

## MANUAL DE CONFIGURACIÓN BÁSICA DE FIREWALL

**VIRTUAL DATACENTER IPLAN** 

Versión: Mayo de 2015



## 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
  - o 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.



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.

👔 Inicio 🔷 Mi nube 🔠 Catálogos 🖏 Administración								
Administración	M VDC_IPLAN-DEMO							
Recursos de nube     vApps Plantillas de vApp Medios y otros Directivas de alma Puertas de enlace Redes de VDC de Grupos de recursos								
Elementos recientes 4 datos virtuales Elementos recientes 4 🐼 🗸								
IN VDC_IPLAN-DEMO	Nombre 1	Estado	Modo de múltiples interfaces	NICS utiliza	adas Nº de redes externa	s Nº de redes de VDC de orga		
✓ Miembros	Sedge-IPLAN-DEMO	0	✓	3	-🖢 1	<u>4</u> 2		
<ul> <li>Perdidos y encontrados</li> <li>Configuración</li> <li>General</li> </ul>	Configurar servicios: Edge-IPLAN-I	DEMO irutamiento está	ático VPN Load Balancer					
Correo electrónico     El protocolo de configuración dinámica de host (DHCP) automatiza la asignación de direcciones IP a máquinas virtuales conectadas a las redes de VDCs de organización. Puede configurar y gestionar rangos de direcciones IP y parámetros de concesión para cada una de las redes de VDCs de organización conectadas a esta puerta de enlace Edge.								
Personalización de invitado Pederación Metadatos	Aplicado/a sobre		Rango de IPs	Concesión pred	Concesión máxima	Habilitado		

Desde esta pantalla, pueden configurarse las distintas funciones del Gateway



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"

General	Configurar redes exter	Configurar valore	es de IP	Subasignar grupos de IP	Configurar límites de ve	Configuración de serv
Selecciona	ar una red externa y un grupo	de IP:				
	Redes externas		1 🔺	Grupo d	le direcciones IP	
👆 ADI-IF	PLAN-780571-1150					
Subasigna	r este grupo seleccionado a (	otros grupos de IP e	estáticas:			
		Agregar				
		Modificar				
Total: 0						
Total: 0	n ID o oo do interfor concetado	autornomanto:				
Total: 0 Subasigna	ar IP a cada interfaz conectada	a externamente:				

Este será el direccionamiento público que se podrá utilizar.



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"

🚮 Inicio l 🛆 Mi nube 📋 Catál	ogos 🛛 🍇 Administración	ı										
Administración	M VDC_IPLAN-DEM	NO										
	vApps Plantillas de	vApp Medios	y otros Directivas de alma.	Pue	rtas de e	nlace Redes	de VDC de	Grupos de recursos				
👻 🕋 Centros de datos virtuales												
Elementos recientes 💠 🌞 🐨						-			C 📀			
The VDC_IPLAN-DEMO	Nombre	1 🔺 Estado	Dirección de puerta de enlac	e i	Тіро	Conectada a	Grupo de dire	cciones IP (utilizadas/total)	Co	ompartida	Propietario	
✓ Miembros	🔔 InternaConSalida	0	11.11.1.254/24	1	Enrutado	Edge-IPLAN-		4,88 %		-	VDC_IPLAN-	DEMO
🔓 Usuarios	🔔 Iplan_Interna		40.40.4.054/04	1	Enrutado	Edge-IPLAN-		4,88 %		×	VDC_IPLAN-	DEMO
🕌 Perdidos y encontrados	👄 Red Interna Nueva	Accione	s: Iplan_Interna		Aislado/:			0.00%		-	VDC IPLAN-	DEMO
- Configuración		Configurar se	rvicios		abradon			0,00 %			100_1 0111	DEMO
🍘 General	🖴 Red-Interna-Aislada	Asignaciones	de IPs	1	Aislado/;			4,00 %		-	VDC_IPLAN-	DEMO
Pcorreo electrónico		vApps conecta	adas 📏									
# LDAP		Restablecer r	ed									
2 Directivas		Eliminar										
······································		Abrir en el clie	nte web de vSphere									
Federación		Propiedades										
6 <b>0</b> 9												

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.

Editar ı	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:	ADI-IPLAN-780571-1150 -	
Descripción:		
Rango/IP de origen (interno) original:	10.10.1.20	*
Rango/IP de origen (externo) traducido:	201.216.251.130	*
✓ Habilitado		
		Aceptar Cancelar

 $(\mathbf{x})$ 



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.

Editar reg	la	NAT	de	destino
------------	----	-----	----	---------

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:	ADI-IPLAN-780571-1	150	•	
Descripción:				
Rango/IP (externo) original:	201.216.251.130		*	
Protocolo:	ТСР 🔻	]		
	Puerto original:	3389	-	
	Tipo de ICMP:	CUALQU	IERA	-
Rango/IP (interno) traducido:	10.10.1.20		*	
Puerto traducido:	3389 💌			
✓ Habilitado				
			Aceptar	Cancelar

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.



## 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:

figurar servicios: Edge-IPLAN-DEMO 🥝								
DHCP NAT Fi	rewall Enrutamie	nto estático VPN Lo	oad Balancer					
Se pueden agregar reglas al firewall para permitir o denegar tráfico de red específico. Para cambiar el orden de las reglas, seleccione una o varias de ellas, arrástrelas y colóquelas en el lugar de la lista que desee. El orden de cualquier regla seleccionada se conserva después de colocarla en otro lugar de la lista.								
Habilitar firewall								
Acción predetermir	nada 💿 Denegar	🔘 Permitir 🔲 Regis	trar					
Se aplica al tráfico qu	e no coincide con las r	eglas de la lista.						
ID de seele	Maarkas	Oriner	Desting	Proto colo	0	Denist	U-billiode	
ib de regia	Nombre	Ongen	Destino	FIOLOCOIO	Addion	Regist	Habiiitado	
1 Tráfico Saliente Any:Any Any:Any CUALQUIERA Permitir -								

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.

Con	onfigurar servicios: Edge-IPLAN-DEMO 🥝 😣								
	DHCP NAT Firewall Enrutamiento estático VPN Load Balancer								
	Se pueden agregar reglas al firewall para permitir o denegar tráfico de red específico. Para cambiar el orden de las reglas, seleccione una o varias de ellas, arrástrelas y colóquelas en el lugar de la lista que desee. El orden de cualquier regla seleccionada se conserva después de colocarla en otro lugar de la lista.								
	🗹 Habilitar firewall								
	Acción predetermin	ada 💿 Denegar	🔘 Permitir 🔲 Regist	rar					
	Se aplica al tráfico que	e no coincide con las re	eglas de la lista.						
	ID de regla	Nombre	Origen	Destino	Protocolo	Acción	Regist	Habilitado	
		RDP_VM1	Any:Any	201.216.251.130:3389	TCP	Permitir	-	×	