centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 889C

Guía de Configuración segura para Oracle OCI - Arquitecturas Híbridas

MARZO 2022

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.04.28 15:47:15 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-138-X

Fecha de Edición: abril de 2022
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

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

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Marzo de 2022

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA PARA ORACLE OCI - ARQUITECTURAS HÍBRIDAS

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

Esta guía muestra el despliegue y configuración de los servicios de Oracle Cloud Infrastructure (OCI) para cargas de trabajo en la nube pública de Oracle siguiendo las exigencias del Esquema Nacional de Seguridad (ENS).

La principal utilidad de esta guía es identificar los servicios de OCI para las Arquitecturas Híbridas en entornos de cliente-nube, o sea, para las organizaciones que necesiten conectar sus centros de datos a la nube de Oracle, cumpliendo con las distintas medidas de seguridad que establece el Esquema Nacional de Seguridad. A su vez, se añaden referencias a la documentación oficial del fabricante con el objetivo de facilitar la lectura y comprensión por parte del usuario de esta guía.

La nomenclatura de algunos servicios o tecnologías descritos se documenta en el glosario de abreviaturas, incluido como anexo al documento.

Para finalizar, se incluye un resumen de las medidas detalladas anteriormente para realizar un control de la configuración a modo de “checklist”.

1.2 DEFINICIÓN DEL SERVICIO

Oracle Cloud Infrastructure (OCI), es la nube de última generación diseñada para ejecutar cualquier aplicación de forma más rápida y segura por menos.

El marco de adopción de OCI ayuda a las organizaciones a facilitar su transición a la nube y proporciona a los clientes una metodología para utilizar eficiencias incorporadas de Oracle Cloud, como los servicios de Networking para la infraestructura de la nube de Oracle, la cual dispone de la Certificación de Conformidad con el Esquema Nacional de Seguridad.

Dentro de los modelos que ofrece OCI, esta guía se centrará en el modelo de Infraestructura como Servicio (IaaS) y en el modelo de Plataforma como Servicio (PaaS).

a) **IaaS**: Es un tipo de modelo de servicio de Cloud Computing en el que los recursos de computación se alojan en la nube. Las empresas pueden usar el modelo IaaS para trasladar parte o la totalidad de su uso de la infraestructura de centro de datos in-situ o localizada a la nube, donde será propiedad de un proveedor de nube y estará administrada por este. Entre estos elementos de infraestructura se pueden incluir hardware de computación, red y almacenamiento, así como otros componentes y software.

b) **PaaS**: es un conjunto de servicios que permite crear y gestionar aplicaciones modernas en la era digital, on-premises o en la nube. Proporciona la infraestructura y los componentes que permiten a los desarrolladores, administradores de TI y usuarios crear, integrar, migrar, implementar, proteger y administrar sistemas y aplicaciones.

Para ayudar a mejorar la productividad, PaaS ofrece componentes de programación listos para usar que permiten a los desarrolladores integrar nuevas características en sus aplicaciones, incluidas tecnologías innovadoras como inteligencia artificial (IA), chatbots, blockchain y el Internet of Things (IoT).

Esto también incluye suites de herramientas de desarrollo de aplicaciones, lo que incluye servicios nativos en la nube, Kubernetes, Docker, motores de contenedor y mucho más.

También se recogen las medidas de aplicación técnica que marca el ENS para la Categoría Alta, según las medidas a establecer en cada una de las tareas de la conectividad híbrida de las que trata este documento, disponiendo para ello de varios servicios que se detallan a continuación.

2. SERVICIOS PARA ARQUITECTURAS HÍBRIDAS

Oracle proporciona una nube híbrida para la ejecución de cargas de trabajo de la nube donde sea que se necesiten, incluso en las ubicaciones más remotas del mundo. La arquitectura de nube híbrida utiliza tanto un proveedor de nube pública como OCI, como una infraestructura local para satisfacer las necesidades de TI de la empresa. Este enfoque proporciona la flexibilidad para mover algunas cargas de trabajo a la nube pública y mantener otras en las instalaciones.

La arquitectura de nube híbrida se encarga fundamentalmente de la interconexión entre todas esas infraestructuras externas e interna mediante una conectividad fácil, rápida y segura para las organizaciones.

Los productos y servicios de redes en la nube de Oracle le permiten administrar y escalar las redes. Puede conectarse de forma segura a una red virtual en la nube (VCN) aislada y personalizable como el núcleo de su implementación en la nube. Los bajos cargos de la salida de datos permiten a las organizaciones ahorrar costos significativos mientras extienden su entorno de Tecnología Informática a la nube. Las tecnologías de red Oracle Cloud brindan soluciones de conectividad para sus redes físicas y virtuales que se detallarán a lo largo de esta Guía.

2.1 SERVICIO NETWORKING

El Servicio de Networking utiliza versiones virtuales de los componentes de red tradicionales con los que debe estar familiarizado y que son necesarios explicar para una correcta comprensión de los términos utilizados en el resto del documento:

a) **Red Virtual en la nube (VCN)**: Red virtual privada que se configura en centros de datos de Oracle. Se parece mucho a una red tradicional, con reglas de firewall y tipos específicos de gateways de comunicación cuya utilización puede elegir. Una VCN reside en una única región de OCI y cubre uno o más bloques CIDR (IPv4 e IPv6, si están activados).

b) **Subredes**: Las subredes son subdivisiones definidas de una VNC que contienen tarjetas de interfaz de red virtual (VNIC), que se conectan a las instancias. Cada subred consta de un rango contiguo de direcciones IP (para IPv4 e IPv6, si está activado) que no se superponen con otras subredes de la VCN. Puede designar una subred para que exista en un único dominio de disponibilidad o en toda una región.

Oracle recomienda el uso de subredes regionales.

Las subredes actúan como una unidad de configuración en la VCN: todas las VNIC de una subred determinada utilizan las mismas tablas de rutas, listas de seguridad y opciones de DHCP (consulte las definiciones siguientes). Puede designar una subred como pública o privada al crearla. Privado significa que las VNIC de la subred no pueden tener direcciones IPv4 públicas y que se prohibirá la comunicación de Internet con puntos finales IPv6. Público significa que las VNIC de la subred pueden tener direcciones IPv4 públicas y que se permite la comunicación a través de Internet con los puntos finales IPv6.

c) **VNIC**: Tarjeta de interfaz de red virtual (VNIC), que se conecta a una instancia y reside en una subred para permitir una conexión con la VCN de la subred. La VNIC determina cómo se conecta la instancia con los puntos finales dentro y fuera de la VCN. Cada instancia tiene una VNIC principal creada durante el inicio de la instancia y no se puede eliminar. Puede agregar VNIC secundarias a una instancia existente (en el mismo dominio de disponibilidad que la VNIC principal) y eliminarlas según desee. Cada VNIC secundaria puede estar en una subred de la misma VCN que la VNIC principal o en una subred diferente que esté en la misma VCN o en una diferente. Sin embargo, todas las VNIC deben estar en el mismo dominio de disponibilidad que la instancia.

d) **IP Privada**: Dirección de IPv4 privada e información relacionada para tratar una instancia como, por ejemplo, un nombre de host para DNS. Cada VNIC tiene una IP privada principal, y puede agregar y eliminar IP privadas secundarias. La dirección IP privada principal de una instancia no cambia durante el ciclo vital de la instancia y no se puede eliminar de la instancia.

e) **IP Pública**: Dirección de IPv4 pública e información relacionada. Opcionalmente, puede asignar una IP pública a las instancias u otros recursos que tengan una IP privada. Las IP públicas pueden ser efímeras o reservadas.

f) **Gateway de Enrutamiento Dinámico (DRG)**: Un enrutador virtual opcional que puede agregar a la VCN. Proporciona una ruta de acceso para el tráfico de red privado entre su red local y la VCN. Puede utilizarse con otros componentes de Networking y un enrutador en la red local para establecer una conexión mediante VPN de sitio a sitio u OCI FastConnect. También puede proporcionar una ruta de acceso para el tráfico de red privada entre la VCN y otra VCN de una región diferente.

g) **Gateway de internet**: Otro enrutador virtual opcional que se puede agregar a la VCN para obtener un acceso directo desde internet.

h) **Gateway de Traducción de Direcciones de Red (NAT)**: Otro enrutador virtual opcional que puede agregar a la VCN. Ofrece acceso desde las VM de la subnet hacia Internet a los recursos en la nube, sin el acceso de direcciones IP públicas a internet y sin exponer dichos recursos a las conexiones de internet entrantes.

i) **Gateway de servicio**: Otro enrutador virtual opcional que puede agregar a la VCN. Proporciona una ruta de acceso para el tráfico de red privado entre su VCN y los servicios admitidos en Oracle Services Network sin necesidad de direcciones IP públicas ni acceso a internet.

j) **Gateway de Intercambio de Tráfico Local (LPG)**: Otro enrutador virtual opcional que puede agregar a la VCN. Permite utilizar un intercambio de tráfico de VCN con otra VCN en la

misma región. El intercambio de tráfico significa que las VCN se comunican mediante direcciones IP privadas, sin el tráfico que atraviesa internet ni el enrutamiento a través de su red local. Una VCN determinada debe tener un LPG independiente por cada intercambio de tráfico que establezca.

k) **Conexión con Intercambio de Tráfico Remoto (RPC)**: Componente que puede agregar a un DRG. Permite utilizar un intercambio de tráfico de VCN con otra VCN en una región diferente.

l) **Tablas de rutas**: Son reglas para enrutar el tráfico desde subredes hasta destinos fuera de la VCN mediante gateways o instancias de configuración especial. La VCN incluye una tabla de rutas por defecto vacía, y es posible agregar sus propias tablas de rutas personalizadas.

m) **Reglas de seguridad**: Reglas del firewall virtual para la VCN. Son reglas de entrada y salida que especifican los tipos de tráfico (protocolo y puerto) cuya entrada y salida de las instancias se permite. Puede elegir si una regla determinada tiene estado o no. Por ejemplo, puede permitir el tráfico SSH entrante desde cualquier lugar a un conjunto de instancias mediante la configuración de una regla de entrada con estado con CIDR 0.0.0.0/0 de origen y el puerto 22 de TCP de destino. Para implantar reglas de seguridad, puede utilizar grupos de seguridad de red o listas de seguridad. Un grupo de seguridad de red consta de un conjunto de reglas de seguridad que se aplican solo a las VNIC asignadas a ese grupo. Compárese con una lista de seguridad, donde las reglas se aplican a todos los recursos de cualquier subred que utilice la lista. La VCN incluye una lista de seguridad por defecto con reglas de seguridad también por defecto.

También cabe indicar que tanto las listas como los grupos de seguridad no son excluyentes, pudiendo utilizar conjuntamente ambas dependiendo de las necesidades de seguridad concretas. Puede ampliar la información acerca del uso combinado de la Listas y Grupos de seguridad en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/securityrules.htm#use_both

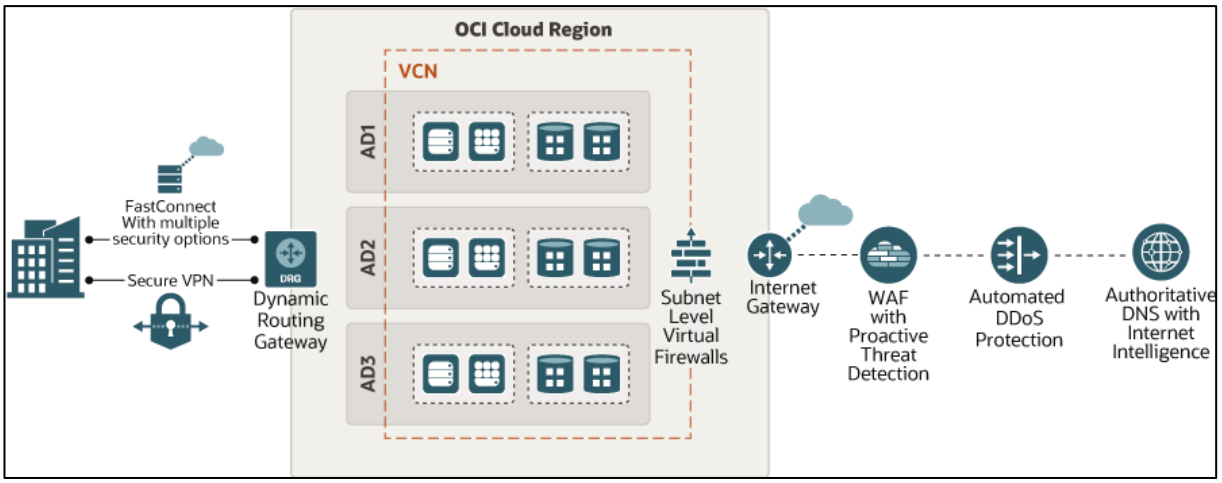


Imagen donde se muestran las opciones de conectividad de red con OCI.

Una VCN tiene los siguientes componentes por defecto que se incluyen durante el proceso de creación:

a) Tabla de rutas por defecto, sin reglas de rutas.

b) Lista de seguridad predeterminada, con reglas de seguridad también predeterminadas.

c) Conjunto predeterminado de opciones de DHCP, con valores predeterminados.

Estos componentes no se pueden eliminar, pero si se pueden modificar, como la lista de seguridad predeterminada, ya que se crea una por defecto, pero luego pueden crearse más posteriormente.

En cuanto a la disposición, una VCN reside en una sola región de OCI. Una región puede tener varios dominios de disponibilidad (AD) para proporcionar aislamiento y redundancia.

Las subredes originales se han diseñado para cubrir solo un AD en una región. Todas son específicas de AD, lo que significa que los recursos de la subred debían residir en un dominio de disponibilidad determinado. Ahora, las subredes pueden ser específicas de AD o regionales. Debe elegir el tipo al crear la subred. Ambos tipos de subredes pueden coexistir en la misma VCN.

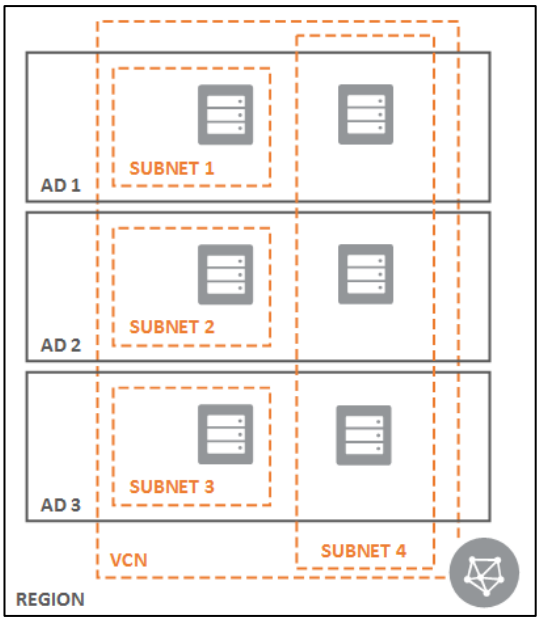


Imagen sobre la localización de las subredes 1-3, que son específicas de AD y la subred 4, regional.

Además de la eliminación de la restricción de AD, las subredes regionales se comportan de la misma manera que las subredes específicas de AD. Oracle recomienda utilizar subredes regionales porque son más flexibles. Facilitan la división eficiente de la VCN en subredes, al tiempo que su diseño se orienta a los fallos de AD.

En cuanto a la conectividad, puede controlar si las subredes son públicas o privadas y si las instancias obtienen direcciones IP públicas. Se puede configurar la VCN de forma que tenga acceso a internet si se desea. También puede conectar de forma privada la instancia de la VCN a servicios públicos de OCI, como Object Storage, a otra red local o a otra VCN.

Acceso a Internet

Para disponer de acceso a Internet, dispone de tres gateways opcionales (enrutadores virtuales) que puede agregar a la VCN en función del tipo de acceso a internet que se necesite:

a) **Gateway de internet**: para los recursos con direcciones IP públicas que precisan el acceso desde internet (por ejemplo: un servidor web) o el inicio de conexiones a internet.

b) **Gateway de NAT**: para los recursos sin direcciones IP públicas que necesitan iniciar conexiones a internet (por ejemplo, para las actualizaciones de software), si bien es necesario protegerlas de las conexiones entrantes de internet.

c) **Gateway de servicio**: para proporcionar una ruta de acceso al tráfico de red privado entre su VCN y los servicios admitidos en Oracle Services Network (por ejemplo, los sistemas de base de datos de una subred privada de la VCN pueden realizar una copia de seguridad de los datos en Object Storage) sin necesidad de acceso a internet ni direcciones IP públicas.

Disponer solo de un gateway de internet no muestra las instancias de las subredes de la VCN directamente a internet. También deben cumplirse los siguientes requisitos:

a) El gateway de internet debe estar activado (por defecto, el gateway de internet se activa al crearse).

b) La subred debe ser pública.

c) La subred debe tener una regla de rutas que dirija el tráfico al gateway de internet.

d) La subred debe tener reglas de lista de seguridad que permitan el tráfico (y el firewall de cada instancia debe permitir el tráfico).

e) La instancia debe tener una dirección IP pública.

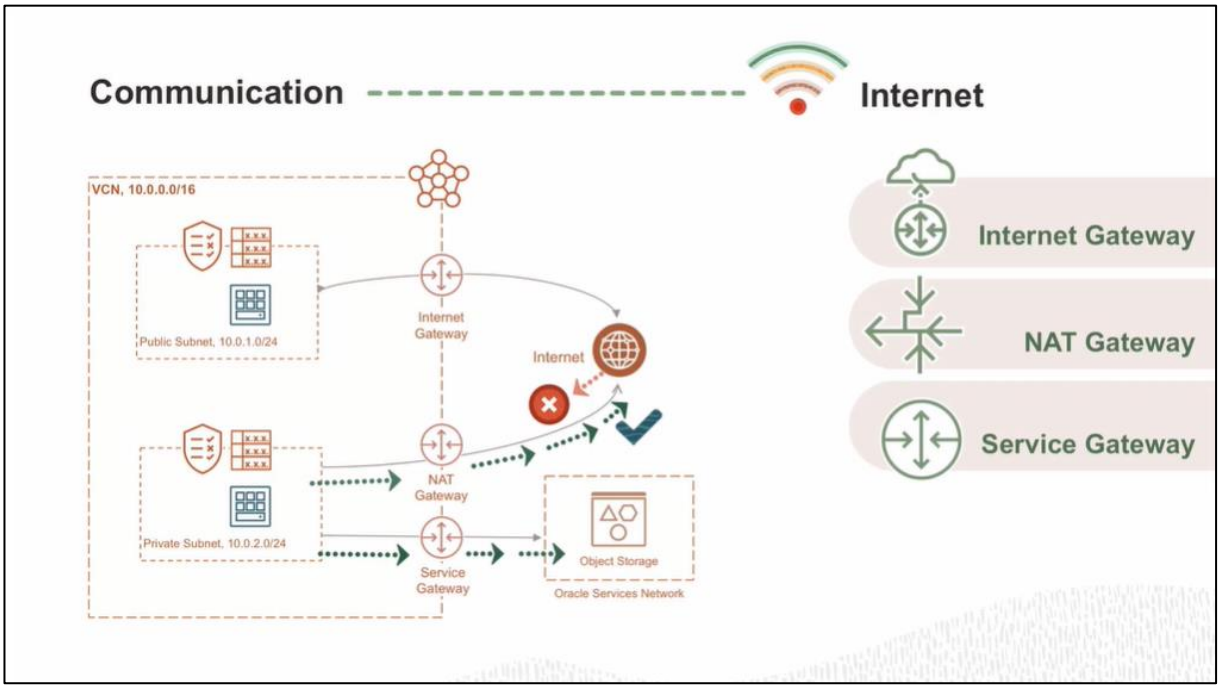


Imagen sobre los diferentes elementos que dispone OCI para proporcionar una salida a las VCN hacia Internet.

Acceso a la red local

Por lo que se refiere al acceso a la red local, Oracle presenta dos formas de conectar la red local a OCI:

a) **VPN de Sitio a Sitio**: ofrece varios túneles de IPSec entre el borde de la red existente y la VCN, a través de un DRG creado y conectado a la VCN.

b) **OCI FastConnect**: ofrece una conexión privada entre el perímetro de la red existente y OCI. El tráfico no atraviesa internet. Se admite tanto el intercambio de tráfico privado como público. Esto significa que los hosts locales pueden acceder a direcciones privadas de IPv4 o IPv6 en la VCN, así como a direcciones regionales públicas de IPv4 o IPv6 en OCI.

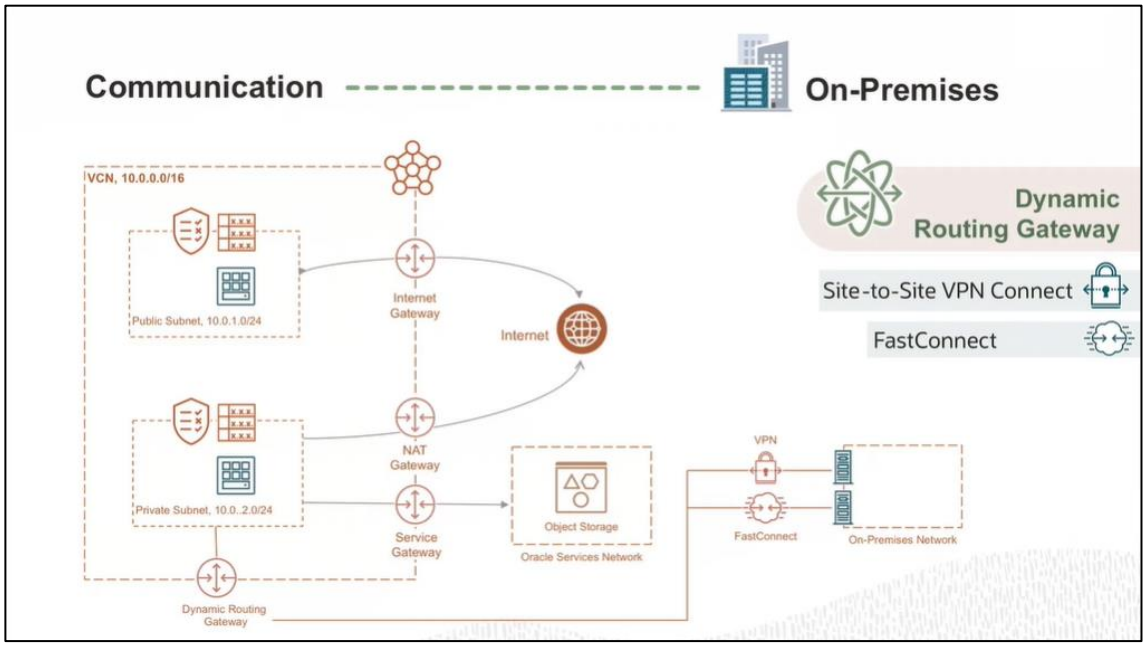


Imagen con los tipos de conectividad híbrida para conectar la red local de OCI con la red On-Premises.

OCI dispone de otros tipos de opciones de conectividad:

a) **Acceso a otra VCN**: Puede conectar la VCN a otra VCN mediante una conexión privada que no requiera que tráfico pase por internet. En general, este tipo de conexión se denomina intercambio de tráfico de la VCN. Cada VCN debe tener componentes específicos para activar el intercambio de tráfico. Las VCN también deben tener políticas de IAM, reglas de rutas y reglas de seguridad específicas que permitan que se realice la conexión y que fluya el tráfico de red deseado a través de la conexión. Puede obtener más información en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/VCNpeering.htm

b) **Conexión a Microsoft Azure**: Oracle y Microsoft han creado una conexión entre varios sistemas en la nube entre OCI y Azure en determinadas regiones. Esta conexión permite configurar cargas de trabajo en varias nubes sin el tráfico que se produce entre ellas al gestionarlo mediante internet. Puede obtener más información en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/azure.htm

c) **Conexión con otras nubes con Libreswan**: Puede conectar una VCN a otro proveedor en la nube mediante VPN de sitio a sitio con una máquina virtual de Libreswan como equipo local de cliente (CPE). Puede obtener más información en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/libreswan.htm

Nota: Oracle dispone de otras formas de conexión, mediante la configuración de DRG y BGP, siendo muy típico la utilización de un partner tipo Megaport, Equinix o similar. Su arquitectura se explica en el siguiente enlace: https://docs.oracle.com/es/solutions/oci-aws-equinix/index.html.

Puede ampliar aún más la información sobre el Servicio Networking (Red) y sus escenarios en los siguientes enlaces de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/overview.htm

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/scenarios.htm

2.1.1 VPN (SITE TO SITE)

La VPN de sitio a sitio proporciona una conexión IPSec de sitio a sitio entre la red local y la red virtual en la nube (VCN). El conjunto de protocolos IPSec cifra el tráfico IP antes de transferir los paquetes del origen al destino y descifra el tráfico cuando llega. La VPN de sitio a sitio se denominaba VPN Connect y VPN con IPSec.

Otras soluciones VPN seguras incluyen OpenVPN, que es una solución VPN de cliente a la que se puede acceder en Marketplace de Oracle. OpenVPN conecta dispositivos individuales a la VCN, pero no sitios ni redes completos.

OCI solo admite el modo de túnel para VPN con IPSec, pudiendo configurar una conexión IPSec en los siguientes modos:

a) **Modo de Transporte**: IPSec cifra y autentica únicamente la carga útil real del paquete, y la información del encabezado permanece intacta.

b) **Modo de túnel** (admitido por Oracle): IPSec cifra y autentica todo el paquete. Después del cifrado, el paquete se encapsula para formar un nuevo paquete IP que tiene información de encabezado diferente.

Cada conexión IPSec de Oracle consta de varios túneles IPSec redundantes. Para un túnel determinado, se puede utilizar un enrutamiento dinámico con el Protocolo de Gateway de Borde (BGP) o un enrutamiento estático para enrutar el tráfico del túnel.

En cuanto al enrutamiento para una VPN de sitio a sitio, al configurar VPN de sitio a sitio, tiene dos túneles IPSec redundantes.

Oracle recomienda configurar el dispositivo CPE para utilizar ambos túneles (si el dispositivo lo admite). Tenga en cuenta que en el pasado Oracle creó las conexiones de IPSec con hasta cuatro túneles de IPSec.

Existen los dos tipos siguientes de enrutamiento y puede seleccionar el tipo de enrutamiento por separado para cada túnel de IPSec en la VPN de sitio a sitio:

a) **Enrutamiento dinámico de BGP**: las rutas disponibles se aprenden de forma dinámica mediante BGP. DRG aprende de forma dinámica las rutas de su red local. En el lado de Oracle, DRG anuncia las subredes de la VCN.

b) **Enrutamiento estático**: al configurar la conexión de IPSec con DRG, debe especificar las rutas específicas a la red local de la que desea que se conozca la VCN. También debe configurar su dispositivo CPE con rutas estáticas a las subredes de la VCN. Estas rutas no se aprenden dinámicamente.

c) **Enrutamiento basado en políticas**: al configurar la conexión de IPSec con DRG, debe especificar las rutas específicas a la red local de la que desea que se conozca la VCN. También debe configurar su dispositivo CPE con rutas estáticas a las subredes de la VCN. Estas rutas no se aprenden dinámicamente.

Al configurar VPN de sitio a sitio para su VCN, debe crear varios componentes de red. Puede crear los componentes desde la consola o desde la API.

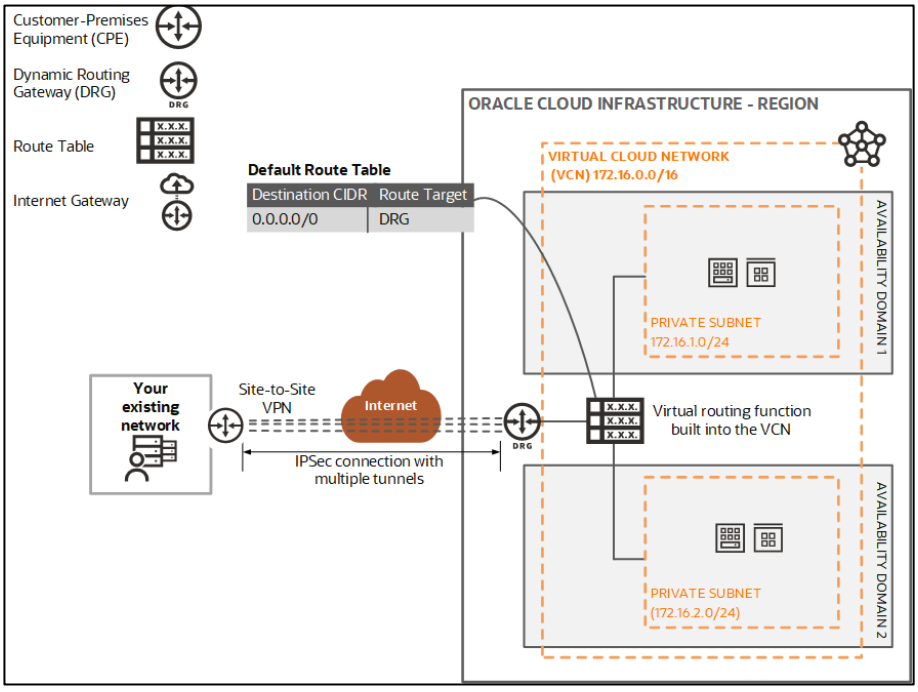


Imagen de los componentes de una VPN de Sitio a Sitio de Oracle.

Puede ampliar la información sobre IPSec de Oracle en el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/overviewIPsec.htm

Al final de la VPN de sitio a sitio se encuentra el dispositivo real de la red local (ya sea hardware o software). El término equipo local de cliente (CPE) se suele utilizar en algunos sectores para hacer referencia a este tipo de equipo local. Al configurar la VPN, debe crear una representación virtual del dispositivo. Oracle llama a la representación virtual un CPE. El objeto CPE contiene información básica sobre el dispositivo que necesita Oracle.

El administrador de redes debe configurar el CPE en su extremo de la conexión de IPSec. Para facilitar esta tarea, Oracle proporciona los siguientes recursos:

a) **Asistente de configuración de CPE**: una herramienta de la consola de Oracle que genera un conjunto de contenido que el ingeniero de redes puede utilizar cuando configura el CPE.

b) **Una lista de dispositivos CPE verificados**: para cada dispositivo, Oracle proporciona instrucciones de configuración.

c) **Una lista de parámetros de IPSec admitidos**: si su CPE no está en la lista de dispositivos verificados, puede utilizar esta lista de parámetros para configurar el CPE.

Puede ampliar la información acerca de los CPE en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/configuringCPE.htm

También puede encontrar más información de las conexiones con otros proveedores de Cloud a través del siguiente enlace de Oracle, con ejemplos:

https://blogs.oracle.com/lad-cloud-experts-es/post/vpn-ipsec-entre-oracle-cloud-y-otros-proveedores-cloud

2.1.2 FAST-CONNECT

Otro tipo de conectividad híbrida es FastConnect de OCI, que proporciona una forma sencilla de crear una conexión privada y exclusiva entre el centro de datos de una organización y OCI. FastConnect ofrece opciones de un gran ancho de banda, así como una experiencia de redes más fiable y coherente en comparación con las conexiones basadas en internet.

Con FastConnect puede optar por utilizar el intercambio de tráfico privado, el intercambio de tráfico público o ambos.

a) **Intercambio de tráfico privado**: para ampliar la infraestructura existente en una red virtual en la nube (VCN) en OCI (por ejemplo, para implementar una nube híbrida o un caso de Subir y Modificar). La comunicación entre la conexión se realiza con las direcciones privadas de IPv4.

b) **Intercambio de tráfico público**: para acceder a los servicios públicos en OCI sin utilizar internet. Por ejemplo, Object Storage, la Consola de OCI y las API o los equilibradores de carga públicos en la VCN. La comunicación en la conexión es con direcciones IP públicas de IPv4. Sin FastConnect, el tráfico destinado a direcciones IP públicas se direccionaría por internet. Con FastConnect, ese tráfico pasa por su conexión física privada. Para obtener una lista de los servicios disponibles con el intercambio de tráfico público, consulte los Servicios en la nube admitidos en FastConnect mediante al siguiente enlace: https://www.oracle.com/cloud/networking/fastconnect/services.

Para obtener una lista de los rangos de direcciones IP públicas (rutas) que Oracle anuncia, consulte Rutas anunciadas de intercambio de tráfico público de FastConnect en el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/fastconnectpublicpeeringaddressranges.htm

Aunque en general, se supone un mayor uso del intercambio de tráfico privado, también es utilizado el intercambio de tráfico público o ambos.

Si la organización decide tener varias rutas desde su red local a Oracle, consulte los detalles de enrutamiento para conexiones a la red local a través de los siguientes enlaces de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/routingonprem2.htm

https://www.oracle.com/es/cloud/networking/fastconnect-connectivity-models.html

Con FastConnect, existen distintos modelos de conectividad entre los que elegir:

a) Partners de Oracle.

b) Proveedor externo.

c) Colocación con Oracle en una ubicación de OCI FastConnect.

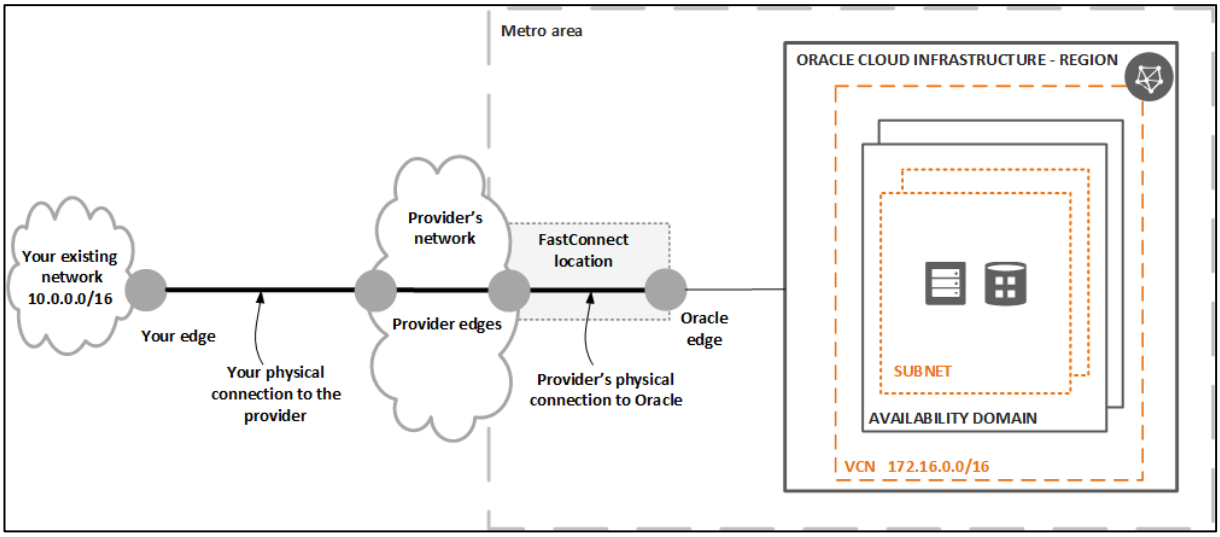


Diagrama de un modelo de conexión a un Partner de Oracle o un Proveedor externo.

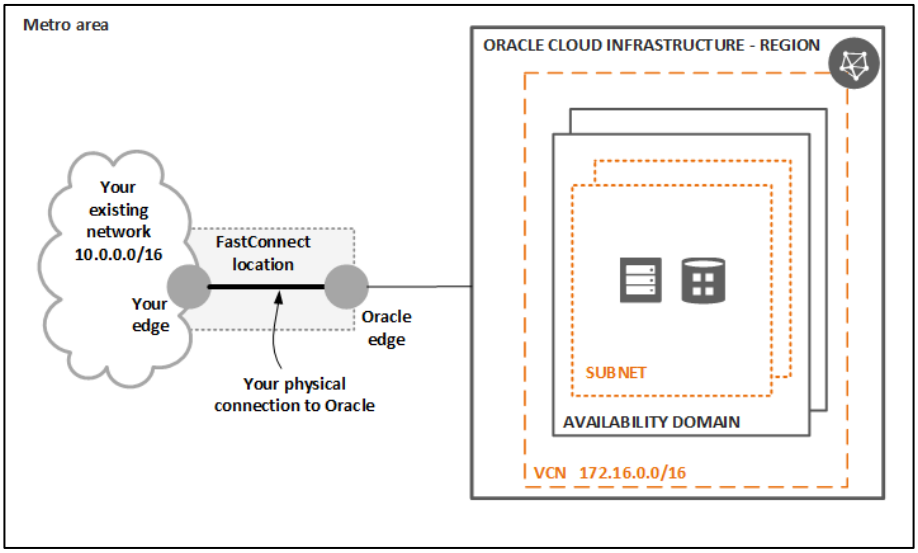


Diagrama de un modelo de colocación con la conexión física a Oracle en la ubicación de FastConnect.

Puede utilizar un único FastConnect para acceder a varias VCN. Existen diferentes escenarios de red disponibles según las necesidades y el modelo de conectividad de FastConnect que utilice la organización. Para obtener más información, puede consultar los siguientes temas:

a) **Enrutamiento en tránsito dentro de una VCN de hub**: este escenario se puede utilizar con FastConnect o con VPN de sitio a sitio. Implica un único DRG y varias VCN en un diseño de hub y radios.

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/transitrouting.htm

b) **FastConnect con varios DRG y VCN**: este caso solo se puede utilizar con FastConnect y solo si utiliza un proveedor externo o se encuentra en la misma ubicación que Oracle. Implica varios DRG y circuitos virtuales privados.

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/fastconnectmultipledrgs.htm

Puede ampliar la información acerca de OCI FastConnect en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/fastconnect.htm

Para finalizar las conectividades híbridas en OCI, a continuación, dispone de una Guía en inglés sobre las conexiones redundantes, tanto con IPSec VPN como con FastConnect en Oracle para ampliar la información de las conexiones híbridas en OCI:

https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/connectivity-redundancy-guide.pdf

También puede revisar el siguiente post en inglés, acerca del uso de FastConnect y VPN con Oracle Integration Cloud (OIC):

https://blogs.oracle.com/integration/post/fastconnect-and-vpn-with-oracle-integration-cloud-oic

3. CONFIGURACIÓN SEGURA PARA ORACLE OCI - ARQUITECTURAS HÍBRIDAS

Las medidas de seguridad se dividen en tres grupos, Marco organizativo, Marco Operacional y Medidas de Protección del Esquema Nacional de Seguridad. En los siguientes puntos, se detallan los grupos Marco operacional y Medidas de protección con las medidas que aplican en la Categoría Alta del ENS.

3.1 MARCO OPERACIONAL

Este grupo está formado por las medidas a tomar para proteger la operación del sistema como un conjunto integral de componentes para un fin. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a las dimensiones de seguridad relevantes en el sistema a proteger y la categoría del sistema de información a proteger.

Se considera, en este sentido, que la organización ha dispuesto todos aquellos mecanismos de control físico necesarios, con objeto de evitar el acceso a la nube existentes por parte de personal no autorizado.

3.1.1 CONTROL DE ACCESO

El conjunto de medidas que establece el Control de acceso cubre todas las acciones que, bien preparatorias o ejecutivas, están orientadas a determinar qué o quién puede o no acceder a un recurso del sistema mediante una determinada acción. Con el cumplimiento de todas las medidas, se garantizará que nadie accederá a recursos sin la debida autorización. Adicionalmente, se establecerá la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema pudiendo configurarlo en Oracle mediante el Servicio OCI Identity and Access Management (OCI IAM).

3.1.1.1 IDENTIFICACIÓN Y REQUISITOS DE ACCESO

Cada VCN tiene varios componentes que afectan directamente al comportamiento de la red (tablas de rutas, listas de seguridad, opciones DHCP, Gateway de internet, etc.). Cada vez que cree un recurso en la nube, como una red virtual en la nube (VCN) o una instancia de recursos informáticos, debe especificar el compartimiento de IAM en el que desea que se encuentre el recurso. Al crear uno de estos componentes, debe establecer una relación entre dicho componente y la VCN. El administrador debe crear compartimentos y las políticas de IAM correspondientes para controlar qué usuarios de la organización acceden a qué compartimentos. En última instancia, el objetivo es garantizar que cada persona solo pueda acceder a los recursos que necesita.

Esto significará que debe permitir en una política tanto la creación del componente como la gestión de la propia VCN. Sin embargo, la capacidad de actualizar dicho componente (para cambiar las reglas de ruta, las reglas de la lista de seguridad, etc.) no necesita permiso para gestionar la propia VCN, aunque el cambio de dicho componente pueda afectar directamente al comportamiento de la red. Oracle ha diseñado esta discrepancia para proporcionar flexibilidad a la hora de otorgar menos privilegios a los usuarios y que no tenga que otorgar acceso excesivo a la VCN para que un usuario pueda gestionar otros componentes de la red.

Se debe tener en cuenta que al otorgar a alguien la posibilidad de actualizar un tipo de componente en particular, está confiándole implícitamente el control del comportamiento de la red. A efectos del control de acceso, cuando configure VPN de sitio a sitio, debe especificar el compartimento en el que desea que residan cada uno de los componentes. Si no está seguro del compartimiento que desea utilizar, coloque todos los componentes en el mismo compartimiento que la VCN. Debe tener en cuenta que los túneles de IPSec siempre residen en el mismo compartimiento que la conexión principal de IPSec.

Por tanto, es necesario gestionar los grupos de identidad para la administración, gestión y uso del servicio Networking para asignarles los permisos que correspondan, manteniendo el mínimo privilegio sin perjudicar la funcionalidad, de los miembros de esos grupos de identidad.

Puede consultar la Guía “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad” donde se detalla el proceso para la identificación y creación de grupos de identidad.

También puede ampliar la información sobre el control de acceso al servicio Networking en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/accesscontrol.htm

3.1.1.2 SEGREGACIÓN DE FUNCIONES Y TAREAS

Para un mayor control de las funciones y tareas es necesario aplicar los principios de gestión del acceso de "necesidad de conocimiento", "privilegios mínimos" y "segregación de funciones". Además, es necesario proporcionar un mecanismo mediante el cual la organización controle el acceso al entorno de los servicios en la nube y al contenido por el personal autorizado.

El control de acceso basado en roles (RBAC) ofrece una alternativa más segura al modelo de superusuario del tipo "todo o nada". Con RBAC, puede aplicar una política de seguridad en un nivel más específico. RBAC utiliza el principio de seguridad del privilegio mínimo.

Privilegio mínimo significa que un usuario dispone exactamente de la cantidad de privilegios necesaria para realizar un trabajo. Los usuarios comunes tienen privilegios suficientes para utilizar sus aplicaciones, comprobar el estado de sus trabajos, imprimir archivos, crear archivos nuevos, etc. Las capacidades que van más allá de las disponibles para los usuarios comunes se deben agrupar en perfiles de derechos. Los usuarios que realizarán trabajos que requieran algunas de las capacidades de superusuario deben asumir un rol que incluya el perfil de derechos adecuado.

Para segregar funciones y tareas para el acceso a la configuración de las redes, se deben crear grupos de identidad específicos y políticas que se centren en tipos de recursos individuales (por ejemplo, solo listas de seguridad), en lugar del concepto más amplio "virtual-network-family". El tipo de recurso "instance-family" también incluye varios permisos para las VNIC, que residen en una subred, pero se conectan a una instancia.

Hay un tipo de recurso denominado "local-peering-gateways" que se incluye en "virtual-network-family" e incluye otros dos tipos de recursos relacionados con el intercambio de tráfico de la VCN local (dentro de la región):

a) local-peering-from

b) local-peering-to

El tipo de recurso "local-peering-gateways" abarca todos los permisos relacionados con gateways de intercambio de tráfico local (LPG). Los tipos de recursos "local-peering-from" y "local-peering-to" se utilizan para otorgar permisos para conectar dos LPG y definir una relación de intercambio de tráfico dentro de una sola región.

Puede encontrar información acerca de los detalles de los servicios básicos en el siguiente enlace de Oracle, donde encontrará las combinaciones de verbo + tipo de recurso apropiado para segregar los permisos en el servicio de Networking:

https://docs.oracle.com/es-ww/iaas/Content/Identity/Reference/corepolicyreference.htm

3.1.1.3 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

En el proceso de gestión de derechos, es necesario asignar permisos esenciales y cómo deben gestionarse, debiendo crear políticas que limiten el nivel de acceso mediante un verbo de política diferente ("use" frente a "manage"). Si se da el caso, existen algunas diferencias que deben comprenderse sobre los verbos de la política de Networking.

Es necesario tener en cuenta que el verbo "inspect" no solo devuelve información general sobre los componentes de la red en la nube (por ejemplo, el nombre y el OCID de una lista de seguridad o de una tabla de rutas). También incluye el contenido del componente (por ejemplo, las reglas reales de la lista de seguridad, las rutas de la tabla de rutas, etc.).

Además, los siguientes tipos de capacidades están disponibles solo con el verbo "manage", no con el verbo "use":

a) Actualizar (activar/desactivar) "internet-gateways".

b) Actualizar "security-lists".

c) Actualizar "route-tables".

d) Actualizar "dhcp-options".

e) Conectar un gateway de enrutamiento dinámico (DRG) a una red virtual en la nube (VCN).

f) Crear una conexión de IPSec entre un equipo de DRG y equipos locales de cliente (CPE).

g) VCN de peer.

Los recursos de red, como VCN, subredes, tablas de rutas, listas de seguridad, gateways de servicio, gateways de NAT, conexiones VPN y conexiones FastConnect, se pueden mover de un compartimento a otro. Cuando se mueve un recurso a un nuevo compartimiento, las políticas inherentes del nuevo compartimiento se aplican inmediatamente.

Para configurar las políticas debe acceder mediante el menú de la consola en OCI → Identidad y seguridad → Políticas.

El enfoque más sencillo para otorgar acceso al Networking es la política que se muestra a continuación:

Política	Descripción
Allow group [NetworkAdmins] to manage virtual-network-family in compartment [VCN]	Permitir a los administradores de red gestionar una red en la nube.

Nota: Estas políticas utilizan nombres de grupos de seguridad y compartimentos de ejemplo. Debe asegurarse de sustituir los nombres entre corchetes por sus propios nombres dentro de la organización.

Esta política abarca la red en la nube y todos los demás componentes de Networking (subredes, listas de seguridad, tablas de rutas, gateways, etc.). También, para proporcionar a los administradores de red la capacidad de iniciar instancias y así poder probar la conectividad de red.

Política	Descripción
Allow group [NetworkAdmins] manage instance-family in compartment [VCN]	Permitir a los administradores de red gestionar instancias.

Debe gestionar diferentes permisos, utilizando diferentes verbos para el resto de grupos, que deban usar, gestionar o administrar los componentes de las redes de la organización.

Puede obtener más información acerca de la sintaxis de las Políticas en OCI mediante en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Identity/policysyntax/policy-syntax.htm

También dispone de más información acerca de las Políticas más comunes en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Identity/Concepts/commonpolicies.htm

3.1.2 EXPLOTACIÓN

Se incluyen en este apartado, todas aquellas medidas designadas como parte de la explotación de los servicios. El ENS define, a través de ellas, una serie de procesos tanto para el control como para la gestión que deberán llevarse a cabo por parte de las entidades.

Las medidas atienden a diferentes tareas que deberán ser llevadas a la práctica por el departamento de informática.

3.1.2.1 INVENTARIO DE ACTIVOS

El servicio Tagging (Etiquetado) de OCI permite agregar metadatos a los recursos, lo que brinda la posibilidad de definir claves y valores y asociarlos a recursos. Podrá utilizar las etiquetas para organizar y visualizar las redes según las necesidades de su organización. También podrá llevar el inventario de las redes definidas, su uso, su gestión, incluso gestionar el control de acceso para una mayor segregación de roles y funciones de los administradores y de los usuarios que las utilicen.

OCI dispone del servicio Tagging (Etiquetado), que permite agregar metadatos a los recursos, lo que brinda la posibilidad de definir claves y valores y asociarlos a los recursos, para dar cobertura a la medida y poder gestionar un inventario con el uso de estas etiquetas, pudiendo ser utilizadas para organizar y visualizar los recursos según las necesidades de una organización.

Este servicio ha sido tratado en la Guía “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad”, en la cual encontrará mas detalles acerca del uso y configuración de este servicio de Etiquetado en OCI.

3.1.2.2 CONFIGURACIÓN DE SEGURIDAD

En cuanto a la configuración de seguridad que exige el ENS en esta medida, requiere de la aplicación de una regla de “mínima funcionalidad” y “seguridad por defecto” para todos los recursos.

Para acceder a los servicios de Networking (Red) debe ir a la consola de OCI → Red → Redes virtuales en la nube.

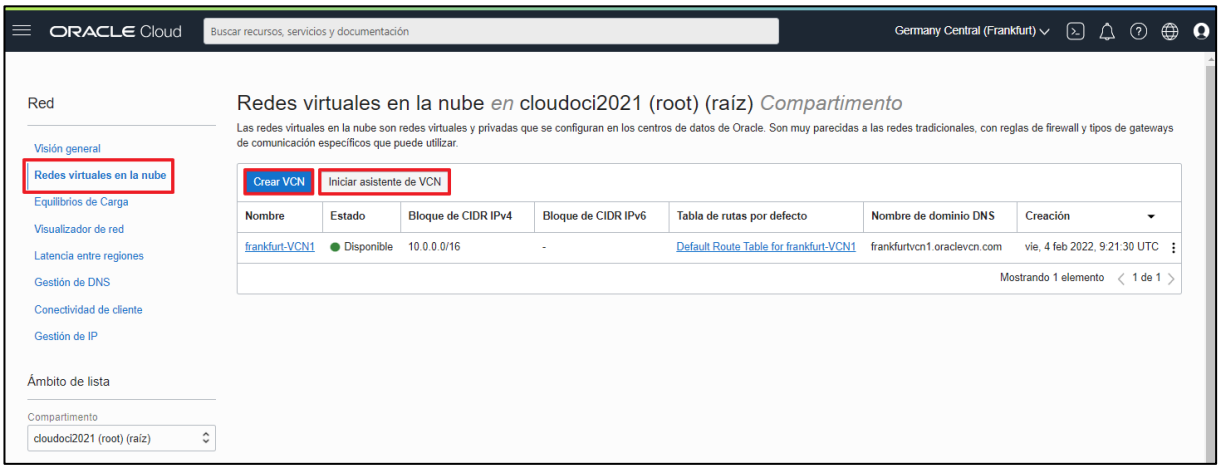


Imagen de la gestión de las VCN, donde se puede crear una VCN directamente o a través del asistente de VCN.

Desde esta consola puede gestionar todas las VCN creadas realizando una búsqueda por compartimentos si se ha realizado una segregación de funciones por ellos.

Dentro del servicio de red hay varias formas de controlar la seguridad de la red en la nube mediante los siguientes elementos:

a) **Subredes públicas frente a privadas**: puede designar una subred como privada, lo que significa que las instancias de la subred no pueden tener direcciones IP públicas. Puede obtener más información consultando el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/managingVCNs_topic-Overview_of_VCNs_and_Subnets.htm

Se recomienda segregar o particionar las VCN en subredes privadas y públicas. Asignar sus recursos en cada una de las subredes, usando las subredes privadas para proteger los recursos que deben estar aislados de internet y cumpliendo con las reglas de mínima funcionalidad y seguridad por defecto.

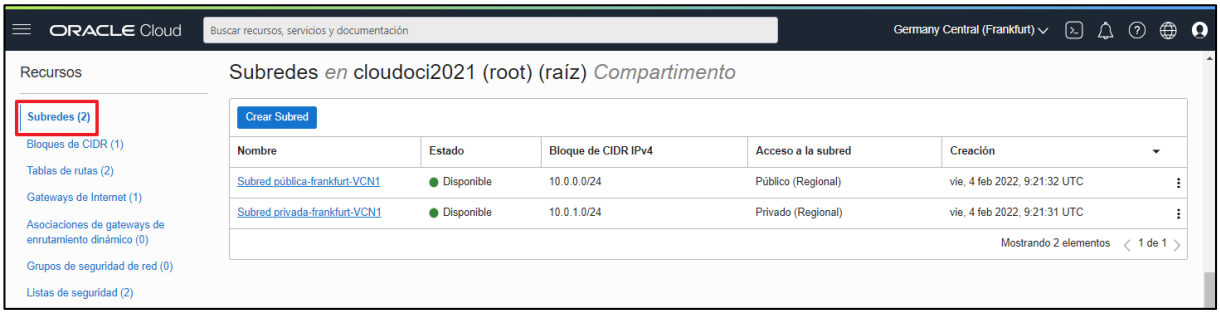


Imagen de las subredes creadas por defecto al crear una VCN.

b) **Reglas de seguridad**: para controlar el tráfico de nivel de paquetes dentro y fuera de una instancia. Las reglas de seguridad se configuran en la API de OCI o en la consola. Para implantar reglas de seguridad, se puede utilizar o Grupos de seguridad de red o Listas de seguridad. Estas reglas son tratadas en profundidad en el punto 3.2.1.3 SEGREGACIÓN DE REDES de este documento.

Puede obtener más información consultando el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/securityrules.htm

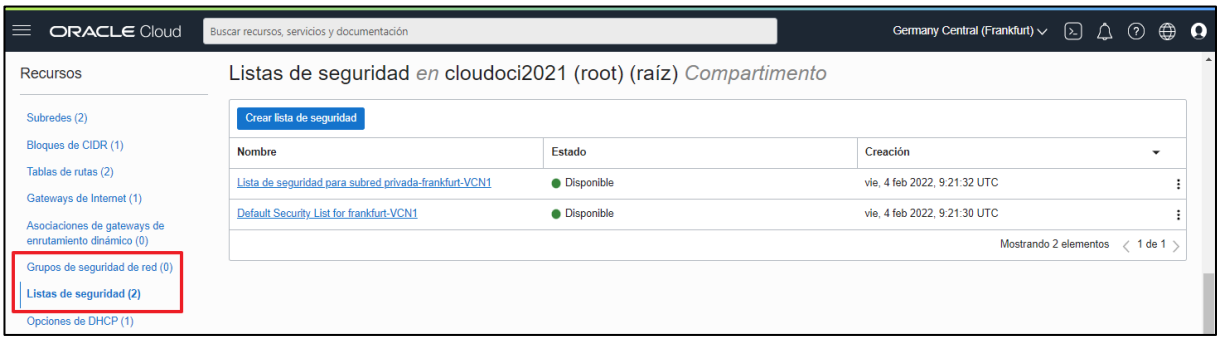


Imagen de las reglas de seguridad definidas por defecto en una lista de seguridad al crear una VCN.

c) **Reglas del firewall**: para controlar el tráfico de nivel de paquetes de entrada y salida de una instancia. Las reglas de firewall se configuran directamente en la propia instancia. Debe tener en cuenta que las imágenes de plataforma que ejecutan Oracle Linux incluyen automáticamente reglas predeterminadas que permiten la entrada en el puerto 22 de TCP para el tráfico SSH. Además, las imágenes de Windows incluyen reglas predeterminadas que permiten la entrada en el puerto 3389 de TCP para el acceso de escritorio remoto.

No obstante, debe definir las reglas de firewall que necesite para el control de acceso a las aplicaciones y servicios desplegados en las mismas instancias, autorizando solo a aquellas direcciones IP conocidas y puertos de origen y destino seguros para el establecimiento de las comunicaciones.

Nota: La lista de seguridad por defecto no incluye ninguna regla que permita el acceso de RDP. Para establecer una conexión con una instancia de Windows, se debe agregar una regla de entrada con estado para el tráfico TCP en el puerto de destino 3389 desde las direcciones IP y puertos de origen autorizados.

Es Importante saber que las reglas de firewall y las reglas de seguridad funcionan a nivel de instancias. Sin embargo, las listas de seguridad se configuran en el nivel de subred, lo que significa que todos los recursos de una subred determinada tienen el mismo conjunto de reglas de listas de seguridad. Además, las reglas de seguridad de un grupo de seguridad de red solo se aplican a los recursos del grupo. Al solucionar problemas de acceso a una instancia, debe asegurarse de que todos los siguientes elementos estén configurados correctamente: los grupos de seguridad de red en los que se encuentra la instancia, las listas de seguridad asociadas a la subred de la instancia y las reglas de firewall de la instancia.

d) **Gateways y tablas de rutas**: para controlar el flujo de tráfico general de la red en la nube a destinos externos (internet, la red local u otra VCN). Debe configurar los gateways de la red en la nube y las tablas de rutas en la API de OCI o la consola. Puede obtener más información de las tablas de rutas consultando el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/managingroutetables.htm

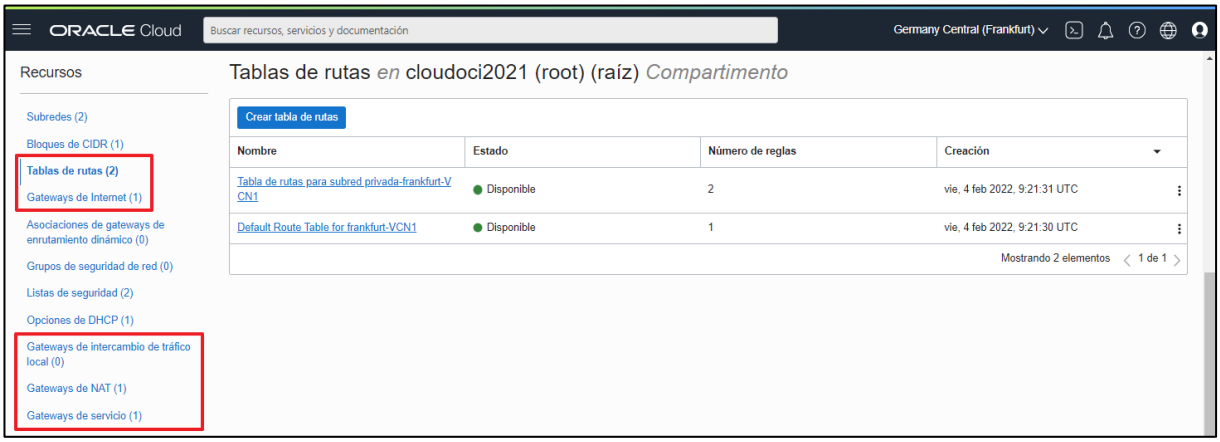


Imagen con las Tablas de rutas por defecto y los menús para ver el resto de Gateways de una VCN.

e) **Políticas de IAM**: para controlar quién tiene acceso a la API de OCI o a la propia consola. Puede controlar el tipo de acceso y los recursos en la nube a los que se puede acceder. Por ejemplo, puede controlar quién puede configurar la red y las subredes o quién puede actualizar las tablas de rutas, los grupos de seguridad de red o las listas de seguridad. Las políticas se configuran en la API de OCI o en la consola. Este tema ha sido tratado en el punto 3.1.1.3 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO de este documento

f) **Zonas de seguridad**: para asegurarse de que la red y otros recursos en la nube cumplen los principios de seguridad y las mejores prácticas de Oracle, debe crearlos en una zona de seguridad. Una zona de seguridad está asociada a un compartimento y comprueba todas las operaciones de gestión de red con respecto a las políticas de zona de seguridad. Por ejemplo, una zona de seguridad no permite el uso de direcciones IP públicas y solo puede contener subredes privadas.

Puede obtener más información consultando el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/security-zone/using/security-zones.htm

Para acceder a este menú, debe entrar desde OCI → Identidad y seguridad → Zonas de seguridad.

Imagen del menú de Zonas de seguridad desde el menú de Identidad y seguridad.

3.1.2.3 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

En esta medida es necesario registrar las actividades de los usuarios en el sistema, de forma que se compruebe quién realiza una actividad, cuándo la realiza y sobre qué recurso, como son las redes. Se debe incluir detalles de la actividad de los usuarios operadores y administradores de las redes para este caso concreto y OCI dispone del servicio Audit (Auditoría) para ello.

El servicio Auditoría de OCI registra automáticamente llamadas a todos los puntos finales soportados de la interfaz pública de programación de aplicaciones (API) de OCI como eventos de log. Actualmente, todos los servicios soportan el registro mediante Auditoría como el servicio de Networking.

Este servicio ha sido descrito en la Guía “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad”, en la que encontrará más detalle sobre el registro de la actividad de los usuarios.

3.1.2.4 PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

La protección de los registros del sistema es una medida que establece el ENS y que establece la necesidad de garantizar la protección de registros mediante un periodo de retención de los registros, en los que se asegurará la fecha y hora de los mismos, así como que estos, no puedan modificarse ni ser eliminados por personal n autorizado. Además, las copias de seguridad, si existen, deben mantener la misma seguridad antes mencionada.

Oracle cumple con las normas establecidas por el ENS para la protección de los registros a través de sus servicios de Auditoria y Registro de logs, disponiendo del correspondiente Certificado de Conformidad con el ENS en la categoría Alta, proporcionando una retención de registros en dichos servicios y que ha sido detallado en la Guía “CCN-STIC-889B Guía de Configuración segura para Monitorización y gestión”, en la que encontrará más detalle sobre la protección de los registros de actividad.

3.1.2.5 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

Esta medida requiere que las claves criptográficas se protejan durante todo su ciclo de vida, desde la generación, su transporte al punto de explotación, la custodia durante la explotación, el archivo posterior a su retirada de la explotación activa y su destrucción final cuando ya no sean necesarias.

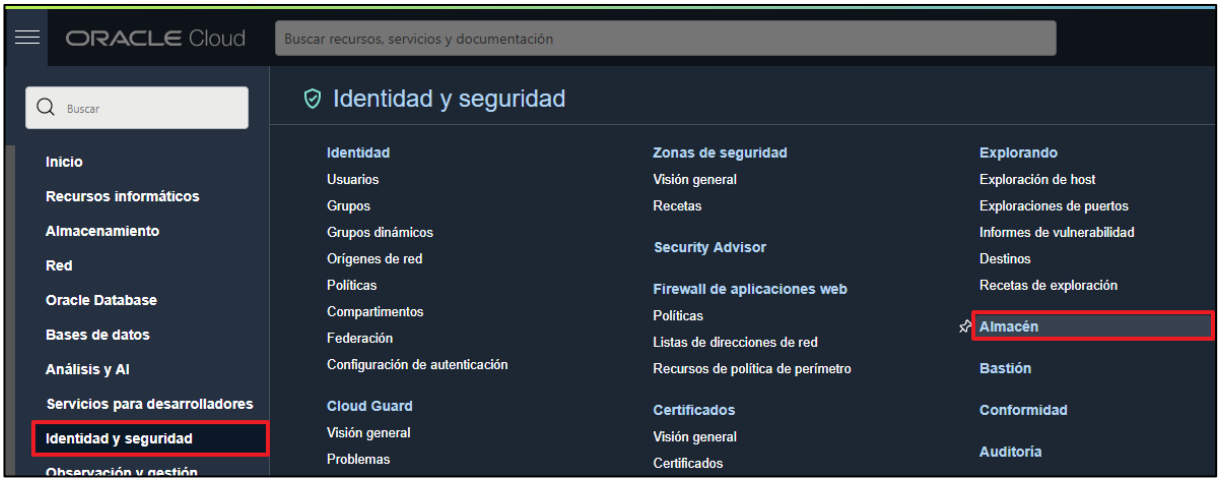
OCI dispone de claves gestionadas de forma automática para muchos de los servicios de la nube, pero también es posible elegir el uso de claves gestionadas por la organización. Para ello dispone del servicio Vault (Almacén) que permite gestionar de forma central las claves de cifrado que protegen los datos y las credenciales secretas que utiliza para acceder de forma segura a los recursos. Los almacenes guardan de manera segura secretos y claves de cifrado maestras que puede almacenar en los archivos de configuración o en el código. Específicamente, según el modo de protección, las claves se almacenan en el servidor o se almacenan en módulos de seguridad de hardware altamente disponibles y duraderos (HSM) que cumplen con la certificación de seguridad de nivel 3 de seguridad de los estándares de procesamiento de información federal (FIPS) 140-2.

El servicio Vault admite el acceso privado desde recursos de OCI en una red virtual en la nube (VCN) mediante un gateway de servicio. La configuración y el uso de un gateway de servicio en una VCN permite a los recursos (como las instancias a las que están asociados los volúmenes cifrados) acceder a servicios públicos de OCI, como el servicio Vault, sin exponerlos a Internet. No es necesario ningún gateway de Internet y los recursos pueden estar en una subred privada y utilizar solo direcciones IP privadas.

Puede obtener más información consultando el siguiente enlace de Oracle sobre los Gateway de servicio:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/servicegateway.htm

El servicio Vault se encuentra en la consola de OCI → Identidad y seguridad → Almacén.



El uso y configuración de este servicio queda detallado en la Guía "CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad" en el mismo punto para la protección de las claves criptográficas.

Finalmente, se recomienda la configuración del servicio Vault limitando el acceso solamente al grupo de usuarios administradores de claves.

3.1.3 MONITORIZACIÓN DEL SISTEMA

El ENS establece al respecto de esta norma que los sistemas estarán sujetos a medidas de monitorización de su actividad. El sistema de monitorización debe disponer de herramientas de detección o de prevención de intrusión, así como poder recopilar los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen, de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35 del RD 3/2010, de 8 de enero, por el que se regula el ENS.

3.1.3.1 SISTEMA DE MÉTRICAS

Para esta medida, se recopilarán los datos necesarios atendiendo a la categoría alta del sistema para conocer el grado de implantación de las medidas de seguridad. Puede supervisar el estado, la capacidad y el rendimiento de los recursos de OCI mediante métricas, alarmas y notificaciones.

Hay varios espacios de nombres de métricas del servicio de OCI Monitoring (supervisión) relacionados con los recursos de red.

a) Para conectividad de instancias:

   i. **oci_vcn**: métricas relacionadas con las VNIC.

b) Para conectividad en la nube:

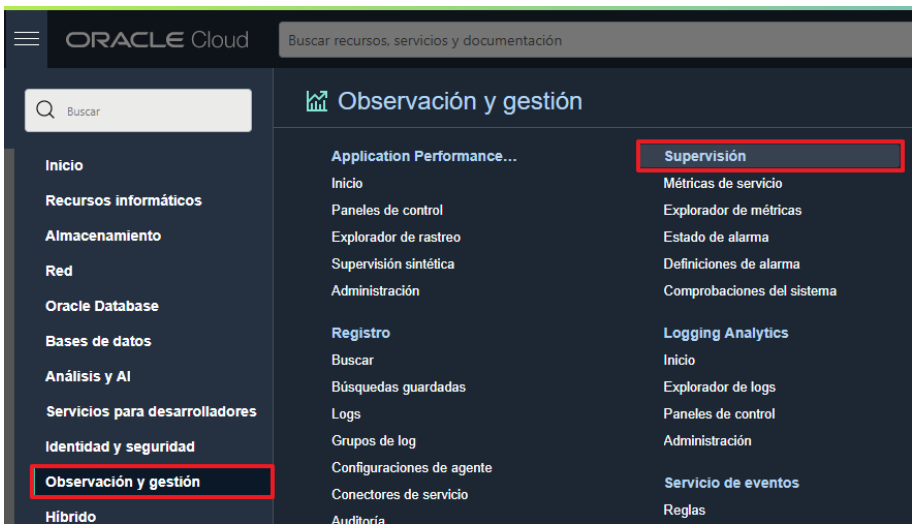
   i. **oci_fastconnect**: métricas relacionadas con FastConnect.

   ii. **oci_vpn**: métricas relacionadas con una conexión de IPSec.

   iii. **oci_service_gateway**: métricas relativas a un gateway de servicio.

   iv. **oci_nat_gateway**: métricas relacionadas con un gateway de NAT.

Se accede desde el menú de OCI → Observación y gestión → Supervisión.



Puede ampliar la información acerca de las métricas de cada tipo de conectividad de red en OCI a través del siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Reference/networkmetrics.htm

También puede consultar la Guía "CCN-STIC-889B Guía de Configuración segura para Monitorización y gestión", en la que encontrará más detalle sobre el servicio Monitoring (Supervisión) de OCI.

Finalmente, se recomienda supervisar de forma activa y pasiva los recursos de red a través de los servicios de monitorización de OCI. Configurando la prioridad de las alarmas dependiendo de la importancia del recurso, temas y suscripciones en el servicio de Notificaciones y métricas para las conexiones VPN y/o FastConnect.

3.2 MEDIDAS DE PROTECCIÓN

Este grupo de medidas cubre el espectro de aplicación de mecanismos más amplios en cuanto a dimensión. No obstante, debe tenerse en consideración que incluye una gran variedad de las mismas y que son aplicables desde las más puramente procedimentales, a las puramente físicas o a las de aplicación técnica.

Solo éstas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado es de aplicación sobre las funcionalidades de la nube.

Se considera, en este sentido, que la organización ha dispuesto todos aquellos mecanismos de control físico necesarios, con objeto de evitar el acceso a la nube existentes por parte de personal no autorizado.

3.2.1 PROTECCIÓN DE LAS COMUNICACIONES

El conjunto de medidas orientadas a la protección de las comunicaciones tiene como objetivo proteger la información en tránsito, así como dotar de los mecanismos necesarios para la detección y bloqueo de intrusos en una red.

Aunque fundamentalmente tienen un alcance mayor en cuanto a la implementación de sistemas de electrónica de red y control perimetral que aporta la infraestructura en la nube de Oracle, determinadas medidas pueden ser aplicables y gestionadas desde alguno de los servicios que ofrece OCI.

3.2.1.1 PROTECCIÓN DE LA CONFIDENCIALIDAD

La medida de protección de la confidencialidad dentro del conjunto de la protección de las comunicaciones establece el empleo de redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad, empleando los algoritmos acreditados por el Centro Criptológico Nacional. Para un nivel alto de aplicación del ENS indica que, se emplearán preferentemente dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Como ya se ha mencionado a lo largo de este documento, OCI dispone, dentro de su servicio Networking, del uso de conexiones VPN para conectar la infraestructura de la nube con la red local de la organización, mediante VPN de sitio a sitio u OCI FastConnect.

VPN de Sitio a Sitio

Para crear una conexión VPN de sitio a sitio debe acceder a través del menú de OCI → Red → VPN de sitio a sitio.

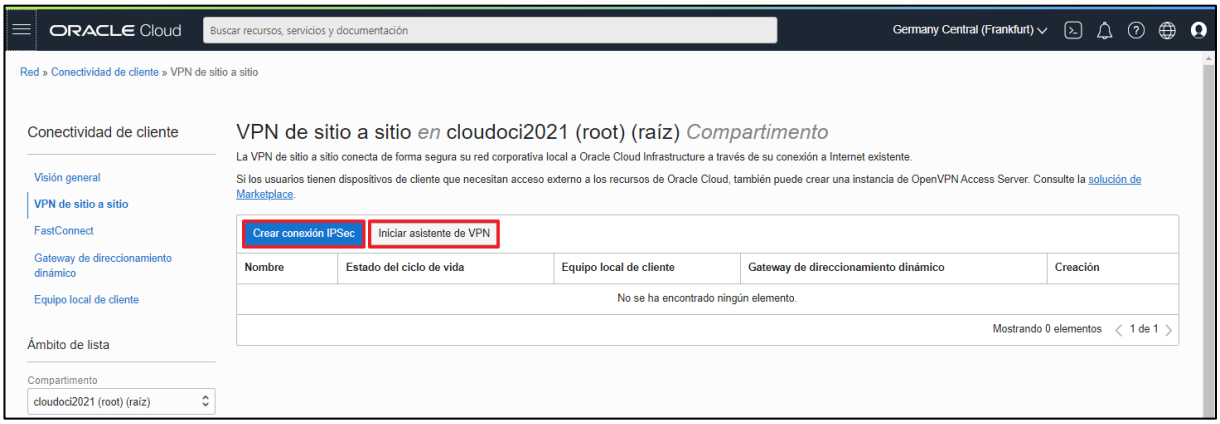


Imagen del menú de VPN de Sitio a Sitio donde crear la conexión IPSec directamente o mediante un asistente.

La creación de una VPN de sitio a sitio queda detallada en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/settingupIPsec.htm

Para utilizar el asistente, el siguiente enlace proporciona instrucciones para crear una conexión de VPN de sitio a sitio:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/quickstartIPsec.htm

Nota: Debe tener en cuenta que para el despliegue de esta conexión será necesario disponer de los permisos tanto para su creación como para su uso. A efectos del control de acceso, cuando configure VPN de sitio a sitio, debe especificar el compartimento en el que desea que residan cada uno de los componentes. Si no está seguro del compartimiento que debe utilizar, coloque todos los componentes en el mismo compartimiento que la VCN. Tenga en cuenta que los túneles de IPSec siempre residen en el mismo compartimiento que la conexión principal de IPSec

También puede encontrar configuraciones específicas de cómo realizar una conexión VPN a otros proveedores de nube, si la organización dispone de ellas, y fuera necesario enlazarlas en cuanto a las comunicaciones, mediante una VPN de sitio a sitio de Oracle. Para ello dispone de los siguientes enlaces de VPN a Azure, VPN a Amazon y VPN a Google:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/vpn_to_azure.htm

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/vpn_to_aws.htm

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/vpn_to_gcp.htm

OCI FastConnect

Para crear una conexión FastConnect debe acceder a través del menú de OCI → Red → FastConnect.

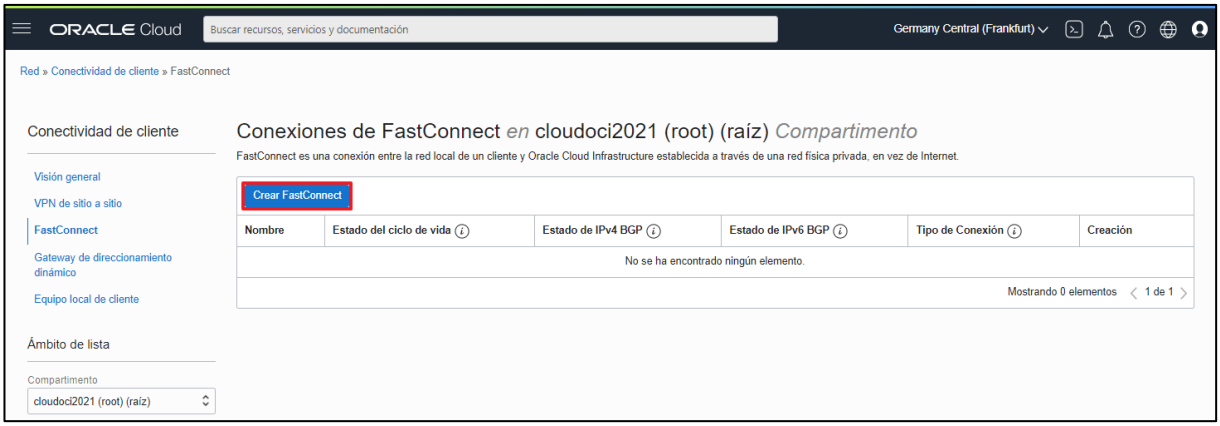


Imagen del menú de FastConnect desde donde se crea la conexión.

Para obtener más información sobre la redundancia con FastConnect en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/fastconnectresiliency.htm

Dentro de FastConnect también están disponibles varios tipos de modelos de conectividad que se indican a continuación:

a) FastConnect: con un partner de Oracle.

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/fastconnectprovider.htm

b) FastConnect: con un proveedor externo.

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/fastconnectthirdpartyprovider.htm

c) FastConnect: colocación con Oracle.

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/fastconnectcolocate.htm

Nota: Debe tener en cuenta que para el despliegue de alguna de estas conexiones o modelos será necesario disponer de los permisos tanto para su creación como para su uso.

Para comprobar los requisitos de hardware y enrutamiento, así como para las Políticas de IAM necesarias para la creación y uso de las conexiones, debe revisar el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/fastconnectrequirements.htm

3.2.1.2 PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

Cada servicio de OCI se integra con IAM con fines de autenticación y autorización para todas las interfaces (la consola, el SDK o la CLI, y la API de REST).

Un administrador de la organización precisará configurar grupos, compartimientos y políticas que controlen qué usuarios pueden acceder a qué servicios y recursos específicos, así como el tipo de acceso. Por ejemplo, las políticas controlan quién puede crear nuevos usuarios, crear y gestionar la red en la nube, iniciar instancias, crear contenedores, descargar objetos, etc.

Si un usuario normal (no un administrador) necesita utilizar los recursos de OCI de la organización, deberá contactar con algún miembro del grupo de administradores del tenant o administradores de redes para que configure su identificador de usuario. En este caso, el administrador debe confirmar qué compartimientos y recursos debe usar.

Sobre la gestión de derechos de usuario, mediante el uso de grupos, compartimientos y políticas, se ha tratado en el siguiente punto del documento 3.1.1.3 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO.

3.2.1.3 SEGREGACIÓN DE REDES

La segregación de redes acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.

La segregación de red es una técnica de seguridad que consiste en dividir una red en distintas subredes más pequeñas, que permiten a los equipos de red compartimentar las subredes y otorgar controles y servicios de seguridad únicos a cada subred.

Los Data Centers de Oracle tienen redes aisladas que se utilizan para prestar servicios en la nube a los clientes. Las tecnologías de red se despliegan con una arquitectura en varias capas, concebida para proteger los datos del cliente a varios niveles: físico, vínculo de datos, red, transporte y programa. Los controles de acceso se aplican a distintas capas: red, sistema, base de datos y programa. El acceso se basa en una política de "denegación por defecto".

La red se debe dividir en segmentos de forma que, haya un control de entrada de los usuarios que llegan a cada segmento, un control de salida de la información disponible en cada segmento y que las redes se puedan segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado.

El servicio de Networking ofrece dos funciones de firewall virtual que utilizan reglas de seguridad para controlar el tráfico en el nivel de paquete. Las dos funciones son:

a) **Listas de seguridad**: la función de firewall virtual original del servicio de Networking.

b) **Grupos de seguridad de red (NSG)**: función posterior diseñada para componentes de aplicaciones que tienen posiciones de seguridad diferentes. Los NSG solo se admiten para servicios específicos.

Ambas funciones utilizan reglas de seguridad, pero ofrecen diferentes maneras de aplicarlas a un conjunto de tarjetas de interfaz de red virtual (VNIC) en la red virtual en la nube (VCN).

A continuación, se resumen las diferencias básicas entre las dos funciones. También se explican los conceptos importantes de las reglas de seguridad que es necesario comprender para su implementación en la organización. El modo de creación, gestión y aplicación de reglas de seguridad varía entre las listas de seguridad y los grupos de seguridad de la red:

a) Las Listas de seguridad permiten definir un conjunto de reglas de seguridad que se aplica a todas las VNIC de una subred completa. Para utilizar una lista de seguridad determinada con una subred concreta, debe asociar la lista de seguridad a la subred, ya sea durante la creación de la subred o más adelante. Una subred se puede asociar con un máximo de cinco listas de seguridad. Todas las VNIC que se crean en esa subred están sujetas a las listas de seguridad asociadas con la subred.

   Puede ampliar la información acerca de la Listas de seguridad y sus reglas en el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/securitylists.htm

b) Los Grupos de seguridad de red (NSG) permiten definir un conjunto de reglas de seguridad que se aplica a un grupo de VNIC de su elección (o los recursos principales de las VNIC, como equilibradores de carga o sistemas de base de datos).

Por ejemplo, las VNIC que pertenecen a un conjunto de instancias informáticas que tienen la misma posición de seguridad. Para utilizar un NSG determinado, agregue las VNIC de interés al grupo. Las VNIC agregadas a ese grupo están sujetas a las reglas de seguridad de ese grupo. Se puede agregar una VNIC a un máximo de cinco NSG.

Puede ampliar la información acerca de los Grupos de seguridad y sus reglas en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/networksecuritygroups.htm

La siguiente imagen, ilustra el concepto del uso de las reglas de seguridad en ambas funciones.

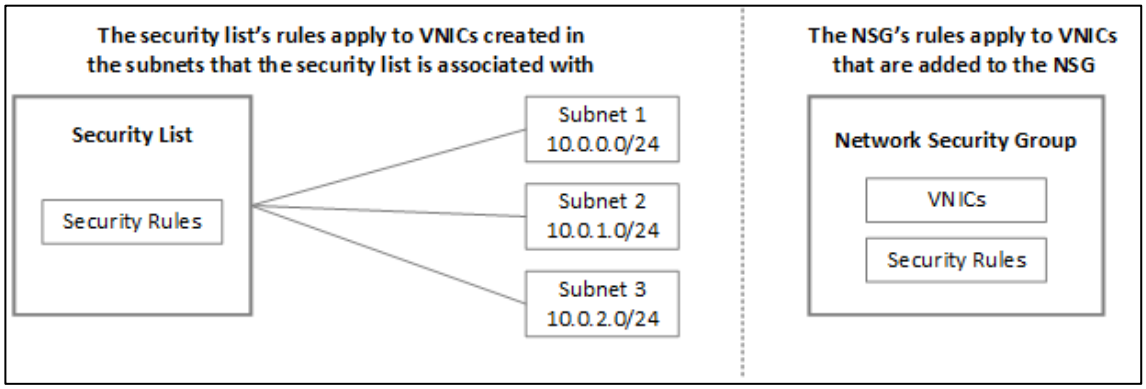


Imagen sobre las diferencias de concepto entre Listas y Grupos de seguridad

VCN proporciona automáticamente una lista de seguridad predeterminada que contiene varias reglas de seguridad definidas que sirven de ayuda para empezar a utilizar el servicio de Networking.

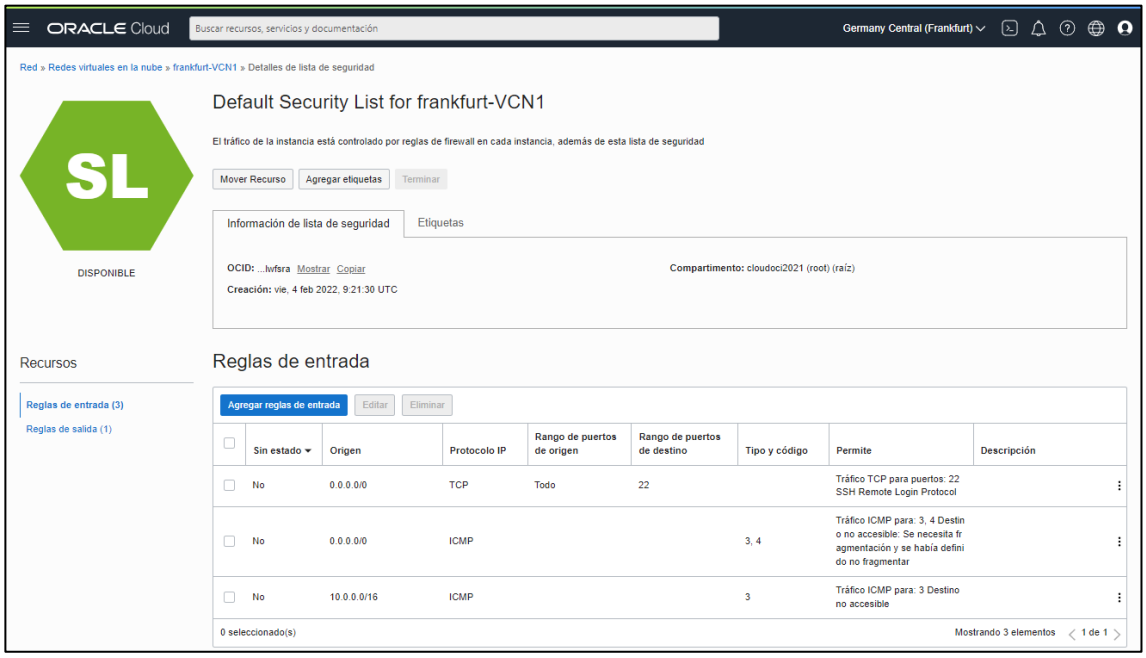


Imagen de la lista de seguridad predeterminada al crear una VCN con las reglas mínimas establecidas.

Al crear una subred, la lista de seguridad predeterminada se asocia a la subred a menos que se especifique una lista de seguridad personalizada ya creada en la VCN. En comparación, la VCN no tiene ningún grupo de seguridad de red predeterminado.

Se recomienda utilizar NSG para los componentes que tienen la misma posición de seguridad.

Por ejemplo, en una arquitectura de varios niveles, tendrá un NSG independiente por cada nivel. Todos las VNIC de un nivel determinado pertenecen a la NSG de ese nivel. En un nivel determinado, es posible que tenga un subconjunto determinado de las VNIC del nivel que tienen requisitos de seguridad adicionales y especiales. Por lo tanto, debe crear otro NSG para esas reglas adicionales y colocar ese subconjunto de VNIC en el NSG del nivel y en el NSG adicional.

Oracle recomienda usar NSG, porque son más flexibles y permiten aplicar políticas de seguridad de grano más fino. Pero también es importante indicar que se puede trabajar con ambas configuraciones a la vez, Listas y Grupos de seguridad ya que no son excluyentes y pueden trabajar conjuntamente.

Puede ampliar la información acerca de las Reglas de seguridad en las redes VCN en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/securityrules.htm

3.2.2 PROTECCIÓN DE LA INFORMACIÓN

Este conjunto de medidas trata todo lo relacionado con la protección de la información, desde lo dispuesto por las diferentes leyes nacionales y de la Unión Europea acerca de los datos personales, así como las distintas dimensiones que alcanzan cada uno de los aspectos relacionados con la información, su clasificación, accesos, responsables, tratamiento, almacenamiento, limpieza o destrucción, cuando ésta ya no sea necesaria.

Siendo uno de los activos más valiosos para cualquier organización, la información debe protegerse para garantizar la confidencialidad, disponibilidad e integridad de los datos. Para ello, la información debe ser clasificada e identificada para la aplicación de las medidas necesarias y adecuadas para su preservación. Sin embargo, la mayoría de estas medidas presentan un carácter más organizativo y procedimental, aunque también existen medidas de carácter técnico para permitir la comprobación de dimensiones como la autenticidad de la procedencia y la integridad de la información.

3.2.2.1 CIFRADO

Dentro de esta medida de seguridad, el ENS establece que la información durante su transmisión debe estar cifrada y el uso de criptografía debe cumplir las normas de protección de la confidencialidad, así como las del uso de criptografía con productos y algoritmos acreditados por el CCN.

A tal respecto, Oracle dispone del Certificado de Conformidad con el ENS en la categoría Alta, por lo que tan solo es necesario implementarlo en las redes privadas virtuales ya que en las comunicaciones internas está presente por defecto sin que sea necesaria ninguna configuración adicional.

En cuanto a las redes privadas virtuales, de las que dispone OCI para conectar diferentes infraestructuras entre sí, se indica el tipo de cifrado usado en cada una de ellas:

Cifrado mediante IPSec en VPN

OCI solo admite el modo de túnel para VPN con IPSec. Cada conexión IPSec de Oracle consta de varios túneles IPSec redundantes. Para un túnel determinado, puede utilizar un enrutamiento dinámico con el Protocolo de gateway de borde (BGP) o un enrutamiento estático para enrutar el tráfico del túnel.

El conjunto de protocolos IPSec cifra el tráfico IP antes de transferir los paquetes del origen al destino y descifra el tráfico cuando llega.

En general, se puede configurar una conexión IPSec en los siguientes modos:

a) **Modo de Transporte**: IPSec cifra y autentica únicamente la carga útil real del paquete, y la información del encabezado permanece intacta.

b) **Modo de túnel** (admitido por Oracle): IPSec cifra y autentica todo el paquete. Después del cifrado, el paquete se encapsula para formar un nuevo paquete IP que tiene información de encabezado diferente.

Sobre el secreto compartido de túnel, y de forma predeterminada, Oracle asigna el secreto compartido al túnel a menos que se proporcione un secreto compartido. Puede proporcionar un secreto compartido para cada túnel al crear la conexión de IPSec, o después de crear los túneles. Para el secreto compartido, solo se permiten letras, números y espacios. Si cambia el secreto compartido de un túnel existente, el túnel se caerá mientras se reaprovisiona.

Los túneles de IPSec con VPN de sitio a sitio ofrecen las siguientes ventajas:

a) Las líneas públicas de internet se utilizan para transmitir datos, de modo que no son necesarias líneas específicas y con un coste adicional de un sitio a otro.

b) Las direcciones IP internas de las redes y los nodos participantes se ocultan a los usuarios externos.

c) Se cifra toda la comunicación entre los sitios de origen y destino, lo que disminuye significativamente las posibilidades de robo de información.

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/workingwithIPsec.htm#edit_shared_secret

Para acceder a la creación de una conexión IPSec, debe ir al menú de OCI → Red → VPN de sitio a sitio, y pulsar el botón de "Crear conexión IPSec".

Imagen para la creación de una conexión de IPSec en una VPN de Sitio a Sitio.

Puede encontrar información acerca de los parámetros de IPSec en el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/Network/Reference/supportedIPsecparams.htm

A continuación, se muestra el enlace al documento en Ingles sobre las mejores prácticas para IPSec en una red VPN de Sitio a Sitio de Oracle:

https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/ipsec-vpn-best-practices.pdf

Cifrado en OCI FastConnect

FastConnect se puede configurar para utilizar MACsec para proteger las conexiones de red a red en la capa 2. Cuando se activa MACsec, se selecciona un estándar de cifrado avanzado (AES) de algoritmo de cifrado, se intercambian y verifican dos claves de seguridad entre dos redes conectadas y, a continuación, se establece un enlace bidireccional seguro. El servicio Vault se encarga de almacenar de forma segura las claves de cifrado reales.

El uso de MACsec tiene los siguientes requisitos:

a) El dispositivo de equipo local de cliente (CPE) también debe admitir MACsec.

b) El circuito virtual de FastConnect o la velocidad del LAG deben ser de 10 Gbps o más.

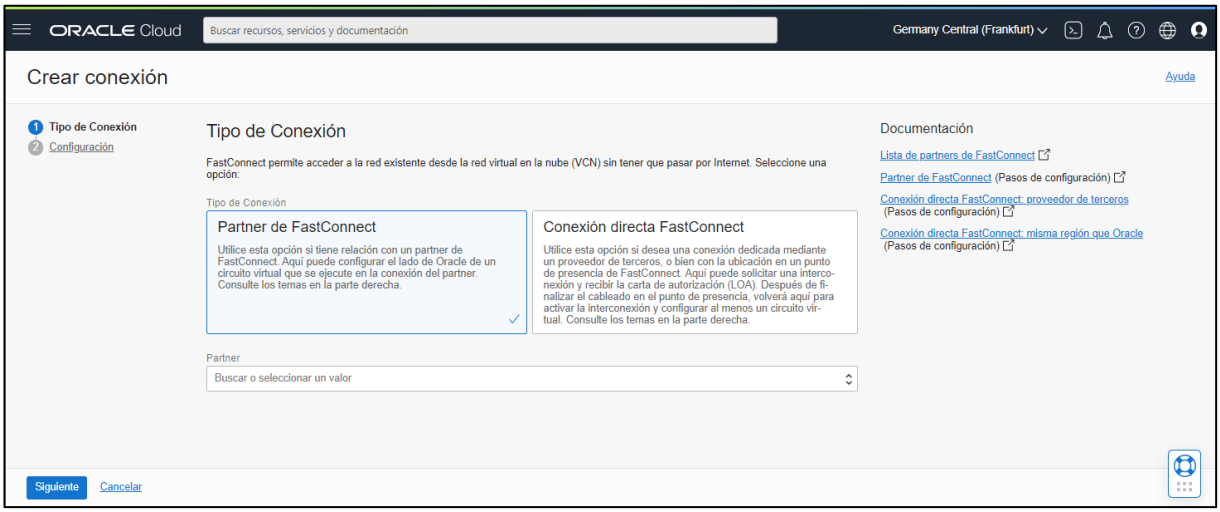
c) No todas las interconexiones o los grupos de interconexiones existentes pueden admitir MACsec. Para actualizar una interconexión o un grupo de interconexiones existente, la página de detalles de la interconexión o el grupo de interconexiones tiene un campo MACsec Encryption que podría establecerse en modo Capable o Incapable.

La conexión debe poder utilizar MACsec. Si la interconexión o el grupo de interconexiones no pueden utilizar MACsec, deberá volver a aprovisionar antes de configurar MACsec.

d) No todos los proveedores de terceros pueden admitir MACsec en el tipo de circuito que proporcionan. Deberá consultar al proveedor para verificar que el tipo de conectividad que adquiera sea compatible con MACsec.

Si decide agregar cifrado MACsec a una interconexión existente de FastConnect, recuerde que, cambiar la configuración de cifrado requiere reiniciar la sesión BGP que suspende brevemente el tráfico BGP.

Para agregar cifrado MACsec a una conexión FastConnect, antes debe crearla desde el menú de OCI → Red → FastConnect, y pulsar el botón de "Crear FastConnect".



Puede ampliar la información del cifrado MACsec, en la conexión FastConnect, en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/fastconnectoverview.htm#macsec

4. GLOSARIO

A continuación de describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía.

Término	Definición
AD	Availability Domain (Dominios de Disponibilidad).
AES	Advanced Encryption Standard (Algoritmo de Cifrado Avanzado).
API	Application Programming Interface (Interfaz de Programación de Aplicaciones).
BGP	Border Gateway Protocol (Protocolo de Gateway de Borde).
C@C	Oracle Cloud at Customer (Nube de Oracle en el cliente).
CAK	(Clave de Asociación de Conectividad).
CCN	Centro Criptológico Nacional.
CKN	(Nombre de Clave de asociación de Conectividad).
CPE	Dispositivo de equipo local de cliente.
DNS	Domain Name Server (Servidor de Nombre de Dominios).
DRG	Dynamic Route Gateway (Gateway de Enrutamiento Dinámico).
ENS	Esquema Nacional de Seguridad.
HSM	Hardware Security Module (Módulos de seguridad por Hardware).
IaaS	Infrastructure as a Service (Infraestructura como Servicio).
IAM	Identity and Access Management (Gestión de Identidad y Acceso).
IPSec	Internet Protocol security (Seguridad del Protocolo de Internet).
IPv4	Internet Protocol versión 4 (Protocolo de Internet versión 4).
IPv6	Internet Protocol versión 6 (Protocolo de Internet versión 6).
LPG	Local Peering Gateways (Gateway de Intercambio de Tráfico Local).
MACsec	Estándar IEEE 802.1AE para proteger las conexiones de red a red en la capa 2.
NAT	Network Address Translation (Traducción de Direcciones de Red).
NSG	Network Security Group (Grupo de Seguridad de Red).
OCI	Oracle Cloud Infrastructure (Infraestructura de Nube de Oracle).
OCID	Oracle Cloud Identity (Identificador de la Nube de Oracle).
OIC	Oracle Integration Cloud (Nube de Integración de Oracle).
PaaS	Platform as a Service (Plataforma como Servicio).
RPC	Remote Peering Conection (Conexión con Intercambio de Tráfico Remoto).
SDK	Software Development Kits (Paquetes de Desarrollo de Software).
SOC	Security Office Center (Centro de Operaciones de Seguridad).
SSH	Secure Shell (Protocolo de Conexión Segura).
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión).
VCN	Virtual Cloud Network (Red Virtual en la Nube).
VNIC	Virtual Network Interface Card (Tarjeta de Interfaz de Red Virtual).
VPN	Virtual Private Network (Red Privada Virtual).
RBAC	Role-Based Access Control (Control de Acceso Basado en Roles).

5. RESUMEN Y APLICACIÓN DE MEDIDAS

El siguiente cuadro, resume las medidas de seguridad a implementar para valorar el nivel de cumplimiento.

Control ENS	Medidas y Configuración	Estado	
OP	MARCO OPERACIONAL		
OP.ACC	CONTROL DE ACCESO		
op.acc.1	Identificación	Aplica	Cumple
	Se ha configurado el uso de cuentas para la administración de las redes del tenant.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.2	Requisitos de acceso	Aplica	Cumple
	Se han creado los grupos de administración, gestión y uso para las redes y compartimentos del tenant.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.3	Segregación de funciones y tareas	Aplica	Cumple
	Se han creado grupos de seguridad basados en roles (RBAC) para los recursos de red.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.acc.4	Proceso de gestión de derechos de acceso	Aplica	Cumple
	Se han creado Políticas de IAM para restringir el acceso a recursos de red solo a los grupos permitidos para gestionar recursos de red.	☐Si ☐No	☐Si ☐No
		Observaciones:	
OP.EXP	EXPLOTACIÓN		
op.exp.1	Inventario de activos	Aplica	Cumple
	Se han creado etiquetas para segregar aun mas los permisos de acceso a los recursos de la red.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han creado etiquetas para inventariar y catalogar los recursos de la red.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.2	Configuración de seguridad	Aplica	Cumple
	Se han particionado las VCN en subredes privadas y públicas.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se han definido reglas de firewall para controlar el acceso a las aplicaciones y servicios de la instancia.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha utilizado un gateway de NAT para la conectividad a Internet desde instancias informáticas privadas.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha utilizado un gateway de servicio para la conectividad a la red de servicios de Oracle.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.11	Protección de claves criptográficas	Aplica	Cumple
	Se ha configurado el servicio Vault (almacén), limitando el acceso tan sólo al grupo de usuarios administradores de claves.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado un almacén para alojar las claves de MACsec de las conexiones FastConnect.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
OP.MON	MONITORIZACIÓN DEL SISTEMA		
op.mon.2	Sistema de Métricas	Aplica	Cumple
	Se está supervisando de forma activa y pasiva los recursos de red a través de los servicios de monitorización de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado la prioridad de las alarmas dependiendo de la importancia del recurso.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han creado temas y suscripciones en el servicio de Notificaciones para la publicación de mensajes.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han configurado las métricas para las conexiones VPN y/o FastConnect.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
MP	MEDIDAS DE PROTECCIÓN		
MP.COM	PROTECCIÓN DE LAS COMUNICACIONES		
mp.com.2	Protección de la confidencialidad	Aplica	Cumple
	Se ha configurado una conexión VPN de Sitio a Sitio.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado una conexión FastConnect.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.com.4	Segregación de redes	Aplica	Cumple
	Se han configurado Compartimentos para alojar las VCN y segregar aun más la red	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han configurado Listas de seguridad para las VCN.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han configurado Grupos de seguridad (NSG) para las VCN.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
MP.INFO	PROTECCIÓN DE LA INFORMACIÓN		
mp.info.3	Cifrado	Aplica	Cumple
	Se ha configurado IPSec para VPN de Sitio a Sitio.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado un almacén para el cifrado MACsec de FactConnect.	☐Si ☐No	☐Si ☐No
		Observaciones:	

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL