



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023
NIPO: pte. de asignar

Fecha de Edición: noviembre de 2023

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA PARA CONECTIVIDAD HÍBRIDA EN AWS ..4	4
1.1. DESCRIPCIÓN DEL USO DE ESTA GUÍA.....	4
1.2. MODELO DE RESPONSABILIDAD COMPARTIDA.....	4
2. SERVICIOS DISPONIBLES PARA LA CONECTIVIDAD HÍBRIDA CON AWS.....6	6
2.1. INTRODUCCIÓN.....	6
3. CONFIGURACIÓN SEGURA PARA CONECTIVIDAD HÍBRIDA EN AWS.....7	7
3.1. SERVICIOS EJECUTADOS EN LOS CENTROS DE DATOS DE AWS	8
3.1.1. <i>Regiones de AWS</i>	9
3.1.2. <i>Zonas de disponibilidad</i>	9
3.1.3. <i>Zonas locales</i>	9
3.1.4. <i>Virtual Private Cloud (VPC)</i>	9
3.1.5. <i>AWS Global Accelerator</i>	10
3.2. SERVICIOS DE INTERCONEXIÓN CON LOS CENTROS DE DATOS DE AWS	12
3.2.1. <i>Virtual Private Network (VPN)</i>	12
3.2.2. <i>AWS Direct Connect</i>	24
3.2.3. <i>AWS Transit Gateway</i>	40
3.2.4. <i>AWS Private Link</i>	41
3.2.5. <i>AWS Route 53 Resolver</i>	41
3.3. SERVICIOS DE AWS EJECUTADOS EN CENTROS DE DATOS LOCALES	42
3.3.1. <i>AWS Outposts</i>	42
3.3.2. <i>AWS Snowball Edge</i>	43
3.3.3. <i>AWS Snowcone</i>	45
4. GLOSARIO DE TÉRMINOS	48
5. GLOSARIO DE SERVICIOS AWS.....	50

1. GUÍA DE CONFIGURACIÓN SEGURA PARA CONECTIVIDAD HÍBRIDA EN AWS

1.1. Descripción del uso de esta guía

El objetivo de la presente guía es documentar las herramientas y recomendaciones de configuración de seguridad para conectividad híbrida en aquellas organizaciones que aprovechan los servicios de AWS para conectar sus centros de datos locales, remotos y la nube. Por su parte, la guía **CCN-STIC 887A Guía de configuración segura para AWS**, recoge los requisitos y configuraciones de seguridad para el cumplimiento del Esquema Nacional de Seguridad, en adelante ENS.

1.2. Modelo de responsabilidad compartida

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre AWS y el cliente. Este modelo compartido puede aliviar la carga operativa del cliente, ya que AWS opera, administra y controla los componentes del sistema operativo host y la capa de virtualización hasta la seguridad física de las instalaciones en las que funcionan los servicios. El cliente asume la responsabilidad y la administración del sistema operativo que utiliza cada instancia (incluidas las actualizaciones y los parches de seguridad), de cualquier otro software de aplicaciones asociado y de la configuración del firewall del grupo de seguridad que ofrece AWS.

Los clientes deben pensar detenidamente en los servicios que eligen, ya que las responsabilidades varían en función de los servicios que utilicen, de la integración de estos en su entorno de TI y de la legislación y los reglamentos correspondientes.

La naturaleza de esta responsabilidad compartida también ofrece la flexibilidad y el control por parte del cliente que permite concretar la implementación. Como se muestra a continuación, la diferenciación de responsabilidades se conoce normalmente como seguridad "de" la nube y seguridad "en" la nube.

Responsabilidad de AWS en relación con la "seguridad de la nube": AWS es responsable de proteger la infraestructura que ejecuta todos los servicios provistos en la nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

Responsabilidad del cliente en relación con la "seguridad en la nube": la responsabilidad del cliente estará determinada por los servicios de la nube de AWS que el cliente seleccione. Esto determina el alcance del trabajo de configuración a cargo del cliente como parte de sus responsabilidades de seguridad.

Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se clasifica como servicios de Infraestructura y, como tal, requiere que el cliente realice todas las tareas de administración y configuración de seguridad necesarias, incluyendo el ya mencionado firewall del grupo de seguridad. Amazon EC2 es una

solución de virtualización similar a los servicios que ofrecen las herramientas de tipo Hipervisor (al menos en lo que a nivel operacional se refiere) en la que un servidor actúa de huésped alojando máquinas virtuales (en este caso, denominadas instancias) e interconectándolas. Los sistemas y servicios instalados en dichas máquinas virtuales y las comunicaciones y permisos entre ellas, así como la protección de datos contenidos y seguridad en dichas comunicaciones, no son gestionados por AWS sino por el cliente.

Los clientes que implementan una instancia de Amazon EC2, por tanto, son responsables de la administración del sistema operativo que usen en la misma (incluidos los parches de seguridad y las actualizaciones), de cualquier utilidad o software de aplicaciones que el cliente haya instalado en las instancias y de la configuración del firewall provisto por AWS (llamado grupo de seguridad) en cada instancia.

En el caso de los servicios gestionados por AWS, como Amazon S3 (servicios de almacenamiento gestionados) y Amazon DynamoDB (servicios de base de datos gestionados), AWS maneja la capa de infraestructura, el sistema operativo y las plataformas, mientras que los clientes acceden a los puntos de enlace para recuperar y almacenar los datos. Los clientes son responsables de administrar sus datos (incluidas las opciones de cifrado), clasificar sus recursos y utilizar las herramientas de AWS Identity and Access Management (IAM) para solicitar los permisos correspondientes.

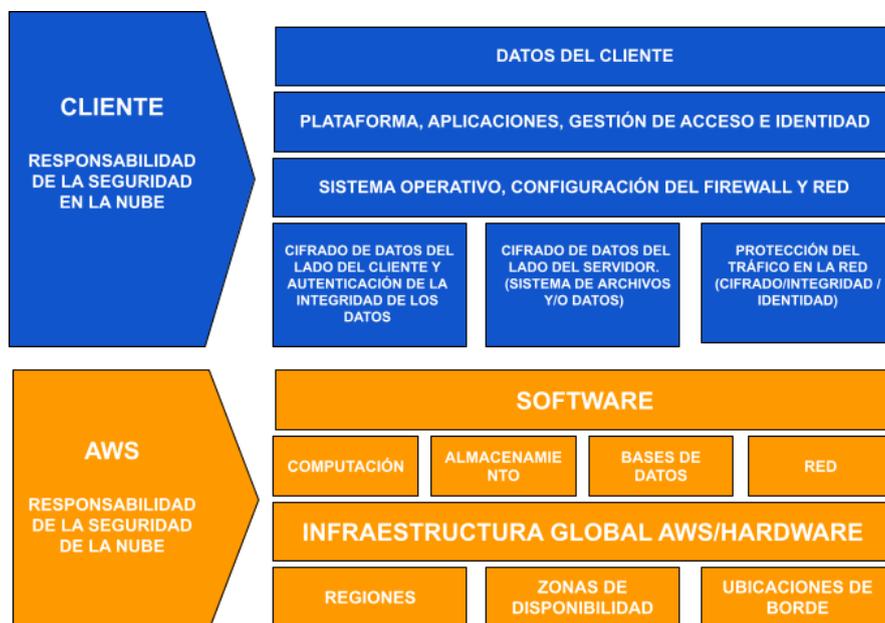


Fig. 1 - Representación del modelo de responsabilidad compartida en AWS

El modelo de responsabilidad compartida entre AWS y sus clientes, abarca también los controles de TI. Del mismo modo que comparten la responsabilidad del entorno, también comparten la administración, el funcionamiento y la verificación de los controles de TI. En este sentido, la presente guía es un recurso para el cliente de AWS referente al ámbito de la responsabilidad del cliente en cuanto a la seguridad de infraestructura y datos según el tipo de servicios utilizados.

Así mismo, los clientes pueden hacer uso de la documentación de conformidad y control disponible en AWS, así como sus procedimientos de verificación y evaluación de los controles.

A continuación, se enumeran varios ejemplos de controles y se especifica a qué entidad corresponde la responsabilidad según el tipo de control:

- **Controles heredados:** Los controles heredados son aquellos que un cliente hereda de AWS en su totalidad. Son aquellos controles sobre los que el cliente no tiene ningún tipo de acceso, como los controles físicos y de entorno.
- **Controles compartidos:** Aplican tanto a la capa de infraestructura como a las capas de clientes. En un control compartido, el encargado de suministrar los requisitos para la infraestructura recae en AWS y la responsabilidad de configuración de aplicaciones, bases de datos y sistemas operativos de las instancias (de los huéspedes). Por ejemplo, la administración de parches, la corrección de imperfecciones o la administración de las configuraciones, serían responsabilidad de AWS en lo que se refiere a los elementos internos de la infraestructura (hosts y servicios gestionados). Sin embargo, el cliente será responsable de configurar y aplicar los parches de sus aplicaciones, bases de datos y sistemas operativos huésped.
- **Controles específicos del cliente:** Aquellos elementos que son de absoluta responsabilidad del cliente incluirían la seguridad de zonas, protección de comunicaciones y servicios. El direccionamiento y el aislamiento para la protección de la información deberá ser definido por el cliente.

2. SERVICIOS DISPONIBLES PARA LA CONECTIVIDAD HÍBRIDA CON AWS

2.1. Introducción

Los entornos empresariales a menudo son una combinación de nube, centros de datos en las instalaciones y ubicaciones de *edge* (entornos operacionales remotos y desconectados donde se almacenan datos, que no pueden ser procesados ni permiten actuar sobre los mismos). Las arquitecturas de nube híbrida ayudan a las organizaciones a integrar sus operaciones en las instalaciones y en la nube para admitir un amplio espectro de casos de uso mediante un conjunto común de servicios, herramientas y APIs. Los principales casos de uso de estas integraciones incluyen, para el abanico de servicios cloud de AWS:

- Compatibilidad con aplicaciones de baja latencia, para todas aquellas aplicaciones que requieren una comunicación inmediata entre el cliente y el servidor con menos de un segundo de retraso.
- Procesado de datos a nivel local, evitando limitaciones de tamaño, ancho de banda o tiempo de tareas de procesamiento.

- Cumplimiento con los requisitos de residencia de datos, evitando la necesidad de crear centros de datos en todo el mundo, pudiendo hacer uso de la infraestructura de nube pública para alojar datos en una ubicación específica que cumpla con los requisitos de seguridad y normativos específicos.
- Adopción de esfuerzos de migración a la nube, permitiendo realizar cambios graduales de traslado de activos digitales a la infraestructura de nube pública con una mínima interrupción del servicio.
- Expansión de los centros de datos, adaptando la inversión en software y hardware en función del uso de servicios en la nube.
- Traslado de aplicaciones a la nube, permitiendo migrar cargas de trabajo de aplicaciones que necesiten estar alojadas en la nube, manteniendo otros componentes en las instalaciones locales.

Se puede consultar la guía del fabricante sobre entornos híbridos para más información y casos de uso en el siguiente enlace: [Conectividad híbrida - AWS Whitepaper](#).

AWS ofrece a sus clientes múltiples herramientas para abordar los diferentes escenarios, necesidades y casos de uso referentes a la conectividad híbrida. A continuación, se describirán los servicios más comunes y sus configuraciones de seguridad recomendadas.

Recordamos, no obstante, que previamente a la configuración de la conectividad híbrida que se vaya a implantar en la organización, se debe hacer uso de la autenticación vía AWS IAM tal y como se recoge en el apartado control de accesos de la guía **CCN-STIC 887A Guía de configuración segura para AWS**.

3. CONFIGURACIÓN SEGURA PARA CONECTIVIDAD HÍBRIDA EN AWS

La informática en la nube ofrece a los desarrolladores y departamentos de IT la capacidad de aligerar cargas de trabajo relacionadas con el aprovisionamiento, mantenimiento o planificación de la capacidad. A medida que el uso de servicios en la nube se ha incrementado, se han desarrollado varios modelos y estrategias de implementación que satisfacen las necesidades de los distintos usuarios y organizaciones. Existen tres modelos principales de informática en la nube, que son:

- **Infraestructura como servicio (IaaS)**. Permite acceder a las características de conexión en red, a los equipos (virtuales o en software dedicado) y al espacio de almacenamiento de datos.
- **Software como servicio (SaaS)**. Proporciona un producto completo que el proveedor cloud ejecuta y administra.
- **Plataforma como servicio (PaaS)**. Elimina la necesidad de administrar la

infraestructura subyacente, pudiendo centrar los esfuerzos de implementación y administración directamente sobre las aplicaciones.

En función de cómo estos sean implementados en la nube, se podrá diferenciar entre tres modelos de servicio:

- **Nube.** Una aplicación basada en la nube se implementa totalmente sobre ella, de modo que todas las partes de la aplicación son ejecutadas en esta.
- **En las instalaciones.** La implementación local de recursos mediante herramientas de administración y virtualización se denomina, en ocasiones, “nube privada”, y se utiliza por su capacidad para ofrecer recursos dedicados.
- **Solución híbrida.** Es una manera de conectar la infraestructura y las aplicaciones entre los recursos basados en la nube y los recursos existentes situados fuera de la nube.

En los siguientes apartados se describen los casos de uso más comunes de solución híbrida.

3.1. Servicios ejecutados en los centros de datos de AWS

Los recursos informáticos en la nube de Amazon están alojados en varias ubicaciones de todo el mundo. Dichas ubicaciones se componen de regiones de AWS, zonas de disponibilidad y zonas locales. Cada región de AWS es un área geográfica independiente que contiene varias ubicaciones aisladas conocidas como zonas de disponibilidad; cuando una extensión de estas regiones se encuentra geográficamente cerca de los usuarios finales, será considerada zona local. En la siguiente figura se puede ver, a muy alto nivel, como se estructuran estas ubicaciones.

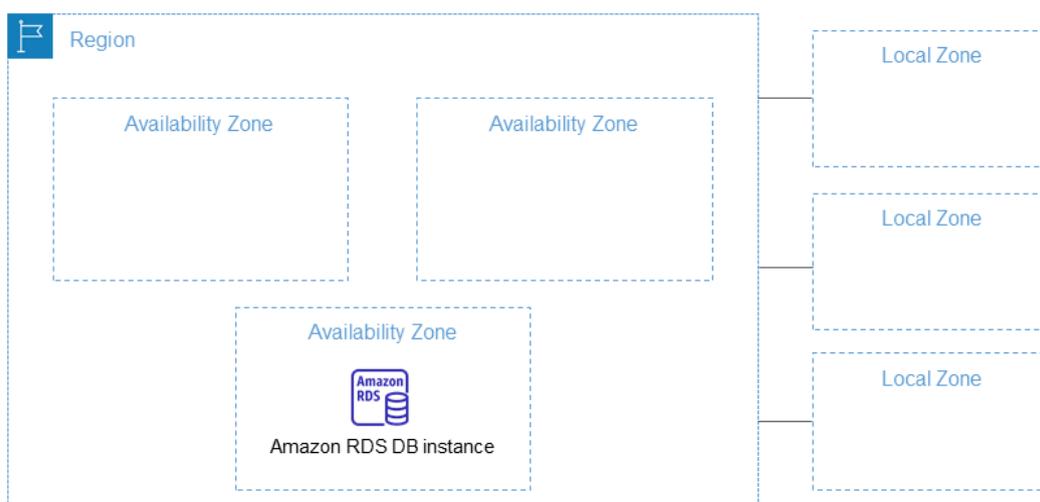


Fig. 2 - Descripción visual de las regiones, zonas de disponibilidad y zonas locales.

3.1.1. Regiones de AWS

Las regiones son ubicaciones físicas donde AWS agrupa los centros de datos. Cada región de AWS está diseñada de forma que esté totalmente aislada de las demás regiones de AWS, lo cual permite lograr una mayor tolerancia a errores posibles, así como una mayor estabilidad en los servicios. Las regiones de infraestructura de AWS cumplen con los niveles más altos de seguridad, cumplimiento y protección de datos.

3.1.2. Zonas de disponibilidad

Las zonas de disponibilidad (AZ) son grupos de centros de datos físicos en ubicaciones aisladas y separadas en un rango de 100 km de distancia dentro de cada región, interconectadas con redes de alta velocidad y baja latencia a través de fibra redundada cuyo tráfico está cifrado. Hay un mínimo de tres AZs por región. Las zonas de disponibilidad permiten que los clientes operen bases de datos y aplicaciones de producción con un nivel de disponibilidad, tolerancia a errores y escalabilidad mayor que el que ofrecería un centro de datos único.

3.1.3. Zonas locales

Una Zona local es una extensión de una región de AWS que está geográficamente cerca de los usuarios finales. Es posible ampliar cualquier VPC perteneciente a una región de AWS a una zona local mediante la creación de subredes asignadas a dicha zona local. Las zonas locales permiten a los usuarios ejecutar aplicaciones con la menor latencia posible en el borde, simplificar la migración de aplicaciones a la nube híbrida o cumplir con los requisitos más exigentes en cuanto a la residencia de datos estatales y locales que aplican sobre diferentes sectores.

Más información sobre regiones, zonas de disponibilidad y zonas locales de AWS en: [Regiones y zonas de disponibilidad de la infraestructura global](#)

3.1.4. Virtual Private Cloud (VPC)

Una [red privada virtual \(VPC\)](#) es una red virtual dedicada en una cuenta y región de AWS y lógicamente aislada de otras redes virtuales en la nube que permite a la organización lanzar recursos de AWS en una red virtual ya definida. Esta red virtual es muy similar a la red tradicional que usaría la organización en su propio centro de datos, pero con los beneficios que supone utilizar la infraestructura escalable de AWS.

Las cuentas de AWS incluyen una VPC predeterminada en cada Región de AWS. Las VPC predeterminadas se configuran de manera que el usuario pueda comenzar a lanzar instancias de EC2 y conectarse a ellas de manera inmediata, si bien se pueden crear VPCs adicionales con las subredes, las direcciones IP, las puertas de enlace y el enrutamiento que necesite.

Las funciones y los elementos principales de Amazon VPC son:

- Nubes privadas virtuales (VPC). Red privada virtual, prácticamente idéntica a la red tradicional del centro de datos local. Una vez creada, se podrán agregar subredes.
- Subredes. Rango de direcciones IP de la VPC. Una subred debe residir en una zona de disponibilidad. Después de agregar subredes, puede implementar recursos de AWS desde la VPC.
- Direccionamiento IP. Se puede asignar direcciones IPv4 e IPv6 a las VPC y subredes. También puede incorporar direcciones GUA IPv4 e IPv6 públicas a AWS y asignarlas a los recursos de la VPC, como las instancias de EC2, las puertas de enlace NAT y los equilibradores de carga de red.
- Enrutamiento. Las [tablas de enrutamiento](#) contienen conjuntos de reglas que determinan a dónde se dirige el tráfico de red desde la subred o puerta de enlace.
- Conexiones de emparejamiento. Las [conexiones de emparejamiento](#) de VPC sirven para enrutar el tráfico entre los recursos de dos VPC.
- Replicación de tráfico. La [replicación de tráfico](#) sirve para copiar el tráfico desde las interfaces de red y enviarlo a dispositivos de seguridad y monitoreo para una inspección profunda de paquetes.
- [Puerta de enlace de tránsito](#). Actúa como un concentrador central para enrutar el tráfico entre las redes VPC, las conexiones VPN y las conexiones de AWS Direct Connect.
- Conexiones de VPN. La VPC se pueden conectar a las redes de las instalaciones locales mediante [AWS VPN](#).

3.1.5. AWS Global Accelerator

AWS Global Accelerator es un servicio en el que se crea aceleradores para mejorar el rendimiento de sus aplicaciones para usuarios locales y globales. Dependiendo del tipo de acelerador que elija, puede obtener beneficios adicionales.

- Mediante el uso de un acelerador estándar, puede mejorar la disponibilidad de las aplicaciones de Internet destinadas al público general. Con un acelerador estándar, AWS Global Accelerator dirige el tráfico a través de la red global de AWS a los puntos finales de la región más cercana al cliente.
- Mediante un acelerador de enrutamiento personalizado, puede asignar uno o más usuarios a un destino específico entre muchos destinos.

De forma predeterminada, AWS Global Accelerator proporciona dos direcciones IP estáticas que se asocian con el acelerador. Con un acelerador estándar, en lugar de utilizar las direcciones IP que proporciona AWS Global Accelerator, puede configurar estos puntos de entrada para que sean direcciones IPv4 de sus propios rangos de direcciones IP que lleve a AWS Global Accelerator. Las direcciones IP estáticas se transmiten desde la red perimetral de AWS.

Para los aceleradores estándar, AWS Global Accelerator utiliza la red global de AWS para enrutar el tráfico hacia el punto final regional óptimo en función del estado, la ubicación del cliente y las políticas que configure, lo que aumenta la disponibilidad de las aplicaciones. Los extremos de los aceleradores estándar pueden ser equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias de Amazon EC2 o direcciones IP elásticas que se encuentran en una región de AWS o en varias regiones. El servicio reacciona instantáneamente a los cambios en el estado o la configuración para garantizar que el tráfico de Internet de los clientes siempre se dirige a los puntos finales en buen estado.

Los aceleradores de enrutamiento personalizados sólo admiten tipos de endpoints de subred de nube privada virtual (VPC) y enrutan el tráfico a direcciones IP privadas de esa subred.

Puede obtener más información sobre AWS Global Accelerator en la siguiente documentación del fabricante. [¿Qué es AWS Global Accelerator?](#)

3.2. Recomendaciones para el control de acceso

Como recomendación general de control de acceso relacionado con la conectividad híbrida, se plantea una mejor práctica de definir para este tipo de arquitecturas, una nueva cuenta de AWS específica, comúnmente llamada Cuenta de Red o Networking Account en inglés. La cuenta de red aísla los servicios, la configuración y el funcionamiento de la red de las cargas de trabajo, la seguridad y otras infraestructuras de las aplicaciones individuales. Esta configuración no solo limita la conectividad, los permisos y el flujo de datos, sino que también permite la separación de funciones y el mínimo privilegio para los equipos que necesitan operar en estas cuentas. Los equipos de redes (y seguridad) administran la mayoría de la infraestructura de esta cuenta. Puede ampliar información sobre entornos multi-cuenta consultando la **Guía CCN-STIC 887D Guía de configuración segura multi-cuenta AWS**

Todas las cuentas y VPC comparten los servicios de red y la infraestructura de red de la cuenta de forma centralizada (similar a un diseño central-radial), incluida la interconexión entre VPCs, interconexión con el on-premises, hibridación de DNS y las arquitecturas o gestión de inspección de tráfico (entrante, saliente, al on-premises o entre VPCs de diferente clasificación).

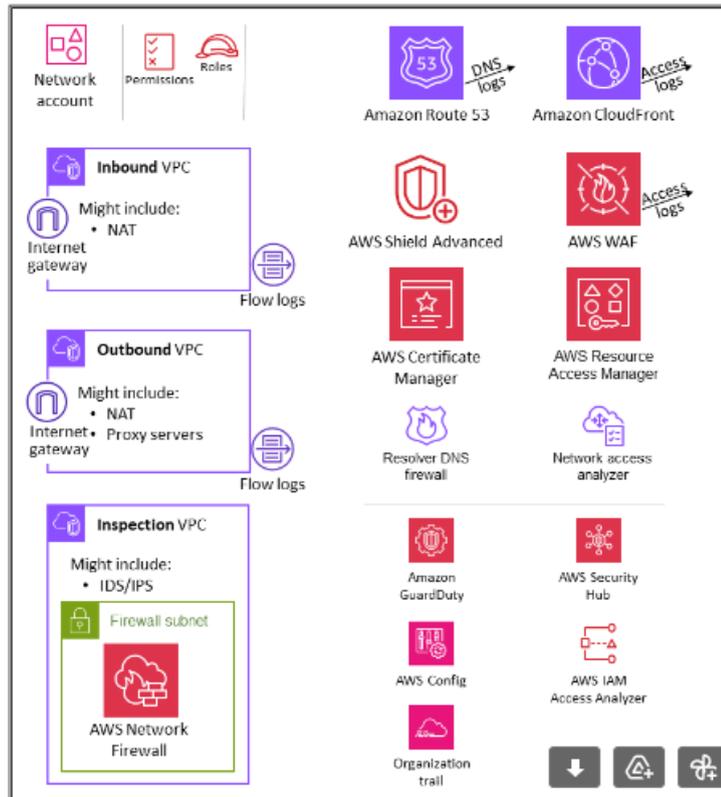


Fig.3 Ejemplo de Networking Account

3.3. Servicios de interconexión con los centros de datos de AWS

3.2.1. Virtual Private Network (VPN)

Las soluciones de red privada virtual de AWS establecen conexiones seguras entre las redes del cliente, las oficinas remotas, los dispositivos móviles y la red global de AWS. AWS VPN se compone de dos servicios: AWS Site-to-Site VPN y AWS Client VPN. Juntos, ofrecen una solución de VPN en la nube de alta disponibilidad, administrada y elástica para proteger el tráfico de red.

AWS Site-to-Site VPN crea túneles cifrados entre la red local y las instancias de Amazon Virtual Private Cloud o AWS Transit Gateway. Para administrar el acceso remoto, AWS Client VPN conecta usuarios a recursos de AWS o en las instalaciones mediante un cliente de software de VPN.

AWS Site-to-Site VPN

AWS Site-to-Site VPN crea una conexión segura entre el centro de datos local del cliente y los recursos de la nube de AWS. Para aplicaciones distribuidas globalmente, la opción Accelerated Site-to-Site VPN proporciona un rendimiento todavía mayor gracias al funcionamiento con AWS Global Accelerator. AWS Global Accelerator, como se ha mencionado anteriormente, es un servicio de redes que envía el tráfico del usuario a través de la infraestructura de red de Amazon Web Services, lo que mejora el rendimiento del usuario de Internet.

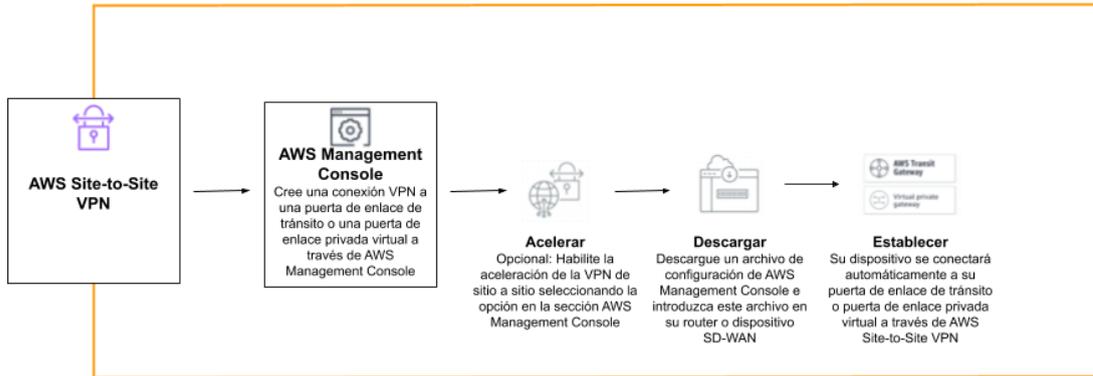


Fig. 4 - Descripción visual de los componentes de configuración para la VPN AWS Site-to-Site

Puede crear una conexión de VPN IPsec entre su VPC y su red remota. Deberá configurarse el dispositivo del gateway de cliente en el lado remoto de la conexión de AWS Site-to-Site VPN. Para obtener más información, consulte la Guía del usuario de AWS Site-to-Site VPN: [¿Qué es AWS Site-to-Site VPN? - AWS Site-to-Site VPN](#)

Dispositivo de VPN por software de terceros

Es posible crear una conexión de VPN a una red remota mediante una instancia Amazon EC2 en una VPC que ejecute un dispositivo de VPN por software de terceros. AWS no mantiene dispositivos de VPN por software de terceros; sin embargo, da a elegir entre un rango de productos de socios y comunidades de código fuente abierto. Este tipo de conectividad quedará fuera del alcance de esta guía.

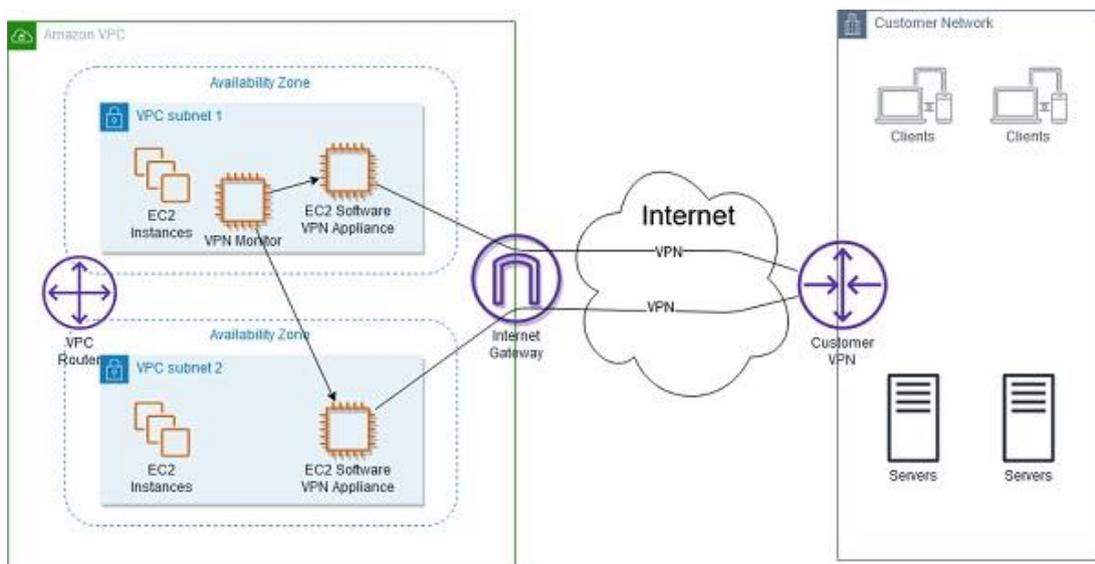


Fig. 5 - Arquitectura de una VPN con software de terceros en una EC2

La creación de una conexión VPC para instancias VPN por software requiere la instalación y configuración de múltiples instancias VPN y una instancia de monitorización para supervisar el estado de las conexiones VPN.

Arquitecturas de VPN

Conexión única de AWS Site-to-Site VPN

En esta arquitectura o diseño la VPC dispone de un virtual private gateway asociado y la red local (remota) contiene un dispositivo de gateway de cliente que deberá configurarse para activar la conexión de AWS Site-to-Site VPN. El direccionamiento para que el tráfico procedente de la VPC vinculada a su red ha de definirse para poder direccionar al virtual private gateway.

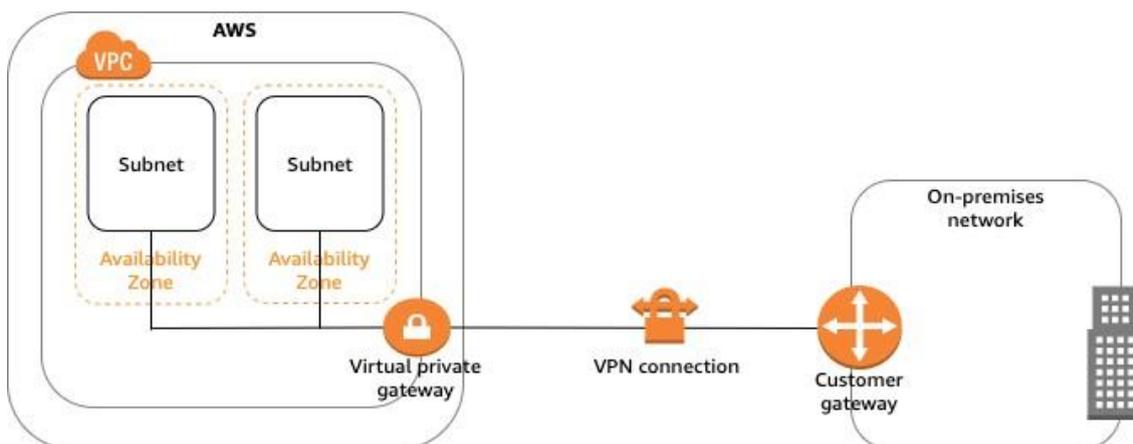


Fig. 6 - Conexión única AWS Site-to-Site VPN

Conexión de AWS Site-to-Site VPN con AWS Transit Gateway

AWS Transit Gateway es un elemento de red de AWS que permite mayor control del tráfico en entornos híbridos. Permite una conectividad y enrutamiento eficiente tanto entre redes de AWS (VPC a VPC) como entre centros de datos físicos y ubicaciones remotas. AWS Transit Gateway también mejora la seguridad al permitir la segmentación entre zonas de seguridad aislando y controlando tráfico a través de múltiples tablas de rutas. Para conocer más detalles sobre este recurso puede consultar la documentación de AWS Transit Gateway en el siguiente enlace: [¿Qué es un Transit Gateway? - Amazon VPC](#)

En el escenario de VPN con AWS Transit Gateway, la VPC dispone de transit gateway y la red local (remota) contiene un dispositivo de gateway de cliente que deberá configurarse para activar la conexión de AWS Site-to-Site VPN. Se deberá configurar el direccionamiento para que el tráfico procedente de la VPC vinculada a la red se dirija a la transit gateway. AWS habilita por defecto dos túneles redundantes en activo-pasivo, lo que garantiza la alta disponibilidad de los enlaces VPN.

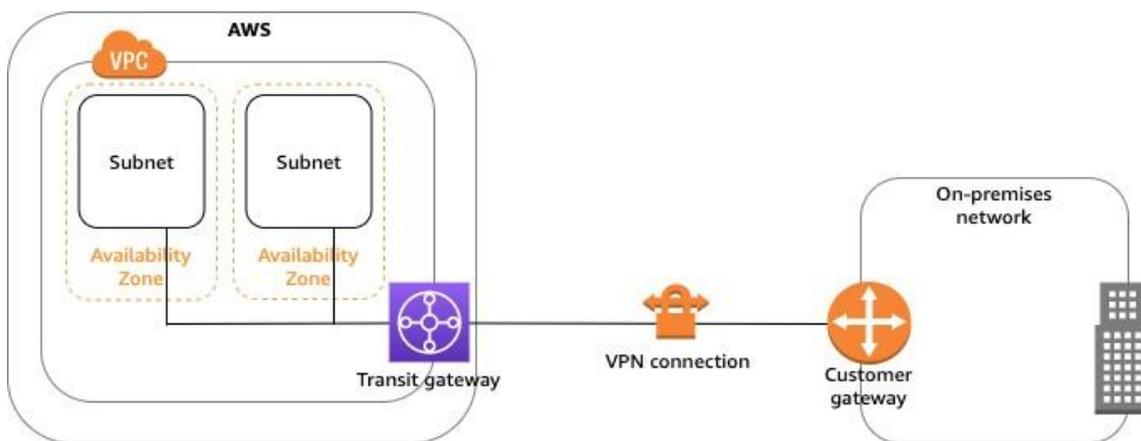


Fig. 7 - Conexión AWS Site-to-Site VPN con transit GW

Conexiones múltiples de AWS Site-to-Site VPN

En este caso, la VPC tiene asociada un virtual private gateway y hay varias conexiones de Site-to-Site VPN con distintas ubicaciones locales. Se configura el direccionamiento para que el tráfico procedente de la VPC vinculada a su red se dirija a la virtual private gateway.

También se puede utilizar esta situación para crear conexiones de AWS Site-to-Site VPN con varias ubicaciones geográficas y proporcionar una comunicación segura entre sitios.

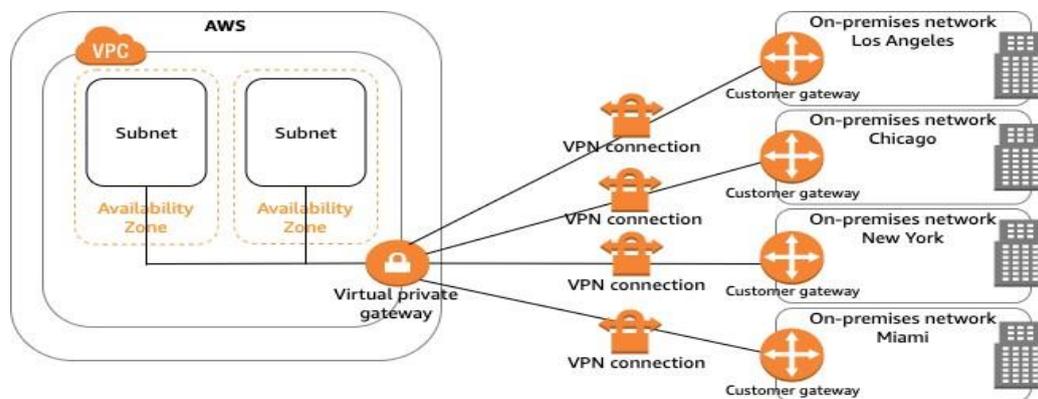


Fig. 8 – Conexiones múltiples de Site-to-Site VPN

Como se detallará más adelante en esta guía (sección 3.1.3 *Continuidad del servicio*), si se crean varias conexiones de AWS Site-to-Site VPN con una única VPC, es posible (y recomendable) configurar un segundo gateway de cliente para crear una conexión redundante con la misma ubicación externa.

Para obtener más detalles sobre estos escenarios y los pasos necesarios para configurarlos, puede consultarse la siguiente documentación de AWS: [Ejemplos de una conexión única y una conexión múltiple de AWS Site-to-Site VPN - AWS Site-to-Site VPN](#)

Esta topología se apoya en la arquitectura de AWS VPN CloudHub. Se puede consultar la siguiente documentación para más detalles sobre dicha arquitectura: [Comunicaciones seguras entre sitios mediante VPN CloudHub - AWS Site-to-Site VPN](#)

AWS VPN CloudHub

Si se tienen varias conexiones de AWS Site-to-Site VPN, es posible proteger la comunicación entre sitios con AWS VPN CloudHub. Esto permite que los sitios remotos puedan comunicarse entre sí y no solo con la VPC. AWS VPN CloudHub funciona con un modelo radial sencillo que puede utilizar con o sin VPC. Este diseño es perfecto cuando existen varias sucursales y conexiones a Internet y se desea implementar un sistema radial cómodo y potencialmente de bajo costo para la conectividad principal o auxiliar entre las sucursales remotas. Se puede encontrar más información sobre AWS VPN CloudHub en la documentación de AWS. [AWS VPN CloudHub](#)

AWS Accelerated Site-to-Site VPN: AWS Transit Gateway

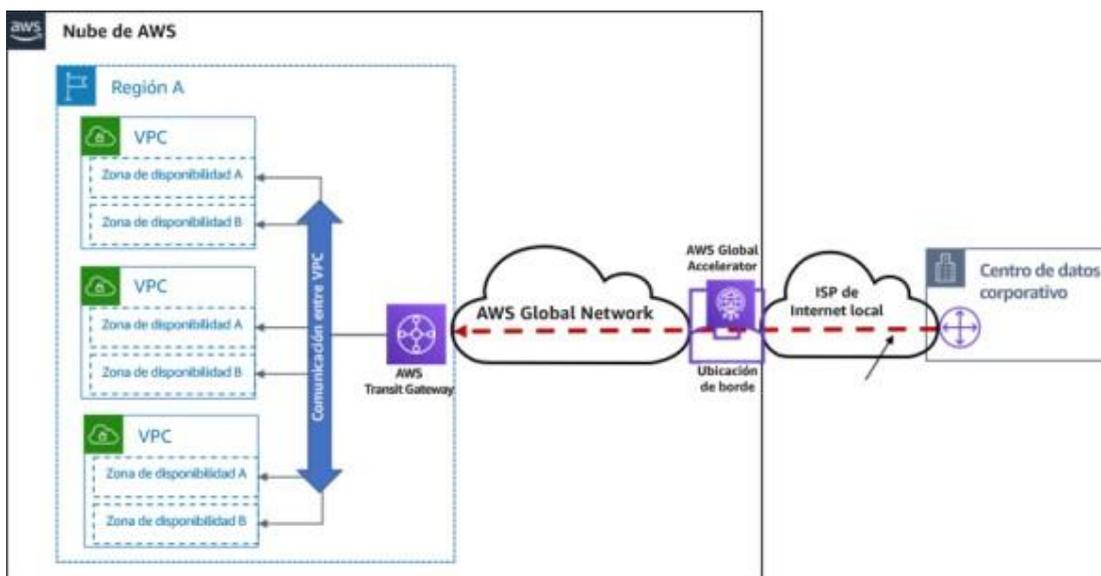


Fig. 9 - VPN administrada de AWS: AWS Transit Gateway, una sola región de AWS

AWS Accelerated Site-to-Site VPN (conexión de VPN acelerada) utiliza AWS Global Accelerator para direccionar el tráfico que se transmite desde la red local hasta la ubicación de AWS que está más próxima al dispositivo de gateway de cliente. AWS Global Accelerator optimiza la ruta de red utilizando la red global de AWS, que está libre de congestiones, para direccionar el tráfico al punto de enlace que ofrece el mejor rendimiento de las aplicaciones.

Recomendaciones para el control de acceso – AWS VPN

La autenticación de túneles punto a punto puede autenticarse en AWS con claves compartidas previamente (pre-shared keys) o bien con certificados.

- En el caso de utilizar certificados, se hace uso del servicio [AWS Certificate Manager](#) junto con [Private CA](#) para la gestión y generación de certificados.

Private Certificate Authority (CA) es un servicio de CA privadas que extiende las capacidades de administración de certificados de AWS Certificate Manager (ACM) a certificados públicos y privados.

- En caso de no utilizar certificados a través de AWS Certificate Manager o Private CA, se debe de usar claves compartidas.

Es importante proteger adecuadamente las claves y certificados empleados en la identificación de los distintos actores de una comunidad VPN, por lo que ante las primeras sospechas de filtración de estas se deberá:

- Aplicar inmediatamente procedimientos para su subsanación. El método que se utilice depende de la opción de autenticación que haya utilizado para los túneles de la VPN.
- Pueden utilizarse las características de AWS Identity and Access Management (AWS IAM) para permitir que otros usuarios, servicios y aplicaciones usen sus recursos de AWS total o parcialmente sin necesidad de compartir sus credenciales de seguridad.

Es recomendable, asimismo, la rotación de los mecanismos de autenticación empleados en la VPN:

- Las opciones de los túneles de la conexión de AWS Site-to-Site VPN permiten especificar una nueva clave de Internet Key Exchange previamente compartida para cada túnel, siendo recomendable la modificación de estas claves cada cierto tiempo. También es posible eliminar la conexión de Site-to-Site VPN temporalmente sin que para ello sea necesario eliminar la VPC ni la virtual private gateway. Posteriormente, se crearía una nueva conexión de Site-to-Site VPN utilizando la misma virtual private gateway y se configurarían las nuevas claves del dispositivo de gateway de cliente.
- En caso de utilizar certificados, para su rotación se deberá seleccionar la opción *Rotate Tunnel Certificates* en el apartado *Actions* del panel de navegación de Site-To-Site VPN, tal y como se explica en el siguiente [documento](#).
- Para cambiar el certificado en el dispositivo de Gateway de cliente se deberá crear un nuevo certificado y agregarlo al dispositivo Gateway. Del mismo modo, ante sospechas de filtración se deberá aplicar un cambio del certificado.

De forma predeterminada, los usuarios de AWS IAM no tienen permiso para crear, ver ni modificar recursos de AWS. Para permitir que un usuario de AWS IAM tenga acceso a determinados recursos, como las conexiones, las virtual private gateways y las gateways de cliente de AWS Site-to-Site VPN, así como para realizar tareas, se deberá definir una política de AWS IAM que conceda los permisos necesarios a los usuarios, teniendo en cuenta en todo caso los requisitos y las recomendaciones del apartado Control de Acceso [op.acc] de la Guía **CCN-STIC 887A Guía de configuración segura para AWS**.

AWS Site-to-Site VPN forma parte de Amazon VPC, que comparte su espacio de nombres de API con Amazon EC2. Para trabajar con conexiones de AWS Site-to-Site VPN, virtual private gateways y gateways de cliente, pueden aprovecharse las

siguientes políticas gestionadas:

- PowerUserAccess
- ReadOnlyAccess
- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess

Se recomienda restringir los permisos a usuarios para utilizar la acción `ec2:DescribeVpnConnections`. Esta acción permite a los usuarios ver la información de configuración de la gateway de cliente sobre las conexiones AWS Site-to-Site VPN de su cuenta.

AWS Site-to-Site VPN utiliza roles vinculados a servicios con los permisos que necesita para llamar a otros servicios de AWS en su nombre. Cuando se emplea una conexión de Site-to-Site VPN que utiliza la autenticación basada en certificados, AWS Site-to-Site VPN utiliza un rol vinculado a servicios llamado `AWSServiceRoleForVPC2SVPN` para invocar las siguientes acciones de AWS Certificate Manager (ACM) en su nombre:

- `acm:ExportCertificate`
- `acm:DescribeCertificate`
- `acm:ListCertificates`
- `acm-pca:DescribeCertificateAuthority`

Para asegurar que este rol no tenga usos inadecuados se debe:

- Borrar cualquier rol cuando ya no se precise utilizar más conexiones de VPN basadas en certificados.
- Como buena práctica, no se debe tener funcionalidades habilitadas que no se necesiten.
- Disponer de políticas de las AWS VPN que tengan exclusivamente las redes con las que se va a establecer la conectividad y evitar políticas genéricas basadas en routing donde se pierde el control granular de las redes permitidas en los SA (asociación de seguridad) de la VPN. Esto evita establecer conectividad con segmentos de red que no lo precisan (principio de mínimo privilegio).

Recomendaciones para el inventariado de activos – AWS VPN

En AWS es posible etiquetar conexiones AWS VPN punto a punto, puertas de enlace privadas virtuales y puertas de enlace de clientes en el momento de su creación. Es posible hacer esto al crear estos recursos a través de AWS Cloud Development Kit(CDK) o AWS Command Line Interface (CLI).

Al etiquetar los recursos en el momento de la creación, se elimina la necesidad de ejecutar scripts de etiquetado personalizados después de la creación del recurso. Además de ello, es posible establecer permisos a nivel de recursos al usar las API de VPN AWS site-to-site, lo que permite implementar políticas de seguridad más sólidas al brindar un control más granular sobre quién tiene acceso a estas API.

También permite imponer el uso de etiquetado y controlar qué claves y valores de

etiqueta se establecen en sus recursos. Para una correcta gestión de acceso a los recursos, se debe:

- Realizar un correcto etiquetado de los recursos en el momento de su creación y usar permisos a nivel de recursos, garantizando que las conexiones VPN estén seguras al momento de la creación, y se facilite el inventariado de recursos y la generación de informes de asignación de costes más precisos.

Para más información sobre el correcto uso de etiquetas, se recomienda seguir el siguiente recurso de AWS: [AWS Tagging Best Practices](#)

Recomendaciones para el registro de la actividad – AWS VPN

El registro de la actividad de las VPNs es necesario para mantener la fiabilidad, la disponibilidad, trazabilidad y el rendimiento de la conexión de AWS Site-to-Site VPN. Es por ello por lo que se recomienda habilitar los registros de AWS Site-to-Site VPN.

Los registros de VPN se pueden habilitar durante la creación de una nueva conexión AWS Site-to-Site VPN o bien en una conexión existente.

- Para habilitar el registro en el momento de la conexión desde el panel de administración, en el apartado Tunnel Options del panel de creación de una nueva VPN se deberán especificar las opciones de VPN logging. Esta opción también se puede ejecutar desde la línea de comandos de AWS o la API, a través de las operaciones [CreateVpnConnection](#) (API de consulta de Amazon EC2) y [create-vpn-connection](#) (AWS CLI).
- Para habilitar el registro de túnel en una conexión de AWS Site-to-Site VPN existente, desde el panel de navegación, se debe buscar las conexiones AWS Site-to-Site VPN y seleccionar la VPN que se quiera modificar. A continuación, en el apartado Actions, seleccionar Modify VPN tunnel options y elegir la dirección IP de la lista VPN tunnel outside IP address, seleccionar Enable en Tunnel activity log y vincularla a un grupo de registros de Amazon CloudWatch. Del mismo modo, esta opción también se puede ejecutar a través de las operaciones [ModifyVpnConnection](#) (API de consulta de Amazon EC2) y [modify-vpn-connection](#) (AWS CLI).

Recomendaciones para la protección de claves criptográficas – AWS VPN

En los entornos de conectividad híbrida de AWS, se debe tener en cuenta la protección de las claves criptográficas utilizadas para la autenticación de los túneles VPN, tanto en el caso de claves compartidas como en el de certificados.

Desde el punto de vista de responsabilidad, el cliente es el encargado de almacenar y gestionar ya sean las claves o los certificados que se usan en el extremo del Customer Gateway, siguiendo las buenas prácticas indicadas en la **Guía de Seguridad de las TIC CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad**, al respecto de almacenes y procesos seguros que tengan en sus centros de datos propios.

En el extremo de AWS, el servicio gestionado de VPN Site-to-site es el responsable de almacenar de forma segura las claves requeridas o hacer uso de AWS Private CA, con el rol correspondiente asignado por el cliente, para el uso de certificado privado, cuando sea la opción de autenticación elegida.

Protección de claves compartidas

Para una correcta protección de claves compartidas, se recomienda hacer uso concreto o combinación de servicios que ofrece AWS como AWS [Systems Manager Parameter Store](#) y [AWS KMS](#). Con Parameter Store, pueden crearse parámetros de cadenas seguras, que son parámetros que tienen un nombre en texto no cifrado y un valor de parámetro cifrado. Parameter Store utiliza AWS KMS para cifrar y descifrar los valores de los parámetros secure string. Puede obtener más información en el siguiente documento del fabricante: [Protección de los datos en AWS Systems Manager](#).

Protección de certificados

Para la generación y gestión de certificados se deberá usar AWS Certificate Manager (ACM) junto con AWS Private CA.

Estos certificados pueden ser empleados en la autenticación de túneles VPN. La autenticación y el control de acceso a este servicio es responsabilidad del usuario y deberá implementar las buenas prácticas de seguridad descritas por el fabricante en el siguiente documento: [Identity and Access Management para AWS Certificate Manager - AWS Certificate Manager](#)

Recomendaciones para la continuidad de servicio – AWS VPN

- Deberá definirse la conectividad de VPN con alta disponibilidad para protegerse frente a la pérdida de conectividad que se produciría si un dispositivo de Gateway de cliente dejase de estar disponible., además de permitir mantener la conectividad cuando se hagan tareas de mantenimiento en cualquiera de los dos extremos de la conexión.
- Además, deberá tener en cuenta la gestión del ciclo de vida de la VPN. Encontrará más información sobre este ciclo de vida en [Control del ciclo de vida del punto de conexión del túnel](#).

Alta disponibilidad de VPN

Para protegerse frente a la pérdida de conectividad que se produciría si un dispositivo de gateway de cliente dejara de estar disponible, puede configurarse una segunda conexión de AWS Site-to-Site VPN con la VPC y el virtual private gateway utilizando otro dispositivo de gateway de cliente. El uso de dispositivos de gateway de cliente y conexiones de AWS Site-to-Site VPN redundantes permite realizar tareas de mantenimiento en uno de los dispositivos y, a la vez, mantener

el flujo de tráfico a través de la conexión de AWS Site-to-Site VPN de la segunda gateway de cliente.

En el siguiente diagrama, se muestran los dos túneles de cada conexión de AWS Site-to-Site VPN y las dos gateways de cliente.

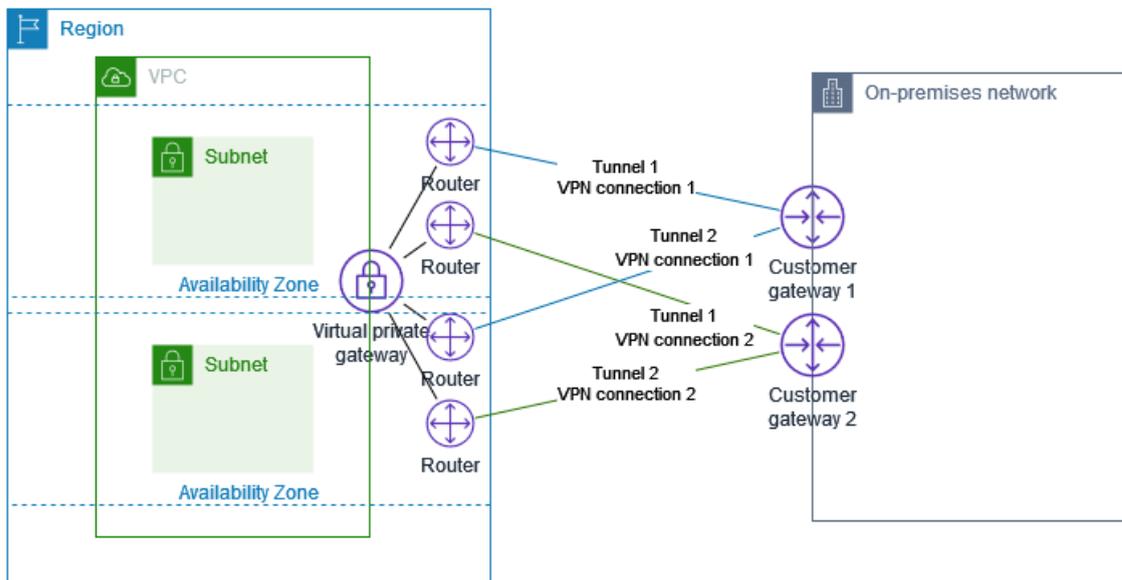


Fig. 10 - Ejemplo de interconexión de centro de datos físico con AWS utilizando VPNs en HA

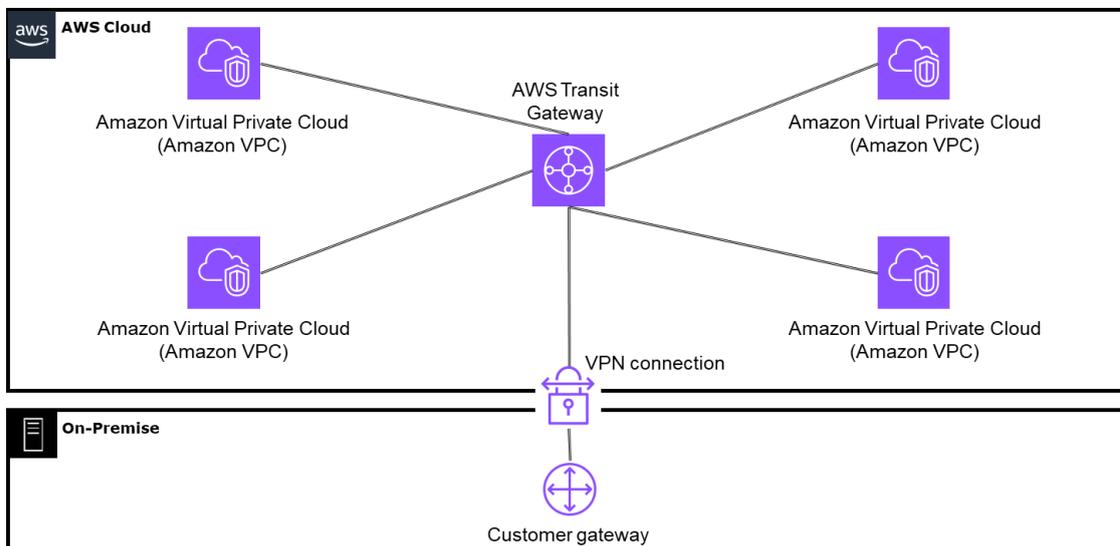


Fig. 11 - Ejemplo de interconexión de centro de datos físico con AWS utilizando VPNs y TGW

Para conseguir esta arquitectura se debe:

- Configurar otra conexión de AWS Site-to-Site VPN utilizando el mismo virtual private gateway y creando una nueva gateway de cliente. La dirección IP de la gateway de cliente de la segunda conexión de AWS Site-to-Site VPN debe estar disponible públicamente.
- Configurar el otro dispositivo de gateway de cliente. Ambos dispositivos

deben anunciar los mismos rangos de IP al virtual private gateway . Se emplea el direccionamiento de BGP para determinar la ruta del tráfico. Si se produce un error en un dispositivo de gateway de cliente, el virtual private gateway dirigirá todo el tráfico al dispositivo de gateway de cliente que sí funciona.

Las conexiones de AWS Site-to-Site VPN de direccionamiento dinámico utilizan el protocolo de enrutamiento BGP y su definición de sistemas autónomos (ASN) para intercambiarla información de enrutamiento entre las gateways de cliente y las virtual private gateways. En las conexiones de AWS Site-to-Site VPN con enrutamiento estático, es necesario que las rutas estáticas de la red remota se escriban en el lado del gateway de cliente.

La información acerca de las rutas que se especifica manualmente y que anuncia mediante BGP permite a los gateways de ambos extremos determinar qué túneles están disponibles para, de este modo, redireccionar el tráfico en caso de error. Por lo tanto, se recomienda configurar su red para que utilice la información de direccionamiento que proporciona BGP (si está disponible) y seleccionar una ruta alternativa. La configuración exacta dependerá de la arquitectura de la red.

BGP es un protocolo de puerta de enlace (EGP) exterior que se utiliza para intercambiar información de encaminamiento entre enrutadores de diferentes sistemas autónomos (SA). BGP utiliza la información de enrutamiento para mantener una base de datos con información sobre el alcance de la red, que intercambia con otros sistemas BGP. BGP usa la información de disponibilidad de la red para construir un gráfico de conectividad, lo que permite a BGP eliminar los bucles de enrutamiento y aplicar las decisiones de la Directiva en el nivel sistema autónomo.

Para conocer más detalles de cómo AWS aprovecha este protocolo para sus distintas soluciones de conectividad se puede consultar el siguiente documento: [Políticas de direccionamiento y comunidades de BGP - AWS Direct Connect](#)

Esto último es importante ya que las mismas prioridades en ambos enlaces podría dar lugar a rutas asimétricas y pérdida de paquetes. Para más información sobre las prioridades de rutas se puede consultar el siguiente documento: [Configurar tablas de enrutamiento - Amazon Virtual Private Cloud](#)

Recomendaciones para la monitorización – AWS VPN

Para una correcta recopilación de datos relacionados con los servicios de conectividad, AWS ofrece el servicio Amazon CloudWatch que puede explotarse con la herramienta de monitorización automatizada de **Amazon CloudWatch Metrics** combinado con **Amazon CloudWatch Alerts**.

Con Amazon CloudWatch Alerts se puede observar una única métrica durante un periodo de tiempo que especifique. También permite realizar una o varias acciones según el valor de la métrica con respecto a un umbral dado durante varios períodos de tiempo. La acción es una notificación enviada a un topic de Amazon SNS. Las alarmas de Amazon CloudWatch no invocan acciones, simplemente por tener un

estado determinado. Es necesario que el estado haya cambiado y se mantenga durante un número especificado de períodos. Se puede conocer más detalles sobre las opciones disponibles en esta herramienta y su activación en el siguiente documento: [Monitoreo de túneles de VPN mediante Amazon CloudWatch](#).

AWS Health

También es posible monitorizar las conexiones de VPN mediante eventos de AWS Health. AWS Site-to-Site VPN envía automáticamente notificaciones a AWS Health Dashboard, que funciona con la API de AWS Health. El panel no requiere instalación y está listo para que lo utilicen los usuarios de AWS autenticados. Se puede configurar varias acciones en respuesta a las notificaciones de eventos a través de AWS Health Dashboard.

AWS Health Dashboard dispone de los siguientes tipos de notificaciones para las conexiones de VPN:

- Notificaciones de sustitución de puntos de enlace de un túnel.
- Notificaciones de VPN con un solo túnel

Se puede ampliar la información en el siguiente documento. [Monitoreo de las conexiones de VPN mediante eventos de AWS Health](#)

Igualmente habrá de tenerse en cuenta el servicio de **VPC Flowlogs** para la correcta monitorización del tráfico entrante a las VPCs que interactúan en un entorno de conectividad híbrida.

También es posible consultar los logs de AWS Site-to-Site VPN. Los logs de AWS Site-to-Site VPN proporcionan una mayor visibilidad de las implementaciones de Site-to-Site VPN. Con esta característica se tiene acceso a los registros de conexión de Site-to-Site VPN que proporcionan detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones de intercambio de claves de Internet (IKE) y los mensajes del protocolo de detección de pares muertos (DPD). Se puede encontrar más información en [Registros de AWS Site-to-Site VPN](#).

Recomendaciones para la protección de la confidencialidad – AWS VPN

Las conexiones de AWS Site-to-Site VPN conectan de forma privada la VPC a la red local. Los datos que se transfieren entre la VPC y la red se direccionan a través de una conexión de VPN cifrada para mantener la confidencialidad y la integridad de los datos en tránsito. AWS da soporte a conexiones de VPN IPsec. IPsec es un conjunto de protocolos que se usa para proteger las comunicaciones por protocolo de Internet (IP) mediante la autenticación y el cifrado de todos los paquetes IP de una transmisión de datos.

Cada conexión de AWS Site-to-Site VPN consta de dos túneles de VPN IPsec cifrados que conectan AWS y la red. El tráfico de cada túnel puede cifrarse con AES128 o

AES256 y usar protocolos Diffie-Hellman para el intercambio de claves, lo que proporciona una confidencialidad directa total. AWS autentica con las funciones de hash SHA1 o SHA2. Es recomendable AES256 siempre que sea soportado por todos los elementos de la VPC, y del Gateway de cliente.

Las instancias de la VPC no necesitan una dirección IP pública para conectarse a los recursos del otro extremo de la conexión de AWS Site-to-Site VPN. Las instancias pueden direccionar el tráfico de Internet hacia la red de las instalaciones a través de la conexión de AWS Site-to-Site VPN. A continuación, se puede obtener acceso a Internet a través de los puntos de tráfico salientes y de los dispositivos de monitoreo y seguridad de la red.

3.2.2. AWS Direct Connect

AWS Direct Connect es una solución que facilita el establecimiento de una conexión de red exclusiva entre el entorno local y de AWS. AWS cuenta con múltiples AWS Direct Connect Locations en todo el mundo donde a través de su proveedor de comunicaciones conectará sus instalaciones directamente a los servicios de AWS sin pasar por internet. Con AWS Direct Connect es posible establecerse una conectividad privada entre AWS y el centro de datos, oficina o entorno de co-ubicación, que emplee la organización, lo que en muchos casos puede reducir los costos de red, aumentar el rendimiento del ancho de banda y suministrar una experiencia de red más estable que las conexiones basadas en Internet. Es importante señalar que para un mayor rendimiento de AWS Direct Connect se utilicen las dos AWS Direct Connect Locations disponibles actualmente España que serían:

- Equinix ITConic MD2, Madrid, España
- Interxion MAD2, Madrid, España

AWS Direct Connect permite establecer una conexión de red dedicada entre la red del cliente y una de las de AWS Direct Connect Locations, que será posible hacerlo bien a través un partner de comunicaciones de AWS o bien a través de un cable físico desde un router al router de la AWS Direct Connect Locations que se haya seleccionado. Gracias al uso de redes basadas en el estándar 802.1Q, esta conexión exclusiva se puede dividir en varias interfaces virtuales, también llamadas VIF. Una interfaz virtual (VIF) es necesaria para acceder a los servicios de AWS, y existen varias opciones de interfaz virtual.

- **Interfaz virtual privada:** una interfaz virtual privada se debe utilizar para acceder a una Amazon VPC mediante direcciones IP privadas.
- **Interfaz virtual pública:** una interfaz virtual pública puede acceder a todos los servicios AWS públicos mediante direcciones IP públicas.
- **Interfaz virtual de tránsito:** se debe utilizar una interfaz virtual de tránsito para acceder a una o más pasarelas de tránsito de Amazon VPC asociadas a las puertas de enlace de Direct Connect. Puede utilizar interfaces virtuales de tránsito con cualquier conexión AWS Direct Connect dedicada o alojada de cualquier velocidad

Esto permite utilizar la misma conexión para obtener acceso a recursos públicos como, por ejemplo, objetos almacenados en Amazon S3 utilizando un espacio de direcciones IP públicas y a recursos privados, por ejemplo, instancias de Amazon EC2 que se ejecuten dentro de una Amazon Virtual Private Cloud (VPC) utilizando un espacio de IP privado al tiempo que se mantiene la separación de red entre los entornos públicos y privados. Las interfaces virtuales se pueden volver a configurar en cualquier momento para que satisfagan necesidades concretas a medida que cambian.

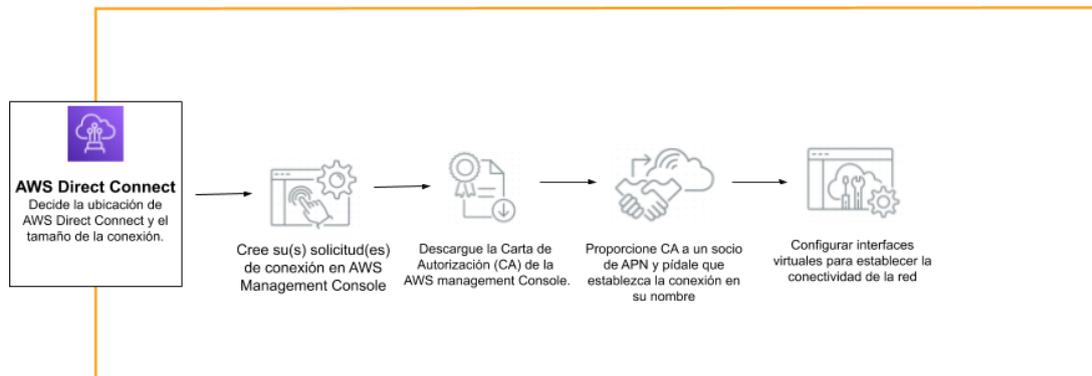


Fig. 12 - Representación gráfica de los pasos necesarios para un alta de AWS Direct Connect

Gateway de AWS Direct Connect

Los gateways de AWS Direct Connect se emplean para conectar VPCs. Los gateways de AWS Direct Connect pueden asociarse cualquiera de los siguientes gateways:

- Transit Gateway cuando tiene varias instancias de VPCs en la misma región
- Un virtual private gateway

Un gateway de AWS Direct Connect es un recurso disponible en todo el mundo. Se puede crear el gateway de AWS Direct Connect en cualquier región y obtener acceso a ella a nivel global. Puede utilizar un gateway de AWS Direct Connect en los diversos escenarios tal y como se documenta de manera actualizada en el siguiente [recurso](#):

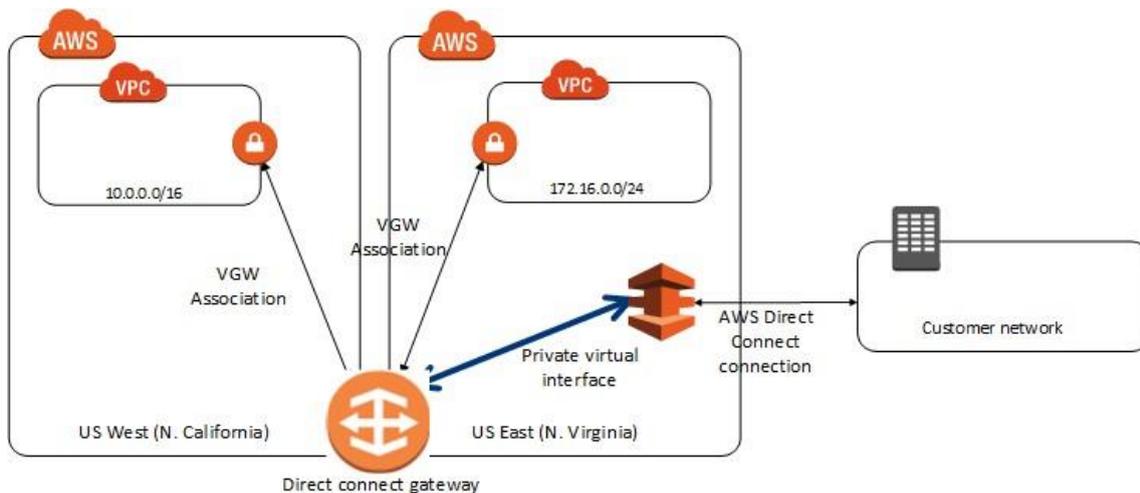


Fig. 13 - Ejemplo de uso de Gateway de AWS Direct Connect para interconexión con VPCs

AWS Direct Connect ofrece múltiples opciones para su despliegue en función de las necesidades y topología del cliente. A continuación, se detalla un ejemplo sencillo para comprender los componentes y flujos que aparecen en una arquitectura con AWS Direct Connect:

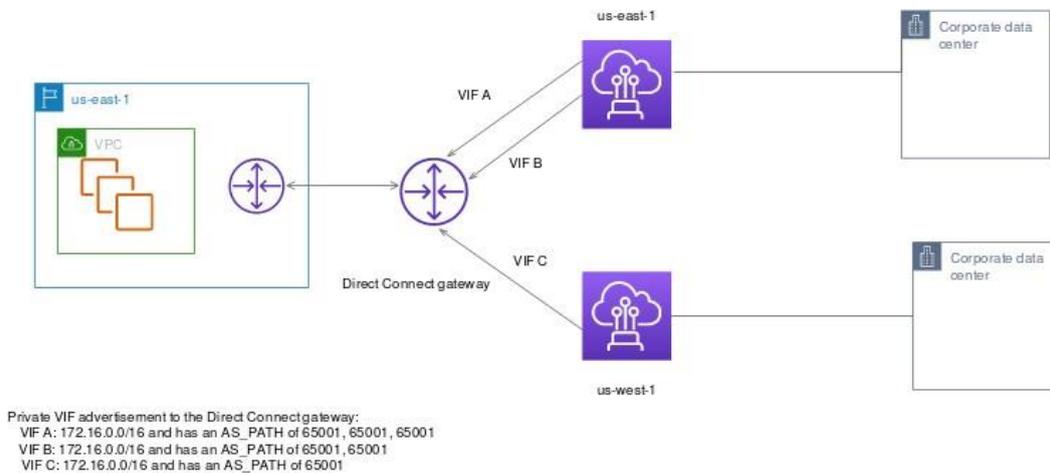


Fig. 14 - Representación gráfica de AWS Direct Connect Gateway usado desde dos conexiones/regiones diferentes

Este esquema representa una configuración donde la región de origen (us-east-1) de la ubicación 1 de AWS Direct Connect es la misma que la región de origen de la VPC. La ubicación 2 de AWS Direct Connect redundante es una región diferente (us-west-1). Hay dos interfaces virtuales (en inglés Virtual Interfaces - VIFs) privados desde la ubicación 1 de AWS Direct Connect a la gateway de AWS Direct Connect. Hay una VIF privada desde la ubicación 2 de AWS Direct Connect a la gateway de AWS Direct Connect.

Para que AWS dirija el tráfico a través de VIF B antes de VIF A, establezca el atributo AS_PATH de VIF B en un valor inferior al atributo VIF AS_PATH.

Las VIFs tienen las siguientes configuraciones:

- VIF A (en us-east-1) anuncia 172.16.0.0/16 y tiene un atributo AS_PATH de 65001, 65001, 65001
- VIF B (en us-east-1) anuncia 172.16.0.0/16 y tiene un atributo AS_PATH de 65001, 65001
- VIF C (en us-west-1) anuncia 172.16.0.0/16 y tiene un atributo AS_PATH de 65001

Para más información sobre AWS Direct Connect puede consultar la documentación del fabricante [AWS Direct Connect](#)

A continuación, se presentan diferentes modelos de conectividad para AWS Direct Connect:

AWS DX: DXGW con AWS Transit Gateway, una sola región

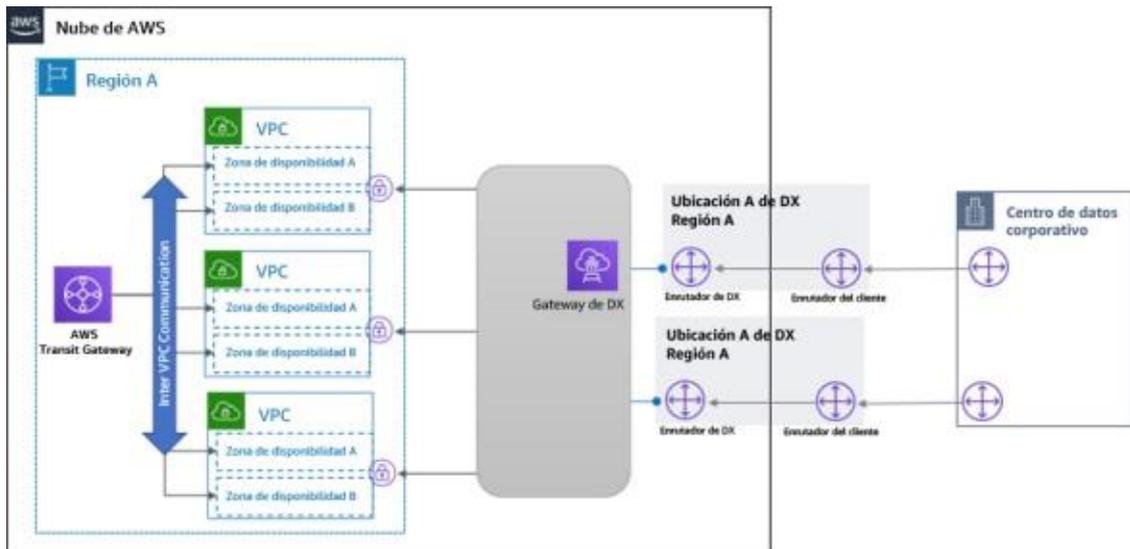


Fig. 15 – AWS DX: DXGW con VGW, una sola región de AWS

Con este modelo de arquitectura se obtienen las siguientes mejoras:

- Brinda la posibilidad de conectarse a conexiones DX o VPC en otras futuras regiones.
- Ofrece conmutación por error automatizada, con enrutamiento dinámico(BGP).
- Con AWS Transit Gateway conectada a las VPC, se puede lograr conectividad de malla completa o conectividad de malla parcial entre las VPC.

AWS DX: DXGW con AWS Transit Gateway, varias regiones y AWS Public Peering

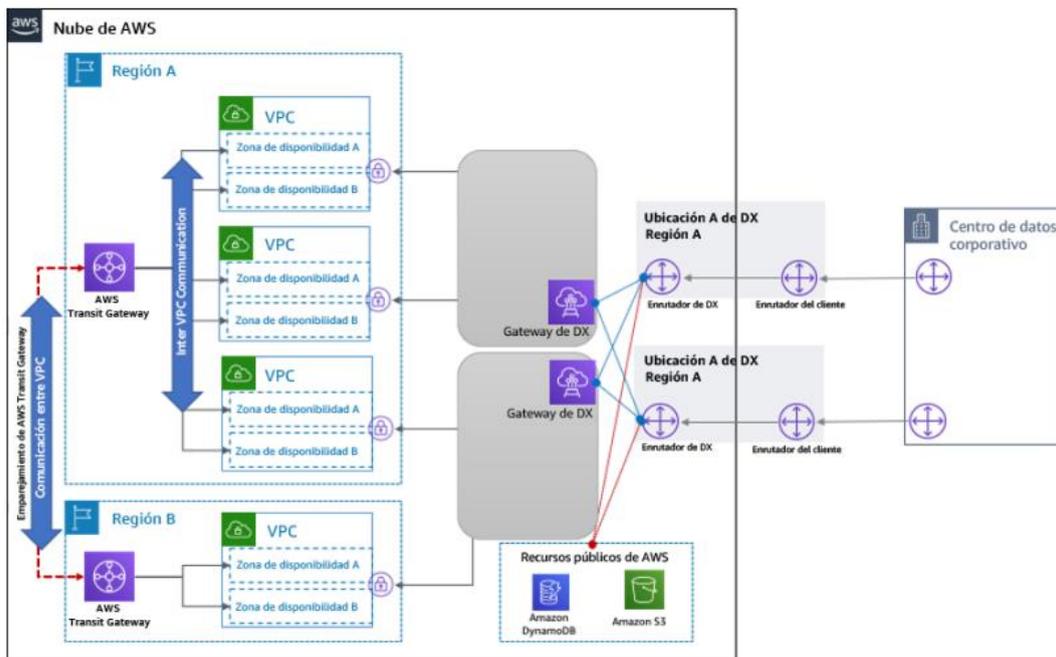


Fig. 16 – DXGW con AWS Transit Gateway, varias regiones y AWS Public Peering

Con este modelo de arquitectura se obtienen las siguientes mejoras:

- Brinda la posibilidad de conectarse a conexiones DX o VPC en otras futuras regiones.
- Con AWS Transit Gateway conectada a las VPC, se puede lograr conectividad de malla completa o conectividad de malla parcial entre las VPC.
- Comunicación entre VPC y entre regiones facilitada por el emparejamiento de AWS Transit Gateway.
- Permite conectarse a los endpoints/servicios públicos usando la misma conexión y sin necesidad de ir por internet, con VIFs públicas.

AWS DX: DXGW con AWS Transit Gateway, varias regiones y VIF pública de AWS

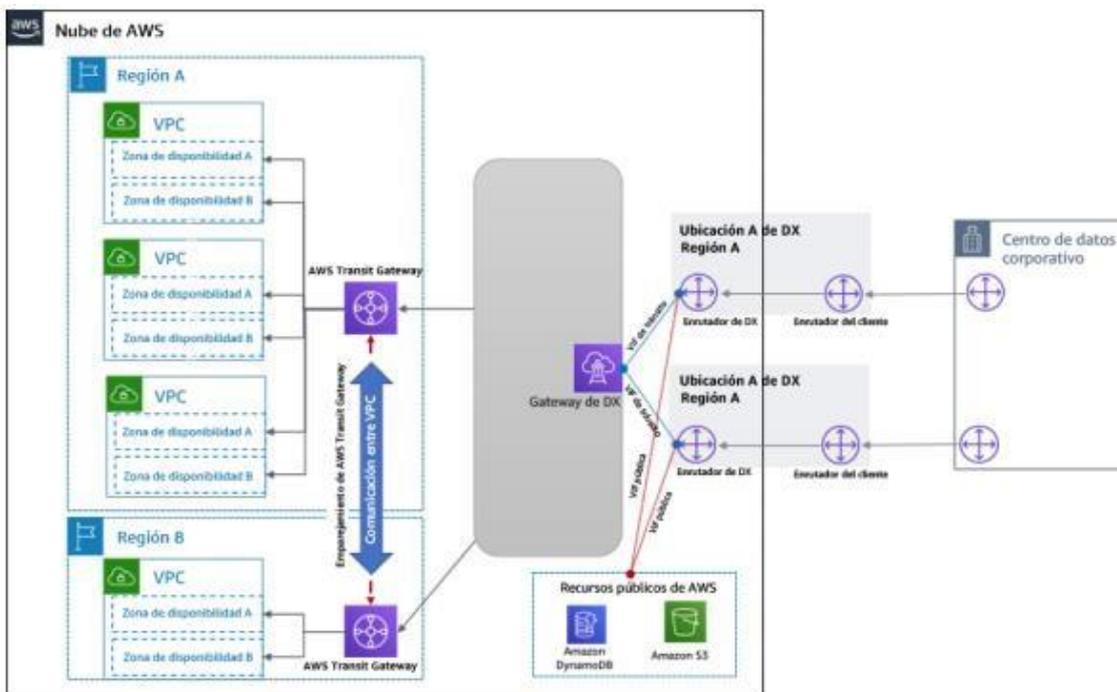


Fig. 17 – DXGW con AWS Transit Gateway, varias regiones y VIF pública de AWS

Con este modelo de arquitectura se obtienen las siguientes mejoras:

- Utiliza el VIF público de AWS DX para acceder a los recursos públicos de AWS, como Amazon S3, con DynamoDB directamente a través de las conexiones de AWS DX.
- Ofrece la posibilidad de conectarse a VPC y/o conexiones DX en otras regiones en el futuro.
- Se obtiene la capacidad de lograr una conectividad de malla total o parcial entre las VPC, con AWS Transit Gateway conectado a las VPC.

AWS DX: DXGW con AWS Transit Gateway, varias regiones

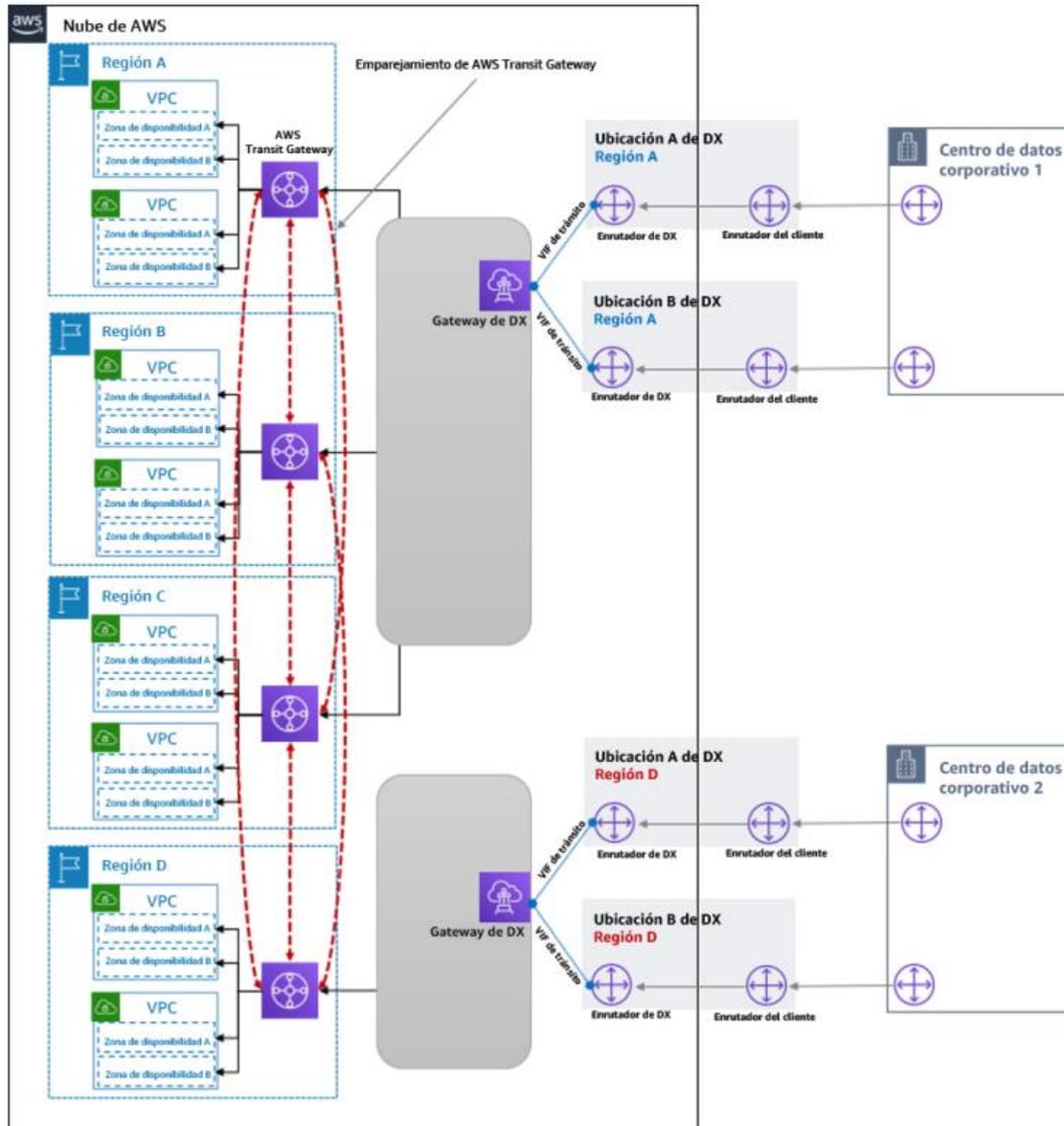


Fig. 18 – DXGW con AWS Transit Gateway, varias regiones

Con este modelo de arquitectura se obtienen las siguientes mejoras:

- Se obtiene un menor coste operativo.
- Brinda la posibilidad de conectarse a conexiones DX o VPC en otras futuras regiones.
- Con AWS Transit Gateway conectada a las VPC, se puede lograr conectividad de malla completa o conectividad de malla parcial entre las VPC.
- El emparejamiento de AWS Transit Gateway facilita la comunicación de VPC entre regiones.
- Ofrece opciones de diseño flexibles para integrar los dispositivos virtuales SD-WAN y de seguridad de terceros en AWS Transit Gateway.

VPN como conexión de respaldo

Los beneficios de esta configuración con redundancia de enlaces hacia AWS pueden complementarse con una conexión VPN de respaldo. Para este escenario habrá de tenerse en cuenta que estos enlaces VPN soportan hasta 1.25Gbps por túnel y no implementan capacidades de ECMP (Equal Cost Multi Path) en caso de implementar múltiples túneles contra el mismo Virtual Gateway (VGW). En caso de Transit Gateway y routing dinámico sí se soporta.

Algunas observaciones para tener en cuenta de cara a definir correctamente este escenario son las siguientes:

- Utilizar el mismo Virtual Private Gateway para AWS Direct Connect y para la VPN que conectan contra la VPC.
- En caso de emplear protocolo BGP, publicar el mismo prefijo tanto por AWS Direct Connect como por VPN.
- En caso de definir una VPN estática, añadir los mismos prefijos estáticos que se estén anunciando vía AWS Direct Connect a la conexión VPN.
- En caso de publicar las mismas rutas tanto por AWS Direct Connect como por VPN el path de AWS Direct Connect deberá ser siempre la ruta con máxima prioridad.

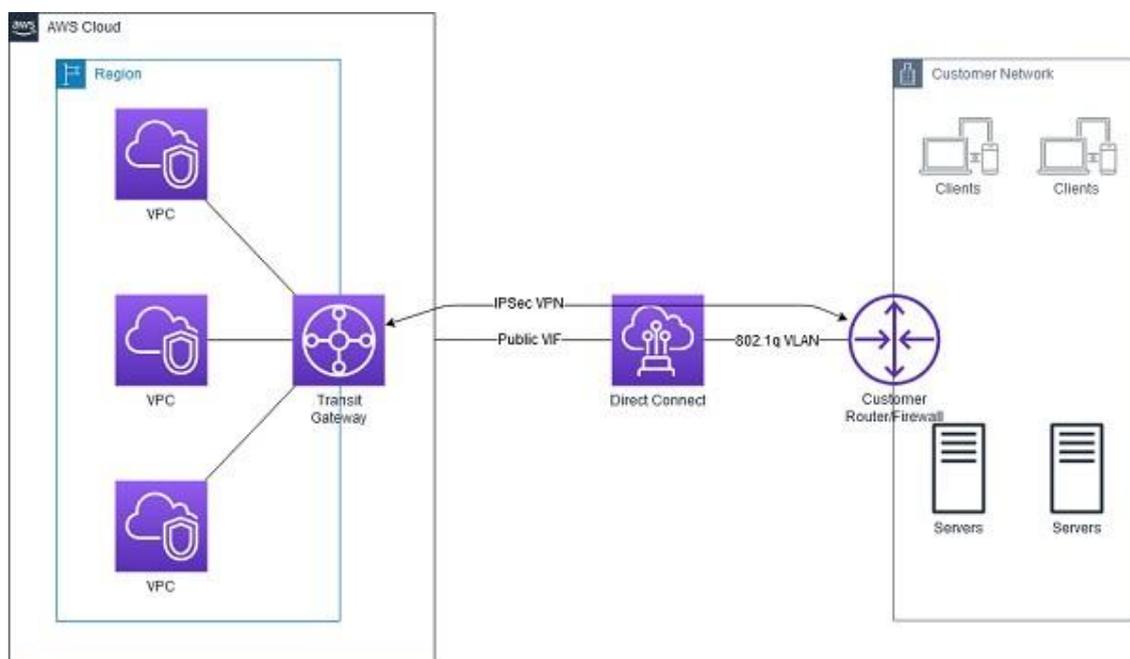


Fig.19 Ejemplo de arquitectura con AWS Direct Connect con VPN de respaldo

MACSec Support (Encryption)

MAC Security (MACSec) es un estándar IEEE que proporciona confidencialidad de datos, integridad de datos y autenticidad de origen de datos. Se puede utilizar conexiones de AWS Direct Connect que admitan MACSec para cifrar los datos desde el centro de datos corporativo a la ubicación de AWS Direct Connect.

En el siguiente diagrama, tanto la conexión dedicada como los recursos locales deben ser compatibles con MACSec. El tráfico de capa 2 que viaja a través de la conexión dedicada hacia o desde el centro de datos está encriptado.

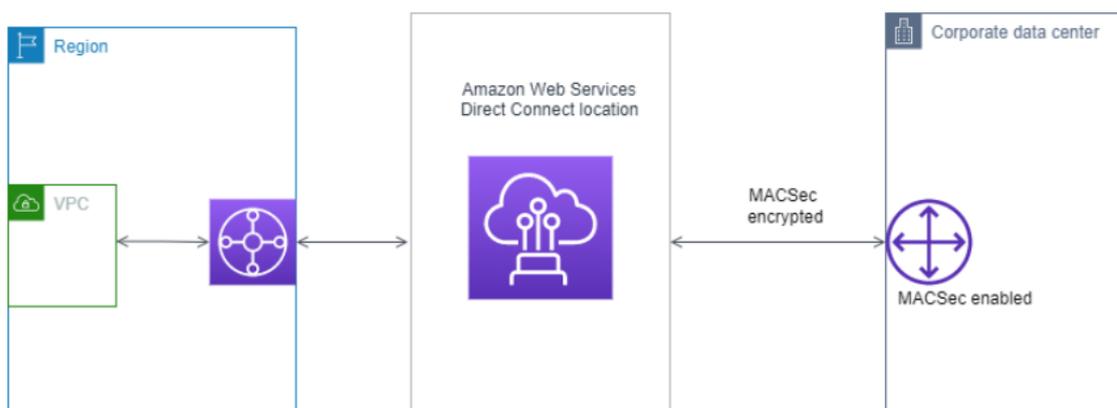


Fig. 20 – Tráfico de datos entre el centro de datos local y la VPC utilizando AWS Direct Connect y MACSec encrypted

MAC Security, sólo está disponible en España en el caso que utilice la AWS Direct Connect Location ubicada en Equinix ITConic MD2, Madrid, España.

Se puede encontrar más información sobre MACSec en [Adición de seguridad MACSec a las conexiones de AWS Direct Connect](#).

AWS SiteLink

AWS SiteLink, una nueva característica de AWS Direct Connect (DX), facilita el envío de datos desde una ubicación de AWS Direct Connect a otra, sin pasar por las regiones de AWS. AWS Direct Connect es un servicio en la nube que vincula la red corporativa hacia AWS, sin pasar por Internet para ofrecer un rendimiento más consistente y de menor latencia. Antes de AWS SiteLink, no era posible enrutar el tráfico directamente entre las ubicaciones de AWS Direct Connect. Ahora se pueden crear conexiones globales, confiables y de pago por uso entre las oficinas y los centros de datos en su red global mediante el envío de datos a través de la ruta más rápida entre las ubicaciones de AWS Direct Connect.

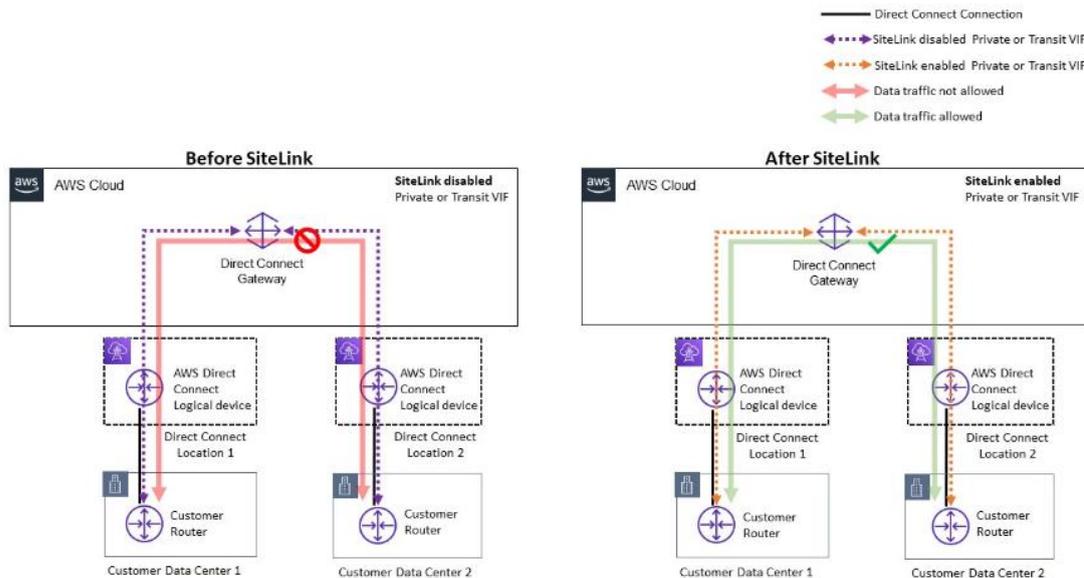


Fig. 21 – Conexiones entre centros de datos utilizando AWS SiteLink

Recomendaciones para el control de acceso – AWS Direct Connect

AWS Identity and Access Management (IAM) es un servicio de AWS que permite al administrador controlar el acceso seguro a los recursos de AWS. Los administradores de IAM son los encargados de controlar quién puede autenticarse (iniciar sesión) y ser autorizado (obtener permisos) para utilizar los recursos de AWS Direct Connect. Tanto el administrador de IAM como el administrador de servicio (AWS Direct Connect) realizarán la gestión de solicitud de permisos cuando un usuario necesite para desempeñar sus tareas un mayor número de funciones. AWS IAM es un servicio que puede utilizarse sin costo adicional.

- En lo referido con la administración del servicio AWS Direct Connect a través de AWS IAM se deberán tener en cuenta todas las exigencias documentadas en la guía **CCN STIC-887A Guía de configuración segura para AWS**.

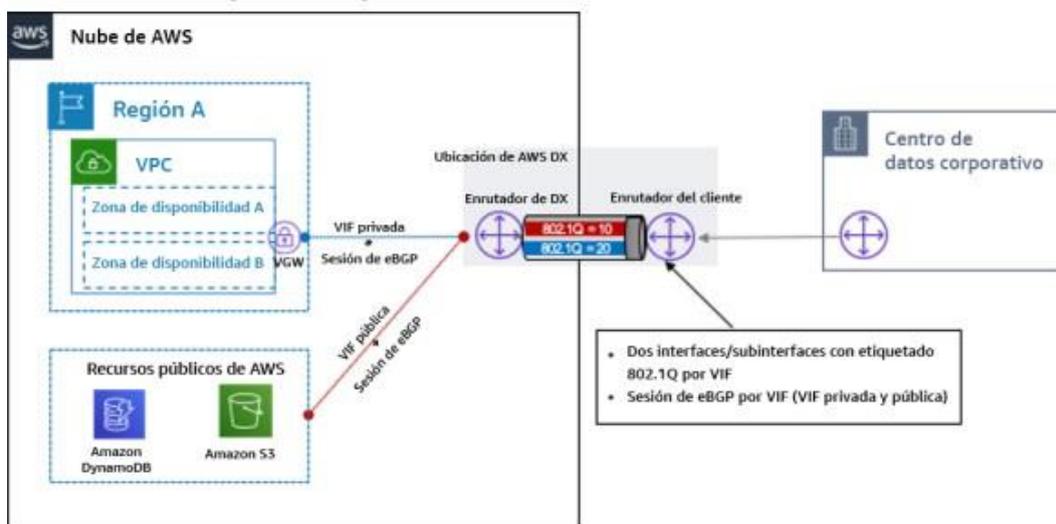


Fig. 22 - VIF privada y pública de AWS Direct Connect

Mediante el uso de políticas basadas en identidades de IAM, se pueden especificar los recursos y las acciones permitidas o denegadas, así como las condiciones en las que se permiten o deniegan las acciones. De forma predeterminada, los usuarios y roles de IAM no tienen permiso para crear, ver ni modificar recursos de AWS Direct Connect. AWS Direct Connect es compatible con acciones, claves de condiciones y recursos específicos. Para una correcta administración de las acciones se debe especificar los recursos y las acciones permitidas o denegadas, así como las condiciones en las que se permiten o deniegan dichas acciones.

El elemento acción de una política basada en la identidad de IAM describe la acción o acciones específicas que una política permite o deniega. Las acciones de las políticas generalmente tienen el mismo nombre que la operación asociada en la API. Cada acción se utiliza en una política para otorgar al usuario los permisos necesarios para llevar a cabo la operación asociada. Para garantizar la integridad de las acciones y controlar el acceso a las mismas se debe:

- Seguir el modelo de mínimo privilegio para la definición de políticas.
- Restringir los permisos de acceso a los recursos de AWS Direct Connect garantizando el acceso mínimo necesario.

Ejemplo de política restringida a la acción “describe” para AWS Direct Connect:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "directconnect:Describe*",
        "ec2:DescribeVpnGateways"
      ],
      "Resource": "*"
    }
  ]
}
```

- Evitar las políticas con comodines que puedan otorgar acceso total al servicio y recursos administrados por AWS Direct Connect.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "directconnect:*",
        "ec2:DescribeVpnGateways"
      ],
      "Resource": "*"
    }
  ]
}
```

- Especificar los diferentes recursos disponibles en AWS Direct Connect al utilizarlos en la definición de cualquier política.

Tipo de recurso	ARN
dxcon	<p>arn:\${Partition}:directconnect:\${Region}:\${Account}:dxcon/\${ConnectionId}</p> <p>\${Partition}: La partición en la que se encuentra el recurso.</p> <p>\${Region}: El espacio de nombres del servicio que identifica el producto de AWS. Por ejemplo, s3 para recursos de Amazon S3</p> <p>\${Account}: Es el ID de la cuenta de AWS sin guiones</p> <p>\${ConnectionId}: Es el Id de la conexión</p>
dxlag	<p>arn:\${Partition}:directconnect:\${Region}:\${Account}:dxlag/\${LagId}</p> <p>\${Partition}: La partición en la que se encuentra el recurso.</p> <p>\${Region}: El espacio de nombres del servicio que identifica el producto de AWS. Por ejemplo, s3 para recursos de Amazon S3</p> <p>\${Account}: Es el ID de la cuenta de AWS sin guiones</p> <p>\${LagId}: Es el ID del LAG</p>
dx-vif	<p>arn:\${Partition}:directconnect:\${Region}:\${Account}:dxvif/\${VirtualInterfaceId}</p> <p>\${Partition}: La partición en la que se encuentra el recurso.</p> <p>\${Region}: El espacio de nombres del servicio que identifica el producto de AWS. Por ejemplo, s3 para recursos de Amazon S3</p> <p>\${Account}: Es el ID de la cuenta de AWS sin guiones</p> <p>\${VirtualInterfaceId}: Es el ID de la interfaz virtual</p>
dx-gateway	<p>arn:\${Partition}:directconnect:::\${Account}:dx-gateway/\${DirectConnectGatewayId}</p> <p>\${Partition}: La partición en la que se encuentra el recurso.</p> <p>\${Region}: El espacio de nombres del servicio que identifica el producto de AWS. Por ejemplo, s3 para recursos de Amazon S3</p> <p>\${Account}: Es el ID de la cuenta de AWS sin guiones</p> <p>\${DirectConnectGatewayId}: Es el ID del AWS Direct Connect gateway</p>

Tabla 1 - Recursos disponibles en AWS Direct Connect

- Evitar el uso de comodines para referenciar a todos los recursos de AWS Direct Connect.

```
"Resource": "arn:aws:directconnect:*"
```

- Definir recursos concretos, como una interfaz, tal y como hace la siguiente descripción de recurso:

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb"
```

- Controlar los AS y el enrutamiento que se lleva por BGP (enlace descripción del protocolo), de modo que se propague el mínimo de rutas.
- Hay que asegurar que no existe redistribución de rutas/redes privadas de entornos del cliente hacia el proveedor de servicios de internet (ISP).

Además de ello, se recomienda hacer uso y consultar el listado actualizado de todas las opciones disponibles de IAM con AWS Direct Connect. Más información en: [Cómo funciona AWS Direct Connect con IAM - AWS Direct Connect](#)

Recomendaciones para el registro de la actividad – AWS Direct Connect

En cuanto al registro de la actividad de los usuarios, AWS Direct Connect está integrado en AWS CloudTrail. CloudTrail permite, de esta manera, capturar las llamadas a la API de AWS Direct Connect y registrarlas como eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de AWS Direct Connect y las llamadas de código a las operaciones de la API de AWS Direct Connect. Para poder crear un registro de seguimiento, se deberá habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3 dedicado.

Mediante la información que recopila CloudTrail, es posible determinar la solicitud que fue enviada a AWS Direct Connect, la dirección IP desde la que se realizó dicha solicitud, quién la realizó, cuándo y los detalles adicionales de la petición.

Recomendaciones para la continuidad de servicio – AWS Direct Connect

Una solución de continuidad de negocio y servicio implica el mantenimiento de la ejecución de operaciones críticas durante un fallo en los sistemas, además de mantener el acceso a los datos en caso de fallo de los servicios. Si bien AWS ofrece numerosas soluciones para conseguir este objetivo, será siempre la entidad la que defina los procedimientos y directrices para cumplir con las medidas correspondientes, pudiéndose apoyar en los servicios ofrecidos por AWS.

Las arquitecturas híbridas son un componente clave para cualquier solución de continuidad de servicio, donde la información crítica puede replicarse y almacenarse en la nube de AWS. Los datos quedan, de esta manera, disponibles en caso de pérdida del servicio a la par que se agilizan los tiempos de operación y costes en caso de fallo.

Para garantizar la continuidad de negocio en organizaciones que extienden su centro de datos físico con infraestructuras en AWS, es necesario garantizar la alta disponibilidad de las comunicaciones en ambos entornos. En este sentido, se recomienda:

- Definir la conectividad de AWS Direct Connect con alta disponibilidad.
- Complementar el enlace de AWS Direct Connect mediante el uso de una VPN de respaldo.

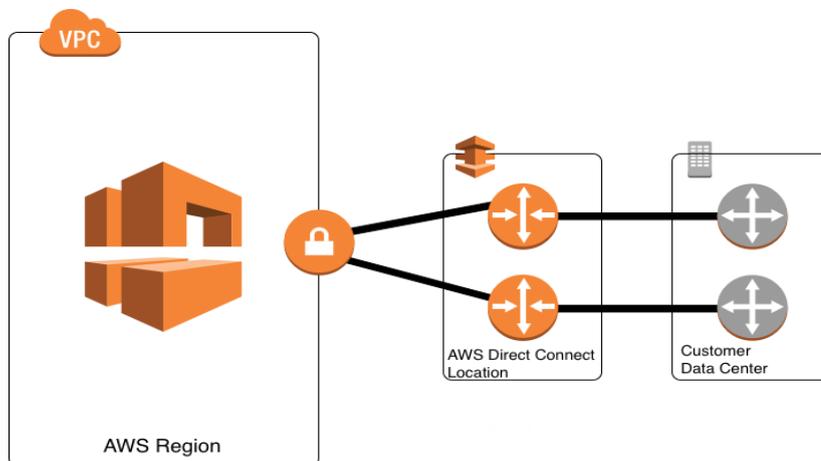


Fig. 23 - Ejemplo de interconexión de centro de datos físico con AWS utilizando AWS Direct Connect

Alta disponibilidad de AWS Direct Connect

En función de los requerimientos de continuidad de negocio de la organización y las cargas que se utilicen de AWS, para obtener la máxima resiliencia posible y garantizar el servicio de AWS Direct Connect incluso en casos de fallo de conexión contra una de las localizaciones, fallo completo de uno de los centros de datos o fallo de dispositivo de comunicaciones, se deberá:

- Desplegar conexiones contra cada una de las ubicaciones físicas de los centros de datos de la organización para cargas de trabajo.
- Disponer de conexiones separadas que terminen contra dispositivos de red separados para cada una de las ubicaciones físicas.

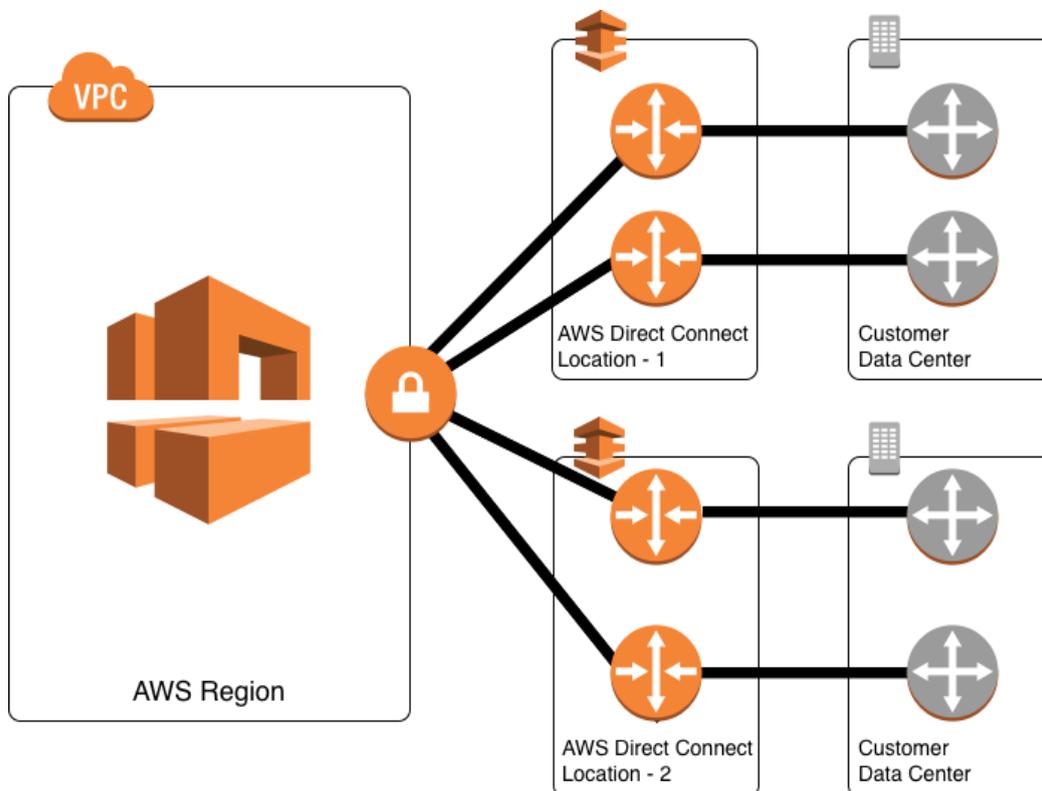


Fig. 24 - Conectividad redundada de AWS Direct Connect contra varias ubicaciones físicas

Grupos de agregación de enlaces (LAG)

Además de definir la conectividad de AWS Direct Connect con alta disponibilidad, es recomendable garantizar la máxima resiliencia para cargas de trabajo críticas, para lo que se debe:

- Implementar la necesaria redundancia en AWS Direct Connect mediante el uso de grupos de agregación de enlaces (LAG).
- Utilizar dos conexiones únicas a varias ubicaciones para garantizar la resiliencia frente a errores de conectividad provocados por un corte de fibra o error de dispositivo. Para ello, se puede hacer uso de la solución AWS Direct Connect Kit. No obstante, como hemos indicado anteriormente, esto dependerá de los requisitos de continuidad de cada organización.

Un grupo de agregación de enlaces (en inglés “Link Aggregation Group” – LAG) es una interfaz lógica que utiliza el protocolo de control de agregación de enlaces (LAGP) para agregar varias conexiones dedicadas en un único gateway de AWS Direct Connect y permite tratarlos como una única conexión gestionada. Los LAG

agilizan la configuración al aplicarse sobre todas las configuraciones de grupo.

Un ejemplo de configuración de redundancia de redes es el siguiente:

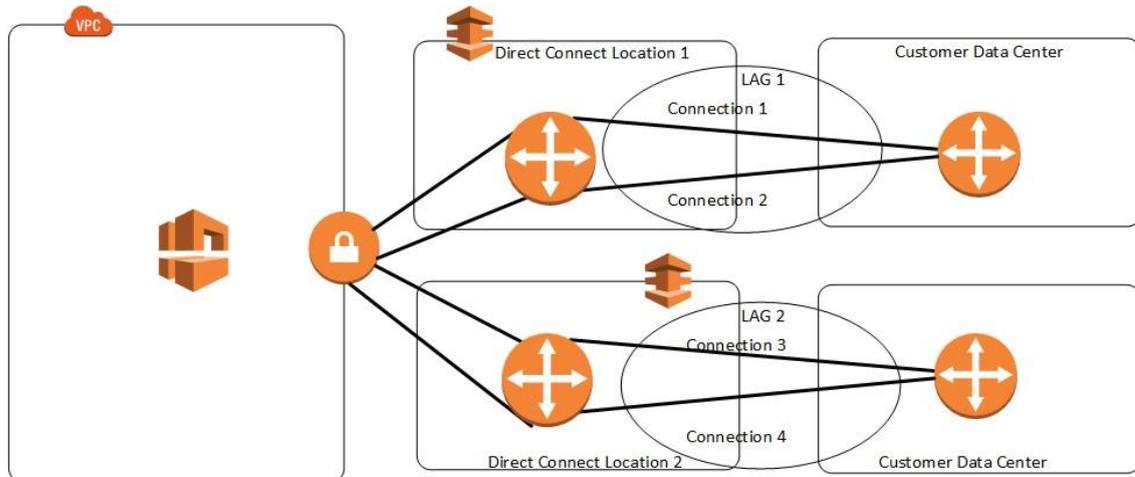


Fig. 25 - Uso de LAG en conexiones de AWS Direct Connect

Un LAG se crea a partir de conexiones dedicadas existentes o aprovisionando nuevas conexiones dedicadas. Tras crear el LAG, pueden asociarse conexiones dedicadas existentes (ya sean independientes o por parte de otro LAG) con el LAG. Para todos ellos, se deben aplicar las siguientes reglas:

- Todas las conexiones deben ser conexiones dedicadas y tener una velocidad de puerto de 1 Gbps o 10 Gbps.
- Todas las conexiones del LAG deben utilizar el mismo ancho de banda.
- Puede tener un máximo de cuatro conexiones en un LAG. Cada conexión del LAG cuenta para el límite de conexión global de la región.
- Todas las conexiones del LAG deben terminar en el mismo punto de enlace de AWS Direct Connect.
- AWS no admite LAG multichasis (MLAG).

Más información sobre grupos de agregación de enlaces y su configuración en: [Grupos de agregación de enlaces \(LAG\) - AWS Direct Connect](#)

AWS Direct Connect Resiliency Toolkit

AWS ofrece a la capacidad de establecer conexiones de red muy flexibles entre Amazon Virtual Private Cloud (Amazon VPC) y la infraestructura local. AWS Direct Connect Toolkit ofrece, además, un asistente de conexión con varios modelos de resiliencia. Estos modelos ayudan a determinar y realizar una petición para el número de conexiones dedicadas para lograr el objetivo de SLA. Los modelos de resiliencia están diseñados para garantizar la disponibilidad ajustando el número adecuado de conexiones dedicadas en varias ubicaciones.

Existen varios modelos disponibles para AWS Direct Connect:

- Resiliencia máxima: Permite solicitar conexiones dedicadas con un SLA del 99,99%
- Alta resiliencia: Permite solicitar conexiones dedicadas con un SLA del 99,9%
- Desarrollo y pruebas: Permite conseguir resiliencia en el desarrollo y las pruebas para las cargas de trabajo que no sean críticas.
- Classic: Destinado a usuarios con conexiones ya existentes y deseen añadir nuevas, este modelo no provee un SLA.

Estos objetivos de SLAs se circunscriben únicamente para el caso de conexiones dedicadas

Una vez configurado el asistente, AWS Direct Connect Toolkit permite realizar pruebas de conmutación por error, reduciendo la sesión de interconexión de BGP para comprobar si el tráfico se enruta hacia una de las interfaces redundantes.

Se puede obtener más información sobre el uso de esta herramienta en la documentación del fabricante: [Uso de AWS Direct Connect Kit de herramientas de resiliencia para comenzar - AWS Direct Connect](#)

Una vez configurado el asistente, AWS Direct Connect Toolkit permite realizar pruebas de conmutación por error, reduciendo la sesión de interconexión de BGP para comprobar si el tráfico se enruta hacia una de las interfaces redundantes.

Para la realización de esta prueba, se puede hacer uso de la información documentada en la guía del fabricante: [Prueba de conmutación por error de AWS Direct Connect - AWS Direct Connect](#)

Cuando implementar AWS VPN, AWS Direct Connect o ambas

Amazon VPC ofrece varias opciones de conectividad de red que podrá aprovechar en función del diseño y los requisitos de su red actual. Estas opciones de conectividad incluyen utilizar la conexión de Internet o una conexión de AWS Direct Connect como eje troncal de la red y terminar la conexión en puntos de conexión de red administrada por el usuario o AWS. En el siguiente [documento](#) se le facilita información para la correcta implementación de una u otra.

Recomendaciones para la monitorización – AWS Direct Connect

Para una correcta recopilación de datos relacionados con los servicios de conectividad, AWS ofrece el servicio Amazon CloudWatch que puede explotarse con la herramienta de monitorización automatizada de **Amazon CloudWatch Metrics** combinado con **Amazon CloudWatch Alerts**.

Con Amazon CloudWatch Alerts se puede observar una única métrica durante un periodo de tiempo que especifique. También permite realizar una o varias acciones

según el valor de la métrica con respecto a un umbral dado durante varios períodos de tiempo. La acción es una notificación enviada a un topic de Amazon SNS. Las alarmas de Amazon CloudWatch no invocan acciones simplemente por tener un estado determinado. Es necesario que el estado haya cambiado y se mantenga durante un número especificado de períodos. Se pueden conocer más detalles sobre las opciones disponibles en esta herramienta y su activación en el siguiente documento: [Monitoreo con Amazon CloudWatch - AWS Direct Connect](#)

- Deberá habilitarse el servicio Amazon CloudWatch para la gestión de eventos de los servicios de conectividad.

Igualmente habrá de tenerse en cuenta el servicio de **VPC Flowlogs** para la correcta monitorización del tráfico entrante a las VPCs que interactúan en un entorno de conectividad híbrida.

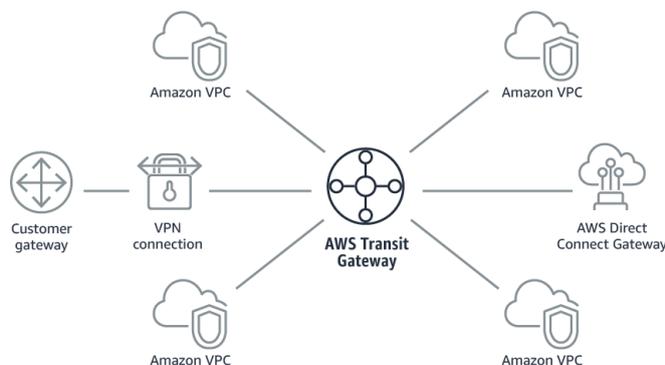
3.2.3. AWS Transit Gateway

AWS Transit Gateway conecta las VPC y las redes en las instalaciones a través de un centro principal lo que simplifica la red y pone fin a las complejas relaciones de interconexión. Además de ello, actúa como un enrutador en la nube, es decir, cada conexión nueva se realiza solo una vez.

A medida que se expande a nivel global, la interconexión entre regiones conecta las AWS Transit Gateways mediante la red global de AWS. Mediante el uso de esta herramienta se consigue que los datos se cifren automáticamente y nunca viajen a través de la Internet pública. Debido a su posición central, el AWS Transit Gateway Network Manager tiene una vista única de toda la red, pudiendo incluso conectarse a dispositivos de red de área amplia definida por software (SD-WAN).

AWS TGW también permite usar Accelerated VPN, lo que permite tener una latencia más baja además de una mejora en la seguridad y privacidad. Puede revisar la sección *AWS Accelerated Site-to-Site VPN: AWS Transit Gateway* que se encuentra dentro de la sección y descripción del servicio AWS Direct Connect.

Se puede encontrar más información en la documentación proporcionada por el fabricante: [Conexiones y pares de Transit Gateway Connect - Amazon VPC](#).



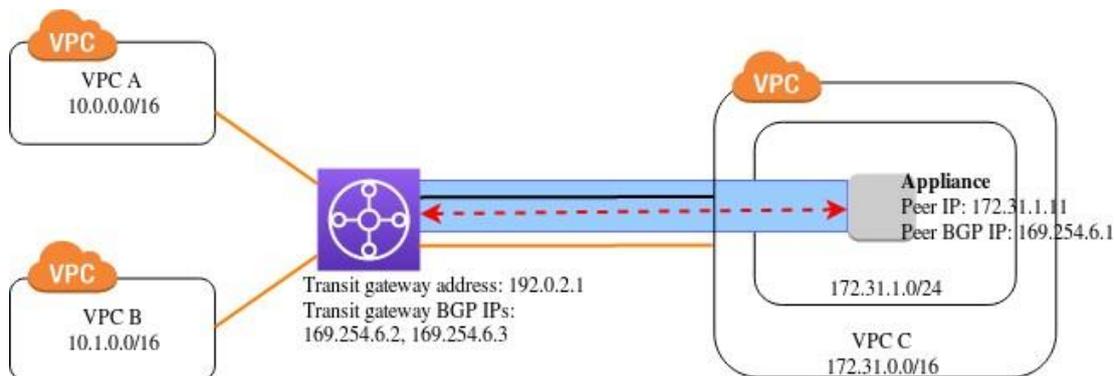


Fig. 26 - Representación gráfica Transit Gateway

Entre los casos más comunes para Transist Gateways, aunque no se limitan a estos casos de uso, encontramos los siguientes: [Algunos ejemplos de Transit Gateway](#)

3.2.4. AWS Private Link

AWS PrivateLink establece conectividad privada entre VPC y servicios alojados en AWS o en las instalaciones del usuario (On-premise), sin exponer los datos a Internet.

El punto de enlace de la VPC permite conectar de forma privada la VPC a los servicios de AWS compatibles y a servicios de la VPC habilitados por AWS PrivateLink sin necesidad de una gateway de Internet, un dispositivo NAT, una conexión de VPN o una conexión de AWS Direct Connect. Las instancias de las VPC no necesitan direcciones IP públicas para comunicarse con los recursos del servicio. El tráfico entre la VPC y el servicio no sale de la red de Amazon.

3.2.5. AWS Route 53 Resolver

Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Puede utilizar Route 53 para realizar tres funciones principales en cualquier combinación:

- Registro de dominio
- Direccionamiento de DNS
- Comprobación de estado

Amazon Route 53 Resolver responde de forma recursiva a las consultas de DNS de recursos de AWS de registros públicos, nombres de DNS específicos de Amazon VPC y zonas alojadas privadas de Amazon Route 53, y está disponible de manera predeterminada en todas las VPC.

Cuando los usuarios solicitan su sitio web o una aplicación web, por ejemplo, escribiendo el nombre de su dominio en un navegador web, Amazon Route 53 ayuda a dirigir a los usuarios a sus recursos, como un bucket de Amazon S3 o un

servidor web de su centro de datos.

3.4. Servicios de AWS ejecutados en centros de datos locales

En relación a los servicios de AWS que son ejecutados en los centros de datos locales, es importante tener en cuenta que, si bien AWS proporciona servicios que permiten el cifrado de datos en reposo y en tránsito, junto con otros controles de seguridad y mecanismos de auditoría, el modelo de responsabilidad compartida general sufre una variación: Al ejecutarse los servicios y/o dispositivos en el centro de datos del cliente, es éste quien asume la responsabilidad sobre la seguridad física y los controles de acceso.

3.3.1. AWS Outposts

[AWS Outposts](#) es un servicio completamente administrado que extiende la infraestructura, los servicios, las API y las herramientas de AWS a las instalaciones del cliente. Al proporcionar acceso local a la infraestructura administrada de AWS, AWS Outposts habilita a los clientes a crear y ejecutar aplicaciones en las instalaciones mediante el uso de las mismas interfaces de programación que en las regiones de AWS, al mismo tiempo que utilizan recursos informáticos y de almacenamiento locales para reducir la latencia y las necesidades de procesamiento de datos locales.

AWS opera, monitorea y administra esta capacidad como parte de una región de AWS. Puede crear subredes en el AWS Outpost y especificarlas al crear recursos de AWS como instancias EC2, volúmenes de EBS, clústeres ECS e instancias RDS. Las instancias en las subredes de AWS Outpost se comunican con otras instancias en la región de AWS mediante el uso de direcciones IP privadas, todo dentro de la misma VPC.

Cada AWS Outpost tiene una única puerta de enlace local, que permite la conectividad entre las subredes de AWS Outpost y la red local y también permite la conectividad entre las subredes de Outpost y la región de AWS principal. Por ejemplo, a través de un gateway de Internet conectado a la VPC, a cualquier punto de enlace de VPC creado en la subred de la zona de disponibilidad de la VPC o a puntos de enlace regionales públicos para los servicios de AWS.

Cada gateway local se compone de: grupos CoIP (opcional), interfaces virtuales (VIFs), asociaciones de grupos e VIFs y asociaciones de VPC. La responsabilidad de los componentes de AWS Outpost es compartida entre AWS y el cliente. AWS es responsable de entregar el hardware, crear la puerta de enlace local, las VIFs y un grupo de VIFs. La responsabilidad del cliente es crear la tabla de rutas del gateway local, asociar una VPC con la tabla de las rutas y asociar un grupo de VIFs con la tabla de rutas.

Por último, en relación con la conectividad entre las instancias de la subred del AWS Outpost y la red local, se puede utilizar:

- Direcciones IP privadas: el gateway local utiliza las direcciones IP privadas de las instancias de la subred de AWS Outpost para facilitar la comunicación con la red local.
- Direcciones IP propiedad del cliente: el gateway local realiza la traducción de direcciones de red (NAT) para las direcciones IP que se asigne a las instancias en la subred de AWS Outpost.

La siguiente imagen muestra como un AWS Outpost extiende la zona de disponibilidad de una región accesible desde la infraestructura local a través de una VPC.

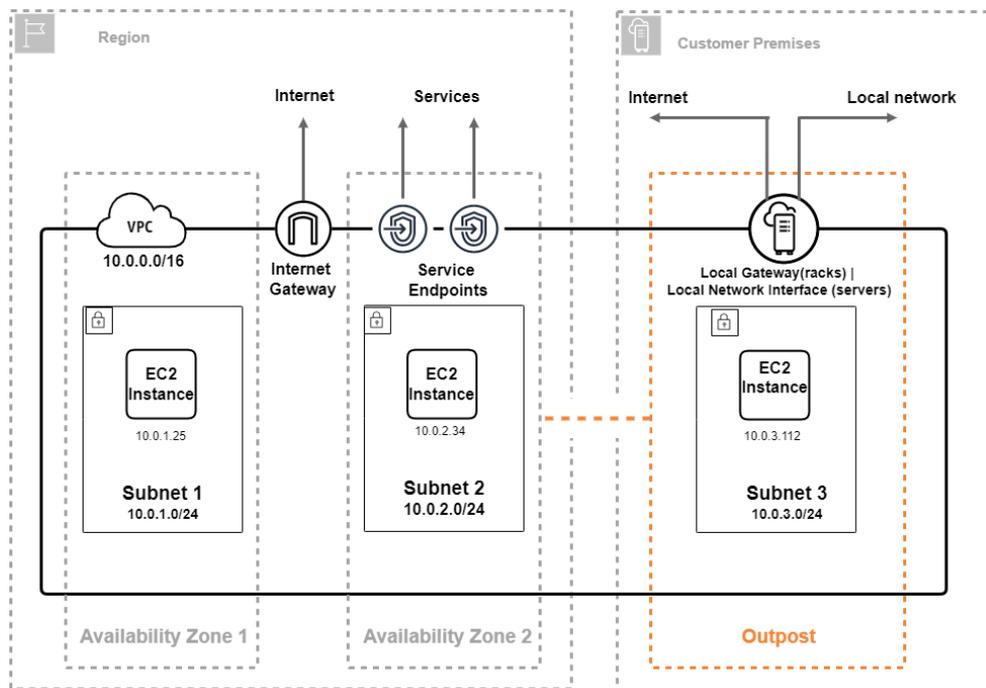


Fig. 27 – Esquema de componentes de red con AWS Outpost

Por último, es importante tener en cuenta que, como parte del modelo de responsabilidad compartida de los servicios de AWS ejecutados en los centros de datos locales, los clientes son los responsables de garantizar la seguridad física, así como los requisitos del sitio para las instalaciones, las redes y la energía, como se detalla [aquí](#).

3.3.2. AWS Snowball Edge

Los AWS Snowball Edge son un tipo de dispositivo con almacenamiento integrado y potencia informática para determinadas capacidades de AWS que se envía al cliente a través de un transportista regional. AWS Snowball Edge permite realizar cargas de trabajo de procesamiento local y edge-computing, además de transferir datos entre el entorno local y la nube de AWS a una velocidad superior a la de Internet.

Con el dispositivo AWS Snowball Edge, cualquier organización puede:

- Transferir grandes conjuntos de datos como bases de datos, copias de seguridad, registros etc. cuando las condiciones de red son limitadas.
- Procesar y analizar datos de forma local, ejecutando las imágenes de máquina de Amazon (AMI) en Amazon EC2 e implementar códigos Lambda directamente en el dispositivo AWS Snowball.
- Optimizar los datos de fabricación mediante la recopilación de datos.

El dispositivo AWS Snowball Edge no solo permite la transferencia de datos a gran escala y almacenamiento de estos, sino también la capacidad, mediante una GPU opcional, de realizar tareas que utilizan aprendizaje automático avanzado o análisis de video en movimiento en entornos sin conexión.

AWS Snowball Edge ofrece, además, interfaces que facilitan y permiten la creación de trabajos, seguimiento de datos y seguimiento del estado de un proceso de transferencia de datos de inicio a fin.

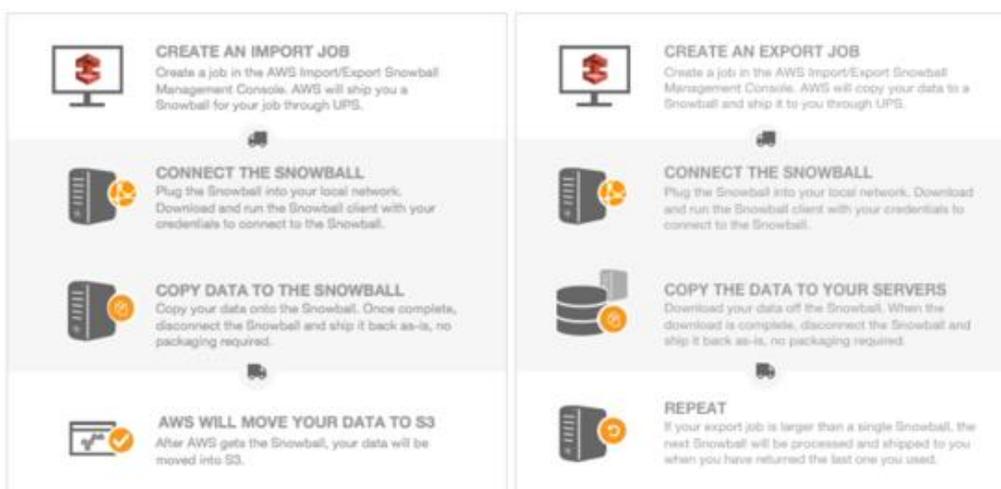


Fig. 28 – Proceso de importación / exportación con el dispositivo AWS Snowball

Sin embargo, a diferencia de AWS Outpost, AWS Snowball Edge funciona con una conectividad en la red local y no extiende su conectividad con los servicios como VPC. En este sentido, se recomienda seguir las siguientes prácticas de seguridad cuando se trabaje con un dispositivo AWS Snowball Edge:

Seguridad general

- No conectar la red el dispositivo AWS Snowball Edge si observa algo sospechoso en él. En este caso, deberá ponerse en contacto con el soporte de AWS.
- No guardar una copia del código de desbloqueo en la misma ubicación que el manifiesto de trabajo.
- Si considera que las credenciales se han perdido o se han visto comprometidas, solicite un nuevo archivo de manifiesto y código de

desbloqueo siguiendo el proceso para actualizar el certificado SSL del dispositivo.

- Puede utilizar las políticas de AWS IAM para controlar el acceso. Consulte más información sobre las [Políticas gestionadas de AWS Snowball Edge](#).

Seguridad de red

- Utilice un único método a la vez para leer y escribir datos de un bucket S3 en un dispositivo AWS Snowball Edge. Utilizar simultáneamente la interfaz de archivos y el adaptador de Amazon S3 en el mismo bucket S3 podría provocar conflictos de lectura/escritura.
- No desconecte el dispositivo AWS Snowball Edge ni cambie su configuración de red mientras transfiere datos.
- No modifique los archivos mientras se están transfiriendo al dispositivo.
- Para obtener más información sobre cómo tener un mejor rendimiento del dispositivo AWS Snowball Edge, consulte la siguiente documentación. [AWS Snowball Edge- Rendimiento](#).



Fig.29 - Dispositivo Snowball Edge

3.3.3. AWS Snowcone

AWS Snowcone es un dispositivo de AWS utilizado para la computación perimetral y la transferencia de datos. La organización puede solicitar tantos dispositivos como sean necesarios en función de la cantidad de datos que se desea transferir y el rendimiento de cómputo que se requiera.

Al igual que ocurre con el dispositivo AWS Snowball Edge, AWS Snowcone funciona

en la red local y no extiende su conectividad con los servicios como VPC.

Con AWS Snowcone cualquier organización puede recopilar, procesar y mover datos a la nube de AWS, bien sea sin conexión, mediante el envío del dispositivo, o en línea mediante el servicio AWS DataSync.



Fig.30 - Transferencia de datos con AWS DataSync

Entre los casos de uso más comunes se encuentran:

- Aplicaciones de computación perimetral para recopilar datos, procesarlos para obtener información inmediata y, a continuación, transferirlos en línea a la nube de AWS.
- Transferencia de datos en línea generados continuamente por sensores o máquinas desde una fábrica u otras ubicaciones de borde a la nube de AWS.
- Distribución de contenido multimedia, científico o de otro tipo desde servicios de almacenamiento de AWS a sus socios y clientes.
- Para agregar contenido mediante la transferencia de contenido multimedia, científico u otro contenido de sus ubicaciones perimetrales a la nube AWS.
- Para escenarios de migración de datos en los que los datos están listos para transferirse, AWS Snowcone ofrece una forma rápida y económica de transferir hasta 8 TB o 14 TB de datos a la nube de AWS, enviando el dispositivo de regreso a AWS tras ello.

AWS Snowcone es el dispositivo más pequeño de la familia Snow (AWS Snow Family), por lo que es necesario conocer las necesidades de la organización para

ajustarse al servicio más adecuado. Se puede consultar la [tabla de comparación de características](#) para obtener más información.

Se recomienda seguir las siguientes prácticas de seguridad a la hora de trabajar con un dispositivo AWS Snowcone:

- Si observas algo sospechoso en el dispositivo AWS Snowcone, no lo conectes a la red interna.
- Recomendamos que no guarde una copia del código de desbloqueo en la misma ubicación de la estación de trabajo donde se encuentra el manifiesto de ese trabajo. Guardarlos por separado ayuda a evitar que personas no autorizadas accedan al dispositivo AWS Snowcone.
- Le recomendamos que utilice solo un método de lectura y escritura de datos en un depósito local de un dispositivo AWS Snowcone a la vez.
- Para evitar que se corrompan los datos, no desconectes un dispositivo AWS Snowcone ni cambies la configuración de red al transferir datos.
- Los archivos deben encontrarse en un estado estático mientras se escriben en el dispositivo. Modificar archivos mientras se están escribiendo puede dar lugar a conflictos de lectura/escritura.



Fig.31 - Dispositivo Snowcone

4. GLOSARIO DE TÉRMINOS

Término	Definición
ACM	AWS Certificate Manager (gestor de certificados de AWS)
Alta disponibilidad	También conocida como High Availability, consiste en la duplicación del hardware del sistema.
API	Application Programming Interface (Interfaz de Programación de Aplicaciones)
AS	Asociación de Seguridad.
BGP	Border Gateway Protocol (BGP) o protocolo de puerta de enlace de frontera. Intercambia información entre sistemas autónomos.
Bucket S3	Contenedor para almacenar objetos pertenecientes al servicio S3
Certificado cualificado	Un certificado electrónico cualificado es un documento electrónico que vincula a una persona física o jurídica con una clave pública y una clave privada y confirma su identidad.
Clave de IKE	Clave que usa el protocolo IKE para establecer una asociación de seguridad en el protocolo IPSec.
CMK	Customer Master Key (clave maestra del cliente)
Comodín	También conocido como wildcard. Son comodines de búsqueda.
Conexión de respaldo	Conexión que utiliza los principios de redundancia para garantizar la disponibilidad de esta en caso de incidente.
DX	Direct Connect
DXGW	Direct Connect Gateway
EBS	Elastic Block Storage (almacenamiento de bloques elástico)
GPU	Unidad de procesamiento de gráficos o Graphics Processing Unit (GPU)
Grupo de agregación (LAG)	Un grupo de agregación de enlaces (en inglés "Link Aggregation Group" – LAG) es una interfaz lógica que utiliza el protocolo de control de agregación de enlaces (LAGP) para agregar varias conexiones dedicadas en un único gateway de AWS Direct Connect y permite tratarlos como una única conexión gestionada.
Hash	Función criptográfica para generar identificadores únicos e irrepetibles.
IaaS	Infrastructure as a Service (infraestructura como servicio)
IPSec	Internet Protocol Security (Protocolo de Seguridad en Internet)
Logging	Registro de los eventos importantes del sistema.
MFA	Multi-factor Authentication (autenticación multi factor)
Mínimo privilegio	Principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.

Término	Definición
NAT	Network Address Translation o Traducción de direcciones de red (NAT). Mecanismo utilizado por los routers IP para el intercambio de paquetes entre dos redes.
Nube híbrida	Interfaz que combina tanto la nube pública como la privada en el mismo lugar.
On-premise	En las instalaciones.
PaaS	Platform as a Service (plataforma como servicio)
Pre-Shared Key	Clave previamente compartida. Es una clave compartida con anterioridad entre las dos partes de la comunicación usando un canal seguro.
Public Peering	Conexión voluntaria de redes de internet con el fin de intercambiar tráfico entre los usuarios de cada red, en este caso, privada y pública.
Redundancia	Principio del uso de recursos de red de reserva con el fin de minimizar o evitar el tiempo de inactividad del sistema en caso de incidente.
Región	Ubicación física en todo el mundo donde se agrupan los centros de datos de AWS.
Resiliencia	Capacidad para adaptarse a las condiciones o situaciones adversas con resultados positivos.
Routing	Es el proceso que se realiza para determinar las tablas de encaminamiento.
SaaS	Software as a Service (software como servicio)
SLA	Acuerdos a Nivel de Servicio (SLA)
Subred (Subnet)	Subdivisión de una red.
Tags	Etiquetas
Túnel de datos	Método para transportar datos por una red mediante el uso protocolos que no son compatibles con esa red.
Ubicación Edge	Áreas que permiten disponer de una fuente de datos, acceder o estar cerca de ella.
VGW	Virtual Private Gateway
VGW	Virtual Private Gateway
VIF	Virtual Interface (VIF).
VPC	Virtual Private Cloud (nube privada virtual)
VPN	Virtual Private Network o Red Privada Virtual (VPN)
Zona de disponibilidad (AZ)	Availability Zone- Zona de disponibilidad

5. GLOSARIO DE SERVICIOS AWS

A continuación, se reúnen los diferentes servicios mencionados a lo largo de esta guía incluyendo enlaces a la documentación concreta de cada uno de ellos. Como complemento de estos documentos se recomienda el uso del siguiente recurso enfocado a los aspectos de seguridad de cada uno de ellos:

<https://docs.aws.amazon.com/security/>

Servicio	URL de documentación del servicio
AWS VPN	AWS Client VPN
Amazon API Gateway	Amazon API Gateway
Amazon CloudWatch	Amazon CloudWatch
Amazon CloudWatch – AWS Direct Connect	Monitoreo con Amazon CloudWatch - AWS Direct Connect
Amazon CloudWatch Alerts	Uso de las alarmas de Amazon CloudWatch - Amazon CloudWatch
Amazon CloudWatch Metrics	Uso de métricas de Amazon CloudWatch - Amazon CloudWatch
Amazon Elastic Computer Cloud (EC2)	Amazon Elastic Compute Cloud - AWS EC2
Amazon Elastic File System (EFS)	Amazon Elastic File System - AWS EFS
Amazon GuardDuty	Amazon GuardDuty
Amazon Private Link	AWS PrivateLink
Amazon S3	Amazon Simple Storage Service - Amazon S3
AWS Certificate Manager	AWS Certificate Manager
AWS Cloud Development Kit (CDK)	AWS Cloud Development Kit
AWS CloudTrail	AWS CloudTrail
AWS Command Line Interface (CLI)	AWS Command Line Interface
AWS Config	Documentación de AWS Config - AWS Config Tipos de recursos admitidos en AWS Config - AWS Config Required Tags - AWS Config
AWS DataSync	AWS DataSync
AWS Direct Connect	AWS Direct Connect
AWS Direct Connect gateways	AWS Direct Connect gateways - AWS Direct Connect
AWS Direct Connect Kit	Uso de AWS Direct ConnectKit de herramientas de resiliencia para comenzar - AWS Direct Connect
AWS Direct Connect Toolkit	AWS Direct Connect Toolkit
AWS Global Accelerator	AWS Global Accelerator

Servicio	URL de documentación del servicio
AWS Identity & Access Manager (IAM)	Identidades de IAM (usuarios, grupos de usuarios y roles) - AWS IAM
AWS Key Management Service (KMS)	AWS Key Management Service - AWS KMS Políticas de claves - AWS KMS
AWS Lambda	AWS Lambda
AWS Outposts	AWS Outposts
AWS Private CA	Private CA
AWS Route 53 Resolver	Amazon Route 53
AWS SiteLink	AWS Direct Connect AWS SiteLink
AWS Site-to-Site	AWS Site-to-Site VPN
AWS Snowball	AWS Snowball
AWS Snowcone	AWS Snowcone
AWS Snowmobile	AWS Snowmobile
AWS Systems Manager	AWS Systems Manager
AWS Systems Manager Parameter Store	Systems Manager Parameter Store
AWS Tags	AWS Tagging Best Practices
AWS Transit Gateway	Amazon VPC
AWS VPN CloudHub	Comunicaciones seguras entre sitios mediante VPN CloudHub - AWS Site-to-Site VPN AWS VPN CloudHub
AWS Web Application Firewall (WAF)	AWS Web Application Firewall - AWS WAF
AWS Whitepaper de conectividad híbrida	Conectividad híbrida - AWS Whitepaper
Grupos de agregación de enlaces (LAG)	Grupos de agregación de enlaces (LAG) - AWS Direct Connect
Regiones y zonas de disponibilidad	Regiones y zonas de disponibilidad de la infraestructura global
SNS	Amazon Simple Notification Service
Virtual Private Cloud	Red privada virtual (VPC)
VPC Flowlogs	VPC Flowlogs
VPN Site-to-Site	AWS VPN Site-to-Site



CCN-STIC 887A



Guía de configuración segura para AWS

