todavía no son operativas. No obstante, si se desea obtener información al respecto, aparecen recogidas en las descargas del Mapa Sanitario, en formato pdf, de las distintas Áreas de Salud y Gerencias Sanitarias.



Mapa de áreas de Salud de Castilla-La Mancha.

DISTRITO	ZBS_F	ZBS_NF	TOTAL	MUNICIPIOS	EXT	POP	CS	PAP	CONSULTORIOS	FARMACIAS	BOTIQUINES
ALBACETE	11	0	11	9	2.726	186.527	10	0	22	98	3
ALCARAZ	3	0	3	14	1525	7.511	3	0	18	15	1
ALCAZAR	6	0	6	8	1.380	64.460	6	0	4	35	0
ALMANSA	3	0	3	7	1.454	41.293	3	1	4	24	0
BELMONTE	5	0	5	36	2.501	21.613	5	0	32	27	8
BELVIS DE LA JARA	5	0	5	26	2.335	16.820	5	0	38	25	4
BRIHUEGA	7	0	7	89	4.115	31.139	7	2	120	36	27
CAÑETE	5	0	5	38	2.663	7.817	5	0	42	11	15
CASAS-IBAÑEZ	4	0	4	25	1.877	28.917	4	0	33	26	6
CIUDAD REAL	9	0	9	21	4.704	98.330	9	0	27	61	4
CONSUEGRA	4	0	4	16	2.341	49.429	4	0	13	33	1
CUENCA	6	0	6	27	2.375	63.943	5	0	47	39	15
DAIMIEL	10	0	10	24	3.339	96.257	10	0	23	58	3
ELCHE DE LA SIERRA	4	0	4	7	1.873	11.424	4	1	35	9	0
GUADALAJARA	11	2	13	47	1.365	210.720	11	1	51	88	15
HELLIN	4	0	4	6	1.478	44.137	4	0	17	28	1
ILLESCAS	7	0	7	31	1.116	172.346	7	0	27	51	1
MENASALBAS	3	0	3	14	1.295	22.712	3	0	12	17	1
MOLINA DE ARAGON	4	0	4	57	2.967	7.180	4	0	85	9	7
MOTILLA DEL PALANCAR	7	0	7	42	3.139	22.767	7	0	37	28	10
OCAÑA	6	0	6	19	2.311	55.813	6	0	13	29	0
PEDROÑERAS,LAS	2	0	2	7	800	20.053	2	0	5	12	0
PRIEGO	4	0	4	40	2.010	5.420	4	0	47	10	18
PUERTOLLANO	9	0	9	16	3.825	71.765	9	1	22	52	7
QUINTANAR DE LA ORDEN	4	0	4	11	1.504	56.976	4	0	7	31	0
QUINTANAR DEL REY	3	0	3	8	686	20.669	3	1	7	13	1
RODA,LA	3	0	3	16	2.221	36.100	3	0	19	24	3
SANTA OLALLA	4	0	4	25	990	22.418	4	0	22	26	1
SIGÜENZA	7	1	8	94	3.701	12.548	7	1	158	14	7
TALAVERA	7	0	7	27	1.834	110.611	8	0	31	77	2
TARANCON	7	0	7	39	2.780	32.700	7	0	52	31	21
TOLEDO	6	1	7	11	574	134.807	6	0	10	58	0
TOMELLOSO-MANZANARES	7	0	7	9	2.557	97.574	7	0	5	56	0
TORRIJOS	4	0	4	25	1.285	62.135	4	0	22	38	1
VALDEPEÑAS	8	0	8	22	3.721	65.815	8	4	15	46	3
VILLARROBLEDO	4	1	5	6	2.015	34.475	4	0	2	21	0
TOTAL	203	5	208	919	79.461	2.045.221	203	12	1.124	1.256	186

ZBS_F: Zonas Básicas de Salud con centro de salud (CS) en funcionamiento.
ZBS_NF: Zonas Básicas de Salud creadas mediante Orden de la Consejería de Sanidad pero que no dispone, hasta el momento, de centro de salud.
Datos I.N.E. 2.020

Distritos de Salud de Castilla-La Mancha

GERENCIA	DISTRITOS	ZBS_F	ZBS_NF	TOTAL	MUNICIPIOS	EXTENSION	POBLACION	CS	PAP	CONSULTORIOS	FARMACIAS	BOTIQUINES
ALBACETE	5	23	0	23	69	8.701	277.940	23	1	96	173	14
ALCAZAR DE SAN JUAN	2	10	0	10	22	3.264	122.816	10	0	14	68	0
ALMANSA	1	3	0	3	7	1.462	41.293	3	1	4	24	0
CIUDAD REAL	2	19	0	19	45	8.050	194.587	19	0	50	119	8
CUENCA	6	32	0	32	210	14.399	139.191	32	0	246	132	86
GUADALAJARA	4	29	3	32	287	12.109	261.587	29	4	414	147	56
HELLIN	2	9	0	9	16	3.668	57.345	9	1	56	40	1
MANZANARES **	1	3	0	3	6	1.379	41.784	3	0	4	25	0
PUERTOLLANO	1	9	0	9	16	3.835	71.765	9	1	22	52	6
TALAVERA	3	16	0	16	78	5.167	149.849	16	0	92	128	7
TOLEDO *	6	30	1	31	116	8.924	497.242	30	0	97	226	4
TOMELLOSO **	1	5	0	5	4	1.165	63.075	5	0	1	35	0
VALDEPEÑAS	1	8	0	8	22	3.767	65.815	8	4	15	46	3
VILLARROBLEDO	2	7	1	8	21	3.571	60.932	7	0	14	41	1
CASTILLA-LA MANCHA	36	203	5	208	919	79.461	2.045.221	203	12	1.125	1.256	186

* Las Gerencias de Atención Primaria y de Atención Especializada de Toledo no están integradas.

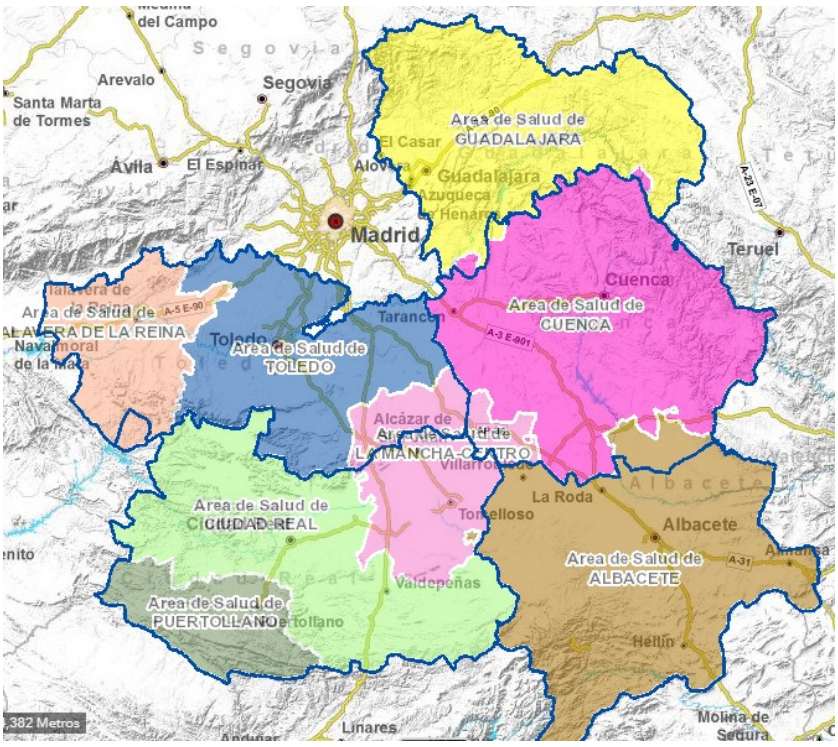
** El Distrito de Salud de Manzanares-Tomelloso comprende ZBS de las dos Gerencias.

ZBS_F: Zonas Básicas de Salud con centro de salud (CS) en funcionamiento.

ZBS_NF: Zonas Básicas de Salud creadas mediante Orden de la Consejería de Sanidad pero que no dispone, hasta el momento, de centro de salud.

Datos I.N.E. 2.020

Gerencias de Castilla-La Mancha



Mapa Sanitario de Castilla-La Mancha

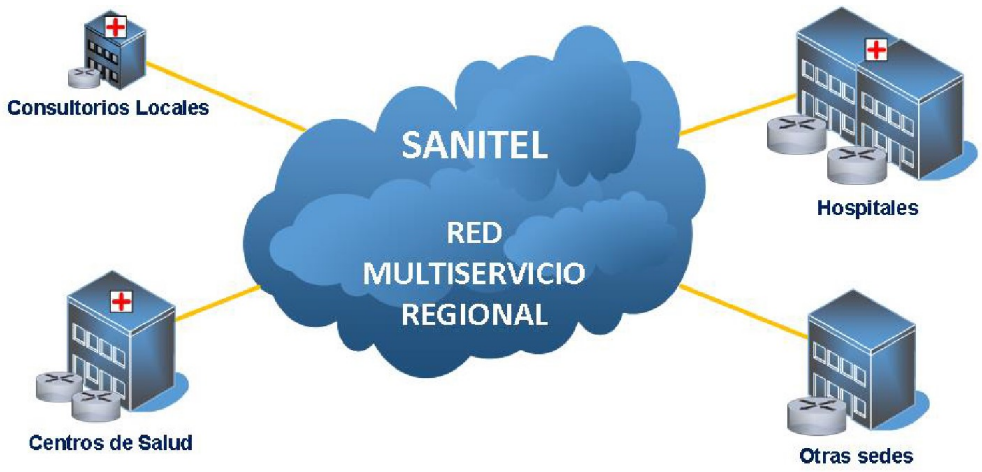
Áreas de Salud del Servicio Sanitario de Castilla-La Mancha:

- Área de Salud de Guadalajara.
- Área de Salud de Cuenca.
- Área de Salud de Albacete.
- Área de Salud de Ciudad Real.
- Área de Salud Puertollano.
- Área de Salud de Talavera de La Reina.
- Área de Salud de Toledo.

Redes de comunicaciones en el SESCAM

Conectividad provincial

Se dispone de conectividad "full-mesh", por provincia, para todas las dependencias administrativas autonómicas, conectadas a la red multiservicio del proveedor de servicios.



Arquitectura conectividad provincial

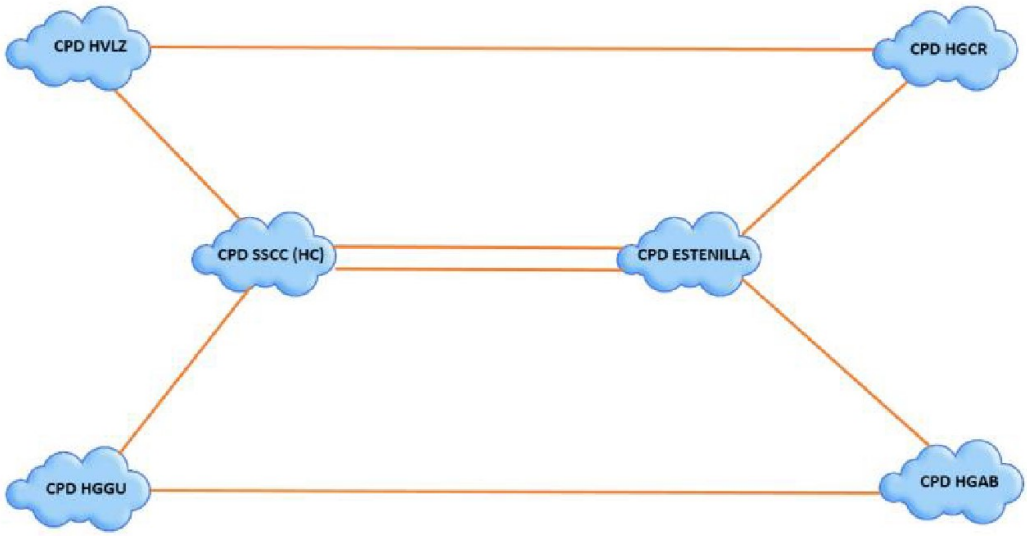
Esta red se estructura en dos niveles: En cada una de las 5 provincias regionales existe una red metropolitana (MAN), y éstas, a su vez, se conectan mediante una red de carácter nacional.

Arquitectura red MPLS

Comunicación inter-CPDs

Por otro lado, actualmente hay desplegada una red DWDM (multiplexado denso por división en longitudes de onda), que interconecta los CPDs Regionales del SESCAM a través de canales de fibra óptica con un ancho de banda de 10 Gbps.

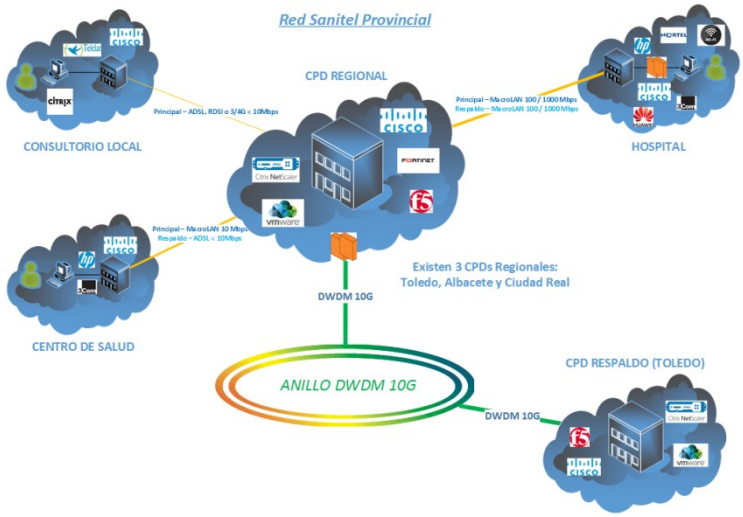
Esta red tiene una arquitectura que proporciona caminos redundantes en cada uno de los nodos, doble trazado diversificado sin puntos únicos de fallo:



Arquitectura inter CPDs

Tipos de sedes en SESCAM

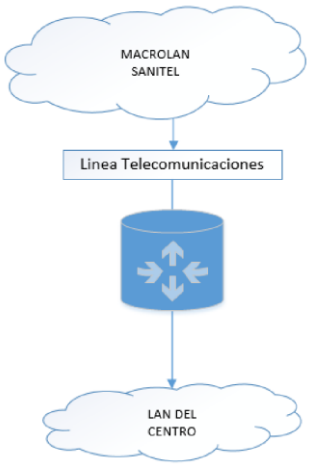
En el siguiente esquema se muestran los tipos de sedes y la interconexión entre ellas de forma resumida:



Arquitectura interconexión tipos de sede

Consultorio local

Los consultorios locales corresponden a pequeños centros sanitarios de atención primaria localizados en pequeñas localidades donde no prestan actividad de atención ininterrumpida y disponen de un número bajo de tarjetas sanitarias. La arquitectura por defecto de los consultorios locales es la siguiente:

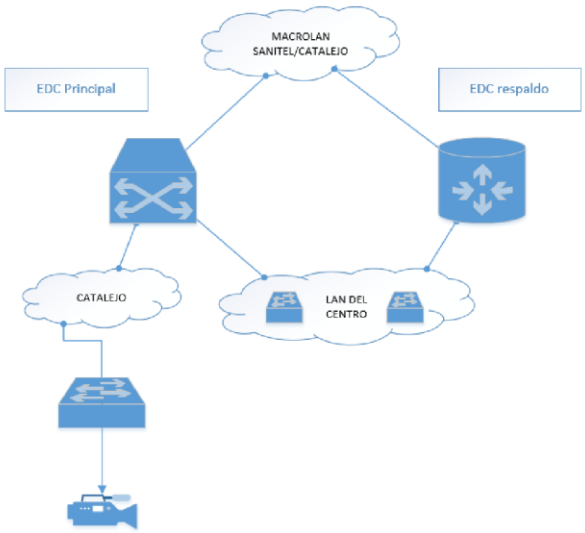


Arquitectura conexión consultorio local

En la mayoría de los casos disponen de un único enlace principal con un ancho de banda no garantizado de hasta 10 Mbps asimétricos dependiente de la tecnología desplegada en cada uno de ellos.

Centros de salud

Los centros de salud (en adelante CS) son sedes que disponen de atención primaria 24x7 en la mayoría de los casos. Disponen de la siguiente arquitectura en su mayoría:



Arquitectura conexión centro de salud

Los CS cuentan todos con doble enlace a la MacroLan (SANITEL) para dotar de redundancia a cada centro. Disponen de una VLAN de datos y una de telefonía IP.

En su mayoría, cuentan con un enlace MacroLAN (fibra óptica) de 10 Mbps como enlace principal y una línea ADSL de respaldo de hasta 10 Mbps.

En ausencia de MacroLAN se instala una línea ADSL VPN-IP con acceso a la red privada del SESCAM a través de la red MacroLAN de Telefónica mediante ADSL/VDSL.

La LAN se encuentra directamente conectada al EDC, y éste es el que gestiona el routing de dicho centro.

Centros de Especialidades de Diagnóstico y Tratamiento (CEDT)

Son centros que se comprometen a garantizar una asistencia cercana a los ciudadanos, ofreciendo servicios sanitarios a varias poblaciones, disponen de consultas de atención primaria y algunas especialidades, el horario asistencial de estos centros es 24x7.

Disponen de un enlace principal MacroLan 100 Mbps VPN-IP y un respaldo de 10 Mbps.

Hospital

Los hospitales disponen de una amplia cartera de servicios asistenciales con atención 24x7, en general presentan consultas de atención primaria, gabinetes de pruebas especiales, urgencias, extenso número de especialidades, camas de hospitalización, quirófanos, UCI,etc.

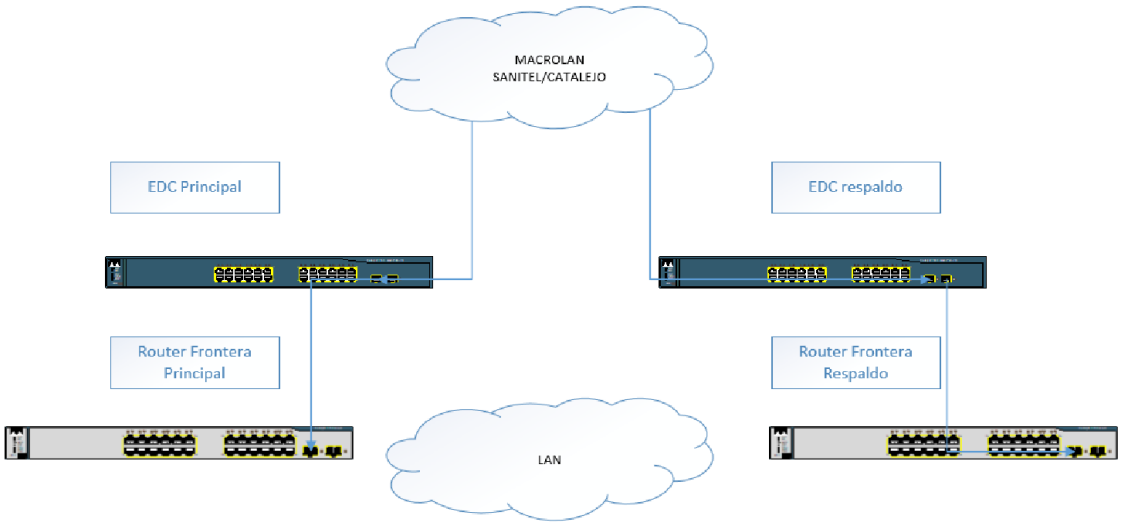
En este sentido, la mayoría de ellos, disponen de líneas principales a la red MacroLan de 100 Mbps y de 1Gbps en los hospitales con mayor actividad asistencial.

Gerencia de Atención Primaria

Las Gerencias de Atención Primaria (en adelante GAP) cuentan con la misma estructura que un hospital/CEDT, estas incluso se hallan junto a centros de salud y dan servicio a éstos diferenciándose por VLANs de servicio.

Actualmente son 15 GAPs cuyas líneas principales presentan acceso MacroLan VPN-IP y van de 10Mbps a 100Mbps dependiendo de las necesidades que presentan cada una de ellas.

El esquema de los CEDTs, GAPs y Hospitales es común:

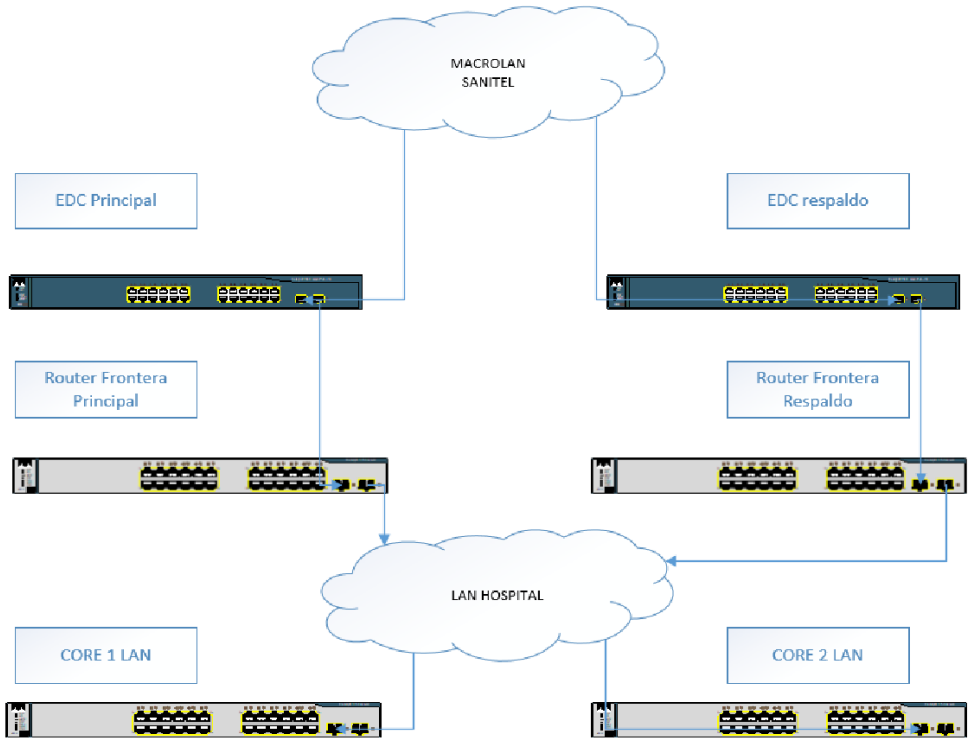


Arquitectura conexión GAP

Los hosts finales se conectan a los routers frontera (switches de capa 3) y en el caso de compartir ubicación con un centro de salud, cuelga un switch de LAN perteneciente a éstos.

Cores

Ubicados en los hospitales y CEDTs del SESCAM, la arquitectura de red establecida presenta una jerarquía que proporciona estabilidad y fiabilidad en cada sede. Estos equipos se encargan del routing y switching. El esquema es el siguiente:



Arquitectura conexión hospital

Cada sede cuenta con 2 EDC's (Equipo de cliente), los cuales dan acceso a la red SANITEL que interconecta todo el SESCAM. Cada EDC consta de doble sesión BGP contra dos PE's (Proveedor Externo) del proveedor de servicio, dotando así de doble redundancia a cada sede. Por un lado, redundancia a nivel lógico para cada equipo, y por otro, redundancia a nivel de equipo físico para la sede.

El siguiente nivel lo componen los routers fronteras (RF), los cuales están igualmente redundados teniendo un equipo principal y uno de respaldo y sirven de enlace entre la WAN y la LAN de la sede.

Esta capa es responsable del transporte de grandes cantidades de tráfico de forma fiable y rápida.

Por último, se disponen de dos equipos que hacen la función de Core/Distribución de LAN y son a los que se conectan toda la electrónica de red repartida en los armarios de acceso de cada sede.

Algunas sedes cuentan con una capa de seguridad adicional, que hacen las funciones de firewall y se sitúa a nivel lógico entre la capa de CORE y los RF.

CPDs Corporativos

Tras un proceso de consolidación de equipamiento y servicios, desde los Hospitales a los CPDs regionales, estos se han convertido en los puntos neurálgicos de la actividad de computación para las aplicaciones implantadas en ellos.

Se ha intentado homogeneizar la arquitectura de los CPDs, para facilitar la gestión, resolución de incidencias y despliegue de nuevos servicios o equipamiento.

El diseño se ha centrado en disponer de una arquitectura de tres CPDs regionales, más un cuarto de respaldo:

- Albacete (Hospital General Universitario de Albacete).
- Ciudad Real (Hospital. General Universitario de Ciudad Real).
- Toledo (Servicios Centrales Huérfanos Cristinos).
- Toledo Respaldo (Consejería de Fomento, Estenilla).

Estos albergan equipamiento de computación que soporta la plataforma de virtualización, equipamiento de balanceo de aplicaciones, cabinas de almacenamiento, servidores de bases de datos y la electrónica de red que interconecta toda esta infraestructura, que, además, da conectividad con el anillo DWDM para la comunicación inter-CPDs, y con las distintas sedes que acceden a los servicios aquí alojados.

Internet

Actualmente se cuenta con un acceso a Internet a través de un único ISP (Proveedor de Servicios de Internet) a través de dos routers en alta disponibilidad en modo activo/pasivo situados en los CPDS de Toledo de modo Activo/Pasivo. El ancho de banda contratado es de 2 Gb. Cada router cuenta con al menos 2 puertos de 10Gb.

El ancho de banda es gestionado por dos gestores de ancho de banda hardware en alta disponibilidad situados cada uno en un CPD y con al menos 4 puertos de 10Gb. Todo el tráfico corporativo a internet se cursó a través de estos accesos.

Por otro lado, el SESCAM dispone de un servicio Proxy para el filtrado del acceso a internet. En concreto:

3 X Appliances físicos distribuidos entre los CPDS de Servicios Centrales y Estenilla.

Es necesario proteger los servicios de la organización permitiendo el control y filtrado del tráfico destinado a los servicios (servidores, aplicaciones, etc.) alojados en el Data Center, asegurando que solo les llegue aquel tráfico que tiene permiso para acceder según la política de seguridad establecida.

Se dispone de una doble barrera de seguridad que se encarga de proteger, hasta la capa 7 o de aplicación, la organización de forma perimetral en el acceso a internet.

Sedes susceptibles de estudio de la tecnología SD-WAN

Las sedes susceptibles de estudio a la posible evolución de red a SD-WAN serían los Centros de Salud por diversos motivos:

- Escaso ancho de banda en la sede.
- Demanda de nuevos servicios.
- Nula posibilidad de gestión del tráfico de las aplicaciones.
- Nulo aprovechamiento de todas las líneas disponibles.
- Nulo nivel de securización en este tipo de sedes.
- Nula visibilidad del tráfico cursado.
- Escasa posibilidad de crecimiento en servicios y personal.

El SESCAM cuenta con 204 centros de salud, el listado de centros se detalla en el ANEXO 1.

Cada vez son más los servicios que se demandan y desarrollan en los Centros de Salud de atención primaria, como pueden ser la incorporación de envío de imágenes digitales y los servicios de teleconsulta sobre todo.

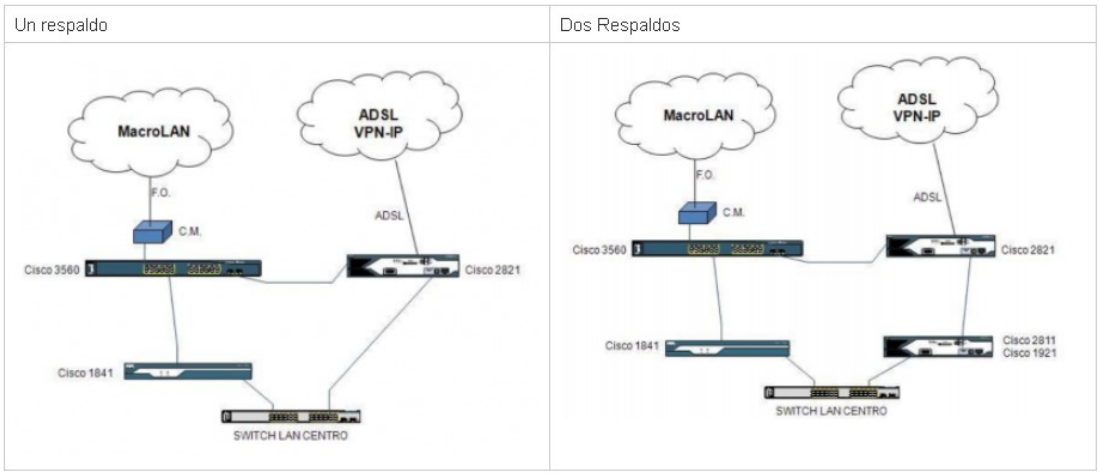
El aumento de servicios asistenciales, en la mayoría de los casos, requiere de un aumento de consumo de recursos que a priori no se suelen tener en cuenta, algunos de ellos son: aumento de capacidad de las líneas de comunicación, necesidad de puertos de electrónica de red, puestos de trabajo, teléfonos, aumento en la capacidad de almacenamiento, etc.

Para poder dar respuesta a la incorporación de nuevos servicios es necesario que las líneas de comunicaciones de los centros estén preparadas para asumir las necesidades.

Uno de los servicios que se está demandando y que ha tomado un crecimiento de forma notable desde la aparición del Covid-19 es la videoconsulta en los Centros de Salud, este servicio permite que los pacientes no tengan que desplazarse para ser atendidos y esta atención sea más completa que una simple llamada de teléfono en relación a las teleconsultas.

Se estima, que el sistema de videoconferencia para poder implantar teleconsulta en los Centros de Salud, a través de una plataforma de videoconferencia ubicada en la nube, consuma alrededor de unos 4 Mbps de ancho de banda para cada sesión de video entre Paciente-Facultativo. Esta estimación pone en riesgo el servicio de los centros claramente, debido a que los Centros de Salud cuentan con una línea principal de 10 Mbps simétricos y un respaldo de ADSL de hasta 10 Mbps de forma asimétrica.

En algunos escenarios, fundamentalmente en Centros de Salud y algunos Consultorios locales de grandes dimensiones, se dispone de un router de acceso por fibra óptica y un router ADSL de respaldo. (F.O.= Fibra Óptica; C.M= Conversor de medios).



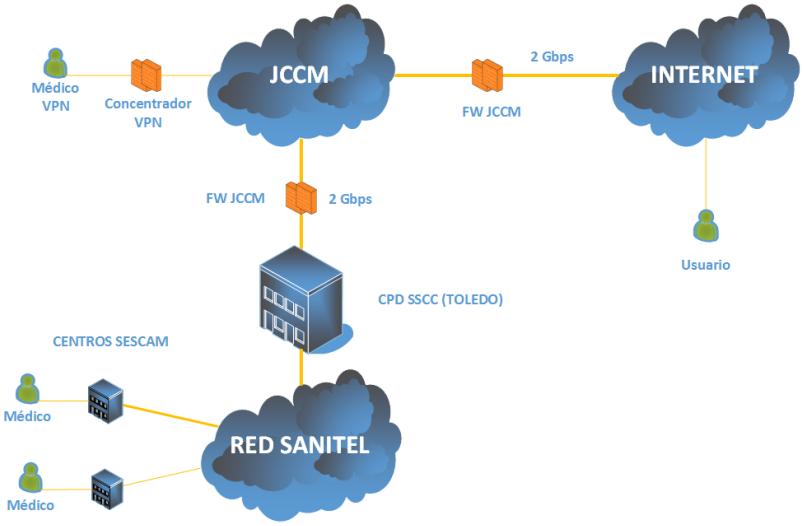
Arquitectura conexión tipos de respaldo

Tipo de centro	Enlace Principal	Ancho de banda	Enlace de respaldo	Ancho de banca
Centro de Salud (CS)	MacroLAN	10 Mbps (simétricos)	ADSL	<= 10 Mbps (asimétricos)

Infraestructura Centro de Salud

El consumo medio habitual en este tipo de centros, en cuanto a tráfico de red, varía dependiendo del volumen de cada uno de ellos, sobre todo por las tarjetas sanitarias que gestionan, pero se puede extraer que presenta un media del 30% del total del ancho de banda que dispone el Centro (3 Mbps), con unos picos del 60% (6 Mbps).

En el siguiente esquema se puede observar el circuito por donde se cursaría el tráfico en las videoconsultas:



Arquitectura conexión videoconsultas

Ante este escenario, sería recomendable no realizar más de 1 sesión simultánea para no comprometer el servicio del centro, dado que la videoconsulta consumiría el 40% del ancho de banda total del mismo y por otro lado no se deberían realizar sesiones cuando esté el centro usando la línea de respaldo, por indisponibilidad de la línea principal.

Esta situación deja poco margen de crecimiento ante nuevas demandas de servicios, por ello es imprescindible que se realice una adecuación de caudales en los Centros de Salud de forma eficaz y eficiente.

Control del consumo de ancho de banda que controlen el tráfico de las aplicaciones y servicios del SESCAM.

Costes actuales de los enlaces:

El SESCAM contrata los servicios de interconexión de red a través de un concurso público, que contempla un pliego de prescripciones técnicas donde los diferentes operadores de comunicaciones presentan sus ofertas en base a él.

Una de las soluciones, sería aumentar el caudal de las líneas para poder afrontar la implantación de nuevos servicios, en este caso, la solución de aumento de caudal por cada una de las sedes, sería pasar de una tipología:

MacroLAN VPN-IP 10Mbps / ADSL VPN-IP hasta 10Mbps.

A tener:

MacroLAN VPN-IP 100Mbps / ADSL VPN-IP hasta 10Mbps.

El incremento de coste sería:

	Costes actuales			
	Coste sede	**Número de sedes**	**Coste mensual**	**Coste anual**
Sede (10Mbps/ADSL VPN-IP hasta 10Mbps TFO)	€490,78	204	€100.119,12	€1.201.429,44

	Costes con aumento de caudal			
	Coste sede	**Número de sedes**	**Coste mensual**	**Coste anual**
Sede(100Mbps/ADSL VPN-IP hasta 10Mbps TFO)	€697,25	204	€142.239	€1.706.868

Incremento de coste anual al aumentar el ancho de banda	***€505.438,56***

Costes e incremento caudal

El coste actual de las líneas es ya muy considerable, si se pretendiera aumentar los caudales, el coste, como puede verse en la tabla anterior, se vería aún más afectado, por tanto, es necesario buscar alguna solución que evite este sobrecoste para poder ofrecer los servicios que se demandan.

Justificación

Problemas actuales:

- El elevado coste económico anual que suponen los enlaces alquilados contemplando un escaso ancho de banda, este elevado coste se incrementaría aún más al aumentar los caudales usando la misma tecnología.
- Escasa posibilidad de crecimiento en los Centros de Salud, el aumento de nuevos servicios en los centros requiere adecuar el ancho de banda que requieren los mismos de manera eficiente.
- Falta de monitorización del tipo de tráfico cursado en la sede remota.
- Inexistencia de una gestión dinámica del ancho de banda para priorizar un cierto tipo de tráfico.
- Necesidad de personal para abordar procesos de monitorización, mantenimiento, gestión de tráfico, visibilidad, inexistencia de posibilidad de realizar las tareas de forma automatizada.

Se pretende buscar:

- Mejorar la escalabilidad.
- Mejorar en la calidad de servicio.
- Gestión dinámica del tráfico de red.
- Aumentar ancho de banda a coste reducido.
- Aumentar líneas redundantes de forma ágil y económica.
- Aprovechar de forma eficiente todas las líneas disponibles en cada sede.
- Dotar de seguridad en el tráfico cursado en los centros.

Actualmente el consumo medio de dichas líneas es el siguiente:

- Visibilidad de la información.
- Seguridad.
- Capacidad de Gestión autónoma.

SD-WAN aporta un plus de ventajas respecto a los sistemas de interconexión más tradicionales.

Dichos sistemas como MPLS son una opción implantada hoy en día debido a su madurez a la confiabilidad y redundancia que aporta, sin embargo, esta solución presenta unos elevados costes

recurrentes y no aporta una redundancia por sí sólo sino con la contratación de nuevas líneas, aumentando aún más los costes.

SD-WAN intenta solventar a estas desventajas, ofreciendo una mayor escalabilidad, menor coste recurrente, una mejor calidad de servicio:

- Reducción de gastos, por permitir implementar líneas de bajo coste.
- Mejorar el rendimiento, al permitir enrutar el tráfico de manera eficaz en función de las necesidades funcionales en cuestión.
- Ofrece redundancia y aumenta la capacidad de ancho de banda al poder usar múltiples enlaces en cada sede.

Objetivos

Los objetivos del presente trabajo son:

- Realizar una descripción de la red actual que da servicio a los Centros de Salud de atención primaria del Servicio de Salud de Castilla-La Mancha, exponiendo ciertas deficiencias actuales.
- Describir a grandes rasgos la tecnología SD-WAN como posible solución a las deficiencias descritas.
- Realizar un análisis de la integración de esta tecnología en el entorno sanitario, contemplando coste/beneficio así como los inconvenientes que puede presentar.

Enfoque y metodología

Se hará una descripción de la red corporativa del SESCAM, contemplando tipos de sedes, CPDs, infraestructura, tipos de redes y algunos servicios, centrando la descripción en las sedes de centros de Salud que es donde se hará foco específico.

Una vez descrito, se expondrán los inconvenientes y problemas de manera específica tanto a nivel técnico como económico.

Para extraer dicha información se mantendrán una serie de reuniones con personal técnico de la unidad de Telecomunicaciones del SESCAM dentro del Área Técnica de la Información, así como acceso a la documentación dentro de la unidad.

Igualmente se realizará una descripción de la tecnología SD-WAN y por último una aplicación a las sedes remotas del SESCAM para exponer las ventajas y desventajas que puede tener esta tecnología en todos los sentidos.

Tecnología SD-WAN

Las redes definidas por software de área extensa (SD-WAN) nacen del movimiento de los fabricantes con el movimiento de nuevas tecnologías en el campo de las redes, que bautizaron con SDN (Redes Definidas por Software). Básicamente lo que nos lleva a este movimiento es a la "virtualización" de los elementos de red, su arquitectura y sobre todo la gestión centralizada.

La gestión de una WAN siempre ha generado un coste de gestión, además de no ser no ser muy flexible ni adaptativa a las necesidades de la organización (siempre entornos cambiantes). La tecnología SD-WAN va a hacer más sencilla la administración de los dispositivos de red, pero también vamos a poder permitir al sistema que sea automático a la hora de la toma de decisiones sobre rutas, consiguiendo que estas decisiones reduzcan y mejoren el rendimiento de nuestra red.

Las limitaciones de las redes actuales, no permiten que tanto las empresas como los proveedores de redes aprovechen al máximo las infraestructuras y necesitan invertir tiempo debido a la complejidad de las necesidades, políticas incoherentes entre los distintos elementos de red, poca escalabilidad y como siempre dependencia del vendedor.

Cada vez surgen más necesidades de una nueva arquitectura de red, ya que las redes tradicionales no tienen más posibilidades de mejora. Muchos de los servicios y necesidades surgidas en los últimos tiempos (heterogeneidad de patrones de tráfico, aumento de carga de trabajo para los administradores de red, aumentó de servicios basado en la nube, Big Data y ancho de banda necesario) implican que la forma de gestionar y controlar las redes sea de forma más flexible y sencilla.

Openflow fue uno de los estándares que surgió de la detección de estas necesidades. Con OpenFlow, una red puede ser gestionada como un todo, no como un número de dispositivos que gestionar individualmente, es el propio servidor el que dice a los switches dónde deben enviar los paquetes. Con esta tecnología, las decisiones que impliquen el movimiento de paquetes están centralizadas, por lo que la red puede ser programada independientemente de los switches. La arquitectura de red cuyo dinamismo, manejabilidad, rentabilidad y adaptabilidad permiten que sea adecuada para la naturaleza dinámica y de alto consumo de ancho de banda de las aplicaciones modernas. La necesidad de separar el control de la red de las funciones de reenvío con una API bien definida entre ambos, permitiendo la programabilidad del control de red y la abstracción de la infraestructura subyacente.

De toda esta evolución de las redes, nos lleva a la aparición de la SD-WAN. La SD-WAN simplifica la gestión y la operativa de las redes de área extensa (WAN), desacoplando los elementos físicos de red y los mecanismos de control de los mismos. La aplicación de las SD-WAN va a permitir a las empresas construir WAN que permitan unos menores costes y sobre todo un mayor rendimiento, tanto a nivel de red como de administración de la misma. Esto va permitir reemplazar WAN privadas sobre sistemas más costosos como MPLS y el uso de internet, como elemento de mayor disponibilidad y sobre todo un menor coste.

Las aplicaciones modernas como las llamadas VoIP, las videoconferencias, streaming, las aplicaciones en la nube y los escritorios virtualizados requieren una latencia baja. Los requisitos de ancho de banda también están aumentando, especialmente para aplicaciones con vídeo de alta definición. Puede resultar caro y difícil ampliar la capacidad WAN, con las correspondientes dificultades relacionadas con la gestión de la red y la resolución de problemas. Los productos SD-WAN están diseñados para abordar estos problemas de red. Al mejorar o incluso reemplazar los enrutadores tradicionales con dispositivos de virtualización que pueden controlar las políticas de nivel de aplicación y ofrecer una superposición de red, los enlaces de Internet de nivel de consumidor menos costosos pueden actuar más como un circuito dedicado.

MEF Forum ha definido una arquitectura SD-WAN que consta de SD-WAN Edge, SD-WAN Controller y SD-WAN Orchestrator. Esta normalización de MEF nos va a ayudar a la definición de los servicios de SD-WAN, pero también a comprender qué están comprando y ayuda a romper con las barreras de los servicios interoperables. La normalización de MEF fomenta un mercado abierto, intentando reducir la confusión inevitable en el nuevo mercado y con crecimiento muy rápido.

Los productos de SD-WAN del mercado, pueden ser productos hardware en appliance o basado solamente en software. Algunas de las características requeridas por la definición de SD-WAN son:

- Disponibilidad de múltiples tipos de conexiones: Internet, MPLS, 4G LTE o 5G.
- Selección dinámica de encaminamiento para repartir la carga, redundancia y alta disponibilidad.
- Un interfaz de configuración y gestión sencillo para los administradores de red.
- Soporte para VPN y servicios de terceros como WAN controllers, firewalls y gateways.

Además de estas características, hay una serie de funcionalidades que se incluyen en las diferentes soluciones SD-WAN del mercado:

- Resiliencia: Reducción del tiempo de parada de la red, detectando en tiempo real los problemas y proporcionando soluciones de forma automática y autónoma.
- Calidad de servicio (QoS).
- Seguridad (IPsec).
- Optimización de las aplicaciones: Entrega de la aplicación utilizando cache para acelerar el acceso y otros sistemas para acelerar su uso.
- ZTP (Zero Touch Provisioning): Aplicar configuraciones automáticamente una vez que hacemos la provisión de un nuevo dispositivo. A través de un repositorio común en la nube disponemos de todo lo necesario para que haga de configuración e interconexión entre las sedes y los equipos centrales.
- Administración y gestión de problemas centralizados: Una configuración centralizada para todas las tareas administrativas. Este tipo de soluciones para los administradores de red aporta una facilidad y una reducción de costes frente a las arquitecturas tradicionales donde la gestión es individualizada, con la complejidad que conlleva.
- Balanceo de líneas: Disponer de varios enlaces de uplink, nos va a permitir que a través de políticas de enrutamiento y balanceo llevar a cabo una importante mejora de cara a la disponibilidad y calidad de los servicios que ofrecemos a los usuarios.
- Ingeniería de tráfico online (análisis y optimización en tiempo real del tráfico de red)
- Gateways multiservicio: De forma muy habitual en las redes SD-WAN concentramos en el gateway de cada sede varios servicios tales como VPN, WiFi, NGFW, etc. permitiendo con un único equipo cubrir varias de las necesidades básicas que podrían darse en un entorno de este tipo.
- Disponibilidad de APIs: tanto la integración de soluciones de terceros, como ofrecernos a nosotros APIs podremos así disponer de ayuda a la hora de automatizar y optimizar tareas de gestión y monitorización.

Todas estas características y funcionalidades nos ofrecen una serie de ventajas principales:

- Ahorro de costes: aplicando inteligencia en tiempo real sobre la combinación de diferentes tipos de enlaces y ofreciendo a las redes SD-WAN un ROI muy atractivo.
- Mejora operativa: gestión centralizada y zero touch provisioning nos permite simplificar la labor del día a día para los administradores de red.

- Seguridad mejorada: Los túneles que conectan los gateways con el core de la red se securizan todas las comunicaciones entre las diferentes sedes, además de unificar el uso de estándares y protocolos de seguridad en la red.
- Disponibilidad e independizar el transporte: con los mecanismos de balanceo y la utilización de varios enlaces de uplink, mejora notablemente la disponibilidad de los servicios requeridos por los usuarios.
- Enfoque a la nube: optimizando el acceso de manera eficiente a todos los servicios/aplicaciones alojadas en la nube que son de uso cada vez más habitual dentro de las organizaciones.

Estudio Alternativas

Introducción

Es importante destacar que, pese a que la tecnología SD-WAN es una tecnología madura y en uso, adolece del mismo problema que muchas otras tecnologías del ámbito de las comunicaciones, la interoperabilidad entre fabricantes. No hay un estándar tecnológico que lo sustente y defina claramente SD-WAN, sino una especificación funcional del servicio que debe ofrecer y los diferentes fabricantes implementan su interpretación. En este documento se utilizarán los conceptos de la organización MEF (Metro Ethernet Forum) fundada en 2001 y ha definido un estándar funcional apoyado por varias de las grandes empresas tecnológicas. Parece que es la iniciativa principal para la estandarización y permite utilizar un marco común con conceptos definidos para hacer una comparativa válida.

Metro Ethernet Forum, define SD-WAN como servicios de red virtual superpuesta (a redes existentes, se entiende) que permite la conectividad entre interfaces de red de usuario, (SD-WAN UNI, del inglés User Network Interface) gestionada por políticas, orquestada y que permite tener en cuenta las aplicaciones que la utilizan; y provee la construcción lógica de una red privada de capa 3 enrutada que reenvía paquetes IP entre los “sites” del suscriptor del servicio.

Un servicio SD-WAN opera sobre uno o más servicios de conectividad subyacentes (UCS, del inglés Underlay Connectivity Services), por lo que puede ofrecer capacidades diferenciadas y adicionales a la utilización de una sola instalación de transporte de red.

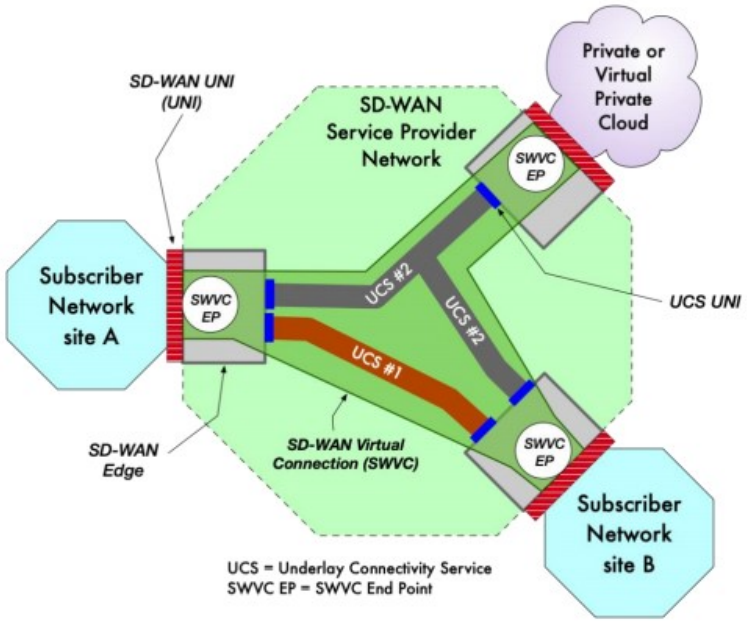
SD-WAN conoce los flujos de tráfico de las aplicaciones y reenvía tráfico en base a dichos flujos. El “acuerdo” de servicio incluye la especificación de los flujos de las aplicaciones, es decir el conjunto de criterios que caracterizan los paquetes IP de estas, así como las reglas y restricciones que hay que aplicar al reenvío de estos paquetes.

Los conceptos básicos para entender cómo funciona SD-WAN que se utilizarán en la comparativa tecnológica son los siguientes:

- UCS. Underlay Connectivity Services. Servicios de conectividad subyacentes.
- SD-WAN UNI. User Network Interface. Interfaz de red de usuario.
- SD-WAN Virtual Connection. Conexión Virtual.

- SD-WAN Virtual Connection End Point. Punto final de conexión virtual.
- Subscriber Network. Red del Suscriptor del servicio.
- Service Provider Network. Red del proveedor de servicios.
- Tunnel Virtual Connection (TVC). Conexión virtual tunelizada.

En el siguiente esquema pueden verse los diferentes componentes de un servicio SD-WAN.



Arquitectura SD-WAN MEF

Metodología utilizada en la comparativa

Para hacer la comparativa, se elegirán los parámetros relevantes a comparar y se le asignará un peso a cada uno. Cada una de las soluciones se puntuará de 1 a 10 cada uno de los parámetros elegidos, de esta forma trasladamos a una métrica cuantitativa información no homogénea y difícil de comparar.

Los parámetros relevantes a utilizar en la comparativa serán los siguientes:

- Fiabilidad: Con esta característica de los sistemas informáticos por la que se mide el tiempo de funcionamiento sin fallos, esto nos dará una confianza en los elementos hardware y software de la solución que nos aporta el proveedor.

- Escalabilidad: La capacidad para poder adaptarse a las necesidades debidas a un crecimiento de la demanda de los servicios ofrecidos, sin perder calidad y respondiendo a las necesidades de crecimiento. Se pueden distinguir dos tipos de escalabilidad: vertical y horizontal.
- Seguridad: La necesidad de proteger la integridad y confidencialidad en un sistema informático, deberemos analizar e identificar para minimizar los riesgos a la infraestructura informática. Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en tres partes: seguridad física, seguridad ambiental y seguridad lógica.
- Coste operación: El esfuerzo económico que una empresa hace por la realización de sus operaciones empresariales o de negocios. El costo operacional nos ayuda a establecer una referencia para medir las ganancias y obtener una aproximación del punto de equilibrio de la entidad. Además, el coste operacional es contemplado en el cálculo del ROI.
- Coste de implantación: Son la inversión que vamos a tener que asumir para poner en marcha la implantación del sistema en el entorno de operación, calculando el esfuerzo y los recursos necesarios para realizar la implantación.
- Calidad del soporte: Cuando un proyecto está operativo y ofreciendo servicio, puede experimentar alguna situación no deseada. En esta situación el proveedor debe ofrecer soluciones para evitar el deterioro del servicio y una mejor experiencia a los clientes.

Análisis alternativas

En el mercado hay multitud de alternativas, algunas de ellas puramente software, principalmente alternativas basadas en soluciones open source y otras basadas en soluciones propietarias e integradas en dispositivos de uso específico. De entre las alternativas Open source, pueden destacarse:

- OpenDayLigth.
- flexiWAN.

Mientras que de las alternativas propietarias puede destacarse:

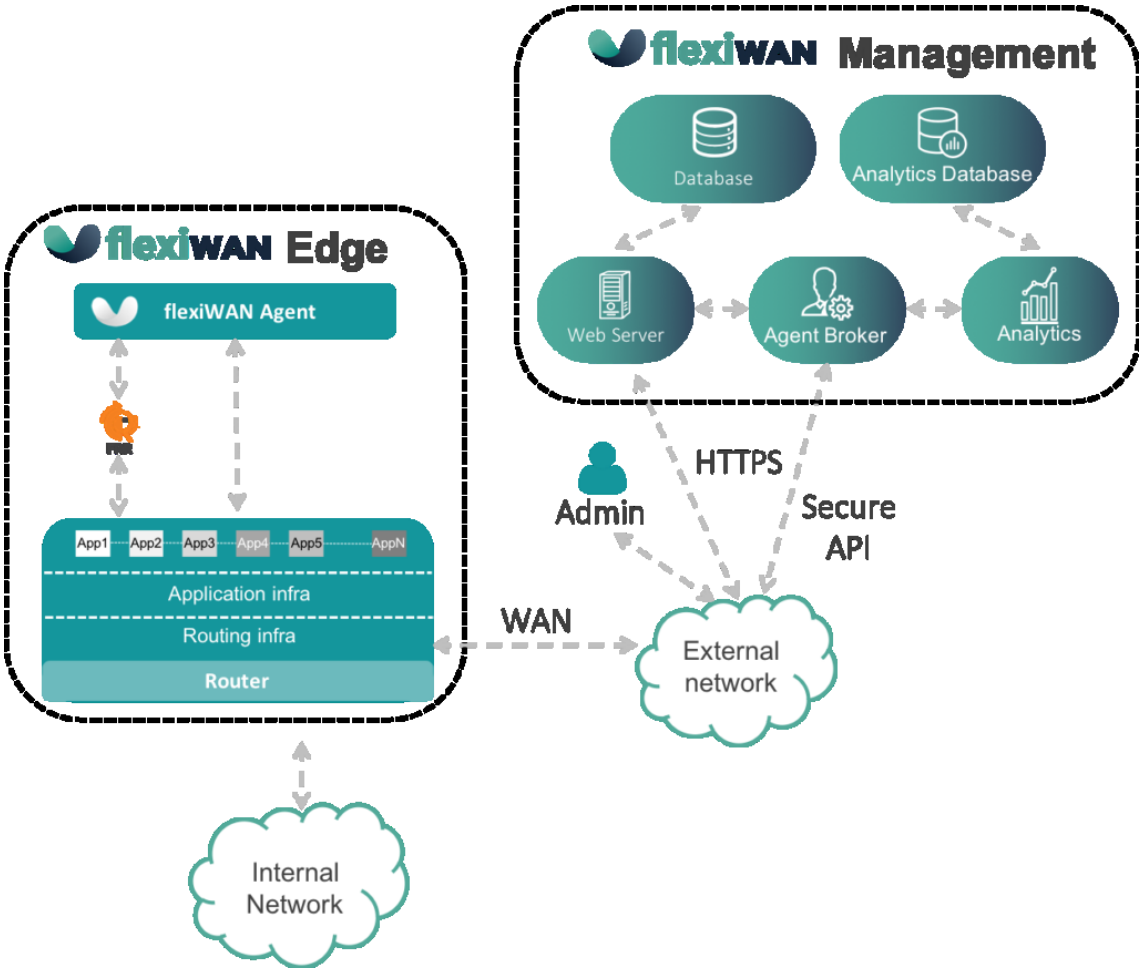
- Nuage Networks (Nokia).
- Cisco SD-WAN.
- Aruba SD-WAN.
- SD-WAN Fortinet.

Obviamente hay muchos más fabricantes y soluciones, pero como ejercicio teórico vamos a centrar la comparativa en solamente 4 opciones, una basada en software libre y tres soluciones comerciales de fabricantes con gran implantación en el sistema sanitario español:

- flexiWAN.
- Cisco SD-WAN.
- Aruba SD-WAN.
- SD-WAN Fortinet.

flexiWAN

La arquitectura de flexiWAN consta básicamente de dos componentes flexiEdge, que es el componente que se despliega en las diferentes ubicaciones y flexiManage, que es el sistema central de administración, que se conecta mediante un API seguro a flexiEdge para la orquestación y administración.



Arquitectura flexiWAN

Fiabilidad. Es un proyecto en crecimiento que ofrece todo el software en modo open source, pero que dispone de un servicio cloud (SaaS) que tiene ya más de 1.000 clientes de primer nivel. Obviamente en este punto no es comparable aún con compañías de gran experiencia y renombre, pero su enfoque está ganando rápidamente cuota de mercado. 7 puntos.

Escalabilidad. Todas las soluciones SD-WAN son por definición escalables. En este caso, hay un punto a favor de flexiWAN puesto que no solo es escalable en cuanto a número de sedes a conectar, sino también en cuanto al número de fabricantes de dispositivos soportados. Al ser unas soluciones open source, puede ser instalada en hardware de cualquier fabricante que soporte. 10 puntos.

Seguridad. Pese a no tener la seguridad como foco, al ser un proyecto open source, garantiza el acceso completo al código fuente, lo que es una garantía adicional. 8 puntos.

Coste operación. Los tres primeros nodos son gratuitos, lo que brinda una oportunidad fantástica de hacer una prueba de concepto a un coste mínimo. Los precios de la solución son públicos y están en la web. 10 puntos.

	Precio por nodo y mes	
Nodos	Pago Mensual	Pago anual
Hasta 3	-	-
4 – 10	$40	$33
11 – 100	$30	$25
101 – 500	$25	$21
501 – 1,000	$20	$17
1,001 – 5,000	$12	$10

Precios flexiWAN

Coste de implantación. En función del tipo de instalación a poner en marcha este coste puede variar, puede contratarse mediante un servicio SaaS, lo que nos llevaría al precio de entrada o con una instalación on-premise, lo que implica la instalación de varios cluster (MongoDB, Redis y recursos devops) y de un número significativo de horas de trabajo que solamente serían asumibles para un despliegue realmente extenso en cuanto a número de sedes. 8 puntos.

Calidad del soporte. El novedoso enfoque de flexiWAN ha hecho que flexiWAN haya crecido mucho en los últimos tiempos, no obstante, no hay información pública sobre los partners oficiales por lo que no es posible conocer este detalle. 5 puntos.

Puntos fuertes:

- Un menor coste de la solución.

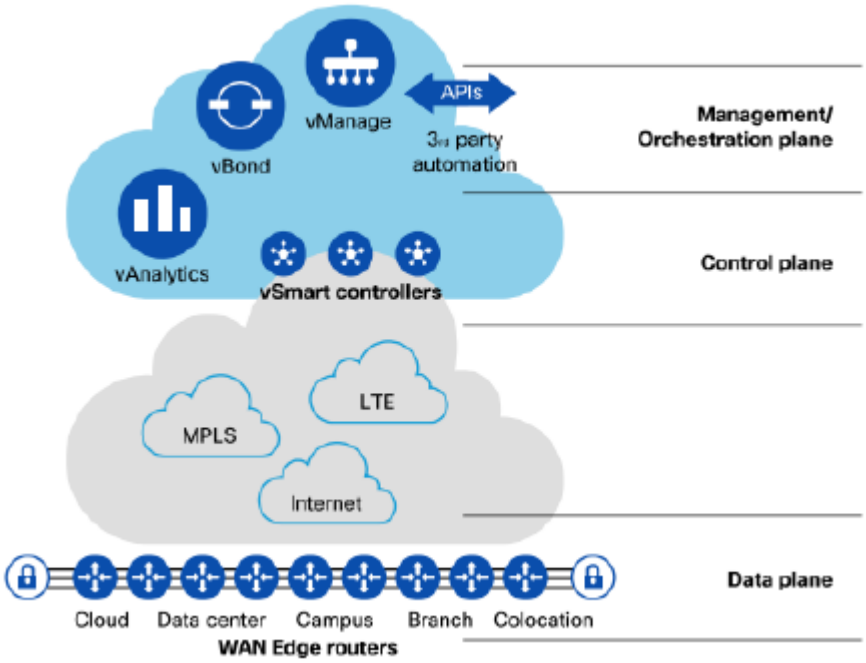
Puntos débiles:

- Poca información sobre los partners.

- Poco tiempo en el mercado.

Cisco SD-WAN

La topología de SD-WAN de Cisco divide la solución en cuatro planos, el plano de datos, el de control, el de administración y el de orquestación, tal como ilustra la siguiente figura:



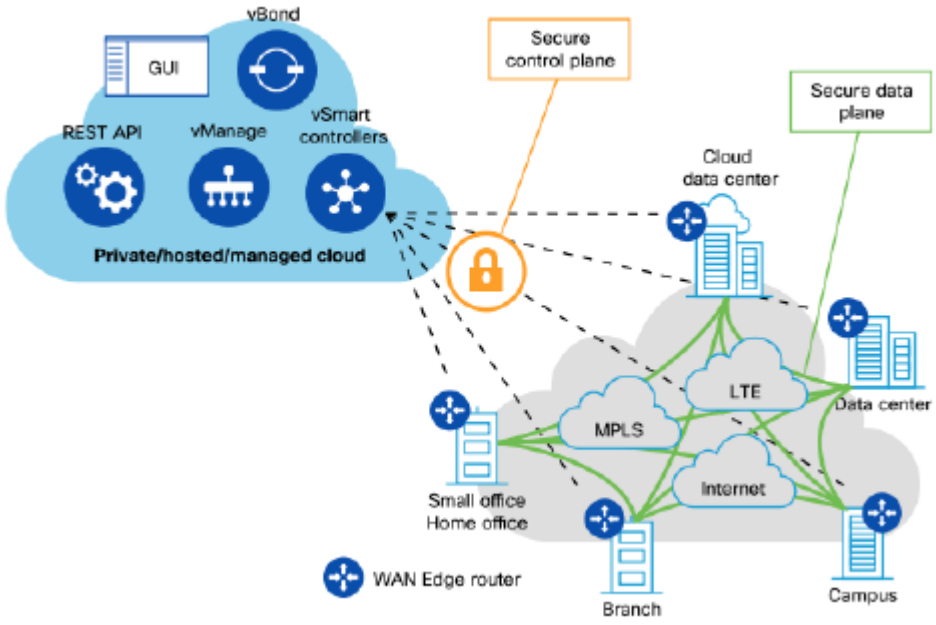
Capas CISCO SD-WAN

Y utiliza cuatro componentes clave, vManage, vBond, vSmart y los routers SD-WAN Edge.

- vManage se encuentra en el plano de administración/gestión y se encarga de proveer el interfaz de usuario para configurar los dispositivos, aprovisionarlos y monitorizarlos.
- vBond se encarga de la orquestación y es quien se encarga del aprovisionamiento zero-touch, cuando un router arranca por primera vez, es vBond quien se encarga de introducirlo en la SD-WAN. Este componente conoce la topología de la red y se encarga de trasladar a todos los dispositivos.
- vSmart es quien traslada las políticas definidas en vManage a toda la red, se encuentra en el plano de control. La información de enrutamiento de cada una de las sedes se intercambia a través de este componente mediante el protocolo (propietario) Overlay Management Protocol (OMP).

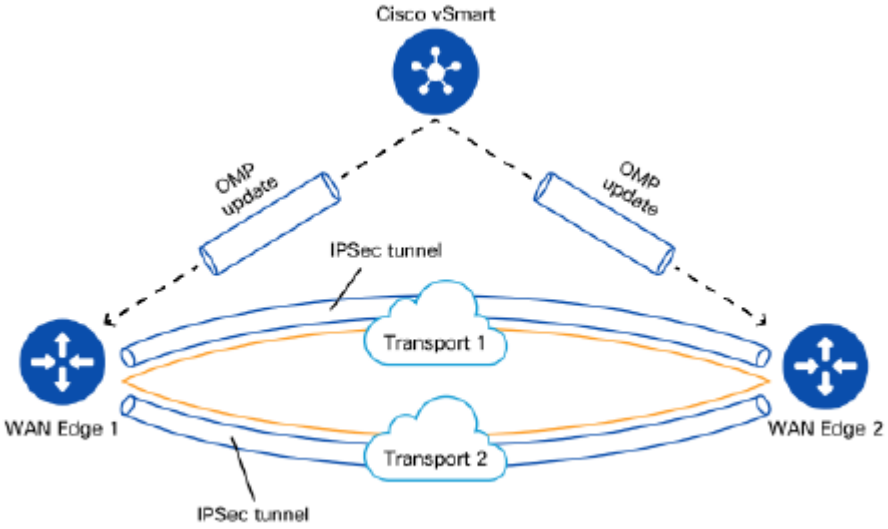
- WAN Edge Routers. La funcionalidad, capacidad, rendimiento y conectividad de las sedes se delega en las diferentes familias de equipo que provee el fabricante.

Las redes SD-WAN de Cisco son denominadas Cisco SD-WAN Fabric y se forman combinando todos estos elementos.



Esquema CISCO SD-WAN

Los routers WAN Edge crean túneles IPsec entre ellos para formar la red y establecen un canal entre ellos y los elementos de control. Por defecto la red es completamente mallada y toda la información se intercambia de forma segura a través de los túneles IPsec y el protocolo OMP.



Esquema conectividad CISCO SD-WAN

Fiabilidad. Cisco es uno de los líderes del mercado de las redes WAN por lo que es obviamente una apuesta segura en cuanto a la fiabilidad. 10 puntos.

Escalabilidad. La solución de Cisco es escalable hasta miles de sitios según indica el fabricante en su web por lo que la puntuación en este aspecto debe ser alta. 9 puntos.

Seguridad. La utilización de túneles IPsec para la comunicación entre las sedes hace que la seguridad sea también muy alta. 9 puntos.

Coste operación. Una vez puesto en marcha, el coste de operación de las redes SD-WAN de cisco no debe ser alto, las herramientas de gestión están diseñadas para centralizar y automatizar las operaciones lo que, sobre todo en redes de gran despliegue, es una significativa ventaja en cuanto a coste. 7 puntos.

Coste de implantación. Las soluciones de CISCO no son baratas, no es fácil encontrar precios públicos del fabricante, pero la experiencia dice que es uno de los puntos débiles de la solución, además, hay que tener en cuenta que las funcionalidades y capacidad varían y condicionan el equipo a instalar. 5 puntos.

Calidad del soporte. El prestigio y la larga experiencia que ofrece CISCO es un gran baluarte a la hora de ofrecer soluciones cuando aparece alguna indisponibilidad del servicio. 9 puntos.

Puntos fuertes:

- Una solución muy madura en el mercado de las comunicaciones.
- Solución tanto en un entorno On-premise como en entorno en la nube.

Puntos débiles:

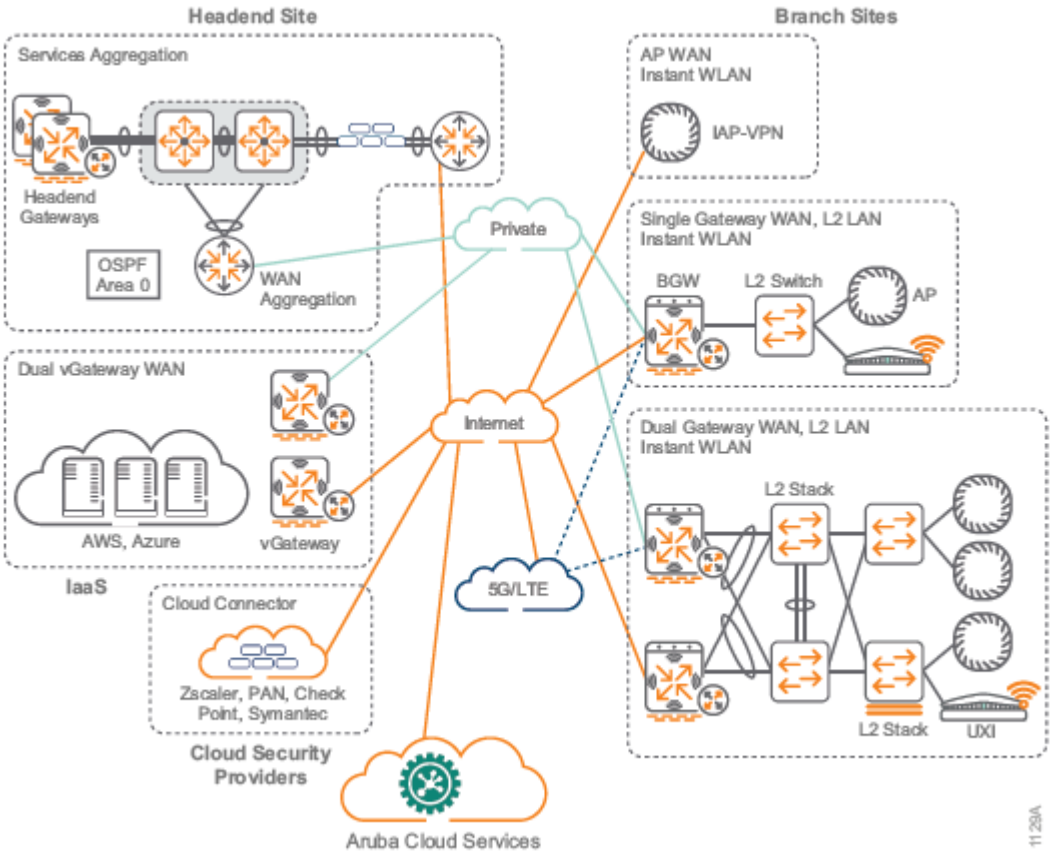
- Solución con un alto coste, tanto en la compra, como en la implantación y soporte.

Aruba SD-WAN

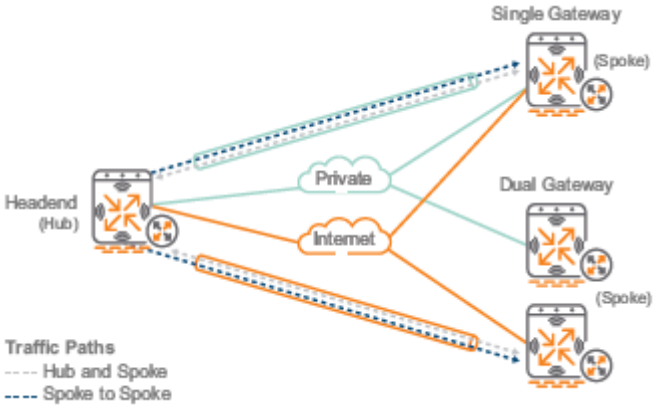
Aruba incluye servicios de SD WAN en su concepto SD-BRANCH, que incluye funcionalidades adicionales y que va un paso más allá e incluye soluciones SD-LAN llevando estos conceptos a toda la infraestructura de red. Se basa en los siguientes componentes:

- Aruba Central. Es el software donde se configuran las políticas y la monitorización de los elementos que componen la red (sd-fabric) y que simplifica y centraliza las operaciones de red y el aprovisionamiento de cualquiera de los elementos.
- Aruba ClearPass. Gestiona la seguridad de la red desde un punto centralizado asegurando que cada dispositivo y usuario tiene asignado el rol que le corresponde dentro del conjunto.
- Aruba Headend gateways. Concentran los túneles que establecen las sedes remotas. Son equipos de la serie 7200. Sus funcionalidades están también disponibles en plataformas virtualizadas para aquellas organizaciones que están migrando sus infraestructuras a servicios (IaaS).
- Aruba Branch Gateways. Son los equipos que se utilizan en las oficinas remotas y que proporcionan los servicios de red (routing, firewalling, security). Cada BGW se conecta a uno o varios concentradores centrales para formar la red.
- SD-WAN Orchestrator. Para simplificar la configuración, Aruba ha introducido en su solución esta herramienta, que automatiza la creación de los túneles y la orquestación del routing. Este software se ejecuta en Aruba Central.
- Otros dispositivos utilizables en el concepto de SD-BRANCH son los Aruba Access Switches y Aruba Access Point, pero no forman parte de la red SD-WAN aunque si son gestionables desde Aruba Central y pueden aplicarse conceptos SD-LAN.

La arquitectura propuesta por Aruba para su SD-BRANCH sería:



Esquema ARUBA



Conectividad ARUBA

Fiabilidad. Es una solución comercial de un fabricante líder en redes LAN, Aruba tiene experiencia en WAN. En España la más potente es INDITEX con la WAN de todas las redes de tiendas (>7000) entre otras. Es un líder mundial en networking y el valor se le supone. 10 puntos.

Escalabilidad. Aruba ha hecho esfuerzos en integrar todas las partes de una red en una única solución que permita gestionar una red homogénea Aruba desde la WAN hasta la LAN y WLAN. Soporta Full-Mesh entre sedes. 9 puntos.

Seguridad. El hecho de que todo el tráfico curse a través de los controladores centrales hace que la seguridad aumente, además el uso de ClearPass (de eficacia demostrada en entornos LAN) es un indicativo de que la seguridad de esta solución es muy alta. Fue el primer (y Es de los pocos) fabricantes que tiene en el catálogo de soluciones seguras del CCN el NAC, wireless, switching y VPN. https://oc.ccn.cni.es. Portfolio fuertemente avalado por certificaciones Common Criteria de Seguridad. Es el fabricante de referencia de DoD USA. Ejemplo el pentágono. 9 puntos.

Coste operación. No presenta un coste de operación, es una de las razones de fidelizar clientes y apenas pierden base instalada por el coste de operación. La solución ZTP de despliegue es muy madura y sólida en el mercado. Miles de equipos se despliegan de forma desatendida. Aruba no tiene protocolos propietarios y es interoperable, por lo que convive en un entorno de competencia. Aruba tiene ciclos de vida largos. Dispone de equipos de uso común en redes empresariales con garantía hardware de por vida (sin letra pequeña). 9 puntos.

Coste de implantación. Aruba apuesta por el concepto de SD-Branch=SD-LAN + SD-WAN. Visión y gestión de las conexiones de forma completa (acceso, seguridad, LAN, WAN) desde una consola. Puede venderse la parte WAN, la parte LAN o ambas, permite concentrar la gestión de la LAN y la WAN. 9 puntos.

Coste de implantación: A través de Aruba Central como herramienta para realizar de una manera ágil y muy flexible la puesta en marcha de la infraestructura a desplegar, simplificando la gestión y la seguridad de la infraestructura SD-BRANCH. Seguridad por defecto y sobre todo zero touch provisioning. 9 puntos.

Calidad del soporte. El soporte de ARUBA en redes LAN y WLAN es bueno. Disponemos de diferentes niveles de soporte para sus clientes, desde el más básico a más avanzado ofreciendo. 9 puntos.

Puntos fuertes:

- Una solución madura.
- Apuesta por la innovación por añadir solución de SD-Branch.

Puntos débiles:

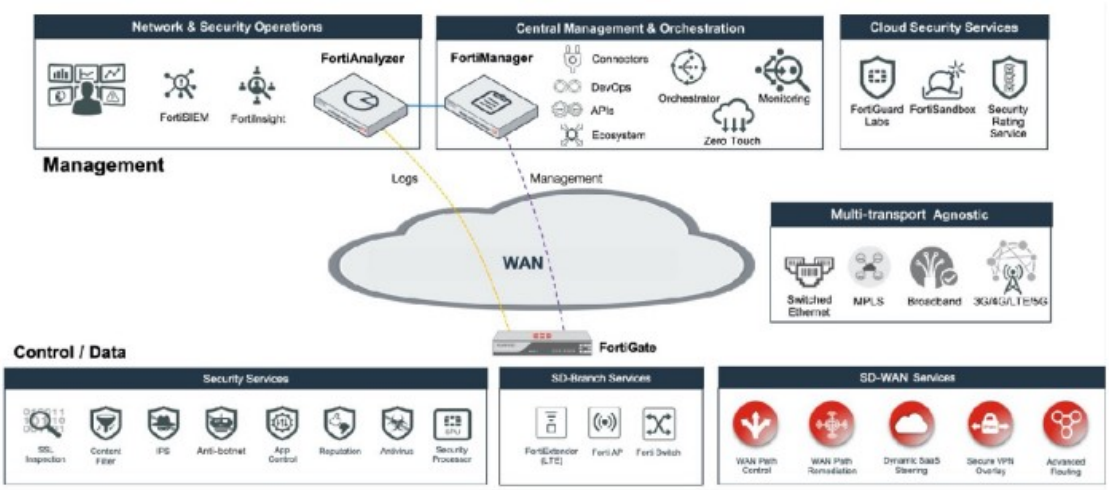
- Solución con un gran coste, al ser uno de los grandes proveedores de soluciones.

SD-WAN Fortinet

La arquitectura SD-WAN que propone Fortinet difiere de una forma importante del resto de fabricantes, es una arquitectura sin controlador central en la que los propios dispositivos de las oficinas remotas mantienen la autonomía sobre el plano de control de la red SD-WAN. Los componentes son los siguientes:

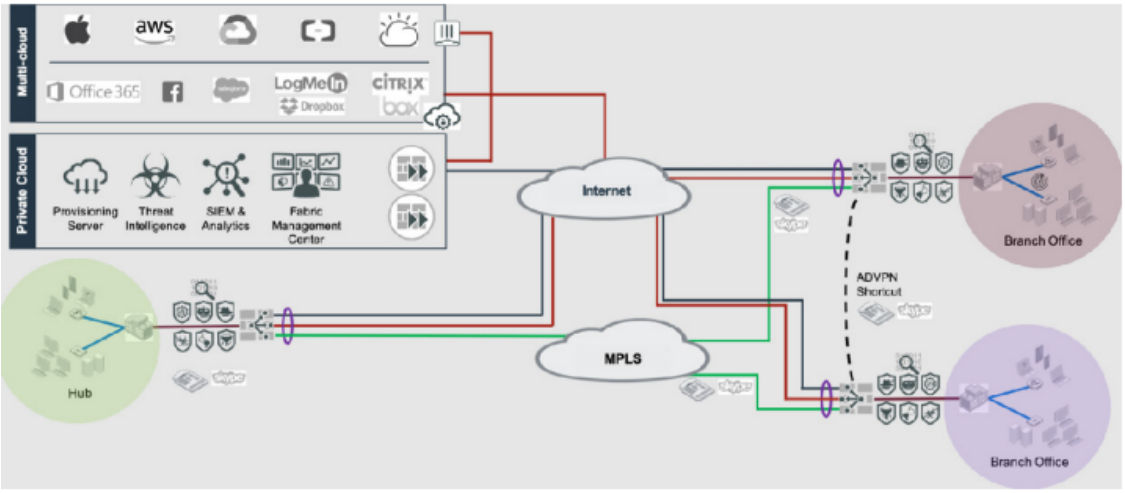
- Fortigate NGFW. Los dispositivos que se utilizan en las oficinas remotas, el sistema operativo que utilizan es FortiOS, que es el núcleo de la SD-WAN de Fortinet.
- FortiManager. Es el componente de gestión centralizada donde se incluye el orquestador de la red Forti-Orchestrator, que automatiza el despliegue de la red
- FortiAnalizer para la monitorización y análisis.
- FortiDeploy para el aprovisionamiento zero-touch.

El sistema FortiOS actúa en todos los roles (gestión, control y plano de datos) y no requiere de un dispositivo centralizado (cloud u on-premise) para la construcción de la red. No obstante, mantiene una gestión centralizada desde el sistema FortiManager. Cada Fortigate se comunica con los componentes centralizados, pero mantiene toda la funcionalidad del plano de control. El transporte de paquetes sobre los enlaces disponibles, las capacidades y funcionalidades de la SD-WAN son gestionados sin la dependencia de entradas de plano de control por un dispositivo externo. Este diseño permite despliegues de más de 15.000 puntos de red, permitiendo la conexión directa entre ellos.



Capas Fortinet

La solución de Fortinet, construye una red utilizando túneles IPsec creando en la práctica un red full-mesh entre todas las oficinas. La siguiente figura una topología hub-and-spoke con accesos directos entre oficinas.



Esquema Fortinet

Fiabilidad. Es una solución comercial de un fabricante líder en firewalls y VPNS por lo que tiene experiencia demostrada en la tecnología subyacente (VPS). 10 puntos.

Escalabilidad. El diseño sin controlador y la conexión directa entre sedes favorece la escalabilidad, el propio fabricante habla de la posibilidad de redes de más de 15.000 oficinas. 9 puntos. 9 puntos.

Seguridad. Los equipos (y sistema operativo) de Fortigate son los mismos equipos que se utilizan para sus soluciones de seguridad e incluyen inspección SSL como funcionalidad básica. Es un fabricante que viene de la seguridad de red. 10 puntos.

Coste operación. Además de ofrecer productos a un menor coste que otros proveedores con más experiencia, añade la posibilidad de un servicio llamado 360 Protection bundle. El cual aporta la experiencia que tiene Fortinet en el área de seguridad, como servicio avanzado de detección de malware, IPS, Web filtering, etc. 9 puntos.

Coste de implantación. Ofrece la posibilidad para el despliegue ágil, a través de soluciones más habituales tanto para la nube pública (Amazon AWS, Microsoft Azure, Oracle OCI/OPC, Google GCP o Alibaba Cloud) como para la nube privada (VMWare VSphere, Citrix Xen, Xen, KVM, Microsoft Hyper-V o Nutaix AHV) de su FG-MV. 9 puntos.

Calidad del soporte. En otros productos (FW), el soporte de Fortinet es bueno, los equipos a utilizar son los mismos por lo que el soporte no debe disminuir en calidad ofrecida por este tipo de solución.

Ofrece soporte Premium RMA con reemplazamiento de productos en cuatro horas, además del servicio típico de soporte de 24x7. 9 puntos.

Puntos fuertes:

- Una solución madura.
- Proveedor con mucha experiencia en la rama de la seguridad.

Puntos débiles:

- Solución con poco recorrido y menor implantación que la ofrecida por otros proveedores especialistas en las comunicaciones.

Tabla comparativa final

Aspecto	Peso	FlexiWAN		Cisco		Aruba		Fortinet	
		Ptos	Pond.	Ptos	Pond.	Ptos	Pond.	Ptos	Pond.
Fiabilidad	1	7	7	10	10	10	10	10	10
Escalabilidad	0,5	10	5	9	4,5	9	4,5	9	4,5
Seguridad	1	8	8	9	9	9	9	10	10
Coste Operación	0,8	10	8	7	5,6	9	7,2	9	7,2
Coste Implantación	0,5	8	4	5	2,5	9	4,5	9	4,5
Soporte	0,8	5	4	9	7,2	9	7,2	9	7,2

Comparativa alternativas SD-WAN

Selección de la solución a implantar

Se ha optado por seleccionar como solución SD-WAN a ARUBA por diversos motivos, el principal ha sido la integración con equipamiento y ciertos servicios ya implantados en el SESCAM, por un lado, con la solución del Control de Acceso a Red (NAC) a través de ClearPass.

Existe una integración total a la hora de establecer las políticas de seguridad en base a roles, equipos, IOT, etc esto integrado con la parte de SD-LAN hacen que la solución adopte una dimensión más completa y efectiva.

Otro punto a su favor es la existencia en el SESCAM de la plataforma de Gestión ARUBA Central Device Management que centraliza la gestión de todo el equipamiento ARUBA en una única herramienta.

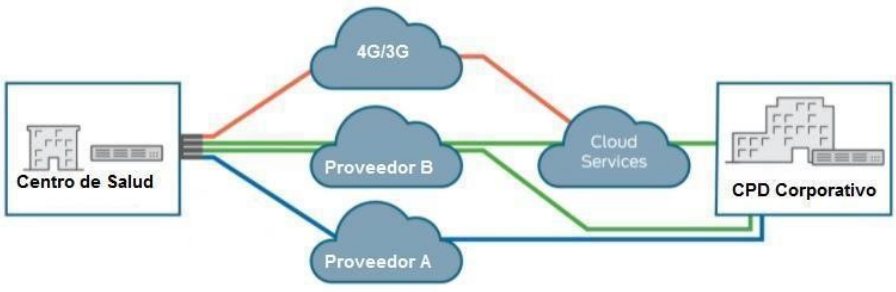
Igualmente, la existencia de switches ARUBA en los Centros de Salud presenta grandes ventajas a la hora de aplicar seguridad en base a ROLES, establecimiento de túneles, identificación de equipos de forma más completa, etc.

Por otro lado, aunque la solución ARUBA esté entre las 2 puntuaciones más altas, la valoración anterior puede ser algo subjetiva, se consideran fundamentales las integraciones anteriormente descritas.

La descripción técnica del equipamiento se incluye en el ANEXO 2 del presente documento a través de los datasheets del fabricante.

La solución estaría compuesta de 2 equipos centralizados en los CPDs corporativos, para disponer de alta disponibilidad y redundancia física, uno se instalaría en el CPD principal de Huérfanos Cristinos y el otro en el CPD de respaldo de Estenilla.

Por otro lado, se instalarán 2 equipos en cada sede remota o Centro de Salud para disponer de redundancia en caso de caída de uno de ellos.



Esquema conectividad centro de salud

Coste de implantación

Se considera que los costes de implantación de la solución serán:

- Costes de infraestructura:
  - Equipamiento.
  - Líneas
- Costes de Servicios:
  - Costes de instalación.
  - Costes de Ingeniería.
  - Costes de Formación.

A continuación, se desglosan cada uno de los costes anteriormente mencionados.

Costes de equipamiento

Los costes son aproximados y pueden variar, en concreto los equipos centralizados tendrían un coste aproximado:

Descripción	Precio unitario	Cantidad	Sub Total	Descuento	Total
GATEWAYs CENTRALES					
Aruba 7210 (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller	€15.923,00	2	€31.846,00	50,00 %	€15.923,00
Aruba PSU-350-AC 7200 Series S3500-24T S3500-48T and S3500-24F 350W AC Power Supply	€464,00	2	€928,00	50,00 %	€464,00
PC-AC-EC Continental European/Schuko AC Power	€5,00	4	€20,00	50,00 %	€10,00

Cord					
Aruba 3Y FC NBD Exch HW7210 Cntrl SVC	€1.189,00	2	€2.378,00	5,00 %	€2.259,10
Aruba 3Y FC NBD Exch PSU-350-AC SVC	€48,00	2	€96,00	5,00 %	€91,20
OPCIONES LICENCIAS GATEWAYs CENTRALES					
Aruba 72xx Gateway Foundation 3yr Sub E-STU	€17.245,00	2	€34.490,00	50,00 %	€17.245,00
			TOTAL		€35.992,30

Coste ARUBA equipos centralizados

El coste de cada sede o Centro de Salud, sería:

Descripción	Precio unitario	Cantidad	Sub Total	Descuento	Total
OPCIONES GATEWAYs REMOTAS					
Aruba 9004 (RW) LTE Branch Gateway	€1.708,00	2	€3.416,00	40,00 %	€2.049,60
OPCIONES LICENCIAS GATEWAYs REMOTAS					
Aruba 90xx Gateway Foundation plus Security 3yr Sub E-STU	€3.066,00	2	€6.132,00	50,00 %	€3.066,00
SOPORTES GATEWAYs REMOTAS					

Aruba 3Y FC NBD Exch HW 9004 LTE SVC	€128,00	2	€256,00	5,00 %	€243,20
ARUBA CENTRAL					
Aruba Central Device Management 1 Token 3 Year Subscription E-STU	€187,00	2	€374,00	50,00 %	€187,00
			TOTAL		€5545,80

Coste ARUBA equipos de sedes/centro de salud

La solución se aplicaría sobre los 204 Centros de Salud pertenecientes al Servicio de Salud de Castilla-La Mancha, de esta manera el coste de la infraestructura sería la suma del coste de los equipos centralizados más el coste del equipamiento de todas las sedes o Centros de Salud.

- **Coste equipos centralizados: 35.992,30 euros.**
- **Coste equipos de Centros de Salud: 5.545,8 euros/sede X 204 sedes=1.131.343,2 euros.**
- **Routers para linea FTTH 300/300: 620 euros aprox. X 2 proveedores/sede=1.240 euros/sede X 204 sedes=252.960 euros**

Coste total infraestructura=Coste equipos centralizados + Coste equipos de Centros de Salud + routers en CS.

35.992,30 euros + 1.131.343,2 euros + 252.960 euros =**1.420.295,50 euros**

El coste de los routers se ha contemplado según catálogo de 2 proveedores diferentes.

El coste del equipamiento lleva implícito el coste de la garantía durante un periodo de 3 años con un soporte de fabricante NBD 24x7.

Este coste es aproximado y no tiene el IVA aplicado.

Costes de líneas por cada sede

Actualmente como se ha comentado en apartados anteriores las líneas actuales en cada Centro de Salud son:

Tpo de centro	Enlace principal	Ancho de banda	Enlace de respaldo	Ancho de banda
Centro de Salud - CS	MacroLAN	10 Mbps (simétricos)	ADSL	<= 10 Mbps (asimétricos)

Costes de líneas por sede

Para dotar de redundancia y flexibilidad se va a optar por incluir en cada sede de 2 líneas FTTH más una tercera 4G de proveedores diferentes.

- **Coste de línea FTTH por sede:**

Detalle - Sede Tipo (FTTH 300Mbps/300Mbps): 52 euros aprox x 2 proveedores/sede=104 euros x 204 sedes=21.216 euros mensuales

- **Coste de línea 4G por sede:**

  Detalle- Sede Tipo (Acceso radio de navegación):29 euros aprox X 204 sedes=5.916 euros mensuales.

Para calcular el coste de las líneas FTTH, se ha contemplado la media del coste de 2 proveedores diferentes.

La estimación de coste de líneas total sería de: 21.216 euros + 5.916 euros= 27.132 euros mensuales X 12= 325.584 euros anuales.

Costes de instalación

La instalación se llevará a cargo por parte del personal técnico de cada una de las gerencias, por tanto, no supondrá un sobrecoste, el equipamiento se adecuará en los racks de los centros de salud, contemplando que hay hueco disponible en dichos armarios y no habrá que ampliarlos ni adquirir nuevos, igualmente se contempla que los SAIs ubicados en cada uno de los Centros disponen de potencia suficiente para dar soporte a todos los equipos ubicados en cada uno de los racks.

La configuración necesaria de cada uno de los equipos estará contemplada en la parte de ingeniería, dicha configuración será consensuada con personal de TI del SESCAM y personal experto de la parte

de proveedor y será desplegada con personal TI del SESCAM una vez se reciba la formación necesaria para poder asumir el servicio de nivel 1.

Coste de ingeniería

Los trabajos de ingeniería, definición del servicio, configuración inicial y puesta en marcha se llevarán a cabo durante 15 jornadas con un coste total estimado de 13.500 euros.

Estos costes son estimatorios y se han calculado teniendo en cuenta los costes de otros proyectos similares en envergadura e impacto en la organización.

Estos trabajos se definirán con personal técnico del SESCAM y de la parte integradora.

Coste de Formación

La formación estará orientada a describir lo que puede aportar la solución en la organización y a detallar las tareas necesarias para poder asumir el soporte de nivel 1 mientras esté en producción el servicio.

Tendrá las siguientes características:

- Duración: 7 días.
- In situ en las oficinas del SESCAM.
- Capacidad para 15 asistentes.
- Horario: de lunes a viernes de 9:00 a 15:00 horas.

Tiene un coste estimado de 12.000 euros.

Estos costes son estimatorios y se han calculado teniendo en cuenta los costes de otros proyectos similares en envergadura e impacto en la organización.

Resumen de costes

Elemento	Coste	Tipo
Equipamiento	€1.420.295,50	3 años

ºLíneas	€325.584,00	Anual
Instalación	- €	Inicial
Ingeniería	€13.500,00	Inicial
Formación	€12.000,00	Inicial
TOTAL	**€1.771.379,50**	

Resumen de costes

El coste actual anual es aproximadamente de:

	Costes actuales			
	Coste sede	**Número de sedes**	**Coste mensual**	**Coste anual**
Sede (10Mbps/ADSL VPN-IP hasta 10Mbps TFO)	€490,78	204	€100.119,12	**€1.201.429,44**

Resumen costes actuales

Para poder comparar los costes actuales anuales con los costes anuales de la nueva solución, hay que tener en cuenta que hay ciertos gastos que facturarían en un momento dado y no serían recurrentes, por tanto, los costes de la nueva solución los repartimos en 3 años, para calcular el coste anual, de esta manera dichos costes se quedarían de la siguiente forma:

Elemento	**Coste**	**Tipo**	**Costes Anuales**
Equipamiento	€1.420.295,50	3 años	€473.431,83
Líneas	€325.584,00	Anual	€325.584,00
Instalación	€	Inicial	€
Ingeniería	€13.500,00	Inicial	€4.500,00
Formación	€12.000,00	Inicial	€4.000,00

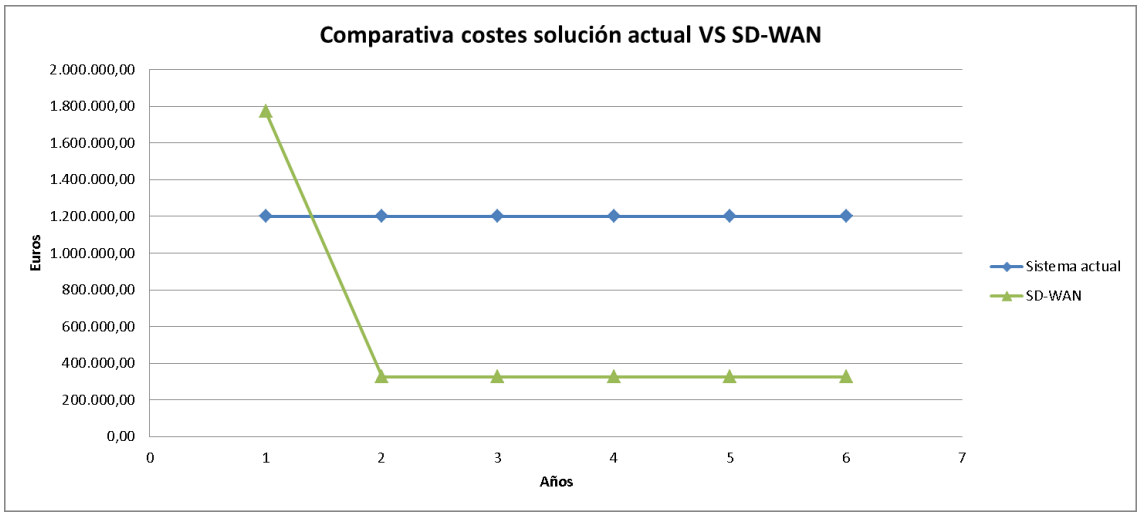
TOTAL	€1.771.379,50		€807.515,83

Resumen costes anuales

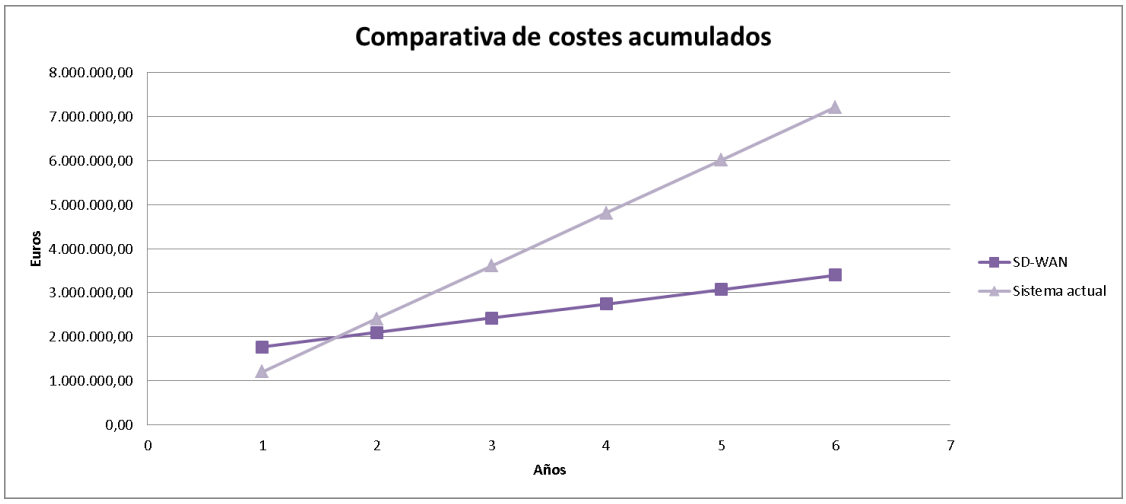
A partir del 4º año se eliminarían los costes no recurrentes como el hardware, la ingeniería, y la formación, solamente se quedarían los costes de las líneas y de las licencias de soporte para otros 3 años.

Descripción	Coste	UDS	Total 3 años	Total Anual
Aruba 3Y FC NBD Exch HW7210 Cntrl SVC	€2.259,10	1	€2.259,10	€753,03
Aruba 3Y FC NBD Exch PSU-350-AC SVC	€91,20	1	€91,20	€30,40
Aruba 72xx Gateway Foundation 3yr Sub E-STU	€17.245,00	1	€17.245,00	€5.748,33
Aruba 90xx Gateway Foundation plus Security 3yr Sub E-STU	€3.066,00	204	€625.464,00	€208.488,00
Aruba 3Y FC NBD Exch HW 9004 LTE SVC	€243,20	204	€49.612,80	€16.537,60
Aruba Central Device Management 1 Token 3 Year Subscription E-STU	€187,00	204	€38.148,00	€12.716,00
Líneas Sede Tipo (FTTH 300Mbps/300Mbps)	€52,00	408	€763.776,00	€254.592,00
Líneas Sede Tipo (Acceso radio de navegación)	29,00 €	204	€212.976,00	€70.992,00
			€1.709.572,10	**€569.857,37**

Costes recurrentes



Comparativa costes acutal VS SD-WAN



Comparativa de costes acumulados

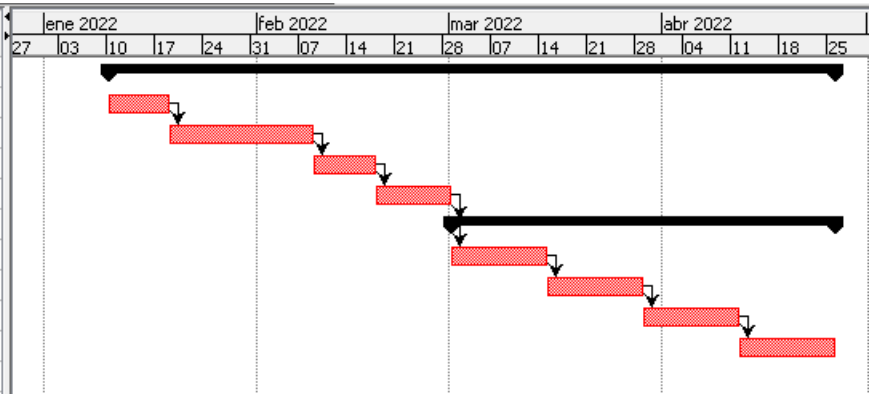
Planificación de la puesta en marcha

Se plantea una planificación teórica de 76 días contando a partir del día 10 de enero de 2022. Los primeros 36 días se dividen en cuatro periodos de definición y diseño antes del despliegue:

- Formación en la solución y soporte asociado. 7 días de formación previa para capacitar al equipo de trabajo en la toma de decisiones sobre el despliegue.
- Definición y establecimiento de la Solución. 15 días dedicados al diseño de la solución y a la recepción del material y a la planificación detallada que deben de servir de base fundamental para la puesta en marcha del piloto y del despliegue global de la solución.
- Integración e Instalación del piloto. 7 días de instalación y puesta en marcha del piloto en los centros definidos.
- Pruebas de Validación del piloto. 7 días de pruebas para validar el funcionamiento del piloto.

- El resto de los 40 días se definen como un despliegue en cuatro fases de 10 días para el despliegue en el total de centros (204), la planificación detallada de estas cuatro fases se definirá en el período de diseño y planificación detallada.

	Nombre	Duracion	Inicio	Terminado
1	**Proyecto**	76 days	**10/01/22 9:00**	**26/04/22 9:00**
2	Formación de la solución y soporte asociado	7 days	10/01/22 9:00	19/01/22 9:00
3	Definición y establecimiento de la Solución	15 days	19/01/22 9:00	9/02/22 9:00
4	Integración e Instalación de piloto	7 days	9/02/22 9:00	18/02/22 9:00
5	Pruebas de Validación del piloto	7 days	18/02/22 9:00	1/03/22 9:00
6	**Despliegue**	40 days	**1/03/22 9:00**	**26/04/22 9:00**
7	Fase I	10 days	1/03/22 9:00	15/03/22 9:00
8	Fase II	10 days	15/03/22 9:00	29/03/22 9:00
9	Fase III	10 days	29/03/22 9:00	12/04/22 9:00
10	Fase IV	10 days	12/04/22 9:00	26/04/22 9:00



Planificación de la puesta en marcha

Riesgos

La implantación de esta nueva forma de desplegar y gestionar las comunicaciones de los sistemas informáticos, puede llevar a una serie de problemas a la hora de poner en valor el uso de la tecnología SD-WAN.

Hemos detectado los siguientes puntos a tener en cuenta:

- Problemas de cobertura: Falta de cobertura 4G y FTTH en algunas poblaciones.
- Estabilidad: Posibles microcortes a la hora de priorizar el tráfico al cambiar de una línea a otra.
- Ancho de banda: Indisponibilidad del caudal en ciertos momentos al ser líneas compartidas.
- Dependencia de un único proveedor de acceso.
- Dependencia del proveedor de hardware y software de comunicaciones.
- Dependencia de los técnicos de las gerencias para la instalación del equipamiento.

Problemas de cobertura

Debido a que la extensión y dispersión de la comunidad es grande, esta no cuenta con buena cobertura de tecnologías como 4G ni como FTTH (Fiber To The Home) en muchos de los pueblos donde están ubicados los centros de Atención Primaria en el mundo rural. Este problema de falta de unas buenas infraestructuras de comunicaciones rurales no solamente le pasa a Castilla La Mancha, sino también a otras como Castilla y León o Asturias.

Además, dependemos del proveedor de comunicaciones, ya que no todos tienen la misma cobertura ni servicios, esto es un tema a tener en cuenta a la hora de los pliegos de contratación pública.

Estabilidad

El desconocimiento de estas herramientas en la gestión de nuestra infraestructura de comunicaciones y la experiencia que hemos adquirido en nuestras organizaciones a lo largo de años, nos lleva a pensar en que no es tan ideal la conmutación transparente cuando haya

cambios producidos por cambios en las políticas de enrutamiento debido a problemas en las líneas o por tráfico en las mismas.

Ancho de banda

La necesidad y dependencia cada día más de los sistemas informáticos para la labor diaria de los usuarios de nuestros sistemas, lleva aparejado una necesidad de usar más servicios y a una mejor necesidad.

Muchas de las soluciones de uso habitual, ya pasan de ser en modo on-premise al mundo de la cloud pública, por lo tanto, tenemos una necesidad de uso más intenso de internet. Este uso siempre lleva unos tiempos de respuesta mayores que en la red local o la WAN corporativa.

Desde el punto de visto teórico, SD-WAN llega para mitigar la optimización del ancho de banda, pero las necesidades de los usuarios crecen día y estamos limitados por los contratos con los proveedores, que no son nada flexibles y cualquier modificación va a suponer un gravemente mayor que lo acordado en la adjudicación del concurso.

Dependencia de un único proveedor de acceso

Debido a que los concursos públicos, aunque se dividan por lotes, la parte de comunicaciones sólo puede ser adjudicado a un proveedor esta situación además de depender únicamente de la infraestructura de ese proveedor, también tiene acarreado el problema de que las líneas de contingencia (backup) van a ser del mismo.

Debido a que la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 facilita la división por lotes. Pero a pesar de disponer la creación de un lote específico para las líneas de contingencia de nuestros sistemas informáticos, la ley indica siempre la libre concurrencia de las empresas y habría que justificar que este lote específico no se le diera al mismo proveedor. La administración debe ser siempre eficiente y austera, pero la Ley de Contratos del Sector Público nos permite en la contratación tener otros criterios y así podríamos adjudicar este lote de las comunicaciones de contingencia a otro proveedor. A su vez está adjudicación del lote debemos tener cuidado, ya que se enlaza con el problema de cobertura en las zonas rurales.

Dependencia del proveedor de hardware y software de comunicaciones

Una vez hemos elegido un proveedor y hemos definido nuestra infraestructura de SD-WAN con su solución, quedamos “atados” a él. Ya que el cambio de proveedor, no solamente implica un cambio en el software, que siempre es más asumible, sino también en el hardware.

A pesar de la existencia del estándar MEF 70, este solamente se refiere a una visión de alto nivel sin tener en cuenta la estandarización a nivel operativo. La falta de un estándar a nivel operativo, da lugar a la incompatibilidad y falta de heterogeneidad a nivel hardware de nuestras infraestructuras de comunicaciones. Lo cual nos lleva a la dependencia del proveedor y un cambio lleva aparejado un desembolso económico muy fuerte.

Conclusiones

A continuación, se describen los aspectos más relevantes que se consiguen con la solución SD-WAN:

Ahorro de costes

La ventaja más destacable que se puede extraer es la enorme reducción de costes que tendría esta solución, se puede observar del apartado coste de implantación, que, incluyendo los costes iniciales relacionados con equipamiento, servicios de ingeniería y formación ya existiría un ahorro considerable anualmente, más aún si vemos los costes a partir del 4º año, una vez pagados el equipamiento y servicios, el coste se reduciría a la mitad aproximadamente.

El pilotaje sería un factor clave a la hora de valorar cómo configurar la solución y por ende valorar la respuesta que tendría la definición de requisitos deseables.

Se ganarían prestaciones no disponibles hasta el momento como contemplar una capa de seguridad en dichos centros, priorización de tráfico de servicios o aplicaciones que se consideran más relevantes y por tanto con necesidad de reducción de tiempos de respuestas, aumento de ancho de banda, etc. Capacidad de gestionar todas las líneas de manera autónoma sin necesidad de contar con el operador, adecuando servicios en cada una de ellas según se considere, por ejemplo, ante una degradación de servicio o incluso una caída.

Una valoración más objetiva se podría realizar una vez se haya implantado la solución, realizando una recogida de datos de forma anual para considerar y evaluar la estabilidad tanto del servicio como de las líneas y confirmar o no si es posible prestar un servicio de conexión a red en centros sanitarios a través de líneas FTTH o no.

Robustez

La solución está diseñada para disponer de enlaces ascendentes redundantes, esto no garantiza una disponibilidad del 100% de los enlaces ascendentes. Para garantizar el funcionamiento del centro incluso sin enlace ascendente, la solución debe ser capaz de almacenar en caché las autenticaciones mientras el servidor RADIUS esté inalcanzable. Los controladores del centro necesitarán tener el certificado del servidor RADIUS precargado (para actuar en su lugar) y confiar en la CA corporativa.

Los switches Aruba admiten "Tunneled-Node", una función que permite al switch de acceso tunelizar todo el tráfico de un puerto o conjunto de puertos hacia el Gateway SD-WAN. Esto permite a un administrador configurar un conjunto común de políticas en un servidor ClearPass central y utilizar un único punto de aplicación de políticas, el Branch Gateway inspecciona todas las comunicaciones del centro, incluso cuando la comunicación se produce entre dispositivos de la misma subred.

La solución SD-WAN proporciona la capacidad de controlar qué aplicaciones y protocolos se pasan en función de la política. Del mismo modo, tiene la capacidad de determinar qué tráfico se envía a través de cada circuito WAN basado en una combinación de rol de usuario, aplicación, origen/destino, etc.

La solución SD-WAN supervisa el estado de todas las interfaces de enlace ascendente para garantizar el cumplimiento de los SLA configurados. El tráfico debe ser dirigido sin problemas a una interfaz compatible en caso de que no se cumpla.

Tras la degradación del circuito WAN, el tráfico se dirige en 10-12s. Aruba Central generará los eventos necesarios y el panel de control mostrará la información correspondiente.

Para evitar que determinados usuarios/aplicaciones acaparen todo el ancho de banda de la WAN, la solución SD-WAN proporciona mecanismos para aplicar cuotas de ancho de banda a esas aplicaciones/usuarios.

Las pasarelas SD-WAN limitarán el ancho de banda que puede consumir una determinada aplicación.

Los circuitos WAN públicos no suelen respetar las etiquetas DSCP, lo que reduce drásticamente el impacto de las políticas de marcado L3. La programación de la WAN debe aplicarse para asignar prioridad a las aplicaciones críticas para el negocio sobre las que no son tan importantes.

Para ello en un grupo determinado, hay que establecer primero la velocidad de la WAN en y luego aplicar el marcado QoS en Políticas.

De esta forma Las pasarelas SD-WAN priorizarán las aplicaciones críticas para el negocio sobre otras con menor prioridad.

Firewall de aplicación

La solución es capaz de proporcionar políticas de seguridad basadas en roles de una manera que se puede escalar fácilmente a cientos de lugares.

El tráfico se permite/se elimina según las políticas configuradas. Los registros pueden enviarse a través de Syslog directamente desde las puertas de enlace o desde la plataforma de gestión de la nube a través de las API de transmisión.

La solución Aruba SD-WAN puede aplicar políticas basadas en roles para limitar el alcance de lo que un usuario puede acceder. Cuando se integra con la infraestructura LAN/WLAN de Aruba, el tráfico del usuario puede ser tunelizado a la puerta de enlace para forzar que todo el tráfico pase primero por las políticas de los cortafuegos.

El tráfico intra-VLAN pasa por el cortafuegos, permitiendo la microsegmentación.

La infraestructura de la sucursal proporciona un filtrado de contenido basado en roles y reputación para los usuarios que se conectan a las redes de la sucursal sin necesidad de separarlos en diferentes VLAN.

El tráfico es permitido/borrado según las políticas configuradas. Los resultados se pueden ver en tiempo real a través de la página de monitorización. Los registros se envían a través de Syslog desde la Central a través de las APIs de streaming.

Las reglas estándar del firewall de seguridad basadas en las direcciones IP ya no son adecuadas. Es necesaria una protección que se aplique dinámicamente independientemente del rol del usuario, el tipo de dispositivo o la ubicación.

Está disponible una solución integral de control de acceso basada en roles, denominada Policy Enforcement Firewall (PEF), que ayuda específicamente a resolver este problema. Esta tecnología probada es el único cortafuegos centrado en el usuario y el dispositivo que proporciona un límite de "confianza cero" en el punto de acceso y lleva la designación Marsh Cyber Catalyst para reducir el riesgo.

Todas las puertas de enlace de Aruba incluyen el PEF, que es también la tecnología subyacente que permite la segmentación dinámica, una solución técnica clave que simplifica y asegura las redes cableadas e inalámbricas. Gracias a los controles de usuarios y aplicaciones, el departamento de TI puede eliminar la necesidad de añadir VLAN, SSID o ACL, lo que reduce drásticamente la complejidad. La función de visibilidad de las aplicaciones de PEF permite a los administradores de la red obtener una visión completa de las aplicaciones que se ejecutan en la red y de quién las utiliza.

El PEF stateful proporciona controles basados en el contexto para aplicar la seguridad y la priorización de la capa de aplicaciones. Es posible aplicar políticas de acceso a la red basadas en las funciones de los usuarios, los tipos de dispositivos, los flujos de aplicaciones, la

ubicación, etc. El PEF proporciona un conocimiento a nivel de usuario de todo el tráfico en la red. Esto elimina el coste y la complejidad asociados a la configuración manual de las VLAN estáticas, las listas de control de acceso y la infraestructura de conmutación por cable.

Visibilidad en la red

La solución también incluye Inspección Profunda de Paquetes (DPI) que proporciona visibilidad y control inteligente de las aplicaciones, la tecnología AppRF del PEF aprovecha la DPI para clasificar más de 3.200 aplicaciones y cuenta con un asistente de políticas para bloquear, priorizar y limitar el ancho de banda de cualquier aplicación o grupo de aplicaciones.

Junto con la función de cortafuegos con estado, existe la flexibilidad de separar cualquier tipo de flujo de tráfico. Con políticas contextuales basadas en identidades, dispositivos y ubicaciones. Los flujos de tráfico simplemente se adaptan al estado de movilidad del usuario y del dispositivo móvil, y la solución proporciona un conocimiento a nivel de usuario de todo el tráfico en la red. La solución admite varias categorías de usuarios en una única red, que abarca tanto la cableada como la inalámbrica. Durante el proceso de inicio de sesión en la red, se aprende la identidad y la función de cada usuario o dispositivo. Una vez que se determina el rol del usuario o dispositivo, se aplican políticas basadas en una serie de plantillas definidas por el administrador. Estas políticas siguen al usuario en toda la red y se aplican de manera uniforme en las conexiones inalámbricas y por cable.

Gestión y control del tráfico

PEF incluye controles que optimizan la utilización del tráfico. Las políticas basadas en roles pueden limitar la cantidad máxima de consumo de ancho de banda para un usuario o clase de usuarios en particular, y evita que los usuarios avanzados monopolicen los recursos de la red.

Detección y protección de intrusos

El Sistema de Detección y Prevención de Intrusiones (IDPS) supervisa, detecta y previene las amenazas para el tráfico entrante y saliente. El Sistema de Detección de Intrusiones (IDS) supervisa la red en busca de cualquier actividad maliciosa y genera eventos de amenaza. El Sistema de Prevención de Intrusiones (IPS) tiene todas las capacidades del IDS junto con la capacidad de prevenir intrusiones bloqueando el tráfico o descartando los paquetes de datos maliciosos. Los administradores tienen la opción de activar el IDS o el IPS.

El IDPS proporciona una capa extra de protección que analiza activamente la red y toma acciones sobre los flujos de tráfico basadas en reglas preconfiguradas. Estas acciones incluyen permitir el tráfico, enviar alertas a los administradores y descartar paquetes de datos maliciosos. Tiene la capacidad de analizar los paquetes de datos que entran en la red y actuar rápidamente para prevenir las amenazas en tiempo real. Todas las amenazas identificadas se registran para un análisis de correlación.

Los siguientes pasos describen el flujo de trabajo de Aruba IDPS para detectar y prevenir intrusiones:

- Descarga de conjuntos de reglas de amenazas.
- Habilitar Aruba IDPS.
- Transmitir Eventos en Tiempo Real.
- Enriquecer Eventos con detalles de cliente, red, aplicación y ubicación.
- Envía Alertas y Arroja Paquetes.
- Monitorizar amenazas.
- Compartir Datos de Amenazas con el servidor de Información de Seguridad y Gestión de Eventos (SIEM), si está configurado.

- IDS: El IDS monitoriza la red en busca de cualquier actividad maliciosa y genera una alerta. El IDS no toma ninguna acción sobre las amenazas identificadas. La configuración de IDS ayudará a detectar las amenazas y a capturar los detalles de las amenazas detectadas.

- IPS: El IPS supervisa la red en busca de actividad maliciosa, genera alertas y toma medidas basadas en una regla predefinida. La configuración del IPS ayudará a detectar las amenazas, crear alertas y eliminar los paquetes de las amenazas identificadas.

Hay políticas predefinidas que se pueden habilitar (y las reglas se pueden gestionar) para cada modo.

Además de las políticas de cortafuegos e IDPS que pueden configurarse, hay una serie de otras amenazas de denegación de servicio (DoS) para la detección del plano de control que pueden mitigarse con las capacidades avanzadas de limitación de velocidad de las pasarelas.

La seguridad es una parte integral de la solución Aruba SD-Branch. La seguridad de la solución Aruba SD-Branch se construye en capas, empezando por el endurecimiento del sistema operativo hasta la integración con otras soluciones de seguridad.

- Arranque seguro; imagen de software firmada por TPM. Fuerte restricción de las comunicaciones hasta que la pasarela haya recibido su configuración de Aruba Central.
- Aprovisionamiento seguro Zero Touch. Aprovechamiento del TPM cargado en las pasarelas Aruba para asegurar las comunicaciones con Aruba Central.
- Encriptación AES 256 para todos los túneles rama-hub.
- Aruba Role-based stateful firewall, con soporte para una configuración escalable utilizando alias de firewall y políticas basadas en roles.
- Módulo de Inspección Profunda de Paquetes con capacidad para identificar cerca de 3.200 aplicaciones.
- Filtrado de contenidos web y de reputación utilizando la tecnología de aprendizaje automático de WebRoot para clasificar el contenido, la reputación y la geolocalización de miles de millones de URL.
- Detección y prevención de intrusiones.

Integraciones

Por otro lado, la solución Aruba SD-Branch puede integrarse con ClearPass para formar una verdadera rama basada en políticas. Este modelo asigna dinámicamente políticas basadas en usuarios y dispositivos, en contraposición a la forma tradicional de asignar estas políticas manualmente basadas en puertos, VLANs y direcciones IP.

Por último, la solución Aruba SD-Branch puede integrarse con otras soluciones de seguridad. Con estas integraciones, la arquitectura de Aruba SD-Branch pretende ofrecer una protección avanzada contra amenazas de nivel empresarial de forma escalable. Con esto en mente, la integración con la oferta de Seguridad como Servicio de Zscaler proporciona una solución simple y escalable para la protección de amenazas avanzadas en redes de sedes remotas. Cabe destacar que Aruba también ofrece integración con la seguridad en la nube de Checkpoint, Symantec y Palo Alto (Firewalls perimetrales existentes en SESCAM).

Balanceo

Los Gateways admiten un modelo de despliegue de HA Activo-Standby y Activo-Activo.

En el modelo Activo- Standby, todos los enlaces ascendentes están conectados a cada puerta de enlace del centro, y sólo la puerta de enlace activa envía el tráfico a través de sus enlaces ascendentes conectados directamente.

En el modelo Activo-Activo, un conjunto diferente de enlaces ascendentes WAN puede terminar en cada una de las puertas de enlace de la sucursal. Las pasarelas descubrirán conjuntamente ambos enlaces WAN y establecerán túneles VPN a través de ambos enlaces ascendentes.

La redundancia de Aruba utiliza el Protocolo de Redundancia de Router Virtual (VRRP) en el lado LAN. El segundo GW será un standby para el GW primario.

Cuando el primario no está disponible, el standby se convierte en el primario y toma la propiedad de la dirección IP virtual.

Todos los clientes están configurados para acceder a la dirección IP virtual, proporcionando así una solución redundante transparente. Además, se puede habilitar el tanteo con un retardo de cero segundos para que el primario vuelva a estar en línea tan pronto como vuelva a estar disponible. El nivel de prioridad de la instancia VRRP se utiliza en el mecanismo de elección del maestro. El valor de prioridad más alto se convierte en el maestro VRRP. La implementación de VRRP también soporta el seguimiento de interfaces.

La consecuencia de tener VRRP en el lado LAN de los GWs es que mientras las interfaces orientadas a la LAN se comportarán de forma activa-backup, todas las interfaces WAN pueden estar activas al mismo tiempo. Esto permite que los GWs tengan todas las interfaces de enlace ascendente, así como los túneles de superposición, tanto en la pasarela maestra como en la de respaldo.

En el caso de una conmutación por error de GW, tener todas las interfaces de enlace ascendente y los túneles superpuestos ya configurados es una clara ventaja, ya que minimiza el tiempo de inactividad durante la conmutación por error. Sin embargo, dado que las pasarelas de rama anuncian sus subredes de rama a los concentradores como parte de la negociación de superposición, esto podría dar lugar a bucles de enrutamiento. Para evitar este problema potencial, los GWs suprimen automáticamente los anuncios de rutas para subredes para las que el estado VRRP no es maestro.

Gestión centralizada

Desde una única plataforma se puede gestionar la solución de forma global, consiguiendo mejorar la productividad de manera muy considerable haciendo que las tareas se desarrollen de forma más ágiles y rápidas, ganando en sencillez ante la búsqueda de equipos ,así como en la gestión de los mismos.

Igualmente se consigue ganar en seguridad al establecer de forma centralizada unos controles de acceso claros y contundentes.

La plataforma centralizada adquiere una mayor dimensión en la aplicación de políticas homogéneas y en las tareas de implantación, configuración, despliegue e incorporación de nuevos dispositivos gestionados en la presente solución.

Todas las ventajas de la gestión centralizada culminan en un ahorro de tiempos de operación y en definitiva de un ahorro de costes, son 2 ventajas que justifican enormemente la opción de disponer de una gestión centralizada de una solución o servicio desplegado en sedes remotas y distantes.

Esquema análisis DAFO

Interno	**Debilidades** Falta de estandarización operativa Desembolso por cambio de infraestructura	**Amenazas** Falta de cobertura en ciertas poblaciones Dependencia del proveedor Resistencia al cambio	**Externo**
	Fortalezas Gestión y control del tráfico unificado Ahorro de costes Robustez Seguridad e integración de soluciones	**Oportunidades** Reutilizar infraestructura existente en la organización Mejorar la experiencia del usuario Preparados para el cambio en la tecnología subyacente	

Referencias

Índice de gráficos y tablas

Gráficos

Tablas

Bibliografía

MEF Forum: SD-WAN Service Attributes and Services

https://www.mef.net/wp-content/uploads/2019/07/MEF-70.pdf

Cisco SD-WAN: Cloud scale architecture

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf

Kevin Marshall, Andrew Tanguay: SD-Branch Fundamentals Guide

https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/B3931382-CE7C-43F0-A140-536E907E1582-14-SD-Branch%20Fundamentals%20Guide%20-%20Final%20-%20Fulldoc.pdf

Fortinet: The Network Leader's Guide to Secure SD-WAN

https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-network-leaders-guide-to-SD-WAN.pdf

Webgrafía

- CCN-CERT. Centro Criptológico Nacional

  https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/

- Metro Ethernet Forum MEF

  https://www.mef.net

- flexiWAN

  Web del proyecto

  https://flexiwan.com

Web de documentación

https://docs.flexiwan.com

Soluciones y productos CISCO

Web de productos SD-WAN

https://www.cisco.com/c/es_es/solutions/enterprise-networks/sd-wan/index.html.

Soluciones y productos de ARUBA

https://www.arubanetworks.com/es/productos/sd-wan/.

Soluciones y productos de Fortinet

https://www.fortinet.com/lat/products/sd-wan.

https://docs.fortinet.com/sdwan.

Información de Castilla-La Mancha.

https://www.castillalamancha.es/

https://www.castillalamancha.es/clm/unlugarparavivir

Información del INE:

http://www.ies.jccm.es/

Información de los servicios sanitarios:

https://sanidad.castillalamancha.es/ciudadanos/servicios-sanitarios

Mapa de áreas de salud de Castilla-La Mancha:

https://www.castillalamancha.es/gobierno/sanidad/estructura/dgspoeis/actuaciones/mapa-sanitario

https://www.castillalamancha.es/sites/default/files/documentos/pdf/20210205/mapa_principal_pequeno.pdf

Distritos de Salud de Castilla-La Mancha:

https://www.castillalamancha.es/sites/default/files/documentos/pdf/20210205/0_distritos_clm.pdf

Gerencias de Atención Integrada de Castilla-La Mancha:

https://www.castillalamancha.es/sites/default/files/documentos/pdf/20210205/gai_clm.pdf

Centros de Especialidades de Diagnóstico y Tratamiento de Castilla-La Mancha:

https://www.castillalamancha.es/sites/default/files/documentos/pdf/20210205/cedt_clm.pdf

Red Sanitaria de Castilla-La Mancha:

https://sanidad.castillalamancha.es/files/documentos/pdf/20131115/red_sanitaria_clm.pdf

Mapa Sanitario de Castilla-La Mancha:

https://castillalamancha.maps.arcgis.com/apps/webappviewer/index.html?id=d3105e9b924245b39efd8fb3ae30eab7

ANEXO 1: Infraestructura Centros de Atención Primaria

Provincia	Centro	Tipo	Ancho de banda
Albacete	CHINCHILLA	ADSL VPN-IP	20Mbps
Albacete	ALCADOZO	ADSL VPN-IP	4Mbps
Albacete	ALCARAZ	ADSL VPN-IP	10Mbps
Albacete	ALMANSA	ADSL VPN-IP	4Mbps
Albacete	BALAZOTE	ADSL VPN-IP	4Mbps
Albacete	BOGARRA	ADSL VPN-IP	8Mbps
Albacete	BONETE	ADSL VPN-IP	10Mbps
Albacete	CASAS DE JUAN NÚÑEZ	ADSL VPN-IP	4Mbps
Albacete	CAUDETE	ADSL VPN-IP	10Mbps
Albacete	EL BONILLO	ADSL VPN-IP	10Mbps
Albacete	ELCHE DE LA SIERRA	ADSL VPN-IP	10Mbps
Albacete	HELLIN I	ADSL VPN-IP	4Mbps
Albacete	LA RODA	ADSL VPN-IP	4Mbps
Albacete	MADRIGUERAS	ADSL VPN-IP	10Mbps
Albacete	MUNERA	ADSL VPN-IP	4Mbps
Albacete	NERPIO	ADSL VPN-IP	10Mbps
Albacete	ONTUR	ADSL VPN-IP	4Mbps
Albacete	OSSA DE MONTIEL	ADSL VPN-IP	4Mbps

Albacete	RIOPAR	ADSL VPN-IP	10Mbps
Albacete	SOCOVOS	ADSL VPN-IP	4Mbps
Albacete	TARAZONA DE LA MANCHA	ADSL VPN-IP	4Mbps
Albacete	TOBARRA	ADSL VPN-IP	4Mbps
Albacete	VILLARROBLEDO	ADSL VPN-IP	4Mbps
Albacete	YESTE	ADSL VPN-IP	10Mbps
Albacete	Albacete ZONA 2	ADSL VPN-IP	10Mbps
Albacete	Albacete ZONA 3	ADSL VPN-IP	10Mbps
Albacete	Albacete ZONA 4	ADSL VPN-IP	10Mbps
Albacete	Albacete ZONA 6	ADSL VPN-IP	10Mbps
Albacete	Albacete ZONA 7	ADSL VPN-IP	4Mbps
Albacete	VILLAMALEA	ADSL VPN-IP	10Mbps
Albacete	CASAS IBÁÑEZ	ADSL VPN-IP	4Mbps
Albacete	HELLIN II	ADSL VPN-IP	4Mbps
Albacete	Albacete ZONA 8	ADSL VPN-IP	4Mbps
Ciudad Real	PUERTOLLANO IV	ADSL VPN-IP	4Mbps
Ciudad Real	ALMODÓVAR DEL CAMPO	ADSL VPN-IP	4Mbps
Ciudad Real	ARGAMASILLA DE CALATRAVA	ADSL VPN-IP	10Mbps
Ciudad Real	FUENCALIENTE	ADSL VPN-IP	4Mbps
Ciudad Real	PUERTOLLANO II	ADSL VPN-IP	4Mbps
Ciudad Real	PUERTOLLANO III - Carlos Mestre	ADSL VPN-IP	4Mbps

Ciudad Real	SOLANA DEL PINO	ADSL VPN-IP	10Mbps
Ciudad Real	ABENÓJAR	ADSL VPN-IP	10Mbps
Ciudad Real	ALBALADEJO	ADSL VPN-IP	2Mbps
Ciudad Real	ALCOBA DE LOS MONTES	ADSL VPN-IP	10Mbps
Ciudad Real	ALMAGRO	ADSL VPN-IP	4Mbps
Ciudad Real	BOLAÑOS DE CALATRAVA	ADSL VPN-IP	10Mbps
Ciudad Real	CALZADA DE CALATRAVA	ADSL VPN-IP	4Mbps
Ciudad Real	CARRIÓN DE CALATRAVA	ADSL VPN-IP	10Mbps
Ciudad Real	CIUDAD REAL 2	ADSL VPN-IP	4Mbps
Ciudad Real	CORRAL DE CALATRAVA	ADSL VPN-IP	20Mbps
Ciudad Real	DAIMIEL	ADSL VPN-IP	4Mbps
Ciudad Real	LA SOLANA	ADSL VPN-IP	2Mbps
Ciudad Real	MALAGÓN	ADSL VPN-IP	4Mbps
Ciudad Real	MANZANARES II	ADSL VPN-IP	8Mbps
Ciudad Real	MIGUELTURRA	ADSL VPN-IP	4Mbps
Ciudad Real	MORAL DE CALATRAVA	ADSL VPN-IP	20Mbps
Ciudad Real	RETUERTA DEL BULLAQUE	ADSL VPN-IP	10Mbps
Ciudad Real	SANTA CRUZ DE MUDELA	ADSL VPN-IP	4Mbps
Ciudad Real	VALDEPEÑAS 1	ADSL VPN-IP	4Mbps
Ciudad Real	VILLAFRANCA CABALLEROS	ADSL VPN-IP	4Mbps
Ciudad Real	VILLAHERMOSA	ADSL VPN-IP	4Mbps

Ciudad Real	VILLARRUBIA DE LOS OJOS	ADSL VPN-IP	10Mbps
Ciudad Real	CAMPO DE CRIPTANA	ADSL VPN-IP	4Mbps
Ciudad Real	HERENCIA	ADSL VPN-IP	8Mbps
Ciudad Real	PEDRO MUÑOZ	ADSL VPN-IP	4Mbps
Ciudad Real	SOCUÉLLAMOS	ADSL VPN-IP	8Mbps
Ciudad Real	TOMELLOSO I	ADSL VPN-IP	4Mbps
Ciudad Real	TOMELLOSO II	ADSL VPN-IP	8Mbps
Ciudad Real	VILLARTA DE SAN JUAN	ADSL VPN-IP	10Mbps
Ciudad Real	VALDEPEÑAS II	ADSL VPN-IP	4Mbps
Ciudad Real	ARGAMASILLA DE ALBA	ADSL VPN-IP	8Mbps
Ciudad Real	PORZUNA	ADSL VPN-IP	4Mbps
Ciudad Real	MANZANARES I	ADSL VPN-IP	4Mbps
Ciudad Real	TORRE DE JUAN ABAD	ADSL VPN-IP	10Mbps
Ciudad Real	PIEDRABUENA	ADSL VPN-IP	4Mbps
Ciudad Real	ALCÁZAR DE SAN JUAN II	ADSL VPN-IP	10Mbps
Cuenca	CUENCA 1	ADSL VPN-IP	10Mbps
Cuenca	BELMONTE	ADSL VPN-IP	4Mbps
Cuenca	BETETA	ADSL VPN-IP	6Mbps
Cuenca	CARRASCOSA DEL CAMPO	ADSL VPN-IP	1Mbps
Cuenca	CAÑAVERAS	ADSL VPN-IP	20Mbps
Cuenca	CAÑETE	ADSL VPN-IP	4Mbps

Cuenca	CARBONERAS DE GUADAZAÓN	ADSL VPN-IP	10Mbps
Cuenca	CARDENETE	ADSL VPN-IP	4Mbps
Cuenca	CUENCA 2	ADSL VPN-IP	4Mbps
Cuenca	HONRUBIA	ADSL VPN-IP	10Mbps
Cuenca	HORCAJO DE SANTIAGO	ADSL VPN-IP	20Mbps
Cuenca	HUETE	ADSL VPN-IP	10Mbps
Cuenca	INIESTA	ADSL VPN-IP	10Mbps
Cuenca	LANDETE	ADSL VPN-IP	10Mbps
Cuenca	LAS PEDROÑERAS	ADSL VPN-IP	4Mbps
Cuenca	MINGLANILLA	ADSL VPN-IP	4Mbps
Cuenca	MIRA	ADSL VPN-IP	20Mbps
Cuenca	MONTALBO	ADSL VPN-IP	4Mbps
Cuenca	MOTA DEL CUERVO	ADSL VPN-IP	4Mbps
Cuenca	Motilla del Palancar	ADSL VPN-IP	20Mbps
Cuenca	PRIEGO	ADSL VPN-IP	4Mbps
Cuenca	QUINTANAR DEL REY	ADSL VPN-IP	10Mbps
Cuenca	SAN CLEMENTE	ADSL VPN-IP	10Mbps
Cuenca	SAN LORENZO PARRILLA	ADSL VPN-IP	10Mbps
Cuenca	SISANTE	ADSL VPN-IP	10Mbps
Cuenca	TALAYUELAS	ADSL VPN-IP	20Mbps
Cuenca	TORREJONCILLO REY	ADSL VPN-IP	10Mbps

Cuenca	TRAGACETE	ADSL VPN-IP	20Mbps
Cuenca	VILLALBA DEL REY	ADSL VPN-IP	20Mbps
Cuenca	VILLAMAYOR SANTIAGO	ADSL VPN-IP	10Mbps
Cuenca	VILLARES DEL SAZ	ADSL VPN-IP	20Mbps
Cuenca	VILLAS DE LA VENTOSA	ADSL VPN-IP	20Mbps
Cuenca	CAMPILLO DE ALTOBUEY	ADSL VPN-IP	4Mbps
Cuenca	CASASIMARRO	ADSL VPN-IP	-
Guadalajara	ALCOLEA DEL PINAR	ADSL VPN-IP	6Mbps
Guadalajara	ATIENZA	ADSL VPN-IP	6Mbps
Guadalajara	GUADALAJARA 2 - BALCONCILLO	ADSL VPN-IP	4Mbps
Guadalajara	BRIHUEGA	ADSL VPN-IP	4Mbps
Guadalajara	CIFUENTES	ADSL VPN-IP	20Mbps
Guadalajara	COGOLLUDO	ADSL VPN-IP	10Mbps
Guadalajara	GUADALAJARA 4 - CERVANTES	ADSL VPN-IP	4Mbps
Guadalajara	EL POBO	ADSL VPN-IP	4Mbps
Guadalajara	GUADALAJARA 3 - ALAMIN	ADSL VPN-IP	8Mbps
Guadalajara	CHECA	ADSL VPN-IP	6Mbps
Guadalajara	HIENDELAENCINA	ADSL VPN-IP	20Mbps
Guadalajara	HORCHE	ADSL VPN-IP	10Mbps
Guadalajara	JADRAQUE	ADSL VPN-IP	4Mbps
Guadalajara	MARANCHÓN	ADSL VPN-IP	10Mbps

Guadalajara	MOLINA DE ARAGÓN	ADSL VPN-IP	4Mbps
Guadalajara	MONDEJAR	ADSL VPN-IP	10Mbps
Guadalajara	PASTRANA	ADSL VPN-IP	4Mbps
Guadalajara	SACEDÓN	ADSL VPN-IP	4Mbps
Guadalajara	SIGÜENZA	ADSL VPN-IP	8Mbps
Guadalajara	VILLANUEVA DE ALCORÓN	ADSL VPN-IP	10Mbps
Guadalajara	YUNQUERA DE HENARES	ADSL VPN-IP	4Mbps
Guadalajara	CABANILLAS DEL CAMPO	ADSL VPN-IP	4Mbps
Guadalajara	GUADALAJARA 5 - MANANTIALES,LOS	ADSL VPN-IP	4Mbps
Puertollano	AGUDO	ADSL VPN-IP	20Mbps
Toledo	TOLEDO 5 - BUENAVISTA	ADSL VPN-IP	2Mbps
Toledo	AÑOVER DE TAJO	ADSL VPN-IP	10Mbps
Toledo	BARGAS	ADSL VPN-IP	4Mbps
Toledo	CAMARENA	ADSL VPN-IP	4Mbps
Toledo	CONSUEGRA	ADSL VPN-IP	20Mbps
Toledo	CORRAL DE ALMAGUER	ADSL VPN-IP	4Mbps
Toledo	ESCALONA	ADSL VPN-IP	10Mbps
Toledo	ESQUIVIAS	ADSL VPN-IP	20Mbps
Toledo	FUENSALIDA	ADSL VPN-IP	4Mbps
Toledo	LOS NAVALMORALES	ADSL VPN-IP	4Mbps
Toledo	MADRIDEJOS	ADSL VPN-IP	4Mbps

Toledo	MENASALBAS	ADSL VPN-IP	10Mbps
Toledo	MOCEJÓN	ADSL VPN-IP	4Mbps
Toledo	MORA	ADSL VPN-IP	4Mbps
Toledo	NAVAHERMOSA	ADSL VPN-IP	4Mbps
Toledo	NOBLEJAS	ADSL VPN-IP	4Mbps
Toledo	PUEBLA DE MONTALBÁN,LA	ADSL VPN-IP	10Mbps
Toledo	QUINTANAR DE LA ORDEN	ADSL VPN-IP	8Mbps
Toledo	SANTA CRUZ DE LA ZARZA	ADSL VPN-IP	4Mbps
Toledo	SANTA OLALLA	ADSL VPN-IP	4Mbps
Toledo	SONSECA	ADSL VPN-IP	8Mbps
Toledo	TEMBLEQUE	ADSL VPN-IP	4Mbps
Toledo	TOLEDO1-SILLERIA	ADSL VPN-IP	4Mbps
Toledo	TOLEDO3-BENQUERENCIA	ADSL VPN-IP	20Mbps
Toledo	TOLEDO4-SANTA BARBARA	ADSL VPN-IP	2Mbps
Toledo	VALMOJADO	ADSL VPN-IP	10Mbps
Toledo	VILLACAÑAS	ADSL VPN-IP	4Mbps
Toledo	YEPES	ADSL VPN-IP	10Mbps
Toledo	SESEÑA VIEJO	ADSL VPN-IP	10Mbps
Toledo	ALDEANUEVA DE S.BARTOLOME	ADSL VPN-IP	10Mbps
Toledo	BELVIS DE LA JARA	ADSL VPN-IP	4Mbps
Toledo	CEBOLLA	ADSL VPN-IP	4Mbps

Toledo	LA PUEBLANUEVA	ADSL VPN-IP	20Mbps
Toledo	NAVA DE RICOMALILLO	ADSL VPN-IP	4Mbps
Toledo	NAVAMORCUENDE	ADSL VPN-IP	20Mbps
Toledo	OROPESA	ADSL VPN-IP	4Mbps
Toledo	PUENTE DEL ARZOBISPO	ADSL VPN-IP	10Mbps
Toledo	TALAVERA2-ESTACION	ADSL VPN-IP	4Mbps
Toledo	TALAVERA4-LA ALGODONERA	ADSL VPN-IP	4Mbps
Toledo	VELADA	ADSL VPN-IP	20Mbps
Toledo	OLIAS DEL REY II - LOS OLIVOS	ADSL VPN-IP	4Mbps
Toledo	POLAN	ADSL VPN-IP	8Mbps
Toledo	SIERRA SAN VICENTE (Castillo de Bayuela)	ADSL VPN-IP	4Mbps

ANEXO 2: Equipamiento SD-WAN

ARUBA

Serie 7000

https://www.arubanetworks.com/assets/_es/ds/DS_7200Series.pdf.

Serie 9000

https://www.arubanetworks.com/assets/ds/DS_9000Series.pdf.

ARUBA Central

https://www.arubanetworks.com/assets/_es/ds/DS_ArubaCentral.pdf.

ClearPass Policy Management

https://www.arubanetworks.com/assets/_es/ds/DS_ClearPass_PolicyManager.pdf.

CISCO

SD-WAN vEdge Routers

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-07-vedge-routers-data-sheet-cte-en.html.

Meraki Switches

https://meraki.cisco.com/products/switches/.

Fortinet

Productos SD WAN

https://www.fortinet.com/products/product-compare?cat=sdwan.

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet_secure_sdwan.pdf.

Solution 360 Protection Bundle

https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-360-protection-bundle.pdf.

Firmado por ALEJANDRO FERNANDEZ PRENDES - ***6634** el día 09/10/2021 19:22:01 con un certificado emitido por AC CAMERFIRMA FOR NATURAL PERSONS - 2016