



# ¿Qué es SD-WAN? La solución de Red Definida por Software

Comunidad de Cisco

Eric García Guzmán - Escalation Engineer  
Ian Estrada Lagunas - Escalation Engineer

Jueves 24 de agosto de 2023



# Conecte, Interactúe, ¡Colabore!

## Soluciones

¡Acepte las soluciones correctas y felicite a quienes le ayudaron! Los foros de discusión tienen muchas entradas, de las cuales no todas cuentan con una respuesta correcta o válida.

Ayude a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución”.

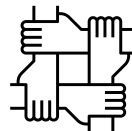
Aceptar como solución

## Agradecimientos

¡Resalte el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndonos la oportunidad de ganar premios además de ser una muestra valiosa de ¡nuestro reconocimiento!

o Útil



© 2023 Cisco and/or its affiliates. All rights reserved.

Cisco Public

# Spotlight Awards

¡Nuevos ganadores cada mes!

Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros. Los Premios Spotlight se otorgan mensualmente para destacar a los miembros más destacados.

¡Ahora también puedes nominar a un candidato! [Haga clic aquí](#)



# Eric García



## Escalation Engineer

Ingeniero en Computación con especialidad en Redes Computacionales por la FES Aragón de la Universidad Nacional Autónoma de México (UNAM). Se unió a Cisco en 2016 y tiene más de cuatro años de experiencia en Arquitectura de Sistemas Operativos dentro del Centro de Asistencia Técnica (TAC) de Cisco y tres años en SD-WAN. Eric ha creado documentación SD-WAN pública para cisco.com y asesorado a ingenieros dentro de TAC. Actualmente es ingeniero de escalamiento para TAC SD-WAN.

# Ian Estrada

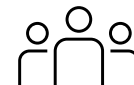


## Technical Consulting Engineer

Ingeniero en Telecomunicaciones, Sistemas y Electrónica egresado de la UNAM. Ingresó al programa de incubadoras de Cisco Academy en 2019 y luego se unió al equipo de TAC para la tecnología SD-WAN. Ian cuenta actualmente con cuatro años de experiencia en esta tecnología y se desempeña como ingeniero de escalación en SD-WAN. Ha creado documentación y videos públicos de SD-WAN para Cisco.

Descargue la  
presentación

<https://bit.ly/CL2doc-aug23>



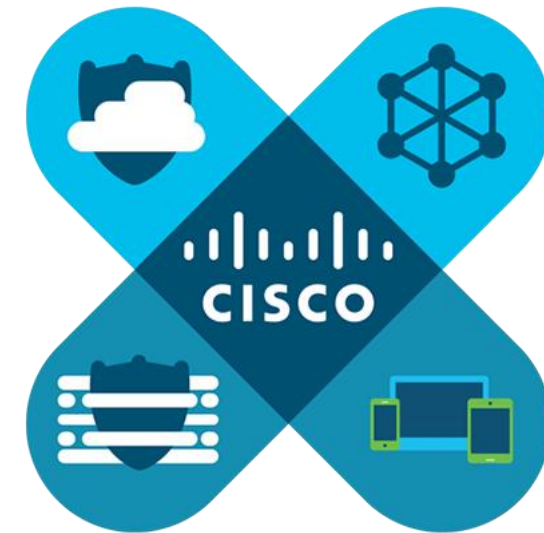
Join at  
**slido.com**  
**#2620 104**

 Passcode: **46riiy**



# Agenda

1. ¿Qué es una red de computadoras?
2. ¿Qué es Software-Defined Networking (SDN)?
3. ¿Qué es SD-WAN?
4. Componentes de la solución SD-WAN.
5. Túneles de Control y de Datos
6. ¿Cómo identifico un router en modo SD-WAN?
7. Laboratorio
8. Integraciones



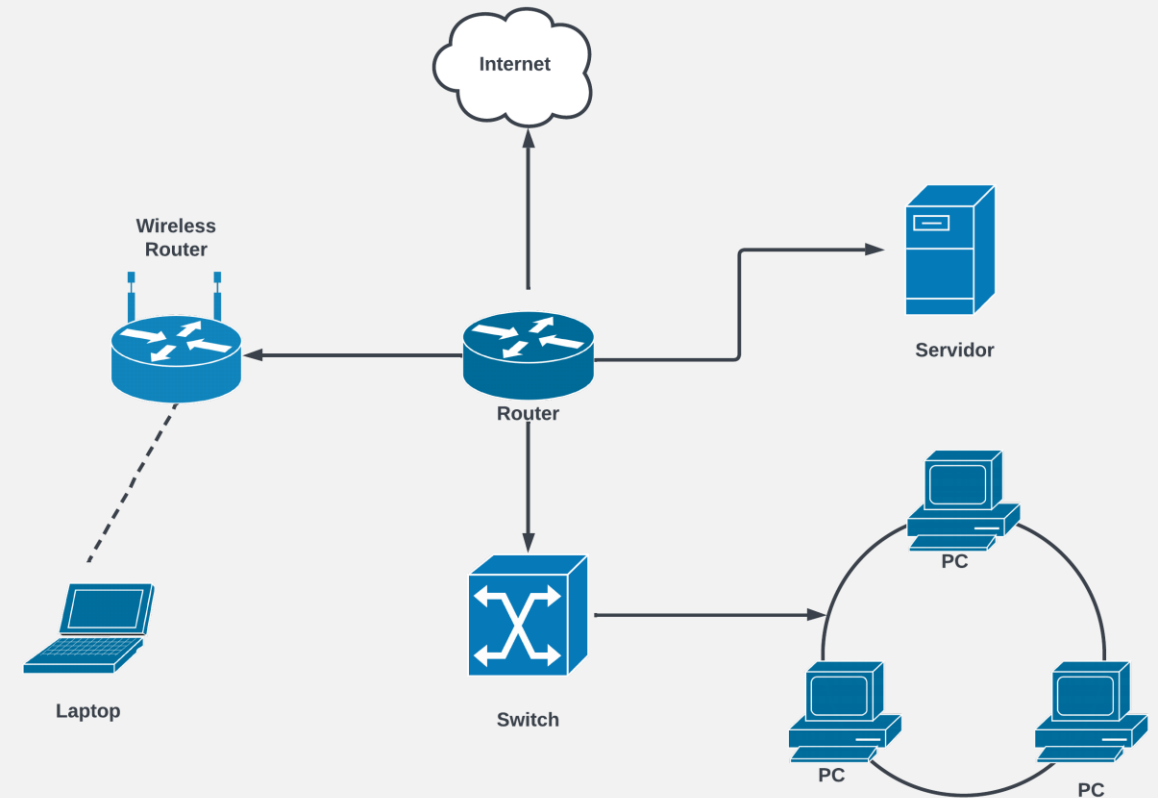
# 1. ¿Qué es es una red de computadoras?

# Red de computadoras tradicional

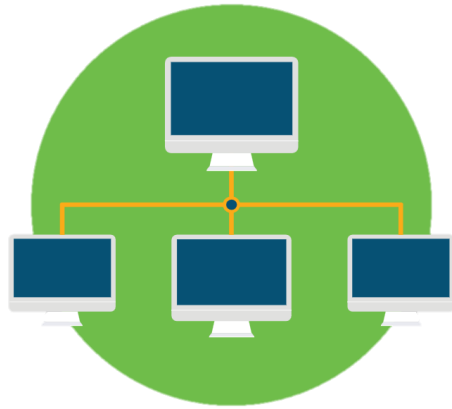
Es la interconexión física o inalámbrica que vincula varios dispositivos informáticos:

- Servidores
- Computadoras
- Teléfonos móviles
- Periféricos
- Entre otros

para que se comuniquen entre sí, con la finalidad de compartir datos y ofrecer servicios.



# Red de computadora tradicional



Una LAN o Red de Área Local, conecta equipos informáticos ubicados en un área geográfica reducida, como un edificio o una habitación.



Una WAN o Red de Área Amplia, es un conjunto de redes LAN que conecta equipos informáticos que se encuentran en diferentes ubicaciones físicas.



## 2. ¿Qué es Software-Defined Networking (SDN)?



# Software-Defined Networking (SDN)

Una red definida por software (SDN) es una arquitectura diseñada para hacer una red más flexible y fácil de administrar.



SDN centraliza la administración abstrayendo el plano de control del plano de envío de datos.

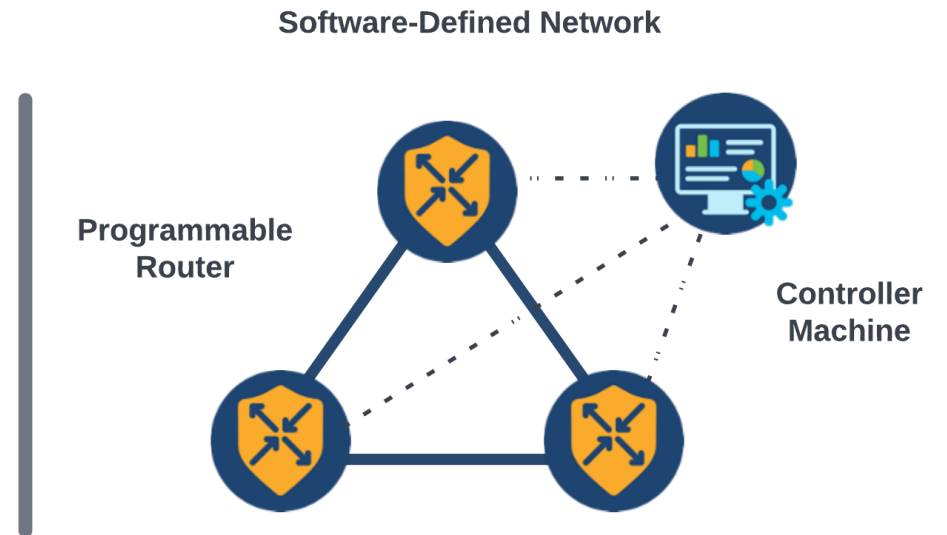
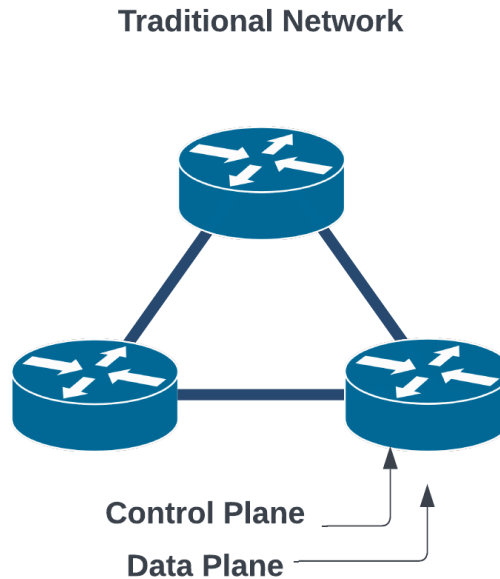
Software: Control

Hardware: Datos

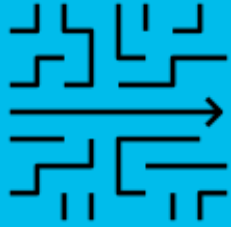
# Elementos de una Red Definida por Software (SDN)

Una arquitectura SDN ofrece una red centralizada y programable donde el control se desvincula totalmente del hardware.

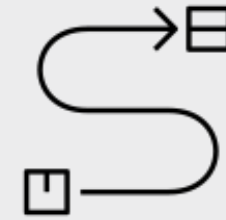
- Un controlador
- Separación de planos de control
- Administración centralizada
- Visibilidad



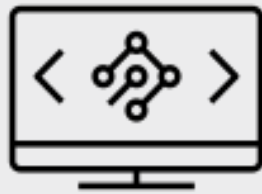
Simplifica  
las operaciones



Logra una rápida  
solución de problemas



Mejora la seguridad



Transforma  
la infraestructura



## 2.1 Redes antes de SDN. Caso de uso.



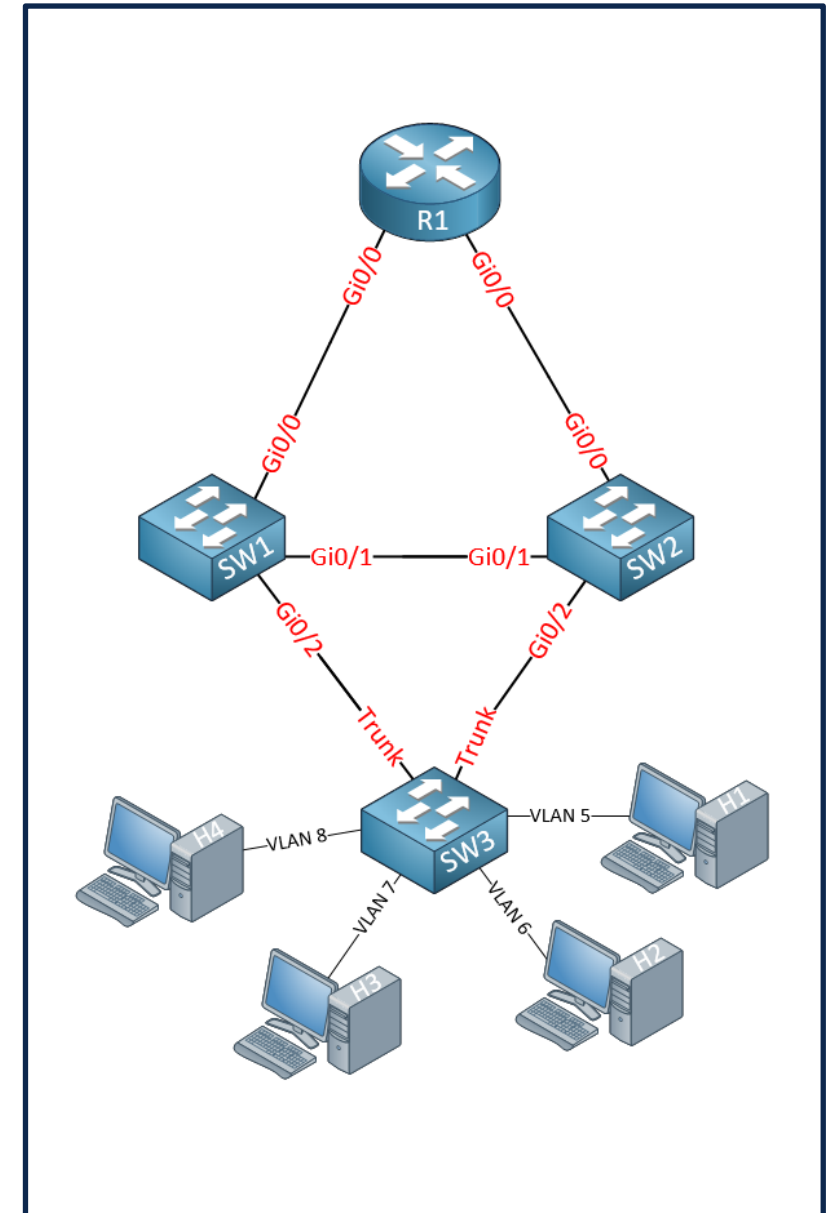
# Red Hospitales en Brasil

- Cadena de hospitales en Brasil
- 55 clínicas fijas
- 4 hospitales principales
- 25 clínicas móviles
- 90 ambulancias
- Nuevas sucursales en implementación



# Estado Actual de la Red

- Red legacy, routers Cisco ISR G2 3900, 2900
- Switches Cisco 3650, 2960
- Transporte MPLS, E1
- Monitoreo SNMP
- Configuración e implementaciones manuales
- No redundancia
- No experiencia de aplicativos
- No ruteo basado en SLA
- No programabilidad (APIs)
- Mano de obra manual



## 2.2 Underlay vs Overlay





# Underlay vs Overlay: Características y Relación

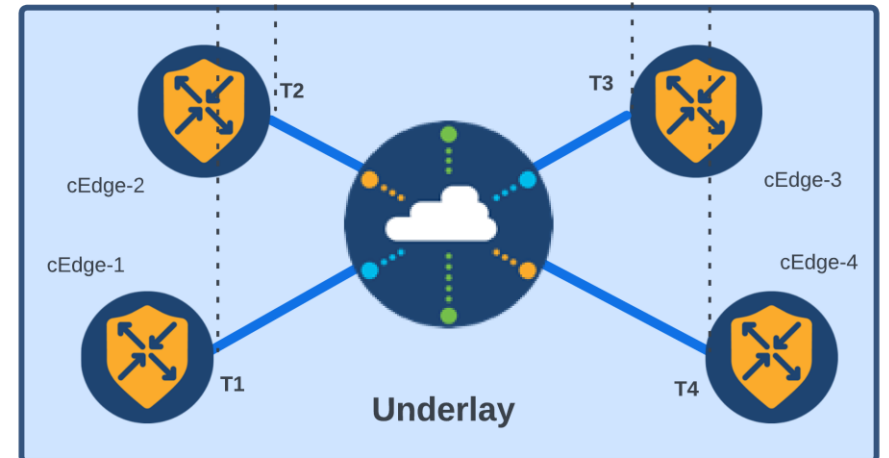
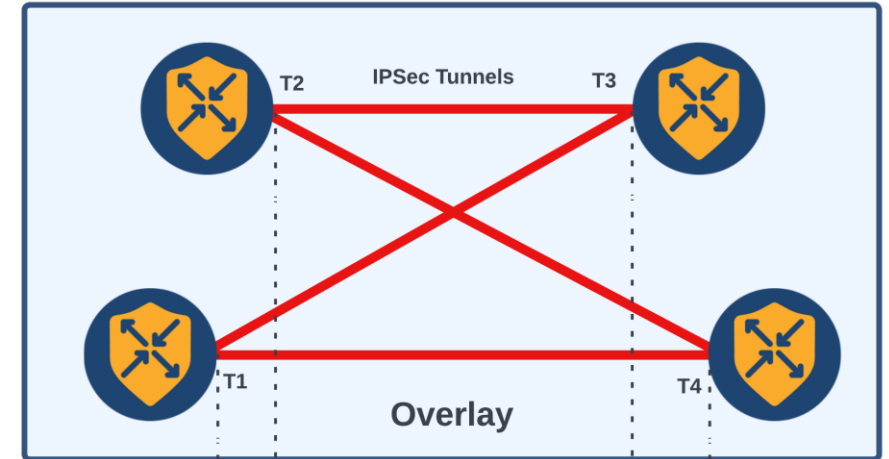
## Overlay

- El **overlay** es la topología lógica que recorre sobre la red underlay, formando la denominada Infraestructura de SD-WAN. Conformado por túneles IPsec o GRE.

---

## Underlay

- El **underlay** es la base de la infraestructura real que realiza el enrutamiento para interconectar sitios en la WAN. También conocido como Proveedor de Servicios de Internet (ISP).



### 3. ¿Qué es SD-WAN?





Join at  
**slido.com**  
**#2620 104**

🔍 Passcode:  
**46riiy**

## ¿Has escuchado hablar de SD-WAN? ¿Qué conocías de SD-WAN?

A) Conocimiento teórico

0%

B) Conocimiento básico, en búsqueda de expandir el conocimiento.

0%

C) Conocimiento general, en búsqueda de profundizar en la solución.

0%

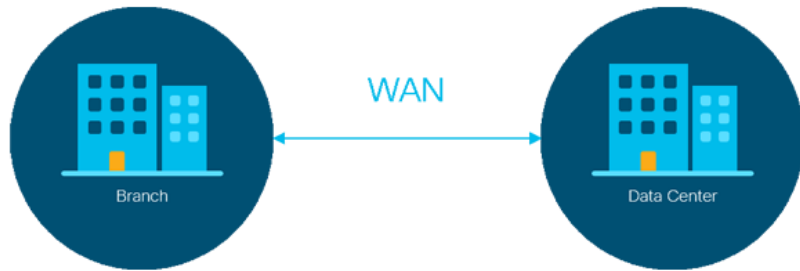
D) Conozco bien la solución, busco actualizarme.

0%

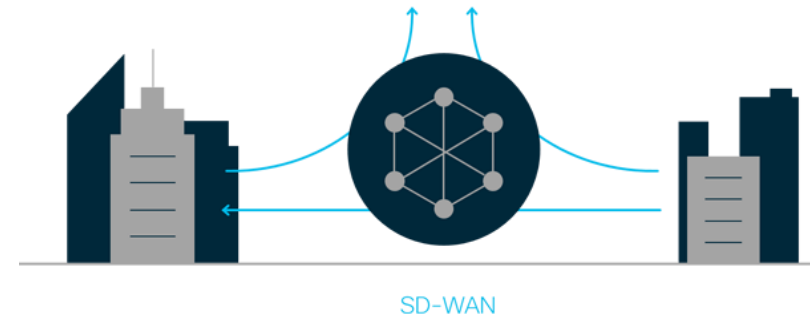
E) Lo desconozco. Busco expandir mis horizontes en esta solución

0%

# Red de Área Amplia Definida por Software



La **WAN tradicional** conectaba a usuarios de sucursales o campus con aplicaciones ubicadas en servidores del centro de datos.



**SD-WAN** es una WAN definida por software.

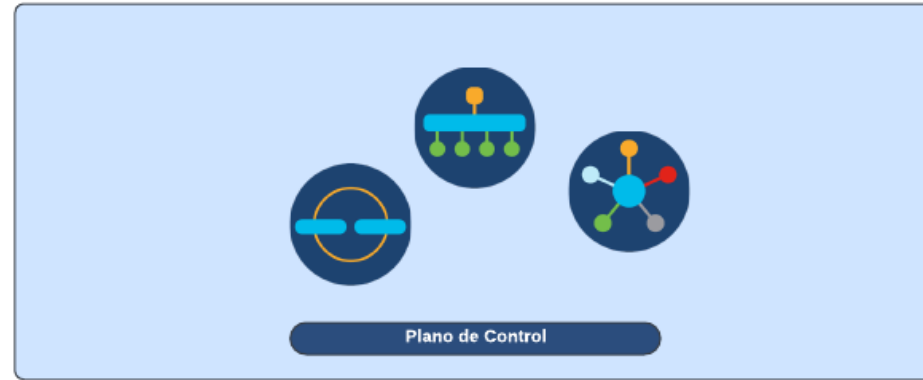
Ésta permite reducir costos, simplificar la administración, reforzar la seguridad y mejorar la experiencia de los usuarios.

# 3.1 Plano de Control y Plano de Datos

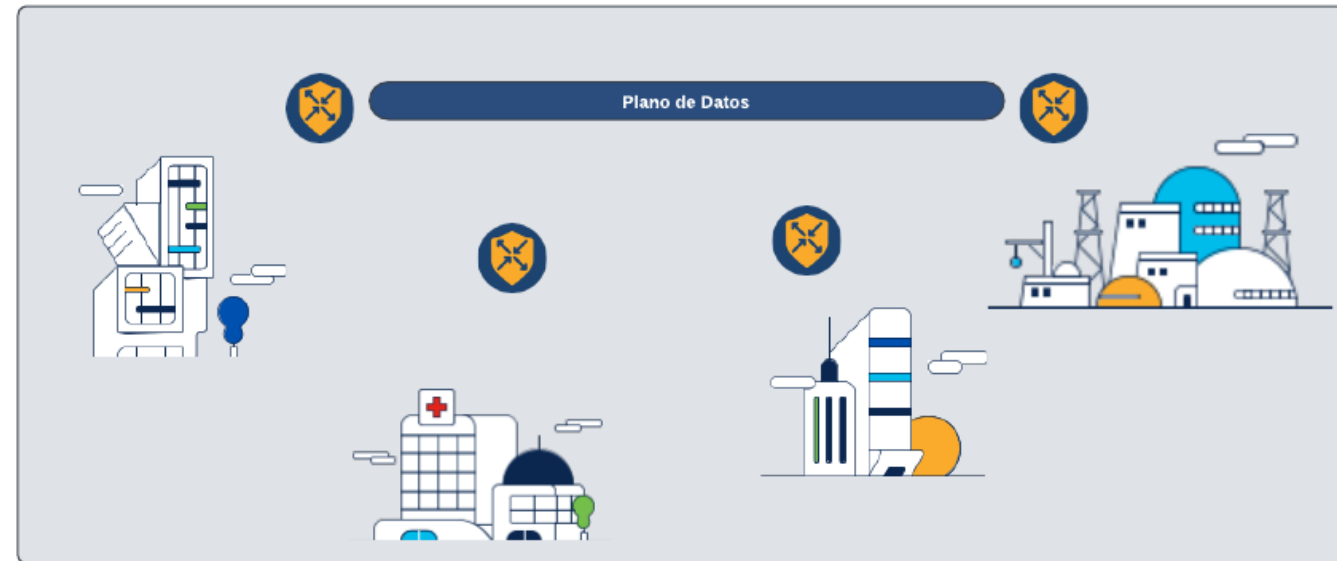


# Elementos del Plano de Control y Plano de Datos

Controladores virtuales



Routers físicos  
o  
virtuales

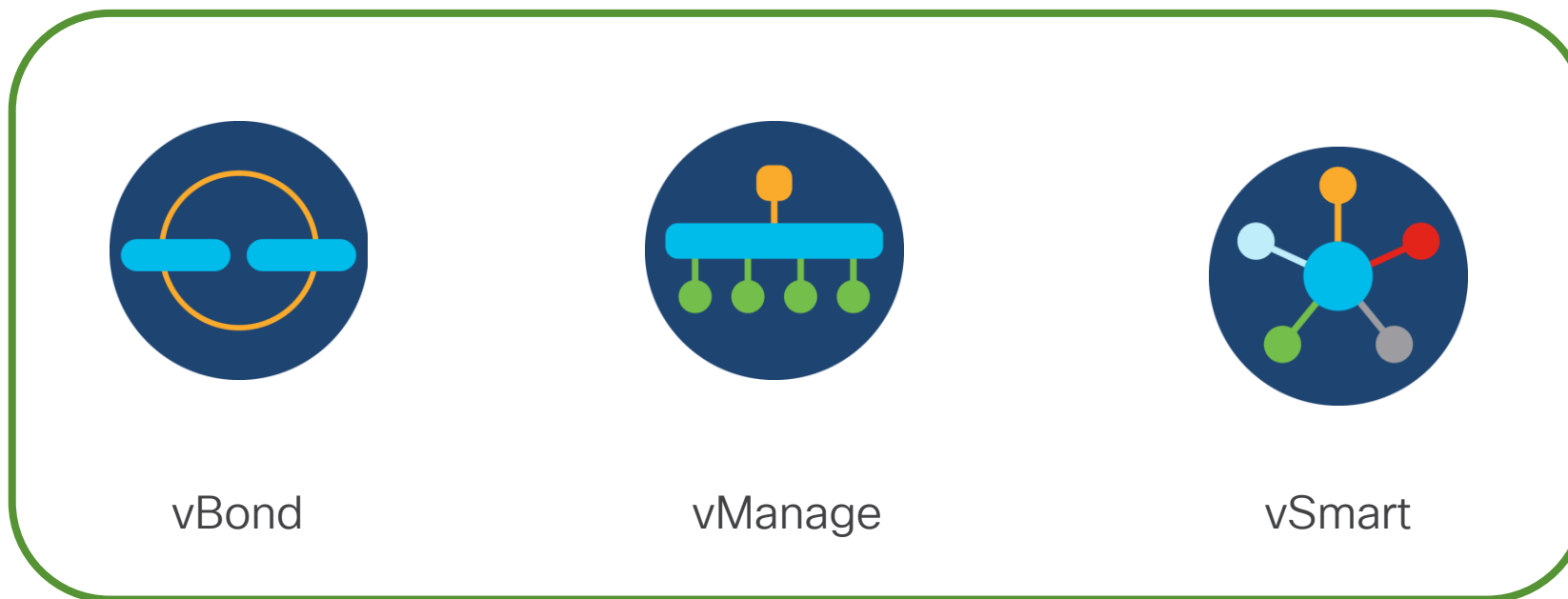


## 4. Componentes de la solución SD-WAN



# Controladores

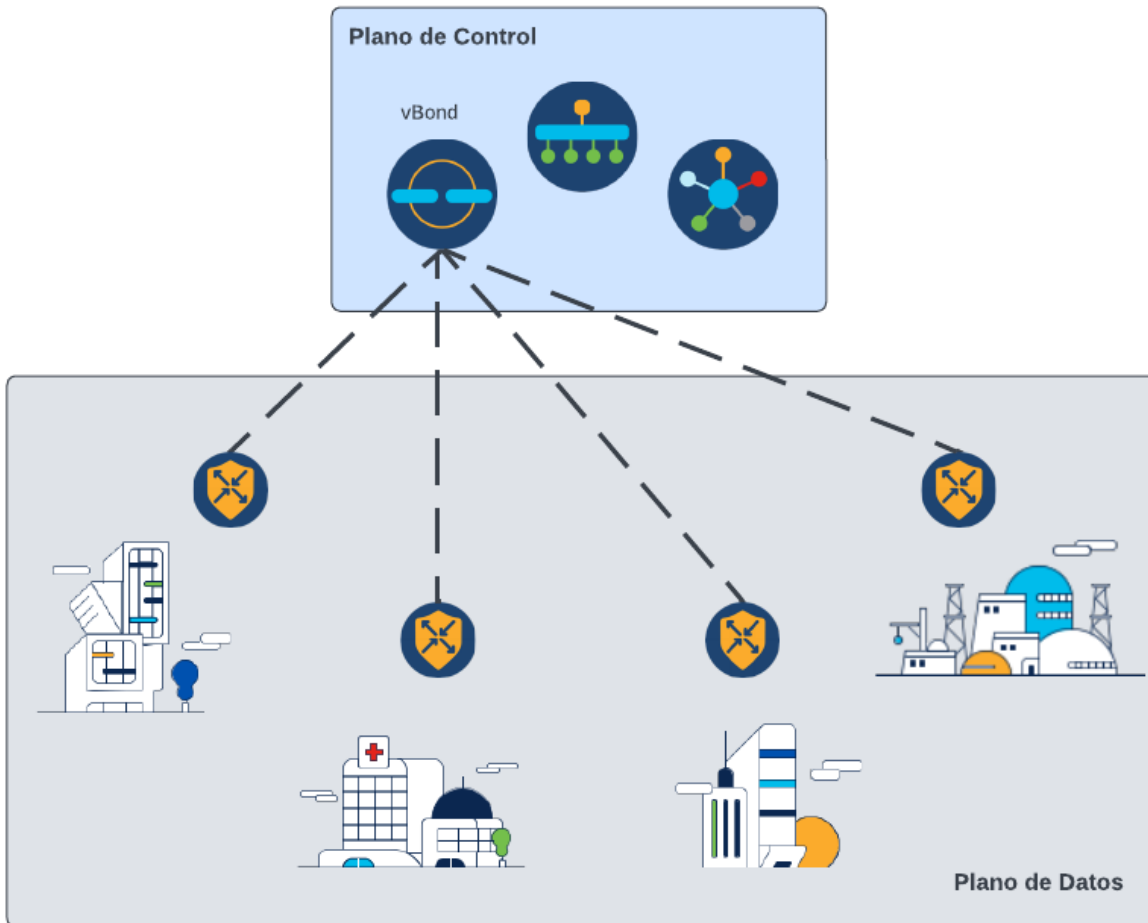
- Los controladores son el centro de la infraestructura SD-WAN.



- Residen lógicamente en la parte superior de la red SD-WAN.



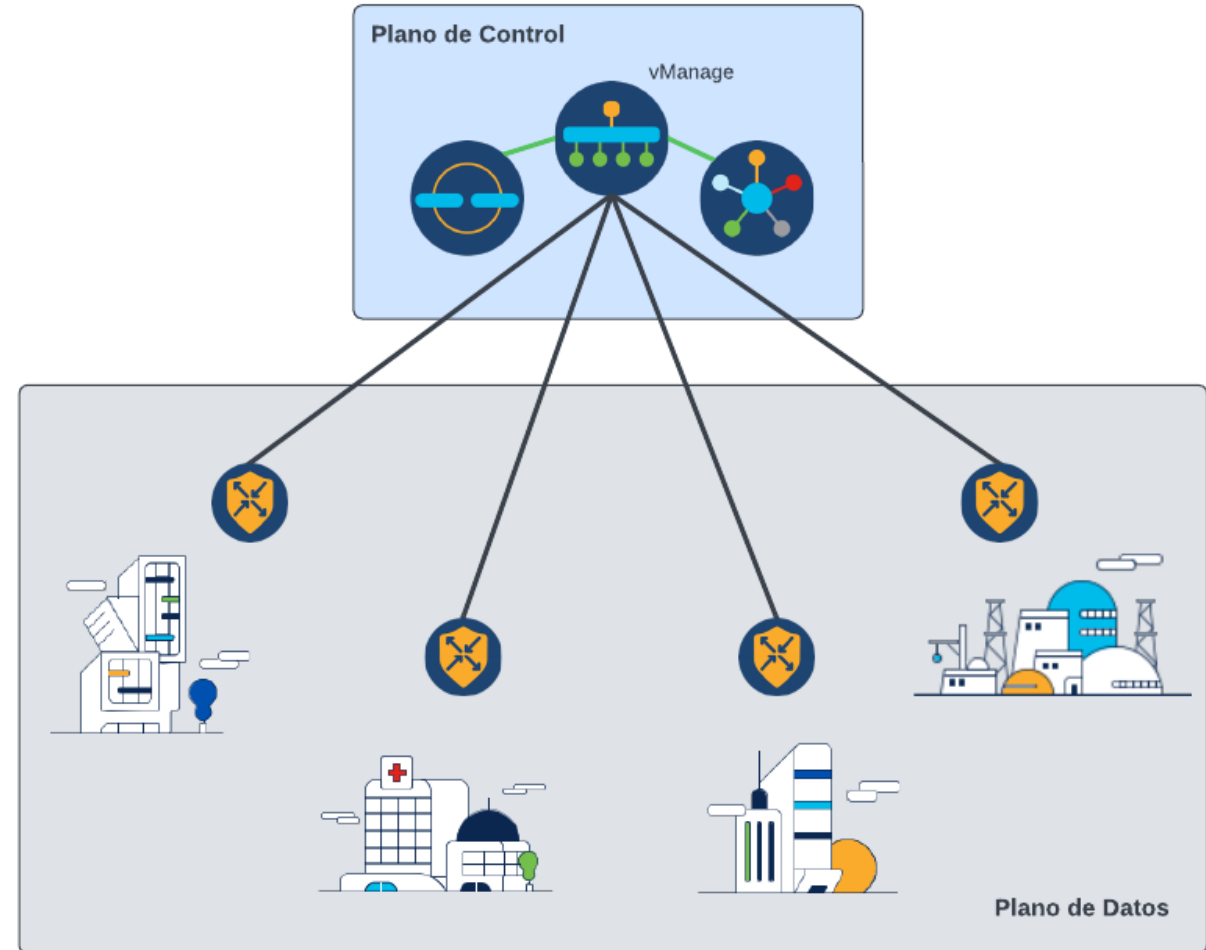
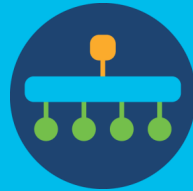
# vBond – Plano de Orquestación



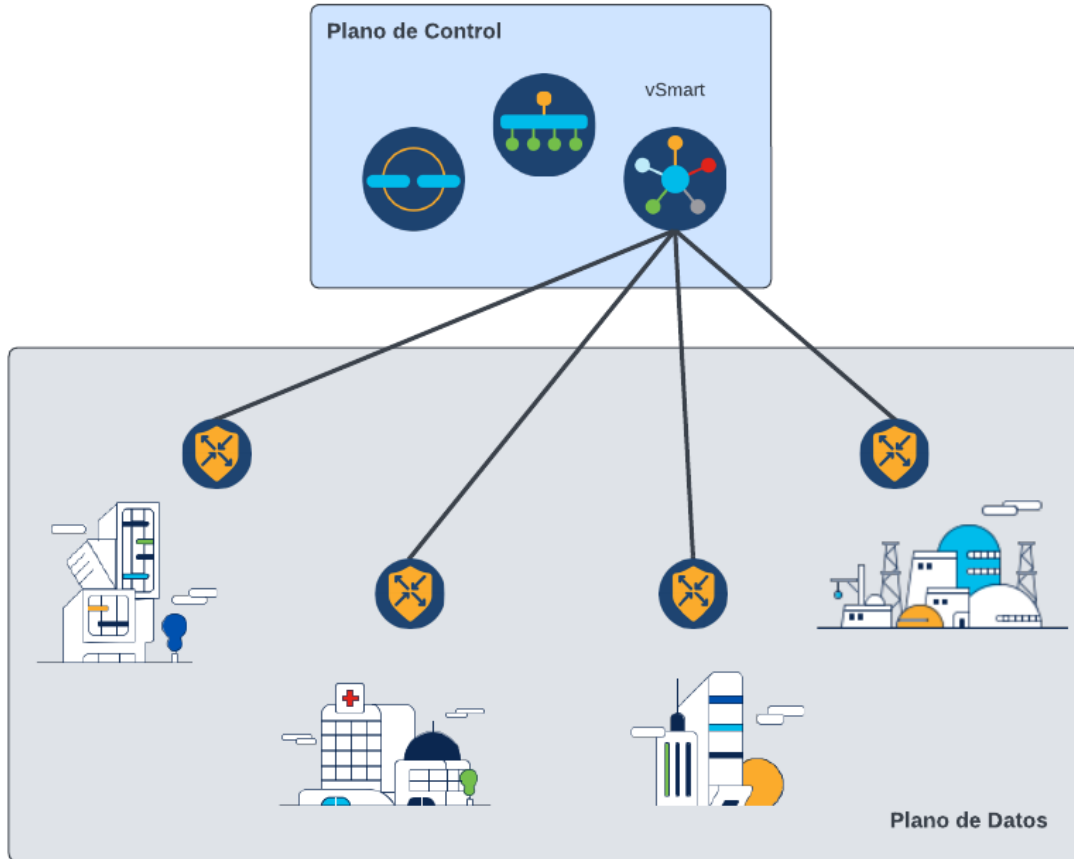
- Incorporación de nuevos dispositivos.
- Punto de autenticación.
- Plano de Orquestación.
- Indica a los Edges las direcciones IP públicas de los controladores vSmart y vManage.
- Todos los componentes en el overlay deben conocer la IP o URL del vBond.

# Cisco vManage – Plano de Administración

- Recopilación de datos de telemetría de red
- Ejecutar análisis
- Alertas sobre eventos
- Plantillas
- Envío de configuraciones
- Administración de usuarios
- Creación de políticas
- Configuración de integraciones
- Actualizaciones de software
- Interfaz gráfica de usuario (GUI)



# Cisco vSmart – Plano de Control



- Plano de control del sistema SD-WAN
- Anuncian enrutamiento, políticas y seguridad hacia la red
- Todos los routers Edge forman conexiones persistentes con todos los vSmarts
- Los vSmarts no forman parte del plano de datos y no participan en el reenvío de paquetes

# Router Edge



- vEdge o cEdge = plano de datos
- OS: Viptela o IOS-XE SD-WAN
- Dispositivos virtuales o físicos
- Objetivo: envío de datos e interconexión de sucursales y centros de datos
- Características por plataforma
- Servicios integrados
- Flexibilidad de configuración

# Portafolio de dispositivos SD-WAN

## Viptela OS



vEdge 100 Series



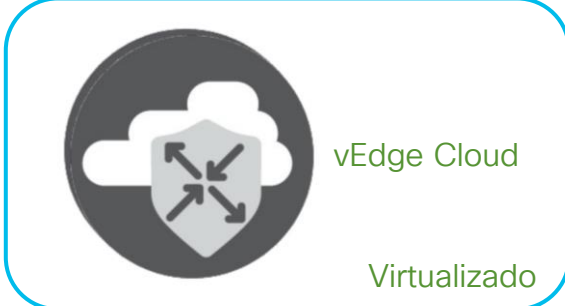
vEdge 1000



vEdge 2000



vEdge 5000



vEdge Cloud

Virtualizado

# Portafolio de dispositivos SD-WAN

## IOS-XE SD-WAN



Industrial Series



ISR1100 Series



ISR4000 Series

IOS-XE SDWAN  
Viptela OS

ISR1100-4G  
Power Reset USB 3.0 4x10/100/1000Mbps RJ45 Console port

ISR1100-4GLTENA  
LTE Antenna connector Micro USB Micro SIM slot 4x1GE 2xSFP RJ45 Console port

ISR1100-4G

ISR1100 Nutella Series



ASR1000 Series



ASR1000 Series

C8000v  
CSR1000v  
ISRv

Virtualizado



Catalyst 8300 Series



Catalyst 8500 Series



ENCS 5000

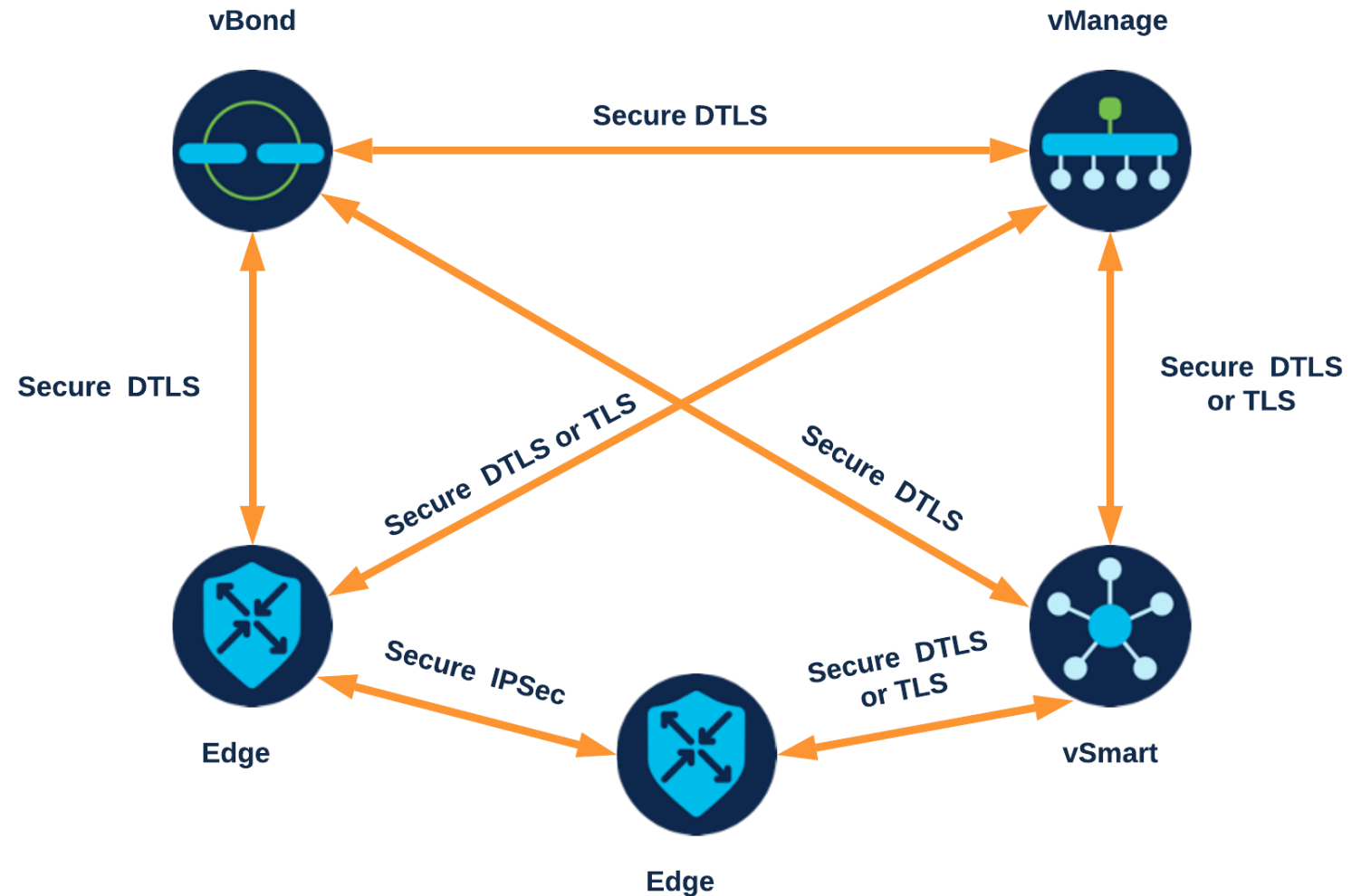


# 5. Túneles de Control y de Datos



# Túneles de Control: DTLS y TLS

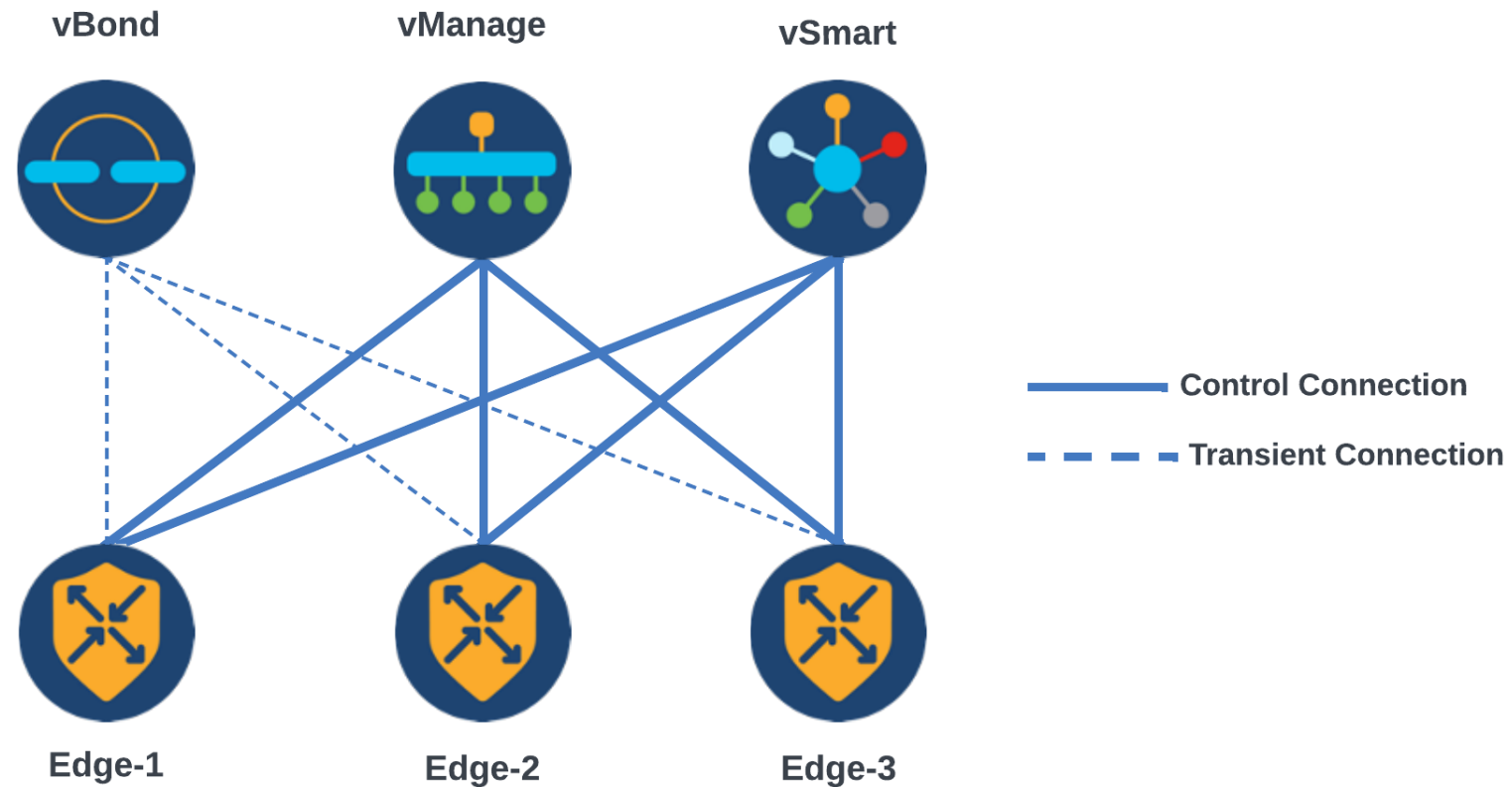
- Seguridad en control.
- La base del plano de control son dos protocolos de seguridad derivados de SSL (capa de sockets seguros):
  - **DTLS:** El protocolo de seguridad de la capa de transporte de datagramas. UDP
  - **TLS:** El protocolo de seguridad de la capa de transporte. TCP





# Sesiones de Control

- Los routers vEdge/cEdge forman túneles seguros contra los controladores vBond, vManage y vSmart y vManage, llamados Sesiones de Control.



# Verificación de Plano de Control

- Para verificar la correcta adición y formación de las Sesiones de Control del router Edge contra los controladores usamos el comando:

*show sdwan control connections*

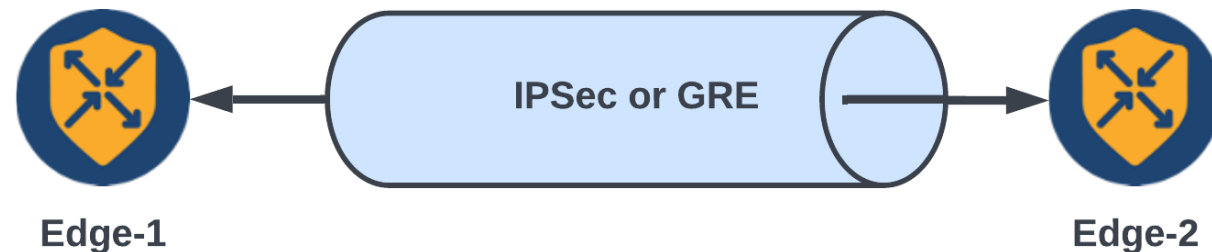
```
cEdge# show sdwan control connections
```

PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER PUBLIC IP	PEER PUB PORT	ORGANIZATION	LOCAL COLOR	CONTROLLER GROUP	PROXY	STATE	UPTIME	ID
vsmart	dtls	1.1.1.3	1013	1	10.2.65.7	12446	54.200.110.23	12446	calo-auto-lab	public-internet	No		up	13:22:43:59	0
vsmart	dtls	1.1.1.3	1013	1	10.2.65.7	12446	54.200.110.23	12446	calo-auto-lab	biz-internet	No		up	13:22:43:59	0
vsmart	dtls	1.1.1.5	1014	1	10.1.140.30	12446	34.207.123.209	12446	calo-auto-lab	public-internet	No		up	13:22:43:58	0
vsmart	dtls	1.1.1.5	1014	1	10.1.140.30	12446	34.207.123.209	12446	calo-auto-lab	biz-internet	No		up	13:22:43:58	0
vmanage	dtls	1.1.1.7	1000	0	10.2.65.42	12446	52.84.96.112	12446	calo-auto-lab	biz-internet	No		up	13:22:43:59	0

*show sdwan control connection-history*

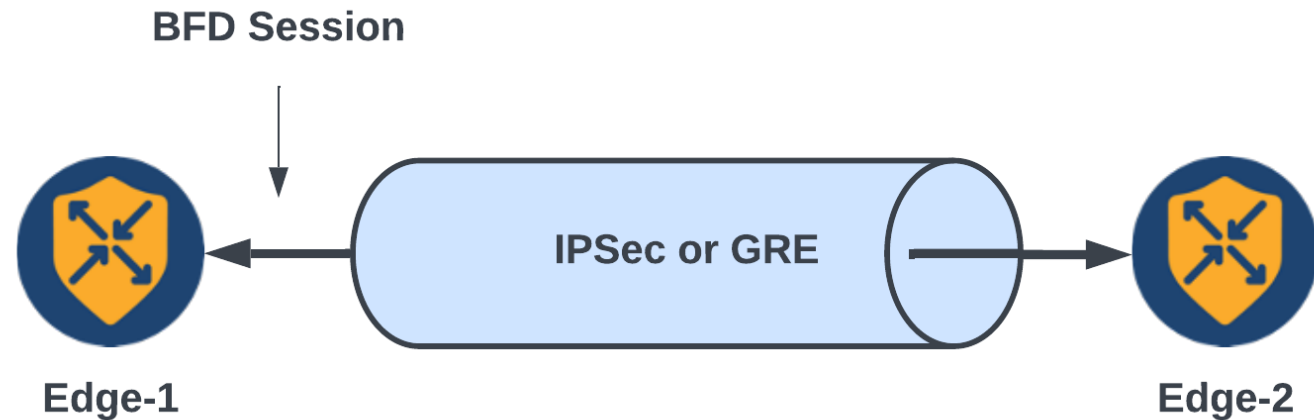
# Túneles de Datos: IPSec, GRE

- El plano de datos es responsable de manejar los paquetes que son transportados a través de la red. También es conocido como plano de envío.
- Los túneles de datos tienen como objetivo interconectar las sucursales entre sí y facilitar la comunicación del lado de servicio o LAN.
- Existen dos protocolos principales para los túneles de datos:
  - **IPSec:** El tráfico del overlay usa Internet Security (IPSec) como método por defecto.
  - **GRE:** Alternativa no segura.



# Bidirectional Forwarding Detection (BFD)

- Las sesiones BFD detectan la salud y fallas en los túneles de datos del overlay.



- Sus características:
  - Están habilitadas por defecto y no se pueden deshabilitar.
  - Residen dentro de los túneles IPsec o GRE.
  - Miden la latencia, pérdida y fluctuación entre dos sitios.
  - Determinan el estado del túnel: up o down.
  - Tienen relación directa con el protocolo de ruteo SD-WAN (OMP).

# Verificación del Plano de Datos

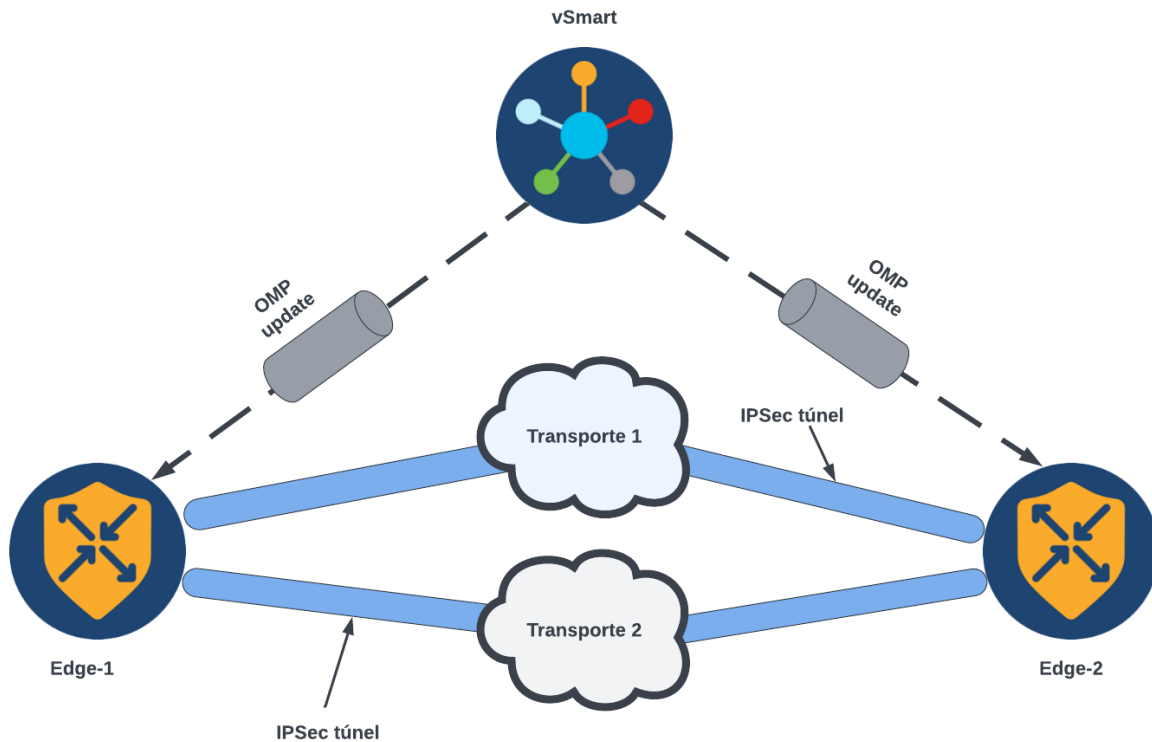
- Para asegurar que las sesiones de BFD se encuentran activas entre sitios usamos el comando:

*show sdwan bfd sessions*

```
cEdge# show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP	DST PUBLIC PORT	ENCAP	DETECT MULTIPLIER	TX INTERVAL (msec)	UPTIME	TRANSITIONS
1.1.1.221	100003	up	public-internet	public-internet	10.2.63.240	34.215.195.22	12366	ipsec	7	1000	14:49:38	0
1.1.1.231	100004	up	public-internet	public-internet	10.2.63.240	52.200.15.125	12346	ipsec	7	1000	02:16:09	2
1.1.1.231	100004	up	biz-internet	biz-internet	10.2.65.30	54.90.200.21	12346	ipsec	7	1000	02:16:09	2
1.1.1.221	100003	up	biz-internet	biz-internet	10.2.65.30	100.21.244.146	12366	ipsec	7	1000	14:49:38	0

# OMP – Overlay Management Protocol



- Cisco OMP es el centro de enrutamiento de la solución SD-WAN.
- Se utiliza para intercambiar información de rutas, políticas y administración entre los vSmarts y routers Edge.
- Segmenta los dominios de datos en VPNs, permitiendo tener tablas de ruteo distintas en un mismo router.
- Por defecto crea una topología Full Mesh entre todo el overlay.
- Está habilitado por defecto y puede desactivarse.

# Repaso SD-WAN



1

## Red WAN Tradicional

Conecta redes LAN que se encuentran en diferentes ubicaciones físicas.

2

## Red Definida por Software

Separa el plano de control del plano de envío de datos

3

## Sesiones de Control

Túneles DTLS o TLS en plano de Control

4

## Sesiones BDF

Túneles IPSEC o GRE en plano de Datos

Independencia  
del transporte



Beneficios de  
SD-WAN



Seguridad con  
tráfico cifrado

Configuración  
centralizada

Escalabilidad y  
diseño flexible

Configuración  
simplificada



Automatización



Priorización  
de tráfico





Join at

**slido.com**

**#2620 104**

🔒 Passcode:

**46riiy**

## ¿Implementarías SD-WAN en tu red? ¿Cuál sería el principal motivo?

A) Tenemos SD-WAN integrado, buscamos mantenernos actualizados.

0%

B) Necesidad de una solución más confiable y escalable.

0%

C) Facilidad de Integración a nuevas Tecnologías.

0%

D) Aprovechar los beneficios de las redes definidas por software vs las Legacy.

0%

E) Otro

0%

Descanso – 5 minutos



## 6. ¿Cómo identifico un router en modo SD-WAN?



# Modo de Funcionamiento

- **Autonomous:** Modo IOS-XE regular.
- **Controller-managed:** Modo SD-WAN.

```
cEdge# show version
<omitted>
cisco ISR4431/K9 (1RU) processor with 1699220K/6147K bytes of memory.
Processor board ID FJC2252A0H1
Router operating mode: Controller-Managed
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7081983K bytes of flash memory at bootflash:.

Configuration register is 0x2102
```

```
cEdge# show platform software device-mode
Device Operating-mode: Controller-Managed
```

```
cEdge# show logging | include System
<omitted>
Feb 22 18:02:22.543: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in
CONTROLLER mode
```

# Cambio de modo de un router IOS-XE

- 16.9 a hasta 16.12, imágenes independientes:

- UCMK9 > SD-WAN

```
Cisco ISR 4300 Series IOS XE SD-WAN Software  
isr4300-ucmk9.16.12.5.SPA.bin
```

- universalk9 > IOS-XE

```
Cisco ISR 4300 Series IOS XE Universal  
isr4300-universalk9.17.09.03a.SPA.bin
```

- 17.2.1r en adelante, imagen universal:

```
# controller-mode enable > modo SD-WAN
```

```
# controller-mode disable > modo IOS-XE
```

# 7. Incorporación de un router cEdge a una solución SD-WAN

Laboratorio

# Configuración Básica para cEdge

## Orden de configuración

- 1.- Interface física
- 2.- Ruta por defecto
- 3.- Guardar cambios
- 4.- Túnel XE en modo SD-WAN
- 5.- Túnel SD-WAN
- 6.- Guardar cambios

```
!Configuración IOS-XE
!  
config-transaction  
interface GigabitEthernet0/0/0  
ip address 192.168.10.2 255.255.255.0  
negotiation auto  
no shutdown  
!  
ip route 0.0.0.0 0.0.0.0 192.168.10.1  
!  
commit  
!  
interface Tunnel0  
no shutdown  
ip unnumbered GigabitEthernet0/0/0  
tunnel source GigabitEthernet0/0/0  
tunnel mode sdwan  
exit  
!  
! Configuración SD-WAN  
!  
sdwan  
interface GigabitEthernet0/0/0  
tunnel-interface  
encapsulation ipsec  
color default  
allow-service all  
!  
commit  
!  
end
```

# Configuración de Sistema

Configuración básica en un cEdge para formar sesiones de control:

**IP del sistema:** Identificador único para el cEdge, viene en formato octal punteado. No es una IP enrutable.

**ID del sitio:** identificador único del sitio.

**Nombre de la organización:** identificador único del overlay de SD-WAN.

**IP y puerto de vBond:** IP y puerto de vBond. Se puede obtener desde el propio vBond con el comando:

```
!  
config-transaction  
system  
system-ip 10.10.10.1  
site-id 10  
organization-name SDWAN-OVERLAY  
vbond 172.16.120.20 port 12346  
!
```

***show sdwan running-config system***



# Laboratorio



# Objetivo



1. Identificar el modo de operación del router
2. Verificar Número de Serial en vManage
3. Verificación de interfaces
4. Configuración básica
5. Verificación de Plano de Control y de Datos

## Versiones:

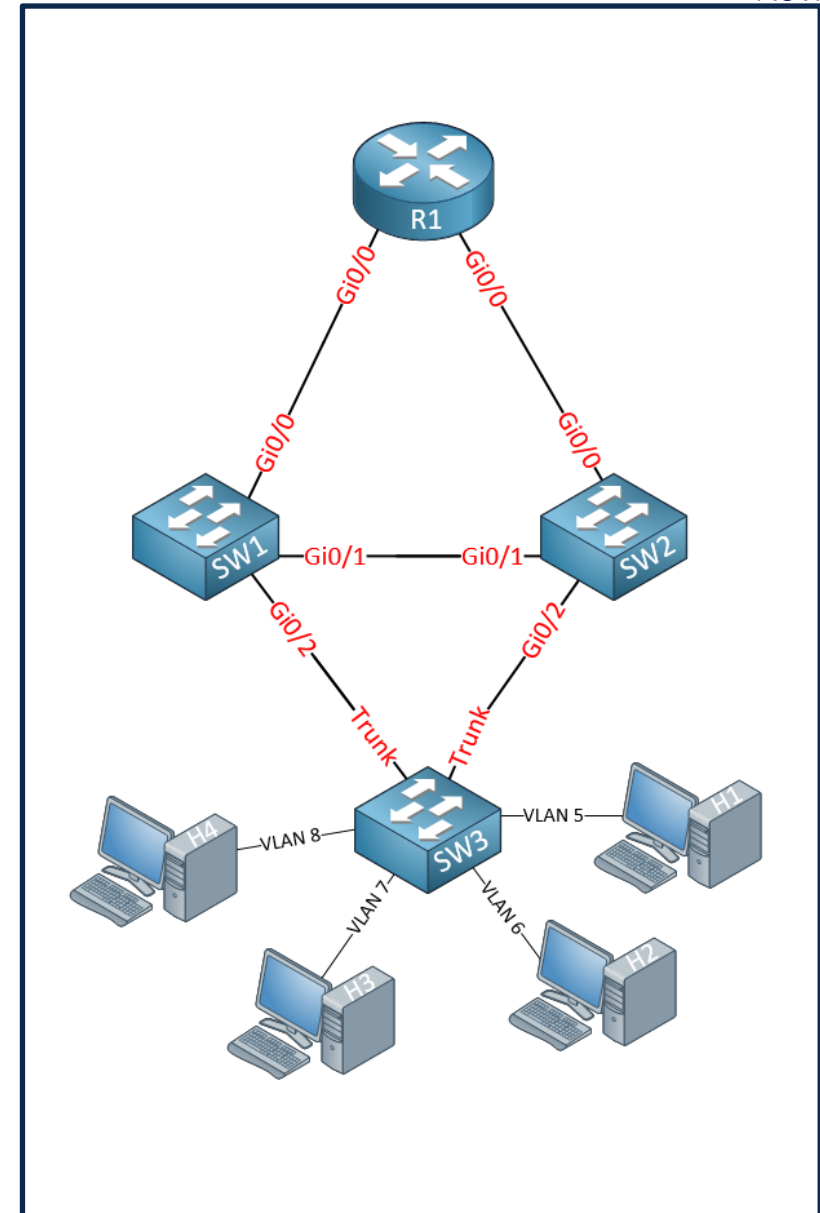
- Controladores: 20.9.3.2
- cEdge: 17.9.3

## 7.2 Solución al caso de uso con SD-WAN



# Estado Actual de la Red

- Red legacy, routers Cisco ISR G2 3900, 2900
- Switches Cisco 3650, 2960
- Transporte MPLS, E1
- Monitoreo SNMP
- Configuración e implementaciones manuales
- No redundancia
- No experiencia de aplicativos
- No ruteo basado en SLA
- No programabilidad (APIs)
- Mano de obra manual



# Hospitales en Brasil con SD-WAN

- Nueva generación de Cisco routers.
- ISR1K módulo de switch integrado. ISR4K/C8k switch NIM.
- Multi transporte: MPLS, Internet público, LTE 4G/5G.
- Monitoreo nativo centralizado en local o en la nube.
- Configuración y despliegue *Zero-Touch* y por plantillas.
- Sitios, transportes y controladores redundantes.
- Selección de ruteo con políticas basadas en SLA.
- Manipulación centralizada de ruteo.
- Motores de programabilidad y APIs nativos.
- Reducción de fuerza de trabajo para administración de red.
- Seguridad integrada ZBFW, IPS, IDS, filtro de URLs.





Join at

**slido.com**

**#2620 104**

🔒 Passcode:

**46riiy**

## ¿Qué ventajas de la solución SD-WAN traerían beneficios a tu red actual?

A) Mayor seguridad en la red.

0%

B) Mayor escalabilidad.

0%

C) Facilidad de administración y monitoreo de red.

0%

D) Facilidad de integración de nuevas soluciones de red.

0%

E) Independencia de transporte.

0%

# 8. Integraciones

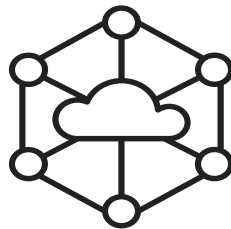


# SD-WAN Cloud OnRamp

Una solución de red WAN que ofrece amplias integraciones en la nube con flexibilidad, seguridad y escalabilidad



Optimiza las experiencias de las aplicaciones y automatiza la conectividad independiente de la nube



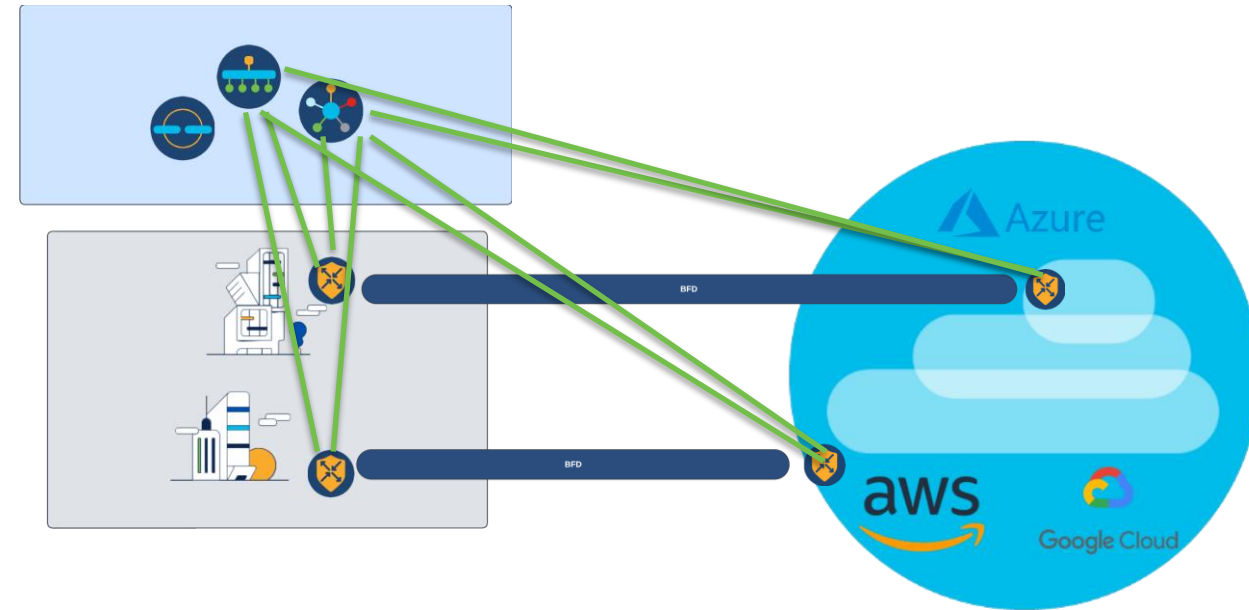
Conectividad fluida a casi cualquier configuración de sitio a nube, de sitio a aplicación o de sitio a sitio.

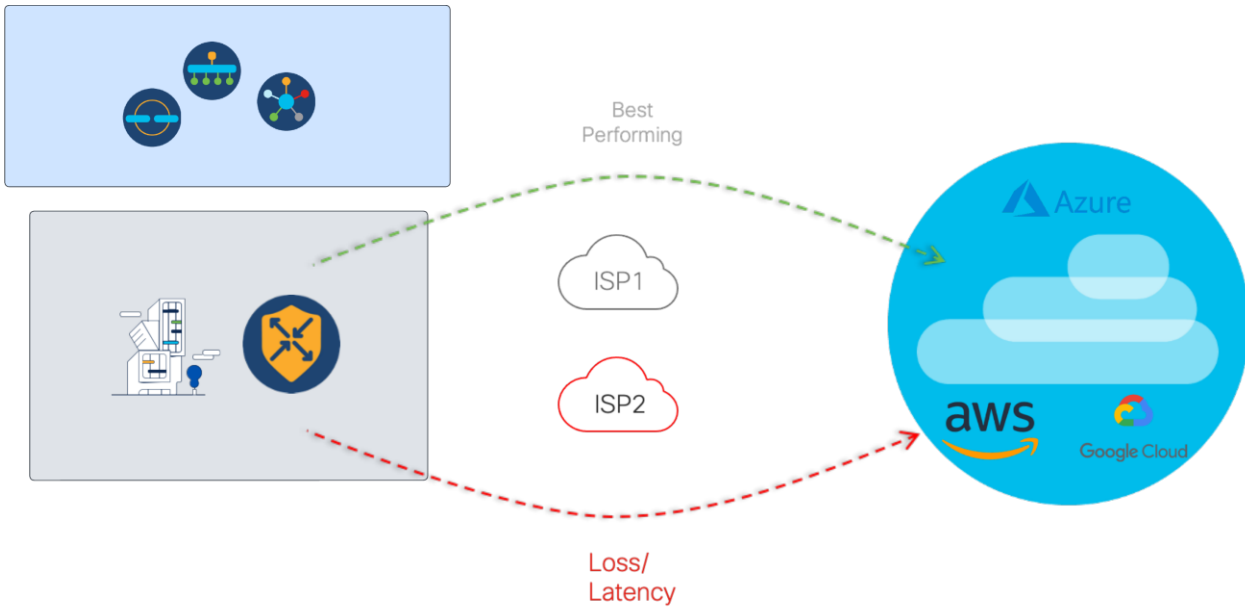




# Cloud OnRamp for IaaS

Permite que Sitios remotos, centros de Datos, campus, aprovechen características como AAR para escoger el mejor camino para alcanzar aplicaciones alojadas en nubes públicas como AWS, Azure o GCP.





# Cloud OnRamp for SaaS

Gateways y Sitios con DIA habilitado realizan una selección de la mejor ruta local para alcanzar las aplicaciones.

## Cloud OnRamp para Multicloud



## Amazon Web Services

Automatiza la conexión a AWS y se integra nativamente a la nube por medio de un Transit Gateway.



Google Cloud



## Microsoft Azure

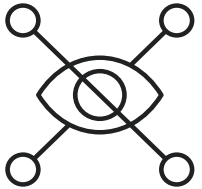
Permite una estrecha integración entre SD-WAN y Azure Virtual WAN optimizando la experiencia del usuario de Microsoft 365.



## Google Cloud Platform

Automatiza la extensión de la estructura SD-WAN y la conectividad de sitio a sitio mediante SD-WAN Cloud Hub con Google Cloud.

Visibilidad  
Completa



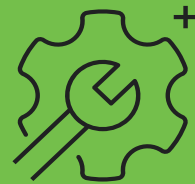
Información  
operativa



Recomendaciones  
de flujo



Top Talkers



# vAnalytics



Cisco vAnalytics recopila y almacena metadatos sobre los flujos de tráfico en su almacenamiento en la nube y produce análisis basados en estos datos recopilados.

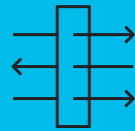
## Secure Web Gateway

Control, transparencia y protección del malware y otros ataques peligrosos.



## Cloud-delivered firewall

El firewall de Umbrella proporciona visibilidad y control para todo el tráfico en todos los puertos y protocolos.



## DNS-layer Security

Establece una conexión segura y cifrada para solicitudes de DNS, refuerza y bloquea destinos maliciosos y no deseados.

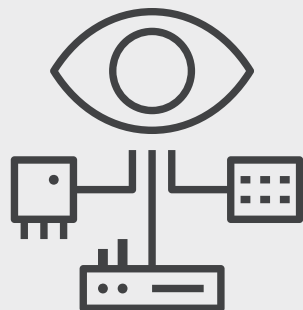


# Integración a SIG

Umbrella / Zscaler



## Integración con ThousandEyes



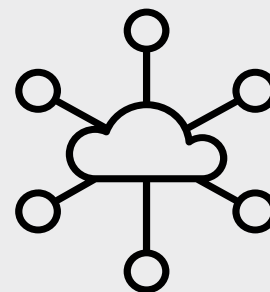
## Observa todo el SD-WAN Fabric

Garantice la accesibilidad y disponibilidad de aplicaciones alojadas internamente y servicios basados en la nube en cualquier red.



## Visibilidad

ThousandEyes Internet y la inteligencia en la nube brindan visibilidad de extremo a extremo desde el borde de la WAN hasta cualquier lugar.



## Monitorea la experiencia de la aplicación

Monitorear y validar el rendimiento de las aplicaciones web, incluidas SaaS y aplicaciones alojadas internamente.

# Preguntas top



# Clausura







## ¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar ¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 1 de septiembre de 2023

<https://bit.ly/CL2doc-aug23>



## Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

**¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!**

Al término de esta sesión, se abrirá una encuesta en su navegador.



# Nuestras Redes Sociales

LinkedIn

[Cisco Community](#)

Twitter

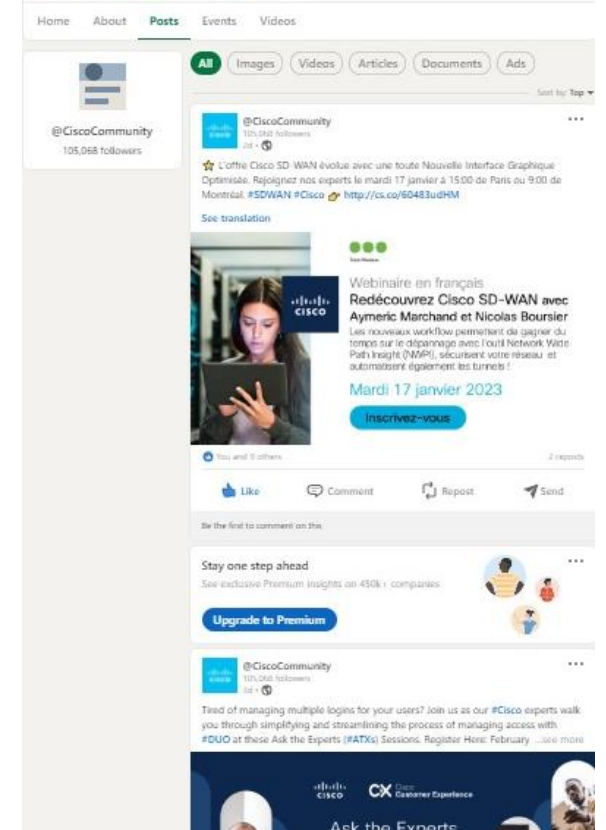
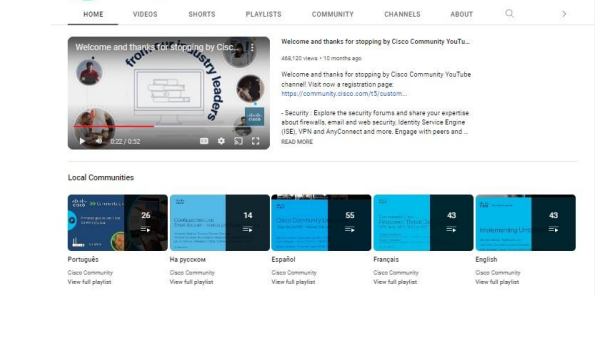
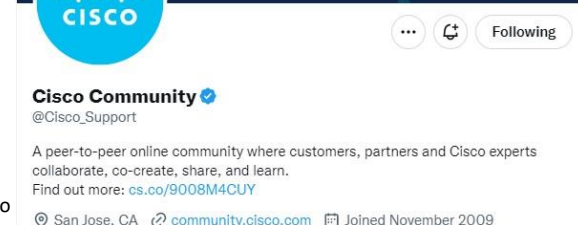
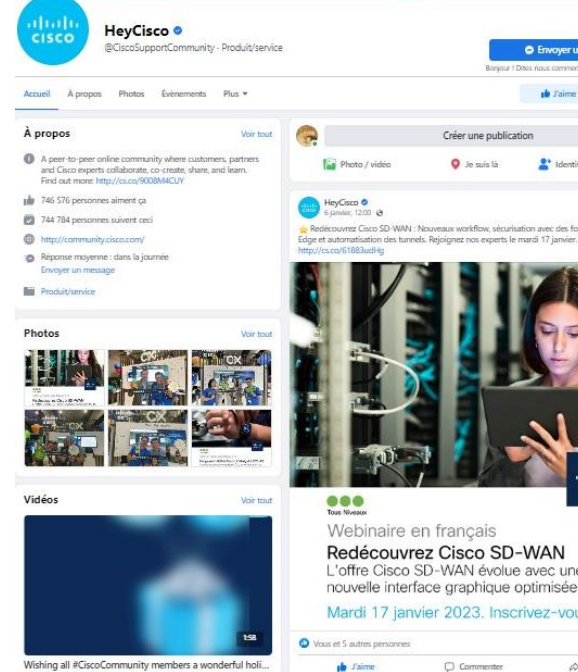
[@CiscoCommunity](#)

YouTube

[CiscoSupportChannel](#)

Facebook

[CiscoSupportCommunity](#)





The bridge to possible