IPLAN

MANUAL DE CONFIGURACIÓN BÁSICA DE FIREWALL

VIRTUAL DATACENTER IPLAN

Versión: Mayo de 2015

IPLAN

Introducción

En este documento se describe cómo realizar la configuración de las funciones de firewall y otras funciones de seguridad perimetral a través del panel de VMWare vCloud Director.

Esto incluye los servicios de:

- **DHCP**
- **Firewall**
  - **filtrado de reglas,**
  - **traducción de direcciones (IP NAT)**

Consulte en el Manual de usuario de Virtual Datacenter más información sobre cómo utilizar el panel para la gestión del resto de infraestructura cloud.

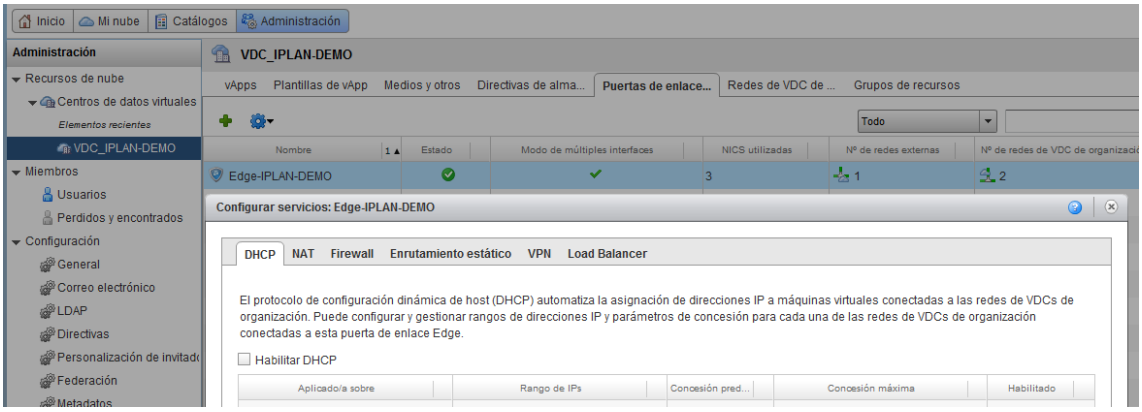
IPLAN

Redes de Organización y Edge Gateway

La implementación de Edge Gateway permite mayor flexibilidad a la hora de configurar interconexión de las distintas redes de un mismo Virtual Datacenter así como la interconexión entre redes internas y redes externas e Internet. Este permite disponer varias redes privadas con direccionamiento IP privado y actuar como puerta de enlace para las redes de organización pudiendo proporcionar servicios adicionales de conectividad.

Un Gateway no puede ser creado por el administrador de organización, tiene que ser creado por el administrador del sistema:

Podrá ver la configuración de Gateway en las propiedades de la organización.



Desde esta pantalla, pueden configurarse las distintas funciones del Gateway

IPLAN

NAT

Existen dos tipos de reglas NAT:

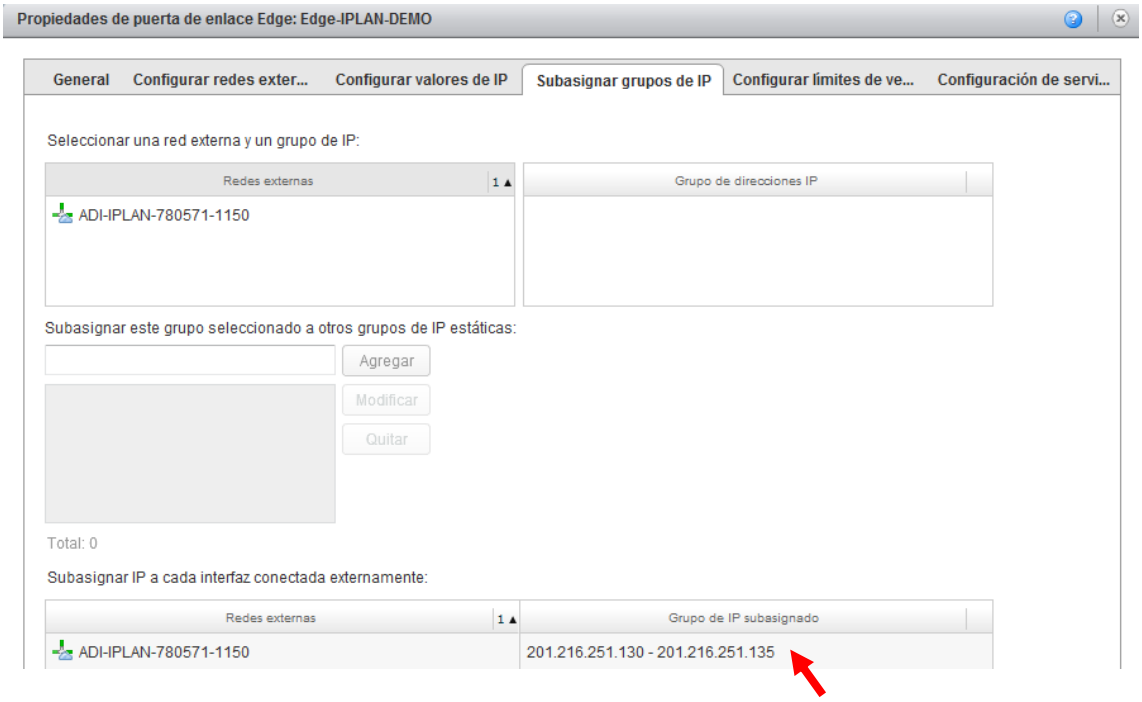
- **SNAT (Source NAT): Esta regla se configura para que una IP o VM tenga salida a Internet y se aplicará siempre sobre la red externa o pata externa del Edge Gateway. Permitirá la salida a Internet con la IP pública que configures en dicha regla de NAT.**

- **DNAT (Destination NAT): Esta permite o posibilita el tráfico entrante a la VM o IP. Puedes permitir el tráfico completo o granularizar hasta el nivel de puerto.**

Es necesario configurar ambas para cada una de las VMs, ya que por defecto las VM no tendrán salida a Internet.

La utilización del direccionamiento público para las patas externas de Edge, debe ser configurado por el administrador del sistema en el Edge y no podrá agregarse o modificarse por parte del usuario de la organización.

Podrá consultar el direccionamiento público que tiene asignado su Edge desde las propiedades del Edge Gateway en la pestaña “Subasignar grupos de IP”

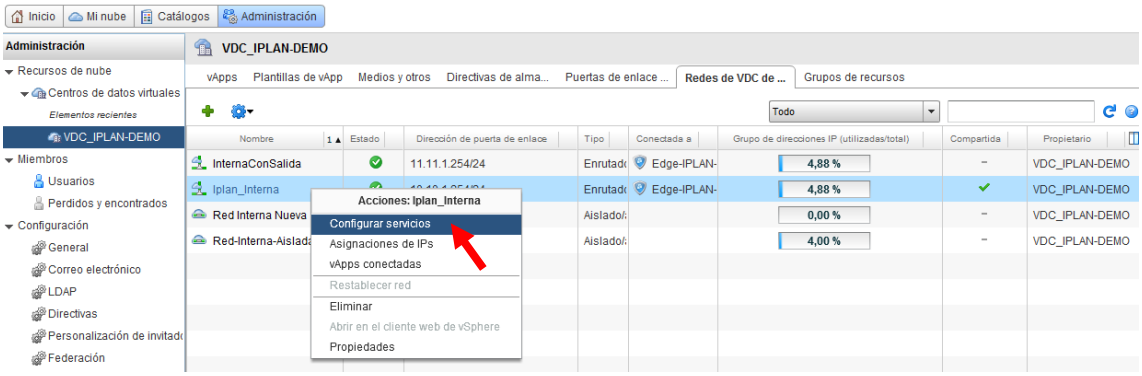


Este será el direccionamiento público que se podrá utilizar.

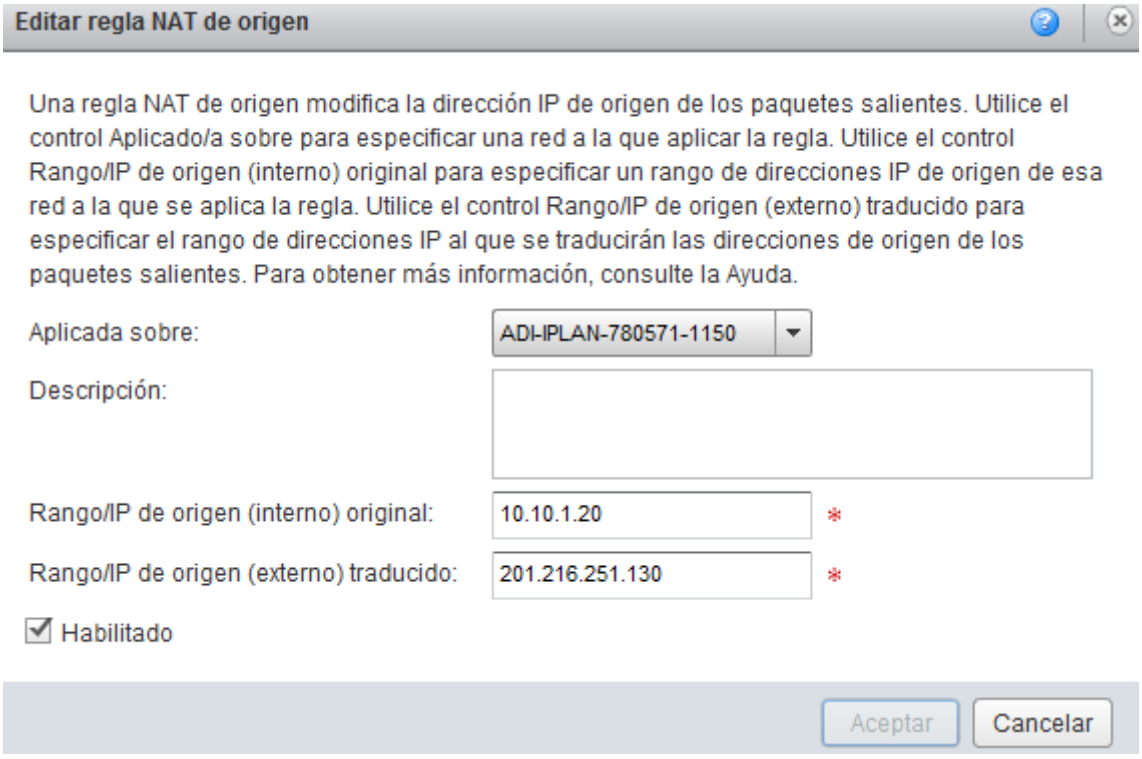
IPLAN

Para configurar la conectividad en una VM se tendrá que configurar dos reglas como mínimo, una SNAT para habilitar el tráfico saliente y un DNAT para habilitar el tráfico entrante.

En el siguiente ejemplo, se va a configurar las dos reglas para una VM a la que se ha agregado a su interface de red una red de organización. Para ello, colocarse sobre la red de organización a la que está conectada la VM y con el botón derecho seleccionar la opción “Configurar Servicios”



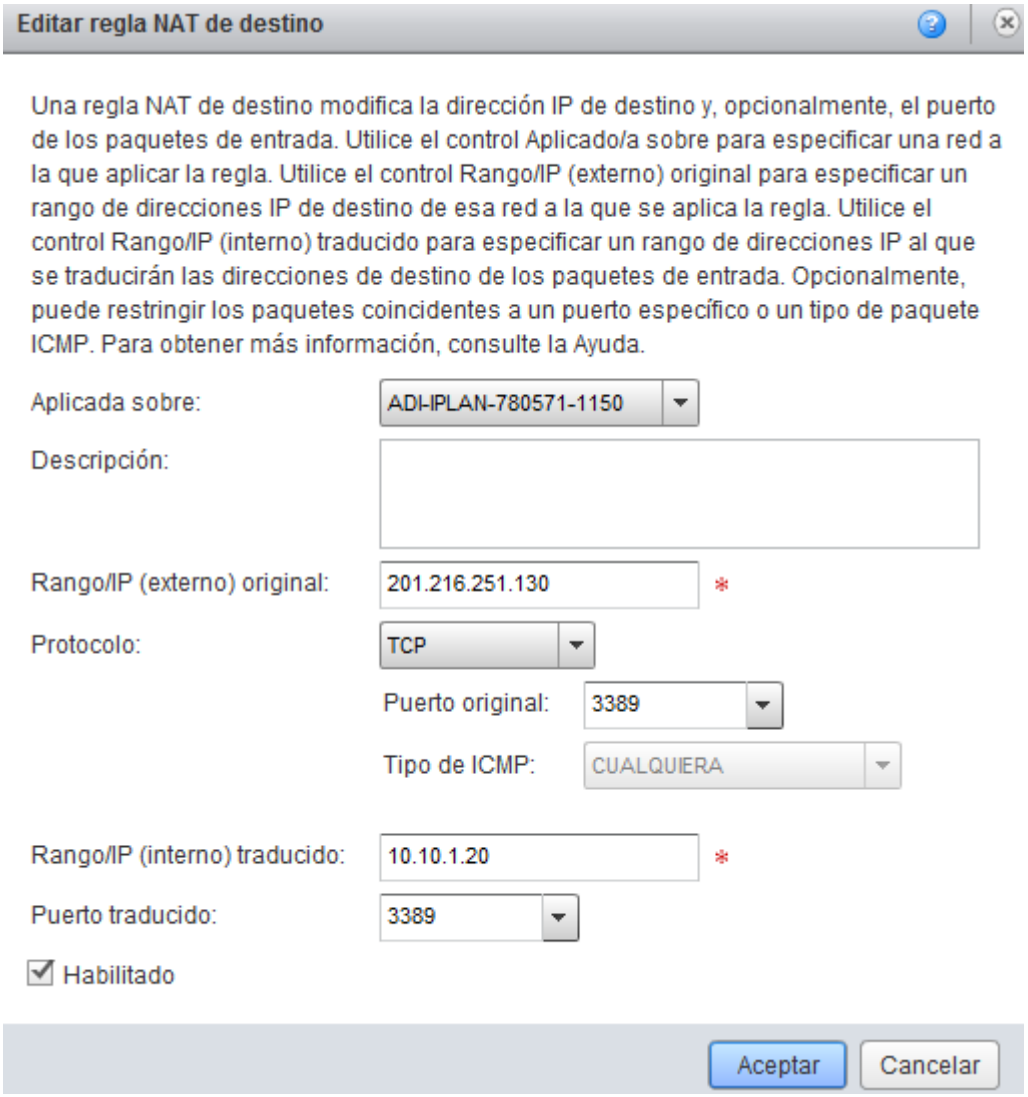
Hacer click en “Agregar SNAT…”, en esta opción tendremos que configurar sobre el interface externo la IP privada que tiene la máquina virtual y la IP pública a la que estará mapeada. De esta manera cuando la VM salga a Internet tendrá la IP de este direccionamiento público.



La dirección IP pública que configure tiene que pertenecer al rango de red que están en la pestaña “Subasignar grupos de IP”.

Ahora se debe configurar una regla NAT Destino. Seleccionar el botón “Agregar DNAT…”, para configurar una regla NAT para que desde la IP púbica se pueda acceder a la IP privada de la máquina virtual haciendo una traslación de IP.

Siempre sobre la pata externa de nuestro Gateway configuraremos por ejemplo el acceso a la VM a través del puerto 3389 de Terminal Service.



Esta configuración permitirá la salida a Internet de la VM con la IP pública 201.216.251.130 y permitirá acceder a la VM a través del puerto 3389 contra la IP 10.10.1.20.

IPLAN

Firewall

Por defecto el tráfico está completamente bloqueado, ni siquiera se podrá hacer ping al Gateway, por lo que si tiene dudas, lo mejor es deshabilitar el Firewall en un primer momento y luego ir habilitando poco a poco hasta dar con las reglas necesarias.

Podrá crear por ejemplo una regla para permitir todo el tráfico y permitirlo por defecto:

En las reglas de Firewall se puede utilizar las palabras: Any, external, internal. Se pueden utilizar configuraciones con redes completas o segmentos de red. Esto nos permite una mayor flexibilidad a la hora de crear reglas.

Crearemos una regla para aceptar el tráfico al puerto 3389 de nuestra IP 201.216.251.130 que hace el NAT a la IP 10.10.1.20. Denegaremos ya el tráfico por defecto y permitiremos todo el tráfico saliente de nuestra VM y sólo permitiremos el 3389 entrante.