

CONFIGURACIÓN DE FIREWALL EN CLOUD DATACENTER

Cloud Datacenter

El centro de datos virtual para
salvaguardar tu información
y operar en la Nube



Calle San Rafael, 14
28108 Alcobendas (Madrid)
900 103 293
www.acens.com

acens
the *Cloud* services company

Una compañía de *Telefonica*

ÍNDICE

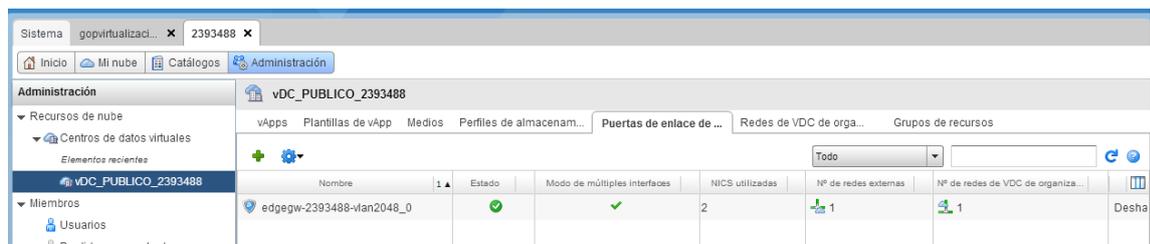
- 1 Firewall en Cloud Datacenter 3
- 2 Direccionamiento IP 4
- 3 Configuración de NAT..... 5
- 4 Configuración de las reglas de Firewall 9

Firewall en Cloud Datacenter

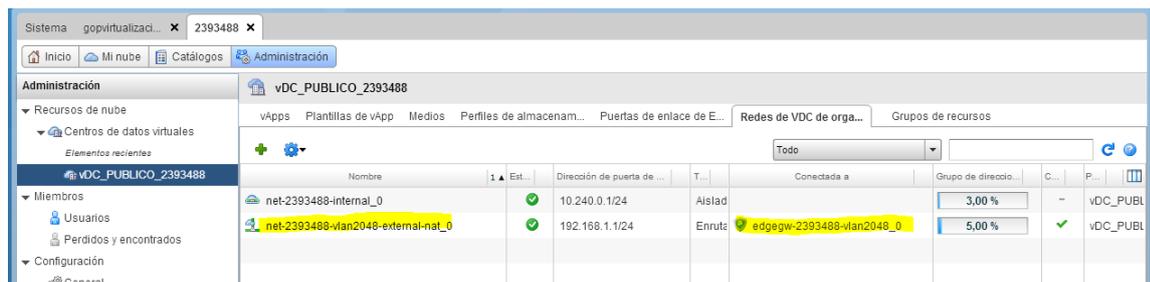
El servicio de **Cloud Datacenter** incluye, para todas las modalidades de VDC, una red privada, red pública y elemento firewall como parte de la infraestructura del Virtual DataCenter. Este elemento es implementado por el VMware vShield Edge como parte de la suite de VMware vCloud Director y proporciona funcionalidades de filtrado, traducción de direcciones IP (NAT) y servicio de balanceo de tráfico.

En este manual se recogen los pasos necesarios para la publicación en Internet de un servidor virtual desplegado dentro del centro de datos virtual y la gestión de permisos de acceso al mismo.

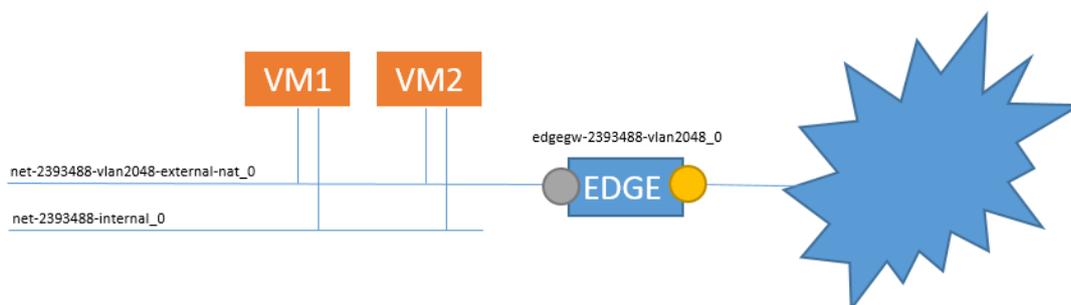
Podemos encontrar dicho elemento en la pestaña ‘Administración’ seleccionando la organización que corresponda dentro de ‘Centro de datos virtuales’



El elemento en la imagen tiene conectadas a éste las llamadas redes de organización, que puedes encontrar en la siguiente captura y como puedes ver, tienen una referencia del vShield Edge al que están conectadas:



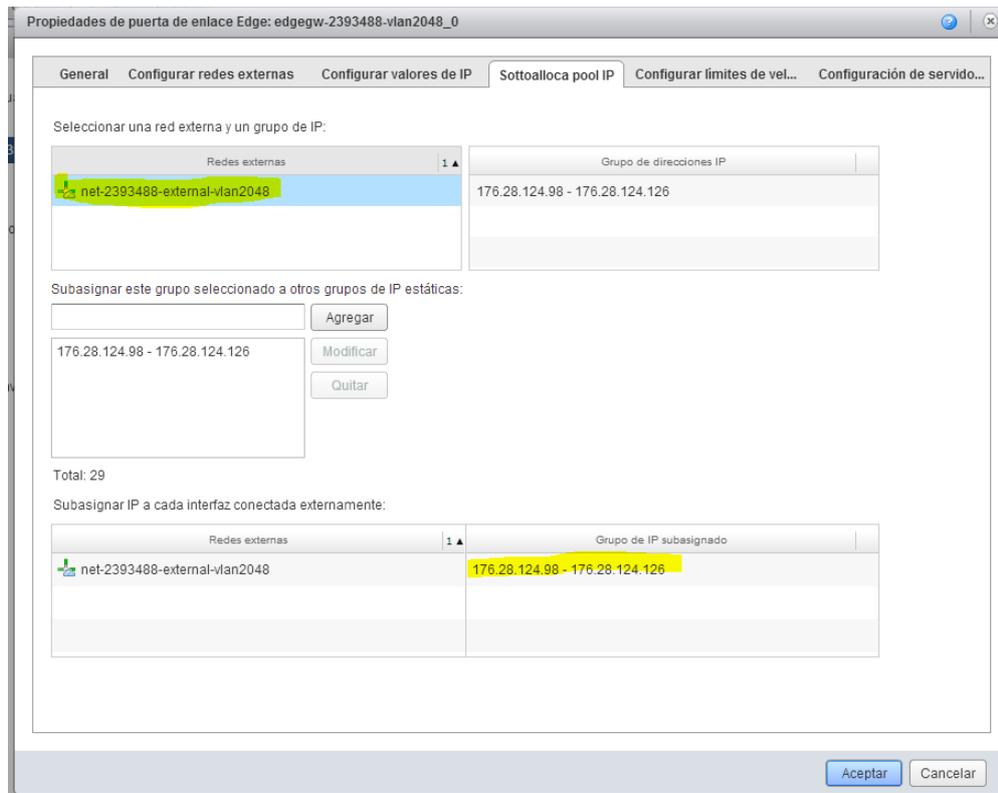
La topología lógica de esta infraestructura sería más o menos así:



Es importante tener en consideración que, por defecto no se incluye ninguna configuración de firewall por lo que **es necesario configurar el tráfico entrante/saliente y las reglas de filtrado entrantes/salientes**. Si no realizamos estas configuraciones no tendremos acceso hacia el exterior.

Direccionamiento IP

Con el servicio de Cloud Datacenter se incluye un rango de direcciones público para la publicación de servicios en Internet (ver [tabla de características](#)). Para averiguar el direccionamiento IP asignado tendremos que seleccionar el Edge y con el botón derecho ir a la opción: **Propiedades** → **Sottoalloca pool IP** → **Seleccionar la red externa** y comprobar en la parte inferior las IPs disponibles:



Hay que tener muy presente este rango de IPs, porque serán nuestras IPs públicas, estas son las IPs que podemos utilizar en nuestra configuración de los servicios.

Una vez que conocemos la disponibilidad de nuestras IPs comenzaremos a realizar las configuraciones necesarias de NAT y Firewall.

Configuración de NAT

El primer paso será la configuración de las reglas de traducción de nombres para la publicación de servicios en Internet. La configuración de las reglas de NAT se realiza para redirigir en tráfico desde una IP externa a una IP interna y para que dicha máquina salga al exterior con una IP concreta (de nuestro pool que hemos podido ver en la [parte anterior del texto](#)). Se hará por lo tanto, una traducción de entrada y una traducción de salidas para el tráfico.

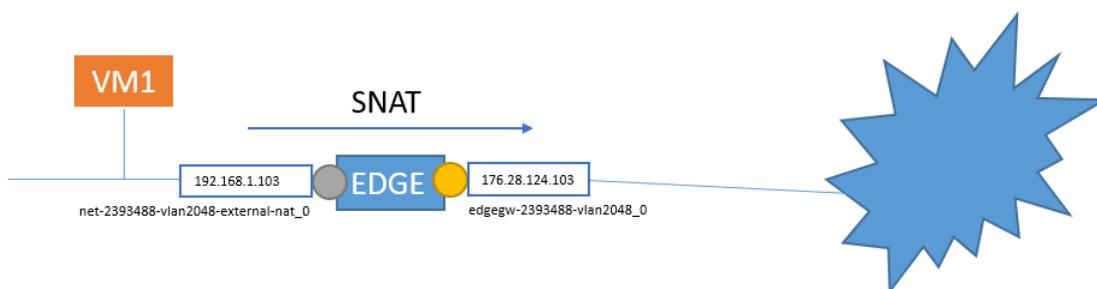
CONFIGURACIÓN DE NAT DE SALIDA (SNAT)

Vamos a configurar el tráfico de salida de una VM. Para ello primero tendremos que comprobar que nuestra máquina tiene una IP de la red de organización y que la tarjeta de red está pinchada a esta y no a otro tipo de red, como pueden ser redes internas o directas:

Diagrama de vApp		Máquinas virtuales	Redes
Consola	1 ▲	Estado	SO
	Encendido	Microso	Redes
			NIC 0*: net-2393488-vlan2048-external-nat_0
			Dirección IP
			192.168.1.103
			IP...
			-

Observa la imagen donde podemos ver donde está conectada la VM y la IP privada que tiene dicha VM. Ahora que tenemos el primer dato, la ip interna (192.168.1.103), necesitamos el segundo dato, que será la IP pública que tendrá esta máquina cuando salga a Internet. Para ello, revisamos nuestro **Sottoalloca pool IP** y elegimos una... la que queramos, por ejemplo la IP 176.28.124.103.

Tendremos que configurar ahora el tráfico saliente para esta máquina:



Dentro del EDGE en la pestaña “NAT” utiliza el botón SNAT. Con la configuración que puedes ver a continuación, tu máquina tendrá tráfico saliente a Internet y hará una conversión de la IP 192.168.1.103 a la IP 176.28.124.103, presentándose en los HOST remotos con este direccionamiento público.

Editar regla NAT de origen

Una regla NAT de origen modifica la dirección IP de origen de los paquetes salientes. Utilice el control Aplicado/a sobre para especificar una red a la que aplicar la regla. Utilice el control Rango/IP de origen (interno) original para especificar un rango de direcciones IP de origen de esa red a la que se aplica la regla. Utilice el control Rango/IP de origen (externo) traducido para especificar el rango de direcciones IP al que se traducirán las direcciones de origen de los paquetes salientes. Para obtener más información, consulte la Ayuda.

Aplicada sobre: net-2393488-external-vlan2048

Rango/IP de origen (interno) original: 192.168.1.103 *

Rango/IP de origen (externo) traducido: 176.28.124.103 *

Habilitada

Aceptar Cancelar

Una vez que hemos configurado el tráfico saliente, tendremos que configurar el tráfico entrante para dicha máquina. Esta configuración será la inversa y se configurará con el llamado DNAT.

Salida de varias IPs:

Tienes la posibilidad de configurar una regla de salida para múltiples máquinas, utilizando el rango de salida a través de la misma IP: 192.168.1.2 – 192.168.1.103

CONFIGURACIÓN DE NAT DE ENTRADA (DNAT)

La configuración de direcciones IP de entrada permite acceder desde Internet a cualquier servidor de red privada a través de una dirección IP pública. La translación de los paquetes desde el direccionamiento público al interno se puede utilizar de dos maneras:

1. Dejando pasar todo el tráfico (ANY) destinado a ese servidor.

Una regla NAT de destino modifica la dirección IP de destino y, opcionalmente, el puerto de los paquetes de entrada. Utilice el control Aplicado/a sobre para especificar una red a la que aplicar la regla. Utilice el control Rango/IP (externo) original para especificar un rango de direcciones IP de destino de esa red a la que se aplica la regla. Utilice el control Rango/IP (interno) traducido para especificar un rango de direcciones IP al que se traducirán las direcciones de destino de los paquetes de entrada. Opcionalmente, puede restringir los paquetes coincidentes a un puerto específico o un tipo de paquete ICMP. Para obtener más información, consulte la Ayuda.

Aplicada sobre:

Rango/IP (externo) original: *

Protocolo:

Puerto original:

Tipo de ICMP:

Rango/IP (interno) traducido: *

Puerto traducido:

Habilitada

2. Dejando pasar el tráfico que va a un protocolo concreto (PUERTO). Esto permite utilizar una única dirección IP en la red externa para publicar servicios de múltiples servidores.

Una regla NAT de destino modifica la dirección IP de destino y, opcionalmente, el puerto de los paquetes de entrada. Utilice el control Aplicado/a sobre para especificar una red a la que aplicar la regla. Utilice el control Rango/IP (externo) original para especificar un rango de direcciones IP de destino de esa red a la que se aplica la regla. Utilice el control Rango/IP (interno) traducido para especificar un rango de direcciones IP al que se traducirán las direcciones de destino de los paquetes de entrada. Opcionalmente, puede restringir los paquetes coincidentes a un puerto específico o un tipo de paquete ICMP. Para obtener más información, consulte la Ayuda.

Aplicada sobre:

Rango/IP (externo) original: *

Protocolo:

Puerto original:

Tipo de ICMP:

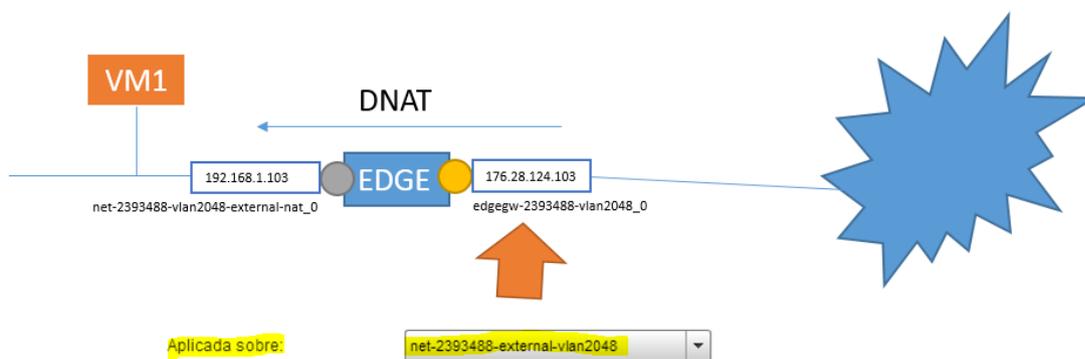
Rango/IP (interno) traducido: *

Puerto traducido:

Habilitada

Esta regla traducirá el tráfico destinado al puerto 3389 de la IP 176.28.124.103 y lo trasladará al puerto 3389 de la dirección IP 192.68.1.103.

Ten muy presente que en estas configuraciones es muy importante la opción **“Aplicada Sobre”** esta debe ser siempre la parte externa del EDGE:



(i!) Hasta aquí sólo se ha configurado la funcionalidad necesaria para la traducción de direcciones IP y el Edge estará preparado para hacer la traslación del tráfico que venga a la IP pública y salga de nuestra IP privada.

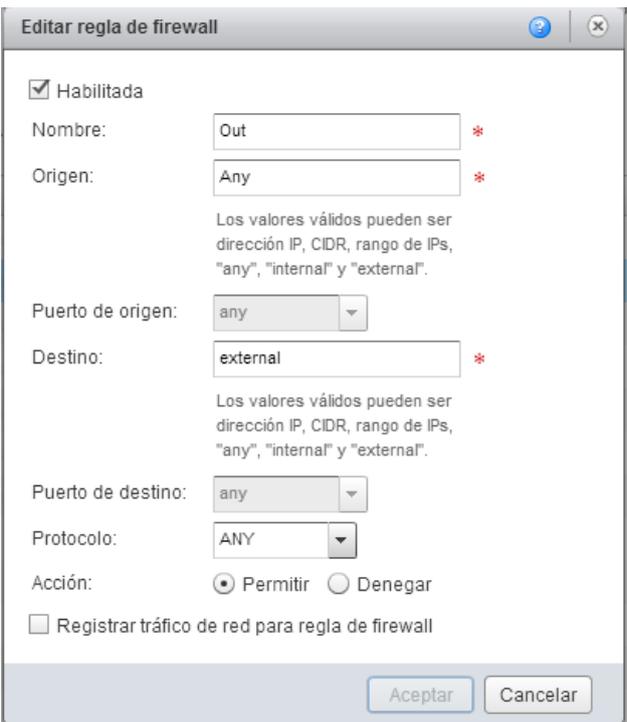
Configuración de las reglas de Firewall

Una vez configurada la función de NAT, sólo quedaría configurar los permisos de acceso. **El Firewall por defecto no viene configurado** de manera que ni el tráfico entrante ni el tráfico saliente está permitido así que para habilitar el acceso es necesario proceder con la configuración de, al menos, dos reglas: **una regla para el tráfico saliente (VDC -> Internet) y una regla entrante (Internet -> VDC).**

CONFIGURACIÓN DE TRÁFICO DE SALIDA

Las reglas de tráfico saliente controlan el acceso desde los servidores virtuales desplegados en la propia infraestructura hacia Internet. La configuración más habitual en estos casos es permitir toda la comunicación desde dentro para todas las IPs y para todos los puertos de manera que no tengamos ningún tipo de restricción de salida.

La captura siguiente muestra cómo configurar una regla de este tipo:



Origen: (Any), porque permitirá que todos los interfaces conectados al EDGE permitan la Salida.

Destino: (External) Cualquier destino que esté fuera del Edge.

Protocolo: (ANY) Utilizarnos un ANY para permitir TCP/UDC y ICMP.

REGLA DE SALIDA

CONFIGURACIÓN DEL TRÁFICO DE ENTRADA

Este tipo de reglas controlan el modo en que cualquier dispositivo conectado a Internet accede a los servicios alojados en nuestra infraestructura. A diferencia del caso anterior, en este tipo de reglas lo más habitual es permitir exclusivamente el mínimo tráfico necesario para la prestación del servicio. Por ejemplo, para publicar un servidor web alojado en el virtual datacenter, sería necesario configurar una regla que permitiera el acceso al puerto 80 para el protocolo TCP.

La siguiente captura muestra el ejemplo de una regla de filtrado para permitir el acceso desde cualquier origen al servicio de escritorio remoto mediante protocolo RDP (3389/TCP) de un servidor alojado en Cloud Datacenter y publicado en Internet en la dirección IP 176.28.124.98

PERMITIR TODO EL TRÁFICO ENTRANTE

Editar regla de firewall

Habilitada

Nombre: *

Origen: *

Los valores válidos pueden ser dirección IP, CIDR, rango de IPs, "any", "internal" y "external".

Puerto de origen:

Destino: *

Los valores válidos pueden ser dirección IP, CIDR, rango de IPs, "any", "internal" y "external".

Puerto de destino:

Protocolo:

Acción: Permitir Denegar

Registrar tráfico de red para regla de firewall

Aceptar Cancelar

Origen: (Any), porque permitirá que todas las IPs que estén en Internet atravessar nuestro Firewall. Si quieres sólo permitir la conexión desde un origen, como tu oficina, especifica aquí la IP de salida que utilizas desde tus PCs de la oficina.

Puerto origen: Aquí normalmente es un ANY ya que en el inicio de una comunicación la máquina origen siempre utiliza un puerto dinámico para la comunicación y como no sabemos cuál es, utilizamos un ANY.

Destino: La IP pública que especificamos en nuestra regla de NAT. No te confundas con la IP privada.

Puerto Destino: Aquí especificamos el puerto que queremos abrir. En este caso el 3389 para la conexión Terminal Service.

Protocolo: TCP/UDP o ICMP

REGLA DE SALIDA