

IPLAN

MANUAL DE CONFIGURACIÓN AVANZADA 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:

- **Balanceo de carga**
- **VPN**

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

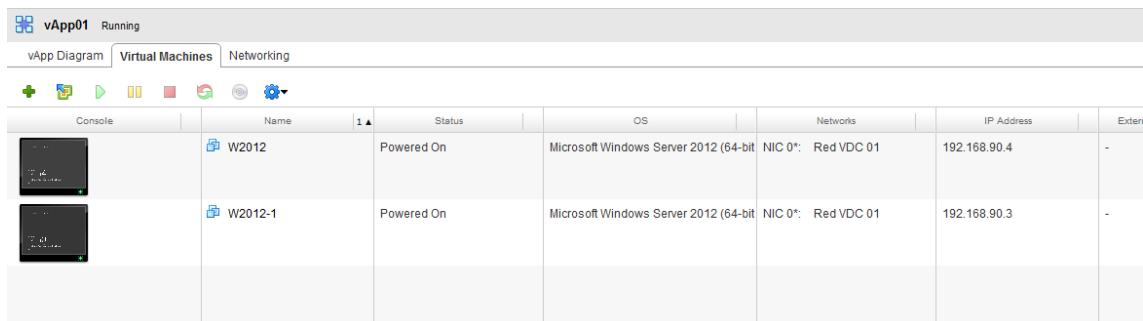
Balanceo de Carga

Esta nueva característica a partir de la versión 5.1 de vCloud Director nos permite crear distintos grupos de tráfico para balancear la carga entre las diferentes MV.



La configuración de esta funcionalidad, se realizará en base a los siguientes conceptos:

- **Pool Servers: Conjunto de servidores que se balancearán y sus propiedades.**
- **Virtual Servers: IP virtual del balanceo y sus propiedades. Esta será la dirección IP en la que se hace público el servicio balanceado.**

Para el ejemplo, tenemos dos servidores conectados a una red de organización.



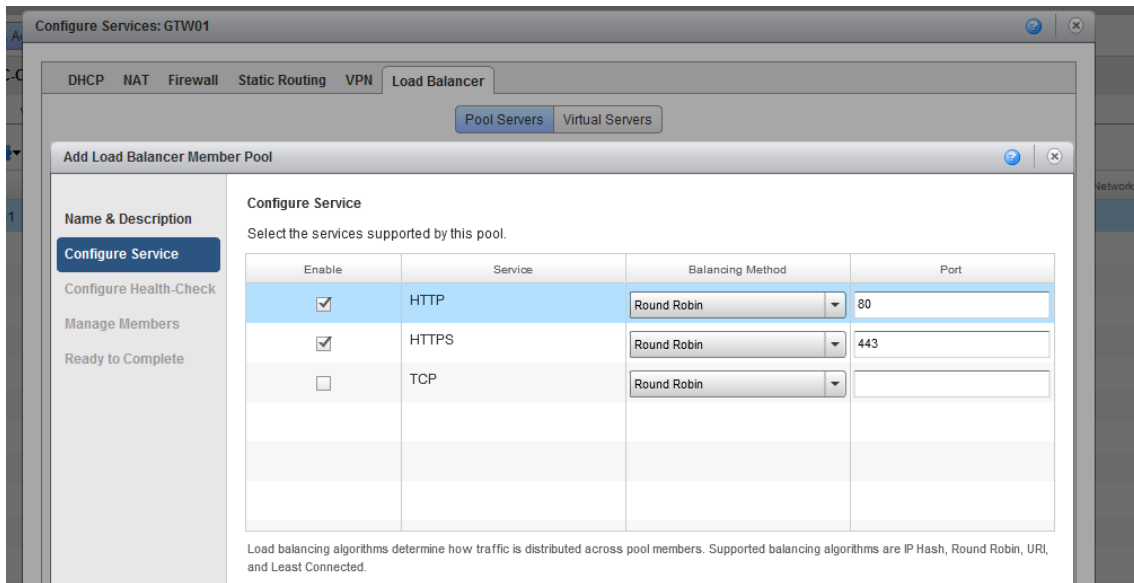
The screenshot shows the vCloud Director interface for a vApp named 'vApp01' in a 'Running' state. The 'Virtual Machines' tab is active, displaying a table with the following data:

Console	Name	Status	OS	Networks	IP Address	Extension
	W2012	Powered On	Microsoft Windows Server 2012 (64-bit)	NIC 0*: Red VDC 01	192.168.90.4	-
	W2012-1	Powered On	Microsoft Windows Server 2012 (64-bit)	NIC 0*: Red VDC 01	192.168.90.3	-

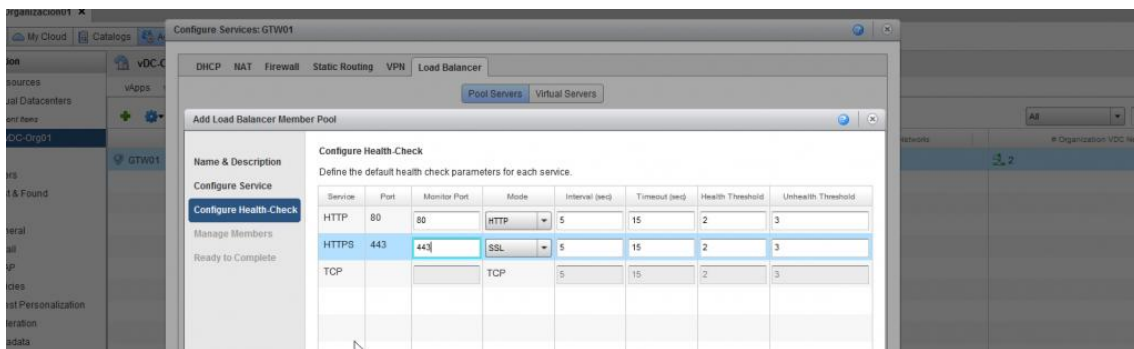
Sobre el Edge Gateway en la pestaña llamada "Load Balance", en la sección "Pool Servers" se creará un nuevo pool de servidores.

IPLAN

Indicar un nombre para el grupo y seleccionar la política de balanceo que se desea para los servidores del grupo.



Configurar los chequeos que se realizan sobre los servidores y el puerto de monitorización.



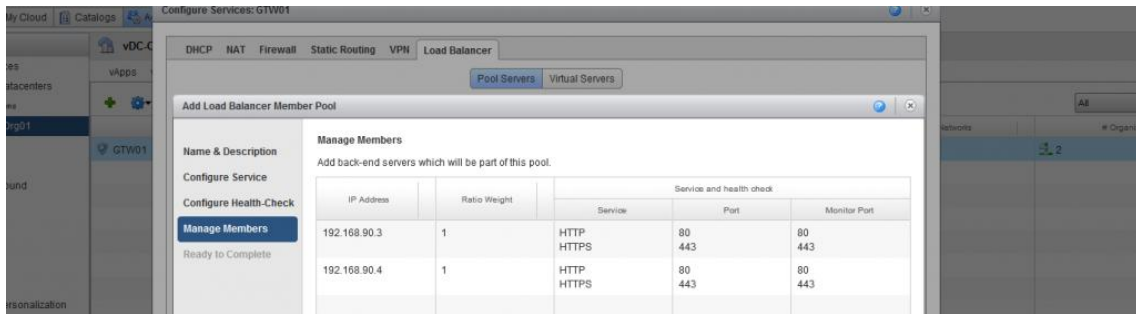
Puede configurar también una URI concreta para monitorizar el servicio:

URI for HTTP service: /

The URI that will be polled at regular intervals to check the health of HTTP service.

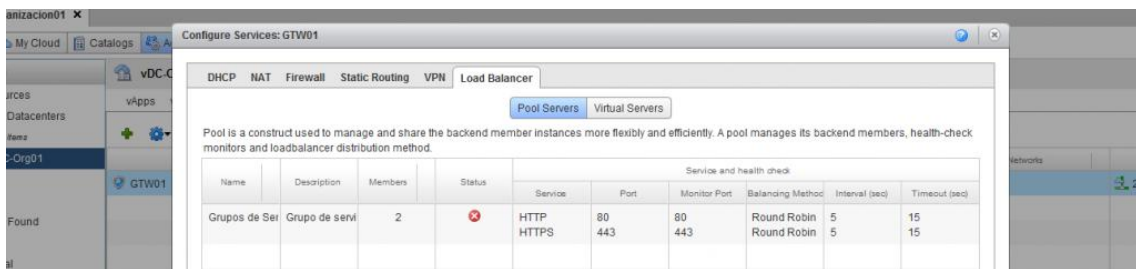
IPLAN

Agregar las IPs privadas de los servidores Web:



Finalizar el asistente.

Comprobar los datos de configuración:

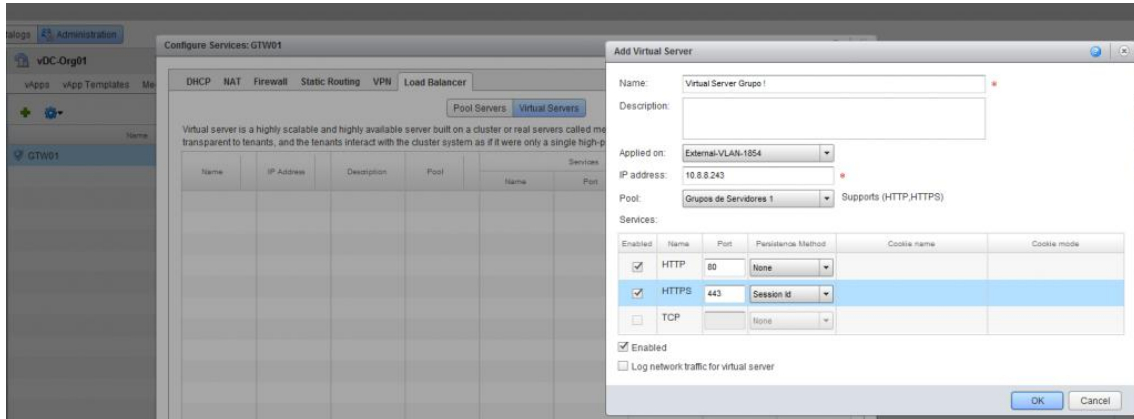


Dar ok para terminar.

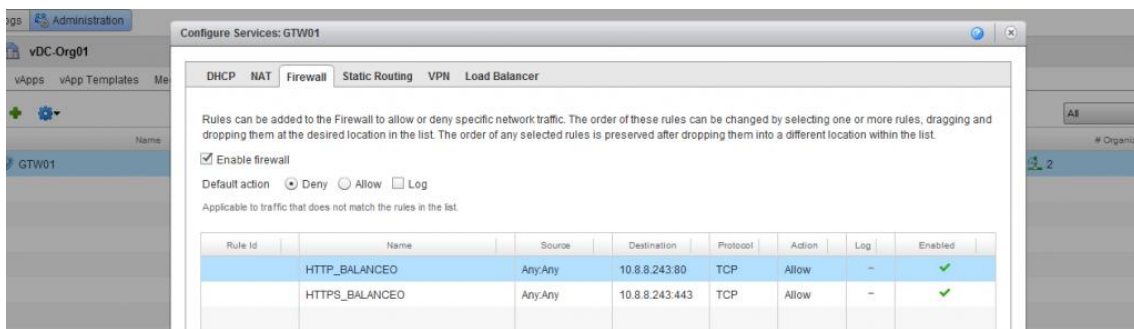
IPLAN

Ahora que ya se tiene configurado el grupo de servidores se debe configurar el virtual Server. Para ello, pulsar en la opción "Virtual Server".

Aquí configuraremos la IP pública y asociaremos el Virtual al grupo de servidores que hemos creado en el paso anterior.



Crear ahora las reglas del Firewall correspondientes:



Ahora se podrá acceder a la IP pública que se ha configurado en el Virtual Server y se podrá ver si se da a F5 para actualizar el explorador como cambia de servidor y hace correctamente el Round Robin

IPLAN

Configuración de túnel VPN para red externa

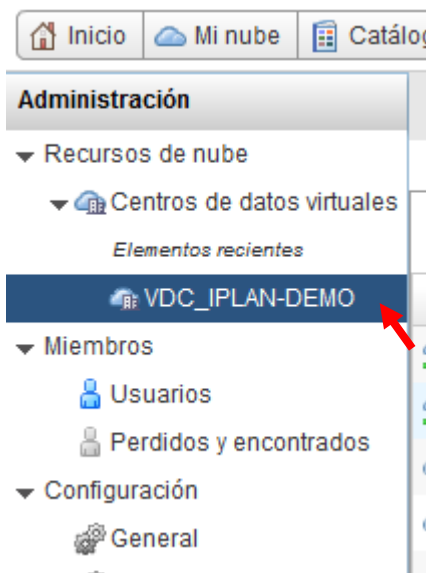
El servicio de Virtual Datacenter incorpora servicio de firewall virtual como dispositivo de seguridad perimetral. Este firewall, entre otras funciones como el filtrado de acceso a servicios instalados en Virtual Datacenter, también ofrece la posibilidad de establecer conexiones de Redes Privadas Virtuales (o VPN) y asegurar así el acceso seguro a los datos y aplicaciones.

En esta sección se explica cómo configurar el servicio necesario para el establecimiento de un túnel IPSec.

Configuración del túnel

La configuración de la VPN se realiza desde el panel de VMWare vCloud Director.

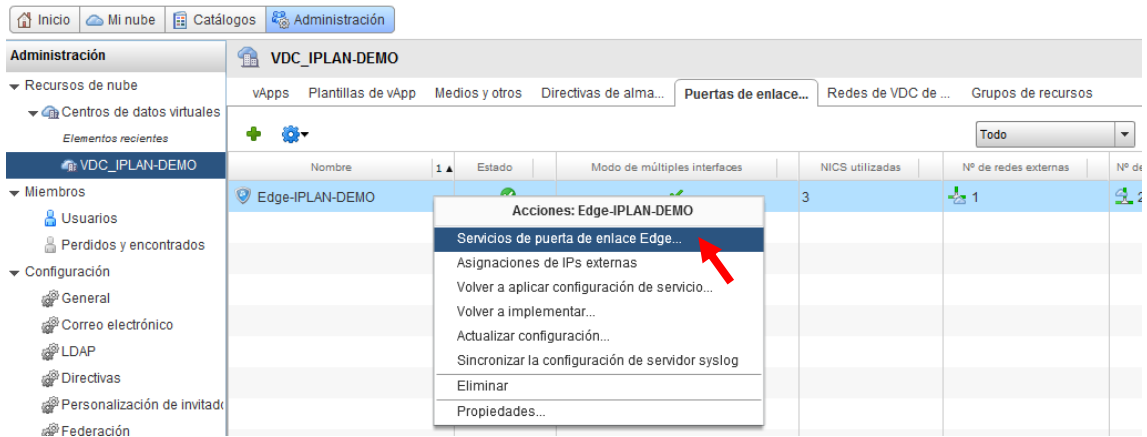
Para acceder a la configuración de nuevos túneles VPNs desde vCloud ir a la pestaña Administración y seleccionar la organización que aparecerá bajo la sección “Centro de datos virtuales”.



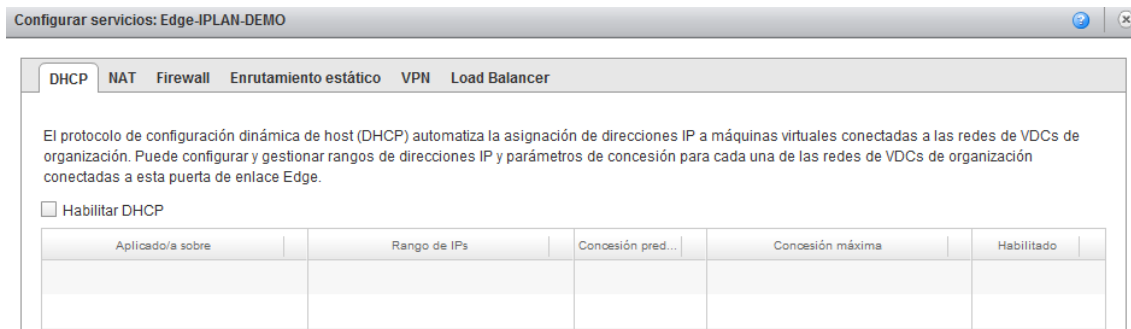
IPLAN

Una vez seleccionado, en la pestaña puerta de enlace (o Edge Gateways según el idioma de su navegador) aparecerá una entrada con el firewall virtual que tenga provisionado.

Para acceder a la configuración del firewall, hacer click con el botón derecho del ratón y seleccionar la primera opción “*Servicios de puerta de enlace Edge...*”



Aparecerá una imagen nueva para la configuración de la funciones de firewall.



IPLAN

Desde la pestaña VPN, se podrá configurar el servicio VPN IPsec que permite crear VPNs seguras entre distintos dispositivos. Recuerde que se pueden configurar VPN de sitio a sitio entre firewalls virtuales y/o dispositivos VPN de terceros fabricantes.

Asegúrese que está marcada la opción 'Habilitar VPN'

El servicio VPN IPsec le ayuda a crear VPNs seguras entre puertos de enlace. Se pueden configurar VPN de sitio a sitio entre puertos de enlace Edge de esta organización, entre organizaciones e incluso en puertos de enlace VPN de terceros.

Habilitar VPN

Configurar IP públicas...

Las IP públicas se pueden configurar para cada una de las redes externas; esto resulta útil cuando se utiliza NAT en el entorno.

Nombre	Punto de acceso l...	Punto de acceso ...	Habilita...	Estado	Red local	Red del mismo ni...	Organización del ...
--------	----------------------	---------------------	-------------	--------	-----------	---------------------	----------------------

Para crear una nueva conexión VPN haz clic en el botón añadir y completar el formulario que aparecerá con los datos de la conexión:

Establecer VPN para: una red remota

Redes locales y de sistemas del mismo nivel

Redes locales:

- InternaConSalida (11.11.1.0/24)
- Iplan_Interna (10.10.1.0/24)

Redes de sistemas del mismo nivel:

Introduzca la dirección de red en formato CIDR. Por ejemplo: 192.168.2.0/24, 192.168.3.0/24.

Configuración de conexión de VPN

Extremo local: ADI-IPLAN-780571-1150

ID local:

ID del mismo nivel:

Redes locales y de sistemas del mismo nivel

ID del mismo nivel:

IP del mismo nivel:

Protocolo de cifrado: AES-256

Clave compartida:

El secreto compartido debe ser una cadena alfanumérica entre 32 y 128 caracteres de longitud y debe incluir al menos una letra mayúscula, una letra minúscula y un dígito.

Mostrar clave

MTU: 1500

Aceptar Cancelar

- Nombre y descripción para identificar el túnel.
- En el campo Establecer VPN para, seleccionar una red remota.
- IP del mismo nivel indica la dirección IP del otro extremo del túnel. Típicamente será la dirección IP pública del dispositivo que sirva como terminador de túneles en el otro extremo de la conexión VPN.
- Protocolo de cifrado. Selecciona el algoritmo de cifrado de entre las opciones disponibles: 3DES / AES / AES-256
- Clave compartida.

IPLAN

En el dispositivo del otro extremo de la VPN se deberá definir los siguientes parámetros IPsec en la configuración del túnel

Primera Fase

- **Protocolo: IKEv1**
- **Modo: Main**
- **Método de autenticación: Preshared Key**
- **Grupo DH: Grupo 2**
- **Algoritmo de cifrado: 3DES / AES / AES-256**
- **Algoritmo de hash: SHA-1**
- **Lifetime: 3600**

Segunda Fase

- **PFS: Activado**
- **Encapsulación: ESP**
- **Algoritmo de cifrado: 3DES**
- **Algoritmo de hash: SHA-1**
- **Lifetime: 3600**

Los únicos datos modificables son el algoritmo de cifrado de la primera fase y la preshared key, el resto de datos tienen que ser los indicados.

Deberá consultar la documentación del fabricante de firewall o router que utilizará en el otro extremo de la conexión para la configuración de éste.